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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студентки *Ігнатової Катерини Євгенівни*

академічної групи *125-16-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка підсистеми захисту від несанкціонованого доступу інформаційно-телекомунікаційної системи Корпорації "N"*

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

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Ігнатової Катерині Євгенівні* **академічної групи** *125-16-3*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка підсистеми захисту від несанкціонованого доступу інформаційно-телекомунікаційної системи Корпорації "N"***

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

Розділ	Зміст	Термін виконання
Розділ 1	Обстеження інформаційно-телекомунікаційної системи Корпорації "N".	29.03.2020
Розділ 2	Проведено аналіз середовища інформаційно-телекомунікаційної системи Корпорації "N", розробка політик безпеки.	24.05.2020
Розділ 3	Економічна доцільність впровадження політики безпеки, розрахунок витрат та ефективності впровадження КСЗІ.	14.06.2020

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2020р.

Дата подання до екзаменаційної комісії: 15.06.2020р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., _ табл., __ додатка, __ джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система Корпорації "N", служба управління інформаційною безпекою Корпорації.

Предмет дослідження: впровадження елементів розробки політики безпеки інформаційного об’єкту.

Мета роботи (проекту): зробити аналіз та розробити політики безпеки інформації інформаційно-телекомунікаційної системи Корпорації "N", служби управління інформаційною безпекою Корпорації.

В першому розділі кваліфікаційної роботи було зроблено аналіз необхідності КСЗІ завдяки нормативно-правової бази у сфері захисту інформації та зроблено обстеження ОІД, де було розглянуто основні відомості про Корпорацію та інформацію, яка обробляється, знаходиться та циркулює там.

У спеціальній частині було розроблено моделі порушника та загроз безпеки інформації, проаналізувавши усі можливі ризики було сформовано профіль захищеності та положення політик безпеки інформації.

В третьому розділі було визначено економічну доцільність впровадження політик безпеки та ефективність впровадження її в систему Корпорації.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АНАЛІЗ РИЗИКІВ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, АКТ ОБСТЕЖЕННЯ, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ.

РЕФЕРАТ

Пояснительная записка: __ стр., __ рис., __ табл., __ приложений, __ источников.

Объект разработки: информационно-телекоммуникационная система Корпорации "N", служба управления информационной безопасностью Корпорации.

Предмет исследования: внедрение элементов разработки политики безопасности информационного объекта.

Цель работы (проекта): сделать анализ и разработать политики безопасности информации информационно-телекоммуникационной системы Корпорации "N", службы управления информационной безопасностью Корпорации.

В первом разделе квалификационной работы был сделан анализ необходимости КСЗИ благодаря нормативно-правовой базе в сфере защиты информации и сделано обследование ОИД, где были рассмотрены основные сведения о Корпорации и информацию, которая обрабатывается, находится и циркулирует там.

В специальной части был разработаны модели нарушителя и угроз безопасности информации, проанализировав все возможные риски были сформированы профиль защищенности и положения политик безопасности информации.

В третьем разделе были определены экономическую целесообразность внедрения политик безопасности и эффективность внедрения в систему Корпорации.

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, АНАЛИЗ РИСКОВ, МОДЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, АКТ ОБСЛЕДОВАНИЯ, ЭКОНОМИЧЕСКАЯ ЦЕЛЕСОБРАЗНОСТЬ.

ABSTRACT

Explanatory note: __ p., __ fig., __ tab., __ additions, __ sources.

Object of development: information and telecommunication system of the Corporation "N", information security management service of the Corporation.

Subject of research: implementation of elements for developing a security policy for an information object.

The purpose of the work (project): to analyze and develop information security policies for the information and telecommunication system of the Corporation "N", the information security management service of the Corporation.

In the first section of the qualification work, an analysis was made of the need for complex of information protection tools thanks to the regulatory framework in the field of information protection and a survey of object of information activity was made, which examined the basic information about the Corporation and the information that is processed, located and circulates there.

In a special part, models of the intruder and information security threats were been developed, having analyzed all possible risks, a security profile and provisions of information security policies were formed.

In the third section, the economic feasibility of implementing security policies and the effectiveness of implementation in the Corporation system were determined.

INTEGRATED INFORMATION PROTECTION SYSTEM, INFORMATION SECURITY POLICY, OBJECT OF INFORMATION ACTIVITIES, RISK ANALYSIS, THREAT MODULE, VIOLATOR MODEL, SURVEILLANCE ACT, ECONOMIC REASONABILITY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІТС – інформаційно-телекомунікаційна система;

КСЗІ – комплексна система захисту інформації;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система; ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ТЗІ – технічні засоби інформації;

ISO – Міжнародна організація зі стандартизації;

ІБ – Інформаційна безпека;

НД ТЗІ – Нормативний документ технічного захисту інформації;

ОС – Обчислювана система;

ПЗ – Програмне забезпечення;

ТЗІ – технічні засоби інформації;

ПК – персональний комп’ютер;

КЗЗ – комплекс засобів захисту.

ЗМІСТ

с.

ВСТУП ... 9

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ ... 11

1.1 Загальні відомості про Корпорацію «N» ... 11

1.2 Обґрунтування необхідності створення КСЗІ ... 12

1.3 Характеристика Корпорації та її організаційна структура ... 13

1.4 Обстеження ОІД ... 16

1.5 Основні та допоміжні технічні засоби ... 25

1.6 Обчислювальна система ОІД ... 28

1.7 Опис інформаційних потоків в ОІД ... 34

1.8 Висновки до першого розділу ... 43

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА ... 44

2.1 Модель порушника ... 44

2.2 Модель загроз ... 48

2.3 Профіль захищеності ... 59

2.4 Рекомендації для покращення системи безпеки ... 62

2.5 Висновки до спеціального розділу ... 77

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ ... 78

3.1 Мета техніко-економічного обґрунтування дипломної роботи ... 78

3.2 Визначення витрат на розробку політики безпеки інформації ... 78

3.2.1 Розрахунок фінансових (капітальних) витрат ... 79

3.2.2 Розрахунок поточних (експлуатаційних) витрат ... 82

3.3 Оцінка величини збиту ... 84

3.4 Загальний ефект від впровадження системи інформаційної безпеки ... 87

3.5 Оцінка економічної ефективності системи захисту інформації ... 88

3.6 Висновки до третього розділу ... 89

ВИСНОВКИ ... 90

ПЕРЕЛІК ПОСИЛАНЬ ... 91

ДОДАТОК А ... 93

ДОДАТОК Б 94
ДОДАТОК В 95
ДОДАТОК Г 96

ВСТУП

У сучасному світі велику роль грає інформація. Саме через стрімкий розвиток інформаційних технологій, жодна компанія не уявляє себе без використання інформаційних ресурсів.

Майже в кожній інформаційній системі знайдеться така інформація, розголошення якої стороннім особам може завдавати збитків її власнику або ж людині, якої стосується інформація. Тому використовується поняття кібербезпеки, яка позначає стан захищеності життєво важливих інтересів особистості, суспільства й держави в умовах використання комп'ютерних систем та / або телекомунікаційних мереж, за якого мінімізується можливість завдати їм шкоди й стосується не лише технічних питань і технологічного складника, а й людського чинника – ворожих інсайдерських дій чи людських помилок, а також проблем владних відносин на національному та міжнародному рівнях.

Особливо актуальним питанням інформаційної безпеки є інформація з обмеженим доступом на підприємствах, організаціях, в яких обробляється інформація. Бо саме такі данні є більш матимуть попит у третіх осіб, бо будь яка організація хвилюється за свій прибуток й використовує усі можливі варіанти зробити його більшим.

Для уникання проблем з безпекою розробляється спеціальні планові заходи, які включають в себе опис об'єкту інформаційної діяльності, моделей порушника та загроз на основі котрих створюються нові нормативні документи та інструкції. Усі ці документи містять в собі розробки політики безпеки підприємства та розробки комплексну систему захисту інформації. Усе це допомагає уникнути проблем з розголошенням інформації та забезпечує високий рівень безпеки інформації. Чим точніше буде усе це реалізовано, тим простішим й швидшим шляхом (методом програмного, апаратного та комплексного підходу) адміністратор безпеки та системний адміністратор зможе це реалізувати.

На період виконання у роботи були сформовані та поставлені наступні задачі:

- розглянути загальні відомості про підприємство;
- виконати обстеження об’єкту інформаційної діяльності;
- зробити класифікацію інформації, аналіз інформаційних потоків;
- розробити моделі порушника та загроз;
- розробити політику безпеки;
- оцінити рівень захищеності інформації комп’ютерних систем від несанкціонованого доступу;
- обґрунтування необхідності затрат на комплекс системи захисту інформації;
- розрахувати затрати на впровадження нових засобів захисту інформації.

Таким чином, більш детально розглянуто основні етапи, які допоможуть уникнути загроз втрати інформації для типової організації роздрібної торгівлі.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1.Загальні відомості про Корпорацію «N»

Корпорація «N» - це об'єднання великих українських компаній, які здійснюють свою діяльність в таких сферах бізнесу як управління активами, роздрібна торгівля, виробництво і продаж продуктів харчування. Головним напрямком діяльності корпорації є розвиток і управління найбільшою мережею в Україні продуктових дисконтерів «N».

Корпорація «N» є лідером галузі України зі сплати податків і зборів на бюджети різних рівнів і спец фондів.

У Дніпрі знаходиться офіс, якій розташований за наступним адресом вул. Січових Стрільців 21а.

Для того що б уникнути вище зазначених витоків інформації, як правило створюється служба, яка може забезпечити захист інформації, яка повинна залишитися всередині компанії. Так як втрата конфіденційної інформації для компанії може принести великі фінансові втрати або зниження конкурентоспроможності. Аналіз саме цього відділу проводиться під час виконання кваліфікаційної роботи.

На 2019 рік. асортимент в магазинах становить понад 3500 найменувань товарів і продовольчої групи, з яких понад 800 - представляють власні торгові марки «N». За рахунок мінімізації витрат на логістику і рекламу, вартість такої продукції нижче середньо-ринкової.

В даний час магазини «N» працюють в 256 населених пунктах, це 22 задіяні області України.

1.2. Обґрунтування необхідності створення КСЗІ

Для досягнення цілей інформаційної безпеки Корпорація розробляє і впроваджує систему внутрішньої нормативної документації. Управління інформаційної безпеки Корпорації є відповідальними за розробку і періодичний перегляд документів в сфері інформаційної безпеки.

Згідно ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах», умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством. Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Згідно ЗУ «Про інформацію» за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Згідно НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці» об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов'язковому категоріюванню.

ДСТУ ISO / IEC 27000 до: 2016 Information technologyI - Security techniques - Information Security Management System - Overview and Vocabulary (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд і словник). ISO 27000 - міжнародні стандарти управління інформаційною безпекою. Включає в себе: міжнародні стандарти, визначення

до вимог системи управління інформаційною безпекою, управління ризиками, метриками і вимірами, а також керівництво по впровадженню.

ДСТУ ISO / IEC 27001 до: 2016 Information technology - Security techniques - Information security management systems - Requirements (Інформаційні технології. Методи захисту. Вимоги). Сертифікат ISO 27001 - це документ підтверджує відповідність системи вимог стандарту. Отримавши такий сертифікат означає, що ваша компанія надійно захищає дані від спроби несанкціонованого доступу.

Згідно НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційнотелекомунікаційній системі» встановлений цим НД ТЗІ порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством.

Виходячи з того в ІТС обробляється інформація, що є комерційною таємницею та інформація, захист якої передбачається інформаційною політикою підприємства (за рішенням власника інформації) та/або законодавством України, має бути створена КСЗІ.

1.3.Характеристика Корпорації «N» та її організаційна стуктура

Організаційна структура - документ, схематично відображає склад та ієрархію підрозділів підприємства. [9]

Організаційна структура встановлюється виходячи з цілей діяльності і необхідних для досягнення цих цілей підрозділів, що виконують функцію, що становлять бізнес-процеси організації.

Організаційна структура Корпорації «N» полягає в наявності безлічі відділів, основні з них представлені нижче(рис.1.1).

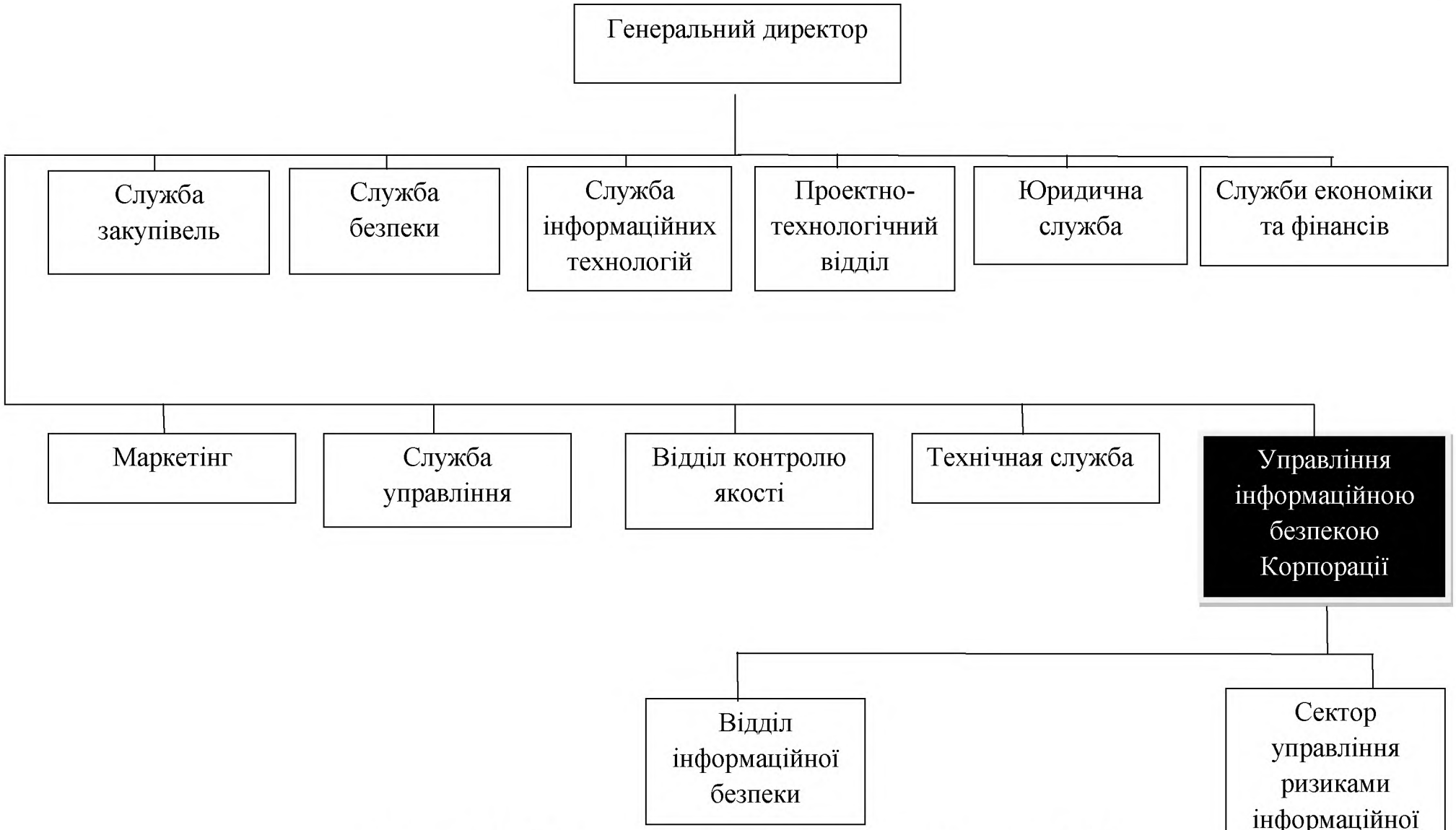

Рисунок 1.1 - Фрагмент організаційної структури Корпорації «N»

Нижче розглянемо Корпорацію «N»більш детальною, а саме Управління інформаційної безпеки Корпорації (далі УІБК).

УІБК ділиться на відділ інформаційної безпеки та сектор управління ризиками інформаційної безпеки. Далі розглянемо більш детально кожен з них.

Відділ інформаційної безпеки займається вирішенням проблем та інформаційної безпеки всієї організації. Відділ інформаційної безпеки підпорядковується начальнику УІБК. Відділ інформаційної безпеки - організаційно-технічна структура системи забезпечення інформаційної безпеки, що реалізує вирішення певних завдань, спрямованих на протидію тій чи іншій загрозі інформаційної безпеки.

Функції відділу інформаційної безпеки[10]:

– організація і координація робіт, пов'язаних із захистом на підприємстві;

– дослідження технології обробки інформації з метою виявлення можливих каналів витоку і інших загроз безпеці інформації, формування моделі загроз, розробка політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;

– розробка проектів нормативних та розпорядчих документів, що діють в межах організації, підприємства, відповідно до якого повинна забезпечуватися захист інформації на підприємстві;

– виявлення та знешкодження загроз;

– реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;

– формування у персоналу і користувачів підприємства розуміння необхідності виконання вимог нормативно-правових актів, нормативних та розпорядчих документів, що стосуються сфери захисту інформації.

Далі розглянемо сектор управління ризиками інформаційної безпеки, який займається зменшенням імовірності втрат організації в результаті інцидентів.

Існує практики у сфері управління ризиками, доцільно виділити чотири найбільш важливі моменти в управлінні ризиками на підприємстві:

1. Недовговічність інформаційного активу. Підприємство і більшість промислових галузей розуміють, що ефективність їх роботи залежить від інформації. Кожен відомий критичний випадок критичного спотворення, пошкоджує або руйнує інформації підсилює їх побоювання з цього пункту.

2. Доказова безпеку. Так як параметри безпеки не завжди мають оцінку, підприємства не здатні виміряти стабільність або ефективність при виборі різних засобів безпеки. Отже, кількість коштів, витрачених на поліпшення безпеки невідомо.

3. Обгрунтування вартості. Підвищення вартості рішень і засобів безпеки призводить до того, що проекти інформаційної безпеки конкурують з іншими інфраструктурними проектами підприємства. Прибутково-вартісний аналіз і розрахунок коштів, що повертаються в інвестиції, стає стандартною вимогою для будь-яких проектів з інформаційної безпеки.

4. Відповідальність. З ростом підприємств їх залежність від ризиків інформаційної безпеки зростає. Необхідний надійний механізм для управління цими ризиками. Для оцінки інформаційної безпеки прибутково-вартісного аналізу і розрахунків коштів, що повертаються в інвестицію недостатньо. Тому потрібно зробити оцінку даних.

1.4. Обстеження ОІД

Далі приведений ситуаційний план(рис.1.2).

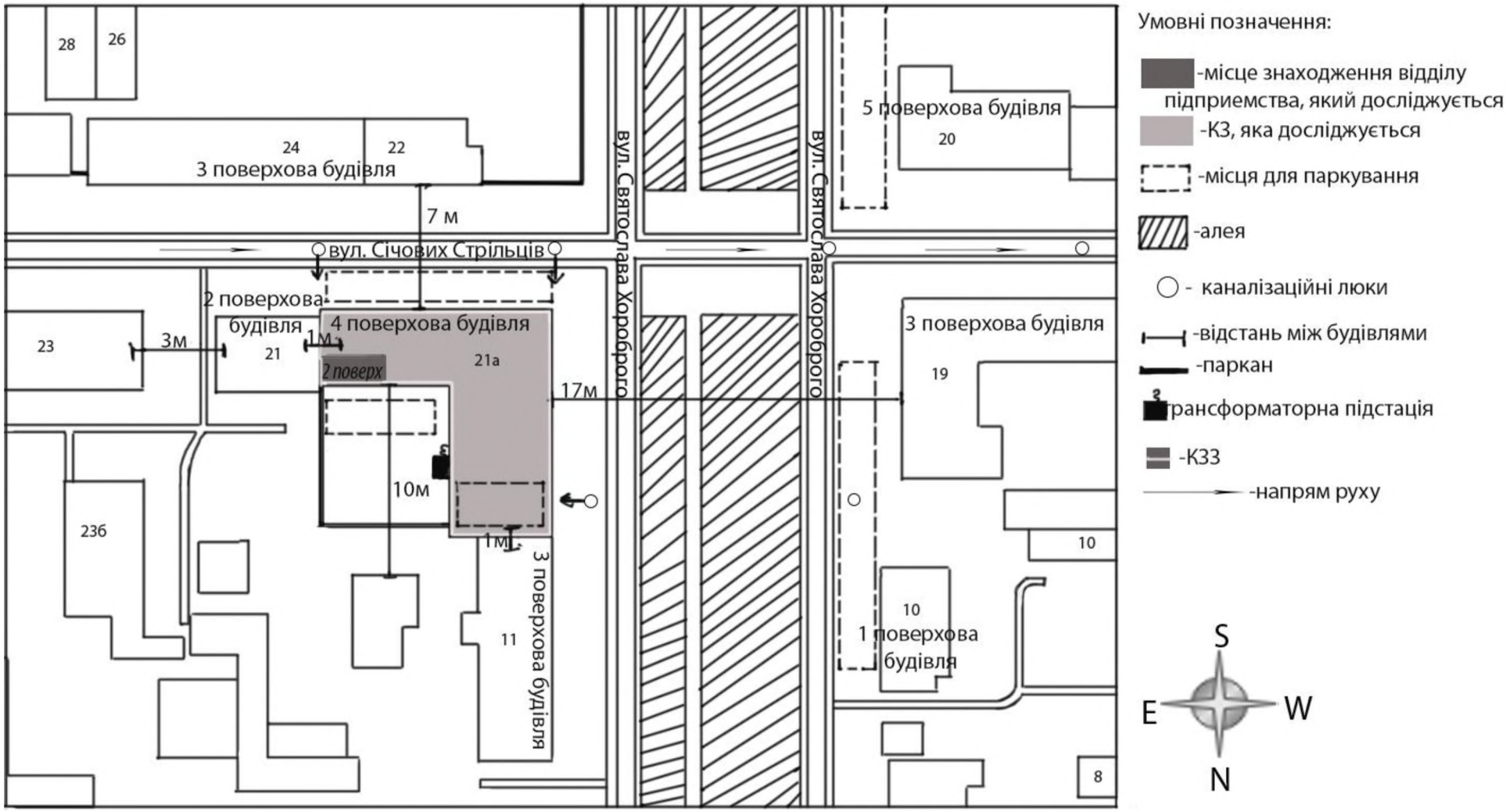

Рисунок 1.2 - Ситуаційний план

– КЗ, в якому знаходиться ОІД має 4 поверхи та нульовий поверх; збудовано з цегли та бетонних конструкцій;

– нульовий поверх не є власністю компанії та здається під оренду аптеці та банку; перший поверх це магазин, який належить ОІД, в який може зайти будь-хто з 8.00-22.00; в магазині наявна охорона; з другого до четвертій поверх можливий підйом по сходам, які не мають охорону, лише відеоспореження; на 2,3 та 4 поверхах знаходиться пункти с КПП охороною; на поверхи з 2 по 4 щоб зайти на територію офісу треба пред'явити пропуск працівників; у вихідні дні або святкові об’єкт обмежений та працює тільки при подачі заявки;

– ОІД, що обстежується знаходиться між 2 та 3 поверхах, стіни зроблені із цегли, товщина стін 24 см; підлога та стеля є бетонні конструкції близько 10-12 см; КЗ має один вхід/вихід на якому встановлені захисні металеві двері товщиною 75мм,які знаходяться з південної сторони, також біля дверей знаходиться система контролю обліку даних; в КЗ знаходиться також 7 міжкімнатних дверей товщиною 60мм; в приміщенні знаходиться 6 віконних отворів з північної та східної сторони товщиною 70мм, складаються з металопластику;

– в КЗ є лінії систем електропостачання та інтернету(рис.2), водопостачання(рис.3), вентиляції(рис.3), пожежна по охоронна сигналізація (рис.4); розетки мають паралельне з’єднання та підключення до електричної щитової в офісі, що підключена к щитовій на поверсі й далі к трансформаторній будці;

– за межі КЗ, в якій знаходиться ОІД , що обмежується виходить лінії системи водопостачання, електроживлення, інтернету;

– навколо КЗ, де знаходиться ОІД, розміщені такі об’єкти , далі приведена таблиця(табл.1.1);

Таблиця 1.1 - Опис ситуаційного плану

№	Найменування	Кількість поверхів	Адреса	Відстань від ОІД
1	Малоповерховий житловий будинок	2	Вул. Січових Стрільців, 21	1м

Продовження таблиці 1.1

№	Найменування	Кількість поверхів	Адреса	Відстань від ОІД
2	Малоповерховий житловий будинок	3	Вул. Січових Стрільців, 23	10м
3	Малоповерхнева зруйнована будівля	3	Вул. Січових Стрільців, 22	7м
4	Малоповерхнева зруйнована будівля	3	Вул. Січових Стрільців, 24	10м
5	Бізнес центр	5	Вул. Січових Стрільців, 20	25м
6	Житловий будинок	3	Вул. Січових Стрільців, 19	17м
7	Малоповерховий житловий будинок	3	Вул. Святослава Хороброго, 11	1м
8	Одноповерховий магазин	1	Вул. Святослава Хороброго, 10	22м

– з західної сторони знаходиться сусіднє приміщення, яке має цеглині стіни товщиною 24 см, підлога та стеля є бетонні конструкції близько 25 см;

– в КЗ, в якій знаходиться ОІД, використовуються серверна, офісна АТС, які розміщені не в межі даного відділу та стаціонарні комп'ютери, маршрутизатор, комутатор, принтера в межі ОІД (структурна схема рис.5, повний список ресурсів приведений в табл.1.2). Використані в системі охорони пожежній ті охоронній сигналізації, список приведений в табл.1.3 інвентаризаційна відомість ВТСС. Повна характеристика складу ІТС приведена в табл.1.4. На ОІД використовуються системні, прикладні та спеціальні програмні забезпечення, детальний опис в таблиці № 5 інвентаризаційна відомість програмного забезпечення ІТС;

– навколо КЗ знаходяться дві вулиці: вул. Січових Стрільців та вул. Святослава хороброго. На вул. Січових Стрільців односторонній рух машин в дві полоси, шириною в 4 метри, який за напрямком йде на захід, вул. Святослава Хороброго має двосторонній рух автомобілів, кожна дорога є по 2 метри.

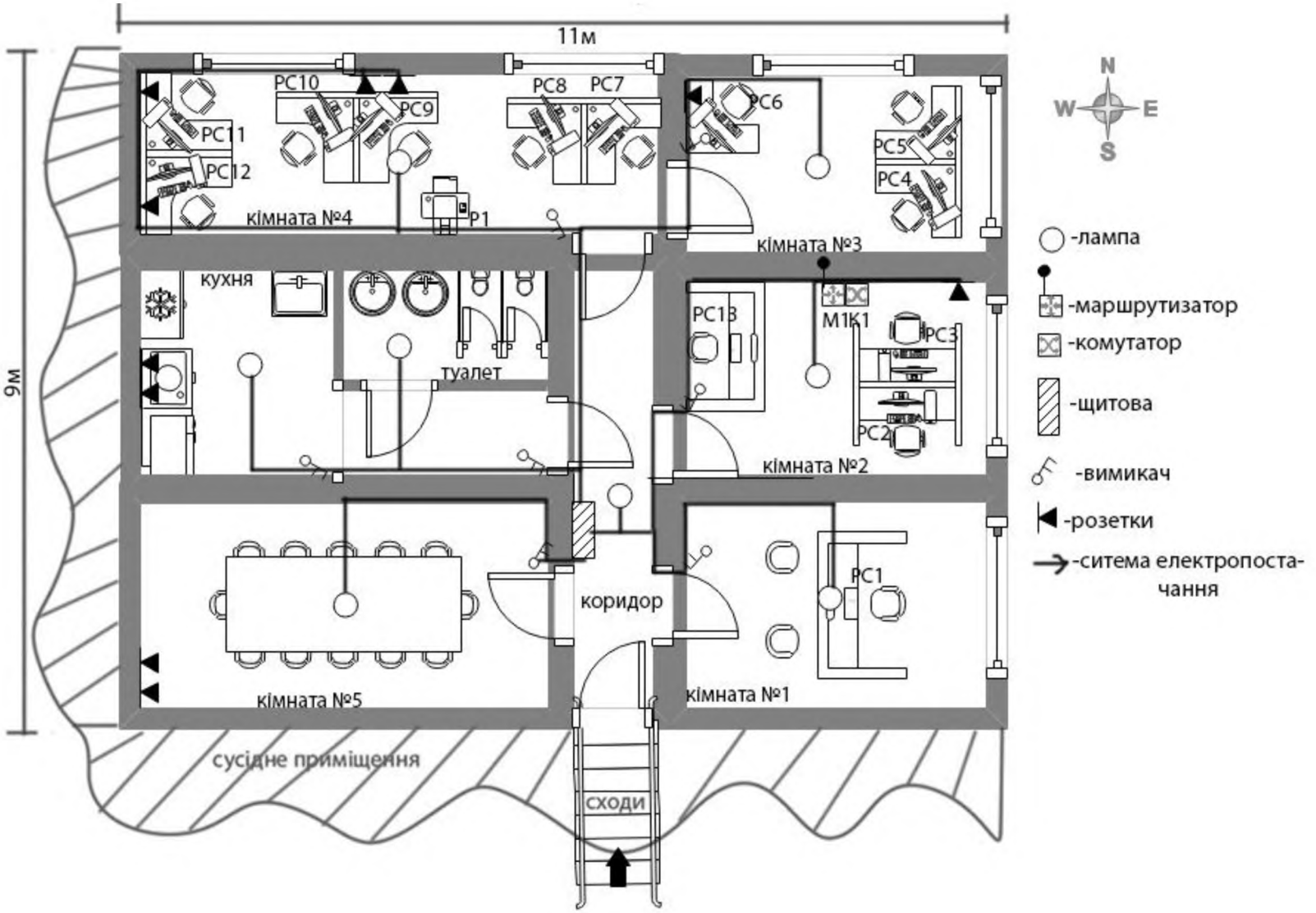

Рисунок 1.3 - Генеральний пан комп’ютерної системи, електрики

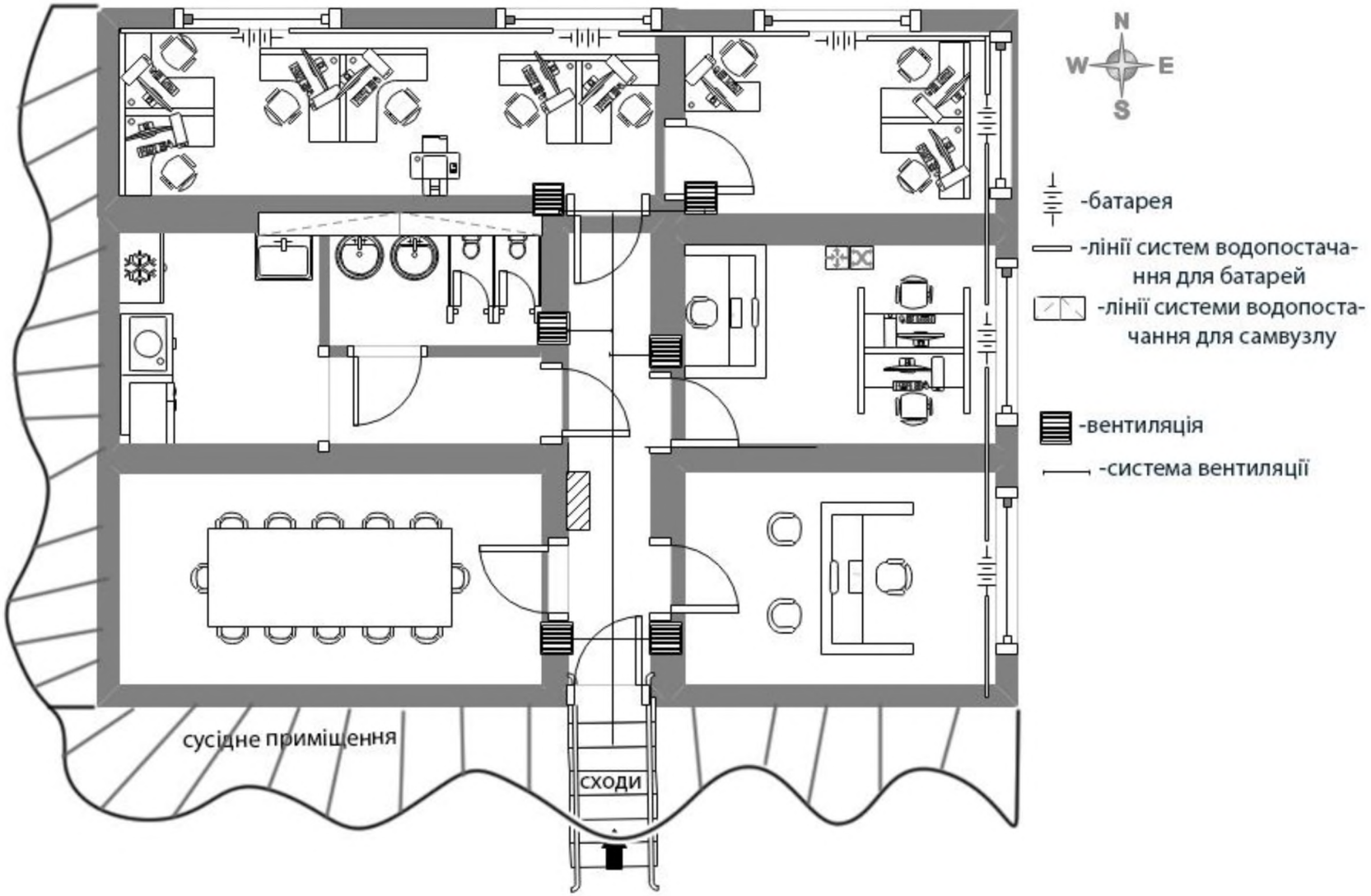

Рисунок 1.4 - Генеральний план системи ліній водопостачання, лінії системи вентиляції

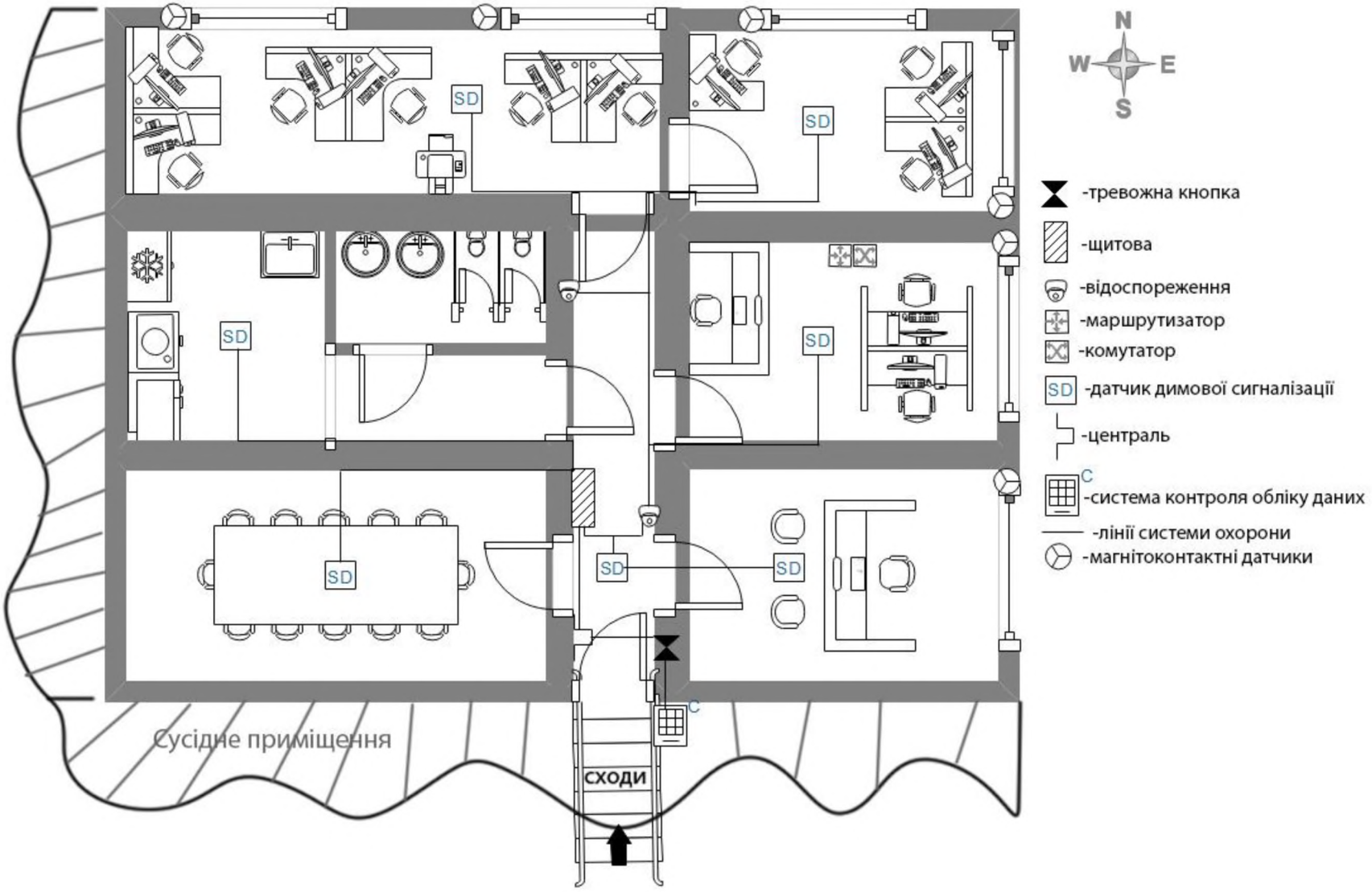

Рисунок 1.5 - Генеральний план системи охорони

1.5.Основні та допоміжні технічні засоби

На генеральному плані (рис.1.3) зображено основні техні засоби, які більш детально описані у таблиці нижче(табл.1.2), де також описано розміщення та відстані до межі контрольованої зони.

Таблиця 1.2 - Інвентаризаційна відомість апаратного забезпечення ІТС

№	Назва (в ІТС)	Характеристика		Розміщення	Відстань до межі ОІД
		Найменування	Модель		
1	PC1 Робоча станція	монітор	Samsung S27F358F	Кімната №1, системний блок під столом, інше на столі	2,2м
		системний блок	Acer X2630G		1,9м
		клавіатура	GEMBIRD KB-U-101-UA		2м
		миша	Logitech B100 USB		2м
2	PC2 Робоча станція	монітор	Samsung S27F358F	Кімната №2 системний блок під столом, інше на столі	1м
		системний блок	Acer X2630G		0,8м
		клавіатура	GEMBIRD KB-U-101-UA		1м
		миша	Logitech B100 USB		0,9м
3	PC3 Робоча станція	монітор	Samsung S27F358F	Кімната №2 системний блок під столом, інше на столі	1м
		системний блок	Acer X2630G		0,8м
		клавіатура	GEMBIRD KB-U-101-UA		1м
		миша	Logitech B100 USB		1,2м
4	PC4 Робоча станція	монітор	Samsung S27F358F	Кімната №3 системний блок під столом, інше на столі	0,3м(П)/ 1,6м
		системний блок	Acer X2630G		0,3м(П)/ 2,5м
		клавіатура	GEMBIRD KB-U-101-UA		0,5м(П)/ 2м
		миша	Logitech B100 USB		0,5м/2,2м

Продовження таблиці 1.2

№	Назва (в ІТС)	Характеристика		Розміщення	Відстань до межі ОІД
		Найменування	Модель		
5	РС5 Робоча станція	монітор	Samsung S27F358F	Кімната №3 системний блок під столом, інше на столі	0,3м(П)/ 1,4м
		системний блок	Acer X2630G		0,3м(П)/ 0,5м
		клавіатура	GEMBIRD KB-U-101-UA		0,5м(П)/1,3м
		миша	Logitech B100 USB		0,5м(П)/1,3м
6	РС6 Робоча станція	монітор	Samsung S27F358F	Кімната №3 системний блок під столом, інше на столі	3,5м(П)/ 1,2м
		системний блок	Acer X2630G		3,8м(П)/ 0,3м
		клавіатура	GEMBIRD KB-U-101-UA		3,4м(П)/ 1м
		миша	Logitech B100 USB		3,8м(П)/ 0,8м
7	РС7 Робоча станція	монітор	Samsung S27F358F	Кімната №4 системний блок під столом, інше на столі	0,7м
		системний блок	Acer X2630G		0,5м
		клавіатура	GEMBIRD KB-U-101-UA		0,9м
		миша	Logitech B100 USB		0,5м
8	РС8 Робоча станція	монітор	Samsung S27F358F	Кімната №4 системний блок під столом, інше на столі	0,7м
		системний блок	Acer X2630G		0,5м
		клавіатура	GEMBIRD KB-U-101-UA		0,9м
		миша	Logitech B100 USB		1м
9	РС9 Робоча станція	монітор	Samsung S27F358F	Кімната №4 системний блок під столом, інше на столі	0,7м
		системний блок	Acer X2630G		0,5м
		клавіатура	GEMBIRD KB-U-101-UA		0,9м
		миша	Logitech B100 USB		0,5м
10	РС10 Робоча станція	монітор	Samsung S27F358F	Кімната №4 системний блок під столом, інше на столі	0,7м
		системний блок	Acer X2630G		0,5м
		клавіатура	GEMBIRD KB-U-101-UA		0,9м
		миша	Logitech B100 USB		1м

Продовження таблиці 1.2

№	Назва (в ІТС)	Характеристика		Розміщення	Відстань до межі ОІД
		Найменування	Модель		
11	РС11 Робоча станція	монітор	Samsung S27F358F	Кімната №4 системний блок під столом, інше на столі	1,4м
		системний блок	Acer X2630G		0,4м
		клавіатура	GEMBIRD KB-U-101-UA		1,2м
		миша	Logitech B100 USB		1м
12	РС12 Робоча станція	монітор	Samsung S27F358F	Кімната №4 системний блок під столом, інше на столі	1,6м
		системний блок	Acer X2630G		1,7м
		клавіатура	GEMBIRD KB-U-101-UA		2м
		миша	Logitech B100 USB		1,9м
13	РС13 Робоча станція	монітор	Samsung S27F358F	Кімната №2 системний блок під столом, інше на столі	3,4м
		системний блок	Acer X2630G		3,5м
		клавіатура	GEMBIRD KB-U-101-UA		3,5м
		миша	Logitech B100 USB		3,5м
14	К1 Комутатор	-	Tenda S16 16xFE Desktop	Кімната №2	2м
15	М1 Маршрутизатор	-	TP-Link WR841n	Кімната №2	2,2м
16	Р1 Принтер	-	HP LaserJet 1022	Кімната №4	2,5м

На генеральному плані системи охорони(рис.1.5) зображені допоміжні технічні засоби, опис ких буде приведений більш детально в таблиці(табл.1.3) нижче, а також розміщення їх в ОІД.

Таблиця 1.3 - Фізичний опис обладнання ВТСС

№	Назва	Марка	Модель	Інвентарний номер	Розміщення
1	Камера відеоспостереження	Hikvision	DS-2CD1321-I 2.8	43570	Коридор

Продовження таблиці 1.3

№	Назва	Марка	Модель	Інвентарний номер	Розміщення
2	Камера відеоспостереження	Hikvision	DS-2CD1321-I 2.8	15757	Коридор
3	Датчик димової сигналізації	Артон	СПД-3.5	67437	Кімната №1
4	Датчик димової сигналізації	Артон	СПД-3.5	23456	Кімната №2
5	Датчик димової сигналізації	Артон	СПД-3.5	65754	Кімната №3
6	Датчик димової сигналізації	Артон	СПД-3.5	12343	Кімната №4
7	Датчик димової сигналізації	Артон	СПД-3.5	87540	Кімната №5
8	Датчик димової сигналізації	Артон	СПД-3.5	2348	Кухня
9	Датчик димової сигналізації	Артон	СПД-3.5	54904	Коридор
10	Система контролю обліку даних	SOKOL ZS	АК-14	27846	Коридор
11	Магнітоконтактні датчики	TANE	met-200ARM	87892	Кімната №4
12	Магнітоконтактні датчики	TANE	met-200ARM	98031	Кімната №4
13	Магнітоконтактні датчики	TANE	met-200ARM	39052	Кімната №3
14	Магнітоконтактні датчики	TANE	met-200ARM	16783	Кімната №3
15	Магнітоконтактні датчики	TANE	met-200ARM	90451	Кімната №2
16	Магнітоконтактні датчики	TANE	met-200ARM	78312	Кімната №1
17	Централь	Орион	8Т.3.2	67342	Коридор

1.6.Обчислювальна система ОІД

В даній схемі(рис.1.6) розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки.

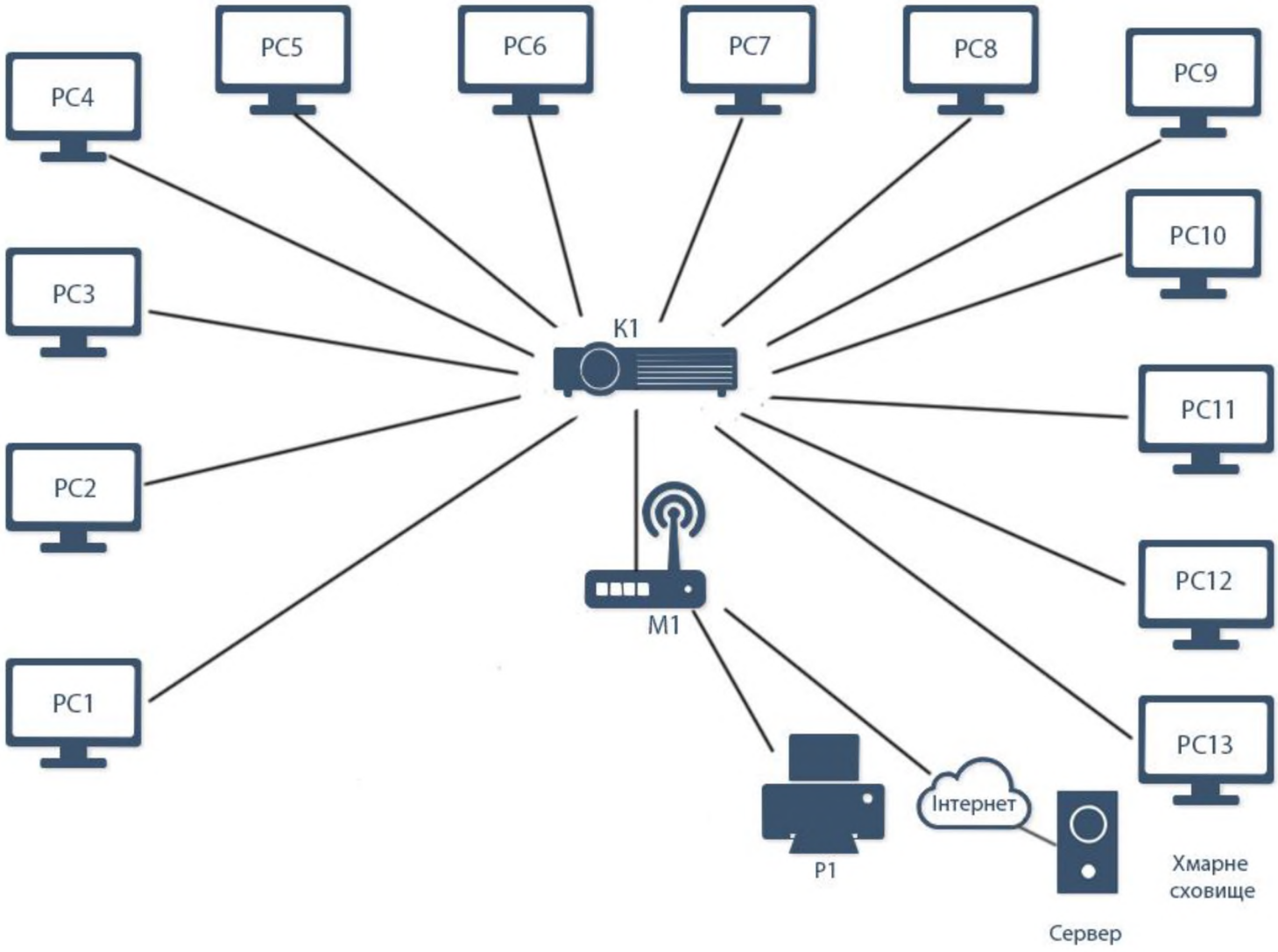

Рисунок1.6 - Структурна схема ІТС

На ній розміщено тринадцять дистанційних комп'ютерів, які об'єднує робоча група. В даній службі можна розглянути 2 відділи, к одному відносяться PC з 3 по 6 та другий, якому відносяться PC 2, з 8 по 12. Також присутні два PC які не належать конкретно відділам, а є робочими місцями для людей, які підкоряються начальнику служби, також PC для начальника служби.

Усі комп'ютери мають доступ до інтернету та можуть віддалено підключатися до серверу або хмарного сховища, також усі робітники мають право використовувати принтер, к якому можна підключитися також віддалено.

В даній Корпорації сервер використовується як середовище для зберігання усіх даних.

Доступ к маршрутизатору мають лише ті люди на яких був оформлено документ, який дозволяє працювати через інтернет та ознайомлює з усіма нормами та правилами роботи. Підключення до інтернету проходить через введення паролю з шифруванням, ключ до якого містить десять символів та має функцію відключення при неправильному введенню пароля більш ніж три рази.

Таблиця 1.4 - Характеристика складу ITC

№	Назва	Назва в ITC	Характеристика	Інвентарний номер	Відповідальний
1	Робоча станція	PC1	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	45672 78564 23789 16875	Системний адміністратор
2	Робоча станція	PC2	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	12709 26745 87219 26579	Системний адміністратор

Продовження таблиці 1.4

№	Назва	Назва в ІТС	Характеристика	Інвентарний номер	Відповідальний
3	Робоча станція	PC3	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	24764 12856 39032 18678	Системний адміністратор
4	Робоча станція	PC4	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	16784 17345 90043 12895	Системний адміністратор
5	Робоча станція	PC5	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	12804 25698 56009 45632	Системний адміністратор
6	Робоча станція	PC6	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	63722 73110 84326 77649	Системний адміністратор
7	Робоча станція	PC7	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	28573 92877 34091 49002	Системний адміністратор

Продовження таблиці 1.4

№	Назва	Назва в ІТС	Характеристика	Інвентарний номер	Відповідальний
8	Робоча станція	PC8	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	37528 68275 93703 15738 97332	Системний адміністратор
9	Робоча станція	PC9	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	73327 95421 13544 46043 73211	Системний адміністратор
10	Робоча станція	PC10	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	63370 86054 71894 62803	Системний адміністратор
11	Робоча станція	PC11	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	77858 96042 21532 92671	Системний адміністратор
12	Робоча станція	PC12	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	69032 45098 11289 38893	Системний адміністратор

Продовження таблиці 1.4

№	Назва	Назва в ІТС	Характеристика	Інвентарний номер	Відповідальний
13	Робоча станція	PC13	INTEL Pentium G4500 (CM8066201927319)/ MSI H110M PRO-VH PLUS/ DDR4 8GB (2x4GB) 2666 MHz eXceleram (E40826666AD) / SSD 2.5' 250GB Samsung (MZ-76E250BW)	26784 37789 22845 19007	Системний адміністратор
14	Комутатор	K1	TP-Link WR841n	34675	Системний адміністратор
15	Маршрутизатор	M1	TP-Link TL-SF1008D	66545	Системний адміністратор
16	Принтер	P1	HP LaserJet 1022	79065	Системний адміністратор

Далі приведена таблиця(табл.1.5) зі всім необхідним програмним забезпечення для роботи персоналу Корпорації. На декількох комп'ютерів знаходиться одразу дві операційні системи, одна з которих потрібна для роботи з створенням звітів, а інша з роботою на серверах.

Таблиця 1.5 - Інвентаризаційна відомість програмного забезпечення ІТС

№	Назва	Тип	Опис	Ліцензія	Встановлена
1	Windows 10 (версія 1909)	Системне	Операційна система для персональних комп'ютерів і робочих станцій	Commercial	PC1-13
2	Linux (Mint 19.3 Tricia)	Системне	Сімейство Unix-подібних операційних систем на базі ядра Linux	Freeware	PC3-6
3	WinRar (версія 5.80)	Системне	Архіватор файлів для 32- і 64-розрядних операційних систем Windows	Shareware	PC1-13

Продовження таблиці 1.5

№	Назва	Тип	Опис	Ліцензія	Встановлена
4	Microsoft Word (версія 2018)	Прикладне	Програми для створення, редагування та оформлення текстових документів	Commercial	PC1-13
5	Microsoft PowerPoint (версія 2018)	Прикладне	Програми створення та показу наборів слайдів	Commercial	PC1-13
6	Microsoft Excel (версія 2018)	Прикладне	Програми, що дозволяють виконувати операції над даними, представленими в табличній формі	Commercial	PC1-13
7	Microsoft Access (версія 2018)	Прикладне	Засоби введення, пошуку, розміщення і видачі великих масивів даних	Commercial	PC1-13
8	Google Chrome (версія 80.0.3987)	Прикладне	Програми для роботи в комп'ютерній мережі	Freeware	PC1-13
9	Visual Studio (версія 16.0)	Спеціальне	Об'єктно-орієнтовані мови програмування	Commercial	PC3-6

1.7. Опис інформаційних потоків в ОІД

В Корпорації «N» присутні: відкрита інформація та з обмеженим доступом(максимальний рівень – конфіденційна). Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Тому, в корпорації циркулює така інформація: інформація про клієнтів, продукт роботи компанії, бухгалтерські звіти діяльності компанії, інформація про

співробітників, науково-технічна, контактна інформація, юридична інформація, інформація про захист підприємства, інформація о веб-сайті(повний звіт табл.1.6).

Основну обробку інформації обробляється робочим персоналом корпорації, а саме: начальника служби безпеки корпорації, начальника відділу інформаційної безпеки, начальника сектору управління рисками інформаційної безпеки, спеціаліст з економічної безпеки, п’ятьма робітниками відділу інформаційної безпеки, трьома робітниками сектору управління рисками інформаційної безпеки та системним адміністратором(табл.1.7).

Далі розглянемо основні потоки інформації, а саме інформацію про клієнтів, про продукт компанії та інформацію на веб-сайті.

В інформацію про клієнтів включає дані, які не мають бути розголошені за територією організації, вони знаходяться на сервері, де до них можна потрапити онлайн.

Продукти компанії розглядаються як розробка різних схем продажу різних товарів и виготовленню продукції компанії. Так як ці данні можуть призвести до великих втрат зі сторони компанії її зберігають у декількох копіях на сервері.

Інформація на сайті та сам сайт знаходиться на сервері, де знаходяться его основні компоненти. Якщо сайт буду ушкодженим, то Корпорація може загубити інвесторів та зазнати втрати, тому його безпека є дуже важливою.

Для отримання даних співробітником створюється електронний запит в системі електронного документообігу, в якому вказується прізвище, ім'я, по батькові та посада співробітників, яким повинен бути наданий доступ. Після отримання доступу, компанія повинна проінформувати співробітників по питанням інформаційної безпеки.

Права доступу видаються з умовою:

– права доступу до об'єктів повинні запитуватися співробітниками і видаватися в мінімальному обсязі, необхідному для виконання службових обов'язків;

– до процесу управління правами доступу в ІС застосовується правило «чотирьох очей» (залучення декількох співробітників) для розмежування повноважень при управлінні правами доступу: узгодження надання прав доступу та видача прав доступу до об'єктів виконуються різними співробітниками Компанії;

– забороняється використання службових облікових записів, а також вбудованих облікових записів в об'єкти адміністраторами при виконанні своїх функцій. Для виконання повсякденних функцій, не пов'язаних з адмініструванням (перегляд електронної пошти, використання Інтернет і т.д.), адміністратори повинні використовувати окремі персоніфіковані облікові записи, що не володіють привілейованими правами доступу;

– забороняється використовувати чужі облікові записи і паролі для доступу до об'єктів Компанії. У разі підозри, що обліковим записом користується не тільки її власник, співробітник, якому став відомий подібний факт, повинен негайно повідомити про нього в УІБК і, по можливості, попередити власника облікового запису. Використання чужих облікових записів і паролів для доступу до об'єктів Компанії ідентифікується як факт несанкціонованого доступу до об'єктів Компанії, що тягне за собою дисциплінарні, адміністративні (аж до звільнення) і / або кримінальні стягнення;

– забороняється використання співробітниками для виконання службових обов'язків облікових записів і паролів звільнених співробітників;

– для запобігання підбору паролів повинен використовуватися механізм блокування облікового запису після п'яти неправильних спроб входу;

– розблокування облікового запису користувача здійснюється співробітниками ОІ на підставі електронної заявки в системі електронного

документообігу або після підтвердження особи співробітника під час телефонного дзвінка (наприклад, з запрашіваніе номера карти доступу співробітника в приміщення Компанії).

При отриманні прав доступу зовнішнім організаціям формується така ж заявка що вказана вище. При її узгодженні співробітники організації інформують зовнішню організацію про збереження інформаційної безпеки і повідомляють про вимогах до даної процедури. Так само складається договір між організаціями і підписує акт про конфіденційності інформації.

Після отримання доступу, співробітники компанії повинні бути проінформовані про експорт документів через кур'єрську службу, з якою укладено договір про нерозголошення і конфіденційності інформації.

Таблиця 1.6.Інформація, яка циркулює на ОІД

№	Вид інформації	Режим доступу	Правовий режим	Вид представлення в ІТС	Вимоги до захисту		
					К	Ц	Д
1	Інформація про клієнтів	Обмежений доступ	Конфіденційна	Електронна, печатна, акустична	К2	Ц3	Д2
2	Закупівельна інформація про продукцію компанії	Обмежений доступ	Конфіденційна	Електронна, печатна, графічна, звукова	К3	Ц2	Д3
3	Інформація про бухгалтерські звіти діяльності компанії	Обмежений доступ	Конфіденційна	Електронна, печатна, графічна	К4	Ц3	Д3
4	Інформація про співробітників	Обмежений доступ	Конфіденційна	Електронна, печатна, акустична	К2	Ц3	Д2
5	Науково-технічна	Обмежений доступ	Конфіденційна	Електронна, печатна	К3	Ц2	Д3

Продовження таблиці 1.6

№	Вид інформації	Режим доступу	Правовий режим	Вид представлення в ІТС	Вимоги до захисту		
					К	Ц	Д
6	Контактна інформація	Відкрита	---	Електронна, акустична	---	Ц3	Д1
7	Юридична інформація	Обмежений доступ	Конфіденційна	Електронна, печатна	К3	Ц3	Д4
8	Інформація про захист підприємства	Обмежений доступ	Конфіденційна	Електронна, акустична	К3	Ц3	Д2
9	Інформація на веб-сайті	Відкрита	---	Електронна	---	Ц3	Д1

Для класифікації інформації використовуються такі вимоги захисту, що описані нижче.

Рівні конфіденційності:

К1 – рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;

К2 – рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;

К3 – рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;

К4 – рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску;

К5 – критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності:

Ц1 – рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;

Ц2 – рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;

Ц3 – рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

Ц4 – рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;

Ц5 – критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

Д1 – рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;

Д2 – рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;

Д3 – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

Д4 – рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;

Д5 – критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Таблиця1.7.Користувацьке середовище

Працівники	Інф. про кваліфікацію	Інформація									Повно-важення керувати КСЗІ	Ресурси
		1	2	3	4	5	6	7.	8	9		
Начальник служби безпеки корпорації(1)	Високо-кваліфіковані робітники	Ч	Ч,З,М	Ч,З,К, В,М,ЗБ	Ч,З,М, В,Д	Ч,З,К, В,М,ЗБ	Ч,З, К,ЗБ	Ч	Ч,З,К, М,В,З Б,Д	Ч	+	РС1-13, Р1
Начальник відділу інформаційної безпеки(1)	Високо-кваліфіковані робітники	Ч	Ч	Ч,З,К, В,М,ЗБ	Ч,М,З	Ч	Ч,З, М	Ч	Ч,З,К, М,В,З Б,Д	Ч	+	РС3-6, Р1
Начальник сектору управління ризками інформаційної безпеки(1)	Високо-кваліфіковані робітники	Ч, З,М,Д	Ч	Ч,З,К, В,М,ЗБ	Ч,М,З	Ч	Ч,З, М	Ч	Ч,З,К, М,В,З Б,Д	Ч	+	РС2, 8-12, Р1
Спеціаліст економічної безпеки(1)	Високо-кваліфіковані робітники	Ч, З,М,Д	Ч,З,М	Ч,З,К, В,М,ЗБ	Ч,М,З	Ч,М,З	Ч,З, М	Ч, М, З	Ч,З,К, М,В,З Б,Д	Ч	---	РС13
Робітники відділу інформаційної безпеки(5)	Кваліфіковані робітники	Ч	Ч	Ч,З,М, ЗБ	Ч	Ч,М,З	Ч	Ч	Ч,З,К, М,В,З Б,Д	Ч	---	РС4-6, Р1

Продовження таблиці 1.7

Працівники	Інф. про кваліфікацію	Інформація									Повно-важення керувати КСЗІ	Ресурси
		1	2	3	4	5	6	7.	8	9		
Робітники сектору управління ризиками інформаційної безпеки(3)	Кваліфіковані робітники	Ч, З, М, Д	Ч	Ч,З, М,З Б,Д	Ч	Ч,М,З	Ч	Ч	Ч,З,К, М,В,З Б,Д	Ч	---	РС8-12, Р1
Системний адміністра-тор(1)	Кваліфіковані робітники	Ч	Ч	Ч,З, М	Ч	Ч,З,М	Ч	Ч	Ч,З	Ч	---	РС-7, Р1, М1, К1

*Примітка

1- Інформація про клієнтів; 2- Закупівельна інформація про продукцію компанії; 3- Інформація про бухгалтерські звіти діяльності компанії; 4- Інформація про співробітників; 5- Науково-технічна; 6- Контактна інформація; 7- Юридична інформація; 8- Інформація про захист підприємства; 9- Інформація на веб-сайті.

Ч-читання; З-запис; К-копіювання; В-видалення; М-модифікація; ЗБ-зберігання; Д-друкування.

*Дана таблиця розглядається з точки зору однієї служби безпеки Корпорації, тому в даній схемі представлено сервер, який не знаходиться в зоні обстеження ОІД.

1.8. Висновки до першого розділу

В результаті обстеження ОІД було зроблено актуальну класифікацію інформації, що зберігається та циркулює в підприємстві, також охарактеризовані технічні засоби, яки використовуються на ОІД.

Усі данні, які були отримані в результаті опису першого розділу будуть використовуються для розробки рекомендацій, що допоможуть зменшити уникнути збитків.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1. Модель порушника

Модель порушника представляє собою опис можливих дій порушника, який здійснює несанкціонований доступ до інформації. Модель складається на основі знань, рівня повноважень, можливостей теоретичного та практичного характеру.

Дії зловмисника можуть буду цілеспрямованими або помилковими, в залежності від цього можуть виникнути різні порушення, що визначаються політикою безпеки Корпорації. Насамперед, порушники повинні бути пов'язані з функціонуванню інформаційною системою, а також з обробкою інформації, що потребує захисту.

Оснівними категоріями порушників можуть бути:

– зовнішні порушники, які знаходяться за межами ОІД, але мають можливість фізичного підключення до каналів зв'язку;

– внутрішні порушники яким надано права доступу до інформації з обмеженим доступом;

– технічний персонал, який обслуговує ОІД.

Проаналізувавши об'єкт інформаційної діяльності, Корпорацію «N» можна зробити висновки що найбільш потенціальними порушниками можуть стати або персонал, або конкуренти інших підприємств.

У кожного інформаційного актива є різні ризики, але найбільшим ризиком можна назвати людину, яка не розуміючи наслідки може поширювати інформацію за межі підприємства. Також можуть бути й зовнішні порушники, але це дуже рідкі випадки.

Далі буде розглянуто практичні та потенціальні можливості, знання для можливого порушення системи безпеки, час та місце дії які можуть охарактеризувати порушника.

Таблиця 2.1 - Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загрози
Внутрішні по відношенню до ІТС		
ПВ1	Технічний персонал, який обслуговує приміщення ОІД, в якій розташовані компоненти ІТС(прибиральниця)	1
ПВ2	Користувачі ІТС(спеціаліст економічної безпеки, робітники сектору управління ризками інформаційної безпеки)	2
ПВ3	Адміністратор ІТС, співробітники служби захисту інформації(Системний адміністратор)	3
ПВ4	Співробітники служби безпеки установи та керівники різних рівнів(начальник служби безпеки корпорації, начальник відділу інформаційної безпеки, начальник сектору управління ризками інформаційної безпеки, робітники відділу інформаційної безпеки)	4
Зовнішні по відношенню до ІТС		
ПЗ1	Представники інших організацій , що взаємодіють з питань технічного забезпечення	1
ПЗ2	Хакери	3
ПЗ3	Конкуренти	3

Таблиця 2.2 – Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загрози
М1	Безвідповідальність	2
М2	Самоствердження	1
М3	Корисливий інтерес	3
М4	Професійний обов’язок(ПЗ3)	4

Таблиця 2.3 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні познаки порушника	Рівень загрози
К1	Володіє низькім рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 2.4 - Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загрози
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує лише штатні засоби та недоліки системи захисту для її подолання	3
З3	Використовувати компактні машинні носії	2
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4
З5	Використовувати технічні засоби перехвату інформації	2

Таблиця 2.5-Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загрози
Ч1	Під час ремонту або оновлення	1
Ч2	Під час модернізації обладнання	2
Ч3	Під час роботи ІТС	3
Ч4	Під час роботи ІТС, але запинки роботи частини системи	4

Таблиця 2.6-Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загрози
Д1	У середині приміщення, але без доступу до ІТС	1
Д2	З робочих місць робітників	2
Д3	У зоні керування засобами безпеки	3
Д4	З робочого місця начальства	4

Завдяки розмежування за рівнями загроз, які приведені в таблицях вище(табл. 2.1-2.6) можна визначити найвищий варіант загроз порушника з відповідними характеристиками.

Таблиця 2.7- Модель порушника

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Начальник служби безпеки корпорації	ПВ4	М2	К3	З4	Ч3	Д2	18
	4	2	3	4	3	2	
Начальник відділу інформаційної безпеки	ПВ4	М2	К3	З4	Ч3	Д2	17
	4	1	3	4	3	2	
Начальник сектору управління рисками інформаційної безпеки	ПВ3	М2	К3	З2	Ч3	Д2	15
	3	1	3	3	3	2	
Спеціаліст економічної безпеки	ПВ3	М1	К1	З3	Ч1	Д2	10
	3	1	1	2	1	2	
Робітники відділу інформаційної безпеки	ПВ4	М2	К3	З4	Ч2	Д2	17
	4	2	3	4	2	2	
Робітники сектору управління рисками інформаційної безпеки	ПВ3	М1	К1	З2	Ч1	Д2	11
	3	1	1	3	1	2	
Системний адміністратор	ПВ3	М1	К1	З1	Ч1	Д1	8
	3	1	1	1	1	1	

З останньої таблиці(табл.2.7) видно, що найбільшу загрозу має начальник служби, так як він має велику кількість прав та доступів до інформації, тому корпорація повинна контролювати виконання обов'язків та не наявність різних типів загроз конфіденційній інформації.

2.2. Модель загроз

В кожній організації є своя модель загроз, яка запобігає загрозам конференційній інформації, в даній Корпорації для запобігання ризикам використовується документ «Методика управління ризиками інформаційної безпеки».

Без детального аналізу можливих загроз ОІД існувати не зможе, тому далі, буде розглянуто можливі актуальні загрози, завдяки яким Корпорація може зазнати збитки.

Усі джерела інформаційної безпеки можуть бути виділені в три основні категорії:

– стихійні;

– антропогенні(загрози, які можуть виникнути завдяки діям різних суб'єктів);

– техногенні(загрози, які виникають у наслідок роботи технічних засобів).

Актуальність загроз можна визначити завдяки коефіцієнту рівня безпеки, далі приведена необхідна формула:

$К_{неб} = \frac{К1*К2*К3}{125}$, 125 - це максимальне число добутку показників $К_{неб}$ [7].

Основні коефіцієнти для розрахунку рівня безпеки для антропогенних джерел:

К1 (можливість виникнення джерела) - ступінь доступності до захищеного об'єкту:

5 - антропогенний джерело загроз має повний доступ до технічних і програмних засобам обробки інформації, що захищається (характерно для

внутрішніх антропогенних джерел, наділених максимальними правами доступу, наприклад, представники служб безпеки інформації, адміністратори);

4 - антропогенний джерело загроз має можливість опосередкованого, що не певного функціональними обов'язками, (за рахунок побічних каналів витоку інформації, використання можливості доступу до привілейованих робочих місць) доступу до технічних і програмних засобів обробки інформації, що захищається (характерно для внутрішніх антропогенних джерел);

3 - антропогенний джерело загроз має обмежену можливість доступу до програмних засобів в силу введених обмежень у використанні технічних засобів, функціональних обов'язків або за родом своєї діяльності (характерно для внутрішніх антропогенних джерел зі звичайними правами доступу, наприклад, користувачі, або зовнішніх антропогенних джерел, які мають право доступу до засобам обробки і передачі інформації, що захищається, наприклад, хакери, технічний персонал);

2 - антропогенний джерело загроз має дуже обмежену можливість доступу до технічних засобів і програм, що обробляють захищається інформацію (характерно для зовнішніх антропогенних джерел).

1 - антропогенний джерело загроз не має доступу до технічних засобів і програм, обробних захищається інформацію. [7]

К2 (готовність джерела) - визначає ступінь кваліфікації і привабливість здійснення діянь зі боку джерела загрози:

5 - захищені інформаційні ресурси містять інформацію, яка може завдати непоправної шкоди і привести до краху організації, що здійснює захист;

4 - захищені інформаційні ресурси містять інформацію, яка може бути використана для отримання вигоди на користь джерела загрози або третіх осіб;

3 - захищені інформаційні ресурси, містять інформацію, розголошення якої може завдати шкоди окремим особам;

2 - захищені інформаційні ресурси містять інформацію, яка при її накопиченні і узагальненні протягом певного періоду може завдати шкоди організації, здійснює захист;

1 - інформація не представляє інтерес для джерела загрози[7].

К3 (фатальність) - ступінь непереборності наслідків прояви загрози:

5 - результати прояви загрози можуть призвести до повного руйнування (знищення, втрати) об'єкта захисту, як наслідок до непоправних втрат і виключення можливості доступу до захищається інформаційних ресурсів;

4 - результати прояви загрози можуть призвести до руйнування (Знищення, втрати) об'єкта і до значних витрат (матеріальним, тимчасовим і ін.) На відновлення наслідків, порівнянних з витратами на створення нового об'єкту і суттєвого обмеження часу доступу до ресурсів, що захищаються;

3 - результати прояви загрози можуть призвести до часткового руйнування об'єкта захисту і, як наслідок, до значних витрат на відновлення, обмеження часу доступу до захищаються;

2 - результати прояви загрози можуть призвести до часткового руйнування (знищення, втрати) об'єкта захисту, які не потребують великих витрат на його відновлення і, практично не впливають на обмеження часу доступу до захищається інформаційних ресурсів;

1 - результати прояви загрози не можуть вплинути на діяльність об'єкта захисту[7].

Кожен з коефіцієнтів оцінюється експертно-аналітичним методом по п’ятибальній схемі, де 1 – це мінімальна ступінь, а 5 – максимальна.

Далі розглянемо основні джерела загроз, які можуть виникнути в Корпорації «N».

Таблиця 2.8 – Перелік можливих антропогенних внутрішніх джерел загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
Начальник служби безпеки Корпорації	5	4	5	100	0,8
Начальник відділу інформаційної безпеки	4	4	4	64	0,512
Начальник сектору управління ризиками інформаційної безпеки	4	3	4	48	0,384
Спеціаліст економічної безпеки	3	2	4	24	0,192

Продовження таблиці 2.8

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
Робітники відділу інформаційної безпеки	3	3	3	27	0,216
Робітники сектору управління ризиками інформаційної безпеки	3	2	3	18	0,144
Системний адміністратор	2	4	3	24	0,192

На таблиці показано можливі найвищі внутрішні загрози, які можуть виникнути. Найбільш загрозу можуть нести начальник служби безпеки, тому що він має доступ до усіх даних та контролює усі питання стосовно інформаційних ресурсів, та начальник відділу інформаційної безпеки, який безпосередньо займається безпекою Корпорації та усі важливі питання стосовно інформаційної безпеки проходять через нього. З найнижчим ризиком будуть працівники, які мають достатньо невеликі доступи до інформації з обмеженим доступом, а саме робітники сектору управління ризиками інформаційної безпеки.

Таблиця 2.9– Перелік можливих антропогенних зовнішніх джерел загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
Допоміжний персонал(прибиральниця, охорона)	2	3	2	12	0,096
Конкуренти	2	4	5	40	0,32
Хакери	2	4	4	32	0,256
Робітники комунальних служб	1	2	2	4	0,008

У переліку можливих антропогенних загроз найвищий показник має конкуренти, які можуть купити інформацію з обмеженим доступом у працівників компанії, або найняти хакерів. Далі за можливістю загрози йдуть хакери, які можуть отримати інформацію. Останні критерії не розглядаються, бо коефіцієнт має результат нижчий ніж 1.

Основні коефіцієнти для розрахунку рівня безпеки для техногенних джерел:

К1 (можливість виникнення джерела) - віддаленість від об'єкта, що захищається:

5 - об'єкти захисту самі містять джерела техногенних загроз і їх територіальне поділ неможливо;

4 - об'єкти захисту розташовані в безпосередній близькості від джерел техногенних загроз і будь-який прояв таких загроз може зробити істотний вплив на об'єкт, що захищається;

3 - об'єкти захисту розташовуються на відстані від джерел техногенних загроз, на якому прояв впливу цих загроз може надати не істотний вплив на об'єкт захисту;

2 - об'єкт захисту розташовується на відстані від джерела техногенних загроз, виключає можливість його прямого впливу;

1 - об'єкт захисту розташовується на значній відстані від джерел техногенних загроз, повністю виключає будь-які дії на об'єкт, що захищається, в тому числі і по вторинним [7].

К2 (готовність джерела) - наявність необхідних умов:

4 - тобто умови сприятливі або можуть бути сприятливі для реалізації загрози (Наприклад, активізація сейсмічної активності);

3 - тобто умови сприятливі для реалізації загрози, проте довгострокові спостереження не припускають можливості її активізації в період існування і активної діяльності об'єкта захисту;

2 - тобто існують об'єктивні причини на самому об'єкті або в його оточенні, перешкоджають реалізації загрози;

1 - тобто відсутні передумови для реалізації передбачуваного події [7].

К3 (фатальність) - ступінь непереборності наслідків прояви загрози.

Таблиця 2.10 – Перелік можливих техногенних загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
Зовнішні					
Мережа інженерних комунікацій (тепло, водо, газопостачання)	4	3	4	48	0,384
Внутрішні					
Неякісні технічні засоби обробки інформації	4	2	4	32	0,256
Неякісне програмні засоби обробки інформації	3	2	4	24	0,192
Неякісні допоміжні засоби обробки інформації	2	3	3	18	0,144

У переліку техногенних загроз велику роль грає мережа інженерних комунікацій, бо неякісне оснащення приміщень може призвести до відсутності робітників та можливості безпеки інформації, далі можна розглянути внутрішні техногенні загрози, так як програмне забезпечення усе ліцензійне, то велику загрозу не несе, а основні та допоміжні технічні засоби можуть нести безпеку, але без допоміжних засобів Корпорація може обійтися, тому основні загрози будуть нести в собі мережа інженерних комутацій та неякісні технічні засоби обробки інформації.

Основні коефіцієнти для розрахунку рівня безпеки для стихійних джерел:

К1 - особливості місцевості:

5 - об'єкт захисту розташований в зоні дії природних катаклізмів;

4 - об'єкт захисту розташований в зоні, в якій багаторічні спостереження показують можливість прояву природних катаклізмів;

3 - об'єкт захисту розташований в зоні в якій по проведеним спостереженням на протягом довгого періоду відсутні прояви природних катаклізмів, але є передумови виникнення стихійних джерел загроз на самому об'єкті;

2 - об'єкт захисту знаходиться поза межами зони дії природних катаклізмів, проте на об'єкті є передумови виникнення стихійних джерел загроз;

1 - об'єкт захисту знаходиться поза межами зони дії природних катаклізмів і на об'єкті відсутні передумови виникнення стихійних джерел загроз [7].

К2 - наявність необхідних умов.

К3 (фатальність) - ступінь неперебірності наслідків прояви загрози.

Таблиця 2.11 – Перелік можливих стихійних загроз

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
Пожежа	2	3	4	24	0,192
Землетрус	1	1	3	3	0,024
Ураган	1	1	3	3	0,024

Продовження таблиці 2.11

Джерело загроз	К1	К2	К3	К1*К2*К3	$К_{неб}$
Повінь	1	2	3	6	0,024
Непередбачені обставини	2	2	3	12	0,096

Розглянувши перелік можливих стихійних загроз можна сказати, що вони не мають великих наслідків, тому що більшість коефіцієнтів дорівнює нижче одиниці. Тому можливою загрозою може бути лише пожежа.

Розглянувши таблиці вище (табл.2.8-2.11) можна зробити висновок, що основними загрозами будуть:

- начальник служби безпеки Корпорації;
- начальник відділу інформаційної безпеки;
- конкуренти;
- хакери;
- мережа інженерних комунікацій (тепло, водо, газопостачання);
- неякісні технічні засоби обробки інформації;
- пожежа.

Загрози виникають не самі по собі, а завдяки факторам – вразливості, завдяки яким порушується безпека інформації з обмеженим доступом. Наявність або усунення вразливості впливає на можливу реалізацію загроз безпеки інформації. Тому далі розглянемо вразливості даних актуальних загроз.

Вразливості можуть бути:

1. Об’єктивні;
2. Суб’єктивні;
3. Випадкові.

Проаналізувавши даний ОІД можна зробити висновки, що для даної ІТС можливі такі вразливості системи:

1. Об’єктивні:

1.1. Можливість підключення до бездротової мережі;

1.2. Відсутність змін паролів для Wi-Fi;

1.3. Недостатній контроль приміщення;

1.4. Відсутність контролю наявності закладних пристроїв.

2. Суб'єктивні:

2.1. Відсутність контролю за змінними накопичувачами інформації;

2.2. Відсутній журнал подій;

2.3. Вільний доступ до мережі Інтернет;

2.4. Помилки робітників.

3. Випадкові:

3.1. Збій;

3.2. Відмова.

Аналіз вразливостей приведено нижче в таблиці 2.12.

За допомогою $(К_{оп})f$ можна визначити коефіцієнт вразливості:

$(Коп)f = \frac{К1*К2*К3}{125}$, 125-максимальнє число добутку.

Де (К1)f – фатальність (визначає ступінь впливу уразливості на фатальність наслідків реалізації загрози), (К2)f – доступність (виявляє можливість використання уразливості), (К3) f – кількість (кількість елементів, на яких може бути виявлена уразливість) [7].

Кожен з коефіцієнтів оцінюється експертно-аналітичним методом по п'ятибальній схемі, де 1 – це мінімальна ступінь, а 5 – максимальна.

К1:

– 1 – використання вразливостей не призведе до серйозних насадків;

– 2 – ймовірність використання вразливостей навряд чи призведе до загрози;

– 3 – середній шанс, що вразливість може спричинити загрозу;

– 4 – середньо-високий шанс, що вразливість може привести до загрози;

– 5 – вразливість призведе до реалізації загрози.

К2:

– 1 – можливість використати вразливість не можлива;

– 2 – для реалізації вразливості буде потрібно багато часу;

– 3 – для реалізації вразливості необхідні деякі умови;

– 4 – вразливість може використати людина, яка володіє відповідними знаннями;

– 5 – вразливість може бути використана будь-якою особою.

К3:

– 1 – 0-1 елемент;

– 2 – 2-5 елементів;

– 3 – 6-10 елементів;

– 4 – 10-15елементів;

– 5 – 16 елементів.

Таблиця 2.12 – Ранжування вразливостей інформації в ІТС

Вразливість	К1	К2	К3	$(К_{оп})f$
Можливість підключення до бездротової мережі	3	2	5	0,24
Відсутність змін паролів для Wi-Fi	3	3	5	0,36
Недостатній контроль приміщення	3	2	2	0,096
Відсутність контролю наявності закладних пристроїв	2	3	2	0,096
Відсутність контролю за змінними накопичувачами інформації	5	5	4	0,8
Відсутній журнал подій	5	4	4	0,64
Вільний доступ до мережі Інтернет	2	3	4	0,192
Помилки робітників	2	5	5	0,4
Збій	1	2	5	0,08
Відмова	2	4	5	0,32

Проаналізувавши вразливості за таблиці(табл.2.12) вище можна зробити висновок, що можливо знехтувати значеннями з коефіцієнтом нижчим нижчім або який дорівнює 0,2. Тому залишаються максимально актуальні вразливості:

– відсутність контролю за змінними накопичувачами інформації;

– відсутній журнал подій;

– помилки робітників.

Далі проведемо аналіз актуальних загроз. Проаналізувавши ОІД та основні джерела загроз та вразливості маємо:

– Д1 - Начальник служби безпеки Корпорації;

– Д2 - Начальник відділу інформаційної безпеки;

– Д3 – Конкуренти;

– Д4 – Хакери;

– Д5 - Мережа інженерних комунікацій (тепло, водо, газопостачання);

– Д6 - Неякісні технічні засоби обробки інформації;

– Д7 – Пожежа;

– В1 - Можливість підключення до бездротової мережі;

– В2 - Відсутність змін паролів для Wi-Fi;

– В3 - Недостатній контроль приміщення;

– В4 - Відсутність контролю наявності закладних пристроїв;

– В5 - Відсутність контролю за змінними накопичувачами інформації;

– В6 - Відсутній журнал подій;

– В7 - Вільний доступ до мережі Інтернет;

– В8 - Помилки робітників;

– В9 – Збій;

– В10 – Відмова.

Далі розглянемо критичність використання джерел, які містять вразливості.

Таблиця 2.13 – Ранжування загроз

	Вразливості									
Джерела загроз	В1	В2	В3	В4	В5	В6	В7	В8	В9	В10
Д1	0,192	0,288	-	-	0,64	0,48	0,153	0,32	-	-
Д2	0,122	0,184	-	-	0,409	0,327	0,098	0,204	-	-
Д3	-	-	0,03	0,03	0,256	-	-	-	-	-
Д4	0,061	0,092	-	-	0,204	0,163	-	-	0,02	-

Продовження таблиці 2.13

Джерела загроз	В1	В2	В3	В4	В5	В6	В7	В8	В9	В10
Д5	-	-	-	-	-	-	-	-	0,03	0,122
Д6	0,061	-	0,024	-	-	-	-	-	0,02	0,081
Д7	-	-	0,288	-	-	-	-	-	0,15	-

Далі відкидаємо усі загрози з коефіцієнтом нижчим за 0,1. Такими загрозами будуть:

– ураження системи через можливість підключення до бездротової мережі(Д4В1/Д6В1);

– несанкціоноване підключення до системи через не зміну паролів для Wi-Fi(Д4В2);

– відсутність наявності камер спостереження у офісі (Д3В3,Д6В3);

– відсутній контроль наявності закладних пристроїв(Д3В4);

– відсутність обмежень на використання мережі Інтернет (Д2В7);

– збій в системі (Д4В9/Д5В9/Д6В9);

– відмова в експлуатації (Д6В10).

Далі розглянемо загрози, які мають вищий коефіцієнт ніж 0,1. Тому кваліфікуємо загрози за їх ризиками в конфіденційності, цілісності та доступності. Класифікація приведена нижче у таблиці 2.14

Таблиця 2.14 - Перелік загроз з визначенням порушень властивостей

Загроза	Ризики для		
	К	Ц	Д
Можливість ознайомлення з даними через несанкціоноване підключення до мережі Інтернет	+	+	-
Можливість підключення стороннім особам до мережі інтернет через незміну паролів	+	+	+
Недостатній контроль приміщень, можлива передача інформація третім особам	-	+	+
Відсутній контроль за наявністю та використанням змінних накопичувачей інформації	+	-	-
Відсутній журнал подій	+	+	-
Контроль трафіку та вільного використання мережі Інтернет	-	+	-

Продовження таблиці 2.14

Загроза	Ризики для		
	К	Ц	Д
Навмисна або ненавмисна помилка робітників	+	+	+
Збій в системі	-	+	+
Відмова технічних засобів	-	-	+

Де К- конфіденційність, Ц - цілісність, Д - доступність, +/- - це вплив певної загрози на певну властивість.

В результаті створення моделі загроз було виявлено яка інформація циркулює та зберігається в підприємстві. завдяки результатам можна сказати що основним ризиком для інформації буде в її цілісності, тому далі буде розглянуто мінімальний стандарт для профіля захищеності.

2.3 Профіль захищеності

Враховуючи характеристики, що розглядалися вище, можна зробити висновок, що нам потрібний цей профіль захищеності(усе обрано відповідно до вимог НД ТЗІ 2.5-005 -99[12]):

3.Ц.1 = { ЦД-1, ЦВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НВ-1 }

Перелік послуг, що входять в обраний профіль захищеності приведено на НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [12]. Далі розглянемо кожний профіль окремо.

ЦД1 – Мінімальна довірча цілісність

Мінімальна довірча цілісність дозволяє керувати потоками інформації від інших користувачів до інформації з обмеженим доступом. Для даної послуги необхідно мати список об’єктів, які відносяться до комп’ютерної системи. Повинно матися розмежування доступом завдяки атрибутам доступу. Атрибут доступу – це будь-яка інформація, яка використовується для надання та керування доступом.

В Корпорації присуне розмежування доступив до захищеного об’єкту та користувача. Насамперед усі користувачі системи мають різні облікові записі та свої паролі для заходження в них. Усі зміни прав доступу обробляються через керівництво, а далі змінюються атрибути доступу.

ЦВ-1 – Мінімальна цілісність при обміні

Мінімальна цілісність при обміні допомагає уникнути модифікації файлів, які експортуються або імпортуються через незахищене середовище, наприклад, мережу Інтернету. Ця послуга визначає число об’єктів, які потребують захисту та дає спроможність користувачу редагувати рівнем захищеності.

Данна функція в Корпорації реалізована як шифрування даних, які проходять незахищене середовище, що дозволяє зменшити ризики модернізації інформації.

НР-2 – Захищений журнал

Захищений журнал допомагає контролювати небезпечні дії для комп’ютерної системи. Дана функція повинна мати перелік подій, які реалізуються в КЗЗ. Захищений журнал повинен мати функцію реєстрації усіх подій, які стосуються безпеки. Повинен мати захист від несанкціонованого доступу, модифікацій та пошкоджень.

Дана функція не реалізована в Корпорації, тому далі буде представлена інструкція для впровадження журналу подій, але зовнішній аналіз використовується.

НИ-2 – Одиночна індикація та автентифікація

Ці операції дозволяють перевірити особистість користувача, який намагається отримати доступ до комп’ютерної системи. Для цього повинні використовуватися атрибути доступу. Якщо з’явиться новий користувач, або буде змінюватися атрибут доступу, повинно бути використано захищений механізм. Система повинна бути захищена від модернізації або руйнування.

Ця операція виконана в Корпорації, бо є відповідальна особа, яка займається реєстрацією нових робітників до системи та надалі робітник змінює свій пароль, який буде знати лише він.

НК-1 – Однонаправлений достовірний канал

Завдяки цій послузі користувач може взаємодіяти з КЗЗ, можливості користувача повинні ініціювати захищений обмін. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації.

Ця послуга використовується в Корпорації, завдяки ній можлива робота з обліковими записами.

НО-1 – Виділення адміністраторів

Виділення адміністраторів допомагає зменшити кількість помилкових дій користувачів. Для даної послуги необхідно виділити роль адміністратора та надати йому відповідні функції.

В Корпорації є декілька адміністраторів, але у службі, яка розглядається є наявність системного адміністратора та адміністратора безпеки, за якого відповідає один з робітників відділу інформаційної безпеки.

НЦ-1 – КЗЗ з контролем цілісності

Ця послуга визначає можливості КЗЗ захищати себе і гарантувати безпеку інформації. Політика цілісності повинна визначати склад та контроль компонентів КЗЗ, при виявлені порушень повинні бути повідомлені адміністратори. Повинні бути читки обмеження для доступу до захищеної інформації. Має проводитись зовнішній аналіз даних.

В Корпорації є читки розмежування доступу та неможливість використання системи без входу до неї.

НВ-1 – Автентифікація вузла

Автентифікація вузла дозволяє використовувати різні КЗЗ та перевіряти його ідентичність. Повинні визначатися можливі атрибути КЗЗ та процедури, які необхідні для індикації при обміні даних. Усе це повинно відбуватися на підставі затвердженого протоколу автентифікації.

Відбувається в Корпорації.

Далі будуть представлені проектні рішення, які допоможуть модернізувати та покращити безпеку для інформації з обмеженим доступом.

2.4 Рекомендації для покращення системи безпеки

Спираючись на дані, які обробляються в Корпорації, було обрано політики безпеки, які допоможуть покращити безпеку до необхідного рівня захисту інформації. Політикою безпеки є основним об'єктом захисту для базового захисту інформації. Завдяки політики встановлюються основні засоби, які запобігають витоку через обробку, збереження, передачу та знищення інформації. Виконання нової політики безпеки є обов'язковим для усіх робітників ОІД.

Від самого початку політика безпеки передбачає базові правила, які повинні виконуватися в Корпорації:

1. В ОІД повинні бути введені чіткі правила розмежування прав доступу, де кожний користувач повинен мати особистий обліковий запис та інфікуватися системою. Кожний інформаційний ресурс повинен мати свій атрибут доступу, завдяки котрому здійснюється організація прав доступу користувача до цього об'єкту.

2. В системі повинна бути ідентифікація та автентифікація користувачів, де автентифікація повинна відбуватися за допомогою захищених механізмів.

3. Кожний користувач повинен мати чіткі права доступу до інформаційних об'єктів , щоб уникнути збитків від ненавмисних або навмисних помилок.

4. Для захисту системи використовувати якісне та ліцензійне програмне забезпечення, а також антивірус, який відповідає усім стандартом якості. Також регулярно оновлювати бази даних сигнатур та ін. з достовірних джерел.

5. Підтримувати та організовувати необхідність процесу навчання, контролю та підготовки персоналу за напрямками інформаційної безпеки.

6. Ввести планові заходи контролю ризиків інформаційної безпеки та виживати різноманітні дії, щоб уникнути можливих витоків інформації.

7. Відсутність не виконання законів та норм можуть призвести до закриття ОІД.

8. Політика безпеки ОІД повинна бути побудована так, що інциденти стосовно безпеки не призводили до значних втрат підприємства.

9. Відповідальним за дотримання інструкцій, що до безпеки є начальник служби інформаційної безпеки та начальники відділів цієї служби.

10. Користувачі системи повинні контролювати щоб жодна третя особа не ознайомилася з інформацією, яка не входить в її службові обов'язки.

11. Системний адміністратор повинен контролювати усі підключення до мережі Інтернет, мати засоби моніторингу та виконання політики безпеки.

Першочергово розглянемо ті загрози, які знаходяться у великому ризику, а саме такі як відсутність контролю за змінними накопичувачами. Завдяки цій загрозі може виникнути перехват інформації з обмеженим доступом шляхом вставки флеш-накопичувача з шкідливим програмним забезпеченням та завдяки ньому отримання інформації.

Також відсутність журналу подій дуже впливає на безпеку, бо без нього можливі несанкціонованого дії над системою без можливого контролю над даними.

Політика використання, зберігання та обліку носіїв інформації

Носій ключової інформації - носій інформації (дискета, флеш-пам'ять, і інші носії) на яких зберігатися електронний ключ, призначений для захисту електронних взаємодій.

Мета політики:

Встановити правила використання , зберігання та обліку носіїв інформації. Користувачі системи повинні дотримуватися, які будуть оговорені в даній політиці.

Область дії:

Політика безпеки розповсюджується на всіх користувачів, які мають доступ до електронної інформації та які не мають право на використання носіїв інформації відповідно до своїх посадових обов’язків.

Відповідальні особи:

Відповідальною особою за політику використання, зберігання та обліку носіїв інформації користувачами системи є системний адміністратор та начальник відділу інформаційної безпеки.

Особи, які мають доступ до носіїв ключової інформації, несуть за неї персональну відповідальність.

Порядок використання носіїв інформації:

Під використанням носіїв інформації в ІС Організації розуміється їх підключення до інфраструктури ІС з метою обробки, прийому / передачі інформації між ІС і носіями інформації.

В ІС допускається використання тільки врахованих носіїв інформації, які є власністю Організації і піддаються регулярної ревізії і контролю.

До наданим носіїв інформації пред'являються ті ж вимоги ІБ, що і для стаціонарних автоматизованих робочих місць (доцільність додаткових заходів забезпечення ІБ визначається адміністраторами ІС).

Носії інформації надаються працівникам Організації з ініціативи Керівників структурних підрозділів у випадках:

– необхідності виконання новоприйнятим працівником своїх посадових обов'язків;

– виникнення у працівника Організації виробничої необхідності.

Процес надання працівникові Організації носіїв інформації складається з наступних етапів:

1. Підготовка заявки в затвердженій формі, здійснюється Керівником структурного підрозділу на ім'я Керівника Організації.

2. Узгодження підготовленої заявки (для отримання висновку про можливість надання працівнику Організації заявленого носія інформації з начальником відділу ІТ.

3. Передача оригіналу заявки до відділу інформаційних технологій для обліку наданого носія інформації і внесення змін в «Список працівників Організації, які мають право роботи пристроями поза територією Корпорації.

При використанні наданих працівникам Організації носіїв інформації необхідно:

1. Дотримуватися вимог цього Положення.

2. Використовувати носії інформації виключно для виконання своїх службових обов'язків.

3. Доводити до відома адміністраторів ІС про будь-які факти порушення вимог цього Положення.

4. Дбайливо ставиться до носіїв інформації.

5. Експлуатувати і транспортувати носії інформації відповідно до вимог виробників.

6. Забезпечувати фізичну безпеку носіїв інформації усіма розумними способами.

7. Сповіщати адміністраторів ІС про факти втрати (крадіжки) носіїв інформації.

При використанні наданих працівникам Організації носіїв інформації заборонено:

– використовувати носії інформації в особистих цілях;

– передавати носії інформації іншим особам (за винятком адміністраторів ІС);

– залишати носії інформації без нагляду, якщо не вжито заходів щодо забезпечення їх фізичної безпеки;

– використовувати правило «чистого столу», дотримуватися щодня. Використовується перед відходом співробітника з робочого місця. Воно

забезпечує захист конфіденційних даних від розголошення і забезпечує періодичний догляд за своїм робочим місцем.

Будь-яка взаємодія (обробка, прийом / передача інформації) ініційоване працівником Організації між ІС і неврахованими (особистими) носіями інформації, розглядається як несанкціоноване (за винятком випадків обумовлених з адміністраторами ІС заздалегідь). Організація залишає за собою право блокувати або обмежувати використання носіїв інформації.

Інформація про використання працівниками Організації носіїв інформації в ІС протоколюється і, при необхідності, може бути надана Керівникам структурних підрозділів, а також Керівництву Організації.

При підозрі працівника Організації в несанкціонованому та / або нецільового використання носіїв інформації проводиться службова перевірка.

Політика безпеки для встановлення журналу подій

Мета політики:

Встановити реалізацію та правила роботи з журналом подій, в якому буде описуватися основні події зв’язані з роботою інформаційної системи, а саме інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Використання даної політики безпеки підвищує рівень контролю та захищеності обробляємо інформації. Журнал повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

Область дії:

Область дії політики безпеки для встановлення журналу подій розповсюджується на всіх користувачів, що мають доступ до електронних документів.

Відповідальні особи:

Відповідальною особою за політику встановлення журналу подій користувачами системи є системний адміністратор та начальник відділу інформаційної безпеки.

Політика безпеки:

Аналіз журналів подій є однією з найважливіших задач в роботі системного адміністратора або фахівця з інформаційної безпеки. Для підтримки безпеки і стабільності роботи комп'ютерних мереж доводиться регулярно відслідковувати події, що відбуваються в мережі. До таких подій належать: спроби входу в системи (вдалі і невдалі), події, пов'язані з використанням різних інформаційних і фізичних ресурсів (створення, відкриття, видалення файлів, використання зовнішніх запам'ятовуючих пристроїв, принтерів) та інше. Процес моніторингу журналів Windows завжди вимагає чимало часу.

Портативна програма для перегляду інформації з журналу подій Windows. Утиліта виведе докладний звіт про використання файлів і виконанні системних процедур із зазначенням дати і часу.

LastActivityView - це унікальне додаток, яке надасть докладні дані про раніше виконаних користувачами діях і значущих випадках внутрісистемної активності на Вашому комп'ютері.

Програма сама не веде записи історії, а являє собою зручну оболонку для структурованого відображення інформації з системного журналу подій ОС.

Глибина перегляду історії, як правило, досягає дати установки операційної системи. У разі якщо використовувалися сторонні утиліти для звільнення вільного дискового простору, велика ймовірність, що записи журналу подій будуть доступні тільки з моменту останньої чистки.

LastActivityView відображаються дані про події:

- початок / завершення роботи системи;
- вхід / вихід користувача;
- запуск / зупинку установника Windows;
- створення точки відновлення;
- переходи системи в сплячий режим і глибокого сну;
- перегляд папки в провіднику;
- перехід за посиланням;
- відкриття або звернення до файлу.

Для всіх подій вказується дата і час початку активності. При перегляді історії роботи з фалами надається інформація про ім'я файлу, шляхи розташування та інші доступні дані.

У програмі є інструмент пошуку, в якому можна вказати, що цікавлять подія або пов'язані з ним атрибути.

При необхідності перегляду історії за конкретний період можна вказати кількість днів, годин, хвилин або секунд для зворотного відліку з поточного моменту.

Так само утиліта дозволяє експортувати отриману інформацію, зберігши всі дані або виділену область в HTML-файл.

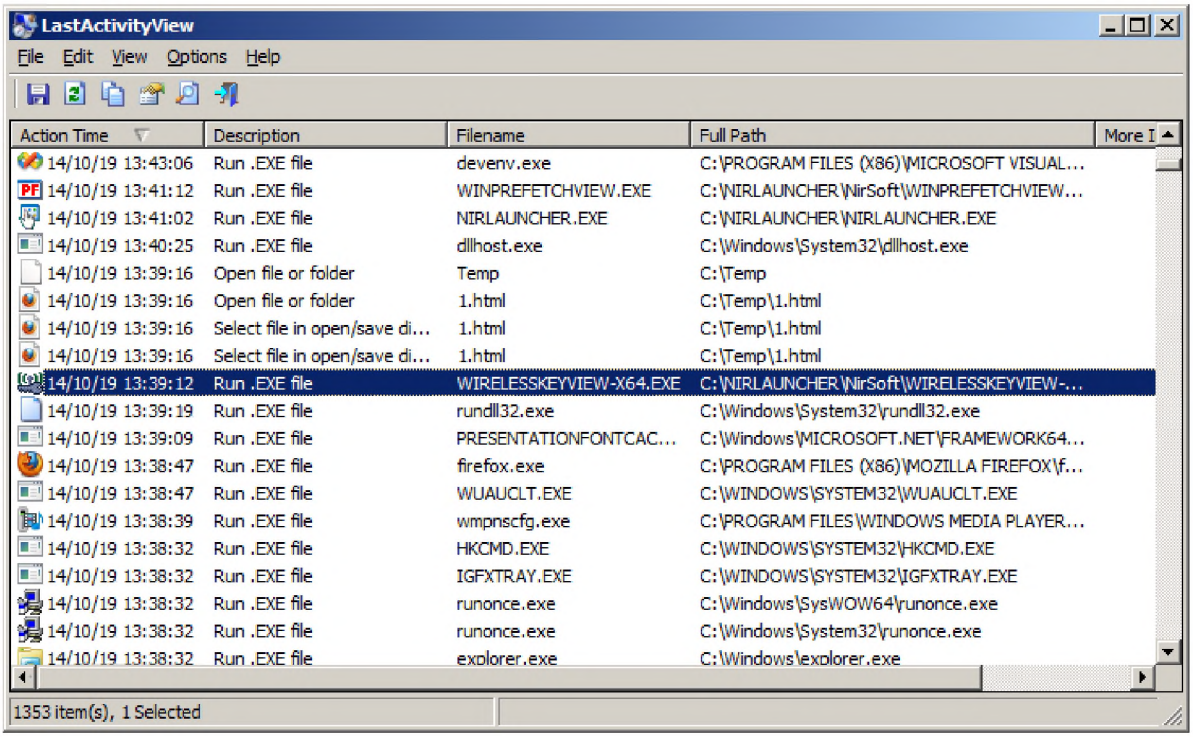

Рисунок 2.1 – Вигляд програми для використання журналу подій

Завдяки цій програмі можна контролювати усі процеси, які відбуваються в системі та котрий користувач робив які дії.

Якщо з’являється якийсь невідомий користувач або процес, то повідомлять керівництву та проводиться службова перевірка.

Далі буде розглянуто менш великі вразливості, але які також можуть принести значні ризики та збиток.

Політика вибору, зміни паролів та використання мережі Інтернет

Мета політики:

Вставити правила використання та зміни паролів, а також зменшити можливість використання мережі не для робочих цілей. Користувачі системи повинні дотримуватися вимог, що регламентуються даною політикою. Використання даної політики зменшить рівень вразливості та допоможе уникнути можливого втручання третіх осіб. Також збільшить коефіцієнт виконання роботи робітниками.

Область дії:

Область дії політики вибору, зміни паролів та використання мережі Інтернет розповсюджується на всіх користувачів, що мають доступ до мережі Інтернет.

Відповідальні особи:

Для отримання паролю потрібно підписати документ, в якому указано усі дані щодо користувача якому дається доступ, цим займається керівник підрозділу. Далі, видачу паролів робить особисто системний адміністратор.

Політика безпеки:

Для того, щоб використовувати мережу Інтернет необхідно отримати до неї доступ. Для цього потрібно укласти договір, в якому указати своє ім'я та посаду. Після цього віддати цей документ до керівника, який передають до системного адміністратора. Опираючись на посаду, системний адміністратор повинен визначити права доступу, які дозволять використовувати мережу. Різницею може бути вільний доступ та тільки до робочої пошти.

Системний адміністратор особисто видає пароль та налагоджує систему. Далі, ведеться контроль та аналіз можливого трафіку. Якщо трафік перебільшує можливий, то повідомляється в службу безпеки Корпорації.

Записи про використання мережі повинні зберігатися протягом 180 діб. Повна планова зміна паролів користувачів повинна проводитися регулярно, не рідше одного разу в 30 днів.

Правила парольного захисту:

1. Не використовуйте один і той же пароль для доступу до облікових записів ОІД і до інших ресурсів (наприклад, доступ в інтернет з дому, систем електронної комерції і т. Д.). По можливості не використовуйте один і той же пароль для доступу до різних ресурсів всередині компанії.

2. Не повідомляйте ваш пароль нікому, навіть вашому секретарю або обслуговуючому персоналу. Всі паролі є конфіденційною інформацією.

3. Список заборонених дій:

4. Не повідомляйте нікому свій пароль по телефону.

5. Не відправляйте свій пароль по електронній пошті.

6. Не повідомляйте свій пароль членам своєї сім'ї.

7. Не повідомляйте свій пароль товаришам по службі перед відходом у відпустку.

8. Не записуйте пароль і не зберігайте його на робочому місці.

9. Не зберігайте паролі у файлі на комп'ютері, включаючи переносний, без шифрування.

Якщо ви вважаєте, що обліковий запис або пароль скомпрометовані, треба повідомити про це керівництву і змініть всі паролі.

Відділ безпеки інформації повинен регулярно проводити підбір або спроби злому паролів. Якщо пароль буде підібраний, то його слід змінити.

Будь-який співробітник, який порушив політику безпеки, може бути підданий покаранню аж до звільнення.

Політика безпеки для контролю доступу

Мета політики:

Встановити необхідне спостереження за робітниками та роботою яку вони виконують. Користувачі системи повинні дотримуватися вимог, що регламентуються даною політикою. Виконання вимог даної політики зніжить шанс передачі інформації конкурентам та покращить роботу робітників.

Область дії:

Область дії політики безпеки відносно паролів розповсюджується на всіх користувачів, що мають доступ електронних документів та особам, які мають доступ до знаходження робочої станції інших робітників з більш великими права до інформації з обмеженим доступом.

Відповідальні особи:

Відповідальною особою за політику доступу системний адміністратор та начальник сектору управління ризиками.

Політика безпеки:

Залежно від способу здійснення доступу до ресурсів системи і наданих їм повноважень внутрішні порушники поділяються на п'ять категорій.

Категорія А: незареєстровані в системі особи, які мають санкціонований доступ в приміщення з обладнанням. Особи, які належать до категорії А можуть: мати доступ до будь-яких фрагментів інформації, що розповсюджується по внутрішніх каналах зв'язку корпоративної мережі; розташовувати будь-якими фрагментами інформації про топології мережі, про використовувані комунікаційних протоколах і мережевих сервісах; розташовувати іменами зареєстрованих користувачів системи і вести розвідку паролів зареєстрованих користувачів.

Категорія В: зареєстрований користувач системи, який здійснює доступ до системи з віддаленого робочого місця. Особи, які належать до категорії В: своєму розпорядженні всі можливості осіб, що відносяться до категорії А; знають, принаймні, одне легальне ім'я доступу; володіють усіма необхідними атрибутами, що забезпечують доступ до системи (наприклад, перелом); мають санкціонований доступ до інформації, що зберігається в БД і на файлових серверах корпоративної мережі, а також на робочих місцях користувачів. Повноваження користувачів категорії В з доступу до інформаційних ресурсів корпоративної мережі підприємства повинні регламентуватися політикою безпеки, прийнятої на підприємстві.

Категорія C: зареєстрований користувач, який здійснює локальний або віддалений доступ до систем входять до складу корпоративної мережі. Особи, які належать до категорії C: володіють всіма можливостями осіб категорії B; мають інформацію про топології мережі, структурі БД і файлових систем серверів; мають можливість здійснення прямого фізичного доступу до технічних засобів ІС.

Категорія D: зареєстрований користувач системи з повноваженнями системного (мережевого) адміністратора. Особи, які належать до категорії D: володіють всіма можливостями осіб категорії C; мають повну інформацію про системний і прикладному програмному забезпеченні ІС; мають повну інформацію про технічні засоби та конфігурації мережі; мають доступ до всіх технічних і програмних засобів ІС і володіють правами налаштування технічних засобів і програмного забезпечення. Концепція безпеки вимагає підзвітності осіб, що відносяться до категорії D і здійснення незалежного контролю над їх діяльністю.

Категорія E: програмісти, відповідальні за розробку і супровід загальносистемного і прикладного ПЗ, що використовується в ІС. Особи, які належать до категорії E: володіють можливостями внесення помилок, програмних закладок, установки троянських програм і вірусів на серверах корпоративної мережі; можуть мати у своєму розпорядженні будь-якими фрагментами інформації про топології мережі і технічних засобах ІС.

Опираючись на можливість отримання інформації третім особами, потрібно встановити відеоспостереження та тримати записи впродовж трьох місяців. Це допоможе уникнути можливої передачі даних конкурентам та отриманню значних втрат. Також требо проводити планові освітні заходи про безпеку інформації.

Існує можливість втрати інформацію методом соціальної інженерії. Цей метод використовують зовнішні порушники для отримання інформації методом психологічного тиску на робітників. Цей ризик вирішується впровадженням планових освітніх заходів, де будуть проводитися бесіди про актуальні питання

безпеки. Якщо робітник отримав такий лист з недостовірного каналу, він повинен повідомити керівнику.

Уся відеозйомка повинна перебувати на сховищі для в випадку потреби можна було пред'явити її в суді та отримати компенсацію в залежності від заподіяної шкоди.

Політика безпеки для пошуку та виявленню закладних пристроїв

Мета політики:

Встановити правила пошуку, виявленню та знищенню закладних пристроїв. Користувачі системи повинні дотримуватися вимог, що регламентуються даною політикою. Виконання вимог даної політики підвищує рівень захищеності інформаційних ресурсів, що циркулюють та обробляються на підприємстві.

Область дії:

Політика безпеки для пошуку та виявленню закладних пристроїв розповсюджуються на усіх робітників Корпорації, виявлення яких займається служба безпеки установи.

Відповідальні особи:

Відповідальною особою за політику безпеки для пошуку та виявленню закладних пристроїв начальник відділу інформаційної безпеки.

Політика безпеки:

При проведенні робіт з використанням конфіденційної інформації та експлуатації технічних засобів ІС можливі наступні канали витоку або порушення цілісності інформації або працездатності технічних засобів:

– побічні електромагнітні випромінювання інформативного сигналу від технічних засобів і ліній передачі інформації;

– акустичне випромінювання інформативного умовного сигналу або сигналу, обумовленого функціонуванням технічних засобів обробки інформації;

– несанкціонований доступ до інформації, що обробляється в автоматизованих системах;

– розкрадання технічних засобів з зберігається в них інформацією або окремих носіїв інформації;

– перегляд інформації з екранів дисплеїв і інших засобів її відображення за допомогою оптичних засобів;

– вплив на технічні або програмні засоби з метою порушення цілісності (знищення, спотворення) інформації, працездатності технічних засобів.

Найбільшу небезпеку в даний час представляють технічні засоби розвідки:

– акустична розвідка;

– розвідка побічних електромагнітних випромінювань і наведень електронних засобів обробки інформації (далі - ПЕМВН);

– в окремих ситуаціях, можуть використовуватися: телевізійна, фотографічна і візуальна оптична розвідка, що забезпечує добування інформації, що міститься в зображеннях об'єктів, що отримуються у видимому діапазоні електромагнітних хвиль з використанням телевізійної апаратури.

Крім перехоплення інформації технічними засобами розвідки можливо ненавмисне влучення конфіденційної інформації щодо осіб, які не допущеним до неї, але знаходяться в межах контрольованої зони. Витік інформації можлива за наступними каналами:

– радіоканали;

– ік-канал;

– ультразвуковий канал;

– провідні лінії.

Як провідних ліній при передачі інформації до зовнішніх засобів реєстрації можуть бути використані:

– мережі змінного струму;

– лінії телефонного зв'язку;

– радіотрансляційні і технологічні (пожежної, охоронної сигналізації, кабелі телеантен і інші) лінії;

– спеціально прокладені провідні лінії.

При застосуванні лазерної апаратури дистанційного прослуховування, що фіксує інформативні коливання скла у вікнах приміщень, можливо отримання акустичної інформації з виділених приміщень, в яких встановлені елементи системи.

В якості типових організаційних заходів, що сприятимуть захисту від перерахованих вище критичних загроз необхідно виконання наступних дій:

1. Регулярне виконання процедури резервного копіювання інформації обмеженого доступу.
2. Використання джерел безперебійного живлення.
3. Установка датчиків реєстрації ознак аварії або стихійного лиха (диму, наявності відкритого вогню).
4. Установка системи автоматичного оповіщення про аварії.
5. Контроль доступу персоналу в приміщення, що підлягає.
6. Контроль доступу персоналу до АРМ.
7. Виконання періодичних регламентних робіт з контролю функціонування АРМ.
8. Контроль графіка періодичного перегляду та аналізу протоколу роботи системи адміністратором безпеки.
9. Реєстрація актів знищення поламаних компонентів системи.
10. Залучення довіреної кваліфікованого персоналу для ремонту елементів АРМ.
11. Використання охоронної сигналізації в приміщенні, що підлягає.
12. Регулярний контроль стану захищається.
13. Регулярний аудит безпеки роботи АРМ.
14. Періодична атестація адміністратора безпеки системи.
15. Контроль доступу до системної документації на апаратно-програмні засоби і настройки.

16. Централізована підтримка і оновлення антивірусного програмного забезпечення.

17. Проведення спеціального дослідження технічних засобів і спеціальної перевірки.

18. Використання спеціальних технічних засобів зашумлення.

19. Навчання користувачів регламентам роботи з АРМ.

20. Наявність організаційно-розпорядчих заходів безпеки.

21. Використання сертифікованого програмного забезпечення.

22. Проведення кадрової роботи для підвищення мотивацій співробітників.

23. Проведення кадрової роботи для виявлення нелояльного персоналу.

Підсистема запобігання витоку інформації технічними каналами призначена для забезпечення захисту інформації при її обробці, зберіганні і передачі по каналах зв'язку, а також конфіденційної умовної інформації, що циркулює в спеціально призначених приміщеннях для проведення конфіденційних заходів (нарад, обговорень, конференцій, переговорів та інші). Вона являє собою сукупність організаційно-технічних заходів з фізичного захисту приміщень, каналів передачі інформації та технічних засобів, електромагнітної розв'язки між інформаційними ланцюгами, по яких циркулює інформація, що захищається, розв'язка ланцюгів електроживлення об'єктів захисту за допомогою мережевих перешкоджаючих та пригнічуючих фільтрів і інші заходи захисту, що вживаються відповідно до вимог та рекомендацій нормативних документів.

Передача конфіденційної умовної інформації по відкритим провідним каналам зв'язку, що виходять за межі контрольованої зони, і радіоканалах повинна бути виключена. При необхідності передачі інформації слід використовувати захищені лінії зв'язку. Використовувані засоби захисту інформації повинні бути сертифіковані за вимогами безпеки інформації.

При захисті конфіденційної цифрової інформації від витоку технічними каналами необхідно керуватися наступними вимогами:

1. Використання технічних засобів, які відповідають вимогам стандартів з електромагнітної сумісності;

2. Використання сертифікованих засобів захисту інформації;

3. Розміщення об'єктів захисту на максимально можливій відстані від кордону контрольованої зони;

4. Розміщення понижуючих трансформаторних підстанцій електроживлення і контурів заземлення об'єктів захисту в межах контрольованої зони;

5. Використання сертифікованих систем гарантованого електроживлення (джерел безперебійного живлення);

6. Розв'язка ланцюгів електроживлення об'єктів захисту за допомогою мережевих перешкоджаючих та пригнічуючих фільтрів, які блокують (пригнічують) інформативний сигнал;

7. Електромагнітна розв'язка між інформаційними ланцюгами, по яких циркулює інформація, що захищається, і лініями зв'язку, іншими ланцюгами допоміжних технічних засобів і систем, що виходять за межі контрольованої зони;

8. Використання захищених каналів зв'язку;

9. Розміщення дисплеїв і інших засобів відображення інформації, що виключає її несанкціонований перегляд;

10. Організація фізичного захисту приміщень та власне технічних засобів обробки інформації з використанням технічних засобів охорони, що запобігають або істотно ускладнюють проникнення в будівлі, приміщення сторонніх осіб, розкрадання документів і носіїв інформації, самих засобів інформатизації.

2.5 Висновки до спеціального розділу

У другому розділі було описано модель порушника, модель загроз, обрано актуальний профіль захищеності та надано перелік політик безпеки, які

допоможуть уникнути затрат зі сторони Корпорації. Завдяки впровадженню засобів покращення безпеки інформації з обмеженим доступом, буде знижено рівень ризиків на систему через виявлені ризики.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Мета техніко-економічного обґрунтування дипломної роботи

Метою виконання економічного розділу є визначення доцільності економічних витрат на запровадження засобів та заходів стосовно покращенню інформаційної безпеки Корпорації.

Необхідність надання політики безпеки було виявлено завдяки аналізу служби безпеки Корпорації «N», де було виявлено інформацію з обмеженим доступом, яка може становити інтерес стороннім особам, таким як хакери або конкуренти. Завдяки загрозам та вразливості системи порушник може отримати доступ до неї, що може призвести до несприятливих умов для ОІД.

Тому далі ми розглянемо основні проблеми, буде зроблено обґрунтування необхідності та актуальності даних проблем, виявлено очікуваний результат після впровадження даних політик безпеки.

На етапі аналізу ризиків було виявлені безпеки для котрих були надані інструкції в політиках безпеки. Згідно цього:

- використання зміни паролів для мережі Інтернет;
- опис використання, зберігання та обліку носіїв інформації;
- використання програмного забезпечення для контрою подій;
- використання системи відеоспостереження;
- впровадження системи контролю закладних пристроїв.

3.2 Визначення витрат на розробку політики безпеки інформації

Основою для визначення витрат на розробку політики безпеки є концепція сукупності вартості володіння, яку було запропоновано Gartner Group . У цій моделі враховуються наступні IT-витрати:

1. Фінансові (капітальні) витрати
2. Поточні витрати

3.2.1 Розрахунок фінансових (капітальних) витрат

Капітальні кошти – це кошти, призначені для створення і придбання довгострокових і нематеріальних активів, які є предметом амортизації.

До капітальних коштів можна віднести:

- Витрати на підготовку проекту про інформацію на підприємстві;
- Вартість залучення зовнішніх консультантів;
- Вартість початкових покупок ліцензійного та додаткового програмного забезпечення;
- Вартість створення основного і допоміжного програмного забезпечення;
- Вартість первинної покупки апаратного забезпечення;
- Вартість інтеграції системи інформаційної безпеки в існуючу систему підприємства (встановлення обладнання, програмне забезпечення та налаштування системи інформаційної безпеки);
- Витрати на навчання технічних фахівців і обслуговуючих співробітники.

Усі витрати на залучення зовнішніх консультантів, навчання працівників, інтеграцію системи захисту виділяються на підставі фактичних даних організації. Стосовно ліцензованого програмного забезпечення усі витрати вказані в прайс-листах відповідних фірм.

Вартість розробки політики безпеки для Корпорації «N» буде враховуватися за двома показниками:

1. Складність розробки
2. Вартість розробки

Визначення складності розробки політики безпеки буде визначатися:

$$t=t_{тз} + t_{об}+t_{а}+t_{вз}+t_{обз}+t_{д}, \text{ годин}, \quad (3.1)$$

Де $t_{тз}$=7 – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{об}$=15 – тривалість проведення обстеження АС підприємства;

$t_а$=10 – тривалість процесу аналізу ризиків;

$t_{вз}$=8 – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$=10 – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_д$=5 – тривалість документального оформлення політики безпеки.

Згідно цієї формули та даних зібраних в процесі:

$$t=7+15+10+8+10+5=55(год.)$$

Витрати на розробку політики безпеки($K_{рп}$) складають з витрат на оплату спеціалісту($З_{зп}$) та вартості машинного час($З_{мч}$), таким чином:

$$K_{рп}= З_{зп}+ З_{мч} (грн.), \quad (3.2)$$

$$З_{зп}= t*З_{іб}(грн.), \quad (3.3)$$

$$З_{мч}= t*С_{мч}(грн.), \quad (3.4)$$

Де $З_{іб}$ =260 – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину, t =55 – загальна тривалість розробки політики безпеки, годин, $С_{мч}$ – вартість однієї години машинного часу, грн/год.

Розрахунок плати кваліфікованому робітнику становить 10$ на годину, що перерахувавши та якщо округлити вийде 260 грн/годину. Звідси визначаємо по формулі:

$$З_{зп}=55*260=14300 (грн.)$$

Вартість 1 години машинного часу визначається за формулою:

$$С_{мч} = Р * t_{на} * С_е + \frac{Ф_{зал} * Н_а}{F_р} + \frac{К_{лпз} * Н_{апз}}{F_р}, грн, \quad (3.5)$$

Де Р=1,9кВт – встановлена потужність ПК;

$t_{нал}$=1шт. – кількість машин на яких розроблюється політика безпеки;

$С_е$=4грн/кВт·година – тариф на електричну енергію;

$Ф_{зал}$=15000грн. – залишкова вартість ПК на поточний рік;

$Н_а$=0.8 частки одиниці – річна норма амортизації на ПК;

$Н_{апз}$=0,8 частки одиниці – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$=10000грн. – вартість ліцензійного програмного забезпечення;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня 1920 год.).

$$С_{мч}=1,9*1*4+(15000*0,8)/1920+(10000*0,8)/1920=18,05 грн.$$

Отже, вартість машинного часу для розробки політики безпеки інформації на ПК становить:

$$З_{мч}=55*18,05=992,75 грн.$$

Звідси, витрати на розробку політики безпеки буде встановлювати:

$$К_{рп}=14300+992,75=15292,75 грн.$$

Витрати на розроблену таким чином політику безпеки є її частиною разових капітальних витрат разом із витратами на придбання та налагодження обладнання системи захисту інформації.

Таким чином, капітальні витрати на проектування та впровадження системи безпеки складають:

$$К= К_{пр}+К_{зпз} + К_{пр} +К_{аз}+К_{навч}+К_{н}, \quad (3.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$=13000 грн. – вартість закупівель ліцензійного основного й додаткового ПЗ, тис. грн.;

$К_{рп}$=15292,75 грн. – вартість розробки політики безпеки інформації, тис. грн.;

$К_{аз}$=3000 грн. – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн.;

$К_{навч}$=1500 грн. – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн.;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн..

$К_{пр}$ не використовується, тому що зовнішні консультанти не були задіяні. $К_{н}$ частково входить в $К_{аз}$ та $К_{зпз}$, тому також не використовується в даній формулі.

$$К=13000+15292,75+3000+1500=32792,75 \text{ грн.}$$

3.2.2 Розрахунок поточних (експлуатаційних) витрат

Операційні витрати - це поточні експлуатаційні витрати та обслуговування об’єкта протягом певного періоду, виражений у грошовому виразі.

Наступні витрати стосуватимуться цієї компанії:

– зарплата обслуговуючого персоналу;

– кваліфікаційні заходи та перевірка знань працівників стосовно правил, що регулюються політикою безпеки;

– технічне та організаційне управління та обслуговування.

Для даної Корпорації витратами будуть:

1. Заходи стосовно перевірок дотримування правил стосовно зміни паролів для мережі Інтернет;
2. Обслуговування камер спостереження;
3. Навчання персоналу знаходження та утилізація закладних пристроїв;
4. Дотримання правил стосовно носіїв інформації.

Розрахунок експлуатаційних витрат за рік на функціонування системи інформаційної безпеки за формулою:

$$C = C_з + C_{об} + C_{навч} + C_{пр} + C_{ам} + C_{ел} + C_{зп} \text{ грн.}, \quad (3.7)$$

$C_з$ =500 – перевірки дотримання правил стосовно зміни паролів;

$C_{об}$ =3000– обслуговування камер;

$C_{навч}$ =1500– навчання персоналу;

$C_{пр}$ =1000– дотримання правил стосовно носіїв інформації;

$C_{ам}$= (13000+3000)/2=8000 - річний фонд амортизаційних відрахувань;

$C_{зп}$= 3300*12 = 39 600 - додаткова заробітна плата системному адміністратору (22% від основної).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Се), визначається за формулою:

$$C_{ел} = P \cdot F_р \cdot Це , \text{ грн}, \quad (3.8)$$

де P=1,9кВт – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$=1920 год. – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$=4грн/кВт*година – тариф на електроенергію.

Оновлення придбаного програмного забезпечення не буде потрібним, так як придбаний продукт придбається назавжди.

$$С_{ел} = 1,9*4*1920=14592 \text{ грн.}$$

$$С= 500+3000+1500+1000+8000+39\ 600 +14592=68192 \text{ грн.}$$

3.3 Оцінка величини збиту

Мета цієї оцінки - визначити розмір матеріальної шкоди, ґрунтуючись на ймовірності реалізації певної загрози та можливої матеріальні втрати від неї.

Далі буде наведено можливі загрози з економічним впливом на ОІД:

1. Порушення конфіденційності інформації. Ця загроза має достатні наслідки для втрати значного капіталу Корпорації. Вона може бути порушена передачею інформації робітниками, ознайомлення даних хакерами або конкурентами.

2. Порушення доступу до ресурсів, ця загроза може бути порушена через передачу інформації через фото екранів моніторів, де відставній контроль приміщень, також несанкціонований доступ до мережі Інтернет.

3. Порушення цілісності ресурсів, порушення може виникнути при відсутності журналу подій, в якому показані усі події зв'язані з інформацією.

4. Порушення автентичності ресурсів, загроза може нести в собі легкі або одноразові паролі, які можуть бути зламані та це може стати причиною ознайомлення сторонніх осіб інформацію з обмеженим доступом.

Для розрахунку збитків від реалізації даних загроз потрібно використати формулу:

$$U=П_{п}+П_{в}+V \text{ грн.} \quad (3.9)$$

де $П_{п}$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн;

$П_в$ – вартість відновлення працездатності вузла (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

$$П_п=(З_с*Ч_с / F)*t_п , грн., \quad (3.10)$$

де Зс =540000 – загальна кількість витрат на заробітну плату співробітників за місяць, F=160 – місячний фонд робочого часу, $t_п$=5 – час простою внаслідок атак, $Ч_с$=13 – чисельність співробітників атакованого вузла або сегмента мережі, осіб.

$$П_п=(40\ 000*13/160)*5=16\ 250 грн.$$

Витрати на відновлення працездатності вузла або сегмента мережі включають кілька складових:

$$П_в= П_{ви}+ П_{пв}+ П_{зч}, \quad (3.11)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн; $П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн; $П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Вартість повторного введення інформації $П_{ви}$ розраховується на основі розміру зарплати працівників ураженого вузла чи сегменту корпоративної мережі $З_с$=540000 тими, хто зайнятий повторним введенням втраченого інформація з урахуванням необхідного часу $t_{ви}$=10:

$$П_{ви}=(Зс/ F)*t_{ви}, грн. \quad (3.12)$$

F=160 – місячний фонд робочого часу

Отже, $П_{ви}$=(540000/160)*10=33750 грн.

Витрати на відновлення системи визначаються часом відновлення після атаки $t_в$:

$$П_{пв}=(З_{са}/F)*t_в, \text{ грн.} \quad (3.13)$$

де $З_{са}$=40000 – розмір середньогодинної заробітної плати співробітника служби безпеки інформації, $t_в$=10 – час відновлення після атаки, F=160 – місячний фонд робочого часу.

$$П_{пв}=(40000/160)*10=2500 \text{ грн}$$

$П_{зч}$ не буде враховуватися, бо заміни частин не буде відбуватися. Отже,

$$П_в=33750+2500=36250 \text{ грн.}$$

Витрати від зниження працездатності атакованої системи:

$$V=O/ F_г *(t_п+t_в +t_{ви}), \quad (3.14)$$

Де, $F_г$=1920 год. – річний фонд роботи організації, $t_в$=10 – час відновлення після атаки, $t_{ви}$=10 – час затрачений на повторне введення втраченої інформації, $t_п$=5 – час простою внаслідок атак, O=10 000 000 – обсяг продажів атакованого вузла або сегменту корпоративної мережі.

$$V=10\ 000\ 000\ /1920*(5+10+10)=130208,333 \text{ грн.}$$

$$U=130208,333+16\ 250+36250=182\ 708,33 \text{ грн.}$$

Загальний збиток від атаки на ОІД:

$$B = \sum_i \sum_n U, \text{ грн.} \quad (3.15)$$

Так як спроб атак на рік проходить приблизно 3 раз на рік(розглядається не вся Корпорація, а лише служба), так як сервер знаходиться не на території ОІД, то буде розглянуто лише 13 робочих станцій, то загальний збиток буде складати:

$$B=3*13*182\ 708,33=7\ 125\ 624,99\text{грн.}$$

3.4 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи захисту інформації визначається з урахуванням ризиків порушення інформаційної безпеки є:

$$E = B \cdot R - C, \quad (3.16)$$

де, B=7 125 624,99 – загальний збиток від атаки; R=0,25 – очікувана ймовірність атаки; C=36892 – щорічні витрати на експлуатацію системи інформаційної безпеки.

Аналіз інформаційної безпеки проводиться не ріже ніж один раз у квартал, тоді R буде дорівнювати 0,25.

$$E=7\ 125\ 624,99*0,25-68192=\ 1\ 713\ 214,25\text{грн.}$$

3.5 Оцінка економічної ефективності системи захисту інформації

Якщо розглядати повний аналіз ефективності розробки політики безпеки її реалізація в об'єкті інформаційної діяльності, то повинна бути розрахована рентабельність інвестицій, а також рентабельність капіталу інвестиції.

Коефіцієнт рентабельність інвестицій ROSI показує, скільки гривень додатковий дохід приносить одне капітальне вкладення гривні на впровадження системи захисту інформації.

Для обчислення коефіцієнта ROSI необхідно знайти відношення до загального ефекту від впровадження системи захисту інформації до капіталовкладення.

$$ROSI = E/K \qquad (3.17)$$

Де, E=1 713 214,25 – загальний ефект від впровадження системи інформаційної безпеки тис. грн;

K=32792,75 – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

$$ROSI = 1\ 713\ 214{,}25/32792{,}75 = 52{,}243 \text{ частки одиниці}$$

Термін окупності капітальних інвестицій T_o показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження КСЗІ.

$$T_o = 1/ ROSI = 0{,}019 \text{ років.} \qquad (3.18)$$

Після перевірки запропонованих рішень, окупність наступить через менш ніж за рік.

3.6 Висновок до третього розділу

У цьому розділі було детально проаналізовано вартість та рентабельність впровадження політик безпеки до ОІД на основі коефіцієнту впровадження інвестицій. При одноразовому вкладенню коштів на контроль на впровадження системи, було отримано результат 52,243 (ROSI), завдяки якому можна визначити, що окупність нових впроваджених засобів можна очікувати менш ніж за рік. Максимальними витратами при з'явленні загрози будуть становити 7 125 624,99 грн.

ВИСНОВКИ

В процесі виконання кваліфікаційної роботи було розглянуто підприємство та інформацію, яка циркулює, оброблюється та зберігається на ОІД. Було обґрунтовано необхідність створення комплексної системи захисту інформації згідно з законами та нормативними документами.

Для створення КСЗІ було проведено оцінку моделей порушника та загроз, аналіз та оцінку інформаційних ризиків. Завдяки яким було виявлено місця які потребують додаткового захисту та створення політики безпеки для актуальних вразливостей системи. Окрім цього було складено потрібний стан функціонального профілю захищеності.

На основі даних, що були отримані, було розроблено комплекс рекомендацій, які підвищать рівень захисту в Корпорацій «N» та знизять шанс реалізації загроз. Опис доцільності використання та вартості даних рекомендацій було описано в економічній частині кваліфікаційної роботи.

На основі економічної частини можна зробити висновок, що впровадження політики безпеки є цілком доцільним та окупність системи дуже швидко відбудеться.

ПЕРЛІК ПОСИЛАНЬ

1 Закон України «Про інформацію» [Електронний ресурс] // 2657- XII. – 01.01.2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12

2 Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс] // 80/94-ВР. – 19.04.2014. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-вр

3 НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці» [Електронний ресурс] – 15.04.2013 – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=107993&cat_id=89734&ctime=1366373635138

4 IEC 27000 до: 2016 Information technologyI - Security techniques - Information Security Management System - Overview and Vocabulary [Електронний ресурс] – 2016 – Режим доступу до ресурсу: http://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27000-2014.pdf

5 IEC 27001 до: 2016 Information technology - Security techniques - Information security management systems - Requirements [Електронний ресурс] – 2016 – Режим доступу до ресурсу: https://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27000-2016.pdf

6 НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційнотелекомунікаційній системі» [Електронний ресурс] – 2005. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=46074&cat_id=38835

7 Віхорєв С. В. «Класифікація загроз інформаційній безпеці» [Електронний ресурс] / С. В. Віхорєв. – 2001. – Режим доступу до ресурсу: https://elvis.ru/upload/iblock/f60/f602ee2337fcc7250c71c2a138fe9ecc.pdf

8 Експлуатація систем інформаційної безпеки [Електронний ресурс] – Режим доступу: https://lektsii.org/15-1904.html

9 Організаційна структура [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Организационная_структура

10 Функції відділу інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу:
https://ru.wikipedia.org/wiki/Служба_информационной_безопасности

11 НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [Електронний ресурс] – 1999 – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.1-003-99.pdf

12 НД ТЗІ 2.5-005 -99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» – 1999 – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	32	
6	А4	2 Розділ	37	
7	А4	3 Розділ	14	
8	А4	Висновки	1	
9	А4	Список літератури	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

Керівник