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 *Шуклінової Дарини Анатоліївни*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему ***Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ "AdMark"***

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	К.т.н. доцент Сафаров О.О.			
розділів:				
спеціальний	ас. Мілінчук Ю.А.			
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

студентці *Шукліновій Дарині Анатоліївні* **академічної групи** *125-17-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ "AdMark"***

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

Розділ	Зміст	Термін виконання
Розділ 1	Загальні відомості та опис організаційної структури підприємства; аналіз нормативно-правової бази; аналіз ситуаційного та генерального плану; аналіз обчислювальної та інформаційної системи; обґрунтовано постановку задачі.	10.05.2021
Розділ 2	Розробка моделі порушника, моделі загроз та вибір профілю захищеності. Розробка програмно-апаратних рішень для захисту інформації.	24.05.2021
Розділ 3	Економічні розрахунки для підтвердження економічної доцільності запропонованих проектних рішень та ефекту впровадження політики.	31.05.31

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

Дата видачі: 08.01.2021р.

Дата подання до екзаменаційної комісії: 15.06.2021р.

Прийнято до виконання _____ **Шуклінова Д.А.**
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 71 с., 9 рис., 15 табл., 6 додатка, 14 джерел.

Об`єкт дослідження: інормаційно-телекомунікаційна система ТОВ «AdMark».

Предмет дослідження: система безпеки інформації на підприємстві «AdMark».

Мета роботи: підвищити рівень захисту інформації в інформаційно-телекомунікаційній системі ТОВ «AdMark».

Методи розробки: спостереження, порівняння, аналіз, опис.

В першому розділі кваліфікаційної роботи надано загальний опис підприємства «AdMark», його організаційна структура, проведено аналіз нормативно-правової бази, проведено дослідження ситуаційного та генерального плану та інформаційно-обчислювальної системи підприємства «AdMark».

В спеціальній частині кваліфікаційної роботи розроблено модель загроз та модель порушника, проаналізовані актуальні загрози та вразливості, обрано профіль захищеності та надані програмно-організаційні рішення для захисту інформації на підприємстві «AdMark».

В економічному розділі кваліфікаційної роботи розраховано капітальні та поточні витрати, проведено оцінку можливого збитку від атаки та виконано аналіз економічної доцільності запропонованих рішень.

Практичне значення роботи полягає у підвищенні рівня захисту інформації в інформаційно-телекомунікаційній системі ТОВ «AdMark», за рахунок розробки рекомендацій щодо впровадження проектних рішень.

ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ЗАХИСТ ІНФОРМАЦІЇ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ВРАЗЛИВОСТІ, АКТ ОБСТЕЖЕННЯ, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ.

РЕФЕРАТ

Пояснительная записка: 71 с., 9 рис., 15 табл., 6 приложения, 14 источников.

Объект исследования: информационно-телекоммуникационная система ООО «AdMark».

Предмет исследования: система безопасности информации на предприятии «AdMark».

Цель работы: повысить уровень защиты информации в информационно-телекоммуникационной системе ООО «AdMark».

Методы разработки: наблюдение, сравнение, анализ, описание.

В первом разделе квалификационной работы предоставлено общее описание предприятия «AdMark», его организационной структуры, предоставлен анализ нормативно-правовой базы, проведено обследование ситуационного и генерального плана, и информационно-вычислительной системы предприятия «AdMark».

В специальной части квалификационной работы разработано модель угроз и модель нарушителя, проанализированы актуальные угрозы и уязвимости, выбран профиль защищенности и предоставлены программно-организационные решения для защиты информации на предприятии «AdMark».

В экономическом разделе квалификационной работы рассчитаны капитальные и текущие расходы, проведена оценка возможного ущерба от атаки и выполнен анализ экономической целесообразности предлагаемых решений.

Практическое значение работы представляется в повышении уровня защиты информации в информационно-телекоммуникационной системе ООО «AdMark», за счет разработки рекомендаций по поводу внедрения проектных решений.

ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, ЗАЩИТА ИНФОРМАЦИИ, КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, УЯЗВИМОСТИ, АКТ ОБСЛЕДОВАНИЯ, ЄКОНОМИЧЕСКАЯ ЦЕЛЕСООБРАЗНОСТЬ.

ABSTRACT

Explanatory note: 71 p., 9 Fig., 15 Table, 6 Annex, 14 sources.

Object of research: Information and telecommunication system LLC "Admark".

Research subject: information security system at the company "AdMark".

Purpose of work: to increase the level of information protection in the information and telecommunication system of LLC "AdMark".

Development methods: observation, comparison, analysis, description.

The first section of the qualification work provides a general description of the AdMark enterprise, its organizational structure, provides an analysis of the regulatory framework, conducted a survey of the situational and general plan, and the information and computing system of the AdMark enterprise.

In a special part of the qualification work, a threat model and an intruder model were developed, current threats and vulnerabilities were analyzed, a security profile was selected, and software and organizational solutions were provided to protect information at the AdMark enterprise.

In the economic section of the qualification work, capital and operating costs were calculated, the possible damage from the attack was assessed, and an analysis of the economic feasibility of the proposed solutions was carried out.

The practical significance of the work is to increase the level of information protection in the information and telecommunications system of LLC "AdMark", through the development of recommendations for the implementation of design solutions.

THE OBJECT OF INFORMATION ACTIVITY, INFORMATION PROTECTION, A COMPREHENSIVE INFORMATION SECURITY SYSTEM, A MODEL OF THREATS, A MODEL OF AN OFFENDER, VULNERABILITY, AN ACT OF EXAMINATION, ECONOMIC EXPEDIENCY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система

ОС – обчислювальна система

ДТЗС – допоміжні технічні засоби

ІТС – інформаційно-телекомунікаційна система

КЗЗ – комплекс засобів захисту від несанкціонованого доступу

КС – комп'ютерна система

КСЗІ – комплексна система захисту інформації

НД – нормативний документ

НД ТЗІ – нормативний документ системи технічного захисту інформації

НСД – несанкціонований доступ

ОТЗ – основні технічні засоби

ТЗІ – технічний захист інформації

КМ – Кабінет Міністрів

БФП – багатофункціональний пристрій

ОП – оперативна пам'ять

ЗП – заробітна плата

ЗМІСТ

ВСТУП

Сучасний світ постійно трансформується і з ним трансформується і маркетинг. Ці зміни спровоковані нашим впливом, адже ми все більше часу проводимо в інтернеті за своїми пристроями. Тому метою сучасних маркетингових компаній є аналіз цих змін і створення такої структури, яка може задовольняти потреби користувачів в реальному часі, працюючи в соціальних мережах, медійній рекламі та електронній комерції [1]. Кожна маркетингова компанія, яка стрімко розвивається, вивчає сутність злиття маркетингу та сучасних технологій. Важливо розуміти вплив нових технологій на стратегію розвитку компанії та на реакцію споживачів, адже поєднання творчого і креативного підходу зі статистикою і програмуванням не простий процес[2]. Тому зараз маркетологи потребують не тільки вдосконалення своїх професійних навичок, а й максимальної їх реалізації через ІТ-технології.

Кожного року з'являються нові маркетингові інструменти основані на технологічному розвитку. Їх впровадження звичайно ж не змінює основних принципів маркетингу, але їх використання значно впливає на процент успіху чи невдачі. Кожна компанія аналізує зміни на технологічному рівні, адже важливо не просто слідкувати за тенденціями сьогоднішніх днів, але й розуміти як зміни вплинуть на бізнес та чи підуть вони на користь клієнтам.

З впровадженням технологічних рішень з кожним роком збільшуються очікування клієнтів. Деякі інструменти, які тільки з'являються на ринку вже активно використовуються компаніями для задоволення потреб користувачів. І в такому темпі все менше часу приділяється виявленню слабких місць і вразливостей даних методів, які впливають на подальше життя компанії.

Зі зростанням впливу технологій постає також питання безпеки інформації [3]. З підвищенням впливу компаній на ринку з'являються конкуренти, впроваджується нове програмне забезпечення, обладнання та технологічні рішення. З цим зростає шанс перехоплення конфіденційної інформації, її знищення або модифікація.

Щоб уникнути завеликих збитків компанії використовують комплексні системи захисту інформації – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС. Адже гарантований захист інформації, вдосконалення впроваджених технологій, постійний аналіз існуючих системи безпеки і сучасних технологічних змін забезпечує розвиток компаній та закріплення їх позицій на світовому ринку.

В цій роботі буде розглянуто підприємство «AdMark», його фізичну та інформаційну структуру, обґрунтування необхідності створення КСЗІ для інформаційно-технологічної системи підприємства. У наступних розділах частково змінено інформацію для збереження анонімності компанії.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про підприємство ТОВ «AdMark».

Підприємство «AdMark» – маркетингова компанія, яка займається створенням рекламної продукції, ребрендингом, аналізом товарного ринку, тестуванням нової продукції за участю покупців. Організація працює на ринку вже 5 років. Компанія орендує офіс на 2 поверсі офісного комплексу «Aran» (3-х поверхова будівля) за адресою вулиця Олени Пчілки, 82. Робочі години підприємства – з понеділка по п’ятницю з 9:00-18:00.

Схема організаційної структури підприємства «AdMark» надана на рисунку 1.1, штат працівників підприємства – таблиця 1.1.

Таблиця 1.1 – Штат працівників підприємства «AdMark»

№	Посада	Роль в системі	Кількість працівників на посаді	Рівень кваліфікації	Стаж на підприємстві
1	Директор (Керівник напряму 1)	Системний адміністратор	1	Високо кваліфікований користувач	5 років
2	Заступник директора	Користувач	1	Високо кваліфікований користувач	4 років
3	Керівник напряму 2	Користувач	1	Високо кваліфікований користувач	5 років
4	Бухгалтер	Користувачі	2	Кваліфіковані користувачі	5 років 4 років
5	Менеджер напрямку 1	Користувачі	9	Кваліфіковані користувачі	5 років
6	Менеджер напрямку 2	Користувачі	8	Кваліфіковані користувачі	5 років
8	Менеджер напрямку 2	Користувачі	1	Середньо кваліфікований користувач	1 рік
9	Прибиральниця	-	1	Низько кваліфікований користувач	3 роки

Обов'язки працівників:

- Директор (Керівник напрямку 1) – проводить маркетинговий аналіз, а саме аналіз відомостей про те, наскільки ефективні рекламні оголошення та кошти, які виділені на поширення реклами; ребрединг продукції; створення рекламної продукції; введення зустрічей з клієнтом в режимі онлайн конференцій Google Meet; проведення особистих зустрічей з клієнтом при необхідності.
- Заступник директора – підтримує роботу обладнання та слідкує за забезпеченням безпеки інформації; допомагає керівнику напрямку 1 проводити маркетинговий аналіз, ребрединг продукції та створення дизайну продукції.
- Керівник напрямку 2 – проводить маркетингові дослідження товарів та ринку, а саме пошук нових методів маркетингового використання продукції, що випускається; вивчення можливостей спростити асортимент; визначення характеру і розмірів ринку; маркетингові дослідження споживачів, виявлення інформації про географічне положення покупців, а також про питому вагу продукції основних конкуруючих підприємств в умовах загального обсягу збуту в галузі ринку; аналіз структури, організація діяльності та склад мережі збуту, що займається обслуговуванням даного ринку; аналіз загальноекономічних та інших зовнішніх тенденцій, що здатні вплинути на ринкову структуру; введення зустрічей з клієнтом в режимі онлайн конференцій Google Meet; проведення особистих зустрічей з клієнтом при необхідності.
- Менеджери напрямку 1 – проводять аналіз відомостей про те, наскільки ефективні рекламні оголошення та кошти, які виділені на поширення реклами, а також сама рекламна робота; ребрединг продукції; створення рекламної продукції. Процеси контролюються керівником напрямку 1 або його заступником.
- Менеджери напрямку 2 – проводять аналіз варіантів по створенню нових товарів; тестування нової продукції за участю покупців; дослідженням по упаковці; вивчення можливостей спростити асортимент; визначати характер і розмір ринку (клієнти повинні бути охарактеризовані з урахуванням віку, статі, професії, соціального статусу, положення, доходу); маркетингові дослідження споживачів, виявлення

інформації про географічне положення покупців, а також про питому вагу продукції основних конкуруючих підприємств в умовах загального обсягу збуту в галузі ринку; аналіз структури, організація діяльності та склад мережі збуту, що займається обслуговуванням даного ринку; аналіз загальноекономічних та інших зовнішніх тенденцій, що здатні вплинути на ринкову структуру.

- Бухгалтери – повне введення бухгалтерського обліку юридичної особи; робота з клієнт-банком в національній та іноземній валюті; робота з первинною документацією; виконують розпорядження керівників.
- Прибиральниця – проводить прибирання приміщень в сб в першій половині дня. За чистотою офісу кожен день слідкує черговий менеджер. Сантехнік, електрик, персонал провайдера Інтернету – представники зовнішніх організацій, які залучаються за необхідністю і можуть перебувати в офісі лише при наявності працівників підприємства.

Рисунок 1.1 – Схема організаційної структури підприємства «AdMark»

Вид інформаційної діяльності, що передбачається на ОІД – відкрита інформація, конфіденційна інформація та обробка їх технічними засобами.

1.2 Аналіз нормативно-правової бази

Згідно з Законом України «Про інформацію» [4], де описані види інформації і відповідальність за порушення законодавства про інформацію та інше – визначено, що інформації про фізичну особу та інформації з обмеженим доступом повинен надаватися особливий та обов'язковий захист. Тому передбачено спеціальний порядок захисту визначеної інформації.

Згідно з Законом України «Про персональні дані» [5] визначаються суб'єкти відносин, пов'язаних із персональними даними, об'єкти захисту, загальні/особливі вимоги до обробки персональних даних та контроль за додержанням законодавства про захист персональних даних.

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» [6] розглядається забезпечення захисту інформації в системі та інше. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Організація технічного захисту інформації на підприємстві покладена на його керівництво. Також визначається відповідальність у разі порушення вимог до захисту технічної інформації згідно Положення про технічний захист інформації в Україні.

Для того, щоб створити комплексну систему захисту інформації (КСЗІ), використовуються засоби для захисту інформації, які мають сертифікати відповідності/затверджений експертний висновок (Положення про державну експертизу в сфері технічного захисту інформації).

Згідно з НД ТЗІ 3.7-003-2005 [7] встановлено порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

Концепція технічного захисту інформації в Україні затверджена Постановою КМ України від 08.10.1997 №1126.

1.3 Акт обстеження

1.3.1 Ситуаційний план

Підприємство «AdMark» орендує офіс на 2 поверсі офісного 3-х поверхового комплексу. Об’єктом інформаційної діяльності (ОІД) є приміщення та коридори офісу. Схема ситуаційного плану та умовні позначення наведені на рисунку 1.2.

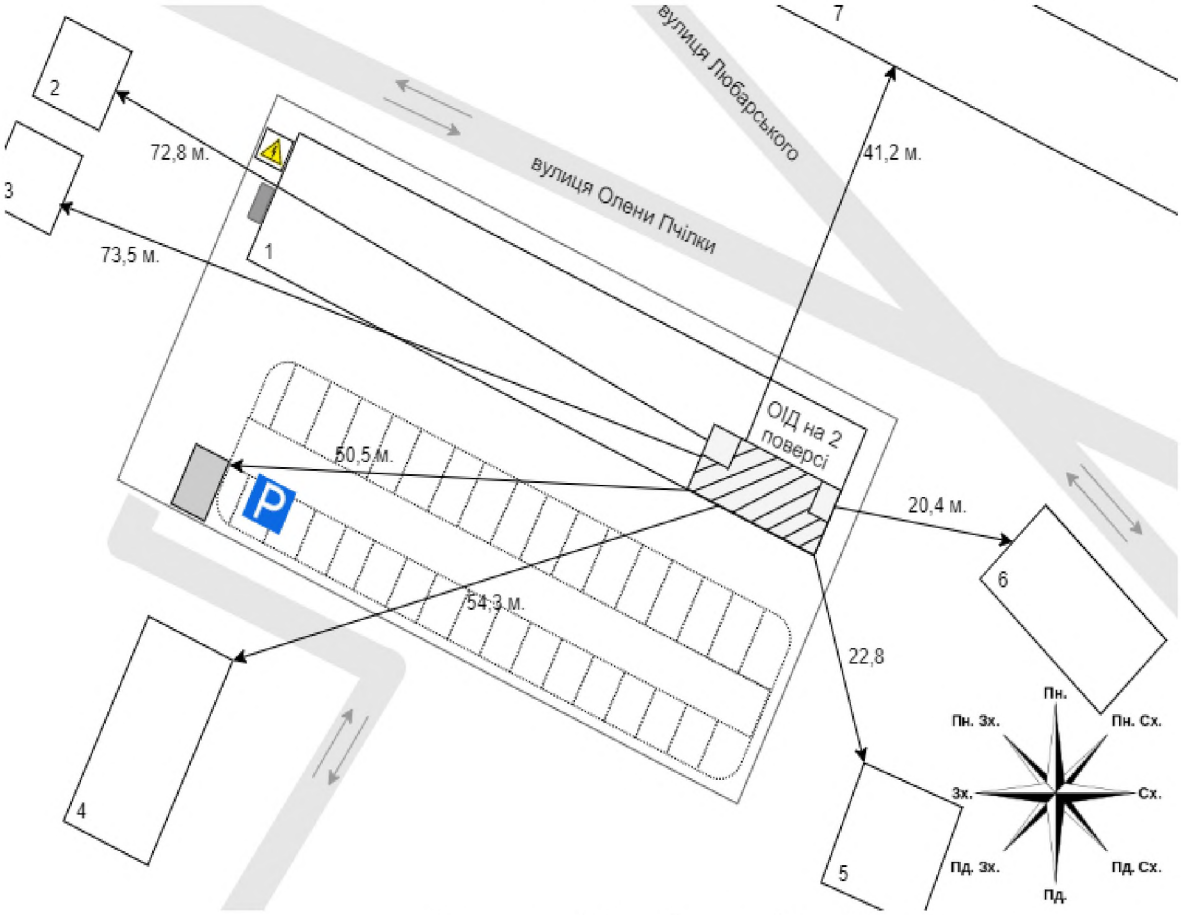
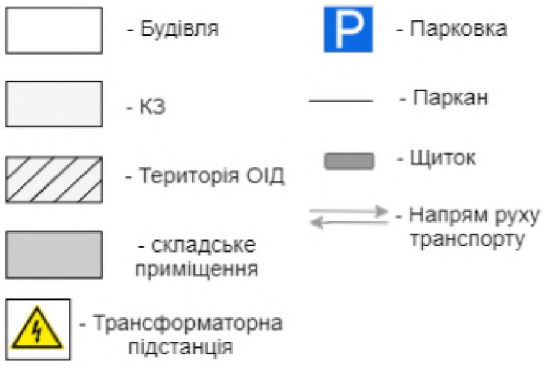


Рисунок 1.2 – Ситуаційний план

Умовні позначення



Територія офісного комплексу «Aran» – закрита; огороджена металевим парканом. Вхід на територію комплексу через автомобільне КПП (контрольно-перепускний пункт) – шлагбаум автоматично відкривається після сканування перепустки. Вхідні двері (металеві, 55 мм.) до комплексу оснащенні магнітною стрічкою, для ініціалізації перепусток (вхід/вихід). На території комплексу діє централізована охорона(цілодобово). Охоронний пункт, на першому поверсі біля вхідних дверей, контролює в'їзд на територію офісного комплексу та переміщення по комплексу через системи відеоспостереження. Відеоспостереження – зовнішнє та внутрішнє цілодобове.

Територія навколо будівлі асфальтована, з південно-західної та західної сторони є місця паркування. З південно-східної сторони за парканом знаходиться невелика зелена зона. З північно-східної сторони будівлі прилягає дорога з двостороннім рухом. Підвал та криша зачинені, до них має доступ лише охоронець, що має ключ.

Інформація про навколишні будинки та споруди надана в таблиці 1.2.

Доступ в офіс - цілодобовий для осіб, які мають перепустку до офісного комплексу та до офісу підприємства. У суботу в офісній частині проводиться прибирання всього приміщення. Прибиральниця – найманий співробітник підприємства.

Таблиця 1.2 – Характеристика будівель та споруд

№	Призначення будівлі	Адреса	Кількість поверхів	Відстань від ОІД
1	Офісний комплекс, в якому знаходиться ОІД	Вулиця Олени Пчілки, 82	3	-

Продовження таблиці 1.2 – Характеристика будівель та споруд

№	Призначення будівлі	Адреса	Кількість поверхів	Відстань від ОІД
2	Приватна житлова будівля	Вулиця Олени Пчілки, 56	1	72,8 м.
3	Приватна житлова будівля	Вулиця Олени Пчілки, 59	1	73,5 м.
4	Житлова будівля	Вулиця Прогресивна, 17	5	54,3 м.
5	Міні-маркет	Вулиця Мурманська, 1а	1	22,8 м.
6	Медичний центр	Вулиця Мурманська, 1	2	20,4 м.
7	Магазин меблів	Вулиця Любарського, 85/1	2	41,2 м.

Схема комунікацій, що підходять до будівлі комплексу та місце розташування трансформаторної підстанції та щитка відносно межі контрольованої зони надані на рисунку 1.3.

Система електроживлення – централізована. Трансформаторна підстанція розташована на території комплексу. Від неї система електроживлення підземно підключається до щитка в підвальному приміщенні комплексу.

Система заземлення – заземлення на спільний контур (замкнутий), з’єднаний з щитком в підвальному приміщенні.

Система водопостачання – централізована. Підключена до водоканалу та підземними комунікаціями під’єднана через підвальне приміщення.

Система каналізації – централізована. Підключена до міської мережі та підземними комунікаціями під’єднана через підвальне приміщення.

Система опалення – централізована. Підключена до системи теплопостачання та підземними комунікаціями під’єднана через підвальне приміщення.

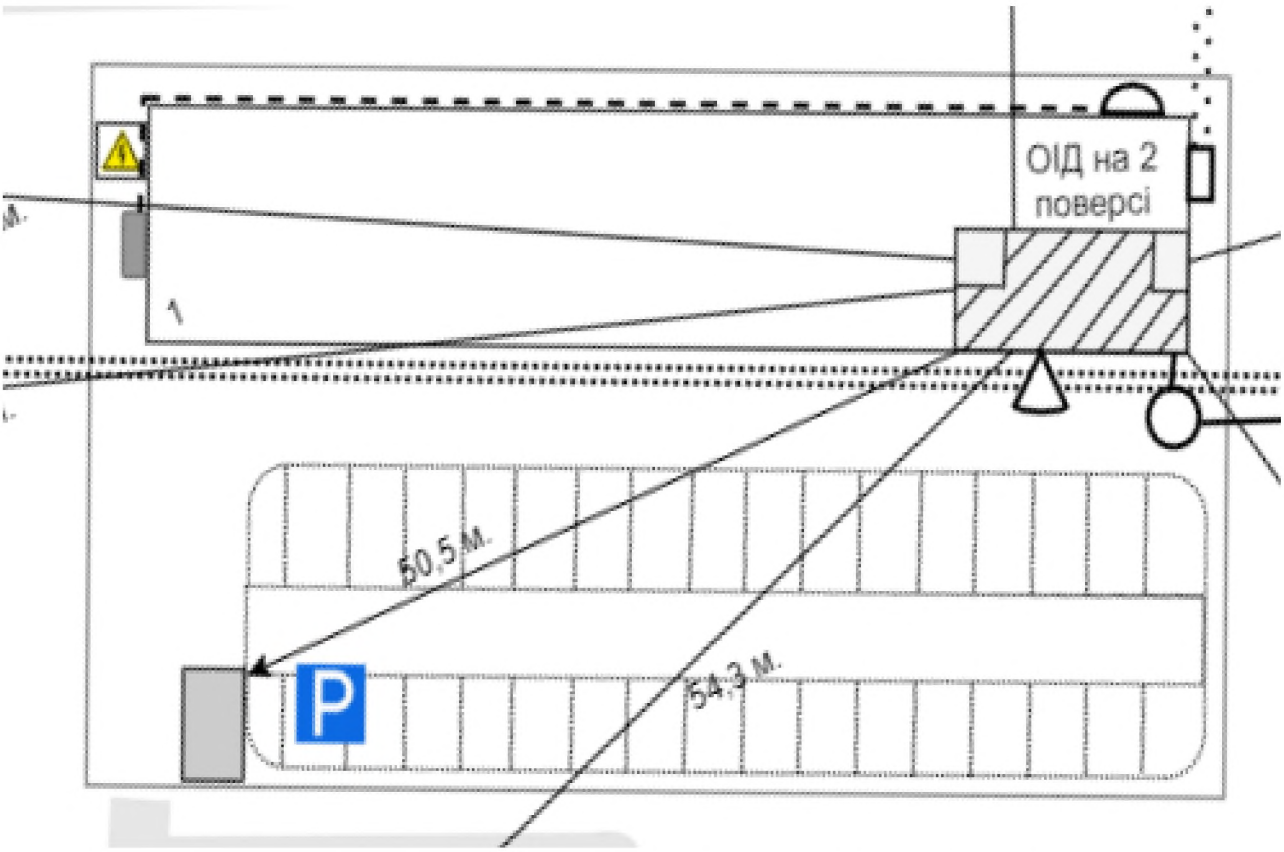
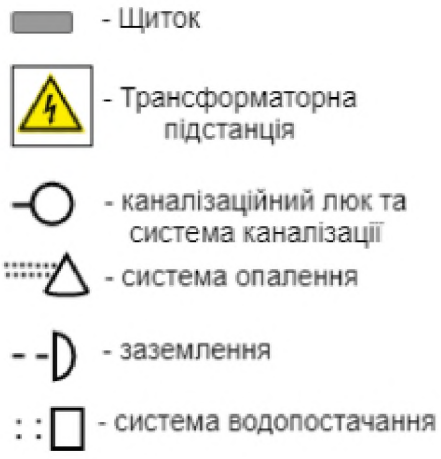


Рисунок 1.3 – Ситуаційний план. Схема комунікацій

Умовні позначення



Контрольована зона, ОІД обмежені: північний захід – внутрішні стіни будівлі; південний захід – зовнішні стіни будівлі; південний схід – зовнішні стіни будівлі; північний схід – стіни будівлі, які суміжні з сусідніми; зверху та знизу – стелею та підлогою, за якими сусідні офіси.

Складові КЗ – 9 приміщень і загальний коридор. Розміри приміщень:

- Вбиральня чоловіча – 3,2 m. x 2,2 m.
- Вбиральня жіноча – 3,2 m. x 2,2 m.
- Кухня – 6 m. x 4,4 m.
- Склад – 4,4 m. x 2 m.
- Робоче приміщення 1 – 4m x 3m.
- Робоче приміщення 2 – 4m x 3m.
- Кабінет керівника напрямку 1 – 3,2 m. x 3 m.
- Кабінет керівника напрямку 2– 4 m. x 3 m.
- Кабінет керівника напрямку 3– 3,2 m. x 5 m.

1.3.2 Генеральний план

ОІД це частина офісу на 2 поверсі, який знаходиться в 3-поверховому офісному комплексі. Площа ОІД – 220 м². Розміри – 20 х10 м. Висота стелі – 3 м. Поверх – 2-й. Стеля: матеріал – залізобетон, товщина – 35 см; підлога: матеріал – залізобетон, товщина – 35см; стіни: залізобетон + гіпсокартон, товщина – 25см. Вікна: 5 одиниць, матеріал – пластик (полівінілхлорид або ПВХ), розміри – 1410см х 1390см. Сектор видимості – буд.№ 4,5,6 (південно-західна та південно східна сторона). Двокамерні. Всі 5 одиниць – відчиняються. На всіх вікнах встановленні датчики на відкриття та розбиття скла та елементи сонцезахисту – горизонтальні жалюзі. Двері: один вхід/вихід – металеві двері, 55 мм. Висота – 2,1 м. Ширина – 1,6 м. Оснащенні сканером відбитків пальців та магнітною стрічкою. На території ОІД встановлено 9 дерев'яних дверей, виконаних в різних стилях, з врізаними замками на ключ. Висота – 2 м. Ширина – 0,80 м. Ключ – металевий.

Виявлені характерні особливості ОІД, що впливають на вибір заходів та засобів ТЗІ: наявність вертикальних жалюзі; 2-й поверх будівлі; на території ОІД в складському приміщенні зберігається інформація в паперовому вигляді та в закритій шафі (дерев'яна, три окремі полиці в середині шафи, кожна закривається на металевий ключ, ключі зберігаються у керівників) зберігаються електронні носії інформації. В

трьох окремих полицях зберігаються 3 окремі (2 ТБ) з'ємні диски на яких записується та зберігається інформація кожен день.

Схема генерального плану, розміщення ОТЗ, ДТЗС, пожежних датчиків та датчиків сигналізації наведені на рисунку 1.4

Система електроживлення – централізована. Система виходить за межі ОІД до етажного розподільчого щитку і проведена до підвального приміщення, де підключена до головного щитка, який в свою чергу з'єднаний з трансформаторною підстанцією. Система електроживлення та освітлення надана на рисунку 1.5.

Система заземлення – підключена до системи електроживлення, яка виходить за межі ОІД.

Система комп'ютерної мережі – Інтернет забезпечує провайдер «Київстар». Проведений до офісу оптоволоконним кабелем. Вита пара підключена до комутатора, який утворює локальну мережу (VLAN). Кабель виходить за межі ОІД до сходового майданчика, де з`єднується між поверхами та з'єднується в підвальному приміщені. Система комп'ютерної мережі надана на рисунку 1.6.

Система телефонної лінії – локальна. Доступ робітників через міні АТС «Panasonic», до якої підключено 4 телефона менеджерів. Система телефонного зв'язку надана на рисунку 1.6.

Система опалення – централізована. Підключена до системи теплопостачання, яка знаходиться за межами ОІД. Труби системи опалення проходять через всі поверхи будівлі і з'єднуються в підвальному приміщенні. На ОІД встановлено 8 біметалевих радіатора вертикального з'єднання. Система опалення надана на рисунку 1.7.

Система вентиляції – Приточно-витяжна, виходить за межі ОІД до сходового майданчика. Шахти вентиляції проходять через всі поверхи будівлі. Система вентиляції надана на рисунку 1.7.

Система сигналізації – централізована, з виходом на пульт сигналізації, виходить за межі ОІД. При спрацьовуванні охоронних датчиків, сигнал з панелі сигналізації направляється на пульт охорони. Пост охорони знаходиться на 1 поверсі,

а також офісний комплекс співпрацює з охоронною фірмою – група реагування буде на об'єкті максимум через 5 хв. На кожному поверсі знаходяться камери спостереження, за якими цілодобово слідкує охоронець. Система охоронної сигналізації - Лунь-9Р та система пожежної безпеки - датчиків диму Артон СПД-3.4. надані на рисунку 1.4.

Крім камер відеоспостереження, за якими слідкує охоронець, на території КЗ знаходиться власна камера – онлайн відеоспостереження з панорамою 180% (Turbo HD Камера Hikvision DS-2CC52H1T-FITS) перед вхідними дверима з постійним записом на жорсткий диск і дублюванням інформації в хмару. Відеоспостереження внутрішнє цілодобове.

На території ОІД на всіх вікнах (5 штук) встановлені датчики Philio PST02-A-Z-Wave 4-в-1 на відкриття вікна, рівня освітленості, температури і руху. На стіні в основному коридорі - датчик руху Feron sen11 / lx39 чорний (180 градусів кут виявлення) інфрачервоний. На вхідні двері –магнітоконтактний накладний ЭСМК-8. З зовнішньої сторони вхідної двері – світло-звукова сигналізація MAKS Siren White. Датчики диму знаходяться у всіх приміщеннях і коридорах на території КЗ.

Система кондиціювання – виходить за межі КЗ і ОІД. На території ОІД встановлено 5 пристроїв фірми Electrolux Monaco EACS/I-09HM/N3 з спліт системою (ширина – 79 см, висота – 27,5 см). Система кондиціювання надана на рисунку 1.7.

Відомості про основні технічні засоби (А.1) та відомості про допоміжні технічні засоби і системи (А.2) надані в ДОДАТКУ А.

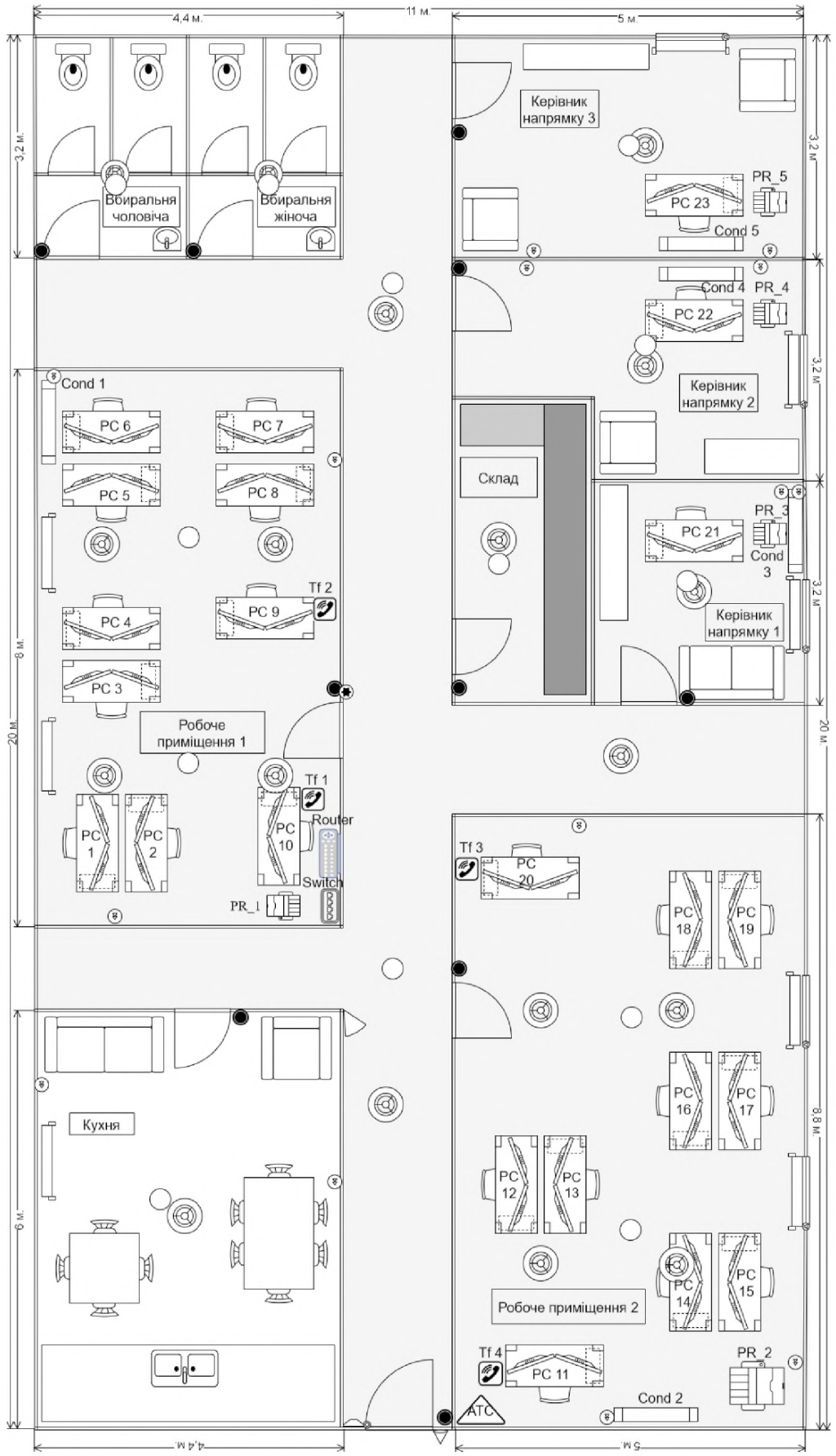


Рисунок 1.4 – Генеральний план. Розміщення ОТЗ, ДТЗС, пожежних датчиків та датчиків сигналізації

Умовні позначення:

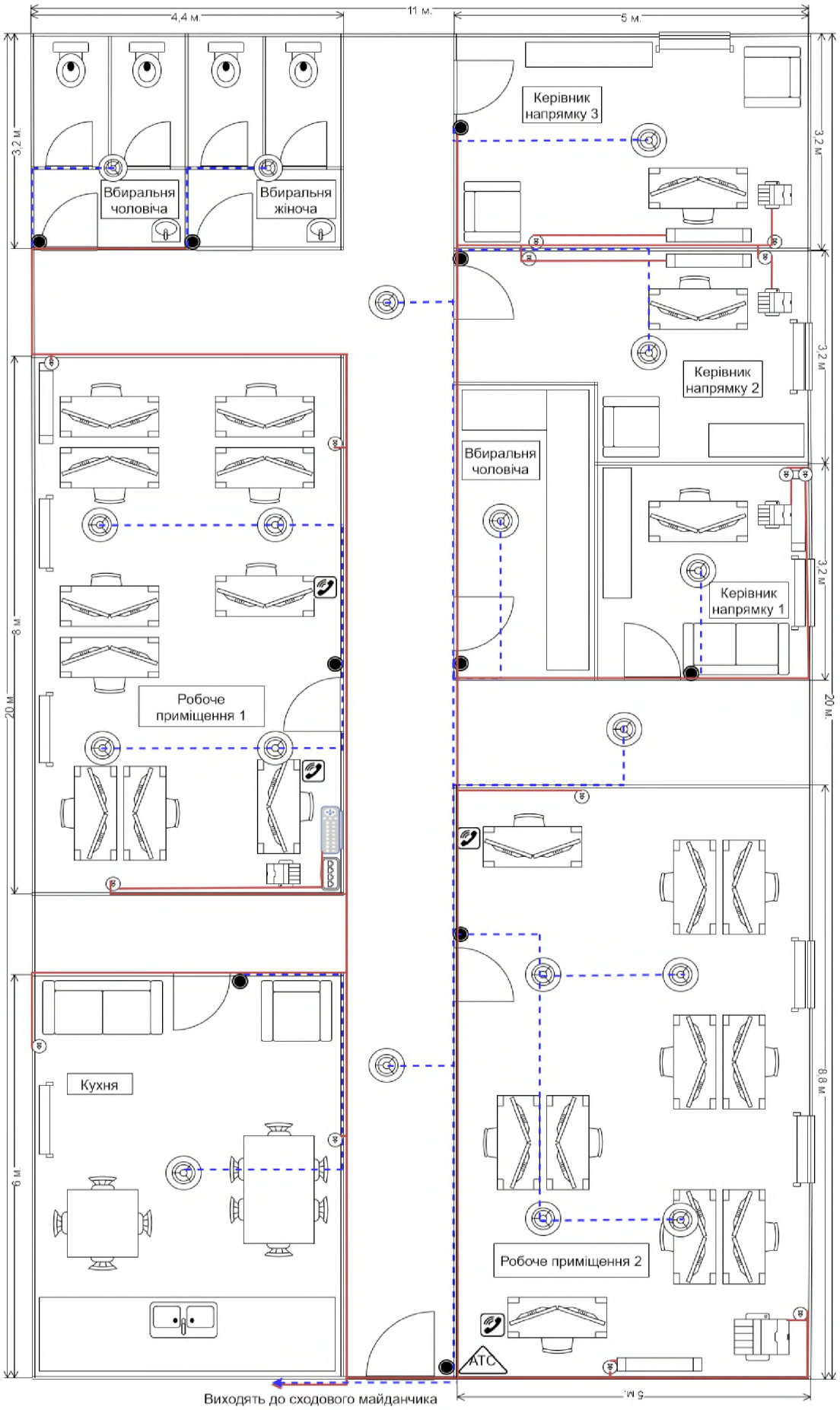


Рисунок 1.5 – Генеральний план. Лінії систем електропостачання та освітлення

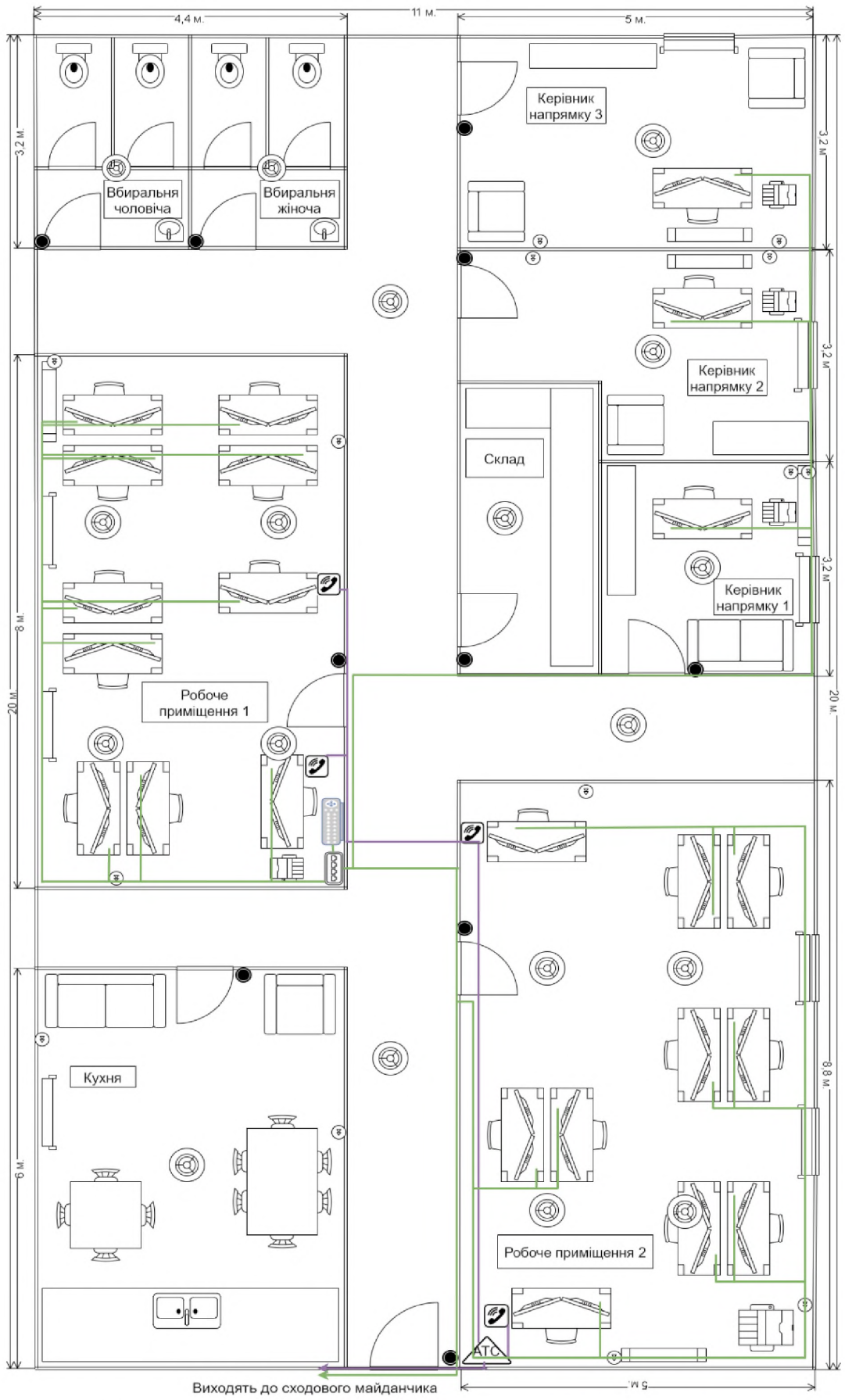


Рисунок 1.6 – Генеральний план. Лінії систем телефонного зв’язку та комп’ютерної мережі

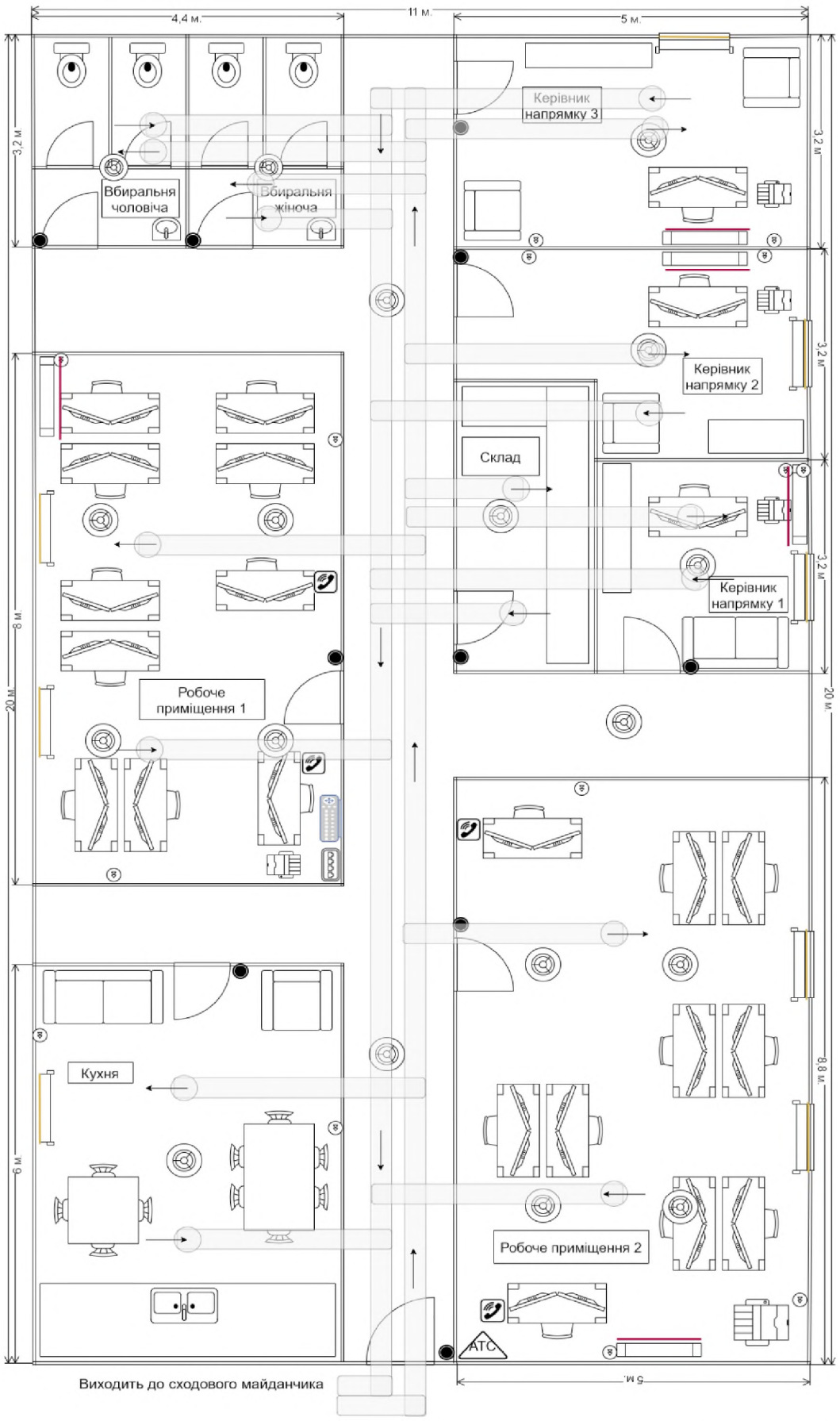


Рисунок 1.7 – Генеральний план. Лінії систем опалення та кондиціювання та систем вентиляції

Умовні позначення:

1.3.3 Обчислювальна та інформаційна система

Опис програмного забезпечення та його локалізація на комп'ютерах на підприємстві «AdMark» надані в таблиці 1.3.

Таблиця 1.3 – Програмне забезпечення в ІС підприємства

№	Назва ПО	Тип	Ліцензія	Призначення	Термін дії	Встановлено
1	Windows10 (версія 1909)	Системне	Commercial	Операційна система	Безстроково	PC 1...PC 23
2	Драйвера (Nvidia 442.19)	Системне	Freeware	Доступ та управління апаратним забезпеченням або пристроями	Безстроково	PC 1...PC 23
3	Microsoft Word (версія 2019)	Прикладне	Commercial	Створення та редагування текстових документів	Безстроково	PC 1...PC 23
4	Microsoft Exel (версія 2019)	Прикладне	Commercial	Створення та редагування данних, представлених у вигляді таблиць	Безстроково	PC 1...PC 23
5	Adobe Photoshop (версія 2020)	Прикладне	Commercial	Багатофункціональний графічний редактор	Безстроково	PC 1...PC 9 PC12...PC23
6	Adobe Illustrator (версія 2020)	Прикладне	Commercial	Створення ілюстрацій, логотипів та іконок для сайтів; верстання макетів для друку	Безстроково	PC 1...PC 9 PC12...PC23

Продовження таблиці 1.3 – Програмне забезпечення в ІС підприємства

№	Назва ПО	Тип	Ліцензія	Призначення	Термін дії	Встановлено
7	Adobe Indesign (версія 2020)	Прикладне	Commercial	Робота з макетами та дизайнами сторінок	Безстро-ково	PC 1...PC 9 PC12...PC23
8	Dr.WEB (версія 12.0)	Спеціалі-зоване	Commercial	Антивірусна програма	Безстро-ково	PC 1...PC 23
9	Printoffice24 (версія 8.1)	Прикладне	Shareware	Система обліку замовлень	До 07. 08.2021	PC 1...PC 23
10	M.E.Doc (версія 11.02.038)	Прикладне	Commercial	Подання звітності до контролюючих органів та обміну юридично значимими первинними документами між контрагентами в електронному вигляді	Безстро-ково	PC10...PC11 PC20...PC23
11	1С Бухгалтерія (версія 3.0.67.74)	Прикладне	Commercial	Бухгалтерська програма для автоматизованого обліку	Безстро-ково	PC10...PC11 PC20...PC23
12	CRM (версія 3.0)	Прикладне	Shareware	Контроль за комунікаціями з клієнтами та автоматизація продажів	До 07. 08.2021	PC 1...PC 23

Продовження таблиці 1.3 – Програмне забезпечення в ІС підприємства

№	Назва ПО	Тип	Ліцензія	Призначення	Термін дії	Встановлено
13	ERP (версія 2.5.6)	Прикладне	Shareware	Планування ресурсів підприємства	До 07. 08.2021	PC 1...PC 23

ІТС складається з 23 комп'ютерів, 2 принтерів типу БФП і 3 принтерів, 1 комутатора, 1 роутера. Характеристу складу ІТС підприємства «AdMark» надано в ДОДАТКУ А (А.3).

Інформаційну систему, підприємства «AdMark» надано на рисунку 1.8.

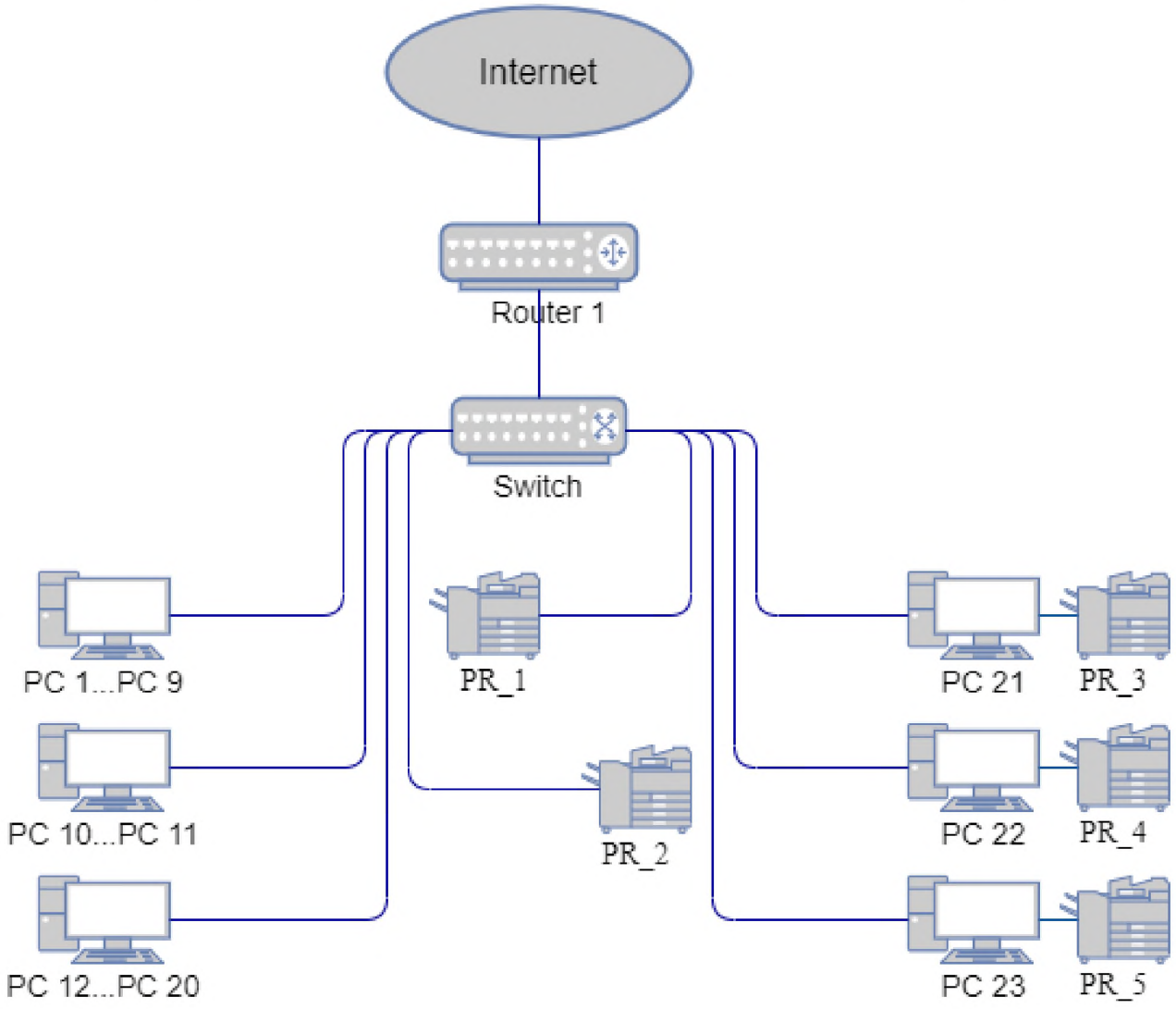


Рисунок 1.8 – Схема інформаційної системи підприємства

Кабель інтернету проведений до офісу оптоволоконним кабелем. Вита пара підключена до маршрутизатора (локальна мережа (VLAN)), до якого прямим підключенням під'єднаний до комутатора. PC 1…PC 23 з'єднуються прямим підключенням з комутатором (вита пара). Принтери PR_1, PR_2 – під'єднані до комутатора прямим підключенням. Принтери PR_3, PR_4, PR_5 підключені локально до PC 21, PC 22, PC 23 відповідно. PC 1…PC9 – комп'ютери менеджерів напрямку 1, PC 10…PC11 – комп'ютери бухгалтерів, PC 12…PC20 – комп'ютери менеджерів напрямку 2. PC 1…PC 20, PR_1, PR_2 об'єднані в одну віртуальну локальну мережу VLAN 1, а PC 21…PC 23 в іншу - VLAN 2, для того щоб комп'ютери з VLAN 1 не мали доступ до мережі комп'ютерів VLAN 2.

Інформація, що циркулює на ОІД це – персональна інформація про клієнтів та працівників підприємства, фінансова та бухгалтерська звітність, та інформація про роботу компанії (продукти, проекти...), відкрита інформація (реклама). Класифікація цієї інформації наведена в таблиці 1.4.

Таблиця 1.4 – Класифікація інформації, яка циркулює на ІТС

№	Вид інформації	Режим доступу	Правовий режим	Вид представ-лення в ІТС	Вимоги до захисту		
					К	Ц	Д
1	Інформація про клієнтів (персональна)	ІзОД	Конфіден-ційна інформація	Текстовий Електрон-ний	3	2	3
2	Інформація про працівників (персональна)	ІзОД	Конфіден-ційна інформація	Текстовий Електрон-ний	4	4	4

Продовження таблиці 1.4 – Класифікація інформації, яка циркулює на ІТС

№	Вид інформації		Режим доступу	Правовий режим	Вид представ-лення в ІТС	Вимоги до захисту		
						К	Ц	Д
3	Продукти роботи підприємства	Вхід./вихід. документи	ІзОД	Конфіден-ційна інформація	Текстовий Електрон-ний	4	5	4
		Матеріали про проект				4	5	4
		Дизайн				4	5	4
4	Бухгалтерська звітність, договори		ІзОД	Конфіден-ційна інформація	Текстовий Електрон-ний	4	5	4
5	Фінансова звітність (банківські рахунки, виручка)		ІзОД	Службова інформація	Електрон-ний	3	4	4
6	Реклама		Відкри-та інфор-мація	Відкрита інформація	Електрон-ний	1	2	3

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 до неї;

– 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.

Всі ресурси обробляються працівниками підприємства – 18 менеджерів двох різних напрямків, 2 бухгалтера, 2 керівника різних напрямків та заступник директора.

Вся текстова документація зберігається в складському приміщенні (окреме приміщення, зачинене на ключ), до якого доступ мають тільки керівники напрямків. Електронна інформація записується та зберігається на 3 різних полицях (зачинені на ключ), у вигляді 2Тб дисків. Резервування всієї інформації виконується кожен день на ці диски, а також в хмарне сховище.

Інформація про клієнтів (персональна) – менеджер домовляється з клієнтом про проект (замовлення), після чого вносить його в систему замовлень (CRM, ERP, Printoffice24) та передає до бухгалтера – інформація обробляється бухгалтерами (Microsoft Exel) та керівниками напрямків, може бути роздрукована. Зберігається на полицях в закритому складському приміщенні.

Інформація про працівників (персональна) – обробляється керівниками напрямків та бухгалтерами, може бути роздрукована. Зберігається на полицях в закритому складському приміщенні.

Продукти роботи підприємства – вхідні та вихідні документи (правки, розрахунки, аналітика…), матеріали про проекти, дизайнерські рішення та розробки – при роботі над проектом, менеджера постійно зберігають результати на певному етапі і передають на перевірку керівникам напрямків. Після внесення всіх правок, готовий проект передається замовнику, а також зберігається в електронному вигляді на полицях в закритому складському приміщенні на дисках.

Бухгалтерська та фінансова звітність обробляється бухгалтерами та контролюється керівниками напрямків. Бухгалтера зберігають звітність по зарплатам працівників у електронному та друкованому вигляді.

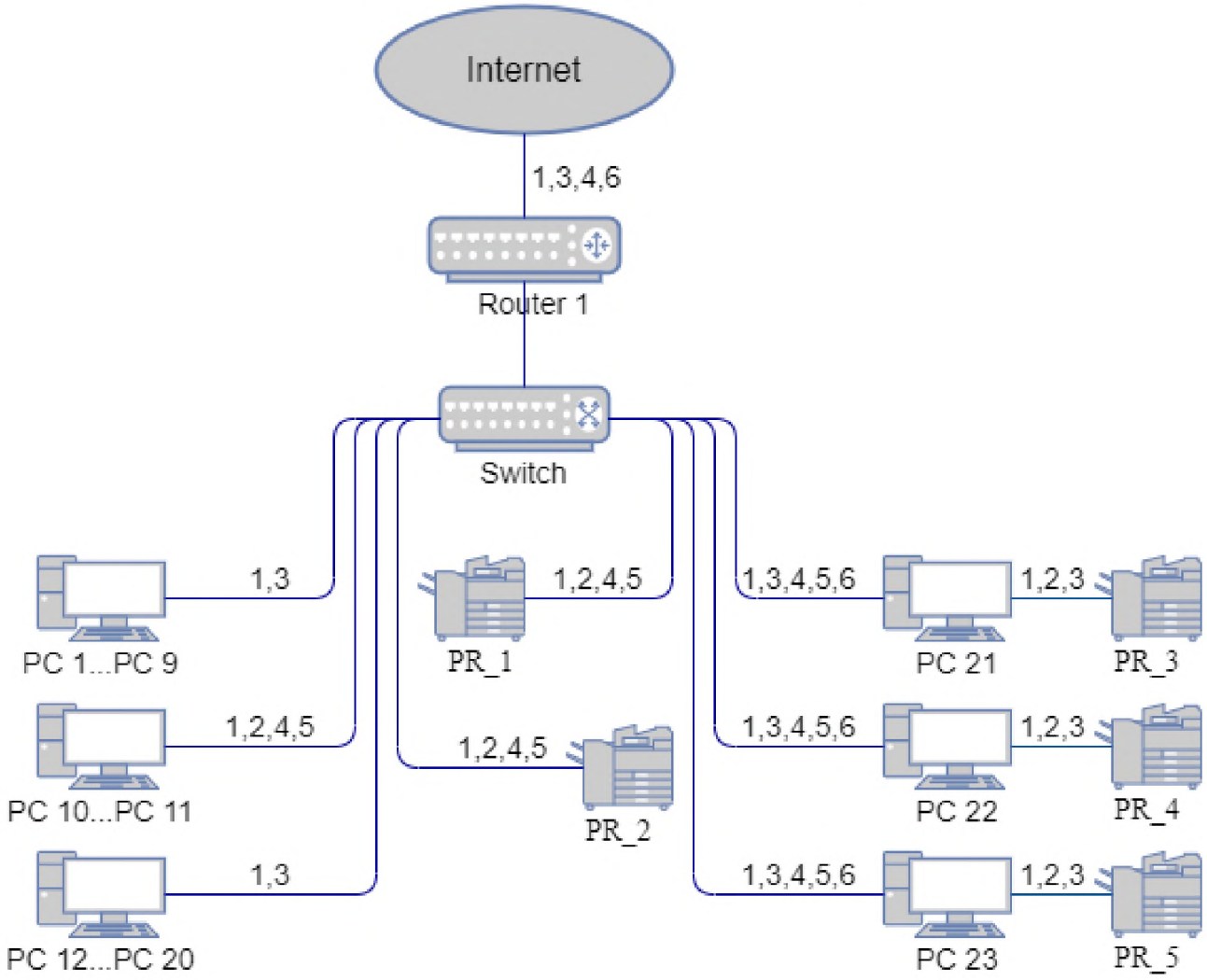
Реклама – підприємство активно рекламує свої послуги в соціальних мережах та на просторах інтернету.

Клієнти самі звертаються до компанії (реклама) або менеджери самі знаходять потенційних клієнтів (спеціальні платформи, аналіз та опрацювання нових компаній та підприємств); клієнт звертається до компанії з своїм проектом/ідеєю до менеджера компанії з яким ведуться переговори з приводу проекта (мета, ціль, розвиток, потенціал та прибуток) та його можливостей. Клієнта вносять в програми (CRM, ERP, Printoffice24). Всю допоміжну інформацію по проекту та свої персональні данні клієнти пересилають на корпоративну пошту. Після ознайомленням з проектом керівниками напрямків, його приймає в роботу керівник одного напрямку або два керівника різних напрямків одразу (залежить від проекту) – розробляється план робіт та визначаються терміни (період вивчення ринку, період створення моделі проекту, корективи, графічна робота, корективи, побудова фінальної моделі та виведення результатів на ринок). З клієнтом також зв'язуються бухгалтери та створюють договір (M.E.Doc, 1С Бухгалтерія), після якого клієнт вносить повну оплату проекту (під час проекту можуть виникати додаткові витрати, про які інформують клієнтів). Менеджери працюють над проектом, використовуючи Adobe Photoshop, Adobe Indesign, Adobe Illustrator та Інтернет, для пошуку певної інформації та її аналізу. При кожному етапі відтворення проекту, керівники вносять корективи. Для конкретного проекту створюють свої терміни для кожного етапу, під час яких з клієнтом підтримується зв'язок (інформується по виконанню певного етапу та його результатів) через керівника напрямку (Google Meet). Клієнти також можуть вносити свої корективи. Для коректівів проекту на кожній стадії він може друкуватися як БФП (2 одиниці), так і принтерами, які локально підключені до кожного керівника. Після завершення проекту бухгалтера перевіряють фінансові звітності, тому що можуть вноситися певні доплати під час проекту. Після завершення проекту керівник тримає зв'язок з клієнтом для підтвердження результатів та у ролі допомоги для правильного просування проекту у ринок.

Схема інформаційних потоків надана на рисунку 1.9.

Матриця розмежування доступу надана в таблиці 1.5.

Рисунок 1.9 – Схема інформаційних потоків



Інформаційні потоки:

1. Обробка інформації про клієнтів
2. Обробка інформація про працівників
3. Обробка продуктів роботи підприємства
4. Обробка бухгалтерської звітності, договорів
5. Обробка фінансової звітності
6. Обробка рекламних даних

Таблиця 1.5 – Матриця розмежування доступу

Користувач		Директор	Заступник директора	Кер. Н. 2	Бух-галтери	Мен. Н. 1	Мен. Н. 2
Ін-фор-ма-ція	Інформація про клієнтів	R, W, M, D, C, T	R, W, M, D, A, C, T	R, W, M, D, C, T	R, W, M, C, T	R, W, C, T	R,W, C, T
	Інформація про працівників	-	-	-	R, W, M, D, C, T	-	-
	Продукти роботи підприємства	R, W, M, D, C, T	R, W, M, D, A, C, T	R, W, M, D, C, T	-	R, W, M, D, C, T	R, W, M, D, C, T
	Бухгалтерська звітність, договори	R, W, M, D, C, T	R, W, M, D, A, C, T	R, W, M, D, C, T	R, W, M, C, T	-	-
	Фінансова звітність	R, W, M, D, C, T	R, W, M, D, A, C, T	R, W, M, D, C, T	R, W, C, T	-	-
	Реклама	R, W, M, D, C, T	R, W, M, D, A, C, T	R, W, M, D, C, T	R	R, W, M, C, T	R,W, M,C, T
Повноваження інсталювання ПЗ		+	+	+	+	+	+
Ресурси		PC 21	PC 22	PC 23	PC 10 PC 11	PC 1 … PC 9	PC 12 … PC 20

R – читання;

W – запис;

M – модифікація;

D – видалення;

A – права адміністратора;

C – створення нових файлів;

T – перенесення.

1.4 Постановка задачі

Так як на підприємстві ТОВ «AdMark» обробляється інформація з обмеженим доступом, рішення щодо її безпеки приймає її власник – директор ТОВ «AdMark» Глущенко А.І.. Було прийнято рішення про створення КСЗІ, а для цього необхідно виконати:

- проаналізувати модель загроз;
- проаналізувати модель порушника;
- обрати профіль захищеності;
- запропонувати програмно-організаційні заходи для підвищення безпеки інформації;
- проаналізувати рівень загроз та збитків після запропонованих проектних рішень.

1.5 Висновки до першої частини

Розглянуто актуальність теми маркетингу і технологій, а також захисту інформації з розвитком технологій.

Проведено аналіз нормативно-правової бази – визначені основні положення, закони України та накази у сфері захисту інформації, а саме персональних даних, інформації з обмеженим доступом та технічного захисту інформації.

Розглянуті загальні відомості про підприємство «AdMark», виконано обстеження ситуаційного та генерального плану, обчислювальної та інформаційної системи, організаційної структури підприємства. Обґрунтовано необхідність створення КСЗІ на підприємстві «AdMark» та виконано постановку задачі.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Модель порушника

Користувачі, їх відносини та людська поведінка фактично відображають питання безпеки захищених ІТС, адже злочини здійснюються саме людиною. Згідно з НД ТЗІ 1.1-003-99 модель порушника це абстрактний опис порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії.

Порушниками можуть бути клієнти, відвідувачі, представники організацій, будь-які особи за межами контрольованої зони і так далі. Їх можна розділити на внутрішніх та зовнішніх. Внутрішніми порушниками можуть бути користувачі системи, персонал, що обслуговує технічні засоби, співробітники відділів розробки та супроводження програмного забезпечення, технічний персонал, що обслуговує будівлю, співробітники служби безпеки і так далі. Зовнішніми – добре озброєна та технічно оснащена група або поодинокі порушники, що не мають допуску на об'єкт. Метою порушників може бути отримання, модифікація, знищення необхідної інформації, нанесення збитків шляхом знищення матеріальних цінностей, а також безвідповідальність, самоствердження та корисливий інтерес.

Для розробки моделі порушника можна використовувати систему таблиць (Таблиці 2.1 – 2.6). Для побудови моделі використовуються категорії, ознаки та характеристики порушників для більш точного їх аналізу, при цьому рівень загрози кожної з них вказується в дужках і оцінюється за 4-бальною шкалою.

Таблиця 2.1 – Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов’язок (ПЗ4)	4

Таблиця 2.2 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	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 2.3 – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 2.4 – Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	4

Таблиця 2.5 – Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Таблиця 2.6 – Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
Внутрішні по відношенню до ІТС		
ПВ1	Технічний персонал, який обслуговує будови та приміщення,в яких розташовані компоненти ІТС	1
ПВ2	Персонал, який обслуговує технічні засоби ІТС (інженери,техніки)	2

Продовження таблиці 2.6 – Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
ПВ3	Користувачі (оператори) ІТС	2
ПВ4	Адміністратори ІТС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
Зовнішні по відношенню до ІТС		
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачанняі таке інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4

На основі систем таблиць будується 2 моделі – модель внутрішнього порушника – таблиця 2.7, та модель зовнішнього порушника – таблиця 2.8.

Таблиця 2.7 – Модель внутрішнього порушника

Посада	Мотив	Кваліфі-кація	Можли-вості	Час дії	Місце дії	Категорія порушника	Сума загроз
Директор	М2	К3	З3	Ч3	Д4	ПВ3	17
Заступник директора	М3	К4	З3	Ч4	Д4	ПВ4	21
Керівник напрямку2	М3	К3	З3	Ч3	Д4	ПВ3	18

Продовження таблиці 2.7 – Модель внутрішнього порушника

Посада	Мотив	Кваліфікація	Можливості	Час дії	Місце дії	Категорія порушника	Сума загроз
Бухгалтер	М1	К2	З2	Ч3	Д3	ПВ3	13
Бухгалтер	М1	К2	З2	Ч3	Д3	ПВ3	13
Менеджера напрямку 1	М1	К2	З2	Ч3	Д2	ПВ3	12
Менеджера напрямку 2	М1	К2	З2	Ч3	Д2	ПВ3	12
Менеджер напрямку 2	М2	К2	З2	Ч3	Д2	ПВ3	12

Таблиця 2.8 – Модель зовнішнього порушника

Посада	Мотив	Кваліфікація	Можливості	Час дії	Місце дії	Категорія порушника	Сума загроз
Персонал офісного комплексу	М3	К2	З2	Ч2	Д1	ПЗ1	11
Конкуренти	М4	К3	З4	Ч3	Д1	ПЗ4	19
Прибиральниця	М1	К1	З1	Ч1	Д2	ПВ1	7
Працівники, які представляють ремонтні послуги	М3	К2	З2	Ч2	Д2	ПЗ2	13
Хакери	М4	К3	З4	Ч3	Д1	ПЗ3	18

Продовження таблиці 2.8 – Модель зовнішнього порушника

Посада	Мотив	Кваліфі-кація	Можли-вості	Час дії	Місце дії	Категорія порушника	Сума загроз
Комунальний персонал офісного комплексу	М1	К1	З2	Ч1	Д2	ПЗ2	9
Користувач	М3	К2	З1	Ч2	Д2	ПВ3	12

Основними потенційними порушниками можуть бути:

- заступник директора;
- керівник напрямку 2;
- конкуренти і хакери.

Тому організація роботи цих осіб має бути найбільш контрольованою.

2.2 Модель загроз

Загрози для інформації залежать від ряду факторів, наприклад таких як персонал, програмних чи апаратних засобів, фізичного середовища та технологій.

Згідно з НД ТЗІ 1.1-003-99 модель загроз це абстрактний опис засобів та методів, завдяки яким реалізація загроз стає можливим.

Модель загроз визначає класифікацію та типи загроз, вказує на які властивості інформації спрямовані загрози, визначає способи втілення загроз і так далі.

Перелік загроз з визначенням порушень властивостей інформації та ІТС надано в таблиці 2.9

Таблиця 2.9 – Перелік загроз з визначенням порушень властивостей інформації та ІТС

№	Загрози	Ймовірність	Ймовірні Збитки	Властивості		
				К	Ц	Д
1	Пожежа	Низька	Низькі	+	+	+
2	Затоплення	Низька	Низькі	+	+	+
3	Збої електроживлення	Середня	Високі	-	+	+
4	Пошкодження носіїв інформації	Низька	Високі	-	+	+
5	Несанкціонований доступ, викрадення носіїв інформації	Низька	Високі	+	+	+
6	Несанкціоноване підключення до технічних засобів	Середня	Високі	+	-	-
7	Несанкціоноване копіювання інформації на зовнішні носії	Середні	Високі	+	-	-
8	Створення клонів системи	Низька	Високі	+	-	+
9	Підслуховування	Низька	Низькі	+	-	-
10	Перегляд інформації з екранів моніторів через вікно	Низька	Низькі	+	-	-
11	Несанкціоновані дії системного адміністратора	Середня	Високі	+	+	+
12	Порушення правил розмежування доступу	Середні	Середні	+	+	+
13	Занесення вірусу до комп’ютерної системи	Середня	Високі	+	+	+
14	Використання стороннього ПЗ	Висока	Середні	-	+	+
15	Розголошення інформації персоналом ІТС	Середня	Низькі	+	-	-

Продовження таблиці 2.9 – Перелік загроз з визначенням порушень властивостей інформації та ІТС

№	Загрози	Ймовірність	Ймовірні Збитки	Властивості		
				К	Ц	Д
16	Помилки персоналу ІТС	Середня	Низькі	+	-	-
17	Підкуп працівників підприємства з метою отримання ІзОД	Низька	Середні	+	+	+
18	Використання вразливостей ПЗ	Середня	Середні	+	+	+
19	Несанкціоноване використання продуктів роботи та програм	Середня	Низькі	+	-	+

Рівні ймовірності загрози та збитків:

Високий – здійснення загрози призводить до великих збитків (3 бали);

Середній – здійснення загрози призводить до помірних збитків (2 бали);

Низький – здійснення загрози призводить до незначних збитків/їх нема (1 бал).

Найбільш актуальними загрозами для підприємства «AdMark» є:

1. Порушення доступності та цілісності інформації через збої електроживлення. Це можливо через відсутність безперебійного джерела живлення та відсутність постійного збереження даних проектів/клієнтів протягом робочого дня. Це може привести до значних фінансових втрат та уповільнення роботи над проектами.

2. Порушення конфіденційності інформації співробітниками (менеджерами напрямків) шляхом несанкціонованого копіювання на зовнішні носії. Це можливо через відсутність обліку та контролю зовнішніх носіїв інформації, відсутності протоколювання роботи зі змінними носіями. Це може привести до занесення вірусу до комп'ютерної системи, значних фінансових втрат та витоку інформації.

3. Порушення всіх властивостей інформації співробітником (заступник

директора) шляхом несанкціонованих дій, використовуючи права системного адміністратора. Це можливо через відсутність контролю за діями адміністратора та порушення правил розмежування доступу (немає адміністратора безпеки). Це може привести до значних фінансових втрат та витоку інформації.

4. Порушення конфіденційності, цілісності, доступності інформації співробітниками (менеджери, бухгалтери) шляхом інсталяції стороннього ПЗ. Це можливо оскільки не має чіткого контролю за встановленням ПЗ та відсутністю обмеження прав інсталювання ПЗ працівниками підприємства. Це може привести до значних фінансових втрат та витоку інформації.

5. Порушення конфіденційності інформації співробітниками (менеджери напрямків, бухгалтери) через ненавмисні помилки. Це можливо шляхом безвідповідальності працівника (середньо кваліфікований менеджер напрямку 2), та відсутності проведення періодичних навчань/перевірок знань. Це може привести до значних незначних фінансових втрат та витоку інформації.

6. Порушення всіх властивостей інформації сторонніми особами (конкурентами, хакерами) шляхом хакерських дій на вразливості ПЗ. Це можливо оскільки не все ПЗ оновлено до останньої версії. Це може призвести до незначних фінансових втрат та витоку інформації.

7. Порушення конфіденційності інформації сторонніми особами (конкурентами, комунальним персоналом офісного комплексу, працівниками, які представляють ремонтні послуги) шляхом перегляду ІзОД на екранах моніторів користувачів ІТС. Це можливо оскільки РС 15, 17, 19 (їх монітори) повернені до вікна. В денний час жалюзі не закриваються , офіс на другому поверсі, з можливістю переглядати інформацію з сусідньої будівлі або за територією комплексу при наявності спеціальної техніки. Допоміжним захистом вікна не облаштовані. Це може призвести до незначних фінансових втрат та витоку інформації.

2.3 Профіль захищеності

При створенні КСЗІ [11] визначається спроможність системи забезпечувати захист інформації. Розглядається захист оброблюваної інформації як від НСД так і від витоку технічними каналами. Критерії комп'ютерної системи – набір функціональних послуг і функцій, що забезпечують захист від певних загроз [12].

АС – організаційно-технічна система, що включає в себе персонал, оброблювану інформацію, ОС та фізичне середовище. Для нашого ОІД вибрана АС «3» класу. Згідно з НД ТЗІ 2.5-005-99 [9]: «Розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу. Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки».

Обрані стандартні функціональні профілі захищеності в КС, що входять до складу АС класу «3», з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації:

3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

КД-2. Базова довірча конфіденційність. Реалізована. Політика довірчої конфіденційності, що реалізується КЗЗ, визначає множину об'єктів КС, до яких вона відноситься: продукти роботи підприємства. КЗЗ здійснює розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. [НИ-1].

КА-2. Базова адміністративна конфіденційність. Реалізована. Політика адміністративної конфіденційності, що реалізується КЗЗ, визначає множину об'єктів КС, до яких вона відноситься: продукти роботи підприємства, інформація про клієнтів та співробітників, рекламні данні, бухгалтерська та фінансова звітності. КЗЗ надає можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і

об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта. [НИ-1, НО-1].

КО-1. Повторне використання об’єктів. Реалізована. До того як користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об’єкт, встановлені для попереднього користувача або процесу права доступу до даного об’єкту скасовуються, а також вся інформація, що міститься в даному об’єкті, стає недосяжною. [НИ-1, НО-1].

КК-1. Аналіз прихованих каналів - виявлення. Реалізована. Канал по пам’яті може бути реалізований, якщо не буде реалізоване повторне використання об’єктів. Канал по часу може бути реалізований, оскільки з високою вірогідністю користувачі не будуть перевіряти схеми закриття і відкриття файлів, однак це можна попередити використовуючи наприклад «port knocking», який вимагає дотримання певних заданих послідовностей для відкриття портів. [КО-1].

КВ-2. Базова конфіденційність при обміні. Реалізована. Множина об’єктів та інтерфейсних процесів – сервер документів, драйвер файлової системи, захищенні документи. Наявні протоколи захисту інформації при обміні (HTTPS – використовує додатковий шар шифрування/автентифікації, WPA2 - посилена безпека даних і посилений контроль доступу до бездротових мереж - підтримує шифрування відповідно до стандарту AES,...), оновлення ПО. [НО-1].

ЦД-1. Мінімальна довірча цілісність. Реалізована. КЗЗ надає користувачу можливість для кожного захищеного об'єкта (продукти роботи підприємства), що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. [НИ-1].

ЦА-2. Базова адміністративна цілісність. Реалізована. Політика адміністративної цілісності, що реалізується КЗЗ, визначає множину об'єктів КС, до яких вона відноситься: продукти роботи підприємства, інформація про клієнтів та співробітників, рекламні данні, бухгалтерська та фінансова звітності. КЗЗ розмежовує доступ на підставі атрибутів доступу – процесу і захищеного об’єкту. [НИ-1, НО-1].

ЦО-1. Обмежений відкат. Реалізовано. Множина об’єктів – захищенні документи, файли, технологічна інформація. Існують автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій - редагування інформації, наприклад в WORD – Ctrl+Z, видаленні файли можна відновити, система контролю версії, резервне копіювання..., виконаних над захищеним об'єктом за певний проміжок часу.

ЦВ-2. Базова цілісність при обміні. Реалізована. Об’єкти - документи, файли, технологічна інформація (оновлення ПО, антивірусу). Хеш функція (функція, що здійснює перетворення масиву вхідних даних довільної довжини в (вихідну) бітову послідовність встановленої довжини, що виконується певним алгоритмом; не зворотний процес, фіксована довжина на виході, не значні зміни даних повинні значно змінювати результат функції, для різних вхідних даних може створитися один хеш; один з видів алгоритмів – MD5), наявні протоколи передачі по мережі та комутаційні пристрої. [НО-1].

ДР-1. Використання ресурсів - квоти. Реалізована. Відносяться до таких ресурсів системи: об’єм пам’яті, дисковий простір, пропускна спроможність каналів зв’язку... [НО-1].

ДС-1. Стійкість при обмежених відмовах. Реалізована. Об’єкт – оперативна пам’ять. [НО-1].

ДЗ-1. Гаряча заміна – модернізація. Реалізована. Відноситься не тільки до конструкції, а й до апаратного і програмного забезпечення. Оновлення антивірусу, системних файлів. [НО-1].

ДВ-1. Відновлення після збоїв – ручне відновлення. Реалізована. (тільки після збоїв системи, а не інформації). Точки відновлення, резервне копіювання. [НО-1].

НР-2. Реєстрація – Зовнішній аналіз, захищений журнал. Реалізована. [НИ-1, НО-1].

НИ-2. Зовнішня ідентифікація і автентифікація, одиночна. Реалізована. Вхід до локального запису відбувається з використанням пароля. Також є можливість

скористатися фізичним ключом безпеки [НК-1].

НК-1. Одно-направлений достовірний канал. Реалізовано. З'єднання з системою проводить тільки людина(користувач) – введення паролю тільки з клавіатури.

НО-2. Розподіл обов'язків адміністраторів. Реалізована. Політика розподілу обов'язків, що реалізується КЗЗ, визначає ролі адміністраторів і звичайного користувача і притаманні їм функції, визначає дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Однак на нашому об'єкті одна людина наділена функціями адміністратора безпеки та системного адміністратора. [НИ-1].

НЦ-2. Цілісність комплексу засобів захисту – КЗЗ з гарантованою цілісністю. Реалізована. Політика цілісності КЗЗ визначає домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ підтримує домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Політика цілісності КЗЗ визначає склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ: антивірус, вбудовані механізми у системі, хеш функція...

НТ-2. Самотестування за запитом - Самотестування при старті. Реалізована. Система та антивірус автоматично починають перевірку при ініціалізації. [НО-1].

НВ-1. Автентифікація вузла. Реалізована. Обмін даними може відбуватися через блютуз з'єднання, через USB...

НА-1. Базова автентифікація відправника. Реалізована. Наявний цифровий підпис. [НИ-1].

НП-1. Базова автентифікація отримувача . Реалізована. Наявний цифровий підпис. [НИ-1].

2.4 Розробка програмно-організаційних рішень для захисту інформації

КСЗІ включає в себе заходи, що направлені на аналіз ризиків та їх зниження, а також на зниження можливостей реалізації загроз через вразливості ІТС. Після аналізу моделі порушника та моделі загроз виявлено загрози, що мають високий рівень реалізації на підприємстві «AdMark». До таких загроз належать збої електроживлення, несанкціоноване копіювання на зовнішні носії, інсталяція стороннього ПЗ, ненавмисні помилки співробітників, хакерські дії на вразливості ПЗ, перегляд ІзОД на екранах моніторів. Зниження ризиків цих загроз є першочерговою задачею.

Збої електроживлення можливі через перепади напруги. На ОІД немає безперебійного джерела живлення, але в той же час є два принтери типу БФП та ще 3 принтера, через які може статися падіння напруги в електромережі. Це стає можливим оскільки робота принтерів не контролюється – вони всі можуть працювати одночасно, а також у персоналу впродовж робочого часу немає фіксованих правил, за якими вони зберігають проекти/документи в певний проміжок часу протягом дня. Отже, потрібно ввести для даної системи джерело безперебійного живлення – ENERSOL 33 10XL, а також налагодити роботу менеджерів – ввести в ПЗ, в якому відбувається створення/модифікація проектів, функцію автоматичного зберігання через певний проміжок часу. Також ввести правило постійного зберігання даних для персоналу.

Через відсутність обліку та контролю зовнішніх носіїв інформації, протоколювання роботи зі змінними носіями можливе несанкціоноване копіювання на зовнішні носії. Отже потрібно заборонити підключати до робочого комп'ютера будь-які зовнішні накопичувачі інформації (USB Flash, SD-карти, телефони/смартфони) без підтвердження таких дій з директором. Також можна впровадити систему контроль знімних носіїв і пристроїв (Device Control) - це дозволить контролювати і управляти процесом використання знімних носіїв і зовнішніх пристроїв будь-яких типів на робочих станціях користувачів і серверах корпоративної мережі. Як найпростіший приклад таких політик можна привести

дозвіл на підключення до комп'ютера корпоративних flash-карт і повна заборона на підключення та використання будь-яких інших носіїв.

Через відсутність контролю за діями системного адміністратора та порушення правил розмежування доступу (заступник директора фактично виконує ролі як системного адміністратора так і адміністратора безпеки) можливі несанкціоновані дій з боку заступника директора. Для того щоб зменшити ризики потрібно розділити ролі адміністраторів з мінімізацією функцій кожного так, щоб включати тільки ті функції, які необхідні для виконання даної ролі, та передати роль адміністратора безпеки довіреному персоналу – керівнику напрямку 2 чи директору (вони можуть виконувати цю роль, оскільки володіють потрібним рівнем знань та навичок). Наказ на суміщення відповідальності надан в ДОДАТКУ Б.

Через відсутність чіткого контролю за встановленням ПЗ працівниками, можливе використання ПЗ в власних цілях або занесення вірусу до комп'ютерної системи. Для того щоб зменшити ризики потрібно ввести постійні перевірки знань, та тести для підвищення кваліфікації, які будуть стосуватися всього персоналу, включаючи керівництво. Також ввести правило «DownloadRestrictions», щоб заборонити користувачам завантажувати підозрілі файли, такі як шкідливі програми та заражені файли. При цьому можна заборонити завантажувати всі файли або тільки ті, які Google (безпечний перегляд) визначає як небезпечні. При спробі завантажити такий файл користувачеві буде показано попередження, яке не можна буде обійти; ввести «білий список» сайтів в Інтернеті, які будуть відкритими для персоналу, інші – заблокувати; заборонити використання телефонів/смартфонів за робочим місцем; удосконалювати роботу з підбору та розстановки кадрів, а також заходи контролю за персоналом – це ускладнює можливість створення коаліцій порушників, тобто злочинного угрупування (змови) і цілеспрямованих дій з подолання системи захисту двох і більше порушників.

На підприємстві встановлена антивірусна програма Dr.WEB версії 12.0, але краще встановити антивірусну програму, яка затверджена експертним висновком –

програмний комплекс антивірусного захисту «Avast Business Antivirus» версії 19.X.Y виробництва компанії AVAST Software s.r.o. (Чеська республіка), експертний висновок №936, дійсний з 27.03.2019 до 27.03.2022. Ця програма відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Програмний комплекс антивірусного захисту «Avast Business Antivirus» версії 19», «Технічні вимоги щодо захисту інформації від несанкціонованого доступу».

Через відсутність контролю за останніми версіями ПЗ можливі хакерські дії на його вразливості. Було виявлено, що встановлено M.E.Doc версія 11.02.038 і не оновлено до останньої версії. Отже потрібно ввести чіткий контроль за своєчасним оновлення ПЗ – підключити функцію автоматичного оновлення в певний час (неробочі години) та більш чіткого контролю виконанням цієї функції системним адміністратором. Також, оскільки є можливість переглядати інформацію з екранів моніторів, потрібно ввести правило, яке забезпечує закриття в денний час жалюзі на вікнах. Це унеможливить переглядання інформації з сусідньої будівлі або за територією комплексу при наявності спеціальної техніки.

2.5 Аналіз загроз після впровадження програмно-організаційних рішень

Перелік загроз з визначенням порушень властивостей інформації та ІТС після впровадження програмно-організаційних рішень надано в таблиці 2.10.

Таблиця 2.10 – Перелік загроз з визначенням порушень властивостей інформації та ІТС після впровадження програмно-організаційних рішень

№	Загрози	Ймовірність	Ймовірні Збитки	Властивості		
				К	Ц	Д
1	Пожежа	Низька	Низькі	+	+	+
2	Затоплення	Низька	Низькі	+	+	+
3	Збої електроживлення	Низька	Низькі	-	+	+

Продовження таблиці 2.10 – Перелік загроз з визначенням порушень властивостей інформації та ІТС після впровадження програмно-організаційних рішень

№	Загрози	Ймовірність	Ймовірні Збитки	Властивості		
				К	Ц	Д
4	Пошкодження носіїв інформації	Низька	Високі	-	+	+
5	Несанкціонований доступ, викрадення носіїв інформації	Низька	Середні	+	+	+
6	Несанкціоноване підключення до технічних засобів	Низька	Середні	+	-	-
7	Несанкціоноване копіювання інформації на зовнішні носії	Низька	Середні	+	-	-
8	Створення клонів системи	Низька	Високі	+	-	+
9	Підслуховування	Низька	Низькі	+	-	-
10	Перегляд інформації з екранів моніторів через вікно	Низька	Низькі	+	-	-
11	Несанкціоновані дії системного адміністратора	Низька	Середні	+	+	+
12	Порушення правил розмежування доступу	Низька	Середні	+	+	+
13	Занесення вірусу до комп’ютерної системи	Низька	Середні	+	+	+
14	Використання стороннього ПЗ	Низька	Середні	-	+	+
15	Розголошення інформації персоналом ІТС	Середня	Низькі	+	-	-
16	Помилки персоналу ІТС	Низька	Низькі	+	-	-
17	Підкуп працівників підприємства з метою отримання ІзОД	Низька	Середні	+	+	+

Продовження таблиці 2.10 – Перелік загроз з визначенням порушень властивостей інформації та ІТС після впровадження програмно-організаційних рішень

№	Загрози	Ймовірність	Ймовірні Збитки	Властивості		
				К	Ц	Д
18	Використання вразливостей ПЗ	Низька	Середні	+	+	+
19	Несанкціоноване використання продуктів роботи та програм	Середня	Низькі	+	-	+

Рівні ймовірності загрози та збитків:

Високий – здійснення загрози призводить до великих збитків (3 бали);

Середній – здійснення загрози призводить до помірних збитків (2 бали);

Низький – здійснення загрози призводить до незначних збитків/їх нема (1 бал).

Порівнюючи з таблицею 2.9 – Перелік загроз з визначенням порушень властивостей інформації та ІТС, можемо зробити висновок, що знизилась ймовірність реалізації і збитки від збоїв електроживлення (було 5 – зараз 2), несанкціонованого доступу (4 – 3), викрадення носіїв інформації (4 – 3), несанкціонованого підключення до технічних засобів (5 – 3), несанкціонованого копіювання інформації на зовнішні носії (5 – 3), від перегляду інформації з екранів моніторів через вікно (3 – 2), несанкціонованих дій системного адміністратора (5 – 3), порушень правил розмежування доступу (5 – 3), використання вразливостей ПЗ (4 – 2), занесення вірусу до комп’ютерної системи (5 – 3), від використання стороннього ПЗ (5 – 3) та помилок персоналу (4 – 2).

2.6 Висновки до спеціальної частини

Ігнорування загроз та вразливостей інформаційно-телекомунікаційної системи може призвести до значних фінансових втрат та витоку інформації. Тому в другому розділі детально досліджено безпеку інформації на ІТС.

В ході виконання другого розділу розроблено модель порушника та модель загроз. Також обрано стандартний профіль захищеності, який використовується на підприємстві. Виявлено найбільш актуальні загрози, запропоновані організаційні та програмні рішення для їх мінімізації для підприємства «AdMark»: запропоновано джерело безперебійного живлення, ПЗ «Device Control», передано роль адміністратора безпеки керівнику напрямку 2, введено правило «DownloadRestrictions» та правило «білого списку», змінено програму антивірусного захисту та оновлено M.E.Doc, введено правило, яке забезпечує закриття в денний час жалюзі на вікнах.

Проведено аналіз та порівняння загроз до та після реалізації запропонованих рішень, а саме їх ймовірності та збитків, після впровадження проектних рішень.

ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічного розділу є підтвердження економічної доцільності впровадження комплексної системи захисту інформації інформаційно-телекомунікаційної системи ТОВ «AdMark» [13]. До розрахунків входить розрахунок капітальних витрат на придбання та налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення; розрахунок річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування; визначення річного економічного ефекту від впровадження об'єкта проектування; визначення та аналіз показників економічної ефективності запропонованого проектного рішення; підведення висновків щодо доцільності проектного рішення.

3.1 Розрахунок капітальних (фіксованих) витрат

3.1.1 Визначення трудомісткості розробки політики безпеки інформації

Трудомісткість розробки політики може бути розрахована на основі трудомісткості робіт, які виконуються.

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин}, \quad (3.1.1.1)$$

де $t_{тз}$ – тривалість складання ТЗ на розробку політики;

$t_{тз}$ = 13 годин;

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

$t_{в}$ = 14 годин;

$t_{а}$ – тривалість процесу аналізу ризиків

$t_{а}$ = 18 годин;

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

$t_{вз}$ = 9 годин;

$t_{озб}$ – тривалість виробу основних рішень з забезепечення безпеки інформації;

$t_{озб}$ = 19 годин;

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

$t_{овр}$ = 17 годин;

$t_д$ – тривалість документального оформлення політики безпеки;

$t_д$ = 8 годин.

t=13+14+18+9+19+17+8 = 98 годин.

3.1.2 Розрахунок витрат на створення політики безпеки інформації.

$$К_{рп} = З_{зп} + З_{мч}, \quad (3.1.2.1)$$

Де $К_{рп}$ – витрати на розробку політики безпеки інформації;

$З_{зп}$ – витрати на заробітну плату спеціалісту з інформаційної безпеки;

$З_{мч}$ – вартость витрат машинного часу, що необхідний для розробки політики.

$К_{рп}$ = 15974 + 345= 16319 грн.

Заробітна плата виконавця враховує основну і додаткову ЗП, відрахування на соціальні потреби.

$$З_{зп} = t*З_{іб}, \text{ грн}, \quad (3.1.2.2)$$

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

$З_{зп}$ = 98*163 = 15974 грн.

$$З_{мч} = t*С_{мч}, \text{ грн}, \quad (3.1.2.2)$$

де t – трудомісткість розробки політики на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

$З_{мч}$ = 98*3,52 = 344,96 грн.

$$C_{мч} = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot H_a}{F_p} + \frac{K_{лпз} \cdot H_{апз}}{F_p}, \text{ грн,} \quad (3.1.2.3)$$

Де Р – встановлена потужність ПК, кВт;

$t_{нал}$ – кількість задіяних робочих станцій пр написані політики;

C_e – тариф на електроенергію, грн./кВт*година;

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

H_a – річна норма амортизації на ПК, частки одиниці;

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$K_{лпз}$ – вартість ліцензійного прогрпмного забезпечення, грн;

F_p – річний фонд робочого часу (за 40-годинного робочого тижня F_p = 1920).

$C_{мч}$ = 0,7*2*1,68 + ((6879*0,3)/1920) + ((1958*0,1)/1920) = 3,52 грн.

На підприємстві ТОВ «AdMark» планується додатково використовувати програмні засоби наведені в таблиці 3.1.

Таблиця 3.1 – Додаткові програмні засоби

Програмний засіб	Вартість, грн
Avast Business Antivirus версії 19	838
Device Control	17380 (790*22=17380)
Всього	18218

Відповідно до прийнятих проектних рішень, на впровадження апаратних рішень витрати не виникають.

Капітальні (фіксовані) витрати на створення політики безпеки інформації:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н}, \quad (3.1.2.4)$$

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

$К_{пр} = 0$.

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

$К_{зпз} = 18218$ грн.

$К_{рп}$ – вартість розробки політики, тис. грн;

$К_{рп} = 16319$ грн.

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

$К_{аз} = 0$.

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

$К_{навч} = 2500$ грн.

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

$К_{н} = 0$.

$К = 0 + 18218 + 16319 + 0 + 2500 + 0 = 37037$ грн.

3.2 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – поточні витрати на обслуговування об’єкта проектування за визначений період.

Річні поточні витрати на функціонування системи інформаційної безпеки:

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн}, \quad (3.2.1)$$

де $С_{в}$ – вартість відновлення й модернізації системи;

$С_{в} = 628$ грн.

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

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки.

$С_{ак} = 0$.

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

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{єв} + С_{ел} + С_{о} + С_{тос}, \text{ грн}, \quad (3.2.2)$$

де $С_н$ – це витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації;

$С_н$ = 2500 грн.

$С_а$ – це річний фонд амортизаційних відрахувань визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів ($П_з$);

Вартість ПК, яка складає 26889 грн., ділимо на термін корисного використання, який складає 10 років, і отримаємо 2689 грн.

$С_а$ = 2689 грн.

$С_з$ – це річний фонд заробітної плати інженерно–технічного персоналу, що обслуговує систему інформаційної безпеки;

$$С_з = З_{осн} + З_{дод}, \text{ грн.}, \quad (3.2.3)$$

Де основна заробітна плата ($З_{осн}$) визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата ($З_{дод}$) – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата спеціаліста з інформаційної безпеки – 16319 грн./місяць.

Виконання робіт вимагає залучення спеціаліста з інформаційної безпеки на 0,25 ставки.

$С_з$ = (16319*12 + 16319*12*0,1)*0,25= 53853 грн.

З 01.12.2021 р. ставка ЄСВ (єдиний соціальний внесок) складає 22%.

$С_{єв}$ = 37037 * 0,22 = 8148 грн.

$С_{ел}$ – вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року;

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (3.2.4)$$

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.

$С_{ел}$ = 0,7*1920*1,68 = 2258 грн.

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1%.

$С_о$ – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування та сертифікацію обслуговуючого персоналу;

$С_о$ = 0.

$С_{тос}$ = 37037 *0,01 = 370 грн.

$С_к$ = 2500 + 2689 + 53853 + 8148 + 2258 + 370 = 69818 грн.

Річні поточні витрати на функціонування системи інформаційної безпеки складають 69818 грн.

3.3 Оцінка можливого збитку від атаки (взлому) на вузол або сегмент корпоративної мережі

3.3.1 Оцінка величини збитку

Вихідні дані для розрахунку:

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

$t_п$ = 2 години;

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

$t_в$ = 3 години;

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

$t_{ви}$ = 1.5 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.);

$З_о$ = 25400 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі;

$З_с$ = 20000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.);

$Ч_о$ = 1 особа;

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

$Ч_с$ = 22 особи;

О – обсяг збитку атакованого вузла або сегмента корпоративної мережі;

О = 5000000;

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

I – число атакованих сегментів корпоративної мережі;

I = 1;

N – середнє число атак на рік,

N = 7.

Упущена вигода від простою атакованого сегмента корпоративної мережі:

$$U = П_п + П_в + V, \quad (3.3.1.1)$$

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

$$П_п = \frac{\sum Зс}{F} \cdot t_п, \quad (3.3.1.2)$$

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

$П_п$ = ((20000 * 23)/176)*2 = 5227 грн,

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

$$П_в = П_{ви} + П_{пв} + П_{зч}, \quad (3.3.1.3)$$

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.

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви}, \quad (3.3.1.4)$$

$П_{ви}$ = ((20000 *23)/176) *1,5 = 3920 грн.

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_{в}, \quad (3.3.1.5)$$

$П_{пв}$ = ((25400 *1)/176) *3 = 433 грн.

$П_{в}$ = 3920 + 433 = 4353 грн.

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

$$V = \frac{O}{Fг} \cdot (t_{П} + t_{в} + t_{ви}), \quad (3.3.1.6)$$

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.

V = (500000/2080) * (2+3+1,5) = 15625 грн.

U = 5227 + 4353 + 15625 = 25205 грн.

Загальний збиток від атаки на сегмент корпоративної мережі організації:

$$B = \sum_i \sum_n U, \quad (3.3.1.7)$$

B = 1 * 7 * 25205 = 176435 грн.

3.3.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C, \text{ грн.}, \quad (3.3.2.1)$$

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

B = 176435 грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці;

R = 60 %;

C – щорічні витрати на експлуатацію системи інформаційної безпеки;

C = 73518 грн.

E = 176435 * 0,6 – 73518 = 32343 грн.

3.4 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:

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \quad (3.4.1)$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

E = 32343 грн.

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

K = 37037 грн.

ROSI = 32343 / 37037 = 0,87

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

$$ROSI > (N_{деп} – N_{інф})/100), \quad (3.4.2)$$

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

$N_{деп}$ = 8 %.

$N_{інф}$ – річний рівень інфляції;

$N_{інф}$ = 5 %.

Розрахункове значення коефіцієнта повернення інвестицій:

0,87> (8 – 5)/100 = 0,03

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

T = 1/0,87 = 1,1 років.

3.5 Висновки до економічного розділу

В цьому розділі проведено розрахунки капітальних (фіксованих) витрат на створення політики безпеки інформації, які складають 37037 грн.; розрахунки поточних (експлуатаційних) витрат на функціонування системи інформаційної безпеки, які складають 69818 грн.. Провели оцінювання можливого збитку від атаки (взлому) на вузол або сегмент корпоративної мережі, де визначили, що загальний збиток від атаки на сегмент корпоративної мережі організації складає 176435 грн.. Розрахували загальний ефект від впровадження системи інформаційної безпеки, який складає 32343 грн.. Згідно з коефіцієнтом повернення інвестицій ROSI, який показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки, який складає 0,87 на 1 грн., а також з терміном окупності капітальних інвестицій, який складає 1,1 років, можемо зробити висновок, що проектне рішення, яке прийняте на підприємстві «AdMark» економічно доцільне.

ВИСНОВКИ

На сьогоднішній день захист інформації – це основна задача для підприємств усіх напрямків розвитку, адже безпека інформації це безпека не тільки технічних інформаційних систем чи у чисельному або електронному вигляді, але стосується усіх аспектів захисту даних незалежно від форми, у якій вони перебувають.

Комплексні системи захисту інформації – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС. Згідно з законодавством України, інформація з обмеженим доступом підлягає обов'язковому захисту, вимоги до якого встановлені законом.

У процес створення КСЗІ обов'язково залучається організація, для якої здійснюється побудова КСЗІ – в кваліфікаційній роботі це ТОВ «AdMark».

В цій кваліфікаційній роботі показано наскільки вирішення питання безпеки інформації є важливим на підприємстві на прикладі ТОВ «AdMark».

В першому розділі надані загальні відомості та детально описано організаційну структуру підприємства. Проведено аналіз нормативно-правової бази, де обґрунтовано причини створення КСЗІ. В акті обстеження детально розглянуто ситуаційний та генеральний плани, також було проведено аналіз обчислювальної та інформаційної системи на підприємстві.

Згідно з даними першого розділу, в спеціальній частині обстежено модель порушника, модель загроз та профіль захищеності. Проаналізувавши ці дані, проведено розробку програмно-організаційних рішень для захисту інформації.

В економічному розділі провели основні розрахунки, результатом яких стало підтвердження економічної доцільності запропонованих проектних рішень.

ПЕРЕЛІК ПОСИЛАННЬ

1. Розумний маркетинг [Електронний ресурс] Режим доступу до ресурсу: https://martech.org/smart-marketing-still-hinges-on-humanity-not-technology/.

2. Як технології змінюють маркетинг [Електронний ресурс] Режим доступу до ресурсу: https://www.theguardian.com/media-network/media-network-blog/2014/sep/29/technology-changing-marketing-digital-media.

3. Створення комплексних систем захисту інформації [Електронний ресурс] Режим доступу до ресурсу: https://tzi.com.ua/stvorennya-kompleksnix-sistem-zaxistu-nformacz.html.

4. Закон України «Про інформацію» від 02.10.1992 No2657-XII // Відомості Верховної Ради України-1992-No 48. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12.

5. Закон України «Про захист персональних даних» від 01.06.2010 No 2297-VI // Відомості Верховної Ради України-2010-No 5. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17.

6. Закон України «Про захист інформації в інформаційно- телекомунікаційних системах» від 05.07.1994 No80-VI // Відомості Верховної Ради України-1994-No 80. [Електронний ресурс] Режим доступу до ресурсу: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 .

7. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. [Чинний від 08.11.2005] - К.: ДССЗЗІ, 2005- No125(Нормативний документ системи технічного захисту інформації).

8. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.[Чинний від 28.04.1999] - К.: ДСТСЗІ СБУ, 1999- No22 (Нормативний документ системи технічного захисту інформації).

9. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. [Чинний від 28.04.2000] - К.: ДСТСЗІ СБУ, 2000- No22 (Нормативний документ системи технічного захисту інформації).

10. НД ТЗІ 1.6-005 - Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. [Чинний від 15.04.2013] - К.: ДССЗЗІ, 2013-No125 (Нормативний документ системи технічного захисту інформації).

11. Етапи побудови КСЗІ [Електронний ресурс] Режим доступу до ресурсу: http://altersign.com.ua/korysna-informacija/pobudova-kszi/etapy-pobudovy-kszi.

12. Вадим Гребенніков «Комплексні системи захисту інформації. Проектування, впровадження, супровід» [Електронний ресурс] Режим доступу до ресурсу: https://ru.bookmate.com/books/dqaXNzVz?dscvr=top_result.

13. Методичні вказівки до виконання економічної частини дипломного проекту /Упорядн. Д. П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.

14. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / О.Ю. Гусєв, О.В. Герасіна, О.М. Алексеев, О.В. Кручинін – Дніпро: НГУ, 2018– 52

ДОДАТОК А. Перелік ДТЗ, ОТЗ та апаратних засобів підприємств

Таблиця 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
1	PC 1	Блок персонального комп’ютера	ARTLINE Business Plus B59 v21	56787	Робоче приміщення 1	0,80 м.
2	PC 1	2 Монітори персонального комп’ютера	21.5" HP Z22n G2 Display (1JS05A4)	76835 70899	Робоче приміщення 1	0,85 м.
3	PC 1	Клавіатура бездротова	HP Link-5 (T6U20AA)	93845	Робоче приміщення 1	0,95 м.
4	PC 2	Блок персонального комп’ютера	ARTLINE Business Plus B59 v21	10465	Робоче приміщення 1	1,60 м.
5	PC 2	2 Монітори персонального комп’ютера	21.5" HP Z22n G2 Display (1JS05A4)	47583 17272	Робоче приміщення 1	1,65 м.
6	PC 2	Клавіатура бездротова	HP Link-5 (T6U20AA)	76810	Робоче приміщення 1	1,75 м.
7	PC 3	Блок персонального комп’ютера	ARTLINE Business Plus B59 v21	67685	Робоче приміщення 1	0,45 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
8	PC 3	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	30506 28473	Робоче приміщення 1	0,50 м.
9	PC 3	Клавіатура бездротова	HP Link-5 (T6U20AA)	25593	Робоче приміщення 1	0,60 м.
10	PC 4	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	86990	Робоче приміщення 1	0,45 м.
11	PC 4	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	12422 28222	Робоче приміщення 1	0,50 м.
12	PC 4	Клавіатура бездротова	HP Link-5 (T6U20AA)	45211	Робоче приміщення 1	0,60 м.
13	PC 5	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	61049	Робоче приміщення 1	0,45 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
14	PC 5	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	19194 20299	Робоче приміщення 1	0,50 м.
15	PC 5	Клавіатура бездротова	HP Link-5 (T6U20AA)	14839	Робоче приміщення 1	0,60 м.
16	PC 6	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	69706	Робоче приміщення 1	0,45 м.
17	PC 6	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	59609 89009	Робоче приміщення 1	0,50 м.
18	PC 6	Клавіатура бездротова	HP Link-5 (T6U20AA)	14145	Робоче приміщення 1	0,60 м.
19	PC 7	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	69089	Робоче приміщення 1	2,64 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
20	PC 7	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	13940 77333	Робоче приміщення 1	2,70 м.
21	PC 7	Клавіатура бездротова	HP Link-5 (T6U20AA)	22230	Робоче приміщення 1	2,80 м.
22	PC 8	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	42531	Робоче приміщення 1	2,64 м.
23	PC 8	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	98808 77007	Робоче приміщення 1	2,70 м.
24	PC 8	Клавіатура бездротова	HP Link-5 (T6U20AA)	10890	Робоче приміщення 1	2,80 м.
25	PC 9	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	60345	Робоче приміщення 1	2,64 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
26	PC 9	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	90876 39909	Робоче приміщення 1	2,70 м.
27	PC 9	Клавіатура бездротова	HP Link-5 (T6U20AA)	16781	Робоче приміщення 1	2,80 м.
28	PC 10	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	65758	Робоче приміщення 1	3,32 м.
29	PC 10	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	29503 77995	Робоче приміщення 1	3,40 м.
30	PC 10	Клавіатура бездротова	HP Link-5 (T6U20AA)	18921	Робоче приміщення 1	3,50 м.
31	PC 11	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	32950	Робоче приміщення 2	0,80 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
32	PC 11	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	70005 18898	Робоче приміщення 2	0,85 м.
33	PC 11	Клавіатура бездротова	HP Link-5 (T6U20AA)	80576	Робоче приміщення 2	0,95 м.
34	PC 12	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	13375	Робоче приміщення 2	2,80 м. 3,60 м.
35	PC 12	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	18475 90005	Робоче приміщення 2	2,85 м. 3,65 м.
36	PC 12	Клавіатура бездротова	HP Link-5 (T6U20AA)	29756	Робоче приміщення 2	2,95 м. 3,75м.
37	PC 13	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	14759	Робоче приміщення 2	2,80 м. 4,08 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
38	PC 13	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	19575 24353	Робоче приміщення 2	2,85 м. 4,15 м.
39	PC 13	Клавіатура бездротова	HP Link-5 (T6U20AA)	19755	Робоче приміщення 2	2,95 м. 4,25 м.
40	PC 14	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	59639	Робоче приміщення 2	0,80 м. 1,70 м.
41	PC 14	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	19505 20032	Робоче приміщення 2	0,85 м. 1,75 м.
42	PC 14	Клавіатура бездротова	HP Link-5 (T6U20AA)	18365	Робоче приміщення 2	0,95 м. 1,85 м.
43	PC 15	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	38673	Робоче приміщення 2	0,80 м. 0,90 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
44	PC 15	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	29604 90121	Робоче приміщення 2	0,85 м. 0,95 м.
45	PC 15	Клавіатура бездротова	HP Link-5 (T6U20AA)	28575	Робоче приміщення 2	0,95 м. 1,05 м.
46	PC 16	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	19576	Робоче приміщення 2	4,00 м. 1,70 м.
47	PC 16	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	12959 18187	Робоче приміщення 2	4,05 м. 1,75м.
48	PC 16	Клавіатура бездротова	HP Link-5 (T6U20AA)	47896	Робоче приміщення 2	4,15 м. 1,85 м.
49	PC 17	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	19054	Робоче приміщення 2	4,00 м. 0,90 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
50	PC 17	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	19840 10223	Робоче приміщення 2	4,05 м. 0,95 м.
51	PC 17	Клавіатура бездротова	HP Link-5 (T6U20AA)	13468	Робоче приміщення 2	4,15 м. 1,00 м.
52	PC 18	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	21333	Робоче приміщення 2	6,80 м. 1,70 м.
53	PC 18	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	15790 80089	Робоче приміщення 2	6,80 м. 1,70 м.
54	PC 18	Клавіатура бездротова	HP Link-5 (T6U20AA)	77001	Робоче приміщення 2	6,80 м. 1,70 м.
55	PC 19	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	89080	Робоче приміщення 2	6,80 м. 0,90 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
56	PC 19	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	78133 77707	Робоче приміщення 2	6,85 м. 0,95 м.
57	PC 19	Клавіатура бездротова	HP Link-5 (T6U20AA)	69134	Робоче приміщення 2	6,95 м. 1,05 м.
58	PC 20	Блок персонального комп'ютера	ARTLINE Business Plus B59 v21	46890	Робоче приміщення 2	7,44 м. 3,80 м.
59	PC 20	2 Монітори персонального комп'ютера	21.5" HP Z22n G2 Display (1JS05A4)	55542 10021	Робоче приміщення 2	7,50 м. 3,85 м.
60	PC 20	Клавіатура бездротова	HP Link-5 (T6U20AA)	12426	Робоче приміщення 2	7,60 м. 3,95 м.
61	PC 21	Блок персонального комп'ютера	ARTLINE WorkStation W75 v15	37593	Робоче приміщення керівника напрямку 1	0,90 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
62	PC 21	2 Монітори персонального комп'ютера	27" Samsung Curved C27F396F (LC27F396F HIXCI)	92030 10909	Робоче приміщення керівника напрямку 1	0,95 м.
63	PC 21	Клавіатура бездротова	Logitech K270 (920-003757)	58794	Робоче приміщення керівника напрямку 1	1,00 м.
64	PC 21	З'ємний SSD	Samsung T7 TOUCH 2TB USB 3.2 Type-C (MU-PC2T0K/WW	97855	Робоче приміщення керівника напрямку 1	0,90 м.
65	PC 22	Блок персонального комп'ютера	ARTLINE WorkStation W75 v15	72624	Робоче приміщення керівника напрямку 2	0,90 м.
66	PC 22	2 Монітори персонального комп'ютера	27" Samsung Curved C27F396F (LC27F396F HIXCI)	10293 70383	Робоче приміщення керівника напрямку 2	0,95 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
67	PC 22	Клавіатура бездротова	Logitech K270 (920-003757)	13245	Робоче приміщення керівника напрямку 2	1,00 м.
68	PC 22	З'ємний SSD	Samsung T7 TOUCH 2TB USB 3.2 Type-C (MU-PC2T0K/WW	57691	Робоче приміщення керівника напрямку 2	0,90 м.
69	PC 23	Блок персонального комп'ютера	ARTLINE WorkStation W75 v15	39586	Робоче приміщення керівника напрямку 3	0,90 м. 2,40 м.
70	PC 23	2 Монітори персонального комп'ютера	27" Samsung Curved C27F396F (LC27F396F HIXCI)	68729 22721	Робоче приміщення керівника напрямку 3	0,95 м. 2,45 м.
71	PC 23	Клавіатура бездротова	Logitech K270 (920-003757)	11949	Робоче приміщення керівника напрямку 3	1,05 м. 2,55 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
72	PC 23	З'ємний SSD	Samsung Portable SSD T7 TOUCH 2TB USB 3.2 Type-C (MU-PC2T0K/WW	22552	Робоче приміщення керівника напрямку 3	0,90 м. 2,40 м.
73	PR_ 1	Принтер МФП (Багатофункціональний пристрій)	HP LaserJet Pro M428dw with Wi-Fi, Ethernet, ADF (W1A28A)	67800	Робоче приміщення 1	0,80 м. 0,40 м.
74	PR_ 2	Принтер МФП (Багатофункціональний пристрій)	HP LaserJet Pro M428dw with Wi-Fi, Ethernet, ADF (W1A28A)	37589	Робоче приміщення 2	0,80 м. 0,40 м.
75	PR_ 3	Принтер	HP Neverstop Laser 1000w (4RY23A)	18476	Робоче приміщення керівника напрямку 1	0,40 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
76	PR_4	Принтер	HP Neverstop Laser 1000w (4RY23A)	47728	Робоче приміщення керівника напрямку 2	0,40 м.
77	PR_5	Принтер	HP Neverstop Laser 1000w (4RY23A)	35589	Робоче приміщення керівника напрямку 3	0,40 м. 2,40 м.
78	Switch	Комутатор	D-Link DGS-3000-28SC	67301	Робоче приміщення 1	4,15 м.
79	Router	Маршрутизатор	D-Link N300 (DWR-921)	10190	Робоче приміщення 1	4,15 м.
80	ATC	Автоматична телефонна станція	KX-NS500UC	78460	Робоче приміщення 2	0,20 м. 4,60 м.

Продовження таблиці 1 – Основні технічні засоби на підприємстві «AdMark»

№	На-зва	Складові	Марка	Серійний номер	Розміщення	Відстань до границі ОІД
81	Tf 1	Телефон	Panasonic KX-NT630RU-B Black	66240	Робоче приміщення 1	3,84 м.
82	Tf 2	Телефон	Panasonic KX-NT630RU-B Black	20002	Робоче приміщення 1	4 м.
83	Tf 3	Телефон	Panasonic KX-NT630RU-B Black	14350	Робоче приміщення 2	0,60 м. 3,80 м.
84	Tf 4	Телефон	Panasonic KX-NT630RU-B Black	29048	Робоче приміщення 2	4,60 м.

Таблиця 2 – Характеристика допоміжних технічних засобів підприємства «AdMark»

№	Назва	Марка	Серійний номер	Розміщення
1	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	69337	Робоче приміщення 1 (на столах з правої сторони від клавіатури)
2	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	87958	Робоче приміщення 1 (на столах з правої сторони від клавіатури)
3	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	28565	Робоче приміщення 1 (на столах з правої сторони від клавіатури)
4	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	28576	Робоче приміщення 1 (на столах з правої сторони від клавіатури)
5	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	29076	Робоче приміщення 1 (на столах з правої сторони від клавіатури)

Продовження таблиці 2 – Характеристика допоміжних технічних засобів підприємства «AdMark»

№	Назва	Марка	Серійний номер	Розміщення
6	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	28565	Робоче приміщення 1 (на столах з правої сторони від клавіатури)
7	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	28576	Робоче приміщення 1 (на столах з правої сторони від клавіатури)
8	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	29076	Робоче приміщення 1 (на столах з правої сторони від клавіатури)
9	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	67587	Робоче приміщення 1 (на столах з правої сторони від клавіатури)
10	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	75668	Робоче приміщення 1 (на столах з правої сторони від клавіатури)

Продовження таблиці 2 – Характеристика допоміжних технічних засобів підприємства «AdMark»

№	Назва	Марка	Серійний номер	Розміщення
11	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	80908	Робоче приміщення 2 (на столах з правої сторони від клавіатури)
12	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	14211	Робоче приміщення 2 (на столах з правої сторони від клавіатури)
13	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	44530	Робоче приміщення 2 (на столах з правої сторони від клавіатури)
14	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	12332	Робоче приміщення 2 (на столах з правої сторони від клавіатури)
15	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	88080	Робоче приміщення 2 (на столах з правої сторони від клавіатури)

Продовження таблиці 2 – Характеристика допоміжних технічних засобів підприємства «AdMark»

№	Назва	Марка	Серійний номер	Розміщення
16	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	24422	Робоче приміщення 2 (на столах з правої сторони від клавіатури)
17	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	14450	Робоче приміщення 2 (на столах з правої сторони від клавіатури)
18	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	70978	Робоче приміщення 2 (на столах з правої сторони від клавіатури)
19	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	13212	Робоче приміщення 2 (на столах з правої сторони від клавіатури)
20	Мишка бездротова	HP Z4000 Wireless Black/Silver (H5N61AA)	57890	Робоче приміщення 2 (на столах з правої сторони від клавіатури)

Продовження таблиці 2 – Характеристика допоміжних технічних засобів підприємства «AdMark»

№	Назва	Марка	Серійний номер	Розміщення
21	Мишка бездротова	Logitech M330 Silent Plus Wireless Black (910-004909)	66547	Робоче приміщення керівника напрямку 1 (на столах з правої сторони від клавіатури)
22	Мишка бездротова	Logitech M330 Silent Plus Wireless Black (910-004909)	76755	Робоче приміщення керівника напрямку 2 (на столах з правої сторони від клавіатури)
23	Мишка бездротова	Logitech M330 Silent Plus Wireless Black (910-004909)	98870	Робоче приміщення керівника напрямку 3 (на столах з правої сторони від клавіатури)
24	Камера відеоспосте-реження	Камера Hikvision DS-2CC52H1T-FITS	67456	Коридор

Продовження таблиці 2 – Характеристика допоміжних технічних засобів підприємства «AdMark»

№	Назва	Марка	Серійний номер	Розміщення
25	Датчики диму	Артон СПД-3.4.	34656	Кухня
26	Датчики диму	Артон СПД-3.4.	23132	Робоче приміщення 1
27	Датчики диму	Артон СПД-3.4.	13234	Робоче приміщення 1
28	Датчики диму	Артон СПД-3.4.	16411	Вбиральня чоловіча
29	Датчики диму	Артон СПД-3.4.	33600	Вбиральня жіноча
30	Датчики диму	Артон СПД-3.4.	27763	Коридор
31	Датчики диму	Артон СПД-3.4.	37452	Коридор
32	Датчики диму	Артон СПД-3.4.	30400	Робоче приміщення 2
33	Датчики диму	Артон СПД-3.4.	37467	Робоче приміщення 2
34	Датчики диму	Артон СПД-3.4.	93749	Склад
35	Датчики диму	Артон СПД-3.4.	38477	Робоче приміщення керівника напрямку 1

Продовження таблиці 2 – Характеристика допоміжних технічних засобів підприємства «AdMark»

№	Назва	Марка	Серійний номер	Розміщення
36	Датчики диму	Артон СПД-3.4.	70099	Робоче приміщення керівника напрямку 2
37	Датчики диму	Артон СПД-3.4.	60112	Робоче приміщення керівника напрямку 3
38	Датчики відкриття/ розбиття скла	Philio PST02-A - Z-Wave	35454	Робоче приміщення керівника напрямку 1
39	Датчики відкриття/ розбиття скла	Philio PST02-A - Z-Wave	38575	Робоче приміщення керівника напрямку 2
40	Датчики відкриття/ розбиття скла	Philio PST02-A - Z-Wave	33434	Робоче приміщення керівника напрямку 3
41	Датчики відкриття/ розбиття скла	Philio PST02-A - Z-Wave	14153	Робоче приміщення 2
42	Датчики відкриття/ розбиття скла	Philio PST02-A - Z-Wave	10193	Робоче приміщення 2
43	Магніто-контактний датчик на двері	ЭСМК-8	46686	Внутрішня сторона вхідних дверей

Продовження таблиці 2 – Характеристика допоміжних технічних засобів підприємства «AdMark»

№	Назва	Марка	Серійний номер	Розміщення
44	Інфрачер-воний датчик	Feron sen11 / lx39	85746	В коридорі на стіні
45	Світло-звукова сигналізація	MAKS Siren White	46587	Зовнішня сторона вхідних дверей
46	ПКП	Лунь-9Р	67680	Біля вхідних дверей з внутрішньої сторони
47	Світлодіодні лампи	MAXI-1	79808	Кухня
48	Світлодіодні лампи	MAXI-1	96968	Робоче приміщення 1
49	Світлодіодні лампи	MAXI-1	45680	Робоче приміщення 1
50	Світлодіодні лампи	MAXI-1	10040	Робоче приміщення 1
51	Світлодіодні лампи	MAXI-1	28586	Робоче приміщення 1
52	Світлодіодні лампи	MAXI-1	87879	Вбиральня чоловіча
53	Світлодіодні лампи	MAXI-1	52546	Вбиральня жіноча
54	Світлодіодні лампи	MAXI-1	55458	Коридор

Продовження таблиці 2 – Характеристика допоміжних технічних засобів підприємства «AdMark»

№	Назва	Марка	Серійний номер	Розміщення
55	Світлодіодні лампи	MAXI-1	07989	Коридор
56	Світлодіодні лампи	MAXI-1	14242	Коридор
57	Світлодіодні лампи	MAXI-1	41423	Робоче приміщення 2
58	Світлодіодні лампи	MAXI-1	75645	Робоче приміщення 2
59	Світлодіодні лампи	MAXI-1	14141	Робоче приміщення 2
60	Світлодіодні лампи	MAXI-1	14243	Робоче приміщення 2
61	Світлодіодні лампи	MAXI-1	24355	Склад
62	Світлодіодні лампи	MAXI-1	73545	Робоче приміщення керівника напрямку 1
63	Світлодіодні лампи	MAXI-1	79800	Робоче приміщення керівника напрямку 2
64	Світлодіодні лампи	MAXI-1	98000	Робоче приміщення керівника напрямку 3

Таблиця 3 – Характеристика складу ІТС підприємства «AdMark»

№	Назва	Характеристики	Інвентар. номер	Відповідальний
1	PC 1	Intel Core i7-9700 (3.0 - 4.7 ГГц) RAM 16 ГБ SSD 480 ГБ Intel UHD Graphics 630 Діагональ дисплею 21.5" Споживча потужність Макс. 30 Вт, Стандарт: 17 Вт Режим очікування: 0.5Вт Габарити монітора, маса З підставкою: 48.83 x 20.5 x 44.87 см, 5.3 кг	001	Мен. напрям 1
2	PC 2		002	Мен. напрям 1
3	PC 3		003	Мен. напрям 1
4	PC 4		004	Мен. напрям 1
5	PC 5		005	Мен. напрям 1
6	PC 6		006	Мен. напрям 1
7	PC 7		007	Мен. напрям 1
8	PC 8		008	Мен. напрям 1
9	PC 9		009	Мен. напрям 1
10	PC 10		010	Бухгалтер
11	PC 11		011	Бухгалтер
12	PC 12		012	Мен. напрям 2
13	PC 13		013	Мен. напрям 2
14	PC 14		014	Мен. напрям 2
15	PC 15		015	Мен. напрям 2
16	PC 16		016	Мен. напрям 2
17	PC 17		017	Мен. напрям 2
18	PC 18		018	Мен. напрям 2
19	PC 19		019	Мен. напрям 2
20	PC 20		020	Мен. напрям 2

Продовження таблиці 3 – Характеристика складу ІТС підприємства «AdMark»

№	Назва	Характеристики	Інвентари-заційний номер	Відповідальний
21	PC 21	Intel Core i7-10700F (2.9 - 4.8 ГГц) RAM 64 ГБ HDD 2 ТБ + SSD 480 ГБ nVidia GeForce RTX 3060, 12 ГБ Діагональ дисплею 27" Споживча потужність 25 Вт В режиме очікування: 0.3 Вт Габарити монітору, маса З підставкою: 622.9 x 466.2 x 242.6 мм, 4.1 кг	021	Керівник напрямку 1 Директор
22	PC 22		022	Заступник директора
23	PC 23		023	Керівник напрямку 2
24	Комутатор Switch	Порти: 20 SFP, 4 SFP комбінований, VLAN 4 x 10GBase-X SFP+1x Консольний порт RJ-45 1 x Роз'єм RPS для резервного джерела жив. Об'єм ОП: 256 МБ Flash-пам'ять: 32 МБ	231	Заступник директора

Продовження таблиці 3 – Характеристика складу ІТС підприємства «AdMark»

№	Назва	Характеристики	Інвентари-заційний номер	Відповідальний
25	Маршрутизатор Router	1xRJ-45 10/100BASE-TX WAN, 4xRJ-45 10/100 BASE-TX LAN Стандарт зв'язку Wi-Fi 802.11b / g / a Швидкість Wi-Fi 300 Мбіт/с, Процесор: MT7620N 600 МГц ОП: 64 МБ, DDR SDRAM, підтримка VLAN	15	Заступник директора
26	АТС	6 зовнішніх і 18 внутрішніх ліній; До 64 зовнішніх SIP-ліній; До 32 зовнішніх IP-ліній (по протоколу H.323); До 128 SIP / IP / SIP-DECT-телефонів; До 32 базових станцій; Підтримка передачі відео для внутрішніх SIP-абонентів (програмних і апаратних).	781	Бухгалтер

Продовження таблиці 3 – Характеристика складу ІТС підприємства «AdMark»

№	Назва	Характеристики	Інвентаризац. номер	Відповідальний
27	Принтер PR_1	Лазерний друк, БФП HP FastRes1200 Чорно-білий ,Споживча потужність 510 Вт активний стан, друк, 7.5 Вт режим готовності 0.9 Вт сплячий режим. Вага 12.6 кг, Розміри 430 x 634 x 325 мм	112	Бухгалтер
28	Принтер PR_2		113	Бухгалтер
29	Принтер PR_3	Лазерний друк, Принтер, Чорно-білий, Споживча потужність 365 Вт активний стан\друк 2.8 Вт режим готовності, 0.6 Вт сплячий режим. Вага 6.95 кг, Стандартний об'єм пам'яті: 32 Мбайт Розміри, мм 380.5 x 293.4 x 211	114	Керівник напрямку 1
30	Принтер PR_4		115	Керівник напрямку 2
31	Принтер PR_5		116	Керівник напрямку 3

ДОДАТОК Б. Наказ на суміщення відповідальності

Товариство з обмеженною відповідальністю «AdMark»

НАКАЗ

«___»_____ Дніпро №_____

Про запровадження
суміщення відповідальності
у товаристві з обмеженною відповідальністю
«AdMark»

ДОРУЧИТИ:

Корневиру Дмитру Павловичу, керівнику напрямку 2, без увільнення його від основної роботи, обумовленної трудовим договором, виконання додаткової роботи на умовах суміщення за посадою адміністратора безпеки зі щомісячною доплатою в розмірі 50% посадового окладу, з дати підписання наказу.

Директор товариства _____ Глущенко А.І.

ДОДАТОК В. 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	2	
5	А4	1 Розділ	28	
6	А4	Спеціальна частина	17	
7	А4	Економічний розділ	9	
8	А4	Висновки	1	
9	А4	Список літератури	2	
10	А4	Додаток А	28	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	2	

ДОДАТОК Г. Перелік документів на оптичному носії

1. Пояснювальна_записка_Шуклінова.doc
2. Пояснювальна_записка_Шуклінова.pdf
3. Презентація_Шуклінова.pptx

ДОДАТОК Ґ. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

ДОДАТОК Д. Відгук керівника кваліфікаційної роботи

Відгук

на кваліфікаційну роботу студенки групи 125-17-2

Шуклінової Дарини Анатоліївни

на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ "AdMark"»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 71 сторінці.

Метою кваліфікаційної роботи є підвищити рівень захисту інформації в інформаційно-телекомунікаційній системі ТОВ «AdMark».

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 нормативно-правової бази у сфері забезпечення кібербезпеки; аналіз організаційної структури; аналіз інформаційно-обчислювальної системи; складено акт обстеження.

Розроблено рекомендації по впровадженню організаційно-програмних рішень для підвищення безпеки інформації на ТОВ «AdMark».

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня захисту інформації в інформаційно-телекомунікаційній системі ТОВ «AdMark».

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Шуклінова Д.А. проявила 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 « відмінно ».

Керівник кваліфікаційної роботи:
Керівник: Ас. Мілінчук Ю.А.