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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Астафурова Романа Антоновича*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи відділення ТОВ "Ukr-Delivery"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. каф. БІТ Сафаров О.О.			
розділів:				
спеціальний	к.т.н., доц. каф. БІТ Сафаров О.О.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Астафурову Р.А.* **академічної групи** *125-17-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи відділення ТОВ "Ukr-Delivery"*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021 № 317-С

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Створення КСЗІ, кібератаки у сфері інформаційної безпеки, та нормативно-правову базу у сфері ТЗІ	03.05.2021 07.05.2021
Розділ 2	Обстеження на ОІД, аналіз ризіків, політика захисту підприємства ТОВ “Ukr-Delivery”	10.05.2021 24.05.2021
Розділ 3	Розглянуто економічну доцільність впровадження КСЗІ, та разрахунок витрат	04.06.2021 07.06.2021

Завдання видано _____ Сафаров О.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 30.04.2021р.

Дата подання до екзаменаційної комісії: 17.06.2021р.

Прийнято до виконання _____ Астафуров Р.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 65 с., 5 рис., 16 табл., 4 додатки, 11 джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система ТОВ “Ukr-Delivery”.

Предмет дослідження: комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ “Ukr-Delivery”.

Мета кваліфікаційної: підвищення ефективності інформаційної безпеки в інформаційно-телекомунікаційної системі ТОВ “ Ukr-Delivery ”.

У першому розділі розглянуто створення КСЗІ, надано загальну інформацію про компанію, в результаті проведеного дослідження виявлено які бувають кібератаки у сфері інформаційної безпеки, розглянули нормативно-правову базу у сфері ТЗІ.

У другому розділі розглянуто, обстеження на ОІД, середовище користувачів, класифікацію інформації в компанії, аналіз загроз та вразливостей, розробили політику безпеки інформації. В результаті проведеного дослідження виявлено всю структуру захисту інформації на підприємстві, та основні поняття ІТС.

В третьому розділі було розраховано доцільність впровадження КСЗІ, економічну ефективність впровадження на об’єкті інформаційної діяльності.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ОБ`ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА

РЕФЕРАТ

Пояснительная записка: 65 с., 5 рис., 16 табл., 4 приложения, 11 источников.

Объект разработки: информационно-телекоммуникационная система ООО "Ukr-Delivery".

Предмет исследования: комплексная система защиты информации информационно-телекоммуникационной системы ООО "Ukr-Delivery".

Цель квалификационной: повышение эффективности информационной безопасности в информационно-телекоммуникационной системе ООО "Ukr-Delivery".

В первой главе рассмотрено создание КСЗИ, предоставлено общую информацию о компании, в результате проведенного исследования выявлено которые бывают кибератаки в сфере информационной безопасности, рассмотрели нормативно-правовую базу в сфере ТЗИ.

Во втором разделе рассмотрены, обследование на ОИД, среду пользователей, классификацию информации в компании, анализ угроз и уязвимостей, разработали политику безопасности информации. В результате проведенного исследования выявлено всю структуру защиты информации на предприятии, и основные понятия ИТС.

В третьем разделе было рассчитано целесообразность внедрения КСЗИ, экономическую эффективность внедрения на объекте информационной деятельности.

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМ

ABSTRACT

Explanatory note: 65 pages, 5 drawings, 16 tables, 4 appendices, 11 sources.

Object of development: information and telecommunication system of Ukr-Delivery LLC.

Subject of research: complex information protection system of information and telecommunication system of Ukr-Delivery LLC.

The purpose of the qualification: to increase the effectiveness of information security in the information and telecommunications system of LLC "Ukr-Delivery".

The first section considers the creation of KSZI, provides general information about the company, as a result of the study identified cyber attacks in the field of information security, considered the regulatory framework in the field of TCI.

The second section discusses the survey on OID, the user environment, the classification of information in the company, the analysis of threats and vulnerabilities, developed information security policy. As a result of the research, the whole structure of information protection at the enterprise and the basic concepts of ITS were revealed.

In the third section, the feasibility of the implementation of KSZI, the economic efficiency of implementation at the object of information activities was calculated.

A COMPLEX SYSTEM FOR RECEIVING INFORMATION, OBJECT OF INFORMATION DIAGNOSTICITY, MODEL OF ZAGROZ, MODEL OF A GUARDIAN, INFORMATION SECURITY, INFORMATION TELECOMMUNICATION SYSTEM

СПИСОК УМОВНИХ СКОРОЧЕНЬ

КСЗІ - комплексна система захисту інформації;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

ОС - обчислювальна система;

ПЗ - програмне забезпечення;

ОІД - об’єкт інформаційної діяльності;

ІТС - інформаційно-телекомунікаційна система;

ДСТУ - державний стандарт України;

КЗЗ - комплекс засобів захисту;

ТЗІ - технічні засоби інформації.

ЗМІСТ

ВСТУП

Поняття інформаційної безпеки в сучасному світі надзвичайно широке. Воно включає в себе як контроль за непоширенням інформації, яка вважається таємною, так і міркування вчасного, повного та якісного інформування громадян про події в країні і світі, вільного доступу до різних джерел інформації - і разом із тим сприяння цілісності суспільства, підтримання його морального добробуту, захисту від несприятливих інформаційних впливів.

Необхідність побудови КСЗІ:

Відповідно до чинного законодавства України і вимог окремих нормативних документів Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та Закону України "Про захист персональних даних" обов'язковому захисту інформації підлягає: інформація, що є власністю держави, або інформація з обмеженим доступом, вимоги по захисту якої встановлені законом, в т.ч. персональні дані громадян.

Комплексна система захисту інформації – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. Організаційні заходи є обов'язковою складовою побудови будь-якої КСЗІ. Інженерно-технічні заходи здійснюються в міру необхідності.

Інформаційна безпека – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації (НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу).

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Ми живемо в епоху інформаційного суспільства, коли коп'ютери, смартфони та інші гаджети стали невід'ємною частиною життєдіяльності людини та держави. Однак, таке стрімке поширення засобів комунікації не могло пройти без наслідків. Кінець 20 – початок 21ст. позначився появою нової кіберзлочинністю. Нині боротьба з кіберзлочинністю є однією з найбільш актуальних проблем у світі. Зростаюча кількість кіберзлочинців, постійне вдосконалення інформаційних технологій і, як наслідок, поява нових можливостей для вчинення таких злочинів створюють загрозу для глобальних інформаційних мереж і суспільства загалом [2].

Кіберзлочинність є об'єктивним наслідком глобалізації інформаційних процесів і появи глобальних комп'ютерних мереж. Зі зростанням використання інформаційних технологій у різних сферах діяльності людини зростає й використання їх із метою вчинення злочинів. Поняття «кіберзлочинність» охоплює весь спектр злочинів у сфері інформаційних технологій, будь це злочини, вчинені за допомогою комп'ютерів, або злочини, предметом яких є комп'ютери, комп'ютерні мережі та інформація, яка зберігається в них [5].

1.2 Нормативна-правова база захисту інформації

Основні нормативні акти:

- концепція технічного захисту інформації в Україні. Постанова КМУ №1126 8.10.97;
- ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423;
- ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511;
- ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р.№200;

- НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

- НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

Ці нормативно-правові документі потрібні для створення комплексної системи захисту інформації.

1.3 Постановка задачі

Товариство з обмеженою відповідальністю "Ukr-Delivery" займається експрес доставкою посилок по всій території України, має велику мережу відділень. Всі відділення компанії побудовані на єдиному стандарті, тому відділення котре ми розглядаємо знаходиться за адресою вул. Велика Ковалівка, 3, м. Новомосковськ. Компанія уже 20 років на ринку України, заснування відбулося у 2001 року.

Тому ТОВ "Ukr-Delivery" розробила внутрішню базу захисту інформації для запобігання витоку інформації клієнтів та внутрішньої документації компанії.

Для створення комплексної системи захисту інформації з обмеженим доступом, вимога якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

У побудові КСЗІ можна виділити наступні етапи:

- підготовка організаційно-розпорядчої документації;
- обстеження інформаційної інфраструктури Замовника;
- розробка "Технічного завдання на створення КСЗІ";
- розробка "Плану захисту інформації";
- розробка "Технічного проекту на створення КСЗІ";
- приведення інформаційної інфраструктури Замовника у відповідність з "Технічним проектом на створення КСЗІ";
- розробка "Експлуатаційної документації на КСЗІ";

- впровадження КСЗІ;
- випробування КСЗІ;
- проведення державної експертизи КСЗІ і отримання "Атестата відповідності".

Підготовка організаційно-розпорядчої документації. Фахівці Виконавця проводять аналіз організаційно-розпорядливих документів Замовника і нормативно-правових документів в області захисту інформації, що впливають на діяльність Замовника. До організаційно-розпорядливих документів зазвичай відносяться: організаційна структура, штатний розклад, положення про відділи і посадові інструкції співробітників, пов'язаних з експлуатацією ІТС, документи, що регламентують доступ до ІТС і так далі.

За результатами проведеного аналізу Виконавець спираючись на нормативну базу, що діє в Україні, у сфері захисту інформації, готує проекти документів, які визначають організаційну складову КСЗІ (проект наказу про створення КСЗІ, проект положення про службу захисту інформації [6], проекти посадових інструкцій і процедур і ін.), які затверджуються Замовником.

Обстеження інформаційної інфраструктури замовника. Для кожної конкретної ІТС склад, структура і вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи і умовами її експлуатації. Фахівці Виконавця проводять обстеження (аудит) ІТС Замовника. Аналізується архітектура системи, її топологія і складові елементи. Визначаються типи користувачів системи, типізується інформація, що обробляється в ІТС.

За результатами виконання етапу Виконавець розробляє наступні документи:

- акт обстеження ІТС (містить опис, принципи побудови і архітектуру ІТС);
- перелік об'єктів ІТС що підлягають захисту, які затверджуються Замовником.

Розробка "Технічного завдання на створення КСЗІ". Фахівці виконавця розробляють і погоджують із замовником документ "Технічне завдання на створення КСЗІ", яке визначає всі основні вимоги до КСЗІ і можливих варіантів реалізації її складових елементів. Після узгодження "Технічного завдання на створення КСЗІ" із Замовником, документ узгоджується з контролюючим органом.

У ТЗ викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, які забезпечують безпеку інформації в процесі її обробки в обчислювальній системі ІТС, а також вимоги до організаційних, фізичних та інших заходів захисту, які реалізуються поза обчислювальною системою ІТС в доповнення до комплексу програмно-технічних засобів захисту інформації.

"Технічне завдання на створення КСЗІ" може розроблятися для вперше створюваних ІТС, а також під час модернізації вже існуючих ІТС у вигляді окремого розділу ТЗ на створення ІТС, окремого (часткового) ТЗ або доповнення до ТЗ на створення ІТС.

Розробка "Плану захисту інформації". За результатами виконання другого етапу, а саме, грунтуючись на переліку об'єктів ІТС, що підлягають захисту, Виконавець розробляє пакет документів "План захисту інформації":

- документ "Модель загроз інформації. Модель порушника";
- документ "Положення про Службу захисту інформації";
- документ "Політика безпеки інформації», які затверджуються Замовником.

Розробка "Технічного проекту на створення КСЗІ". Після узгодження "Технічного завдання на створення КСЗІ" з Контролюючим органом Виконавець розробляє пакет документів "Технічний проект на створення КСЗІ". "Технічний проект на створення КСЗІ" є комплектом документів, в який входить частина документів розроблених на попередніх етапах і ряд нових документів, в яких описано, як саме створюватиметься, експлуатуватиметься і, у разі потреби, модернізуватиметься КСЗІ. "Технічний проект на створення КСЗІ" розробляється на підставі і відповідно до "Технічного завдання на створення КСЗІ". Під час розробки проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають можливість реалізувати вимоги технічного завдання, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації. В результаті створюється комплект робочої і експлуатаційної документації, необхідної для забезпечення тестування, проведення пусконалагоджувальних робіт, випробувань та управління КСЗІ.

Приведення інформаційної інфраструктури Замовника у відповідність з "Технічним проектом на створення КСЗІ". Особливістю цього етапу є те, що на момент ухвалення рішення про створення КСЗІ вартість цього етапу є невідомою як для Замовника, так і для Виконавця. Також, зважаючи на великий можливий спектр виконання робіт, на цьому етапі існує велика вірогідність підключення до його виконання Підрядчиків.

На цьому етапі можуть виконуватися монтажні, будівельні, пусконалагоджувальні роботи, роботи, пов'язані зі встановленням необхідних технічних або криптографічних засобів захисту інформації, засобів фізичного захисту елементів ІТС (встановлюється необхідне устаткування і програмне забезпечення, засоби контролю доступу, охоронна і пожежна сигналізації) і так далі.

Розробка "Експлуатаційної документації на КСЗІ". На цьому етапі Виконавець КСЗІ створює пакет документів "Експлуатаційна документація на КСЗІ", який включає:

- інструкції експлуатації КСЗІ і її елементів;
- процедури регламентного обслуговування КСЗІ;
- правила і положення по проведенню тестування і аналізу роботи КСЗІ;
- керівництво адміністраторів і користувачів;
- формуляр КСЗІ ІТС.

Впровадження КСЗІ. На цьому етапі Виконавець (або Підрядчик під наглядом Виконавця) проводить всі пусконалагоджувальні роботи, навчає і інструктує персонал Замовника правилам і режимам експлуатації КСЗІ.

Включає такі заходи:

- організація захисту інформації від несанкціонованого доступу (НСД);
- організація антивірусного захисту інформації;
- розробку програми і методики попередніх випробувань;
- проведення попередніх випробувань.

Після реалізації цього етапу упроваджена КСЗІ готова до подальшого випробування.

Випробування КСЗІ. На цьому етапі Замовник при активній підтримці Виконавця проводить попередні випробування КСЗІ, з метою підтвердження результативності її роботи і відповідності положенням, визначеним в "Технічному завданні на створення КСЗІ". В процесі випробувань виконуються тестові завдання і контролюються отримані результати, які і є індикатором працездатності спроектованої КСЗІ.

По результату випробування КСЗІ робиться вивід відносно можливості представлення КСЗІ на державну експертизу. Під час попередніх випробувань перевіряються працездатність КСЗІ і відповідність її вимогам ТЗ [5].

Під час дослідної експлуатації:

- відпрацьовують технології обробки інформації, облік машинних носіїв інформації, управління засобами захисту, розмежування доступу користувачів до ресурсів ІТС і автоматизованого контролю за діями користувачів;

- співробітники служби захисту інформації і користувачі ІТС набувають практичних навиків по використанню технічних і програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних і розпорядливих документів по питаннях розмежування доступу до технічних засобів і інформаційних ресурсів;

- здійснюється (за потреби) доопрацювання програмного забезпечення, додаткове налагодження і конфігурація комплексу засобів захисту інформації від несанкціонованого доступу;

- здійснюється (за потреби) коректування робочої і експлуатаційної документації.

За результатами дослідної експлуатації приймається рішення про готовність КСЗІ в ІТС до подання на державну експертизу.

Проведення державної експертизи КСЗІ і отримання "Атестата відповідності" складається з:

- підготовка КСЗІ до проведення державної експертизи в Адміністрації Держспецзв'язку і супроводі експертних випробувань;

- узгодження з Адміністрацією Держспецзв'язку результатів експертизи і видача Замовникові Атестата відповідності.

Державна експертиза проводиться з метою визначення відповідності КСЗІ "Технічному завданню на створення КСЗІ", вимогам нормативної документації після захисту інформації і визначення можливості введення КСЗІ на ІТС в експлуатацію.

1.4 Висновки до першого розділу

У даному розділі було розглянуто кібератаки у сфері інформаційної безпеки, методи захисту інформації, нормативно-правову базу у сфері ТЗІ, зроблено аналіз нормативно-правових документів в сфері захисту інформації та побудову КСЗІ. Здійснено опис загального стану розвитку загроз інформаційної безпеки компанії.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство ТОВ “Ukr-Delivery”

ТОВ “Ukr-Delivery” діяльність якої – експрес доставка посилок по всій території України. Компанія має мережу відділень, на яких видає та відправляє посилки клієнтів.

Характеристики об’єкту:

Об'єкт інформаційної діяльності розташований на 1 поверховому орендованому будинку за адресою Україна, м. Новомосковськ вул. Велика. Ковалівка 2б.

Форма власності: оренда.

Час роботи:

Понеділок – п’ятниця: (08.00 – 19.00)

Субота: (09.00 – 18.00)

Неділя: (10.00 – 18.00)

Штат відділення ТОВ “Ukr-Delivery” котрого ми розглядаємо:

Керівник відділення – 1 особа

Оператор відділення – 3 особи

Адміністратор – 2 особи

Приймальник відділення – 1 особа

Режим КЗ забезпечується таким чином:

- у робочий час забезпечується охоронної організації та системою сигналізації. Працівники відділення мають тривожну кнопку, яка застосовується для виклику охорони;

- у неробочий час забезпечується силами охорони з використанням засобів відеоспостереження, грати на вікнах, вхідними металопластиковими дверями, які закриваються на ключ. Також застосовується автономна сигналізація всього приміщення, яка підключена до пристрою, який знаходяться біля входу в приміщення.

Сигналізація КЗ входить до всього приміщення.

Стіни будинку цегляні.

Територія навколо будинку не огороджена, асфальтована, є місця для парковки машин. Інформація про навколишні будинки та споруди (таблиця 2.1).

До даного будинку підключені наступні комунікації які вказані на:

- електропостачання - від трансформаторної підстанції через підземні комунікації до розподільного щитка, який розташований на стіні всередині будинку біля входу до приміщення;

- каналізація та водооснащення - підключені до міських магістралей та заходять до підвального приміщення даного будинку;

- схема заземлення зображена на Ситуаційному плані (рисунок 2.1);

- заземлення іде від трансформаторної підстанції до розподільного щита. Безпосередньо у приміщенні заземлення немає;

- КЗ розташована в орендованому будинку, комунікації, а саме лінія електропостачання та лінія комп'ютерної мережі. Комунікації виходять за межі КЗ.

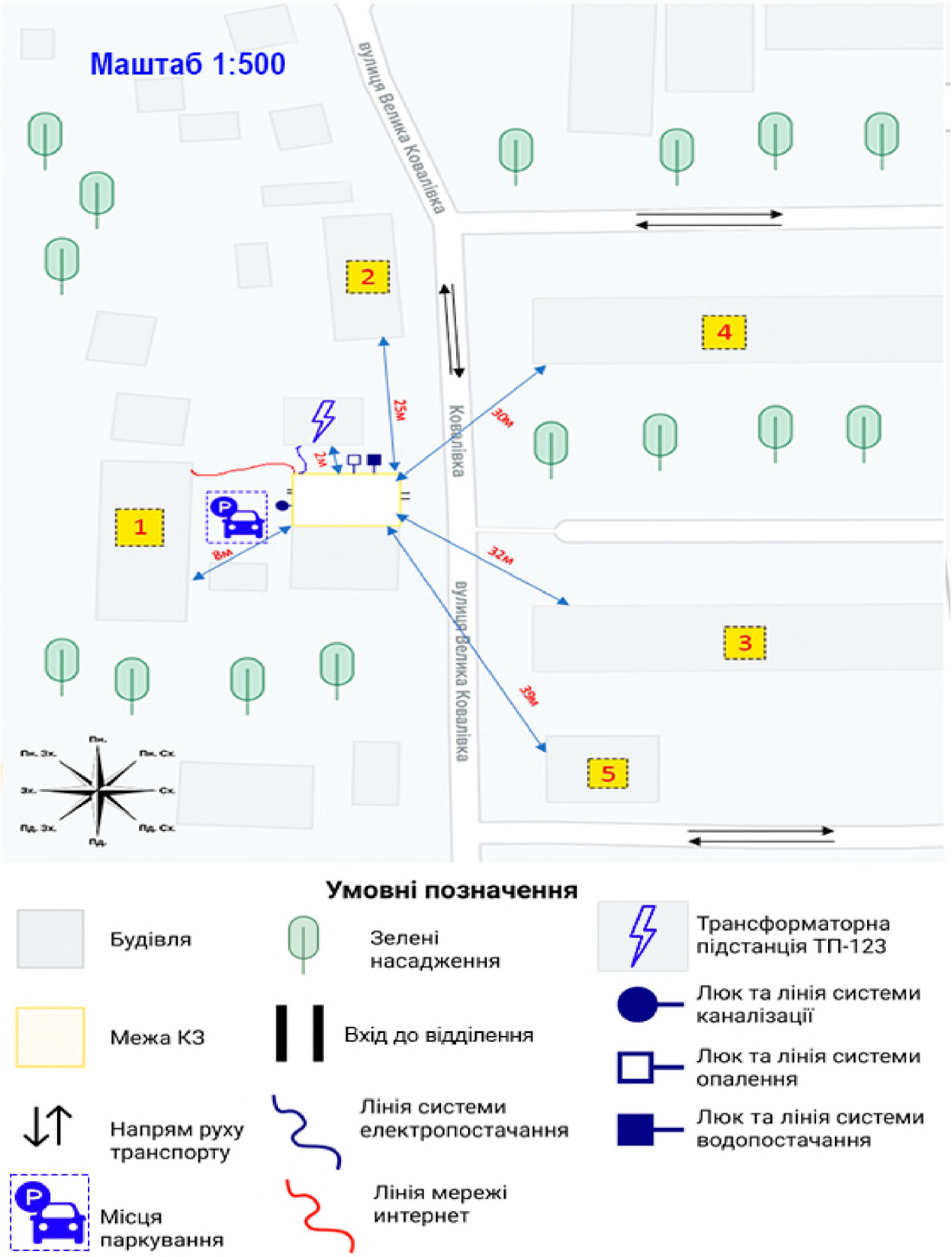

Рисунок 2.1 - Ситуаційний план ОІД (масштаб 1:500)

Таблиця 2.1 - Характеристика будівель

Найменування	К-ть поверхів	Адреса	Відстань до КЗ, м
Лікарня	5	вул. Велика Ковалівка, 1	8
Торговий центр	2	вул. Велика Ковалівка, 2	25
Трансформаторна підстанція ТП-104	1	біля приміщення КЗ	2
Житловий будинок	9	вул. Велика Ковалівка,10а	32
Житловий будинок	5	вул. Велика Ковалівка, 5	39

Характеристики будівлі:

- площа: 29м^2;
- висота стелі: 3м.;
- стеля: (матеріал – бетон, товщина – 0.6м.), в стелю вбудована вентиляція;
- підлога: (матеріал – бетон та кахель, товщина 0.5м.);
- стіни: (матеріал – цегла та покрита шпаклівкою, товщина 0,5м);
- вікна: (кількість 4шт, матеріал ПВХ.), вікна виходять на паркувальні місця біля будівлі;
- сектор прямої видимості – ближні жилі будинки;
- територія навколо будівлі – відкрита.

Комунікація будівлі:

- лінія електропостачання (рисунок 2.3), іде від трансформаторної підстанції ТП-123, місце знаходження за межами КЗ;

- каналізація та водооснащення - підключені до міських магістралей та заходять до підвального приміщення даного будинку;
- інтернет – інтернет провайдер “Фрегат телеком” (рисунок 2.4);
- кондиціонування – COOPER&HUNTER PRIMA PLUS CH-S09XN7 x2;
- система сигналізації – Складається з датчиків руху та відеокамер;
- обслуговування через охорону фірму “Бест”, охоронне обладнання (Дунай-4L).

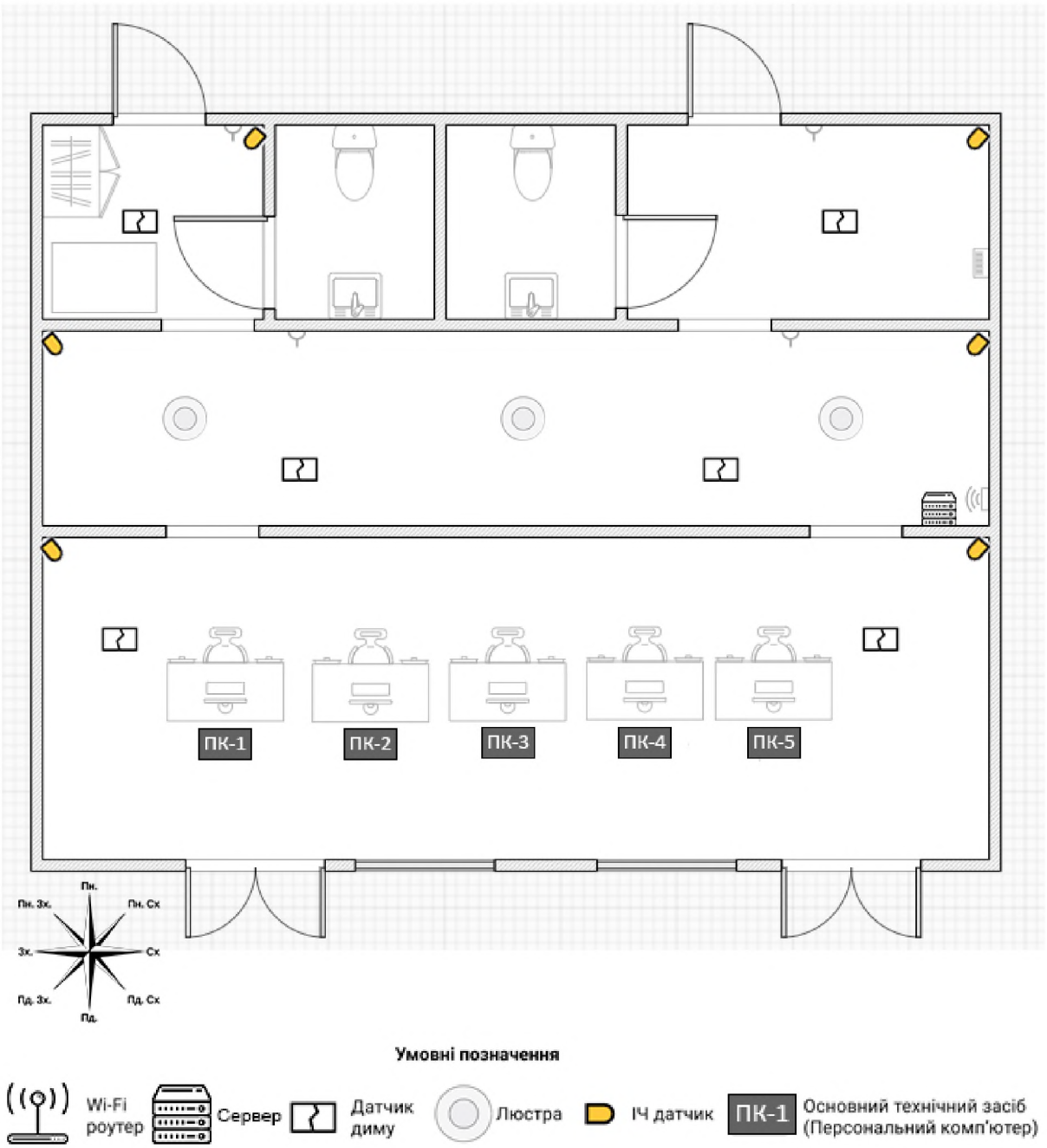

Рисунок 2.2 - Генеральный план відділення

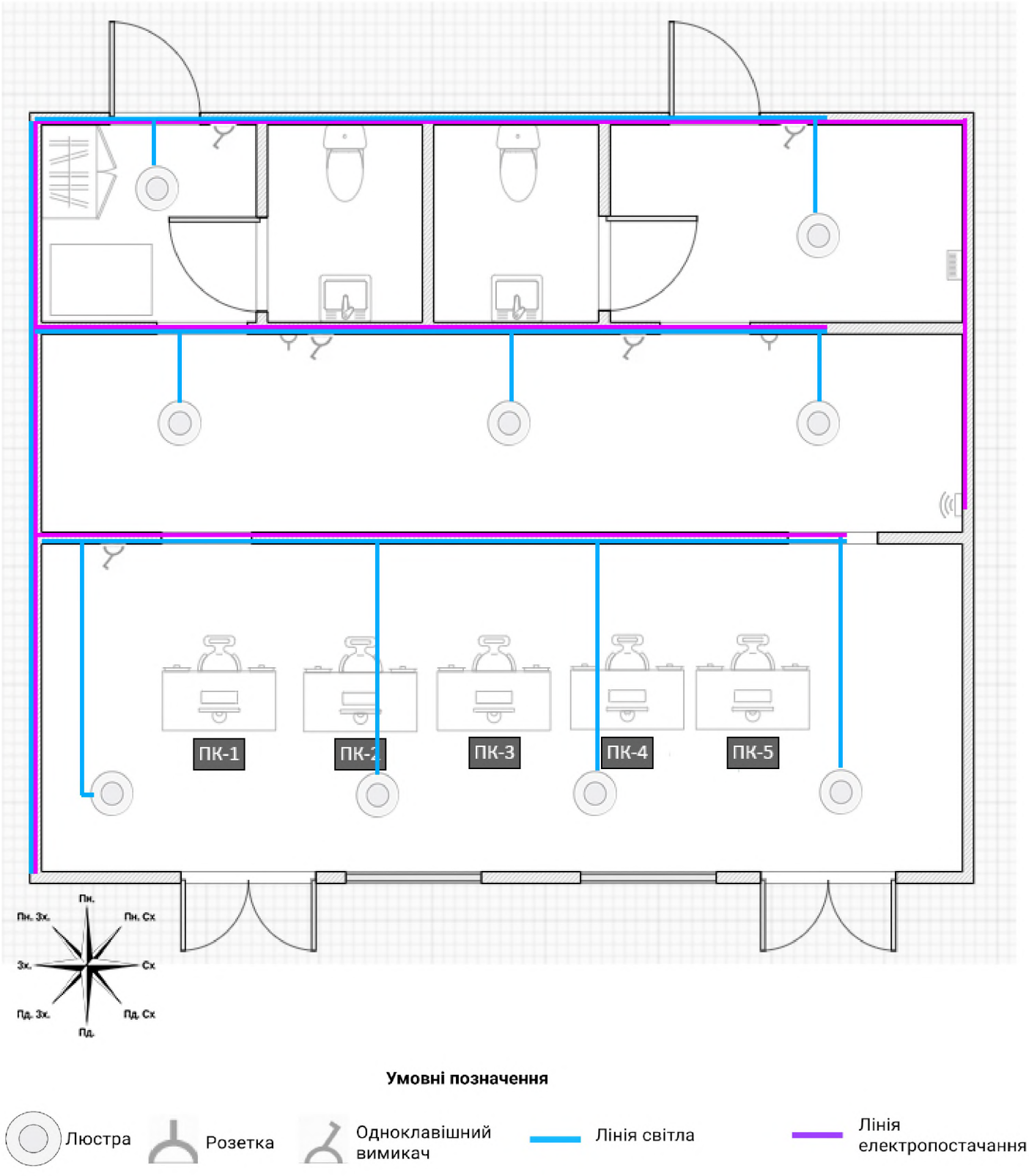

Рисунок 2.3 - Генеральный план відділення. Система електропостачання та освітлення

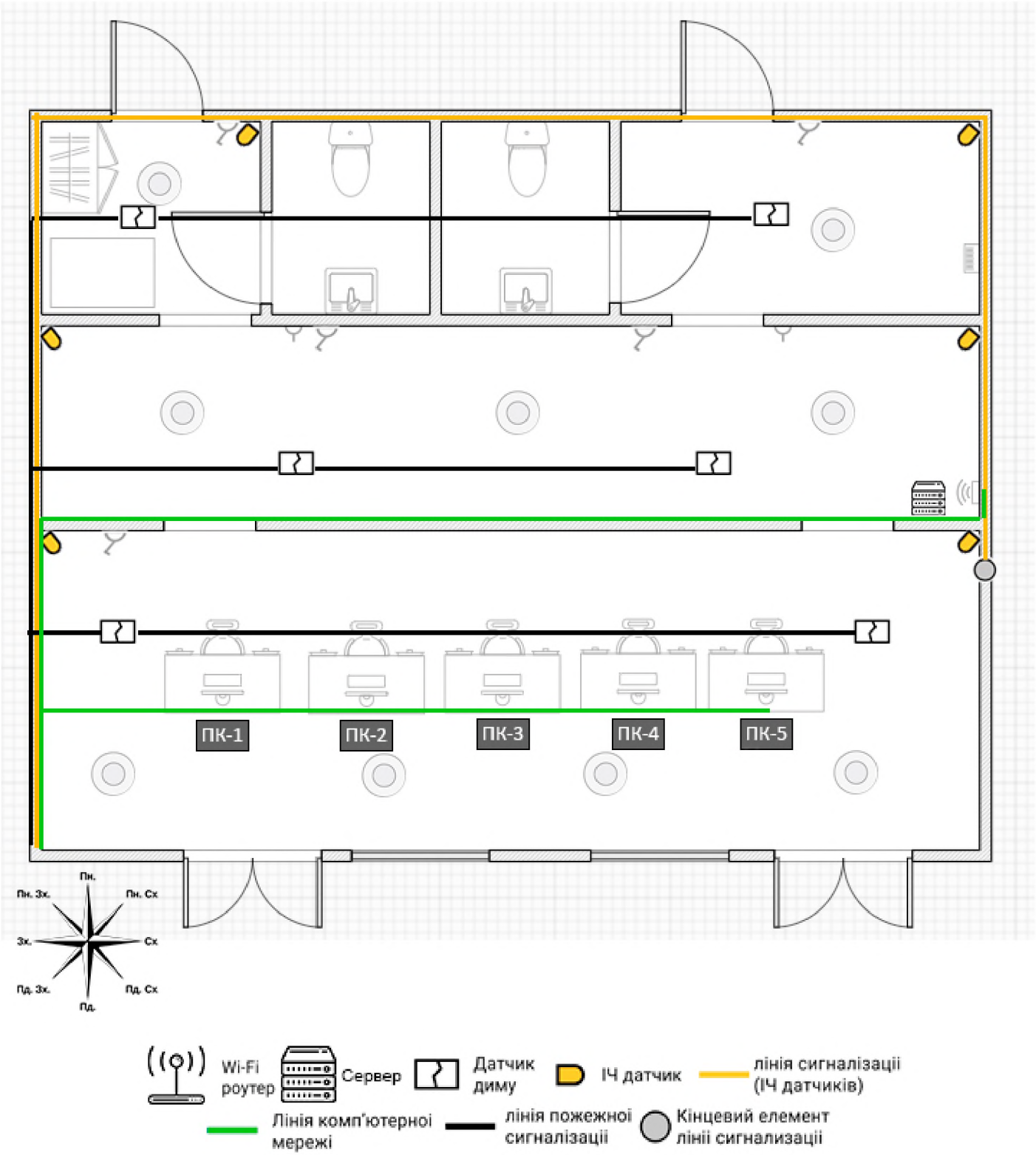

Рисунок 2.4 - Генеральный план відділення. Схеми ліній комп'ютерної мережі, системи сигналізації та системи опалення

Серед основних технічних засобів виділяються наступні: комп'ютери, роутер, комутатор, сервер (таблиця 2.2).

Серед допоміжних технічних засобів слід виділити сповіщувачі диму, інфрачервоні сповіщувачі (таблиця 2.3).

Таблиця 2.2 - Перелік ОТЗ

Номер на рисунку	Назва	Марка	Модель	Розміщення
ПК-1	Портативний комп'ютер	Lenovo	MiniPC	На столі
ПК-2	Портативний комп'ютер	Lenovo	MiniPC	На столі
ПК-3	Портативний комп'ютер	Lenovo	MiniPC	На столі
ПК-4	Портативний комп'ютер	Lenovo	MiniPC	На столі
ПК-5	Портативний комп'ютер	Lenovo	MiniPC	На столі
Wi-Fi роутер	Wi-Fi роутер	Cisco	AIR-LAP1142N-E-K9	На стіні
Комутатор	Комутатор	TP-LINK	TL-SF1016	В сервері

Таблиця 2.3 - Перелік ДТЗ

Назва	Модель	Розміщення
Датчик диму (6)	Артон Спд-3.4	на стелі
ІЧ датчик (6)	Crow Swan PGB	на стіні

2.2 Обстеження ОС

Під час роботи відділення циркулює інформація з обмеженим доступом, у кожного робітника свій доступ до інформації [4], котра регламентована політикою безпеки компанії.

На відділенні стоїть сервер котрий дає доступ до бази даних компанії кожному робочому місцю, через комутатор.

Кожний робітник має доступ доступ до певної інформації, у кожній вакансії є свої права та обмеження.

Для обміну інформацією між робітниками є корпаративна почта, доступ до якої може бути тільки на робочому місці робітника.

Характеристики системи (таблиця 2.4).

Таблиця 2.4 - Перелік та склад обладнання

Специфікація	Назва в системі
CPU: 3,7 GHz 2-Core Intel Pentium Gold G5400 | 4GB 2400 MHz DDR4 | 250GB HDD | Видеокарта: Intel Graphics	ПК-1
CPU: 3,7 GHz 2-Core Intel Pentium Gold G5400 | 4GB 2400 MHz DDR4 | 250GB HDD | Видеокарта: Intel Graphics	ПК-2

Продовження таблиці 2.4

CPU: 3,7 GHz 2-Core Intel Pentium Gold G5400 | 4GB 2400 MHz DDR4 | 250GB HDD | Видеокарта: Intel Graphics	ПК-3
CPU: 3,7 GHz 2-Core Intel Pentium Gold G5400 | 4GB 2400 MHz DDR4 | 250GB HDD | Видеокарта: Intel Graphics	ПК-4
CPU: 3,7 GHz 2-Core Intel Pentium Gold G5400 | 4GB 2400 MHz DDR4 | 250GB HDD | Видеокарта: Intel Graphics	ПК-5

2.2.1 Особливості внутрішнього серверу та доступу до нього

Мережа складається з 5 комп'ютерів, які підключені до мережі інтернет за допомогою оптики від локального серверу, котрий підключен к головному серверу компанії (рисунок 2.5). Доступ по оптиці захищен сервером.

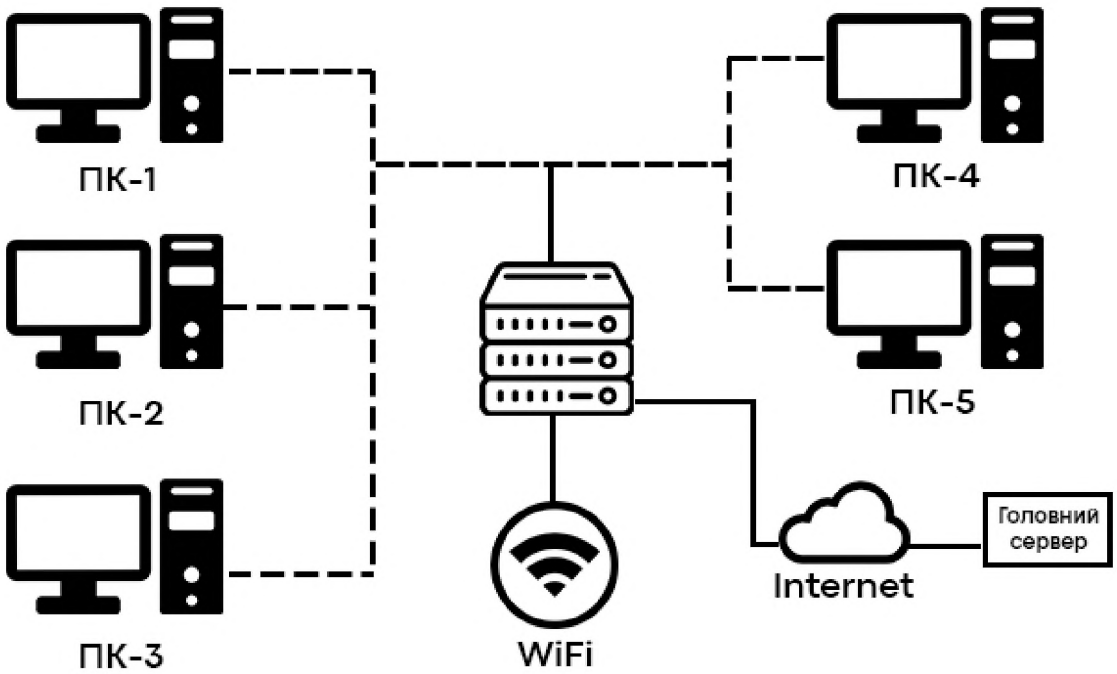

Рисунок 2.5 - Структурна схема мережі

2.3 Обстеження інформаційного середовища

Обстеження інформаційного середовища це інформація, що планується для обробки за допомогою ІТС. Власником інформації являється компанія. В системі не присутня таємна інформація або власність держави, яка становить державну таєницю.

Обмін інформацією може відбуватися за допомогою електроної пошти. Основна інформація компанії на відділенні, яка церкулює на ОІД (таблиця 2.5). Також вказаний режим доступу та критерії конфедеційності, класифікація доступу до інформації (таблиця 2.6).

Таблиця 2.5 - Класифікація інформації

Вид інформації	Режим доступу	Правовий режим	К	Ц	Д
Документи компанії	З обмеженим доступом	Конфедеційна	1	2	2
База даних клієнтів	З обмеженим доступом	Конфедеційна	1	1	2
Документи транспортування посилок	З обмеженим доступом	Конфедеційна	3	2	1
База даних робітників	З обмеженим доступом	Конфедеційна	1	2	3

Таблиця 2.6 - Класифікація доступу до інформації

Назва	Н1	Н2	Н3
Конфедеційність	Максимальне забезпечання конфедеційності інформації (К1)	Середній рівень забезпечення конфедеційності (К2)	Мінімальний рівень конфедеційності (К3)

Продовження таблиці 2.6

Цілісність	Максимальне забезпечання цілістності інформації (Ц1)	Середній рівень забезпечення цілістності (Ц2)	Мінімальний рівень цілістності (Ц3)
Доступність	Максимальне забезпечання Доступністі інформації (Д1)	Середній рівень забезпечення Доступністі (Д2)	Мінімальний рівень Доступністі (Д3)

2.4 Аналіз технології обробітку інформації “Документи компанії”

Документи компанії створюються по за межами відділення і зберігаються на внутрішньому сервері компанії, доступ здійснюється через внутрішній портал компанії, для ознайомлення та навчання нового робітника відділення.

Документи поділяються на такі види як:

- кадрові документи робітника;
- постанови нових правил компанії;
- правила пакування та палетування посилок;
- документи для клієнтів такі як (претензія, акт приймання-передачі, повернення коштів);
- маршрутні листи.

Заповнення кадрових документів: друкується макет вже готового документу, для заповнення робітником та віддається керівнику відділення на підпис. Потім керівник відділення відправляє по внутрішній пошті в відділ кадрів для опрацювання заяви.

Постанови нових правил компанії: це оновлення правил самої компанії, інформація знаходиться на внутрішньому порталі для вивчення працівниками.

Правила пакування та палетування посилок:

Вантаж поділяється на такі категорії як :

- дрібні відправлення (ДВ);

- посилка (П);
- особливі відправлення (ОВ).

Для кожної категорії є своє пакування, для запобігання пошкодження посилок.

Документи для клієнтів: це документи котрі, використовуються для компенсації клієнту, якщо його посилка зникла або приїхала пошкоджена.

Маршрутні листи: це документація котра створюється для водія, в котрій вказано кількість завантажених посилок та місце прибуття вантажівки.

2.5 Програмне забезпечення

Робота з програмним забезпеченням:

- завантаження програмного забезпечення, що не належить компанії та захищена авторським правом, використовуючи інтернет, заборонено з причини безпеки і правових наслідків;
- користувачі несуть відповідальність за отримання ліцензії та дозволи від власника авторських прав на використання та/або розповсюдження захищених авторським правом матеріали;
- користувачі не повинні умисно задійснювати пошук особитої інформації, отримувати копії ПЗ, файлів, даних або паролів, які належать інтернет-користувачам, або представляти себе за іншу особу;
- користувачі повинні поважати цілісність інформації інших користувачів;
- користувачі не повинні умисно змінювати або видаляти ПЗ, файли, дані або паролі інших користувачів, якщо це прямо не дозволено цими користувачами;
- на всіх комп'ютерах компанії встановлена операційна система (Ubuntu v16.04) котру змінили під простір компанії вказано в (Таблиці 2.7), для авторизації у систему треба мати обліковий запис робітника;
- робочий простір здійснюється через сайт AWIZ, в котрому є доступ до бази даних, він працює тільки на комп'ютерах компанії, на цьому сайті відбувається оформлення посилок та видача посилок, ще інформація перебування посилки.

Таблиця 2.7 - Інформація о ПЗ

ПО	Версія	Де встановлено	Ліцензія
Ubuntu	16.04(dev UkrDelivery)	ПК-1	Безкоштовна
Ubuntu	16.04(dev UkrDelivery)	ПК-2	Безкоштовна
Ubuntu	16.04(dev UkrDelivery)	ПК-3	Безкоштовна
Ubuntu	16.04(dev UkrDelivery)	ПК-4	Безкоштовна
Ubuntu	16.04(dev UkrDelivery)	ПК-5	Безкоштовна

2.6 Середовище користувачів

Штат робітників відділення (таблиця 2.8), та правила доступу (таблиці 2.9).

Таблиця 2.8 - Середовище користувачів

Посада	Рівень кваліфікації користувача	Час роботи
Оператор відділення	Середній	8.00-19.00
Оператор відділення	Початківець	8.00-14.00
Оператор відділення	Досвідчений	10.00-19.00
Адміністратор	Початківець	10.00-14.00
Адміністратор	Середній	10.00-18.00
Приймальний відділення	Досвідчений	10.00-19.00
Керівник відділення	Досвідчений	10.00-19.00

Таблиця 2.9 - Правила доступу

Посада	Доступ	Рівень доступу	Обладнання
Оператор відділення	До клієнтської бази та всієї документацій	Оформлення та видача посилок.	PC-1
Оператор відділення 2	До клієнтської бази та всієї документацій	Оформлення та видача посилок.	PC-2

Продовження таблиці 2.9

Оператор відділення 3	До клієнтської бази та всієї документацій	Оформлення та видача посилок.	РС-3
Адміністратор	До клієнтської бази та всієї документацій	Видача посилок та допомога операторам відділення	Мобільний телефон з додатком AWIZ
Адміністратор	До клієнтської бази та всієї документацій	Видача посилок та допомога операторам відділення	Мобільний телефон з додатком AWIZ
Приймальник відділення	До клієнтської бази и бази транспортування	Вивантаження, завантаження авто, та контроль повної кількості, цілісності посилок	РС-4
Керівник відділення	До всього	Управління персоналом, контроль показника якості відділення, та навчання персоналу	РС-5

2.7 Аналіз загроз та вразливостей

2.7.1 Модель порушника

Модель порушника – це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії тощо. Як порушник розглядається особа, яка може одержати несанкціонований доступ [10].

Модель порушника розробляється для того, щоб отримати відповіді на наступні питання:

- від кого захищати інформацію;
- яка мета порушника;
- якими знаннями володіє порушник;
- які повноваження в системі має потенційний порушник;
- якими методами і засобами користується порушник;
- яка обізнаність порушника щодо об'єкта інформаційної діяльності і системи охорони.

Інформація – відомості про об'єкти та явища навколишнього середовища, їхні параметри, властивості й стани, які зменшують наявну про них ступінь невизначеності, неповноти знань.

Модель порушника представляє собою опис можливих дій порушника, який складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Порушників прийнято поділяти на зовнішніх і внутрішніх. До внутрішніх належать співробітники, користувачі інформаційної системи, які можуть наносити шкоду інформаційним ресурсам як ненавмисно, так і навмисно; технічний персонал, який обслуговує будівлі і приміщення (електрики, сантехніки, прибиральниці тощо); персонал, який обслуговує технічні засоби (інженери, техніки). Зовнішні порушники - це сторонні особи, які знаходяться поза контрольованою зоною організації або не авторизовані для використання даної комп'ютерної системи. Це означає, що вони не мають в системі облікового запису і згідно системної політики безпеки взагалі не можуть

працювати в даній системі. Приклад зовнішніх порушників: відвідувачі, які можуть завдати шкоди навмисно або через незнання існуючих обмежень; кваліфіковані хакери; особи, яких найняли конкуренти для отримання необхідної інформації; порушники пропускного режиму.

При розробці моделі порушника необхідно визначитись, що і у якій мірі має відображати отримана модель. Для цього необхідно визначитись з необхідним ступенем деталізації моделі порушника.

Можна запропонувати наступні ступені деталізації:

- змістовна модель порушників - відображає причини й мотивацію дій порушників, переслідувані ними цілі і загальний характер дій у процесі підготовки і здійснення порушення інформаційної безпеки. Побудувавши змістовну модель, адміністратори безпеки можуть визначити мету порушника, його рівень знань, кваліфікацію, розташування;

- сценарії впливу порушників - визначають класифіковані типи порушень з конкретизацією алгоритмів і етапів, а також способи дії на кожному етапі. Розробивши сценарії впливу, адміністратори безпеки отримають можливу послідовність дій зловмисника для нанесення збитків інформаційним ресурсам;

- математична модель впливу порушників представляє собою формалізований опис сценаріїв у вигляді логіко-алгоритмічної послідовності дій порушників, кількісних значень, що параметрично характеризують результати дій, і функціональних (аналітичних, числових чи алгоритмічних) залежностей, які описують процеси взаємодії порушників з елементами об'єкту і системи охорони. Цей вид моделі слід використовувати для кількісних оцінок вразливості об'єкту і ефективності охорони.

Для того, щоб модель порушника найбільш точно і детально характеризувала порушників, алгоритм їх дій і давала кількісні оцінки вразливості об'єкту і ефективності охорони рекомендується розробляти комплексну модель з урахуванням усіх ступенів деталізації.

Способи класифікацій порушників:

- під час побудови моделі порушника спочатку необхідно проаналізувати усіх користувачів системи, розподілити їх за категоріями та визначити найбільш критичні. Користувачі таких категорій будуть прийняті як можливі внутрішні порушники системи. Далі необхідно визначитись, які категорії відвідувачів можуть бути зовнішніми порушниками;

- усіх можливих порушників необхідно класифікувати за різними показниками для того, щоб надалі скласти модель порушника.

Нижче наведені можливі види класифікацій:

- класифікація порушників інформаційної безпеки за метою порушення. Класифікація за метою порушення проводиться для визначення мотивів порушника. Дії порушника в залежності від мети можуть бути спрямовані як на інформацію, так і на матеріальні носії інформації. Знаючи мету порушника, адміністратори безпеки будуть орієнтуватись, на захист якого ресурсу необхідно приділити більше уваги першочергово;

- класифікація порушників інформаційної безпеки за рівнем знань про автоматизовані системи. Кожен порушник має певний рівень кваліфікації та поінформованості відносно організації функціонування лабораторії зовнішніх та внутрішніх мереж інформаційного комп'ютерного комплексу. В залежності від рівня знань, якими володіє порушник, може бути нанесений певний рівень збитків інформаційним ресурсам організації. В класифікації враховуються знання можливого порушника та його практичні навички у роботі з комп'ютерними системами та інформаційними технологіями;

- класифікація порушника за місцем дії. Ця класифікація проводиться для визначення розташування порушника відносно організації під час здійснення спроби несанкціонованого доступу до інформаційного ресурсу;

- класифікація порушників за методами і способами, якими вони користуються. Порушник може отримати конфіденційну інформацію та інформацію з обмеженим доступом, користуючись при цьому різними методами та засобами. Порушення може бути скоєне або з використанням певних засобів для отримання

інформації, або без них. Методи можуть бути різними, як дозволеними, так і забороненими. Дозволеним вважається отримання інформації без порушення прав власності. Як приклад можна привести використання методів соціальної інженерії;

- класифікація порушників за рівнем можливостей, які надані їм засобами автоматизованої системи та обчислювальної техніки. Внутрішніх порушників можна класифікувати за наданим рівнем повноважень у системі. Адже чим більше повноважень, там більше можливостей доступу до інформації з обмеженим доступом [3];

- класифікація порушників за мотивом порушень. Зловмисники можуть порушувати інформаційну безпеку з різних причин. Порушення можна розбити на дві групи - навмисні та ненавмисні. Особи, які ненавмисно наносять збитків інформаційним ресурсам, порушуючи конфіденційність, цілісність або доступність інформації [1], не складають плану дій, не мають мети та спеціальних методів та засобів реалізації запланованого порушення. Ненавмисні порушення частіше всього здійснюються в результаті недостатньої кваліфікації, неуважності персоналу. Порушники, які наносять збитків інформаційним ресурсам навмисно, мають певну мету, готують план реалізації атаки на інформаційний ресурс. Навмисні порушення інформаційної безпеки здійснюються для нанесення збитків організації (матеріальних чи моральних), для власного збагачення за рахунок отриманої інформації, а також для нейтралізації конкурентів.

Майже в кожній інформаційній системі знайдеться така інформація, розголошення якої стороннім особам може нанести збитків її власнику або ж людині, якої стосується інформація. Особливо актуальним стає питання інформаційної безпеки на підприємствах, організаціях, які займаються обробкою інформації з обмеженим доступом. Одним з етапів побудови комплексної системи захисту інформації є розробка моделі порушника. Чим точніше буде визначено образ, алгоритм дій ймовірного порушника, тим простіше буде адміністраторам безпеки розробити комплекс заходів для того, щоб запобігти успішним атакам. Важливу роль в розробці моделі порушника грає вибір класифікацій порушників. Отже, для найбільш точного визначення можливих порушників, збитки від яких будуть

максимальними, необхідно класифікувати всі типи суб'єктів, які мають потенційну можливість взаємодії з інформаційними ресурсами за всіма можливими для системи показниками, що суттєво спростить процедуру організації ефективної системи інформаційної безпеки.

Таблиця 2.10 - Категорії порушників

Позначення	Визначення категорії	Рівень загроз
Внутрішні по відношенню до ІТС		
ПВ1	Технічний персонал (електрики, прибиральники тощо), який обслуговує приміщення в яких розташовані компоненти ІТС	1
ПВ2	Приймальники відділення	2
ПВ3	Оператори відділення	2
ПВ4	Керівник відділення	4
Зовнішні по відношенню до ІТС		
П30	Відвідувачі	1
П31	Комунальні служби	2
П32	Хакери	3

Таблиця 2.11 - Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність, помилка	1
М2	Самоствердження	1
М3	Корисний інтерес	1

Таблиця 2.12 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Мотив порушення	Рівень загроз
К1	Низький рівень знань, вміння працювати з компонентами ІТС	1
К2	Середній рівень знань, має практичний досвід з роботи з компонентами ІТС та їх обслуговування	2
К3	Високий рівень знань, вміння у галузі програмування, та експлуатації ІТС	4

Таблиця 2.13 - Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту (обізнаність щодо використання технічних засобів розвідки)

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Підглядання за робочим процесом	1
З2	Взлом, підбір паролю до облікових записів	2
Специфікація моделі порушника за часом дії		
Ч1	Під час призупинення використання компонентами ІТС (залишити ноутбук в офісі та піти)	2
Ч2	Під час ремонту компонентів ІТС	1
Ч3	Під час роботи компонентів ІТС	1
Ч4	У будь-який час, маючи доступ до інформації у хмарному сховищі (до обл. зап.)	2
Специфікація моделі порушника за місцем дії		
МД1	Робочі місця робітників	2
МД2	У приміщенні, де розташовані ІТС	2
МД3	У будь-якому місці, маючи доступ до інформації у хмарному сховищі (до обл. зап.)	2

Таблиця 2.14 - Модель порушника (зовнішнього та внутрішнього)

Посада	Кат. пор.	Мотив поруш.	Можливості	Рів.обіз. ІТС	Час	Місце	Сума загроз
Оператор відділення	ПВ3	М1	З2	К2	Ч3	МД1	10
	2	1	2	2	1	2	
Керівник відділення	ПВ4	М1	32	К2	Ч3	МД1	12
	4	1	2	2	1	2	
Технічний персонал	ПЗ1	М3	31	К1	Ч3	МД2	6
	1	1	1	1	1	2	
Приймальник відділення	ПЗ1	М3	31	К1	Ч3	МД2	8
	1	1	1	1	1	2	
Відвідувачі	П30	М3	31	К1	Ч1	МД2	8
	1	1	1	1	2	2	
Комунальні служби	ПЗ1	М3	31	К1	Ч3	МД2	7
	1	1	1	1	1	2	
Хакери	П32	М3	З2	К3	Ч4	МД3	14
	3	1	2	4	2	2	

Висновок: найбільшу загрозу представляють хакери та внутрішні робітники організації, а саме керівник відділення, оператори відділення, оскільки вони мають безпосередній доступ до системи ІТС та працюють з її компонентами. Тому їм слід більш уважно ставитись до роботи.

2.7.2 Модель загроз

Методика розроблення такої моделі полягає в тому, що в один із стовпчиків таблиці заноситься по можливості повний перелік видів загроз. Надалі для кожної із можливих загроз шляхом їх аналізу (можливо і методом експертних оцінок) необхідно визначити:

- ймовірність виникнення таких загроз. Перший крок визначення такої ймовірності можна використати її якісні оцінки. В таблиці можуть бути наведені якісні оцінки їх ймовірності - неприпустимо висока, дуже висока, висока, значна, середня, низька, знехтувано низька;

- на порушення яких функціональних властивостей захищеності інформації вона спрямована (порушення конфіденційності - к, цілісності - ц, доступності - д); [8]

- можливий (такий, що очікується) рівень шкоди. Приклад цієї оцінки наведено також за якісною шкалою (відсутня, низька, середня, висока, неприпустимо висока). Наявність таких оцінок, навіть за якісною шкалою, дозволяє обґрунтувати необхідність забезпечення засобами захисту кожної з властивостей захищеності інформації;

- механізми реалізації (можливі шляхи здійснення) загроз;

- наявність такої інформації дозволяє побудувати більш предметну загальну модель системи захисту; оцінити значення залишкового ризику, як функцію захищеності по кожній із функціональних властивостей захищеності; визначити структуру системи захисту та її основні компоненти.

Таблиця 2.15 - Модель загроз

Загроза	Ймовірність	Рівень шкоди	К	Ц	Д
Неправомірна змінна даних клієнта	Висока	Високий	-	+	-
Застаріле програмне забезпечення	Висока	Низький	+	+	+
Збій баз даних клієнтів	Висока	Середній	+	+	+
Невиконання правил роботи компанії	Середня	Середній	+	+	+
Умисне пошкодження обладнання	Низька	Сердній	-	+	-
Поширення вірусного програмного забезпечення	Низька	Сердній	+	+	+
Помилка оператора відділення	Середня	Сердній	+	+	+

Продовження таблиці 2.15

Загроза	Ймовірність	Рівень шкоди	К	Ц	Д
Доступ до бази керівника відділення	Середня	Високий	+	+	+
Навмисне розголошення даних клієнта	Середня	Високий	+	+	+
Піратське програмне забезпечення	Середня	Низький	+	+	+

2.7.3 Опис загроз

Неправомірна змінна даних клієнта – це коли оператор відділення змінює данні клієнта без визначених правил, та без відома самого клієнта, в своїх цілях. За порушення звільнення робітника.

Застаріле програмне забезпечення – це коли використовується не актуальне версія програмного забезпечення, котре не відповідає нормам компанії.

Збій баз даних клієнтів – це коли не має доступу працівникам до баз даних, інформаційний відділ компанії завжди оперативно реагує на помилки системи, та ліквідує їх в короткий час.

Невиконання правил роботи компанії – коли працівник навмисно не виконує правила компанії, це порушує весь процес роботи, за систематичне порушення звільнення працівника.

Умисне пошкодження обладнання – це недбале ставлення працівника до інвентару компанії.

Поширення вірусного програмного забезпечення – це коли працівник навмисно поширює в системі компанії вірусне програмне забезпечення. В компаній “Ukr-Delivery” це майже не можливо тому що : флеш носії неможливо підключити до робочого місця , доступ тільки до сайтів компанії, та операційна система обмежена, завантаження та установка програми заборонена. При перезавантаженні операційної системи, всі файли в системі видаляються.

Помилка оператора відділення – це коли оператор відділення не вивчає посадову інструкцію та порушує правила, для цього є система штрафів за невиконання цих самих правил.

Доступ до бази керівника відділення – навмисний доступ до інформації, котра не доступна іншим працівникам відділення.

Навмисне розголошення даних клієнта – це навмисне розголошення даних клієнтів стороннім особам, за це порушення не тільки звільнення а кримільнальна відповідальність.

Піратське програмне забезпечення – це застосування працівником стороннього, не ліцензійного ПЗ, в компанії заборонено використання не ліцензійного ПЗ [9].

Якщо загрози використовують відповідні взразливості і призведуть до інциденту інформаційної безпеки, негативними наслідками для підприємства може стати повна втрата інформації. Враховуючи існуючу ІТС та вимог до властивостей інформації, відповідно до НД ТЗІ 2.5-005 -99, обрано функціональний профіль захищеності для системи:

Довірча конфіденційність.

КД-2. Базова довірча конфіденційність. Реалізована. Користувачі можуть вказувати, які користувачі та процеси можуть отримувати інформацію від об’єктів їхнього домену.

КД-3. Повна довірча конфіденційність. Не реалізована. КЗЗ не забузпечує більш вибірковість керування доступом до інформації об’єктів.

Адміністративна конфіденційність.

КА-1. Мінімальна адміністративна конфіденційність. Не реалізована. У системі не передбачений адміністратор, який би визначав зміну прав доступу до об’єктів.

Повторне використання об’єктів.

КО-1. Повторне використання об’єктів. Не реалізоване. Попередня інформація від процесів та об’єктів не стає недосяжною при зміні користувачів.

Аналіз прихованих каналів.

КК-1. Виявлення прихованих каналів. Не реалізується. У системі не проводиться аналіз прихованих каналів.

Конфіденційність при обміні.

КВ-1. Мінімальна конфіденційність при обміні. Не реалізована. Інформація не шифрується перед імпортом або експортом каналами зв’язку.

Довірча цілісність.

ЦД-1. Мінімальна довірча цілісність. Реалізована. Користувачі можуть модифікувати лише об’єкти лише якщо вони належать ним, або при дозволі з боку власника об’єкта.

ЦД-2. Базова довірча цілісність. Реалізована. Користувачі мають змогу накладати обмеження на те, які процеси можуть модифікувати об’єкт.

ЦД-3. Повна довірча цілісність. Не реалізована. Більш висока вибірковість процесів, які можуть або не можуть модифікувати об’єкти не забезпечена.

Адміністративна цілісність.

ЦА-1. Мінімальна адміністративна цілісність. Не реалізована. У системі не передбачений адміністратор, який може визначати права на модифікацію об’єктів.

Відкат.

ЦО-1. Обмежений відкат. Реалізована. У системі існує можливість автоматизованого відкату операцій, виконаних над певним об’єктом за допомогою вбудованих інструментів Ubuntu.

Цілісність при обміні.

ЦВ-1. Мінімальна цілісність при еспорті. Реалізована. У разі необхідності передачі об’єкта можливо отримання хеш-функції для подальшого порівняння з хеш-фунцією переданого об’єкту.

ЦВ-2. Базова цілісність при обміні. Не реалізована. Система не забезпечує захист від помилок користувача, або від несанціонованих користувачів.

Використання ресурсів.

ДР-1. Квоти. Реалізована. У системі передбачений адміністратор, який може виділяти кількість ресурсів, таких як місце на диску для кожного користувача.

ДР-2. Недопущення захоплення ресурсів. Реалізована. Користувачі не можуть захопити решту ресурсу, не виділеного для них.

ДР-3. Пріоритетність використання ресурсів. Не реалізована.

Стійкість до відмов.

ДС-1. Стійкість при обмежених відмовах. Реалізована частково. Не визначена множина компонентів КС та рівні відмов. Відмова одного компонента не призводить до недоступності всіх послуг.

Гаряча заміна.

ДЗ-1. Модернізація. Реалізована. Заміна окремих компонентів комп'ютера або програмного забезпечення не перешкоджає роботі КЗЗ.

ДЗ-2. Обмежена гаряча заміна. Не реалізована. Множина компонентів КС, які можуть бути замінені без переривання обслуговування не визначена.

Відновлення після збоїв.

ДВ-1. Ручне відновлення. Реалізовано умовно. Множина типів відмов КС та переривань обслуговувань не визначена. У разі відмови КС або переривання КЗЗ адміністратор може повернути систему до нормального стану.

ДВ-2. Автоматизоване відновлення. Реалізовано. КЗЗ має механізм для визначення можливості використання автоматизованих процедур для повернення КС до нормального функціонування.

Реєстрація.

НР-2. Захищений журнал. Реалізовано. Журнал зберігається у зашифрованому вигляді. Наявні механізму для аналізу подій адміністратором.

НР-3. Сигналізація про небезпеку. Не реалізовано. У системі не існує можливості контролювання повторюваних порушень та сигналізування про це адміністратору.

Ідентифікація і автентифікація.

НИ-1. Зовнішня ідентифікація і автентифікація. Реалізовано. Перед входом у систему користувачу необхідно ввести пароль до свого облікового запису.

НИ-2. Одиночна ідентифікація і автентифікація. Реалізовано. Неможливо змінити або отримати доступ до паролю користувача без згоди самого користувача.

НИ-3. Множинна ідентифікація і автентифікація. Не реалізовано. У КЗЗ не використовується два або більше механізмів автентифікації.

Достовірний канал.

НК-2. Двонаправлений достовірний канал. Реалізовано. Канал може зініціюватися лише з боку користувача.

Розподіл обов'язків.

НО-1. Виділення адміністратора. Реалізована. У системі забезпеченні ролі адміністратора та користувача.

НО-2. Розподіл обов'язків адміністраторів. Не реалізовано. У системі не забезпеченно декілька адміністраторів з різними обов'язками.

НО-3. Розподіл обов'язків на підставі привілеїв. Не реалізовано. Множина ролей користувачів не визначена.

Цілісність компексу засобів захисту.

НЦ-1. КЗЗ з контролем цілісності. Реалізовано. КЗЗ має можливість перевіряти власну цілісність та повідомити адміністратора про несправність.

НЦ-2. КЗЗ з гарантованою цілісностю. Реалізовано. КЗЗ має механізми захисту від зовнішніх впливів. Реалізовано за допомогою вбудованих інструментів.

НЦ-3. КЗЗ з функціями диспетчера доступу. Реалізовано. Неможливо увійти в системи, оминувши КЗЗ, або отримати доступ до ресурсів, не виділених користувачу.

Самотестування.

НТ-1. Самотестування за запитом. Не реалізовано. У системі не передбачено тестування функцій КЗЗ.

Ідентифікація і автентифікація при обміні.

НВ-1. Автентифікація вузла. Не реалізовано. Механізми автентифікації інших КЗЗ при обміні об'єктів не реалізована.

Автентифікація відправника.

НА-1. Базова автентифікація відправника. Умовно реалізовано. Можливо дізнатися. Хто створив об'єкт у властивостях об'єкту.

НА-2. Автентифікація відправника з підтвердженням. Умовно реалізовано. Можливо встановити приналежність об'єкту до певного користувача у властивостях об'єкту.

Автентифікація отримувача

НП-1. Базова автентифікація отримувача. Реалізовано. У властивостях об'єкта можна переглянути, чи отримував користувач доступ до нього.

НП-2. Автентифікація отримувача з підтвердженням. Реалізовано Умовно. Можливе підтвердження факту передачі об'єкта незалежною третьою особою у властивостях об'єкту.

2.8 Розробка політики безпеки інформації

Політика інформаційної безпеки — набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації.

Необхідність впровадження : Головною причиною запровадження політики безпеки зазвичай є вимога наявності такого документа від регулятора — організації, що визначає правила роботи підприємств даної галузі [7]. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності.

Крім того, певні вимоги (рекомендації) пред'являють галузеві або загальні, місцеві чи міжнародні стандарти. Зазвичай це виражається у вигляді зауважень зовнішніх аудиторів, які проводять перевірки діяльності підприємства. Відсутність політики викликає негативну оцінку, яка в свою чергу впливає на публічні показники підприємства — позиції в рейтингу, рівень надійності і т. д.

Згідно з дослідженням з безпеки, проведеного компанією Deloitte в 2006 році, підприємства, які мають формалізовані політики інформаційної безпеки, значно рідше піддаються злому. Це свідчить про те, що наявність політики є ознакою зрілості

підприємства в питаннях інформаційної безпеки. Те, що підприємство виразно сформулювало свої принципи і підходи до забезпечення інформаційної безпеки означає, що в цьому напрямку була проведена серйозна робота.

Бізнес сучасного підприємства неможливий без наявності комплексної системи мережевої безпеки. Серед загроз з якими стикаються підприємства — зовнішні зломи корпоративної мережі і як наслідок недоступність корпоративних сервісів, витік конфіденційних даних, нездатність контролю web-трафіку, а так само проникнення вірусів і троянських програм, різні види внутрішніх загроз.

Основні види захисту компанії:

- системою запобігання вторгнень;
- web-фільтрацією;
- антиспам-системою;
- системою запобігання витоку інформації;
- антивірусний захистом.

Цілями системи захисту інформації підприємства є:

- запобігання витоку, розкраданню, втраті, спотворенню, підробці інформації;
- запобігання погрозам безпеці особи, підприємства, суспільства, держави;
- запобігання несанкціонованим діям із знищення, модифікації, спотворення, копіювання, блокування інформації;
- запобігання іншим формам незаконного втручання в інформаційні ресурси і системи, забезпечення правового режиму документованої інформації як об'єкту власності;
- захист конституційних прав громадян на збереження особистої таємниці і конфіденційності персональних даних, наявних в інформаційних системах;
- збереження, конфіденційності документованої інформації відповідно до законодавства;
- ефективний захист інформації компанії та наших клієнтів, для запобігання витоку конфіденційної інформації;
- захист інформаційних активів організації;
- забезпечення стабільної діяльності організації;

- мінімізації ризиків інформаційної безпеки;
- створення позитивних для організації інф. відносин з партнерами, клієнтами та всередині організації.

Основним завданням інформаційної безпеки є захист інформаційних активів від зовнішніх та внутрішніх навмисних та ненавмисних загроз.

Політика безпеки інформації ТОВ «Ukr-Delivery» створена з урахуванням вимог чинного законодавства України.

Етапи захисту інформації на відділеннях ТОВ «Ukr-Delivery» :

- web-фільтрація;
- заборона підключення флеш носіїв;
- доступ до сервісів компанії тільки на відділеннях;
- вхід до системи доступний тільки працівникам;
- повний контроль активності користувача.

Web-фільтрація – внутрішній сервер відділення обмежує доступ до сторонніх сайтів, працівник відділення зможе зайти тільки на сайти компанії.

Заборона підключення флеш носіїв – повна заборона завантаження файлів на флеш носії, для запобігання витоку інформації.

Доступ до сервісів компанії тільки на відділеннях – робочі сайти компанії доступні тільки у внутрішній локальній мережі, з другої мережі доступ обмежений.

Вхід до системи доступний тільки працівникам – користування системою не можливий без облікового запису працівника, кожен працівник має свій унікальний ідентифікатор і пароль.

Повний контроль активності користувача – вся активність користувача відображається в системі.

В компанії є великий відділ підтримки для працівників, котрий має технічну підтримку, та всі питання стосовно робочих моментів.

Якщо працівник подає заявку на внутрішньому сайті компанії, після підтвердження заявки, системний адміністратор дистанційно допомагає у розв'язанні проблеми. У компанії тільки свої працівники з технічної підтримки, для запобігання витоку інформації.

2.8.1 Політика захисту персональних даних:

Згідно закону “Про захист персональних даних” обробка персональних даних здійснюється співробітниками Дирекції з персоналу або працівниками, які відповідно до своїх функціональних обов’язків потребують доступ до них.

З метою належного збереження персональних даних:

- забороняється обробляти (копіювати, пересилати) інформацію, яка може складати персональні дані поза межами інформаційних систем/ресурсів компанії, за винятком випадків, коли обробка здійснюється в рамках виконання внутрішніх положень і процедур або погоджена юридичним департаментом чи відділом безпеки.

Внутрішні нормативні документи політики інформаційної безпеки:

- політика використання мережі інтернет;
- політика управління інцидентами;
- інформаційна безпека робочого місця;
- управління паролями;
- допустиме використання інформаційних актів;
- поводження з інформацією.

Відповідальність:

Кримінальний кодекс України:

- стаття 232 Розголошення комерційної або банківської таємниці карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян;

- стаття 231 Незаконне збирання з метою використання, відомостей, що становлять комерційну або банківську таємницю карається штрафом від трьох тисяч до восьми тисяч неоподаткованих мінімумів доходів громадян;

- стаття 262 Несанкціоновані дії за інформацією, яка обробляється в електронно-обчислювальних машинах (комп’ютерах), автоматичних системах, комп’ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має права доступу до неї караються позбавлення волі на строк до трьох років.

Кожен клієнт може бути спокійним, що користуючись послугами компанії, він отримує:

- захист своїх персональних даних;
- безпечність збереження даних про платежі клієнта;
- безпечність збереження даних із записами телефонних дзвінків до контакт-центру;
- підтримку у рамках законодавства.

2.8.2 Політика використання пошти

Для запобігання порушення інформаційної безпеки, заборонено:

- використання особистої електронної пошти для отримання або обробки конфіденційної інформації та комерційної таємниці компанії;
- відправлення незатребуваних повідомлень електронною поштою особам, які конкретно не запитують цього матеріалу (спам в електронній пошті);
- отримання, перегляд, відправка, передача, зберігання матеріалу чи інформації непристойного, образливого характеру, домагання, погроз, та файлів великого розміру (більше 20МБ);
- розсилати листи не працівникам компанії з корпоративної електронної пошти компанії;
- не можна відправляти повідомлення, що містять конфіденційну інформацію у відкритому (незашифрованому) вигляді;
- забороняється налаштовувати автоматичне пересилання електронних повідомлень у зовнішні системи;
- не можна користуватися однією електронною скринькою одночасно з кимось іншим;
- при надсиланні важливих повідомлень рекомендується зв'язатися з адресатом і переконатися, що лист отримано;
- забороняється розсилати повідомлення, що ображають, дискримінують або принижують гідність інших людей. Слід дотримуватися етикету електронного спілкування;

- необхідно очищати ящик від спаму, ні в якому разі не переадресовуючи такі повідомлення;
- не слід відкривати прикріплені файли або переходити за посиланнями, якщо відправник невідомий, ненадійний або викликає сумніви. Слід одразу видаляти підозрілі повідомлення з кошика поштової скриньки;
- у кожного працівника повинен буди свій підпис.

2.8.3 Політика використання Інтернету

Доступ в інтернет повинен здійснюватися через проксі-сервери та мережеві екрани. Використання з'єднань peer-to-peer (torrent, eDonkey) обмежена, використання повинно бути обґрунтовано виробничою необхідністю, схвалено безпосереднім керівником та погоджено з менеджером з питань безпеки. Співробітникам дозволяється використовувати корпоративний доступ в інтернет в особистих цілях за умови, що це:

- не відбивається негативно на комунікаціях з партнерами і замовниками та на виробничих процесах Товариства;
- не знижує персональні показники продуктивності праці співробітника;
- не шкодить репутації Товариства;
- дотримується законодавства України та «Політики (правил) інф-ї безпеки».

2.8.4 Політика використання Робочого ПК

У публічному місці монітор комп'ютера повинен бути прихований від сторонніх очей. Якщо потрібно перервати роботу з ПК ненадовго, потрібно активувати заставку (Windows+L).

Забороняється:

- зберігати конфіденційну інформацію на робочих комп'ютерах локально в незашифрованому вигляді. Забороняється копіювати конфіденційну інформацію на зовнішні USB накопичувачі. Конфіденційна і важливі робочі дані повинні зберігатися на серверах, користуватися зовнішніми USB накопичувачами: вони можуть сприяти витоку інформації або спричинити зараження вірусом файлової системи. Будь-які налаштування програм виконуються лише системним адміністратором;

- їжу і напої необхідно зберігати та вживати далеко від робочих комп'ютерів. Після закінчення роботи обов’язково потрібно вимикати ПК та всі робочі пристрої. Користувачі несуть відповідальність за захист обладнання від крадіжки чи пошкоджень.

2.8.5 Політика роботи з логіном та паролем

- під час входу в систему будьте уважні та обережні, слідкуйте, щоб ніхто не міг побачити ваш пароль;
- не дозволяйте нікому, крім ІТ-служби, вводити будь-які команди запускати програми на вашому комп’ютері;
- створіть унікальний, складний пароль, який ніде більше не використовуєте, довжиною більше 8 символів;
- при користуванні послугами технічної підтримки, вводьте свій пароль самостійно;
- не повідомляйте пароль до свого облікового запису будь-якого, навіть ІТ-спеціалістам;
- паролі не повинні зберігатись у незахищеному вигляді (на моніторі, на клавіатурі, на липучих нотатках, у текстових файлах, тощо);
- не використовуйте персональну інформацію в паролях.

2.8.6 Політика фізичної безпеки

Завжди майте при собі власний пропуск, який знаходиться у легкодоступному для вас місці.

Негайно повідомляйте Департамент безпеки та свого керівника про:

- втрату посвідчення;
- будь-які крадіжки або злочинні дії з вашим пропуском;
- не залишайте двері відкритими, особливо ті, що потребують спеціального пропуску для відчинення;
- не допомагайте увійти особам, що не мають права входу в приміщення;
- не залишайте конфіденційні данні на принтерах, факсах та іншому обладнанні;

- при вході з офісу в кінці робочого дня, залишайте ваш робочий стіл чистим, комп’ютер і монітор – вимкненим.

2.9 Висновок

У другому розділі було проведено обстеження на ОІД, середовище користувачів, класифікацію інформації в компанії, основні поняття ІТС, аналіз загроз та вразливостей, розроблено політику безпеки інформації та всю структуру захисту інформації на підприємстві.

3 ЕКОНОМІЧНА ЧАСТИНА

Розробка комплексної системи захисту інформації комп'ютерної мережі потребує обґрунтування економічної її доцільності, виходячи з аналізу витрат на розробку та впровадження. Тому метою економічного розділу є здійснення відповідних розрахунків, які дозволять встановити економічного ефекту від впровадження та налагодження комплексів засобів захисту інформації комп'ютерної мережі.

3.1 Розрахунок (фіксованих) капітальних витрат

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

До капітальних витрат належать витрати на розробку політики безпеки інформації, які визначаються виходячи з трудомісткості розробки політики безпеки інформації.

Визначення трудомісткості розробки політики безпеки інформації

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин}, \quad (3.1)$$

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

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ – тривалість процесу аналізу ризиків;

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

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

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

tд – тривалість документального оформлення політики безпеки.

Визначено, що відповідно до етапів розробки політики безпеки інформації, тривалість операцій склала наступні величини:

$t_{тз}$=7 годин, $t_{в}$=13 годин, $t_{тз}$=10 годин, $t_{вз}$=10 годин, $t_{озб}$=5 годин, $t_{овр}$=5 годин, $t_{д}$=10 годин. Згідно з формулою (3.1):

$$t=7+13+10+10+5+5+10= 60 \text{ годин.}$$

Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку політики безпеки інформації $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

Розрахуємо витрати на створення ПБ. Розрахунок проводиться за формулою :

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

де $К_{рп}$ - витрати на створення політики безпеки;

$З_{зп}$ - заробітна плата спеціаліста з інформаційної безпеки;

$З_{мч}$ - вартість витрат машинного часу, що необхідні для створення ПБ.

Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою :

$$З_{зп} = t \cdot Зіб, \text{ грн.}, \quad (3.3)$$

де t - загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ - средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить - 68 грн/год.

Відповідно до формули (3.3), витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 60 \text{ год} \cdot 68 \text{ грн/год.},$$

$$З_{зп} = 4080 \text{ грн.}$$

У свою чергу, витрати машинного часу визначаються за формулою:

$$З_{мч}=t \cdot С_{мч} = 60 \cdot 4,44=266,4 \text{ грн.},$$

де t - трудомісткість розробки політики безпеки інформації на ПК, годин;

$С_{мч}$ - вартість 1 години машинного часу ПК, грн./година. Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = Р \cdot tнал \cdot Се + \frac{Фзал \cdot На}{Fр} + \frac{Клпз \cdot Напз}{Fр} \text{ грн.}, \quad (3.4)$$

де Р - встановлена потужність ПК, кВт;

$С_е$ - тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ - залишкова вартість ПК на поточний рік, грн;

$Н_а$ - річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ - річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ - вартість ліцензійного програмного забезпечення, грн;

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

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання. Згідно з формулою (3.4):

$$Смч = 0,7 \cdot 3 \cdot 1,68 + \frac{6100 \cdot 0,29}{1920} = 4,44 \text{ грн.}$$

Згідно з формулою (3.2), витрати на створення КСЗІ становлять:

$$К_{рп}= 4346,4 \text{ грн.}$$

Серед апаратних засобів, які відповідно до розроблених рекомендації, необхідно придбати (таблиця 3.1).

Таблиця 3.1 - Апаратні засоби до придбання

Обладнання	Кількість шт.	Ціна, грн.
Камера відеоспостереження Dahua DH-IPC-HDBW1230EP-S4	4	8176
Сервер для web-фільтрування ARTLINE Business R25 v12 (R25v12)	1	28 701
Керований комутатор TP-LINK T2500-28TC	1	1719

Всього буде затрачено на нове обладнання 38596 грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають 20% відсотків від первісної вартості програмного забезпечення, тобто 7719,2 грн.

Таким чином, капітальні (фіксовані) витрати на створення політики інформаційної безпеки підприємства складають:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 4346,4 + 38596 + 7719,2 = 50661,6 \text{ грн.},$$

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

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн.;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

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

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

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

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки, згідно з формулою (3.5) складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad грн., \tag{3.5}$$

$$С = 0 + 102883,73 + 0 = 102883,73 \text{ грн.},$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.} \tag{3.6}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_{н} = 0$ грн.).

Річні амортизаційні відрахування усього купленого обладнання із корисним строком використання 5 років, за прямолінійним методом нарахування амортизації складуть:

$$С_{а} = 38596 / 5 = 7719,2 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_{з}$), складає:

$$С_{з} = З_{осн} + З_{дод}, \text{ грн.} \tag{3.7}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 7000 грн. Додаткова заробітна плата – 10% від основної заробітної плати.

Згідно з формулою (3.7), $С_з = 7000 \cdot 12 + 7000 \cdot 12 \cdot 0,1 = 92400$ грн.,

Ставка ЄСВ для всіх категорій платників з 01.01.2019 р. складає 22%.

$$С_{єв} = 92400 \cdot 0,22 = 20328 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.,} \quad (3.8)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,7 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р = 1920$ год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е = 1,68$ грн/кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки, згідно з формулою (3.8) протягом року складає:

$$С_{ел} = 0,7 \cdot 1920 \cdot 1,68 = 2257,92 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат:

1% ($С_{тос} = 50661,6 \cdot 0,01 = 506,61$ грн).

Витрати на керування системою інформаційної безпеки ($С_к$), згідно з формулою (3.6) визначаються:

$$С_к = 0+7719,2 +92400+2257,92+0+506,61 = 102883,73 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 102883,73 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 2 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 1 година;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 2 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (інженерів-програмістів), 8000 грн/міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 9000 грн/міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (системний-адміністратор), 3 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 6 осіб;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 4000 тис. грн у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 10.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V., \quad (3.9)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

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

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

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{9000 \cdot 12}{176} \cdot 2 = 1227{,}26 \text{ грн.},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

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

$$П_в = П_{ви} + П_{пв} + П_{зч}, \quad (3.10)$$

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.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{9000 \cdot 12}{176} \cdot 2 = 1227{,}26 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів), згідно з формулою (3.10) складає:

$$П_{пв} = \frac{8000 \cdot 1}{176} \cdot 1 = 45{,}45 \text{ грн.},$$

$$П_в = 1227{,}26 + 45{,}45 = 1272{,}71 \text{ грн.}$$

Витрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі, згідно з формулою (3.11) складає:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ}), \quad (3.11)$$

$$V = \frac{10000000}{2080} \cdot (2 + 1 + 2) = 24038{,}45 \text{ грн.},$$

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

$$U = 1227{,}26 + 1272{,}71 + 24038{,}45 = 26538{,}42 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_1 \sum_{10} 26538{,}42 = 265384{,}2 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.}, \quad (3.12)$$

де В – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (60%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки, згідно з формулою (3.12):

$$E = 265384{,}2 \cdot 0{,}60 - 102883{,}73 = 56346{,}79 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці}, \quad (3.13)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки грн;

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

Коефіцієнт повернення інвестицій ROSI згідно з формулою (3.13):

$$ROSI = \frac{56346{,}79}{50661{,}6} = 1{,}11 \text{ частки одиниці.}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100), \quad (3.14)$$

де $N_{деп}$ – річна депозитна ставка, (21 %);

$N_{інф}$ – річний рівень інфляції, (8 %).

Розрахункове значення коефіцієнта повернення інвестицій згідно з формулою (3.14):

$$1{,}11 > (21 - 8)/100 = 1{,}11 > 0{,}13.$$

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

$$T_o = \frac{К}{Е} = \frac{1}{ROSI} = \frac{1}{1{,}11} = 0{,}90 \text{ років}$$

3.4 Висновок

Розробка комплексної системи захисту інформації комп'ютерної мережі ТОВ «Ukr-Delivery» є економічно доцільним, оскільки капітальні та експлуатаційні витрати будуть меншими за можливий відвернений збиток. Капітальні витрати складають 50661,6 грн, експлуатаційні – 102883,73 грн. Величина річного економічного ефекту складає 56346,79 грн. Коефіцієнт повернення інвестицій ROSI складає 1,11 грн/грн.

ВИСНОВКИ

У першому розділі кваліфікаційної роботі було розглянуто кібератаки у сфері інформаційної безпеки, методи захисту інформації, нормативно-правову базу у сфері ТЗІ, зроблено аналіз нормативно-правових документів в сфері захисту інформації та побудову КСЗІ. Описали загальний стан розвитку загроз інформаційної безпеки компанії.

У рамках другого розділу було проведено обстеження на ОІД, середовище користувачів, класифікацію інформації в компанії, основні поняття ІТС, аналіз загроз та вразливостей, розроблено політику безпеки інформації та всю структуру захисту інформації на підприємстві, на ОІД виділено недосконалості інформаційно-телекомунікаційної системи підприємства. Недоліки можуть спричинити виток інформації та произвести до завдання збитків підприємству. Згідно з проведеним аналізом, запропоновані до впровадження побудову КСЗІ та політику безпеки для забезпечення ефективного захисту.

У рамках третього розділу було виявлено що: Розробка комплексної системи захисту інформації комп'ютерної мережі ТОВ «Ukr-Delivery» є економічно доцільним, оскільки капітальні та експлуатаційні витрати будуть меншими за можливий відвернений збиток. Капітальні витрати складають 50661,6 грн, експлуатаційні – 102883,73 грн. Величина річного економічного ефекту складає 56346,79 грн. Коефіцієнт повернення інвестицій ROSI складає 1,11 грн/грн.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про інформацію».

2. Закон України «Про захист персональних даних».

3. Закон України ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р.№200.

4. Закон України. Захист інформації. Технічний захист інформації. Основні положення.

5. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

6. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

7. Політика інформаційної безпеки. [Електронний ресурс] – Режим доступу: https://cutt.ly/wnUY8bV.

8. Модель загроз в інформаційних мережах: [Електронний ресурс] – Режим доступу: https://onsto.re/WRaa1.

9. Модель загроз для інформації в ІТС: [Електронний ресурс] – Режим доступу: https://it.wikireading.ru/1000009748.

10. Модель порушника безпеки інформації в ІТС: [Електронний ресурс] – Режим доступу: https://it.wikireading.ru/1000009747.

11. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофеєв, О.В. Кручінін, Ю.А. Мілінчук -Дніпро: НТУ «ДП», 2020.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	1	
5	А4	Стан питання. Постанова задачі	8	
6	А4	Спеціальна частина	38	
7	А4	Економічна частина	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
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 Презентація Астафуров.pptx

2 Диплом Астафуров.docx

ДОДАТОК В. Відгуки керівників розділів

Керівник розділу _____ Пілова Д.П

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу студента групи 125-17-2

Астафурова Романа Антоновича

на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи відділення ТОВ "Ukr-Delivery"»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 65 сторінках.

Метою кваліфікаційної роботи є підвищення ефективності інформаційної безпеки в інформаційно-телекомунікаційної системі ТОВ “Ukr-Delivery”

Тема кваліфікаційної роботи безпосередньо пов’язана з об’єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз стану інформаційної безпеки та особливості організації захисту інформації на підприємстві, яка займається експрес доставкою посилок на території України, аналіз нормативно-правової бази у сфері захисту інформації.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні ефективності процесу ідентифікації інформаційних активів, за рахунок розробки рекомендацій для проведення ідентифікації.

За час дипломування Астафуров Р.А. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі не перевищує вимог “Положення про систему виявлення та запобігання плагіату”.

Кваліфікаційна робота заслуговує оцінки «добре».

Керівник кваліфікаційної роботи доц. каф. БІТ, к.т.н. Сафаров О.О.

Керівник спец. Розділу доц. каф. БІТ, к.т.н. Сафаров О.О.