Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Мамчіца Єгора Юрійовича*

академічної групи *125м-22-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методика та заходи вдосконалення процесу управління ризиками інформаційної безпеки комерційного підприємства*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Ковальова Ю.В.			
розділів:				
спеціальний	к.т.н., доц. Ковальова Ю.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту ***Мамчіцу Єгору Юрійовичу*** **академічної групи** ***125м-22-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Методика та заходи вдосконалення процесу управління ризиками інформаційної безпеки комерційного підприємства***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Процес управління ризиками інформаційної безпеки на комерційних підприємствах	02.11.2023
Розділ 2	Інформативні ознаки в процесі управління ризиками інформаційної безпеки та експериментальні дослідження розроблених рішень	16.11.2023
Розділ 3	Економічна частина	30.11.2023

Завдання видано _____ Ковальова Ю.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Мамчіц Є.Ю.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи містить: 102 сторінки, 8 рисунків, 13 таблиць, 4 додатки, 21 посилання.

Мета кваліфікаційної роботи – підвищення рівня інформаційної безпеки шляхом розробки рекомендацій з оптимізації процесу управління ризиками інформаційної безпеки.

Предмет дослідження – інформативні ознаки інформаційної безпеки.

Об'єкт дослідження – процес управління ризиками інформаційної безпеки на комерційних підприємствах.

У роботі проаналізований процес управління ризиками інформаційної безпеки.

У спеціальній частині складений перелік рекомендацій з оптимізації процесу управління ризиками інформаційної безпеки та наведений приклад їх використання.

В економічному розділі проведено розрахунок вартості проєктування та проведення визначення величини ризиків на торгівельному підприємстві та зроблено висновок щодо доцільності проведення визначення величини ризиків на підприємствах.

Наукова новизна полягає у складанні переліку рекомендацій, який допоможе оптимізувати процес управління ризиками інформаційної безпеки.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНИЙ РИЗИК, УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, КОМЕРЦІЙНЕ ПІДПРИЄМСТВО, ІНФОРМАТИВНІ ОЗНАКИ

ABSTRACT

The explanatory note of qualification work consists of: 102 pages, 8 figures, 13 tables, 4 appendices, 21 references.

The purpose of the qualification work is to increase the level of information security by developing recommendations for optimizing the information security risk management process.

The subject of the research is informative signs of information security.

The object of the study is the process of information security risk management at commercial enterprises.

The work analyzes the process of information security risk management.

The special part contains a list of recommendations for optimizing the information security risk management process and an example of their use.

In the economic section, the cost of designing and determining the size of risks at the commercial enterprise was calculated and the conclusion was made regarding the expediency of determining the size of risks at enterprises.

The scientific novelty consists in compiling a list of recommendations that will help optimize the process of information security risk management.

INFORMATION SECURITY, INFORMATION RISK, INFORMATION SECURITY RISK MANAGEMENT, COMMERCIAL ENTERPRISE, INFORMATION SIGNS

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ISO/IEC – International Organization for Standardization/International Electrotechnical Commission;

АС - автоматизована система;

ДСТУ – державні стандарти України;

ІБ – інформаційна безпека;

ІТ – інформаційні технології;

ОІД - об'єкт інформаційної діяльності;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

СМІБ - система менеджменту інформаційної безпеки;

СУІБ – система управління інформаційною безпекою;

СУІР – система управління ризиками інформаційної безпеки.

ЗМІСТ

ВСТУП 8

РОЗДІЛ 1. ПРОЦЕС УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА КОМЕРЦІЙНИХ ПІДПРИЄМСТВАХ 10

1.1 Аналіз процесу управління ризиками інформаційної безпеки 10
1.2 Ризики інформаційної безпеки 25
1.3 Аналіз існуючих комерційних підприємств в Україні 31
1.4 Постановка задачі 34
1.5 Висновки до першого розділу 36

РОЗДІЛ 2. ІНФОРМАТИВНІ ОЗНАКИ В ПРОЦЕСІ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ РОЗРОБЛЕНИХ РІШЕНЬ 37

2.1 Аналіз інформативних ознак на етапі ідентифікації ризику 37
2.2 Аналіз інформативних ознак на етапі встановлення контексту 51
2.3 Аналіз інформативних ознак на етапі оцінки ризику при виборі оптимальної методики 53
2.4 Рекомендації про прийняття рішень на основних етапах моделі процесу УРІБ 61
2.5 Характеристика об'єкта інформаційної діяльності 62
2.6 Побудова моделі порушника для ОІД ТОВ «Еталон-Прилад» 72
2.7 Модель загроз для ОІД ТОВ «Еталон-прилад» та оцінка ризику 74
2.8 Організаційні заходи з управління ризиками інформаційної безпеки ТОВ «Еталон-Прилад» 81
2.9 Висновки до другого розділу 82

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА 84

3.1 Вступ 84
3.2 Розрахунок капітальних витрат 84
3.3 Розрахунок поточних (експлуатаційних) витрат 87
3.4 Оцінка можливого збитку від порушення інформаційної безпеки 89
3.5 Визначення збитку від поломок обладнання 89
3.6 Загальний ефект від впровадження моделі 91
3.7 Визначення та аналіз показників економічної ефективності моделі 92
3.8 Висновок 93

ВИСНОВКИ 94

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 95

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ 98

ДОДАТОК Б. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ 99

ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ 100
ДОДАТОК Г. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ 101

ВСТУП

В сучасному середовищі економіки, інформація, що стосується усіх напрямків діяльності підприємства, стає найбільш цінним і дорогим ресурсом, а проблеми інформаційної безпеки – усе більш складними і практично значущими. Інформаційна безпека є однією зі складових частин економічної безпеки, яка формує модель захищеності підприємства.

В умовах різних форм власності завдання забезпечення інформаційної безпеки повністю лягає на плечі підприємців, керівників організацій, різних комерційних структур. Комерційна діяльність націлена на отримання прибутку – її невід'ємною частиною є прогнозування та врахування всіх ризиків, зокрема інформаційних, а однією зі складових системи управління інформаційною безпекою є управління ризиками інформаційної безпеки.

Наслідком ускладнення інформаційних систем є зростання множини факторів, що впливають на інформаційну безпеку, поява нових процесів, станів і варіантів поведінки в системах та поза їх межами. Тому при створенні надійних, гнучких систем захисту особливої актуальності набуває моделювання.

Одна з головних цілей моделювання в галузі управління ризиками інформаційної безпеки (УРІБ) – побудова алгоритму, який враховував би найбільшу кількість впливових факторів і дозволяв розраховувати ймовірність виникнення вразливості та реалізації загрози, обчислити час реалізації загрози і можливі збитки, визначити ефективність впровадження засобів захисту та ступінь захищеності системи. Визначення показників та обґрунтування кожної інформативної ознаки етапів УРІБ дозволить приймати рішення щодо ІБ системи, тобто управляти ризиками інформаційної безпеки.

Розв'язанням проблеми ефективного управління ризиками інформаційної безпеки є визначення інформативних ознак для алгоритму прийняття рішень, який дозволить спростувати механізм управління ризиками.

Впродовж даної роботи буде розглянутий процес управління ризиками інформаційної безпеки на комерційних підприємствах та будуть визначені інформативні ознаки інформаційної безпеки.

Відмінною рисою даної роботи стане розроблений перелік рекомендацій щодо вибору методики оцінки ризиків інформаційної безпеки на основі аналізу існуючих методик. Такий перелік дасть змогу спеціалісту з інформаційної безпеки вибрати таку методику оцінки ризиків інформаційної безпеки, за допомогою якої можна буде найкращим чином реалізувати процес управління ризиками інформаційної безпеки.

Складання описаного вище переліку ознак допоможе оптимізувати процес управління ризиками інформаційної безпеки на етапах встановлення контексту та оцінки ризиків. У даній роботі не підніматиметься питання оптимізації процесу управління ризиками інформаційної безпеки на етапі обробки ризиків, так як реалізація даного етапу повністю залежить від вибору переліку активів та їх коштовності, котрі являються унікальними для кожного підприємства.

Використання розробленого переліку рекомендацій буде показано на прикладі окремо вибраного підприємства. Ефективність запропонованих у даній роботі рекомендацій буде доведена на основі обробки даних окремо вибраного підприємства.

РОЗДІЛ 1. ПРОЦЕС УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА КОМЕРЦІЙНИХ ПІДПРИЄМСТВАХ

1.1 Аналіз процесу управління ризиками інформаційної безпеки

Розробка і впровадження СУІР - процес досить трудомісткий, що вимагає високого професіоналізму і великого досвіду в управлінні ризиками. Теоретично кожна організація, що починає усвідомлювати свої потреби в забезпеченні інформаційної безпеки, в змозі рухатися по шляху створення СУІР самостійно, однак на практиці багато заходять в глухий кут на цьому шляху. Це відбувається не тільки через нестачу досвіду, професійної кваліфікації та глибини усвідомлення інформаційних ризиків.

Для організацій, в яких інформаційні ризики не є основними, існує варіант віддачі процесу управління ризиками на аутсорсинг спеціалізованій організації. Теоретично аутсорсинг повинен забезпечити скорочення витрат при збереженні достатнього рівня контролю над процесами управління ризиками.

Оцінка ризиків полягає в наступних діях:

- інвентаризація активів;
- ідентифікація бізнес-вимог і вимог законодавства;
- оцінка цінності активів;
- аналіз загроз і вразливостей;
- визначення величини ризику;
- оцінювання і ранжування ризиків.

Рисунок 1.1 – Структура системи управління ризиками

СУІР включає в себе наступні основні групи взаємопов'язаних процесів.

Обробка ризиків:

– вибір способів обробки ризиків і варіантів контрзаходів;
– прийняття рішення щодо контрзаходів;
– реалізація контрзаходів.

Контроль і перегляд:

– аудит і аналіз з боку керівництва;
– оцінка ефективності контрзаходів;
– моніторинг ситуації з ризиком.

Удосконалення:

– реалізація превентивних і корегуючих заходів.

Процеси СУІР:

– оцінка ризиків;
– обробка ризиків;
– контроль і перегляд;
– вдосконалення.

Оскільки процеси управління ризиками є складовою частиною загальної системи управління організації, для їх опису використовується та ж процесна модель, що і в інших стандартах систем управління. Ця модель визначає чотири групи процесів: Планування - Реалізація - Перевірка - Дія (ПРПД), що відображає стандартний цикл управління, вперше описаний в роботах Демінга. У той час як ISO 27001 описує загальний безперервний цикл управління безпекою, в стандартах BS 7799-3 і ISO 27005 міститься його проєкція на процеси управління ризиками. [1]

Рисунок 1.2 – Модель Демінга процесів управління ризиками

Розглянемо проєкцію процесів управління ризиками на процесну модель ПРПД більш детально по кожній групі процесів.

На етапі планування визначаються політика, контекст і методологія управління ризиками, інвентаризуються (ідентифікуються) активи і визначається їх цінність, формулюються профілі загроз і вразливостей, оцінюється ефективність контрзаходів і проводиться обробка ризиків.

Керівництво організації приймає відповідні рішення і затверджує план обробки ризиків, [2].

Згідно ISO 27001, оцінка ризиків інформаційної безпеки необхідна для розуміння вимог інформаційної безпеки та ризиків для бізнес-активів організації.

Вона включає в себе наступні заходи:

– ідентифікація активів;

– ідентифікація вимог законодавства і бізнесу, які можна застосувати до ідентифікованим активам;

– оцінювання активів з урахуванням ідентифікованих вимог законодавства і бізнесу, а також наслідків порушення конфіденційності, цілісності та доступності;

– ідентифікація значущих загроз і вразливостей для активів;

– оцінка ймовірності виникнення загроз і величини вразливостей;

– обчислення ризиків;

– оцінювання ризиків за заздалегідь визначеною шкалою ризику, що була визначена в результаті аналізу, [3].

Наступним кроком в процесі управління ризиками є ідентифікація відповідних заходів по обробці ризиків для кожного з ризиків, ідентифікованих в ході оцінки ризиків. Управляти ризиками можна шляхом комбінування превентивних і детектуючих механізмів контролю, тактики уникнення, страхування та (або) простого прийняття ризику. Після того як ризик був оцінений, має бути прийнято бізнес-рішення щодо вжиття необхідних заходів. У всіх випадках це рішення повинно бути економічно обґрунтованим і зрозумілим для керівників і власників бізнесу, в чию компетенцію входять прийняття або оспорювання даного рішення.

На рисунку 1.3 зображений цикл управління ризиками і показано взаємозв'язок процесів в рамках цього циклу. Процес управління ризиками інформаційної безпеки включає визначення контексту, оцінку ризиків,

обробку ризиків, прийняття ризиків, комунікацію ризиків, а також моніторинг та перегляд ризиків.

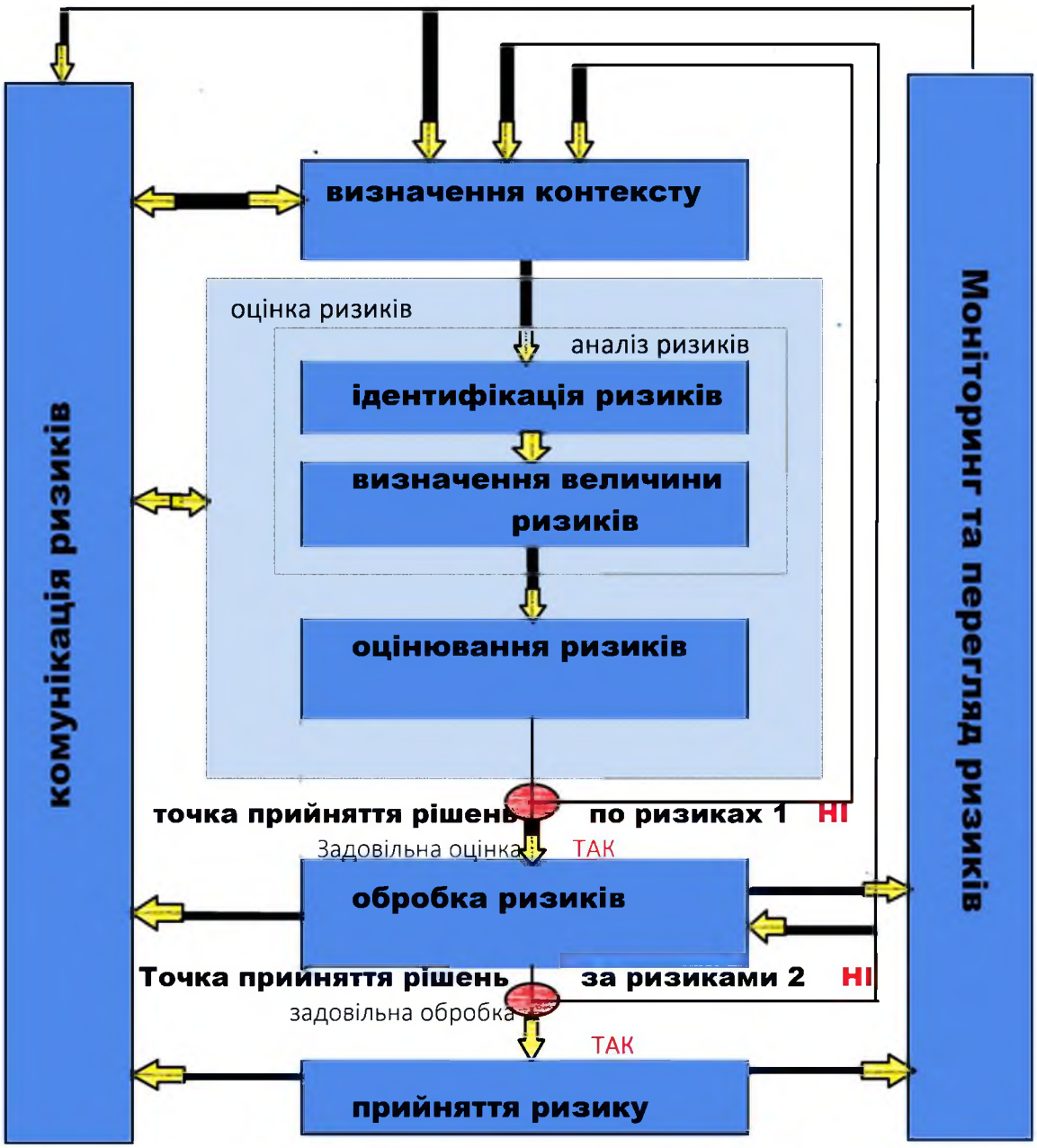

Рисунок 1.3 – Взаємозв'язок процесів управління ризиками

Цей процес може носити циклічний характер для діяльності з оцінки та (або) обробки ризиків. Циклічний підхід до проведення оцінки ризиків дозволяє зробити оцінку більш глибоку і детальну при кожній наступній ітерації. При цьому повинен забезпечуватися баланс між мінімізацією часу і

зусиль, що витрачаються при визначенні механізмів контролю, і забезпеченням належної оцінки високих ризиків.

Спочатку визначається контекст, потім проводиться оцінка ризиків. Якщо в результаті цього отримано достатньо інформації для ефективного визначення заходів, які необхідно вжити для зменшення ризиків до прийнятного рівня, то завдання виконане, і можна переходити до обробки ризиків. Якщо інформації недостатньо, проводиться черговий цикл оцінки ризиків в переглянутому контексті (наприклад, критерії оцінювання ризиків, критерії прийняття ризиків або критерії оцінки впливу (збитку), можливо, для окремих частин області оцінки (рисунок 1.3) - «Точка прийняття рішення по ризикам 1».

Ефективність обробки ризиків залежить від результатів їх оцінки. Можливо, обробка ризиків не призведе одразу ж до прийнятного рівня залишкового ризику. У цьому випадку може знадобитися черговий цикл оцінки ризиків, після чого проводиться додаткова обробка ризиків (рисунок 1.3) - «Точка прийняття рішення за ризиками 2».

Діяльність в сфері прийняття ризиків повинна забезпечувати явне прийняття ризиків керівництвом організації. Це особливо важливо в ситуації, коли впровадження механізмів контролю не провадиться або відкладається, наприклад, через їх високу вартість.

В ході всього процесу управління ризиками інформаційної безпеки важливо, щоб інформація про ризики та їх обробку доводилася до відома відповідних керівників і персоналу. Навіть до початку обробки ризиків інформація про виявлені ризики може виявитися дуже корисною для управління інцидентами і може допомогти зменшити потенційні збитки. Поінформованість менеджерів і персоналу про ризики, характер наявних механізмів контролю, спрямованих на їх зменшення, а також про питання, що викликають стурбованість організації, допомагає врегулювати інциденти і непередбачені події найбільш ефективним чином. Результати по кожній дії в

процесі управління ризиками інформаційної безпеки та точкам прийняття рішень повинні докладно документуватися.

На етапі реалізації проводиться впровадження необхідних механізмів безпеки та інші дії по реалізації плану обробки ризиків, які можуть включати в себе, наприклад, укладення договорів страхування, угод про рівень сервісу і навіть коригування планів розвитку бізнесу з метою уникнення певних ризиків.

Після прийняття рішень по обробці ризиків і впровадження обраних механізмів контролю повинні починатися безперервні дії з управління ризиками. Ці дії включають в себе процес моніторингу ризиків і ефективності СУІБ, це дозволяє гарантувати, що впроваджені механізми контролю функціонують належним чином.

На етапі перевірки відстежується функціонування реалізованих механізмів безпеки, контролюється зміна факторів ризику (активів, загроз, вразливостей), проводяться аудити і виконуються різні контролюючі процедури.

На етапі дії здійснюється вдосконалення процесів управління ризиками за результатами моніторингу та аудиту, в разі необхідності переглядаються певні ризики, які використовуються підходи і методи їх оцінки, вносяться зміни в нормативну і операційну документацію організації, уточнюється контекст управління ризиками. Постійне вдосконалення є суттєвою частиною безперервних дій з управління ризиками, що вживаються з метою підвищення ефективності впроваджених механізмів контролю для досягнення цілей, які були встановлені для СУІБ.

Далі описаний цикл управління ризиками переходить на новий виток, знову проходячи стадії Планування, Реалізації, Моніторингу та Вдосконалення. Процес функціонування, розвитку і вдосконалення СУІР реалізується по спіралі. В кінцевому підсумку всі чотири групи процесів виконуються паралельно і безперервно. Вихідні дані одних процесів надходять на вхід інших.

Систематичне управління ризиками в організації повинно починатися з визначення контексту для управління ризиками, який згідно ISO 27005 включає в себе наступне:

1 Мета управління ризиками. Загальна мета - це підтримка СУІБ, однак для якихось приватних завдань можуть ставитися і більш вузькі цілі, наприклад планування безперервності бізнесу, реагування на інциденти і т.п. [6]

2 Критерії управління ризиками, що включають в себе: критерії оцінки збитку, критерії оцінки ризиків і критерії прийняття ризиків.

3 Область і межі управління ризиками, які зазвичай збігаються з областю дії і межами СУІБ.

4 Організаційну структуру, що визначає функціональні ролі з управління ризиками, обов'язки і розподіл відповідальності.

Контекст управління ризиками полягає у наступному:

– мета;
– критерії;
– область і межі;
– організаційна структура.

Область дії СУІР (область управління ризиками) в ідеалі повинна збігатися з областю дії СУІБ і охоплювати всю організацію. Однак оцінити відразу всі ризики для всіх активів і впровадити СУІР відразу у всій організації досить складно. Тому найчастіше застосовується стратегія поетапного впровадження. У цьому випадку область дії СУІР може охоплювати тільки частину організації.

Аналіз ризиків інформаційної безпеки включає в себе два основних етапи:

– ідентифікація ризиків;
– визначення величини ризиків.

Метою ідентифікації ризику є визначення того, що могло б статися, щоб завдати потенційний збиток, і отримати уявлення про те, як, де і чому міг мати

місце цей збиток. Етапи, описані нижче, повинні збирати вхідні дані для діяльності по кількісній оцінці ризику. Види діяльності, описані нижче, можуть проводитися в різному порядку в залежності від застосовуваної методології.

Ідентифікація ризиків це якась система, яка включає в себе ідентифікацію активів, загроз, вразливостей, наслідків та існуючих засобів контролю. Активом є щось, що має цінність для організації і, отже, потребує захисту. При ідентифікації активів слід мати на увазі, що інформаційна система складається не тільки з апаратних і програмних засобів.

Її слід здійснювати на відповідному рівні деталізації, що забезпечує достатню інформацію для оцінки ризику. Рівень деталізації, який використовується при ідентифікації активів, впливає на загальний обсяг інформації, зібраної під час оцінки ризику. Цей рівень може бути більш деталізований при подальших ітераціях оцінки ризику.

Для кожного активу повинен бути визначений власник, щоб забезпечити компетентність і відповідальність за кожен актив. Власник активу може не мати права власності на актив, але він несе відповідну відповідальність за його отримання, розробку, підтримку, використання і безпеку. Найчастіше власник активу є найбільш підходящим особою, яка спроможна визначити реальну цінність активу для організації.

Кордоном перегляду є периметр активів організації, що підлягає менеджменту за допомогою процесу ризик-менеджменту інформаційної безпеки.

Загроза має потенціал заподіяння шкоди активам, таким як інформація, процеси і системи. Загрози можуть бути природного походження або від дій людей, вони можуть бути випадковими або навмисними. Повинні бути ідентифіковані і випадкові, і навмисні джерела загроз. Загроза може виникати як із самої організації, так і поза її межами. Загрози повинні ідентифікуватися взагалі і по виду (наприклад, неавторизовані дії, фізичний збиток, технічні збої), а потім, де це доречно, окремі загрози ідентифікуються всередині

родового класу. Це означає, що жодна загроза, включаючи несподівані, не буде упущена, але обсяг необхідної роботи, незважаючи на це, обмежений.

Деякі загрози можуть впливати більш ніж на один актив. У таких випадках вони можуть бути причиною різних впливів, в залежності від того, на які активи вони впливають.

Вхідні дані для ідентифікації та вимірювання ймовірності виникнення загроз можуть бути отримані від власників активів або користувачів, персоналу відділу кадрів, керівництва організації та фахівців у сфері ІБ, експертів у сфері фізичної безпеки, юридичного відділу та інших структур, включаючи правові органи, метеорологічні служби, страхові компанії, національні урядові установи. При розгляді загроз повинні враховуватися аспекти середовища і культури.

Внутрішній досвід, отриманий в результаті інцидентів, і минулі оцінки загроз повинні бути враховані в поточній оцінці. Може бути використаний в інших реєстрах загроз (можливо, специфічних для організації або бізнесу), щоб заповнити перелік спільних загроз, де це має значення. Реєстри та статистику загроз можна отримати від промислових організацій, національних урядів, правових органів, страхових компаній тощо.

Використовуючи реєстри загроз або результати колишніх оцінок загроз, не слід забувати про те, що відбувається постійна зміна значущих загроз, особливо, якщо змінюються бізнес-середовище або інформаційні системи.

Ідентифікація існуючих засобів контролю повинна бути зроблена, щоб уникнути непотрібну роботу або витрати, наприклад, при дублюванні засобів контролю. Крім того, під час ідентифікації існуючих засобів контролю слід провести перевірку, щоб упевнитися, що засоби контролю функціонують правильно - посилання на вже існуючі звіти по аудиту СМІБ повинні обмежувати час, що витрачається на цю задачу. Якщо засоби контролю не працюють, як очікувалося, це може стати причиною вразливості. Слід приділити увагу ситуації, коли вибрані засоби контролю (або стратегія) відмовляються працювати і тому потрібні додаткові засоби контролю для

ефективного розгляду ідентифікованого ризику. У СМІБ, відповідно до ISO / IEC 27001, це підтримується виміром ефективності засобів контролю. Одним із способів кількісно оцінити дію засобів контролю - подивитися, як воно зменшує ймовірність загрози і простоту використання уразливості або вплив інциденту. Перегляди, здійснювані менеджерами і звіти з аудиту, також забезпечують інформацію про ефективність існуючих засобів контролю.

Засіб контролю, який планується реалізувати у відповідності з планами реалізації обробки ризику, повинен враховуватися тим же самим способом, який вже був реалізований.

Засіб контролю, що існує або планується, може ідентифікуватися як неефективний або недостатній, або необґрунтований. Якщо його порахували необґрунтованим або недостатнім, засіб контролю необхідно перевірити, щоб визначити чи варто його видалити, замінити його іншим, більш відповідним, або варто залишити його на місці, наприклад, за вартісними причинами.

Для ідентифікації існуючих або планованих засобів контролю можуть бути корисні наступні заходи:

1 Перегляд документів, що містять інформацію про засоби контролю (наприклад, плани обробки ризиків). Якщо процеси менеджменту інформаційної безпеки задокументовано належним чином, то всі існуючі або плановані засоби контролю і стан їх реалізації повинні бути доступні.

2 Перевірка разом з людьми, які відповідають за інформаційну безпеку (наприклад, службовець, який займається забезпеченням інформаційної безпеки, службовець, відповідальний за безпеку інформаційної системи, комендант будівлі або керівник робіт) і користувачами, які засоби контролю дійсно реалізовані для розглянутого інформаційного процесу або інформаційної системи.

3 Обхід будівлі з проведенням огляду фізичних засобів контролю, порівняння реалізованих засобів контролю з переліком тих, які повинні бути, і перевірка реалізованих засобів контролю на предмет правильної і ефективної роботи.

4 Розгляд результатів внутрішніх аудитів.

Вразливості можуть бути ідентифіковані в наступних областях:

– організація робіт;
– процеси і процедури;
– сталі норми управління;
– персонал;
– фізичне середовище;
– конфігурація інформаційної системи;
– апаратні засоби, програмне забезпечення та апаратура зв'язку;
– залежність від зовнішніх сторін.

Наявність вразливості не завдає шкоди сама по собі, так як необхідна наявність загрози, яка скористається нею. Вразливість, яка не має відповідної загрози, може не вимагати впровадження засобів контролю, але повинна усвідомлюватися і піддаватися моніторингу на предмет вимірювань. Слід зазначити, що невірно реалізований або неправильно функціонуючий засіб контролю або засіб контролю, який неправильно використовується, сам може бути вразливістю. Засіб контролю може бути ефективним чи неефективним в залежності від середовища, в якому він функціонує. І навпаки, загроза, яка не має відповідної уразливості, може не призводити до ризику.

Повинні бути ідентифіковані наслідки для активів, які можуть бути результатом втрати конфіденційності, цілісності та доступності. Наслідком може бути втрата ефективності, несприятливі операційні умови, втрата бізнесу, збиток, нанесений репутації тощо.

Ця діяльність ідентифікує шкоду для організації або наслідки для організації, які можуть бути обумовлені сценарієм інциденту, що надається загрозою, що використовує певну вразливість в інциденті ІБ. Вплив сценаріїв інцидентів слід визначати, використовуючи критерії впливу, певні протягом діяльності, пов'язаної з встановленням контексту. Він може торкнутися одного або більше активів, або частину активу. Тому активам може призначатися цінність в залежності від їх фінансової вартості і через наслідки для бізнесу в

разі їх псування або компрометації. Наслідки можуть бути тимчасовими або постійними, як у випадку руйнування активів.

В ISO / IEC 27001 описується походження сценаріїв інцидентів, як "недоліків безпеки". Організації повинні визначати операційні наслідки сценаріїв інцидентів на основі:

– часу на розслідування і відновлення;
– втрат (робочого) часу;
– втрачену можливість;
– охорони праці та безпеки;
– фінансових витрат на специфічні навички, необхідні для усунення несправності;
– репутації і іншого "невловимого капіталу".

Оцінка ризику полягає у визначенні його рівня (якісної або кількісної величини) і порівняння цього рівня з максимально допустимим (прийнятним) рівнем, а також з рівнем інших ризиків.

Рівень ризику визначається шляхом комбінування двох величин: ймовірності події та розмірів його наслідків. Подія полягає в реалізації загрози, що використовує уразливість активу для впливу на цей актив і порушення його безпеки.

Під безпекою інформаційного активу розуміються такі властивості інформації, як конфіденційність, цілісність і доступність. Для спрощення подальшого викладу слід розглядати тільки цю класичну тріаду інформаційної безпеки, хоча до інформаційної безпеки відносять також, принаймні, ще автентичність і неспростовності.

Додаткові «вимірювання» інформаційної безпеки необхідні для встановлення підзвітності користувачів за дії, вчинені ними в інформаційних системах. Наприклад, деякі зловмисні або помилкові дії, що здійснюються у фінансовій сфері, можуть бути безпосередньо не пов'язані з порушенням конфіденційності, цілісності або доступності будь-якої інформації.

Порушення безпеки активу зазвичай завдає шкоди організації. Величина цього збитку визначає цінність активу для організації.

Оцінка ризику включає ідентифікацію та оцінку цінності активів, наслідків для бізнесу, ідентифікацію та оцінку загроз і вразливостей, а також комбінування цих факторів для визначення рівня ризику в кількісних і якісних величинах, як показано на рисунку 1.4.

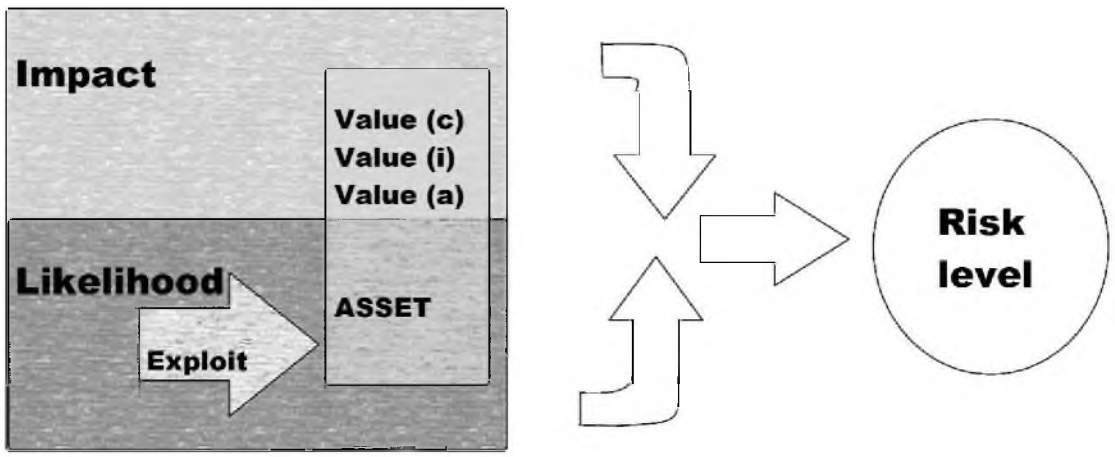

Рисунок 1.4 – Взаємозв'язок активу з рівнем ризику

Після отримання результатів оцінки ризику та отримання задовільної оцінки підприємство переходить до етапу обробки ризику, а саме виробляє подальшу роботу над ризиком, отриманим в результаті роботи.

Як показано на рис.1.5, можна виділити наступні варіанти обробки ризику, а саме:

1 Уникнення ризику - рішення не брати участі в ситуації, пов'язаної з ризиком, або дія, спрямована на вихід з неї [ISO Guide 73: 2002].

2 Зменшення ризику - заходи, що вживаються для зниження ймовірності або негативних наслідків, пов'язаних з ризиком, або того й іншого [ISO / IECGuide73: 2002].

3 Збереження (прийняття) ризику - прийняття тягаря збитку або витягується вигоди від конкретного ризику [ISO / IECGuide73: 2002].

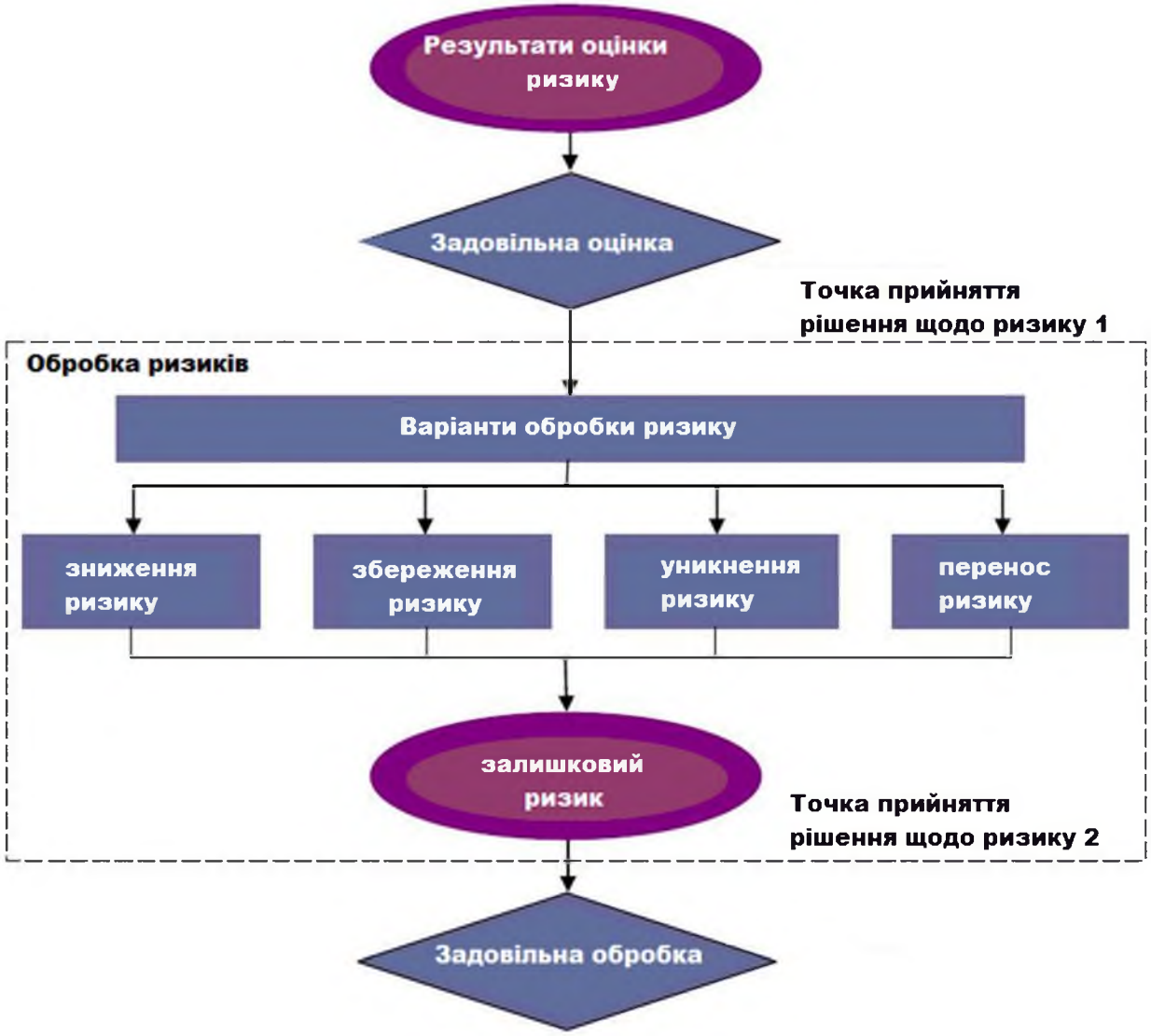

Рисунок 1.5 – Обробка ризиків інформаційної безпеки

Передача ризику - поділ з іншою стороною тягаря збитку або витягується вигоди, пов'язаної з ризиком (ISO / IECGuide73: 2002).

Модель процесу управління ризиками ІБ циклічна. Її циклічність обумовлюється тим, що незалежно від результату обробки ризику (ризик буде прийнятий або не прийнятий), буде розпочато нову ітерацію в силу того, що рівень ризику непостійний і з часом може змінюватися.

1.2 Ризики інформаційної безпеки

Перш за все, необхідно максимально повно і точно визначити поняття ризику. У BS 7799-3 дається найбільш широке визначення ризику як комбінації ймовірності події та її наслідків. ISO 27005 конкретизує поняття інформаційного ризику, розкладаючи його на активи, загрози, вразливості і збитки. Згідно ISO 27005: «Ризик інформаційної безпеки - це потенційна можливість використання вразливостей активу або групи активів конкретної загрози для заподіяння шкоди організації». Розглянемо інші визначення поняття «інформаційний ризик»:

- ризик - комбінація ймовірності події та її наслідків (BS 7799-3: 2006);
- ризик - невизначеність, що припускає можливість втрат (збитків);
- ризик - потенційна проблема;
- ризик - ймовірні втрати організації в результаті інцидентів.

Поняття ризику, дане в ISO 27005, мабуть, є найбільш повним. Ризик є комплексною величиною, завжди визначається через комбінацію ряду інших величин. Це обумовлює помилки у визначенні та описі конкретних ризиків, які нерідко допускаються навіть фахівцями, що викликає труднощі при оцінці ризиків.

Опис факторів ризику, таких як загрози, інциденти, уразливості і види шкоди, окремо не є описом ризику. За визначенням, яке в рекомендаціях ДСТУ ISO 15408 [2], ризик - це ймовірність реалізації загрози інформаційній безпеці. У класичному поданні оцінка ризиків включає оцінку загроз, вразливостей і завдання шкоди. У зв'язку з цим виникають наступні питання. Про ризик можна говорити тільки в тому випадку, якщо всі фактори ризику розглядаються у сукупності. Тільки комбінація оцінних значень для погроз, вразливостей і збитку дозволяє отримати оцінку ризику.

Отже, якщо ми хочемо з'ясувати види ризиків ІБ, нам необхідно провести класифікацію загроз і аналізу шкоди, який може бути нанесений

інформації. Загроза інформаційної безпеки - сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки.

Усі можливі потенційні загрози за природою їх виникнення поділяються на два класи: природні (об'єктивні) і штучні (суб'єктивні).

Рисунок 1.6 – Класифікація загроз за джерелами і мотивацією

Природні загрози - це загрози, викликані впливами на АС і її елементи об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

Штучні загрози - це загрози АС, викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна виділити:

– ненавмисні (ненавмисні, випадкові) загрози, викликані помилками в проєктуванні АС і її елементів, помилками в програмному забезпеченні, помилками в діях персоналу і ін.. ;

– навмисні (навмисні) загрози, пов'язані з корисливими, ідейними чи іншими прагненнями людей (зловмисників).

Штучні загрози, які в свою чергу, діляться на ненавмисні і навмисні загрози. Ненавмисні загрози - це дії, які здійснюють люди з необережності, незнання, неуважність або з цікавості. До такого типу загроз відносять установку програмних продуктів, які не входять до списку необхідних для роботи, і в наслідку можуть стати причиною нестабільної роботи системи і втрата інформації. Сюди ж можна віднести і інші «експерименти», які не були злими намірами, а люди, які здійснювали їх, не усвідомлювали наслідків. На жаль, цей вид погроз дуже важко піддається контролю, мало того, щоб персонал був кваліфікований, необхідно щоб кожна людина усвідомлювала ризик, який виникає при його несанкціонованих діях. До основних ненавмисним штучним загрозам можна віднести:

– ненавмисні дії, що призводять до часткової або повної відмови системи або руйнування апаратних, програмних, інформаційних ресурсів системи (ненавмисна псування устаткування, видалення, спотворення файлів з важливою інформацією або програм, в тому числі системних тощо);

– неправомірне відключення обладнання або зміна режимів роботи пристроїв та програм;

– ненавмисне псування носіїв інформації;

– запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання або зациклення) або здійснюють незворотні зміни в системі (форматування або реструктуризацію носіїв інформації, видалення даних тощо);

– нелегальне впровадження та використання неврахованих програм (ігрових, навчальних, технологічних та ін.) з подальшою необґрунтованою витратою ресурсів (завантаження процесора, захоплення оперативної пам'яті і пам'яті на зовнішніх носіях);

– зараження комп'ютера вірусами;

– необережні дії, що призводять до розголошення конфіденційної інформації, або роблять її загальнодоступною;

– розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, перепусток тощо);

– проєктування архітектури системи, технології обробки даних, розробка прикладних програм, з можливостями, що представляють небезпеку для працездатності системи і безпеки інформації;

– ігнорування організаційних обмежень (установлених правил) при роботі в системі;

– вхід в систему в обхід засобів захисту (завантаження сторонньої операційної системи зі змінних магнітних носіїв тощо);

– некомпетентне використання, настроювання або неправомірне відключення засобів захисту персоналом служби безпеки;

– пересилання даних за помилковою адресою абонента (пристрої);

– введення помилкових даних;

– ненавмисне пошкодження каналів зв'язку.

Статистика показує, що більшість загроз відбувається власними співробітниками організації, в той час як частка зовнішніх загроз порівняно мала, як показано на рис. 1.7.

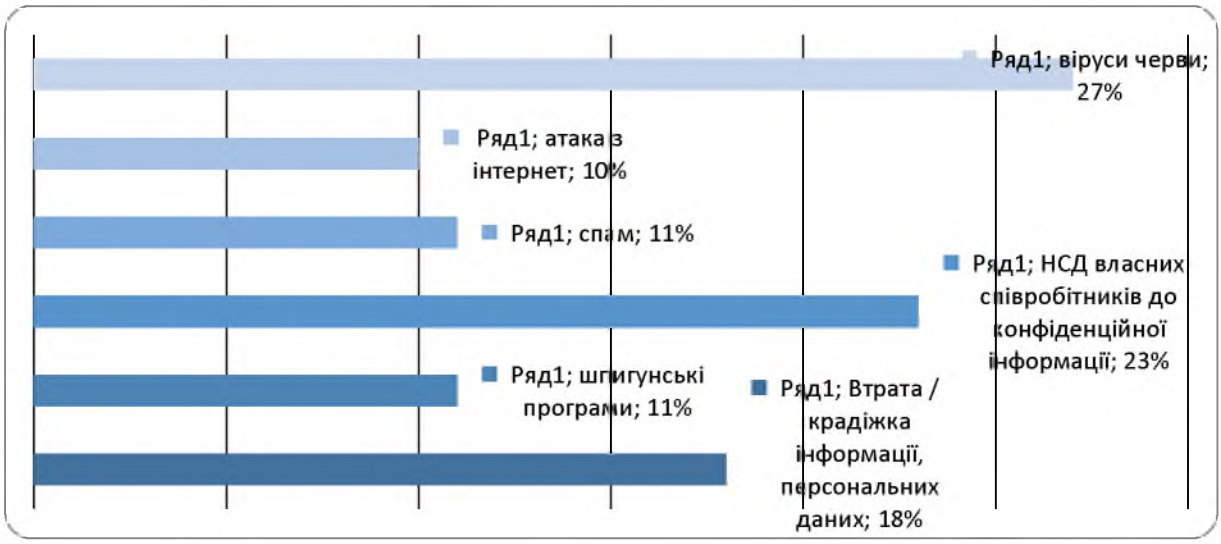

Рисунок 1.7 – Статистика загроз інформаційної безпеки

Найчастішими і небезпечними за розмірами шкоди є ненавмисні помилки користувачів інформаційних систем. Особливу небезпеку становлять

«скривджені співробітники», дії яких пов'язані з бажанням завдати шкоди організації. Такими можуть виявитися як нинішні, так і колишні співробітники. Тому необхідно стежити за тим, щоб при звільненні працівника його доступ до інформаційних ресурсів припинився.

Навмисні загрози ІБ, пов'язані зі злим умислом навмисного фізичного руйнування, згодом виходу з ладу системи. До навмисних загроз відносяться внутрішні і зовнішні атаки. Всупереч поширеній думці, великі компанії зазнають багатомільйонних втрат часто не від хакерських атак, а з вини своїх же власних співробітників (інсайдерів).

До зовнішніх навмисних загроз можна віднести загрози хакерських атак. Якщо інформаційна система пов'язана з глобальною мережею інтернет, то для запобігання хакерських атак необхідно використовувати міжмережевий екран (так званий firewall), який може бути, як вбудований в обладнання, так і реалізований програмно.

Таким чином, можна зробити висновок про те, що дія загроз інформаційній безпеці об'єкту спрямовано на створення можливих каналів витоку інформації, що захищається (передумов до її витоку) і безпосередньо на витік інформації. Одне з ключових понять в оцінці ефективності прояви загроз об'єкту інформаційної безпеки - збиток, що наноситься цьому об'єкту (підприємству) в результаті впливу загроз.

За своєю суттю будь-який збиток, його визначення та оцінка мають яскраво виражену економічну основу. Не є винятком і збиток, що наноситься інформаційній безпеці об'єкта (підприємства).

З позиції економічного підходу загальний збиток інформаційної безпеки підприємства складається з двох складових частин: прямого і непрямого збитку.

Прямий збиток інформаційної безпеки підприємства виникає внаслідок витоку конфіденційної інформації. Непрямі збитки - втрати, які несе підприємство в зв'язку з обмеженнями на поширення інформації, в установленому порядку віднесеної до категорії конфіденційної.

Опис шкоди, що завдається підприємству в результаті витоку конфіденційної інформації, ґрунтується на його кількісних і якісних показниках, які базуються на одному з принципів засекречування інформації (віднесення її до категорії конфіденційної) - принципі обґрунтованості. Він полягає у встановленні (шляхом експертних оцінок) доцільності засекречування конкретних відомостей (віднесення інформації, що міститься в них до конфіденційної), а також можливих наслідків цих дій, з урахуванням розв'язуваних підприємством задач і поставлених цілей.

Введення обмежень на поширення інформації (в зв'язку з її засекречуванням або віднесенням до категорії конфіденційної) призводить і до позитивних, і до негативних наслідків. До основних позитивних наслідків слід віднести запобігання можливого прямого збитку інформаційної безпеки підприємства через витік інформації, що захищається. Негативні наслідки пов'язані з наявністю (ймовірним зростанням) непрямих збитків або витрат у вигляді витрат на захист інформації та величини упущеної вигоди, яка може бути отримана при її відкритому поширенні.

Найважливішою частиною оцінки збитку безпеки підприємства від витоку конфіденційної інформації є проведення класифікації всіх наявних на підприємстві відомостей за ступенем їх важливості. З цією метою методом експертної оцінки з залученням фахівців структурних підрозділів підприємства, що беруть участь у виконанні робіт з різних напрямків його діяльності, розробляють єдину шкалу відомостей, які містять конфіденційну інформацію - так званий рейтинг важливості інформації. У рейтингу відображаються всі відомості, включені до переліків інформації, що підлягає захисту.

Методичною основою для розробки такого рейтингу є метод експертного аналізу в сукупності з методом об'єктивного кількісного оцінювання. На основі рейтингу важливості інформації зіставляють (співвідносять) включені в нього відомості з кількісними показниками можливого збитку, який визначається розрахунковим або експертним шляхом.

Все вищеописане показує, що визначення ризиків інформаційної безпеки є комплексною схемою визначення загроз інформаційній безпеці і аналізу шкоди, а на їх основі - самих ризиків.

1.3 Аналіз існуючих комерційних підприємств в Україні

Аналіз інформативних ознак є основною складовою управління ризиками інформаційної безпеки. Чітке розуміння того, які ознаки впливають на процес УРІБ на кожному його етапі, дозволяє більш повно використовувати потенціал процесу УРІБ. Інформативні ознаки можуть відрізнятися в залежності від обраного випадку використання моделі УРІБ, але сам набір цих ознак залишається незмінним у всіх випадках.

Інформативна ознака - особливість предмета або явища (в нашому випадку предметом є комерційне підприємство), що забезпечує вербалізовану організацію знань, їх осмислення, передавання та кодування і визначає подібність свого носія до інших об'єктів або відмінність від них. Сукупність ознак дозволяє відрізнити предмет від інших предметів.

Підприємство - це самостійно господарюючий суб'єкт, створений (заснований) відповідно до чинного законодавства для виробництва продукції, виконання робіт або надання послуг з метою задоволення суспільних потреб і отримання прибутку.[9]

Підприємства можна класифікувати за багатьма ознаками. Найбільш істотні наступні фактори класифікації підприємств:

- використовувані ресурси;
- галузева приналежність;
- місце розташування;
- розмір підприємства;
- форма власності;
- організаційно-правова форма.

Відповідно до особливостей використовуваних ресурсів підприємства діляться на такі, що:

– використовують в основному трудові ресурси (трудомісткі);

– інтенсивно використовують засоби виробництва (фондоємні);

– інтенсивно використовують матеріали (матеріаломісткі).

Для трудомістких підприємств характерна висока частка витрат на оплату праці в сукупних витратах виробництва. Ці підприємства, як правило, мають високу ступінь поділу праці. Поділ праці має позитивні і негативні наслідки, [10].

Фондоємні підприємства мають особливо велику кількість засобів виробництва. Значна частина витрат виробництва являє собою амортизаційні відрахування.

Матеріаломісткі підприємства мають високі обсяги витрат ресурсів. Цим підприємствам доводиться вирішувати завдання ефективного використання ресурсів і екологічних проблем, пов'язаних з утилізацією відходів виробництва.

Відповідно до галузевої приналежністю підприємства поділяються на:

– промислові підприємства, які здійснюють видобуток і переробку корисних копалин, і виробництво товарів;

– будівельні підприємства;

– торговельні підприємства, які самі не виробляють товари, але виконують дистриб'юторські функції;

– банки, які збирають кошти і надають кредити;

– транспортні підприємства, які займаються перевезеннями з використанням різних транспортних засобів;

– страхові організації, які здійснюють страхування від різних видів ризиків;

– підприємства, які займаються, розробкою і продажем об'єктів інтелектуальної власності.

– підприємства в сфері послуг, наприклад, готелі, турфірми, консалтингові фірми та інші.

Найбільш зручним місцем розташування є таке, коли забезпечується максимально можливий прибуток і рентабельність виробництва при інших рівних умовах. При цьому не можна забувати екологічний принцип діяльності підприємства, [11].

Підприємства можуть бути віднесені до малих, середніх або великих залежно від наступних факторів: кількість працівників, річний оборот, розмір основного капіталу, кількість робочих місць, витрати на оплату праці, використання вихідних матеріалів.

За призначенням готової продукції підприємства діляться на: ті, що виробляють засоби виробництва і виробляють предмети споживання.

За ознакою технологічної спільності розрізняють підприємство: з безперервним і дискретним процесами виробництва.

За спеціалізацією і масштабами виробництва однотипної продукції підприємства діляться на: спеціалізовані, диверсифікаційні і комбіновані.

За типами виробничого процесу підприємства діляться на підприємства з одиничним типом виробництва, серійним, масовим, досвідченим.

За формами власності розрізняють: приватні, державні та змішані підприємства.

Мета цієї роботи – визначення інформативних ознак у процесі управління ризиками інформаційної безпеки, тобто пошук елементів або ознак, що впливають на здійснення процесу, його деталізацію, на дію етапів УРІБ. Саме тому фактори класифікації комерційних підприємств можна вважати інформативними ознаками в процесі управління ризиками. З усіх описаних раніше факторів є лише певна частка, що має вагомий вплив на зміну таких етапів процесу як: встановлення контексту, ідентифікація ризику, визначення рівня ризику та оцінювання ризику. На етапі обробки та прийняття ризику не доречно вести мову про інформативні ознаки, тому що ці етапи є індивідуальними для кожного ризику. Враховуючи всі описані вище фактори (чинники), виділяються наступні групи інформативних ознак:

– тип підприємства за використанням ресурсів;

- галузева приналежність;
- географічне розташування підприємства;
- фактичне розташування підприємства;
- розмір підприємства (чисельність та рівень доходу);
- рівень конкуренції.

1.4 Постановка задачі

Для успішного виконання поставлених на початку даної роботи цілей необхідно поставити завдання, на основі якого далі виконуватиметься ця робота. Завдання формулюється в прямій залежності від поставленої на початку роботи мети, а також доступних засобів і методів досягнення цілей, і завдання повністю відображає дані кроки.

Завданням даної роботи є складання певного переліку рекомендацій з побудови алгоритму проведення оцінки ризиків на підставі аналізу інформативних ознак й експериментальна їх перевірка на окремому обраному підприємстві.

Проте слід зазначити, що етап обробки ризиків не буде розглядатися в даній роботі через те, що він буде повністю індивідуальним для кожного випадку, адже повністю залежить від попередніх етапів процесу управління ризиками інформаційної безпеки; наприклад, від ідентифікації активів чи оцінки ризиків. Тому неможливо надати узагальнені рекомендації, котрі будуть підходити для кожного виду комерційного підприємства.

Під час виконання даного завдання доцільно використовувати стандарти, нормативні документи і рекомендації у сфері управління інформаційними ризиками.

У різних технологічно розвинених країнах розроблено і розробляється велика кількість стандартів інформаційної безпеки. Це насамперед міжнародні та національні стандарти оцінки інформаційної безпеки та управління нею – ISO 15408, ISO 17799 (BS7799), ISO 27001, BSI; стандарти аудиту, що

відображають питання інформаційної безпеки, – COBIT, SAC, COSO, SAS 55/78 і деякі інші, такі як:

– BS 7799-1:2005. Information security management. Code of practice for information security management (Практичні правила управління інформаційною безпекою);

– BS 7799-2:2005. Information security management. Specification for information security management systems (Вимоги до систем управління інформаційною безпекою);

– BS 7799-3:2006. Information security management systems. Guidelines for information security risk management (Керівництво з управління ризиками інформаційної безпеки).

Перші дві частини британського стандарту BS 7799-3 отримали міжнародне визнання і є практичні рекомендації щодо побудови системи ІБ і оціночні вимоги (головним чином сертифікаційні) до систем менеджменту ІБ. Третя частина також отримала міжнародний статус, у вигляді стандарту ISO 27005. Крім проєкту ISO 27005, існує проєкт й іншого більш загального міжнародного стандарту ISO 31000 «Risk management». Необхідно зазначити, що національні стандарти випереджають міжнародні. Наприклад, BS 31100 Code of Practice for risk management, 2007, Draft, випереджає зазначений ISO 31000. Обидва стандарти відносяться до ризиків взагалі, а не тільки до інформаційних ризиків.

Гостра необхідність у стандарті, що регламентує питання оцінки та управління ризиками ІБ, прямо випливає з введеного з 2010 р. у нашій країні СОУ Н НБУ 65.1 «Система управління інформаційною безпекою», який відповідає стандарту ISO/IEC 27001-2005. Згідно стандарту, СМІБ трактується як частина загальної системи управління, заснованої на оцінці бізнес-ризиків і призначеної для створення, впровадження, експлуатації, моніторингу, аналізу, супроводження та вдосконалення ІБ.

Впровадження стандарту ДСТУ 27001 в практику має наявність в організації як мінімум двох документів: політики ІБ та методології оцінки

ризиків ІБ, однак для останнього документа в національній нормативній базі не відображені питання розробки, форма і зміст. Недолік вітчизняної нормативної бази ІБ полягає у відсутності українського ДСТУ по ризиках.

1.5 Висновки до першого розділу

В даному розділі була представлена загальна модель процесу управління ризиками інформаційної безпеки. Дана модель є узагальненою для всіх випадків і не враховує жоден з окремих випадків. Для визначення окремих випадків існують (і були описані) інформативні ознаки.

Аналіз видів підприємств дозволяє чітко визначити межі дії процесу УРІБ в інформаційній системі і акцентувати увагу на найважливіших його (процесу) аспектах.

Також в даному розділі були визначені задачі даної кваліфікаційної роботи і наданий порівняльний аналіз стандартів та рекомендацій у сфері управління інформаційними ризиками.

РОЗДІЛ 2. ІНФОРМАТИВНІ ОЗНАКИ В ПРОЦЕСІ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ РОЗРОБЛЕНИХ РІШЕНЬ

2.1 Аналіз інформативних ознак на етапі ідентифікації ризику

Як вже було сказано в першому розділі, ризик інформаційної безпеки включає в себе можливість реалізації загрози та величину збитку, що несе компанія за рахунок цінності інформаційного активу, чи в грошовому еквіваленті чи в рівні затрат трудових ресурсів на поновлення активу. Інформаційною ознакою, що дозволяє ідентифікувати загрозу є існування вразливостей на підприємстві. Але на етапі ідентифікації загроз, фахівець, що займається оцінкою ризику повинен усвідомлювати, що хоча у системі присутня достатня кількість вразливостей, не всі загрози мають великий ризик її використання. Так, наприклад, невелике підприємство, що займається торгівельною діяльністю, що має незахищені лінії зв'язку навряд чи буде підслуховуватися зовнішнім порушником, таким як хакер, тому що цінність інформації не занадто велика, щоб когось цікавити або можлива повна відсутність появи зовнішніх порушників. Та внутрішні порушники завжди існують, навіть якщо всі співробітники задоволені своїм керівництвом та умовами праці, присутня реалізація випадкових загроз.

В залежності від середи знаходження, вразливості можна поділити на такі групи: вразливості апаратних засобів, вразливості програмного забезпечення, вразливості мережі, вразливості персоналу та вразливості сайту.

До вразливостей першої групи належать: недостатнє обслуговування або дефектна інсталяція з носіїв даних, недоліки схем для періодичних замін, сприйнятливість до вологості або пилу, забруднення, чутливість до електромагнітної радіації, недоліки ефективного контролю внесення змін конфігурації, сприйнятливість до змін напруги, сприйнятливість до температурних змін, незахищене зберігання, недолік в обережності при знищенні, неконтрольоване копіювання, недостатнє обслуговування

апаратних засобів, застаріле телекомунікаційне обладнання, відсутність резервного обладнання.

До вразливостей програмного забезпечення відносять: відсутність або недостатнє програмне тестування, відомі недоліки в програмному забезпеченні, відсутність "виходу з системи" при залишенні робочої станції, передача або багаторазове використання носіїв даних без належного стирання, неправильний розподіл прав доступу, складний призначений для користувача інтерфейс, недоліки в документуванні, некоректно виставлені дати, використання старих версій операційних систем, а також використання неліцензійних версій програмного забезпечення.

В третій групі, що включає в себе вразливості мереж знаходяться: недоліки ідентифікуючих і розпізнавальних механізмів для користувальницької автентифікації, незахищені таблиці паролів, погане управління паролями, недопрацьоване або нове програмне забезпечення, неясні або неповні специфікації для розробників, недоліки ефективного контролю внесення змін, неконтрольоване завантаження і використання програмного забезпечення, недоліки в процедурі резервного копіювання, недоліки фізичного захисту будівлі, дверей і вікон, брак докази посилки або одержання повідомлення, незахищені лінії зв'язку, незахищений чутливий трафік, недоліки ідентифікації і автентифікації відправника та одержувача, небезпечна мережева архітектура, передача паролів у відкритому вигляді, відсутність моніторингу поштових ящиків.

До групи що включає в себе вразливості персоналу можна віднести: недостатнє вивчення правил безпеки, неправильне використання програмного забезпечення і устаткування, недоліки розуміння безпеки, брак механізмів моніторингу, неконтрольована робота з зовнішнім штатом, недоліки політики безпеки для правильного використання носіїв передачі даних і обміну повідомленнями, неналаштований мандатний доступ, відсутність відповідальності за втрату носіїв інформації, відсутність розподілу обов'язків, неправильний порядок знищення інформації.

І до останньої групи вразливостей сайту підприємств належать: місцезнаходження в області, сприйнятливої до затоплення, повінь, брак фізичного захисту будівлі, дверей і вікон, дефіцит або недостатні умови в контрактах з клієнтами і (або) третіми особами, недоліки в процедурі для контролю над засобами обробки інформації, застаріла система пожежогасіння, несправність трансформаторів, відсутність камер відео нагляду. Всі вони є індивідуальними, тому важко оцінити на якому підприємстві одна вразливість буде присутня, а на якому ні.

Усі шаги ідентифікації ризиків залежать один від одного, тому всі вразливості напряму залежать від інформаційних активів, які присутні у тій чи іншій організації. Такий список активів сильно різниться в залежності від самої організації та її бізнес процесу. Наприклад, в одній організації може бути присутній електронний документообіг, так як вона сама є торгівельною компанією, а в іншій – такий процес відсутній.

Для визначення рівня збитку ризиків на етапі ідентифікації ризику, визначають активи компанії та цінність від реалізації загроз порушення основних властивостей активів компанії: цілісності, конфіденційності та доступності в залежності від джерел впливу, наприклад: природного або штучного характеру. Проведемо аналіз визначення основних загроз та ризиків інформаційним активам різних підприємств за типом обраної галузі.

2.1.1. Загрози підприємств в сфері послуг

Сфера послуг - сукупність галузей економіки, що надають послуги населенню. У сферу послуг прийнято включати культуру, освіту, охорону здоров'я, побутове обслуговування, послуги налагодження бізнес-процесу та інше.

Даний вид підприємств відрізняється від інших тим, що в даному випадку в бізнес-процесі беруть участь не товари, а якийсь спектр послуг, що надається компанією. Послуги не вимагають захисту, проте цього вимагає предмет надання послуг. У певних випадках послуги мають на увазі якісь

операції з інформацією. Сюди можна віднести, наприклад, документи, як предмет надання послуг з електронного документообігу. Нерідко така інформація є конфіденційною для клієнтів, а в деяких випадках і на законодавчому рівні. Тому при забезпеченні захисту інформації на такому вигляді підприємств слід звернути увагу і на питання захисту предмета надання послуг.[12]

Також, як і в попередніх випадках, важливо забезпечити захист особистих даних всіх співробітників підприємства і клієнтів, а також забезпечити захист контрактів з клієнтами і партнерами. Останні два види корпоративної інформації сильно впливають на бізнес-процес підприємства, а втрата їх конфіденційності, цілісності або доступності може привести до серйозних фінансових втрат.

Виходячи з вищевказаного документа можна виділити наступні основні загрози інформаційній безпеці даного виду підприємств:

– втрата конфіденційності, цілісності або доступності предмета надання послуг;

– втрата конфіденційності особистої інформації співробітників підприємства;

– втрата конфіденційності особистої інформації клієнтів;

– втрата конфіденційності, доступності або цілісності контрактів з клієнтами підприємства.

2.1.2. Загрози будівельних підприємств

Будівельні підприємства займаються зазвичай не тільки будуванням споруд, а також найчастіше беруть участь у конкурсах на отримання тендера, де кількість конкурентів може сягати декількох сотень, тому найбільшої уваги такі підприємства поділяють саме інформації що потребує захисту від конкурентів. Інформацією, що підлягає захисту, зокрема, стандартної, яка є цінною для інших галузей, може бути креслення конкурсних робіт, що можуть бути викраденні або зіпсовані співробітниками компанії. Тому на будівельних

підприємствах слід приділяти увагу загрозам з боку персоналу. Такі загрози несуть в собі не аби яку небезпеку і можуть мати величезні збитки. Та для зменшення ризику реалізації загроз можливо ввести контр заходи, що забезпечують навчання співробітників та надійне анкетування, що унеможливить появу інсайдерів.

В системі забезпечення інформаційної безпеки будівельних підприємств необхідно реалізовувати дієві заходи з протидії виникнення інформаційних загроз щодо персоналу, який має справу з конфіденційною інформацією підприємства. Так, при прийомі на роботу рекомендується проводити анкетування, за допомогою якого можна зробити висновки про рівень інтелекту, отримати загальне уявлення про кандидата як різносторонньої особи, визначити морально-психологічний рівень, виявити можливі злочинні схильності тощо. У разі успішного проходження кандидатом перевірки і визнання його відповідним посаді здійснюється підписання двох документів:

1 Трудового договору (контракту). Контракт обов'язково повинен містити пункт про обов'язок працівника не розголошувати конфіденційну інформацію і дотримувати заходи безпеки.

2 Договору (зобов'язання) про не розголошування конфіденційної інформації, який є правовим документом, де кандидат на вакантну посаду дає обіцянку не розголошувати ті відомості, які йому буде відомий в період його роботи на підприємстві, а також про відповідальність за їх розголошування або недотримання правил безпеки (розірвання контракту і судовий розгляд).

Велику значимість в загальній системі заходів з подолання впливу людського чинника має повсякденна робота з персоналом. Організація персоналу включає навчання співробітників правилам і прийомам роботи з конфіденційною інформацією. Навчання може бути диференційовано залежно від терміну роботи співробітників на підприємстві - тобто програма навчання для нових співробітників і для співробітників, які мають досвід роботи в даній організації. Крім навчання персоналу, однією з основних задач є постійне

нагадування всім співробітникам про необхідність дотримання правил інформаційної безпеки.

Мотивація співробітників підприємства в цілях забезпечення його інформаційної безпеки може реалізовуватися по двох напрямах – шляхом застосування заохочень і санкцій. Невід'ємним елементом управління персоналом є контроль за дотриманням співробітниками правил забезпечення інформаційної безпеки і за надійністю персоналу. Контроль дотримання правил забезпечення безпеки може проводитися з використовуванням: планових і раптових перевірок, в процесі яких служба безпеки перевіряє дотримання в структурних підрозділах правил роботи з конфіденційною інформацією, а також працездатність технічних засобів захисту; моніторингу ситуації силами позаштатних інформаторів служби безпеки з числа співробітників відповідних підрозділів; моніторингу ситуації з використанням спеціальних технічних засобів спостереження. Контроль надійності персоналу здійснюється службою безпеки в індивідуальному режимі відносно окремих категорій співробітників. В першу чергу, це менеджери, експерти і рядові виконавці, що займають ключові робочі місця, що забезпечують доступ до конфіденційної інформації. Контроль їх лояльності здійснюється в постійному режимі.

Для підвищення загальної ефективності необхідно проводити оцінку надійності даного персоналу. Аналіз підходів до оцінки надійності персоналу показав, що основною характеристикою надійності є лояльність персоналу до підприємства. Вважаємо, що в системі інформаційної безпеки будівельних підприємств рівень надійності також повинні визначати інформаційна і професійна компетентність, а також рівень комунікабельності як здатність до ефективної взаємодії.

2.1.3. Загрози торгових підприємств, які не виготовляють товари самостійно, але виконують дистриб'юторські функції

Під торговим підприємством розуміють майновий комплекс, використовуваний організацією для купівлі-продажу товарів і надання послуг торгівлі. Однією з важливих задач комерційної діяльності роздрібних торгових підприємств є забезпечення ними своєї конкурентоспроможності. Основним способом досягнення цієї задачі є пропозиція покупцям товарів і послуг належної якості, в потрібному асортименті, в необхідні терміни і на вигідніших умовах, ніж у конкурентів. Види торгових фірм: експортні фірми, імпортні фірми, оптові фірми, роздрібні фірми, стокісти.

Беручі до уваги невеликі торгові підприємства (роздрібні), що займаються збутом товару особисто клієнту, як такої інформації, що підлягає захисту і не може бути, бо така фірма має лише невелику кількість матеріальних активів, і загроз майже не існує. [13]

В наш час, торгові підприємства переходять від звичайного документообігу до електронного документообігу. Фірма, що має свій сайт, базу даних клієнтів, велику кількість матеріальних активів, має безліч загроз та ризиків пов'язаних насамперед з підтримкою системи менеджменту інформаційної безпеки, а саме:

- втрата конфіденційності, цілісності або доступності предмета активів пов'язаних з електронним та паперовим документообігом;
- втрата конфіденційності особистої інформації співробітників підприємства;
- втрата конфіденційності особистої інформації клієнтів;
- втрата конфіденційності, доступності або цілісності контрактів з клієнтами підприємства.

2.1.4. Загрози банківських підприємств

Проблема забезпечення інформаційної безпеки банківських установ є однією із передових, при цьому, не потрібно навіть бути фахівцем, щоб

зрозуміти важливість даного питання. Так як , навіть замислюючись над тим, що кожен з нас має певне відношення, і не раз в житті зіштовхувався із банківським сегментом послуг, насамперед, зацікавлений у безпеці таких відомостей, та з особливою обережністю ставиться до них. Так, інформаційна безпека – це формування інформаційних ресурсів банку та організація гарантованого їх захисту. Досягається створенням у банку системи збору та обробки інформації, проведенням відповідних заходів щодо її зберігання та розподілу, визначенням категорій і статусу банківської інформації, порядку і правил доступу до неї, дотриманням усіма працівниками, клієнтами та акціонерами банку норм і правил роботи з банківською інформацією, своєчасним виявленням спроб і можливих каналів витоку інформації та їх перетинанням. [15]

Однак, для того щоб побудувати збалансовану систему інформаційної безпеки, потрібно спочатку, провести аналіз ризиків у сфері банківської інформаційної безпеки. Перш за все проблема починається із неправильного розуміння порушень інформаційної банківської безпеки, що пов'язані із такими категоріями як «загроза», «ризики», «джерело загрози», «фактор загрози», «вразливість», «несприятливі чинники впливу», «негативні прояви», «перешкоди». Спільним для них є те, що усі вони характеризують категорію «небезпеки», що є відповідно протилежною «безпеці».

Незважаючи на таку схожість, дані терміни все ж не є тотожними. Так, попри численні дослідження, які проведені у цих напрямках, ще й сьогодні немає чіткого та однозначного їх трактування, особливо це стосується таких понять, як «ризик» та «загроза». Зазвичай можна зустріти, що термін «загроза» використовують для трактування суті ризиків.

Загроза є специфічною формою ризику, як вважає О.І. Барановський, досліджуючи ризики банківської діяльності, він зупиняється на думці, що перехід ризику в загрозу починається тоді, коли з'являються негативні якісні зміни в економічних системах, що пов'язані зі значними фінансовими

втратами, збитками, які спричиняють банкрутство». Крім того є цікавим такий погляд, що:

– ризик стосовно загрози є первинним, тоді як загроза вторинна і випливає з ризику;

– ризикуючи, банк може отримати як збитки, так і доходи, тоді як реалізація загрози не приносить доходи чи прибутки;

– ризик – неминучий супутник банківської діяльності, тоді як загроза може виникати тільки за наявності певних умов.

Що ж до категорій «джерело» та «фактор» питання є дещо простішим. Так, будь-яке джерело слід розуміти як певне начало, витік, початок. Сама по собі дефініція означає «те, з чого щось бере свій початок». Однак, при цьому слід відмітити, що у випадку, коли мова йде про ризики безпеці зокрема інформаційній), фактор загрози все ж буде передувати її джерелу. Так, як такий фактор буде певним чинником виникнення джерела, тобто його активі затором, з якого починається увесь «механізм» ризиків інформаційній безпеці банківських установ відповідно, на підставі всього вище зазначеного, можна прийти висновку, що під дією негативного впливу певних факторів несприятливих чинників впливу, тобто певних дій) джерело загроз через певну вразливість створює певні ризики та загрози системі безпеки.

Така модель інформаційної безпеки має змогу відображувати сукупність об'єктивних зовнішніх і внутрішніх чинників та їх вплив на стан інформаційної безпеки на об'єкті і на збереження інформаційних ресурсів.

Таким чином, інформаційна безпека, як відомо, має справу з двома категоріями загроз: зовнішніми та внутрішніми.

Водночас, чим більших успіхів досягає людство в боротьбі з зовнішніми загрозами, тим рішучіше на перший план виходять загрози внутрішні, з якими, згідно статистики, пов’язано близько 70% всіх інцидентів безпеки. При цьому, у категорію внутрішніх загроз було віднесено халатність співробітників, саботаж та фінансове шахрайство, а в категорію зовнішніх загроз – віруси, хакери, спами.

Однак, необхідно враховувати, що такі некласифіковані ризики як, наприклад, викрадення інформації або обладнання, найчастіше відносять до внутрішніх ризиків, і так як в даному випадку вони взагалі не враховані, показники розрахунку свідчать, що зовнішні ризики все ж поступаються внутрішнім загрозам. Як показали результати дослідження, у списку найнебезпечніших внутрішніх загроз головне місце посідає порушення конфіденційності інформації 78%), на другому місці – втрата інформації 61%), і на третьому – збій в роботі інформаційних систем 52%).

Тому слід відзначити, що зовнішні джерела загроз можуть напряму, або безпосередньо бути пов'язаними із внутрішніми. Тому аналіз зовнішнього та внутрішнього середовища має проводитися комплексно та одночасно.

Також слід пам'ятати, що захист банківської інформації – завдання в рівній мірі як технічне, так і правове, і організаційне.

З метою запобігання порушенням інформаційної безпеки інформаційних банківських ресурсів потрібно виявляти та аналізувати вразливі місця інформаційної системи банку та ресурси, які потребують захисту, а також ймовірні атаки, які можуть відбутися в конкретному оточенні. Після цього потрібно визначити інформаційні ризики для визначеного інформаційного ресурсу та обрати контрзаходи, згідно обраної політики банківської безпеки та забезпечити за допомогою механізмів і сервісів безпеки. Політика банківської безпеки має визначати взаємопов'язану сукупність механізмів і сервісів безпеки, адекватну ресурсам, що захищаються, і оточенню, в якому їх використовують.

2.1.5 Загрози транспортних підприємств

Транспортні підприємства – це підприємства, що займаються перевезенням сировини, матеріалів, напівфабрикатів як всередині підприємства, так і за його межами, відправлення готової продукції, відходів виробництва здійснюються транспортом. У цьому процесі, як правило, беруть участь дві групи транспорту:

1 Транспорт сторонніх організацій, що здійснює перевезення на договірних умовах.

2 Транспорт, що належить підприємству і що є його власністю, оформлений в одне або кілька підрозділів (за видами транспорту), що входять в інтегральне поняття - транспортне господарство. Транспортне господарство, як правило, доручаються вантажно-розвантажувальні роботи на підприємстві. [16]

Задачі транспортного господарства можна розділити на дві групи:

– забезпечення переміщення сировини, палива, напівфабрикатів, виробів і готової продукції в суворій відповідності до вимог технологічного процесу, прийнятого на підприємстві;

– забезпечення мінімізації витрат на перевезення і вантажно-розвантажувальні роботи.

Це завдання також досить актуальне, оскільки кількість працівників транспортного господарства досягає 25-50% усієї кількості робітників, зайнятих в інших допоміжних і обслуговуючих підрозділах, а витрати на транспортні, вантажно-розвантажувальні роботи і зміст самого транспорту в структурі собівартості продукції підприємства сягає 3-7, а іноді навіть 12%. Ці завдання реалізують підрозділи - цехи, дільниці, що спеціалізуються, як правило, за видами транспортних засобів - залізничний, безрейковий та ін.. До складу цих підрозділів входять транспортні засоби, під'їзні колії та дороги, ремонтні та екіпірувальні пункти.

Виходячи з задач діяльності транспортних підприємств можна зробити наступні висновки щодо забезпечення безперервності бізнес процесу, а також максимального забезпечення такої властивості інформації як доступність та цілісність. Підприємство може понести величезні збитки, якщо буде втрачена або скорегована інформація і наприклад: вантаж А, що повинен був бути відправлений до пункту А, буде відправлений до пункту Б. Тому на етапах встановлення контексту необхідно враховувати максимально критерії ризиків пов’язані за реалізацією загроз щодо безперервності ведення бізнесу та

забезпечення цілісності та доступності. Від цих властивостей залежить нанесення збитку репутації, а репутація вагома властивість існування підприємства.

2.1.6 Загрози страхових організацій

Страхові компанії — це фінансові посередники, які здійснюють виплати своїм клієнтам при настанні певних подій, обумовлених у договорі страхування (страховому полісі).

Страховий поліс є контрактом, згідно з яким власник поліса сплачує премії страховій компанії в обмін на зобов'язання компанії сплатити обумовлені суми в майбутньому при настанні певних подій. Поліс є активом власника і зобов'язанням страхової компанії.

Страхова премія (страховий платіж, страховий внесок) є платою за страхування, яку власник полісу (страхувальник) вносить страховій компанії (страховику) відповідно до договору страхування. Премія може сплачуватись одноразово або у вигляді послідовності періодичних платежів. У випадку, коли власник поліса не сплачує премії, договір страхування розривається.

Укладаючи договори страхування, страхові компанії приймають на себе ризики власників полісів, а отримуючи страхові внески, вони отримують плату за прийняті на себе ризики. Здатність компанії взяти на себе ризики страхувальників пов'язана з відношенням премії, яку він отримує щороку, до величини надлишку, що визначається різницею між активами і зобов'язаннями компанії. Для більшості страхових компаній це відношення становить від 2:1 до 3:1. Діяльність страхової компанії характеризує також величина її особистої брутто норми збитковості. На ринках, що розвиваються, ця норма становить 40—60%, на розвинених ринках — до 80%. [17]

Страхові внески використовуються страховими компаніями для придбання облігацій, акцій, заставних та інших цінних паперів. Близько 90% активів страхових компаній — це цінні папери. Можна стверджувати, що

страхові компанії виступають на ринку інститутом, де одні фінансові активи перетворюються на інші, а саме цінні папери на страхові поліси.

З інвестуванням коштів страхових компаній у різні види активів пов'язаний один із основних ризиків в їх діяльності, а саме кредитний ризик. З метою захисту інтересів страхувальників та для забезпечення фінансової стійкості страховиків державою регулюється структура активів страхових компаній. Як правило, вводяться обмеження на вкладення в прості та привілейовані акції, а також облігації.

Для оцінювання капіталу страхових компаній, як і для оцінювання банківського капіталу, використовують поняття зважених за ризиком активів.

Валовий дохід страхових компаній складається з отриманих премій та доходу від інвестованих в активи (цінні папери) коштів. Витрати страхових компаній пов'язані з формуванням резервів, виплатами при настанні страхових випадків та витратами на продаж полісів. Резерви створюються через невизначеність, пов'язану з часом настання страхових випадків, та через невизначеність сум, які потрібно буде сплатити власникам страхових полісів у разі настання страхових випадків. Під витратами на продаж полісів розуміють усі витрати, пов'язані з функціонуванням компанії: витрати на утримання персоналу, рекламні, маркетингові витрати, на утримання робочих приміщень у належному стані, придбання обладнання, устаткування тощо. Дохід від володіння цінними паперами та частина страхових внесків використовуються компанією для формування резервів, виплати страхових відшкодувань за полісами та на покриття операційних витрат. Кошти, що залишаються в розпорядженні компанії, є її прибутком.

Інформація, що підлягає захисту в страхових компаніях, є сукупність договорів між клієнтами (страховий поліс), особисті данні клієнтів, рахунок оплати поліса, а також конфіденційна інформація підприємства, яка може нашкодити репутації або бізнес-процесу компанії. В залежності від масштабу організації можлива загроза появи інсайдера, до уваги слід враховувати зовнішні загрози, поміж інших:

– загроза втрати конфіденційності цілісності та доступності особистих даних співробітників підприємства;

– загроза втрати конфіденційності цілісності та доступності особистих даних клієнтів;

– загроза втрати конфіденційності цілісності та доступності страхових полісів;

– загроза втрати конфіденційної інформації підприємства, яка може нашкодити репутації або бізнес-процесу компанії.

2.1.7 Загрози промислових підприємств

Промислове підприємство - майновий комплекс, який використовується для здійснення підприємницької діяльності. До складу промислового підприємства входять всі види майна, призначеного для його діяльності, включаючи земельні ділянки, будівлі, споруди, обладнання, інвентар, сировину, продукцію. Тобто всі підприємства що займаються видобутком сировини, палива, заготівлі лісу, переробки продукції, випущеної промисловістю або виробленої сільським господарством, видобуток і переробка сировини, виробництвом товарів або виробництвом електроенергії, знарядь праці для галузей економіки потребують захисту такої інформації як: розробки та схеми, патенти, документообіг (звичайний та електронний) між промисловим підприємством та торговим підприємством, що здійснює збут виготовленого товару. Порушення основних властивостей інформації документообігу може призвести до простою виготовленого товару, погіршення репутації компанії та понесення величезних збитків, як результат криза та припинення існування підприємства. Основні загрози, що можуть реалізуватись на промислових підприємствах – всі види загроз , від зовнішніх та внутрішніх, що несуть за собою порушення конфіденційності , цілісності та доступності інформації, що вказана вище.

2.1.8 Загрози підприємств, які займаються розробкою і продажем об’єктів інтелектуальної власності

Даний вид підприємств виділяється тим, що крім основної інформації необхідно захищати також саму інтелектуальну власність клієнтів або самої компанії, яка зберігається для її поширення і підтримки. Виходячи з цього роду діяльності підприємства важливо захищати ліцензійні угоди і контракти з клієнтами, адже в разі їх втрати неможливо буде довести (в тому числі і в суді) обов'язок виконувати клієнтом ту чи іншу умову, описану в даних угодах і контрактах, в наслідок чого компанія може зазнати втрат. Також згідно з чинним законодавством необхідно налагодити захист особистих даних співробітників підприємства і клієнтів; захист інформації останніх необхідна також тому, що може стати доступна компаніям-конкурентам і тим самим порушити бізнес-процес.

Виходячи з описаного вище, можна виділити основні загрози інформаційній безпеці:

– загроза втрати конфіденційності особистих даних співробітників підприємства;

– загроза втрати конфіденційності особистих даних клієнтів;

– загроза втрати цілісності або доступності ліцензійних угод і контрактів;

– загроза втрати конфіденційності, цілісності або доступності інтелектуальної власності.

2.2 Аналіз інформативних ознак на етапі встановлення контексту

Контекст управління ризиками вперше здійснюється тоді, коли проводиться високорівнева оцінка ризиків. Контекст визначає основні параметри управління, область застосування і критерії. В першу чергу, описуються зовнішні і внутрішні умови, в яких функціонує організація.

Наступним кроком є встановлення цілей управління ризиками. На цьому етапі розподіляються обов'язки, визначається обсяг розглянутого проєкту, а також необхідні дії. Крім того, вибирається відповідний метод оцінки ризиків, виходячи з особливостей функціонування організації і глибини проведеного

аналізу. На підставі отриманої інформації визначаються критерії оцінки та прийнятності ризику.

В якості критеріїв визначення цінності активів, як правило, виступають вимоги законодавства і причетних сторін, встановлених в контексті управління ризиками. Для кожної з властивостей активу, таких як конфіденційність, цілісність і доступність, має бути визначено окреме значення цінності, так як вони є незалежними. На підставі отриманих результатів складається таблиця цінності активів. Визначається загальне значення цінності активу, яке буде враховуватися в подальшому аналізі при оцінці тяжкості наслідків. Найчастіше загальне значення визначається експертним шляхом, минаючи визначення цінності для кожного з властивостей. Однак, такий підхід менш точний.

На етапі опису контексту описується модель взаємодії організації із зовнішнім світом

Область застосування СУІР в ідеалі повинна збігатися з областю дії СУІБ та охоплювати всю організацію. Проте оцінити відразу всі ризики для всіх активів і впровадити СУІР одразу для всієї організації досить складно.

Область застосування залежить від розмірів підприємства. Так, для малих підприємств недоцільно розбивати СУІР на етапи, але це може бути доцільним для великих підприємств – такі підприємства мають забагато інформаційних активів і впровадження СУІР може бути занадто складним. Особливо доцільне виключення із області дії декотрих активів у підприємствах, котрі мають філіали чи децентралізовану структури.

Також область застосування залежить від спеціалізації підприємства. Наприклад, для підприємств, які мають диверсифікаційну структуру бізнесу, доцільно розбити процес впровадження СУІР на етапи, що будуть однакове співвідношення до кожного із усіх бізнес-процесів, так як кожний із них потребує особливого підходу до управління ризиками.

2.3 Аналіз інформативних ознак на етапі оцінки ризику при виборі оптимальної методики

Для вибору оптимальної методики необхідно звертати увагу на позитивні на негативні інформативні ознаки, що сприятимуть ефективному вибору. На даному питанні інформативними ознаками будуть виступати характеристики методик та програмного забезпечення що здійснює їх реалізацію. До них можна віднести наявність або відсутність таких характеристик: завдання збитку, завдання функції збитку, які якості активів враховуються, врахування залежностей між контрзаходами при розрахунку ризиків, врахування залежності ефективності контрзаходу від часу, спрацьовування на загрозу та функції збитку, врахування вартості, впровадження контрзаходів, врахування вартості експлуатації контрзаходів, врахування вартості контрзаходу при його спрацьовуванні на загрозу, можливість завдання власних контрзаходів, можливість завдання власних загроз, можливість завдання власних вразливостей, кількість заздалегідь заданих контрзаходів, мережевої версії програмного продукту, локальної версії програмного продукту, вартість програмного продукту в мінімальній комплектації, мова на якій написано програмне забезпечення.

За статистикою, найбільшою перешкодою на шляху прийняття будь-яких заходів щодо забезпечення інформаційної безпеки в компанії є дві причини:

– обмеження бюджету;

– відсутність підтримки з боку керівництва.

Для вирішення даного завдання були розроблені програмні комплекси аналізу і контролю інформаційних ризиків: британський CRAMM (компанія Insight Consulting) і американський RiskWatch (компанія RiskWatch). Розглянемо далі дані методи і побудовані на їх базі програмні системи.

Метод CRAMM (CCTA Risk Analysis and Managment Method) був розроблений Агентством з комп'ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency) за завданням Британського

уряду і взятий на озброєння в якості державного стандарту. Він використовується, починаючи з 1985 р, урядовими та комерційними організаціями Великобританії. За цей час CRAMM набув популярності у всьому світі. Фірма Insight Consulting Limited займається розробкою і супроводом однойменного програмного продукту, що реалізує метод CRAMM.

В даний час CRAMM - це досить потужний і універсальний інструмент, що дозволяє, крім аналізу ризиків, вирішувати також і ряд інших аудиторських завдань, включаючи:

– проведення обстеження ІС і випуск супровідної документації на всіх етапах його проведення;

– проведення аудиту відповідно до вимог Британського уряду, а також стандарту BS 7799: 1 995 «Code of Practice for Information Security Management»;

– розробка політики безпеки і плану забезпечення безперервності бізнесу.

В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, поєднуючи кількісні та якісні методи аналізу. Метод є універсальним і підходить як для великих, так і для дрібних організацій, як урядового, так і комерційного сектора. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються один від одного своїми базами знань (profiles). Для комерційних організацій є Комерційний профіль (Commercial Profile), для урядових організацій - Урядовий профіль (Government profile). Урядовий варіант профілю, також дозволяє проводити аудит на відповідність вимогам американського стандарту ITSEC.

Концептуальна схема проведення обстеження за методом CRAMM показана на рисунку 2.1.

До недоліків методу CRAMM можна віднести наступне:

– використання методу CRAMM вимагає спеціальної підготовки і високої кваліфікації аудитора;

– CRAMM в набагато більшою мірою підходить для аудиту вже існуючих ІС, що знаходяться на стадії експлуатації, ніж чим для ІС, що знаходяться на стадії розробки;

– аудит за методом CRAMM - процес досить трудомісткий і може зажадати місяців безперервної роботи аудитора;

– програмний інструментарій CRAMM генерує велику кількість паперової документації, яка не завжди виявляється корисною на практиці;

– CRAMM не дозволяє створювати власні шаблони звітів або модифікувати наявні;

– можливість внесення доповнень до бази знань CRAMM недоступна користувачам, що викликає певні труднощі при адаптації цього методу до потреб конкретної організації;

– програмне забезпечення CRAMM існує тільки англійською мовою;

– вартість ліцензії від 2000 до 5000 дол.

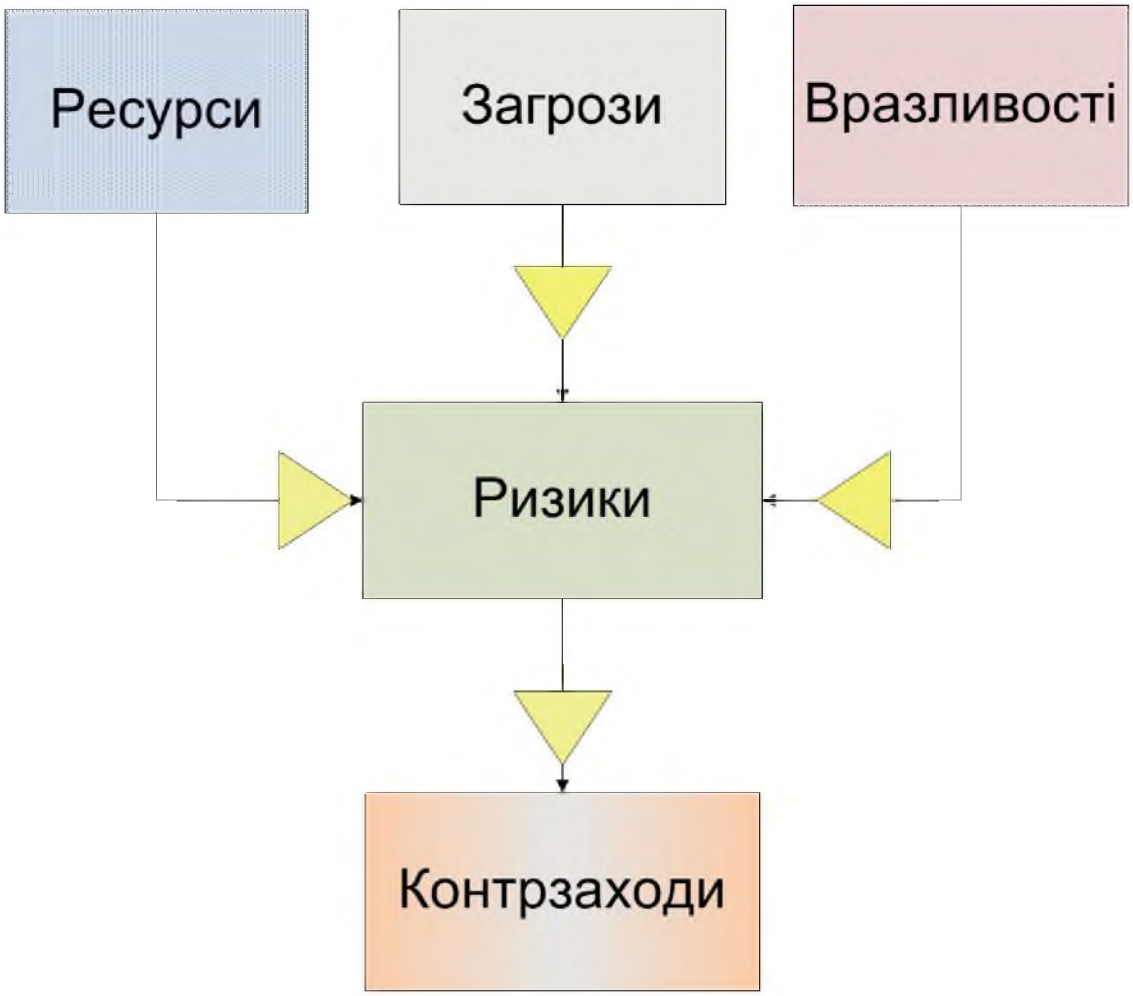

Рисунок 2.1 – Концептуальна схема проведення обстеження за методом CRAMM

Програмне забезпечення RiskWatch є потужним засобом аналізу та управління ризиками. У сімейство RiskWatch входять програмні продукти для проведення різних видів аудиту безпеки. Воно включає в себе наступні засоби аудиту та аналізу ризиків:

– RiskWatch for Physical Security - для фізичних методів захисту ІС;

– RiskWatch for Information Systems - для інформаційних ризиків;

– HIPAA-WATCH for Healthcare Industry - для оцінки відповідності вимогам стандарту HIPAA (US Healthcare Insurance Portability and Accountability Act);

– RiskWatch RW17799 for ISO 17799 - для оцінки вимогам стандарту ISO 17799.

У методі RiskWatch в якості критеріїв для оцінки і управління ризиками використовуються пророкування річних втрат (Annual Loss Expectancy, ALE) і оцінка повернення від інвестицій (Return on Investment, ROI).

Сімейство програмних продуктів RiskWatch має масу переваг. RiskWatch допомагає провести аналіз ризиків і зробити обґрунтований вибір заходів і засобів захисту. Використовувана в програмі методика включає в себе 4 фази.

На відміну від CRAMM, програма RiskWatch більш орієнтована на точну кількісну оцінку співвідношення втрат від загроз безпеки і витрат на створення системи захисту. Треба також зазначити, що в цьому продукті ризики в сфері інформаційної та фізичної безпеки комп'ютерної мережі підприємства розглядаються спільно.

До недоліків RiskWatch можна віднести:

– такий метод підходить, якщо потрібно провести аналіз ризиків на програмно-технічному рівні захисту, без урахування організаційних і адміністративних чинників;

– отримані оцінки ризиків (математичне очікування втрат) далеко не вичерпує розуміння ризику з системних позицій - метод не враховує комплексний підхід до інформаційної безпеки;

– програмне забезпечення RiskWatch існує тільки англійською мовою;

– висока вартість ліцензії (від 10 000 дол. за одне робоче місце для невеликої компанії).

Проведемо порівняльний аналіз розглянутих програмних продуктів системи захисту інформації для визначення їх переваг та недоліків. Порівняльна характеристика програмних продуктів системи захисту інформації наведено у табл. 2.1.

Таблиця 2.1 – Порівняльна характеристика програмних продуктів ЗІ

Показник	Засоби аналізу ризиків	
	CRAMM	RiskWatch
1	2	3
Характеристики алгоритму		
Завдання збитку	як наслідок порушення властивостей активів	як наслідок порушення властивостей активів
Функція збитку	Для властивості доступності залежить від часу. Для властивостей конфіденційності, цілісності постійна	Для властивості доступності залежить від часу. Для властивостей конфіденційності, цілісності постійна
Які якості активів враховуються	Тільки конфіденційність, цілісність, доступність	Тільки конфіденційність, цілісність, доступність
Врахування залежностей між контрзаходами при розрахунку ризиків	Є	Є
Врахування вартості впровадження контрзаходів	Є	Немає
Врахування вартості експлуатації контрзаходів	Немає	Немає
Врахування вартості контрзаходу при його спрацьовуванні на загрозу	Немає	Немає

Продовження табл. 2.1

Додаткові характеристики		
Можливість завдання власних контрзаходів	Є	Є
Можливість завдання власних загроз	н/д	Є
Можливість завдання власних вразливостей	н/д	Є
Кількість заздалегідь заданих контрзаходів	3000	н/д
Наявність мережевої версії програмного продукту	Є	Немає
Наявність локальної версії програмного продукту	Є	Є
Вартість програмного продукту в мінімальній комплектації	2000 дол.	10000 дол.

Виходячи з порівняльного аналізу було визначено наступне:

1 Використання методу CRAMM вимагає спеціальної підготовки і високої кваліфікації аудитора.

2 Для вітчизняних користувачів проблема полягає в тому, що отримати використовувані в RiskWatch оцінки (такі як LAFE і SAFE) для наших умов досить проблематично. Хоча сама методологія може з успіхом застосовуватися і у нас.

3 Висока вартість ліцензії для RiskWatch (від 10 000 доларів за одне робоче місце для невеликої компанії) та CRAMM (від 2 000 до 5 000 доларів за одне робоче місце для невеликої компанії).

В ході аналізу існуючих методик було виявлено такі недоліки як: або обмеження в можливості завдання власних контрзаходів, або забороні дозволу завдання власних властивостей активів, або вимагають спеціальної підготовки і високої кваліфікації аудитора, або програмне забезпечення існує тільки на

англійській мові, або виконання без урахування організаційних та адміністративних чинників, або занадто висока вартість ліцензії, що унеможливлює використання методик для малих та середніх організацій, що мають невисокі доходи. Враховуючи недоліки доцільно рекомендувати використання методики стандарту ISO/IEC 27005:2011 за допомогою матриці зумовлених значень. Вона базується на достатньо простих табличних методах і не передбачає застосування спеціалізованого програмного інструментарію та високої кваліфікації аудитора.

Стандарт ISO/IEC 27005:2011 пропонує визначення ризику інформаційної безпеки за допомогою матриці зумовлених значень, вимагає насамперед визначити інформаційні активи підприємства, на які може вплинути загроза, враховуючи їх важливість для бізнес-цілей, ступінь залежності бізнесу від кожного інформаційного активу, рівень інвестицій в активи та активи, яким підприємство напряму надає цінності (наприклад, за вимогою законодавства). Оцінка ризику здійснюється в 4 етапи:

- визначення активів підприємства та їх цінності;
- визначення вразливостей та їх рівня;
- визначення загроз та вірогідності реалізації;
- визначення рівня ризику за матрицею зумовлених значень.

Рівень ризику встановлюється за визначеними трьома критеріями: цінність інформаційного активу, вірогідність загрози та рівень вразливості, - відповідно до таблиці 2.2.

Таблиця 2.2 - Матриця зумовлених значень

Значення активу	Вірогідність виникнення загрози	Низька (Н)			Середня (С)			Висока (В)		
	Готовність вразливості	Н	С	В	Н	С	В	Н	С	В
	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Дана методика являє собою методику оцінки ризиків високого рівня і дає можливість визначення пріоритетів та хронології дій. У методах оцінки ризику даного виду фактичні або передбачувані фізичні активи оцінюються з точки зору вартості заміни або відновлення (тобто кількісні заходи). Ця вартість потім переводиться в ту ж якісну шкалу, яка використовується для інформації. Фактичні або передбачувані програмні активи оцінюються таким же чином, як і фізичні активи - Ідентифікується вартість придбання або відновлення, а потім переводиться в ту ж якісну шкалу, яка використовується для інформації. Крім того, якщо вважається, що будь-яка прикладна програми має власні притаманні їй вимоги щодо конфіденційності або цілісності (наприклад, якщо вихідний текст програми сам по собі є комерційно критичним), вона оцінюється таким же чином, як і інформація. Здійснити оцінку ризику за такою методикою може звичайний співробітник компанії за невеликі затрати часу.

2.4 Рекомендації про прийняття рішень на основних етапах моделі процесу УРІБ

На етапі встановлення контексту, по-перше, визначити ціль процесу управління ризиками :

– підтримка системи менеджменту інформаційної безпеки у загальному випадку;

– планування безперервності ведення бізнесу: якщо для підприємство дуже важливо не зупиняти процес, від вибору цієї цілі залежить подальша обробка ризику, тобто компанія максимально знижуватиме не ризик, а кількість ризиків, яким задано контрзаходів для зменшення рівня, буде значно більша, ніж в інших.

По-друге, до критеріїв оцінки ризику віднести цінність активу, від низького до найвищого: від рівня збитку (грошового або затрат часу на поновлення), що понесе компанія за спотворення, знищення, крадіжку або розкриття. До критеріїв прийняття (збереження) ризику враховувати лише ті, що матимуть найнижчі рівні ризику, якщо розрахунки показали найвищі рівні ризику, то в залежності від витрат здійснити або передачу, або зниження, або уникнення ризику.

На етапі ідентифікації ризику необхідно визначити загрози відповідно до наявності їх ознак.

На етапі оцінювання ризику використати методику стандарту ISO/IEC 27005:2011 за допомогою матриці зумовлених значень. Вона базується на достатньо простих табличних методах і не передбачає застосування спеціалізованого програмного інструментарію та високої кваліфікації аудитора.

2.5 Характеристика об’єкта інформаційної діяльності

2.5.1 Характеристика підприємства

У цій кваліфікаційній роботі апробацію рішень виконувалось в товаристві з обмеженою відповідальністю «Еталон-Прилад». Об’єктом інформаційної діяльності виступатимуть приміщення, в яких обробляється інформація з обмеженим доступом, що відноситься до відділу розробки та тестування. Офісна будівля, у якій розміщено підприємство, знаходиться за адресою: Україна, Харківська область, місто Харків, вулиця Клочківська, 295. Офіс підприємства розташований на першому поверсі прибудови житлового будинку.

Основним направленням функціонування підприємства є реалізація вимірювальних приладів, таких як метрологічне обладнання, прилади для лабораторій, індивідуальні прилади (мультиметри, струмові кліщі), кабельне обладнання, прилади для енергетики, щитові аналогові і цифрові прилади, датчики тиску та програмного забезпечення; надання послуг з ремонту вимірювальних приладів; розробка вимірювальних приладів та комплексних систем реєстрації та збору даних електричних величин.

2.5.2 Характеристика інформаційного середовища

За результатами аналізу складено таблицю особливостей функціонування інформаційного середовища об’єкту автоматизованої системи на об’єкті інформаційної діяльності товариства з обмеженою відповідальністю «Еталон-Прилад». Дані приведено у таблиці 2.3.

Таблиця 2.3 - Визначення доступу до інформації на ОІД

Інформація	Право-вий режим	Вид носія	Критичні властивості			Особи, що мають доступ	Місце-знаходження інформації
			К	Ц	Д		
1	2	3	4	5	6	7	8
Організаційно – статутна документація	Відкрита інформація	Паперовий, електронний	-	Ц1	Д1	усі співробітники	ПК директора та секретаря, кабінет секретаря
Інформація про підприємство, кількість робітників, систему оплати праці та ін.		Паперовий, електронний	-	Ц1	Д1	Співробітники, клієнти після запиту	ПК директора та секретаря, кабінет секретаря
Послуги підприємства		Паперовий, електронний	-	Ц1	Д1	усі	П
Інформація про товари, що надаються підприємством		Паперовий, електронний	-	Ц1	Д1	усі	
Правова інформація		Паперовий, електронний	-	Ц1	Д1	усі співробітники	ПК директора, продюсерів, бухгалтера
Ліцензійні згоди		Паперовий, електронний	-	Ц1	Д1	Усі	ПК та кабінет директора
Договори з партнерами	З обмеженим доступом	Паперовий	К1	Д2	Ц2	директор, працівники відділу продажу та бухгалтерії	сейф директора
Персональні дані працівників підприємства		Паперовий, електронний	К2	Д1	Ц1	директор, бухгалтер, секретар	ПК секретаря та бухгалтера, сейф секретаря
Приватні дані клієнтів підприємства		Електронний	К2	Д1	Ц2	директор, працівники відділу продажу	ПК директора, секретаря, бухгалтера, продюсерів

Продовження табл. 2.3

1	2	3	4	5	6	7	8
Інформація про комп'ютерну мережу	З обмеженим доступом	Паперовий, електронний	К1	Д1	Ц1	директор, сист. адмі-ністратор	кабінет сист. адміністр, ПК сист. адмі-ністратора
Організаційно – розпоряджувальна документація		Паперовий, електронний	К2	Д2	Ц2	усі співробітники	ПК та сейфи директора, секретаря
Бухгалтерська звітність		Паперовий, електронний	К2	Д2	Ц2	директор, бухгалтер	ПК та сейф бухгалтера
Фінансова інформація		Паперовий, електронний	К2	Д2	Ц2	директор, бухгалтер	ПК та сейф бухгалтера, ПК директора
Документи, пов'язані з торгівельною діяльністю		Паперовий, електронний	К1	Д2	Ц2	працівники відділу продаж, директор, бухгалтер, клієнти після запиту	ПК та кабінети відділу продаж, сервер баз даних
Схеми вимірювальних приладів, що розробляються		Паперовий	К1	Д1	Ц1	Спеціалісти по ремонту	Сейф спеціалістів по ремонту

У таблиці наведені наступні умовні позначення:

К1 – розкриття інформації призведе до незначних фінансових втрат підприємством та не буде суттєво впливати на авторитет підприємства.

К2 – розкриття інформації призведе до втрат, що відобразиться на роботі підприємства та/або суттєво вплине на авторитет.

К3 – розкриття інформації критичне для підприємства

Д1 – підприємство не зазнає значних втрат, якщо доступ до інформації буде відсутній протягом одного робочого дня.

Д2 – підприємство не зазнає значних втрат, якщо доступ до інформації буде відсутній від 4 до 8 годин.

Д3 – щоб підприємство не зазнало значних втрат, доступ до інформації потрібно відновити швидше, ніж за 4 години.

Ц1 – пошкодження інформації не призведе до значних втрат та/або не вплине значно на авторитет підприємства.

Ц2 – пошкодження інформації може завдати значних, але не критичних, втрат, та/або значно вплинути на авторитет організації.

Ц3 – пошкодження інформації завдасть критичних втрат та/або значно вплине на авторитет підприємства.

2.5.3 Умови функціонування і розміщення на місцевості

Підприємство розташовано у прибудові житлового будинку м. Харків з неактивним автомобільним та пішохідним потоком. Окрім офісу ТОВ "Еталон-Прилад" ніхто не займає прибудову.

Контроль доступу

Вхід на контрольовану зону підприємства (і через головний вхід, і через пожежний) здійснюється ключем та спеціальною електронною карткою. Охорона забезпечується агентством "КАСКАД".

Кожна кімната підприємства окремо закривається на ключі, які здаються директору або секретарю (на момент відпустки).

Вхід і перебування сторонніх осіб в контрольованій зоні можливі лише за дозволом директора підприємства. Відповідальна особа має вести неперервний нагляд за сторонніми особами.

Сусідні будівлі

З північного боку, через двополосну проїжджу частину розміщено 4 приватні житлові будинки.

Із західного боку на відстані 13 м розташований двоповерховий приватний житловий будинок, далі – двополосна проїжджа частина із зеленою зоною.

З південної сторони пустир, на відстані 36 м від границі ОІД розташована трансформаторна підстанція, від якої функціонує підприємство. Далі – дворова територія.

Зі східної сторони розміщено житлову будівлю, до якої здійснено

прибудову офісу.

2.5.4 Характеристика комунікацій

На підприємстві організовано кондиціювання приміщень за допомогою спліт-систем (використовується кондиціонери спліт Saturn ST-18HR Bio).

Стояки каналізації і водопостачання розташовані в туалеті, відгалуження води і каналізації йдуть тільки по туалетним кімнатам і в кімнату для відпочинку. Опалення централізоване, труби опалення спускаються вниз, у підвал. Радіатори алюмінієві, розміщені під вікнами.

Інтернет підключено провайдером ТОВ «Тріолан», одна лінія 1 Гб/с (канал зв'язку - вита пара CAT 5e). Щит з мережевим обладнанням провайдера знаходиться на першому поверсі офісної будівлі біля пункту охорони. Мережеві кабелі на підприємстві проходять над підвісною стелею.

Для переговорів з клієнтами та партнерами на підприємстві використовується мобільний зв'язок.

Освітлення виконане за допомогою люмінесцентних ламп денного освітлення.

Захисне заземлення іде по контуру несучих стін, по кутах будівлі забиті сталеві прути діаметром 20 мм (використано 5 заземлювачів довжиною 1000 мм), вертикально в ґрунт, з'єднані між собою методом зварювання. Від землі до шини заземлення використовувалася смуга 40х5, довжина 2м, зварюються послідовно.

Мережа електроживлення має параметри 220 В, 50 Гц. На підприємстві використовуються розетки типу F. Уся електромережа під'єднана до електрощита, що знаходиться у виділеному приміщенні. Електрощит підприємства з'єднаний з електрощитом житлової будівлі, що прибудована з офісом, яка з'єднана з трансформаторною підстанцією (відстань від ТП до ОІД 36 м).

На підприємстві діє система пожежної та охоронно сигналізації, що складається з централі, ліній зв'язку та датчиків. При спрацюванні централь

подає сигнал на пункт охорони офісної будівлі, а також вмикає світлозвукове оповіщення. Технічний склад системи сигналізації, що діє на ОІД, наведено в таблиці 2.4.

Таблиця 2.4 – Характеристика технічного складу сигналізації ОІД

Найменування	Характеристики	Кількість
Плата ППК 16 зон СА-10 Р	максимально 16 зон, 4 групи підтримка шлейфів: NO, NC, EOL, 2EOL/NO, 2EOL/NC, 6 виходів	1
Клавіатура SATEL INTEGRA S-EX	має екран для відображення подій і запрограмованих змін	1
Кабель для програмування Satel USB-RS	Конвертер USB-RS пропонує можливість підключення до комп'ютера пристроїв компанії SATEL, довжина 1,8 м	1
Комбінований датчик LC-102-PIGBSS	Комбінований пасивний інфрачервоний сповіщувач для внутрішньої установки (15 м, кут 90°) + датчик розбиття скла (10 м)	9
Датчик магніто-контактний на відкриття дверей СМК-1Э	Черговий режим – 10 мм, режим тривоги – 20 мм, не потребує живлення	12
Датчик пожежний димовий СПД-3	Робоча напруга 10-30 В, чутливість 0.05-0.2 дБ/м	16
Дротова внутрішня сирена ОСЗ-7	Світлозвукове оповіщення, гучність - 110 дБ Захист від розкриття за допомогою тампера	2
Кабель сигнальний Alarm 4х0.22 екранований	Мідний, довжина 300 м	1

Не діючі комунікації, що потребують демонтування, відсутні.

2.5.5 Характеристика обчислювальної системи

Відділ розробки та тестування ТОВ «Еталон-Прилад» має мережу, що є частиною мережі підприємства, яка включає 25 персональних комп’ютери та має вихід в мережу Інтернет, тому згідно з НД ТЗІ 2.5.005-99 «Класифікація автоматизованих систем та стандартні функціональні профілі захищеності від НСД» дана автоматизована система відноситься до класу АС 3.

В комп’ютерній мережі підприємства використовується топологія «ієрархічна зірка» (інакше «дерево»). Її відмінністю від «зірки» є використання декількох центральних вузлів, ієрархічно з’єднаних між собою

зв'язками типу «зірка». Для зв'язку комп'ютерів локальної мережі використовується стек протоколів TCP/IP.

Апаратний та програмний склад обчислюваної системи наведено у таблицях 2.5, 2.6, 2.7.

Таблиця 2.5 – Характеристики мережевого обладнання ОІД

Найменування	Характеристика	Кількість
Комутатор D-Link DES-1016A	16 портів Gigabit Ethernet, настільний некерований комутатор	2
Кабель UTP кат.5е	Довжина 300 м; 4 пари; оболонка FR-ПВХ (IEC 332.1); діаметр провідника з ізоляцією не більше 0,001 м; діаметр кабелю не більше 0,005 м	1

Таблиця 2.6 Характеристики ПК та комп'ютерна периферія

Найменування	Характеристики	Кількість
Персональні комп'ютери	Марка та модель системного блоку: SmartPC BASE 3362160 Процесор: Intel Celeron D 336 (2.8 ГГц) Оперативна пам'ять: DDR2-800, 2 Гб Відеокарта: інтегрована Intel GMA 3100 HDD: 160GB 7200rpm Блок живлення: 450 Вт Монітор: LG E1940S Клавіатура: Gembird KB-103-UA Миш: Gembird MUS-U-003	25
Epson K301	Настільний принтер, струменевий друк, розмір носія для друку - до А4, мережеві інтерфейси Ethernet	2
HP Scanjet 200 (L2734A)	Планшетний тип сканеру, область сканування до формату А4, мережеві інтерфейси відсутні	1

Таблиця 2.7 – Список програмного забезпечення

Де встановлено	Вид ПЗ	Назва та версія ПЗ	Тип ліцензії
ПК відділу продаж	Операц. система	Microsoft Windows 7 Home Edition (32bit)	GNU GPL
	Прикладне	Mozila Thunderbird	Mozilla Public License
		LibreOffice 4.4.3	GNU GPL
		Mozila Firefox 38	Mozilla Public License
		STDU Viewer 1.6	FreeWare
		VLC 2.5.1	GNU GPL
ПК директора та секретаря	Операц. система	Microsoft Windows 11 Home Edition (32bit)	GNU GPL
	Прикладне	Mozila Thunderbird	Mozilla Public License
		LibreOffice 4.4.3	GNU GPL
		Mozila Firefox	Mozilla Public License
		STDU Viewer 1.6	GNU GPL
		VLC 2.5.1	GNU GPL
		WinDjView 1.0.3	FreeWare
ПК системного адміністра-тора	Операц. система	Microsoft Windows 11 Home Edition (32bit)	GNU GPL
	Прикладне	7zip 6	GNU GPL
		AppServ 2.5.10 (Apache 2.2.8, PHP 5.2.6, MySQL 5.0.51b, phpMyAdmin-2.10.3)	GNU GPL
		LibreOffice 4.4.3	GNU GPL
		Mozila Firefox 38	Mozilla Public License
		STDU Viewer 1.6	FreeWare
		PuTTY	GNU GPL
		VLC 2.5.1	GNU GPL
		WinDjView 1.0.3	GNU GPL
ПК бухгалтерії	Операц. система	Microsoft Windows 11 Home Edition (32bit)	
	Прикладне	Mozila Thunderbird	Mozilla Public License
		LibreOffice 4.4.3	GNU GPL
		Mozila Firefox	Mozilla Public License
		STDU Viewer 1.6	GNU GPL
		VLC 2.5.1	GNU GPL
		WinDjView 1.0.3	FreeWare

Продовження табл. 2.7

Де встановлено	Вид ПЗ	Назва та версія ПЗ	Тип ліцензії
Сервер 1С: Підприєм-ство	Операц. система	Ubuntu 14.04 LTS Server Edition	GNU GPL
	Прикладне	Онлайн-бухгалтерія Dilovod	GNU GPL
Веб-сервер	Операц. система	Ubuntu 14.04 LTS Server Edition	GNU GPL
	Прикладне	Apache 2.2.8, PHP 5.2.6, phpMyAdmin-2.10.3	GNU GPL
	Захисне	IP-tables openSSH OpenSSl	GNU GPL
Сервер баз даних	Операц. система	Ubuntu 14.04 LTS Server Edition	GNU GPL
	Прикладне	MySQL 5.0.51b ftp	GNU GPL
	Захисне	IP-tables openSSH OpenSSl	GNU GPL

2.5.6 Характеристика середовища користувачів

Персонал підприємства ТОВ «Еталон-Прилад» налічує 30 чоловік, а саме:

– директор – 1 чоловік;
– офіс-менеджери– 20 чоловік;
– спеціалісти з ремонту вимірювальних приладів – 2 чоловіка;
– економіст– 1 чоловік;
– системний адміністратор – 1 чоловік;
– секретар – 1 чоловік;
– бухгалтер (виконавець функцій зам. директора) – 1 чоловік;
– прибиральник – 1 чоловік.

Директор є власником підприємства.

Далі наведено службові обов'язки працівників ТОВ «Еталон-Прилад», згідно з їх посадовими інструкціями.

2.6 Побудова моделі порушника для ОІД ТОВ «Еталон-Прилад»

Алгоритм розробки програмного забезпечення можна зобразити чотирма кроками, зображеними у таблиці 2.7. Кожен крок передбачає комунікацію між співробітниками відділу розробки і тестування.

Управління доступом використовує мандатний метод. Працівники мають доступ тільки до інформації, що відноситься до їх роботи.

Оскільки підприємство відноситься до класу малих, має невеликий рівень конкуренції, об'єкт інформаційної діяльності може піддаватись в основному впливу діяльності внутрішніх порушників. Зовнішнім порушником може бути тільки один - це хакер, який випадково натрапив на ресурси підприємства і заради втіхи, їх пошкодить. Вірогідність появи такого порушника занадто низька.

Внутрішніми порушниками по відношенню до ОІД – відділу розробки та тестування – можна вважати усіх співробітників ТОВ «Еталон-Прилад». Клієнти, партнери та обслуговуючий персонал офісної будівлі, де розташоване підприємство, не мають безпосереднього доступу до ОІД.

Введемо позначення для найімовірніших порушників ТОВ "Еталон-Прилад":

- ПВ1 - системний адміністратор;
- ПВ2 - офіс-менеджери;
- ПВ3 - спеціалісти по ремонту;
- ПВ4 - секретар;
- ПВ5 – бухгалтер, економіст;
- ПВ6 - прибиральник;
- ПВ7 - колишні співробітники(бухгалтер та економіст);
- ПВ8 – директор.

За результатами дослідження ОІД, створено модель порушника, наведену у таблиці 2.8.

Таблиця 2.8 - Модель порушника для ОІД ТОВ «Еталон-Прилад»

Вид інформації	Порушник	Рівень реалізації загрози	Тип об'єкту середи	Загроза безпеки	Спосіб реалізації загрози
I6	ПВ2, ПВ4, ПВ5, ПВ7, ПВ8	Рівень процесу торгівлі	Фізичні носії інформації	Порушення конфіденційності, цілісності, доступності	Крадіжка, псування, знищення документів
I7	ПВ4, ПВ5, ПВ7, ПВ8	Рівень бізнес процесу	Фізичні носії інформації, бази даних	Порушення конфіденційності, цілісності, доступності	Крадіжка, псування або знищення персональних даних
I8	ПВ2, ПВ7, ПВ8	Рівень процесу торгівлі	Бази даних	Порушення конфіденційності, цілісності, доступності	Крадіжка, зміна або знищення персональних даних клієнтів
I9	ПВ1, ПВ7, ПВ8	Рівень бізнес процесу	Фізичний носій; ПК	Порушення конфіденційності, цілісності, доступності	Крадіжка, зміна або знищення схеми комп'ютерної мережі
I10	Усі	Рівень бізнес процесу	Фізичний носій; бази даних	Порушення конфіденційності, цілісності, доступності	Крадіжка, несанкціонована зміна, або знищення документів
I11	ПВ5, ПВ7, ПВ8	Рівень бізнес процесу	Фізичний носій; ПК	Порушення конфіденційності, цілісності, доступності	Крадіжка, несанкціонована зміна, або знищення документів
I12	ПВ5, ПВ7, ПВ8	Рівень бізнес процесу	Фізичний носій; ПК	Порушення конфіденційності, цілісності, доступності	Крадіжка, несанкціонована зміна, або знищення документів

Продовження табл. 2.8

Вид інформації	Порушник	Рівень реалізації загрози	Тип об'єкту середи	Загроза безпеки	Спосіб реалізації загрози
І13	ПВ2, ПВ5, ПВ7, ПВ8	Рівень процесу торгівлі	Фізичний носій; ПК; бази даних	Порушення конфіденційності, цілісності, доступності	Перехват електронних документів та їх зміна та знищення. Зміна та знищення паперових торгівельних документів.
І14	ПВ3	Рівень процесу розробки	Фізичний носій	Порушення конфіденційності, цілісності, доступності	Крадіжка, несанкціонована зміна або знищення схем.
Вид інформації	Порушник	Рівень реалізації загрози	Тип об'єкту середи	Загроза безпеки	Спосіб реалізації загрози
І1, І3, І5	Усі	Рівень бізнес процесу	Фізичний носій; бази даних; ПК	Порушення доступності	Знищення прайс-листа, документації або правової інформації

2.7 Модель загроз для ОІД ТОВ «Еталон-прилад» та оцінка ризику

До розробки моделі загроз необхідно визначити, за якою методологією буде оцінюватися ризик інформаційної безпеки, і які фактори необхідно для неї враховувати. Оскільки на підприємстві вперше вводиться система МРІБ, то необхідно насамперед виконати оцінку високого рівня для визначення пріоритетів та хронології дій щодо інформаційної безпеки. Для цієї цілі нам підійде використання матриці зумовлених значень - простий і ефективний спосіб оцінки, який не вимагає розрахунків і призначення активам грошового еквіваленту.

Стандарт ISO/IEC 27005:2011, що пропонує визначення ризику інформаційної безпеки за допомогою матриці зумовлених значень, вимагає

насамперед визначити інформаційні активи підприємства, на які може вплинути загроза, враховуючи їх важливість для бізнес-цілей, ступінь залежності бізнесу від кожного інформаційного активу, рівень інвестицій в активи та активи, яким підприємство напряму надає цінності (наприклад, за вимогою законодавства).

Інформаційні активи були визначенні на етапі обстеження підприємства (визначені на ТОВ «Еталон-Прилад» інформаційні активи було наведено у таблиці 2.1) та класифіковані за важливістю для бізнесу за п'ятибальною шкалою:

0 – актив не має цінності для ведення бізнесу;

1 – актив має низьку цінність для бізнесу, реалізація загроз для нього не вплине значно на підприємство;

2 – актив має середню цінність для бізнесу, для усунення наслідків реалізації загрози підприємство буде змушене витратити кошти;

3 – при реалізації загроз для активу підприємство зазнає значних втрат;

4 – реалізація загрози для активу критично вплине на підприємство.

Таблиця 2.9 - Визначення цінності інформаційних активів, що відносяться до ОІД ТОВ «Еталон-Прилад»

Умовне позначення	Інформація	Правовий режим	Цінність
I1	Організаційно – статутна документація	Відкрита інформація	1
I2	Інформація про підприємство, кількість робітників, систему оплати праці, стан підприємства		0
I3	Послуги та товари підприємства		1
I4	Правова інформація		0
I5	Ліцензійні згоди		1
I6	Договори з партнерами	З обмеженим доступом	3
I7	Персональні дані працівників підприємства		2
I8	Дані про клієнтів		3
I9	Інформація про комп'ютерну мережу		1
I10	Організаційно-розпоряджувальна документація		2
I11	Бухгалтерська звітність		3
I12	Фінансова інформація		3
I13	Електронний документообіг		2
I14	Креслення вимірювальних приладів		2

Далі для визначення ризику за матрицею зумовлених значень необхідно оцінити загрози інформаційним активам. Ця оцінка повинна включати визначення, на які інформаційні активи впливає загроза, та властивості інформації, що порушуються у наслідок реалізації загрози інформаційних активів та вірогідність. Необхідно визначити джерела загроз: для даної кваліфікаційної роботи це загрози персоналу та фізичної безпеки. Введемо позначення джерел загроз, що не стосуються порушників:

ПД - природні катаклізми;

ЕД - внутрішня електромережа;

ОС - операційна система;

ПК - персональний комп'ютер;

КО - телекомунікаційне обладнання.

Вірогідність загрози оцінюється якісно: висока, середня, низька. Результат оцінки наведено у таблиці 2.10.

Таблиця 2.10 – Визначення загроз інформаційним активам ОІД

Позначення	Описання загрози	Вірогідність	Іінформ. актив, що підлягає впливу	Джерело загрози	Властивості, що порушуються			
					К	Ц	Д	С
1.1	Пожежа в наслідок несправності електроприладів	Низька	І1-І14	ПД		+	+	+
1.2	Втрата електропостачання	Середня	І1-І5, І7-І13	ЕД			+	

Продовження табл. 2.10

Позна-чення	Описання загрози	Вірогід-ність	Іінформ. актив, що підлягає впливу	Дже-рело загрози	К	Ц	Д	С
2.1	Крадіжка носіїв або документів або обладнання	Середня	I6,I7,I10,I11,I12	ПВ7	+		+	
			I6,I8,I10,I13	ПВ2	+		+	
2.2	Помилка в використанні	Середня	I1,I2,I4,I5,I7,I9, I10	ПВ1		+	+	
			I1,I4,I8,I10,I13	ПВ2		+	+	
			I1,I2,I5,I4,I7,I10 ,I13	ПВ4		+	+	
			I1-I5,I7,I10,I11,I12	ПВ5		+	+	
2.2	Помилка в використанні	Середня	I1-I5,I7,I9,I10,I11,I 12	ПВ7		+	+	
2.3	Втрата носіїв або документів	Висока	I7,I9,I10	ПВ1	+			+
			I8,I10,I13	ПВ2	+			+
			I7,I10,I13	ПВ4	+			+
			I7,I10,I11,I12	ПВ5	+			+

Продовження табл. 2.10

Позна-чення	Описання загрози	Вірогід-ність	Іінформ. актив, що підлягає впливу	Дже-рело загрози	К	Ц	Д	С
2.3	Втрата носіїв або документів	Висока	I7,I9,I10	ПВ1	+			+
			I8,I10,I13	ПВ2	+			+
			I7,I10,I13	ПВ4	+			+
			I7,I10,I11,I12	ПВ5	+			+
			I7,I9,I10,I11,I12	ПВ7	+			+
			I7,I10	ПВ8	+			+
2.4	«Чорна пошта»	Середня	I7,I9,I10	ПВ1	+			
			I8,I10,I13	ПВ2	+			
			I7,I10,I13	ПВ4	+			
			I7,I10,I11,I12	ПВ5	+			
			I7,I9,I10	ПВ7	+			
2.5	Зловживання правами доступу	Середня	I8,I10,I13	ПВ2	+	+	+	
			I7,I10,I13	ПВ4	+	+	+	
			I7,I10,I11,I12	ПВ5	+	+	+	
			I7,I9,I10,I11,I12	ПВ7	+	+	+	
3.1	Відмова телекомунікаційного обладнання	Середня	I7,I13	КО			+	+
3.2	Програмні збої	Середня	I1-I5, I7-I13	ОС			+	

Продовження табл. 2.10

Позна-чення	Описання загрози	Вірогід-ність	Інформ. актив, що підлягає впливу	Дже-рело загрози	К	Ц	Д	С
3.3	Відмова роботи ПК	Середня	I1-I5, I7-I13	ПК			+	

Останнє, що необхідно визначити, – готовність вразливості, через яку може реалізуватися загроза. Враховуються зручність (можливість) використання вразливості джерелом загроз, складність використання, необхідні кошти, можливість застосування неспеціалізованої апаратури. У результаті оцінки вразливостей була побудована таблиця 2.11.

Таблиця 2.11 – Визначення готовності вразливостей ОІД

Загроза	Вразливість	Позначення	Готовність
1.1	Застаріла система пожежогасіння	A1	Середня
1.2	Несправність трансформаторів	A2	Низька
2.1	Відсутність камер відео нагляду	A3	Висока
2.2	Неналаштований мандатний доступ	A4	Висока
2.3	Відсутність відповідальності за втрату носіїв інформації	A5	Висока
2.4	Моніторингу поштових скриньок	A6	Висока
2.5	Неналаштований мандатний доступ	A4	Висока
3.1	Застаріле телекомунікаційне обладнання	A7	Середня
3.2	Використання старої версії Linux	A8	Середня
3.3	Недостатнє обслуговування апаратних засобів	A9	Середня

Рівень ризику встановлюється за визначеними раніше трьома критеріями: цінність інформаційного активу, вірогідність загрози та рівень вразливості, - відповідно до таблиці (2.12), що була описана в другому розділі.

Підсумкові результати оцінки ризику наведені у таблиці 2.12.

Таблиця 2.12 – Оцінка ризику для ОІД

Інформ. активи	Цін-ність активу	Загроза	Вірогідність загрози	Вразли-вість	Готовність вразли-вості	Рівень ризику
I1,I3,I5,I9	1	1.1	Низька	A1	Середня	2
I7,I10,I13,I14	2	1.1	Низька	A1	Середня	3
I6,I8,I11,I12	3	1.1	Низька	A1	Середня	4
I2,I4	0	1.1	Низька	A1	Середня	1
I2,I4	0	1.2	Середня	A2	Низька	1
I1,I3,I5, I9	1	1.2	Середня	A2	Низька	2
I7,I10,I13	2	1.2	Середня	A2	Низька	3
I8,I11,I13	3	1.2	Середня	A2	Низька	4
I6,I8,I11,I12	3	2.1	Середня	A3	Висока	6
I7,I10,I13	2	2.1	Середня	A3	Висока	5
I2,I4	0	2.2	Середня	A4	Висока	3
I1,I3,I5,I9	1	2.2	Середня	A4	Висока	4
I7,I10,I13,I14	2	2.2	Середня	A4	Висока	5
I8,I9,I10,I11,I12,I13	3	2.2	Середня	A4	Висока	6
I9	1	2.3	Висока	A5	Висока	5
I7,I10,I13	2	2.3	Висока	A5	Висока	6
I8,I11,I12	3	2.3	Висока	A5	Висока	7
I9	1	2.4	Середня	A6	Висока	4
I7,I10,I13	2	2.4	Середня	A6	Висока	5
I8 ,I11,I12	3	2.4	Середня	A6	Висока	6
I9	1	2.5	Середня	A4	Висока	4
I7,I10,I13	2	2.5	Середня	A4	Висока	5
I8,I11,I12	3	2.5	Середня	A4	Висока	6
I7, I13	3	3.1	Середня	A7	Середня	5
I2,I4	0	3.2	Середня	A8	Середня	2
I1,I3,I5, I9	1	3.2	Середня	A8	Середня	3
I7,I10,I13	2	3.2	Середня	A8	Середня	4
I8,I11,I13	3	3.2	Середня	A8	Середня	5
I2,I4	0	3.3	Середня	A9	Середня	2
I1,I3,I5, I9	1	3.3	Середня	A9	Середня	3
I7,I10,I13	2	3.3	Середня	A9	Середня	4
I8,I11,I13	3	3.3	Середня	A9	Середня	5

Останній кроком у процесі управління ризиком після його оцінки є визначення необхідних контрзаходів для зниження ризику до прийнятного (низького) рівня.

2.8 Організаційні заходи з управління ризиками інформаційної безпеки ТОВ «Еталон-Прилад»

Відповідно до методики, що використовує матрицю зумовлених значень, ризики зі значенням 0-2 – низькі, 3-5 – середні, 6-7 – високі. У першу чергу необхідно розглянути і обробити високі ризики, потім середні, низькі ризики можна одразу прийняти.

Згідно із таблицею високі ризики несуть такі вразливості:

- недостатня кількість камер відео нагляду;
- неналаштований мандатний доступ;
- відсутність відповідальності за втрату носіїв інформації.

Джерелом загроз, що може скористатися цими вразливостями для реалізації загроз, є всі співробітники компанії, що працюють на закріплених робочих станціях.

Більшість середніх ризиків виникають від вразливостей, що виходять із застарілого обладнання або програмного забезпечення, що може давати збої в системі, але уникнути або зменшити ризик цих загроз просто неможливо, тому що в компанії просто не вистачить грошей на заміну.

Не зважаючи на те, що низькі ризики приймаються, якщо можливі організаційні заходи для зниження ризику, що не потребують значних коштів на їх введення та не будуть значно заважати роботі працівників, їх також варто застосувати.

Ґрунтуючись на отриманих за допомогою управління ризиками даних, для підвищення рівню захищеності ТОВ «Еталон-Прилад» слід застосувати наступні заходи:

– здійснити встановлення камер відеонагляду до вже встановленої системи відеонагляду в кількості 6 шт. згідно плану: одна у директора, одна у системного адміністратора та по дві камери в кабінетах офіс-менеджерів;

– покласти на системного адміністратора обов'язки за виконанням налаштування мандат орного доступу;

– необхідно регулярно проводити тренінги з інформаційної безпеки для усіх співробітників, розкривати нові загрози, що виникають в інформаційній сфері;

– розробити заходи відповідальності за розголошення конфіденційної інформації та втрати всієї інформації, що має цінність;

– раз на місяць має проводитися ревізія апаратних засобів ОІД.

2.9 Висновки до другого розділу

В даному розділі був проведений аналіз інформативних ознак на етапах ідентифікації ризиків та встановлення контексту, а також при виборі методик оцінки ризиків. Так, етап ідентифікації ризиків тісно залежить від середи знаходження та виду самого підприємства; етап встановлення контексту – від розмірів підприємства та його спеціалізації.

Також був проведений порівняльний аналіз методик оцінки ризиків. За допомогою проведеного аналізу було визначено, які методики для яких видів підприємств підходять. Так, для розглянутого у наступному розділі підприємства доцільнішим вибором буде метод з використанням матриці зумовлених значень.

Були визначений перелік рекомендацій щодо прийняття рішень на основних етапах моделі процесу УРІБ. Даний перелік рекомендацій допоможе значно оптимізувати процес управління ризиками інформаційної безпеки.

Також була надана характеристика підприємства ТОВ «Еталон-Прилад». Були висвітлені наступні моменти: основна інформація (розмір підприємства, його вид, кількість співробітників, місцезнаходження

підприємства та ін.), інформація щодо інформаційних активів організації та інформація щодо структури інформаційної системи.

Були визначені усі загрози та вразливості щодо даного підприємства, вказані їх якісні величини, сформована модель порушника.

Була проведена оцінка ризиків інформаційних активів досліджуваного підприємства.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Вступ

Актуальність питань, розглянутих в спеціальній частині кваліфікаційної роботи, пов'язані із використанням визначених у процесі управління ризиком інформаційної безпеки оптимальних за ефективністю і витратами засобів контролю ризиків і засобів захисту інформації, що враховують цілі і завдання бізнесу. У спеціальній частині були розроблені рекомендації для підвищення захищеності об'єкту інформаційної діяльності ТОВ «Еталон-Прилад».

Метою даного розділу є розрахунки економічної ефективності впровадження цих рекомендацій та підтримки їх виконання.

Для розрахунку вище вказаного необхідно:

– розрахувати капітальних витрат на реалізацію запропонованих рекомендацій;

– розрахувати річні експлуатаційні витрати на виконання рекомендацій;

– сума річних амортизаційних відрахувань на апаратні засоби, необхідні для виконання рекомендацій;

– показники економічної ефективності впровадження системи захисту на підприємстві.

3.2 Розрахунок капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Фіксовані витрати на впровадження системи розраховуватимуться за формулою (3.1):

$$К = К_{пр} + К_{навч} + К_{н} + К_{зпз}, \text{ грн.} \quad (3.1)$$

де $К_{пр}$ – вартість впровадження, грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, грн;

$К_{н}$ – витрати на встановлення та налагодження прийняття мір протидії витокам інформації, грн;

$К_{зпз}$ –вартість закупівель, грн.

Розрахунок капітальних витрат буде проводитися на прикладі впровадження засобів захисту інформації: резервне копіювання, блок безперервного живлення, кодовий замок, журнал обліку носіїв інформації, контроль стану обладнання, інструктаж з ІБ, Firewall Analyzer Standard Edition, ESET Internet Security.

3.2.1 Розрахунок заробітної плати системного адміністратора

Обліком носіїв інформації, резервним копіюванням, встановленням кодового замка, встановленням фаєрволу, антивірусу та обліком носіїв інформації займається системний адміністратор.

Заробітна плата при простій часовій системі оплати праці визначається за формулою:

$$З = ТС* Ф , \quad (3.2)$$

де ТС – тарифна ставка привласненого робітникові кваліфікаційного розряду в одиницю часу (година, день, місяць), грн;

Ф – фактично відпрацьований час;

Почасова тарифна ставка системного адміністратора складає ТС = 200 грн/год.

Час на налагодження резервного копіювання займе 1 год.

$$З = ТС* Ф = 200*1=200 \text{ грн.}$$

Час на встановлення блоку безперервного живлення займе 0,5 год, затрати:

$$З = ТС* Ф = 200*0,5=100 \text{ грн.}$$

Час на встановлення кодового замку займе 1 год, затрати:

З = ТС* Ф = 200*1 = 200 грн.

Час на встановлення фаєрволу займе 0,5 год, затрати:

З = ТС* Ф = 200*0,5 = 100 грн.

Час на встановлення антивірусу займе 0,5 год, затрати:

З = ТС* Ф = 200*0,5 = 100 грн.

Час на створення журналу обліку носіїв займе 4 год, затрати:

З = ТС* Ф = 200*4 = 800 грн.

3.2.2 Розрахунок капітальних витрат

В таблиці 3.1 наведена кількісно-вартісна характеристика заходів, що впроваджується в підприємстві великого бізнесу.

Таблиця 3.1 – Кількісно-вартісна характеристика заходів

Міри	Характеристика	Вартість
Резервне копіювання	SSD Samsung T7 2TB Shield Blue (MU-PE2T0R) 2022, up to 1050MB/s, www.rozetka.com.ua	11499
Блок безперервного живлення	Powercom BNT-800AP USB, www.rozetka.com.ua	4500
Кодовий замок на серверну	RZ M-1603BK-30, встановлюється своїми силами, www.rozetka.com.ua	820
Облік носіїв інформації	Створення журналу (4 год., переоблік раз на тиждень)	400
Фаєрвол	Firewall Analyzer Standard Edition, hhttps://www.fortsoft.com.ua/	18486
Антивірус	ESET Internet Security www.rozetka.com.ua	1276

Фіксовані витрати на проектування та впровадження заходів захисту інформації складатимуть:

Резервне копіювання:

$$К = 200 + 11499 = 11699 \text{ грн.}$$

Блок безперервного живлення:

$$К = 100 + 4500 = 4600 \text{ грн.}$$

Кодовий замок на серверну:

$$К = 200 + 820 = 1020 \text{ грн.}$$

Облік носіїв інформації:

$$К = 400 \text{ грн.}$$

Фаєрвол:

$$К = 100 + 18486 = 18586 \text{ грн.}$$

Антивірус:

$$К = 100 + 1276 = 1376 \text{ грн.}$$

Загальні затрати складуть 37681 грн.

3.3 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проєктування за визначений період (наприклад, рік), що виражені у грошовій формі.

Під «витратами на керування системою» маються на увазі витрати, пов'язані з керуванням й адмініструванням компонентів системи інформаційної безпеки. До цієї статті витрат можна віднести наступні витрати:

- навчання адміністративного персоналу й кінцевих користувачів;
- амортизаційні відрахування від вартості обладнання та ПЗ;
- заробітна плата персоналу;
- навчальні курси й сертифікація обслуговуючого персоналу;
- технічне й організаційне адміністрування й сервіс.

До експлуатаційних витрат віднесено:

- заробітну плату співробітника системного адміністратора;
- витрати на ліцензію антивірусу;
- витрати на резервне копіювання;
- витрати на замок на серверну;
- витрати на ліцензію фаєрволу;
- витрати на блок безперебійного живлення;
- витрати на облік носіїв інформації;

Річні поточні витрати на функціонування системи заходів протидії загрозам інформації визначаються за формулою (3.3):

$$C = C_1 + C_2 + \ldots + C_n, \text{ грн}, \quad (3.3)$$

де С – вартість підтримки заходу протидії загрозам інформації;

n – порядковий номер заходів протидії загрозам інформації.

Обліком носіїв інформації, резервним копіюванням, підтримкою фаєрволу, антивірусу та обліком носіїв інформації займається системний адміністратор.

Заробітна плата системного адміністратора складає $З_{СА}$ = 200 грн/год.

Час на резервного копіювання займе 0,1 год/день.

$$С = ТС^* Ф = 200*0,1*250 = 5000 \text{ грн.}$$

Час на підтримку фаєрволу займе 0,2 год/тиждень, затрати:

$$С = ТС^* Ф = 200*0,2*50 = 2000 \text{ грн.}$$

Час на підтримку антивірусу займе 0,2 год/тиждень, затрати:

$$С = ТС^* Ф = 200*0,2*50 = 2000 \text{ грн}$$

Час на створення журналу обліку носіїв займе 1 год/тиждень, затрати:

$$С = ТС^* Ф = 200*1*50 = 10000 \text{ грн.}$$

Затрати на продовження ліцензії антивірусу складають 700 грн.

Затрати на продовження ліцензії фаєрволу складають 7200 грн.

Значення загальних річних поточних витрат складає:

$$C = 5000 + 2000 + 2000 + 10000 + 700 + 7200 = 26900 \text{ грн.}$$

3.4 Оцінка можливого збитку від порушення інформаційної безпеки

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

- порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
- порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
- порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);
- порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

3.5 Визначення збитку від поломок обладнання

Запобігти поломкам обладнання практично неможливо. Природньо, первинна передумова наступна: витрати на ремонт або заміну деяких деталей обладнання не повинні перевищувати вартість самого обладнання.

Вихідні дані для підрахунку збитку:

–час простою внаслідок поломки, $t_п$ (в годинах), $t_п = 3$ год;

–час відновлення після поломки, $t_в$ (в годинах), $t_в = 2$ год;

–час повторного введення втраченої інформації, $t_{ви}$ (в годинах), $t_{ви} = 1$ год;

–заробітна плата обслуговуючого персоналу, Z_0 (грн. в місяць з податками), $Z_0 = 25000$ грн.;

–заробітна плата співробітників, Z_c (грн. в місяць з податками), Z_c = 20000 грн.;

–кількість обслуговуючого персоналу, N_0, N_0 = 2;

–число співробітників, N_c, N_c = 30;

–прибуток , O (грн. на рік), O = 9200000 грн.;

–вартість заміни обладнання та запасних частин, виправлення помилок в роботі системи, $П_{зч}$ (грн.), $П_{зч}$ = 0 грн;

–число зламаного обладнання, I, I = 1;

–число поломок на рік, n, n = 7.

Вартість втрат від зниження продуктивності співробітників несправного обладнання розраховується за формулою 3.10:

$$П_п = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_п, \text{ грн.}, \quad (3.4)$$

де місячний фонд робочого часу при 40-а годинний робочий тиждень 176 годин.

Підставивши вихідні дані отримаємо:

$$П_п = (30*20000/160)*3 = 11250 \text{ грн.}$$

Вартість відновлення зламаного обладнання розраховується за формулою 3.11:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \quad (3.5)$$

де $П_{ви}$ – вартість повторного введення інформації (формула 3.12),

$П_{пв}$ – вартість відновлення обладнання (формула 3.13).

$$П_{ви} = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_{ви}, \text{ грн.} \quad (3.6)$$

$$П_{пв} = \frac{\sum Z_o}{\frac{N_o}{160}} \cdot t_в, \text{ грн.} \quad (3.7)$$

Отримаємо:

$$П_{ви} = (30*20000/160)*1 = 3750 \text{ грн.}$$

$$П_{пв} = (2*25000/160)*2 = 625 \text{ грн.}$$

Вартість заміни обладнання та запасних частин, виправлення помилок в системі, $П_{зч}$ (грн.)

$$П_{зч} = 0 \text{ грн.}$$

Підставивши отримані результати в загальну формулу отримаємо:

$$П_{в} = 3750 + 625 + 0 = 4375 \text{ грн.}$$

Втрачена вигода від простою зламаного обладнання становить та розраховується за формулою 3.14 й 3.15 відповідно:

$$U = П_{п} + П_{в} + V, \text{ грн.} \quad (3.8)$$

$$V = \frac{O}{Fг} \cdot (t_{п} + t_{в} + t_{ви}), \text{ грн,} \quad (3.9)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить 2080 годин.

$$V = (9200000/2080)*(3+2+1) = 26538,46 \text{ грн.}$$

$$U = 11250 + 4375 + 26538,46 = 42163,46 \text{ грн.}$$

Таким чином, загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складе (формула 3.16):

$$ОУ = \sum_{n}\sum_{I} U, \text{ грн.} \quad (3.10)$$

$$ОУ = 7 * 1 * 42163,46 = 295144,22 \text{ грн.}$$

3.6 Загальний ефект від впровадження моделі

Загальний ефект від впровадження моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компанії визначається за формулою 3.17 з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = ОУ \cdot R - C, \text{ грн}, \quad (3.11)$$

де $ОУ$– загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн;

R – очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для компанії, грн.

Таким чином, загальний ефект від впровадження становить:

$$E = 295144{,}22 * 0{,}4 - 26900 = 91157{,}69 \text{ грн.}$$

3.7 Визначення та аналіз показників економічної ефективності моделі

Оцінка економічної ефективності моделі, розглянутої у спеціальній частині кваліфікаційної роботи, здійснюється на основі визначення та аналізу коефіцієнта повернення інвестицій *ROSI* (Return on Investment for Security) за формулою 3.18 та терміну окупності капітальних інвестицій T_o за формулою 3.19.

$$ROSI = \frac{E}{K}, \text{ частки одиниці}, \quad (3.12)$$

де E – загальний ефект від впровадження системи захисту, грн.;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Підставивши відповідні значення, маємо:

$$\text{ROSI} = 91157{,}69 / 37681 = 2{,}42$$

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань).

Проєкт визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта формула 3.20:

$$ROSI > (N_{деп} - N_{інф})/100) \quad (3.13)$$

де $N_{деп}$ – річна депозитна ставка, %;

$N_{інф}$ – річний рівень інфляції, %.

Підставивши відповідні значення, маємо:

$$ROSI > (17 - 21,8)/100),$$

$$2,42 > -0,048$$

Отже, проєкт є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.14)$$

Підставимо значення:

$$T_o = 1 / 2,42 = 0,41 \text{ року.}$$

3.8 Висновок

Розрахувавши збитки від реалізації можливих несправностей, які склали 295144,22 грн., і порівнявши їх з витратами на забезпечення підтримки працездатності системи 26900 грн., та витратами на розробку моделі 37681 грн., можна зробити висновок, що витрати на забезпечення інформаційної безпеки є не значними у співвідношенні до збитків, впровадження системи є економічно доцільним заходом, термін окупності системи безпеки становить 0,41 року. Для подальшого розвитку діяльності підприємства впровадження даних заходів є необхідною умовою для виконання.

ВИСНОВКИ

У кваліфікаційній роботі розв’язано актуальне наукове завдання щодо розробки переліку рекомендацій для оптимізації процесу управління ризиками інформаційної безпеки. В ході розв’язання поставлених задач були отримані наступні наукові та практичні результати:

1 Проведено аналіз інформативних ознак на комерційних підприємствах. Це дало змогу чітко визначити дії процесу управління ризиками інформаційної безпеки в інформаційній системі та акцентувати увагу на найважливіших його аспектах.

2 Проаналізовано інформативні ознаки на етапах оцінки ризиків та встановлення контексту. Встановлено, що етап ідентифікації ризиків тісно залежить від середи знаходження підприємства та його виду; етап встановлення контексту – від розмірів підприємства та його спеціалізації.

3 На основі проведеного порівняльного аналізу методик оцінки ризиків запропоновано використання для малих підприємств методики з використанням матриці зумовлених значень, так як вона не потребує спеціальних знань та фінансових вливань.

4 Сформований перелік рекомендацій щодо прийняття рішень на основних етапах моделі процесу управління ризиками інформаційної безпеки, який повинен допомогти значно оптимізувати процес управління ризиками інформаційної безпеки.

5 Шляхом застосування на прикладі окремо вибраного підприємства була доведена практична цінність при використанні описаного переліку рекомендацій під час виконання процесу УРІБ. Ефективність впроваджених методик доведена у грошовому еквіваленті.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1 Міжнародний стандарт ISO/IEC 27005:2011 «Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки» [Електронний ресурс] - Режим доступу: www/ URL: https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf.

2 Закон України «Про інформацію» [Електронний ресурс] / Київ, Верховна Рада України - Режим доступу : www/ URL: http://zakon5.rada.gov.ua/laws/show/2657-12 - 21.05.2015 г. - Загл. з екрану.

3 Загрози інформаційній безпеці у банківських установах [Електронний ресурс] - Режим доступу: www/ URL: http://essuir.sumdu.edu.ua/bitstream/123456789/34067/1/Borysova_banking%20establishment.pdf.

4 Операційний менеджмент [Електронний ресурс] - Режим доступу: www/ URL: http://library.if.ua/book/145/9626.html.

5 Страхові компанії [Електронний ресурс] - Режим доступу: www/ URL: http://www.ukrreferat.com/index.php?referat=40165.

6 Управління персоналом в контексті забезпечення інформаційної безпеки будівельних підприємств [Електронний ресурс] - Режим доступу: www/ URL: http://oaji.net/articles/2014/797-1415388159.pdf.

7 Методичні вказівки до виконання економічної частини дипломного проєкту (для студентів напряму підготовки 1701 Інформаційна безпека)/ Упорядн.: О.Г. Вагонова, Ю.О. Волотковська, Н.М. Романюк. – Дніпропетровськ: ДВНЗ "Національний гірничий університет", 2013. – 17 с.

8 Міжнародний стандарт IEC 31000:2010 «Менеджмент ризику. Принципита керівництво» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=51073

9 Левадний С.М., оцінка інформаційних ризиків [Електронний ресурс] - Режим доступу: www/ URL: http://www.rusnauka.com/21_SEN_2014/Informatica/4_174674.doc.htm.

10 Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції [Електронний ресурс] - Режим доступу: www/ URL: http://www.nbuv.gov.ua/old_jrn/natural/Vnulp/ISM/2008_610/03.pdf.

11 An introduction to Risk Management [Електронний ресурс] - Режим доступу: www/ URL: http://www.dphu.org/uploads/attachements/books/books_3632_0.pdf

12 An overview of practical risk assessment methodologies – GIAC [Електронний ресурс] - Режим доступу: www/ URL: https://www.giac.org/paper/gsec/3287/overview-practical-risk-assessment-methodologies/105426

13 Risk Identification and Analysis – GIAC [Електронний ресурс] - Режим доступу: www/ URL: http://www.nap.edu/read/11183/chapter/6

14 Risk Identification [Електронний ресурс] - Режим доступу: www/ URL: http://www.cin.ufpe.br/~if717/Pmbok2000/pmbok_v2/wbs_11.2.html

15 Risk Management Guide for Information Technology Systems [Електронний ресурс]. – Режим доступу : www/ URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

16 Сфера послуг [Електронний ресурс]. – Режим доступу : www/ URL: http://epi.cc.ua/sfera-uslug-33509.html

17 Капітальні вкладення [Електронний ресурс]. – Режим доступу : www/ URL: http://ua-referat.com/Капітальні_вкладення

18 Методика визначення ефективності капітальних вкладень [Електронний ресурс]. – Режим доступу : www/ URL: http://pidruchniki.com/1541010436255/ekonomika/metodika_viznachennya_efektivnosti_kapitalnih_vkladen

19 Оптимізаційні планові розрахунки нововведень продукції та планування витрат на підготовку і освоєння виробництва нової продукції [Електронний ресурс]. – Режим доступу : www/ URL: http://buklib.net/books/29468/

20 Розрахунок річних експлуатаційних витрат [Електронний ресурс]. – Режим доступу : www/ URL: http://studopedia.org/6-128587.html

21 Визначення експлуатаційних витрат та результатів проєктування [Електронний ресурс]. – Режим доступу : www/ URL: http://pidruchniki.com/10480304/ekonomika/viznachennya_ekspluatatsiynih_vitrat_rezultativ_proektuvannya

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Розділ 1	27	
6	А4	Розділ 2	46	
7	А4	Розділ 3	10	
8	А4	Висновки	2	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація_Мамчіц.ppt

2 Кваліфікаційна робота_Мамчіц.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22-1 Мамчіца Є.Ю.
на тему: «Методика та заходи вдосконалення процесу управління ризиками інформаційної безпеки комерційного підприємства»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 102 сторінках.

Об'єктом дослідження є процес управління ризиками інформаційної безпеки на комерційних підприємствах.

Мета кваліфікаційної роботи: підвищення рівня інформаційної безпеки шляхом розробки рекомендацій з оптимізації процесу управління ризиками інформаційної безпеки. Мета є актуальною, оскільки вона спрямована на виявлення і запобігання ризикам інформаційної безпеки і пропонує ефективні засоби вирішення проблем на комерційному підприємстві.

У роботі проаналізований процес управління ризиками інформаційної безпеки.

У спеціальній частині складений перелік рекомендацій з оптимізації процесу управління ризиками інформаційної безпеки та наведений приклад їх використання.

В економічному розділі проведено розрахунок вартості проектування та проведення визначення величини ризиків на торгівельному підприємстві та зроблено висновок щодо доцільності проведення визначення величини ризиків на підприємствах.

Наукова новизна полягає у складанні переліку рекомендацій, який допоможе оптимізувати процес управління ризиками інформаційної безпеки.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Трубка Д.А. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доц. **Ковальова Ю.В.**