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

студента *Куця Максима Олеговича*

академічної групи *125-20-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-комунікаційної системи магазину роздрібної торгівлі «GetApple»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст.викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.	92	відмінно	
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Куцю Максиму Олеговичу*** **академічної групи** ***125-20-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Комплексна система захисту інформації інформаційно-комунікаційної системи магазину роздрібної торгівлі «GetApple»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.24 р. № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Обстеження ІКС. Формування вимог до захисту від НСД	15.03.2024
Розділ 2	Аналіз профілю захищеності. Обґрунтування заходів щодо реалізації послуг безпеки	10.05.2024
Розділ 3	Обґрунтування економічної доцільності впровадження КСЗІ	11.06.2024

Завдання видано _____ Олександр КРУЧІНІН
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 01.07.2024р.

Прийнято до виконання _____ Максим КУЦЬ
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 89 с., 6 рис., 35 табл., 8 додатків, 7 джерел.

Об’єкт розробки: інформаційно-комунікаційна система магазину роздрібної торгівлі «GetApple».

Предмет розробки: комплексна система захисту інформації.

Мета роботи: забезпечення необхідного рівня захисту інформації, що циркулює в інформаційно-комунікаційній системі магазину роздрібної торгівлі «GetApple».

У першому розділі було вказано основні відомості по об’єкту, який розглядається, наведено обґрунтування необхідності створення КСЗІ, проведено обстеження середовищ функціонування, таких як: фізичне середовище, обчислювальне середовище, інформаційне середовище та середовище користувачів. Далі було розроблено модель порушника та модель загроз. В кінці розділу було сформовано профіль захищеності на основі визначених актуальних загроз.

У другому розділі було виконано аналіз наведеного профілю захищеності та виконано обґрунтування заходів щодо реалізації послуг безпеки.

У третьому розділі було виконано розрахунок економічних показників щодо доцільності впровадження комплексної системи захисту інформації на підприємстві «GetApple».

Практична цінність розробки полягає у забезпеченні захисту інформації з обмеженим доступом.

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ.

ABSTRACT

Explanatory note: 89 pp., 6 pic., 35 table, 8 app, 7 sources.

Object of development: information and communication system of the retail store "GetApple".

Subject of development: comprehensive information protection system.

Purpose: to ensure the required level of protection of information circulating in the information and communication system of the retail store "GetApple".

In the first section, the basic information on the object under consideration was given, the justification for the need to create an CIPS was given, and a survey of the operating environments, such as the physical environment, computing environment, information environment, and user environment, was conducted. Next, a model of an intruder and a model of threats were developed. At the end of the section, a security profile was formed based on the identified threats.

The second section analyzed the security profile and justified the measures to implement security services.

In the third section, economic indicators were calculated to determine the feasibility of implementing a comprehensive information security system at the GetApple enterprise.

The practical value of the development is to ensure the protection of information with limited access.

SECURITY POLICY, THREAT MODEL, INTRUDER MODEL, INFORMATION SYSTEM, CYBERSECURITY, COMPREHENSIVE INFORMATION PROTECTION SYSTEM.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІКС – інформаційно-комунікаційна система;

ІС – інформаційна система;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КС – комп’ютерна система;

КСЗІ – комплексна система захисту інформації;

НД ТЗІ – нормативний документ технічного захисту інформації;

НСД – несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер.

ЗМІСТ

с.

ВСТУП

Актуальність полягає в тому, що інформаційні технології дуже стрімко розвиваються та все більше підприємств застосовують інформаційні технології в своїй роботі, але з більшим застосуванням інформаційних технологій підвищується ризик, що хтось може отримати несанкціонований доступ до інформації, що циркулює на підприємстві. Тому для підприємств стає необхідним покращення кіберзахисту в своїй системі. Для впевненості в захисті своєї інформації потрібен організований систематичний захист, який може забезпечити впровадження комплексної системи захисту інформації.

Об'єкт розробки: інформаційно-комунікаційна система магазину роздрібної торгівлі «GetApple».

Предмет розробки: комплексна система захисту інформації.

Мета роботи: забезпечення необхідного рівня захисту інформації, що циркулює в інформаційно-комунікаційній системі магазину роздрібної торгівлі «GetApple».

Завдання роботи включають:

1. Визначення відомостей про підприємство.
2. Обстеження середовищ функціонування.
3. Розробка моделі загроз та моделі порушника.
4. Формування та подальший аналіз профілю захищеності.
5. Обґрунтування заходів щодо реалізації послуг безпеки.
6. Розрахунок економічних показників доцільності впровадження КСЗІ.

Практичне значення роботи полягає у забезпеченні захисту інформації з обмеженим доступом.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про підприємство

Компанія GetApple – займається продажем та сервісним обслуговуванням оригінальної оновленої техніки Apple. Вся техніка проходить діагностику, ретельну перевірку, тестування. Вона має сертифікацію від сервісного центру та оригінальну пломбу на кожному пристрої.

Свою роботу компанія розпочала в 2017 році. В середньому оборот коштів на місяць може становити, близько, 2,5 мільйонів гривень.

Компанія має фізичні магазини в Києві та Дніпрі. Розглядається магазин розташований в місті Дніпро. Також у компанії є свій інтернет-магазин.

В штаті працюють:

– менеджери з продажу;

– прожект-менеджер;

– спеціалісти колцентру;

– бухгалтер;

– логіст;

– СММ-спеціаліст;

– контент-мейкер.

1.2 Обгрунтування створення КСЗІ

Необхідність забезпечення захисту інформації, та безпосередньо створення КСЗІ в ІКС визначається передусім вимогами нормативно-правових документів та в деяких випадках власником інформації.

На підприємстві обробляється інформація з обмеженим доступом. Сюди може входити, як конфіденційна інформація, яка постійно генерується при взаємодії з клієнтами, так і інформація яка необхідна для функціонування системи.

Згідно з Законом України «Про захист інформації в інформаційно-комунікаційних системах» [1, с. 8]:

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.

Згідно з Законом України «Про захист інформації в інформаційно-комунікаційних системах» [1, с. 9]:

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Згідно постанови «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» [2, п. 16]:

Для забезпечення захисту інформації в системі створюється комплексна система захисту інформації (далі – система захисту), яка призначається для захисту інформації від:

– витоку технічними каналами;

– несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

– спеціального впливу на засоби обробки інформації.

Відповідно до проведеного аналізу необхідно прийняти рішення із створення КСЗІ.

1.3 Обстеження середовищ функціонування

1.3.1 Обстеження фізичного середовища

Опис ситуаційного плану:

Деяка інформація була змінена, але це не впливає на роботу в цілому.

ОІД – об’єкт, що знаходиться на першому поверсі п’ятиповерхової будівлі за адресою: місто Дніпро, Шевченківський район, вулиця Центральна, 25.

Контрольована зона обмежена периметром приміщення. Перепускний режим реалізовано наступним чином, в робочий час за людьми, що входять слідкує менеджер, який знаходиться в торгівельній залі, а також за допомогою камери відеоспостереження ведеться постійний нагляд за зоною перед входом в приміщення. Охорона території відсутня. Контроль доступу в не робочий час забезпечено за рахунок замикання вхідних дверей та встановленої сигналізації.

Приміщення має розміри 13м × 6м, загальна площа приміщення 78м^2, висота 2.9м, ОІД включає в себе три кімнати (торгівельна зала, склад, кухня).

Несучі стіни зроблені з цегли, ширина стін 30 см. Перекриття зроблені з використанням залізобетонних плит.

До приміщення присутній один вхід, на якому встановлено розпашні алюмінієві двері. Заповнення виконано з прозорого ударостійкого скла. Двері оснащені врізним циліндровим замком. На дверях встановлено магніто-контактний датчик, який реагує на відкриття дверей. Всередині приміщення використовуються міжкімнатні дерев'яні двері. Оснащені врізним замком.

Ситуаційний план наведено в Додатку Б.

Опис навколишніх будівель наведено в табл. 1.1.

Таблиця 1.1 – Опис навколишніх будівель

№ будівлі	Відстань та розміщення відносно ОІД	Адреса	Опис
1	0м	вул. Центральна, 25	Житлова будівля
2	0м, ПД-СХ	вул. Центральна, 26	Житлова будівля
3	33м, ПД	вул. Сонячна, 10	Житлова будівля
4	20м, ПН-ЗХ	–	Господарча будівля
5	15м, ПД-ЗХ	–	Господарча будівля
6	12м, ПД-ЗХ	–	Господарча будівля
7	40м, ПН-ЗХ	вул. Смарагдова, 8	Ресторан
8	24м, ПД-ЗХ	–	Господарча будівля
9	33м, ПД	–	Господарча будівля

Продовження таблиці 1.1

№ будівлі	Відстань та розміщення відносно ОІД	Адреса	Опис
10	26м, ЗХ	вул. Смарагдова, 9	Адміністративна будівля
11	43м, ПД-ЗХ	вул. Весняна, 15	Медичний заклад
12	52м, ПД	вул. Сонячна, 11	Житлова будівля
13	43м, ПД-ЗХ	вул. Весняна, 16	Житлова будівля

Характеристика комунікацій:

Опалення автономне електричне. Для опалення використовується кондиціонер та два обігрівача.

Системи водопостачання та каналізації – централізовані та входять/виходять від підвалу будівлі в якій знаходиться ОІД. Лінія системи водопостачання йде по металевій трубі, що заходить в приміщення, після лічильника йде пластикова труба. Каналізаційні труби з ПВХ.

Від трансформаторної підстанції (ТП-188) електропостачання надходить до будівлі підземними комунікаціями в якій знаходиться ОІД та заходить в підвал. До щитової приміщення електроживлення йде від розподільної електрощитової, що знаходиться на першому поверсі будівлі в під'їзді за межами КЗ. Елементи системи електропостачання (розетки) в приміщенні заземлені (йдуть 3 дроти), які підключені до щитової приміщення.

Встановлена система охоронно-пожежної сигналізації. Підключена до щитової приміщення. ПКП розташований перед виходом з ОІД. Сигнал до охоронної служби передається за допомогою GSM модулю.

Система мережі Інтернет – від Інтернет-провайдеру «Prosto». Оптоволоконний кабель надходить до приміщення від розподільного щитка, який знаходиться на першому поверсі будівлі в під'їзді за межами КЗ.

Опис генерального плану наведеного в Додатку В:

ОІД складається з трьох кімнат – торгівельна зала, склад (включає в себе також зону для зйомки товару та робочу зону), кухня. З півночі межує з наразі пустим приміщенням. З північного заходу межує з під'їздом будівлі.

З південного сходу розміщується сусідня житлова будівля. З південного заходу розміщений двір. Вище по поверхам розташовані житлові приміщення.

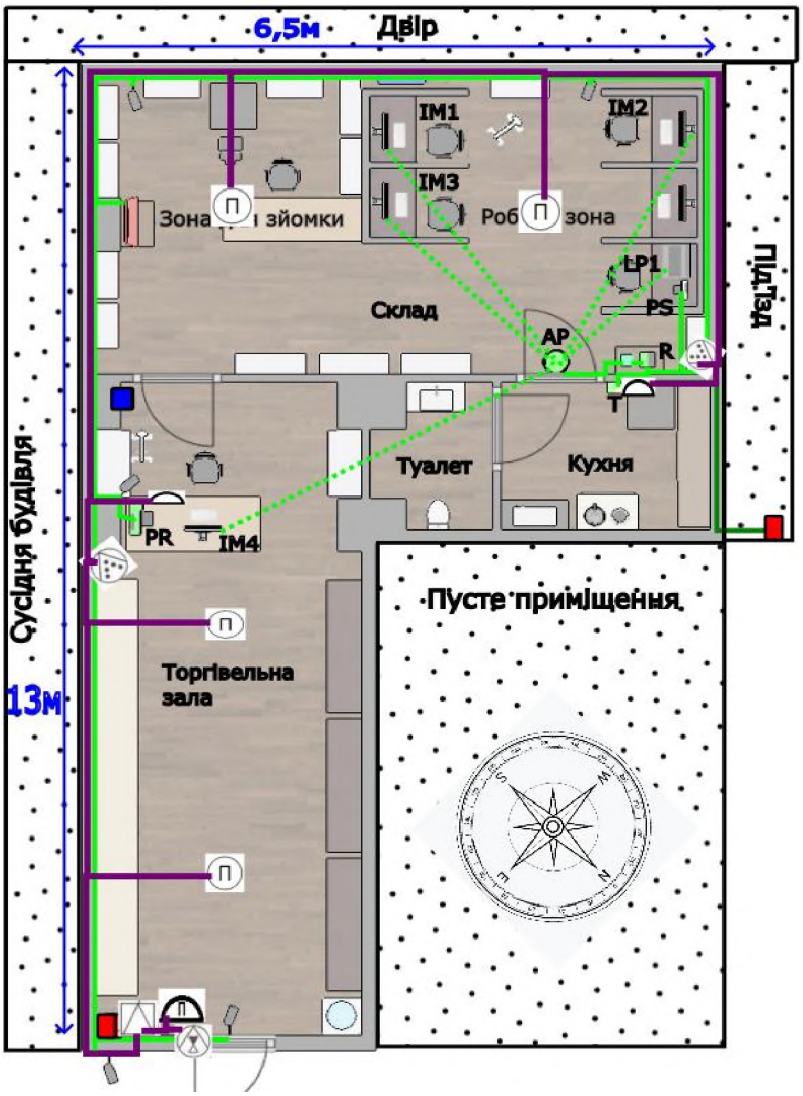

Рисунок 1.1 – Генеральний план (Інтернет-з’єднання на території ОІД, система сигналізації)

Умовні позначення до генерального плану зображеного на рис. 1.1:

	Провідне з’єднання (вита пара)		Безпровідне з’єднання
	Оптоволоконний кабель		З’єднання
П	Пожежний датчик		Точковий магнітоконтактний
	ПКП		Об’ємний інфрачервоний датчик
	Тривожна кнопка	П	Пожежна тривожна кнопка

Опис генерального плану зображеного на рис. 1.1:

Ззовні оптоволоконний кабель входить в абонентський термінал ONU, який знаходиться на кухні в прикрученій до стіни захисній коробці. З терміналу кабель прямує до маршрутизатора, який через PoE адаптер з'єднується з точкою доступу на стіні.

ПКП підключений до інтернету. Підприємство має контракт з охоронною службою, тому наприклад, в разі спрацювання тривожної кнопки, буде екстренно повідомлено охорону.

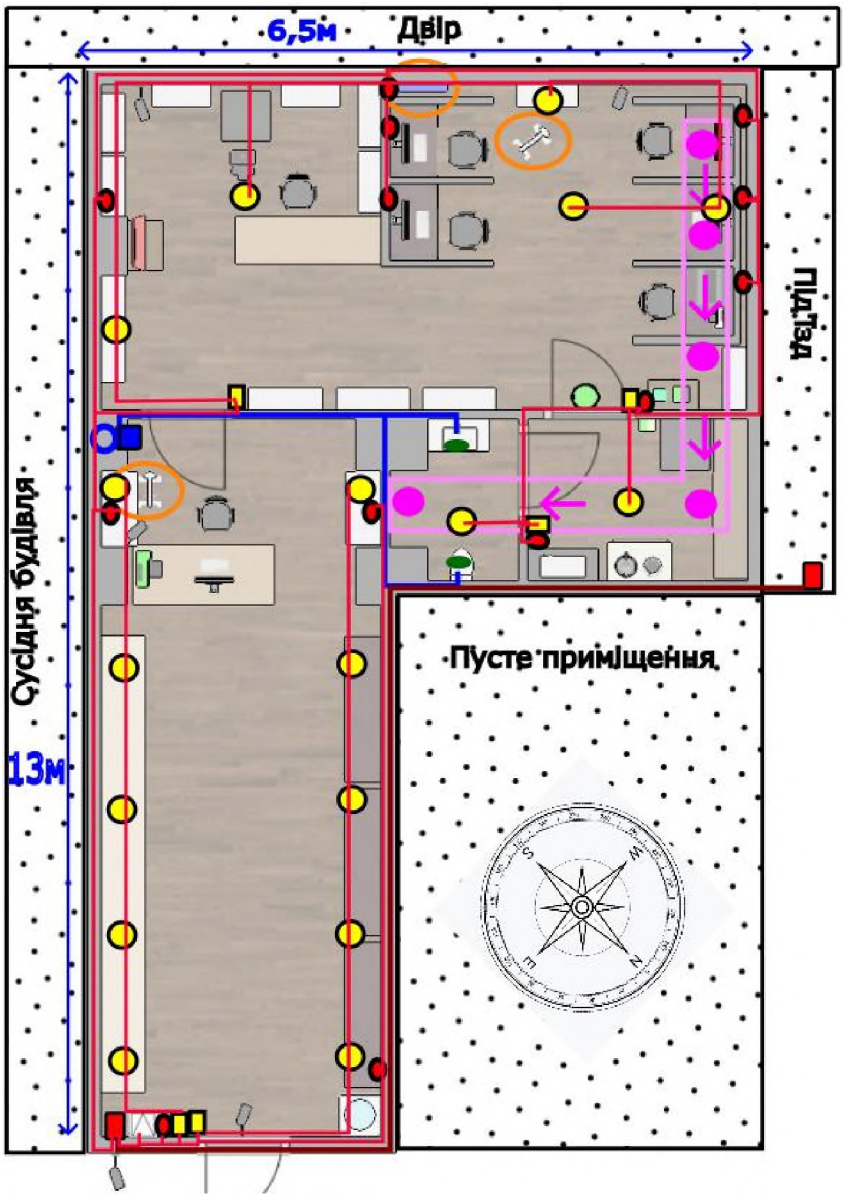

Рисунок 1.2 – Генеральний план (системи водопостачання, опалення, вентиляції, електроживлення та освітлення)

Умовні позначення до генерального плану зображеного на рис. 1.2:

Опис генерального плану зображеного на рис. 1.2:

Від лічильника лінії водопостачання йдуть тільки до туалета, до раковини та унітазу. Стояк каналізації знаходиться в туалеті. В якості елементі системи опалення виступають два обігрівачі (один в торгівельній залі, інший в робочій зоні) та один кондиціонер (на складі). Система вентиляції витяжна.

Нижче в табл. 1.2 наведено перелік основних технічних засобів.

Таблиця 1.2 – Перелік основних технічних засобів

№	Назва	Модель	Серійний номер	Розміщення	Відстань до межі ОІД, м
1	IM1-IM4 (4 шт.)	Apple iMac 27" Retina	C02RL123DC71 C02RL123DC72 C02RL123DC73 C02RL123DC74	Склад 3 шт., Торгівельна зона	0,6, 0,3, 1,3, 0,8
2	LP1	Ноутбук ASUS Vivobook 15 X1502ZA-BQ641	EKLMNO123456789	Склад	0,3
3	R	Маршрутизатор MikroTik RB4011iGS	LNK123456789	Склад, на тумбочці	0,8
4	T	Абонентський термінал EPON (ONU) EP-125	ABCDEFGH1234	Кухня, на стіні	1,3
5	PR	POS термінал Ingenico ICT220Б\B	IWL220A-ABCDE12345	Торгівельна зона	0,2
6	PS	XPrinter XP-370BM	XP0A-AAKDE91917	Склад	0,3
7	AP	Точка доступа Ubiquiti UAP-AC-PRO	12ABCD345678	Склад, на стіні	1,6

Продовження таблиці 1.2

№	Назва	Модель	Серійний номер	Розміщення	Відстань до межі ОІД, м
8	Клавіатура (4 шт.) (до ІМ1-ІМ4)	Клавіатура бездротова Apple Magic Keyboard Bluetooth UA (MK2A3UA/A)	RZR123456781 RZR123456782 RZR123456783 RZR123456784	Склад 3шт., Торгівельна зала	0,6, 0,4, 1,3, 0,8

Перелік допоміжних технічних засобів наведено в Додатку Г.

1.3.2 Обстеження обчислювального середовища

ІКС являє собою однорангову локальну систему з виходом до Інтернет. Структурна схема ІКС зображена на рис. 1.5. Вихід в Інтернет забезпечується в першу чергу за допомогою абонентського ONU терміналу від провайдеру, далі маршрутизатору, що розміщений на території складу та під'єднаної за допомогою PoE адаптера, точки доступу закріпленої на стіні над дверима кухні, яка виступає в ролі репітера для маршрутизатора для посилення сигналу. Для шифрування трафіку застосовується протокол WPA2-PSK.

Бездротовим шляхом до точки доступу підключаються чотири Mac-комп'ютери та ноутбук. Три Mac-комп'ютери та ноутбук розміщуються в робочій зоні на території складу, а один Mac-комп'ютер в торгівельній залі. Дротовим шляхом з використанням витої пари підключаються камери відеоспостереження, телевізор, POS-термінал та принтер для етикеток. Телевізор використовується для транслювання зображення з камер відеоспостереження. POS-термінал знаходиться в торгівельній залі на столі та використовується для друкування чеків. Принтер для етикеток знаходиться в робочій зоні на території складу на столі біля ноутбуку. В табл. 1.4 вказано технічні характеристики складу ІКС.

Робота відбувається на віддаленому сервері, до якого доступ надається за допомогою встановлених інструментів та через VPN.

В табл. 1.5 вказано програмне забезпечення, що застосовується в ІКС. Кожен працівник має доступ до сервера під своїм записом на комп'ютері. Прямого доступу до локальної обчислювальної системи віддалені працівники не мають.

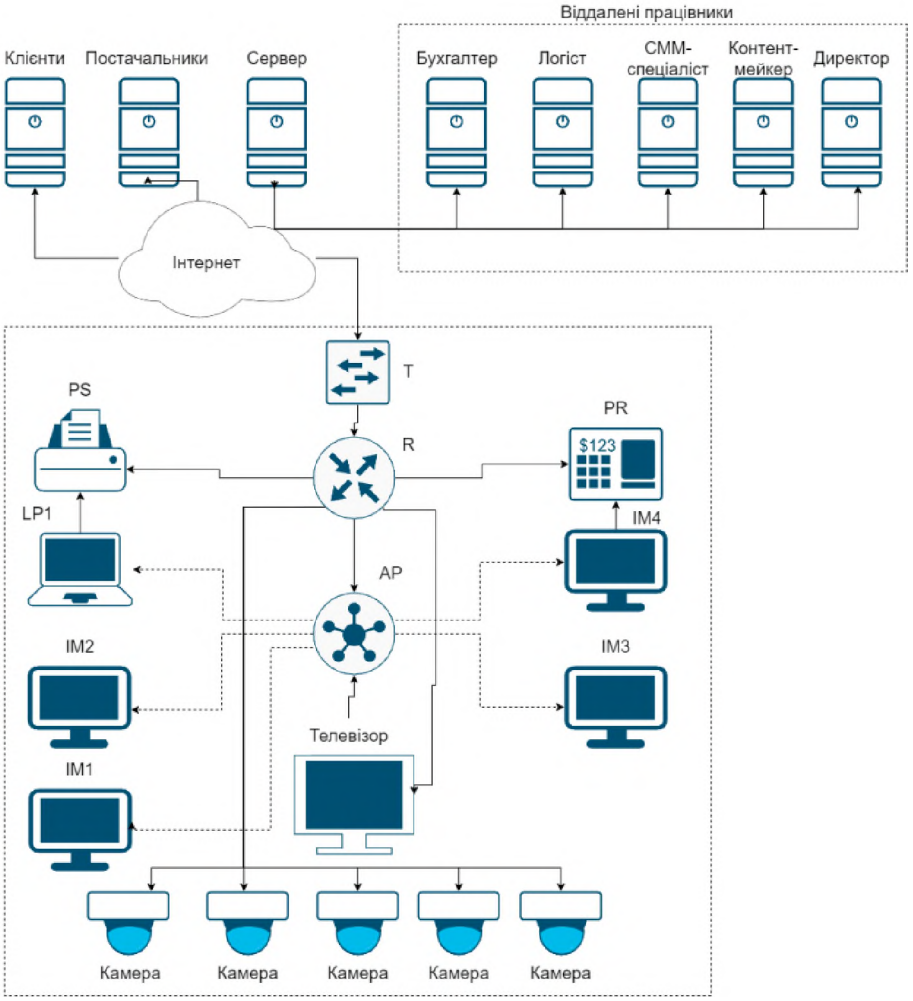

Рисунок 1.3 – Структурна схема ІКС

Умовні позначення до генерального плану зображеного на рис. 1.3:

	Ноутбук		iMac
	ONU термінал		Точка доступу
	Маршрутизатор		POS термінал
	Принтер для етикеток		Телевізор
	Камера відеоспостереження		Робоча станція

Віддалено через Інтернет відбувається зв'язок:

– з постачальниками – комунікує директор. Дані зберігаються в базі даних на сервері;

– з клієнтами – комунікація може відбуватися віддалено через соціальні мережі, сайт. Дані зберігаються в базі даних на сервері;

– з віддаленими працівниками – віддалені працівники не мають прямого доступу до ІТС на ОІД. Працівники мають доступ до загального серверу, де відбуваються всі робочі процеси. Працівники можуть комунікувати з працівниками, що знаходяться локально через соціальні мережі;

– з сервером – віддалений сервер на якому проходять всі робочі процеси компанії. За допомогою програми Microsoft Remote Desktop або AnyDesk та через VPN, працівники під своїми обліковими записами заходять до серверу, де розміщена CRM.

Технічні характеристики складу ІКС наведено в Додатку Ґ.

Таблиця 1.3 – Програмне забезпечення, що застосовується в ІКС

№	Назва	Тип	Опис	Ліцензія	Де встановлена
1	Telegram 4.15	прикладне	месенджер	Free	IM1-IM4, LP1, віддалені працівники
2	AnyDesk 8.0.8	прикладне	програма для віддаленого доступу	Ultimate	IM1-IM4, LP1, віддалені працівники
3	Microsoft Remote Desktop 10.9.6	прикладне	додаток для підключення до віддаленого ПК або віртуальних програм і робочих столів	Free	IM1-IM4, LP1, віддалені працівники
4	1С 8.3	прикладне	програма для організації обліку та зберігання довідкових даних в електронному вигляді	Commercial	Віддалено на ноутбуці бухгалтера
5	Wireguard VPN 1.0.20220627	спеціа-лізоване	протокол віртуальної приватної мережі (VPN)	Free	IM1-IM4, LP1, віддалені працівники

Продовження таблиці 1.3

№	Назва	Тип	Опис	Ліцензія	Де встановлена
6	Google Sheets 1.2024.09202	прикладне	додаток для роботи з електронними таблицями	Free	IM1-IM4, LP1, віддалені працівники
7	Windows 10 19045.4046	системне	операційна система	Pro	IM1-IM4, LP1, віддалені працівники
8	Windows Server 2019 17763.1158	системне	операційна система	Pro	Сервер
9	Google Chrome 122.0.6261.96	прикладне	програма для роботи в інтернет мережі	Free	IM1-IM4, LP1, віддалені працівники

1.3.3 Обстеження інформаційного середовища

На ОІД циркулює відкрита та конфіденційна інформація. Інформація на ОІД представлена тільки у електронному вигляді. Інформація на пристроях обчислювальної системи не зберігається. Інформація зберігається тільки віддалено на сервері.

В табл 1.4 наведена інформація, яка циркулює на ОІД.

В табл 1.5 вказано рівні конфіденційності, цілісності, доступності та їх опис.

Таблиця 1.4 – Інформація, яка циркулює на ОІД

№	Інформація	Класифікація за рівнем доступу	Класифікація за правовим режимом	Вимоги		
				К	Ц	Д
1	Організаційно-розпорядча	ІзОД	Конфіденційна	2	2	2
2	Дані про клієнтів	ІзОД	Конфіденційна	2	2	2
3	Інвентарізаційні дані	ІзОД	Конфіденційна	2	2	2
4	Договори закупки товару	ІзОД	Конфіденційна	2	2	2
5	Замовлення клієнта	ІзОД	Конфіденційна	2	3	2

Продовження таблиці 1.4

№	Інформація	Класифікація за рівнем доступу	Класифікація за правовим режимом	Вимоги		
				К	Ц	Д
6	Бухгалтерська звітність	ІзОД	Конфіденційна	3	3	2
7	Матеріали для реклами	ІзОД	Конфіденційна	1	1	1
8	Дані про вартість товарів та ремонт	Відкрита	–	1	1	1
9	Дані про співробітників	ІзОД	Конфіденційна	3	2	2
10	Логістичні дані	ІзОД	Конфіденційна	2	3	2

Таблиця 1.5 – Опис рівнів конфіденційності, цілісності та доступності

Оцінка рівня наслідків	Опис
Конфіденційність	
К1	Рівень конфіденційної інформації, при якому можна знехтувати збитками у разі розкриття інформації
К2	Рівень конфіденційної інформації, при якому організація зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї
К3	Рівень конфіденційної інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї
Цілісність	
Ц1	Рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації
Ц2	Рівень цілісності інформації, при якому організація зазнає незначних збитків у разі втрати цілісності інформації
Ц3	Рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації.
Доступність	
Д1	Рівень доступності інформації, при якому можна знехтувати втратою доступності інформації
Д2	Рівень доступності інформації, при якому організація зазнає незначних збитків у разі втрати доступності інформації
Д3	Рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації

Всі операції виконуються на віддаленому сервері, до якого користувачі системи входять за допомогою встановлених програм для віддаленого доступу. Пристрої обчислювальної системи, що знаходяться на території ОІД, не виносяться за її межі, окрім ситуацій з ремонтом даної техніки. Організація має свій окремий сервісний центр з ремонту техніки. Робота з зовнішніми носіями не передбачена. Резервне копіювання не застосовуються.

Організаційно-розпорядча інформація формується та редагується прожект-менеджером (ІМ3) та директором. Ця інформація використовується для ефективного функціонування організації, сюди входить: документи, щодо організації робочого процесу, включаючи розпорядчі документи, графіки роботи, плани розвитку; статути, положення та регламенти, що визначають правовий статус та структуру організації; внутрішні нормативно-правові акти, що регулюють діяльність та взаємовідносини між працівниками. Сформована інформація зберігається на сервері, де всі інші працівники можуть ознайомитись з інформацією.

Дані про клієнтів можуть формуватися як віддалено, так і безпосередньо при відвідуванні магазину. Віддалено формують базу даних клієнтів спеціалісти колцентру (ІМ1, ІМ2), які дані отримують або за шаблоном з замовлення, що створюється на сайті компанії, або після взаємодії з клієнтами в соціальних мережах, після чого формують базу даних. Цієї інформацією користується менеджер з продажу в торгівельній залі (ІМ4) при здійсненні операцій. При відвідуванні магазину без попереднього зв'язку віддалено, менеджер з продажу в торгівельній залі заносить дані клієнта в базу даних на місці. Сформована інформація зберігається на сервері.

Інвентаризаційні дані формуються на сервері менеджерами з продажу та прожект-менеджером. Після прийому товарів до магазину менеджери з продажу заносять інформацію до бази даних (ІМ4), за ноутбуком (LP1) розпечатуються етикетки для товарів, та в зоні для зйомки робляться фото для подальшого викладення товару на сайт. Спеціалісти колцентру (ІМ1, ІМ2) оновлюють інформацію на сайті. Сформована інформація зберігається на сервері.

Договори закупки товару формуються директором. Директор є відповідальним за зв'язок з постачальниками. Сформована інформація зберігається на сервері.

Замовлення клієнта на базі шаблону, що заповнюється клієнтами на сайті компанії, формується спеціалістами колцентру (IM1, IM2), після чого цю інформацію може використовувати менеджер з продажу в торгівельній залі для здійснення операцій. Можливе здійснення операцій при відвідуванні магазину без попереднього створення замовлення. Сформована інформація зберігається на сервері.

Бухгалтерська звітність формується віддалено на ноутбуці бухгалтера, за допомогою встановленої програми для ведення бухгалтерського обліку. Сформована інформація зберігається на сервері.

Матеріали для реклами формуються та використовуються віддаленими працівниками, такими як: SMM-спеціаліст та контент-мейкер, для створення реклами. Працівники мають можливість фізично відвідати магазин та використовувати зону для зйомки на території ОІД, для створення фото товарів. SMM-спеціаліст використовує рекламу для розповсюдження інформації про товари компанії в соціальних мережах. Контент-мейкер використовуючи фото- та відео- матеріали для ведення соціальних мереж компанії. Сформована інформація зберігається на ноутбуках SMM-спеціаліста та контент-мейкера.

Дані про вартість товарів та ремонт. Дані про вартість товарів вже формуються при прийомі товару до магазину менеджерами з продажу (IM4) та заносяться в базу даних. Спеціалісти колцентру (IM1, IM2) оновлюють інформацію на сайті. Сформована інформація зберігається на сервері.

Дані про співробітників формуються прожект-менеджером (IM3) та директором. Прожект-менеджер використовує цю інформацію при виплаті заробітної плати, при обліку часу співробітників. Сформована інформація зберігається на сервері.

Логістичні дані формуються віддалено на ноутбуці логіста. Сформована інформація зберігається на сервері.

Нижче на рис. 1.4 зображено схему інформаційних потоків.

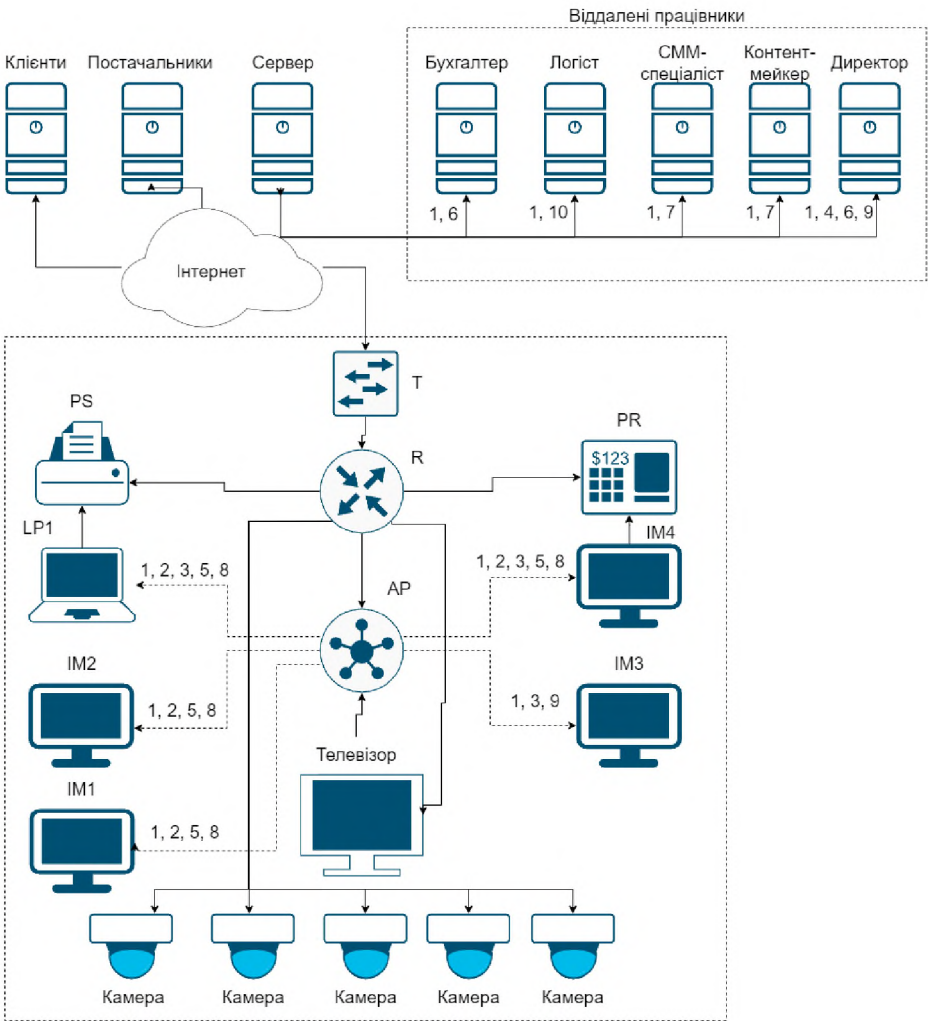

Рисунок 1.4 – Схема інформаційних потоків

1.3.4 Обстеження середовища користувачів

Нижче в табл. 1.6 вказано перелік співробітників підприємства.

Таблиця 1.6 – Перелік співробітників

№	Посада	Роль	Обов'язки	Кваліфікація
1	Прожект-менеджер	Адміністратор	Облік часу співробітників, оплата заробітної плати, організація робочого процесу	Висока
2	Менеджер з продажу (3 особи)	Користувач	Прийом товару, інвентаризація, продаж товару	Середня

Продовження таблиці 1.6

№	Посада	Роль	Обов'язки	Кваліфікація
3	Спеціаліст колцентру (2 особи)	Користувач	Введення сайту, прийом дзвінків, комунікація онлайн	Низька
4	Директор	Користувач	Комунікує з постачальниками, відповідальний за закупку товарів	Середня
5	Бухгалтер	Користувач	Введення бухглатерського обліку	Середня
6	Логіст	Користувач	Управління логістичними процесами	Середня
7	SMM-спеціаліст	Користувач	Просування товарів в соціальних мережах	Середня
8	Контент-мейкер	Користувач	Створення контенту для соціальних мереж	Середня

Адмініструванням системи займається прожект-менеджер. Прожект-менеджер видає кожному користувачу системи свій обліковий запис з визначеними правами.

Менеджери з продажу працюють позмінно (по дві людини). В розпорядженні менеджерів iMac, що стоїть в торгівельній залі (IM4) та ноутбук в робочій зоні на складі (LP1). Кожен має свій особистий обліковий запис, тому при зміні користувача, обов'язково змінюється обліковий запис.

У кожного спеціаліста колцентру в розпорядженні свій iMac (IM1 та IM2).

Нижче в табл. 1.7 вказано матрицю розмежування доступу.

Таблиця 1.7 – Розмежування доступу

№	Інформація	Користувачі							
		Прожект-менеджер	Менеджер з продажу	Спеціаліст колцентру	Директор	Бухгалтер	Логіст	СММ-спеціаліст	Контент-мейкер
1	Організаційно-розпорядча	RWD	R	R	RWD	R	R	R	R
2	Дані про клієнтів	RWD	RWD	RW	RWD	–	–	–	–

Продовження таблиці 1.7

№	Інформація	Користувачі							
		Проже кт-менед жер	Менед жер з прода жу	Спеціа ліст колцен тру	Дирек тор	Бухгал тер	Логіст	SMM-спеціа ліст	Конте нт-мейкер
3	Інвентарізаційні дані	RWDP	RWDP	–	RWD	–	–	–	–
4	Договори закупки товару	RWD	–	–	RWD	–	–	–	–
5	Замовлення клієнта	RWD	RWD	RW	RWD	–	–	–	–
6	Бухгалтерська звітність	RWD	–	–	RWD	RWD	–	–	–
7	Матеріали для реклами	RWD	–	–	RWD	–	–	RWD	RWD
8	Дані про вартість товарів та ремонт	RWD	RWD	RW	RWD	–	–	–	–
9	Дані про співробітників	RWD	–	–	RWD	–	–	–	–
10	Логістичні дані	RWD	–	–	RWD	–	RWD	–	–

Позначення:

– R (читання);

– W (запис);

– D (видалення);

– P (друкування).

1.4 Модель порушника

Таблиця 1.8 – Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
	Внутрішні по відношенню до ІКС	
ПВ1	Працівники, що працюють віддалено	1
ПВ2	Користувачі ІКС	2
ПВ3	Адміністратори ІКС	3

Продовження таблиці 1.8

Позначення	Визначення категорії	Рівень загроз
	Зовнішні по відношенню до ІКС	
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів	4

Таблиця 1.9 – Специфікація моделі порушника за мотивами

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

Таблиця 1.12 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІКС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань та не вміє працювати з технічними засобами ІКС	1
К2	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІКС	2
К3	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІКС та їх обслуговування	3
К4	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІКС	4

Таблиця 1.10 – 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, прослуховування Wi-Fi, зовнішнє спостереження	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІКС	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	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІКС, дезорганізації систем обробки інформації	4

Таблиця 1.11 – Специфікація моделі порушника за часом дії

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

Таблиця 1.12 – Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Поза приміщенням та без доступу до технічних засобів ІКС	1
Д2	Усередині приміщення, але без доступу до технічних засобів ІКС	2
Д3	З робочих місць користувачів ІКС	3
Д4	З робочих місць адміністраторів ІКС	4

Таблиця 1.13 – Профіль внутрішнього порушника по відношенню до ІКС

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІКС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Прожект-менеджер	ПВ3	М3	К4	З3	Ч4	Д4	21
	3	3	4	3	4	4	
Менеджер з продажу	ПВ2	М3	К3	З2	Ч4	Д3	17
	2	3	3	2	4	3	
Спеціаліст колцентру	ПВ2	М1	К2	З1	Ч4	Д3	13
	2	1	2	1	4	3	
Директор	ПВ1	М1	К3	З1	Ч3	Д1	10
	1	1	3	1	3	1	
Бухгалтер	ПВ1	М3	К3	З3	Ч3	Д1	14
	1	3	3	3	3	1	
Логіст	ПВ1	М3	К3	З3	Ч3	Д1	14
	1	3	3	3	3	1	
SMM-спеціаліст	ПВ1	М3	К3	З1	Ч3	Д1	12
	1	3	3	1	3	1	
Контент-мейкер	ПВ1	М3	К3	З1	Ч3	Д1	12
	1	3	3	1	3	1	

Таблиця 1.14 – Профіль зовнішнього порушника по відношенню до ІКС

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІКС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Відвідувачі	ПВ1	М2	К1	З1	Ч3	Д2	10
	1	2	1	1	3	2	
Конкуренти	ПВ4	М4	К3	З2	Ч3	Д1	17
	4	4	3	2	3	1	
Працівники сервісу з ремонту техніки	ПВ2	М3	К3	З4	Ч2	Д1	15
	2	3	3	4	2	1	

З таблиці 1.13 можна побачити, що найбільшу внутрішню загрозу, становить прожект-менеджер, адже він виконує роль адміністратора системи . Також з таблиці 1.14 можна побачити, що найбільшу зовнішню загрозу, становлять конкуренти, що можна пояснити тим, що вони мають найбільшу мотивацію для цього.

1.5 Модель загроз

Виявлення джерел загроз:

Усі джерела загроз безпеці інформації можна розділити на три основні групи:

– I. Зумовлені діями суб'єкта (антропогенні джерела загроз). Антропогенні джерела загроз наведено в табл. 1.15 та табл. 1.16;

– II. Зумовлені технічними засобами (техногенні джерела загрози). Техногенні джерела загрози наведено в табл. 1.17 та табл. 1.18;

– III. Зумовлені стихійними джерелами. Стихійні джерела загроз наведено в табл. 1.19.

Таблиця 1.15 – Антропогенні зовнішні джерела загроз

№	Джерела загроз
I.A.1	Відвідувачі (запрошені з будь-якого приводу)
I.A.2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачанняі таке інше)
I.A.3	Конкуренти

Таблиця 1.16 – Антропогенні внутрішні джерела загроз

№	Джерела загроз
I.B.1	Працівники, що працюють віддалено
I.B.2	Користувачі ІКС
I.B.3	Адміністратори ІКС

Таблиця 1.17 – Техногенні зовнішні джерела загроз

№	Джерела загроз
II.A.1	Лінія системи електропостачання
II.A.2	Лінія мережеі Інтернет

Таблиця 1.18 – Техногенні внутрішні джерела загроз

№	Джерела загроз
II.B.1	Неякісні технічні засоби обробки інформації
II.B.2	Неякісне системне програмне забезпечення
II.B.3	Неякісне прикладне програмне забезпечення
II.B.4	Допоміжні технічні засоби

Таблиця 1.19– Стихійні зовнішні джерела загроз

№	Джерела загроз
III.A.1	Пожежа
III.A.2	Військові дії
III.A.3	Ураган
III.A.4	Інші форс-мажорні обставини

Усі джерела загроз мають різний ступінь небезпеки (Коп)і, яку можна кількісно оцінити, провівши їх ранжування. При цьому, оцінка ступеня небезпеки проводиться за непрямими показниками. Як критерії порівняння (показники) можна, наприклад, вибрати:

Можливість виникнення джерела (К1)і – визначає ступінь доступності до об'єкта, що захищається (для антропогенних джерел), віддаленість від об'єкта, що захищається (для техногенних джерел), або особливості обстановки (для випадкових джерел).

Готовність джерела (К2)і – визначає ступінь кваліфікації та привабливість вчинення діянь з боку джерела загрози (для антропогенних джерел), або наявність необхідних умов (для техногенних і стихійних джерел).

Фатальність (К3)і – визначає ступінь непереборності наслідків реалізації загрози.

Кожен показник оцінюється експертно-аналітичним методом за п'ятибальною системою. Причому, 1 відповідає мінімальному ступеню впливу оцінюваного показника на небезпеку використання джерела, а 5 – максимальному.

У формулі (1.1), (Кнб_д)і для окремого джерела можна визначити як відношення добутку вищенаведених показників до максимального значення (125):

$$\text{Кнб\_д} = \frac{(\text{К1}*\text{К2}*\text{К3})}{125}, \tag{1.1}$$

Нижче в табл. 1.20 виконано ранжування джерел загроз.

Таблиця 1.20 – Ранжування джерел загроз

№	Джерело загрози	(К1)і	(К2)і	(К3)і	(Кнб_д)і
I.A.1	Відвідувачі (запрошені з будь-якого приводу)	2	2	2	0,064
I.A.2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	3	2	3	0,144
I.A.3	Конкуренти	3	5	4	0,48
I.B.1	Працівники, що працюють віддалено	3	2	3	0,144
I.B.2	Користувачі ІКС	4	3	3	0,288
I.B.3	Адміністратори ІКС	5	4	4	0,64
II.A.1	Лінія системи електропостачання	3	2	3	0,144
II.A.2	Лінія мережі Інтернет	3	2	3	0,144
II.B.1	Неякісні технічні засоби обробки інформації	5	3	3	0,36
II.B.2	Неякісне системне програмне забезпечення	5	2	3	0,36
II.B.3	Неякісне прикладне програмне забезпечення	5	3	3	0,36
II.B.4	Допоміжні технічні засоби	3	3	2	0,144
III.A.1	Пожежа	3	2	5	0,24
III.A.2	Військові дії	3	3	5	0,36
III.A.3	Ураган	2	1	4	0,064
III.A.4	Інші форс-мажорні обставини	1	1	2	0,016

Всі джерела загроз, з Кнб_д > 0,144, ми будемо враховувати в подальшій роботі, всі Кнб_д що < 0,144 враховані не будуть, так як для нас вони не актуальні.

Виявлення вразливостей безпеки:

Для зручності аналізу вразливості розділені на класи (позначаються великими літерами), групи (позначаються римськими цифрами) і підгрупи (позначаються малими літерами). Уразливості безпеки інформації можуть бути:

– [A] об'єктивними. Об’єктивні вразливості визначено в табл. 1.21;

– [B] суб'єктивними. Суб’єктивні вразливості визначено в табл. 1.22;

– [C] випадковими. Випадкові вразливості визначено в табл. 1.23.

Таблиця 1.21 – Об’єктивні вразливості

№	Вразливості
A.I	**Супутні технічні засоби випромінювання**
A.I.a	Побічні випромінювання елементів технічних засобів
A.I.b	Побічні випромінювання кабельних ліній технічних засобів
A.I.c	Нерівномірне споживання струму електроживлення
A.II	**Активізовані**
A.II.a	Апаратні закладки встановлювані в приміщеннях
A.II.b	Апаратні закладки встановлювані в технічних засобах
A.II.c	Шкідливе програмне забезпечення
A.III	**Обумовлені особливостями об'єкта, що захищається**
A.III.a	Наявність прямої видимості об’єктів
A.III.b	Відсутність режиму доступу до ОІД
A.III.c	Використання глобальних інформаційних мереж

Таблиця 1.22 – Суб'єктивні вразливості

№	Вразливості
B.I	**Помилки**
B.I.a	Помилки при інсталяції та завантаженні ПЗ
B.I.b	Помилки при експлуатації ПЗ
B.I.c	Помилки при вводі даних
B.II	**Порушення**
B.II.a	Порушення режиму доступу до технічних засобів
B.II.b	Порушення режиму використання інформації

Таблиця 1.23 – Випадкові вразливості

№	Вразливості
C.I	**Збої та відмови**
C.I.a	Відмови та несправності технічних засобів, що обробляють інформацію
C.I.b	Збій операційних систем та СУБД
C.I.c	Збій прикладних програм

Продовження таблиці 1.23

№	Вразливості
C.I.d	Збій антивірусних програм
C.II	**Ушкодження**
C.II.a	Ушкодження комунікацій
C.II.b	Ушкодження стін та перекриття будівель
C.II.c	Ушкодження корпусів технологічного обладнання

Усі вразливості мають різний ступінь небезпеки (Коп)f, яку можна кількісно оцінити, провівши їх ранжування. При цьому, як критерії порівняння (показники) можна вибрати:

Фатальність (К1)f – визначає ступінь впливу вразливості на непереборність наслідків реалізації загрози. Для об'єктивних уразливостей це Інформативність - здатність уразливості повністю (без спотворень) передати корисний інформаційний сигнал.

Доступність (К2)f – визначає зручність (можливість) використання вразливості джерелом загроз (масогабаритні розміри, складність, вартість необхідних засобів, можливість використання неспеціалізованої апаратури).

Кількість (К3)f – визначає кількість елементів об'єкта, яким характерна та чи інша вразливість.

Кожен показник оцінюється експертно-аналітичним методом за п'ятибальною системою. Причому, 1 відповідає мінімальному ступеню впливу оцінюваного показника на небезпеку використання вразливості, а 5 – максимальному.

У формулі (1.2), (Кнб_в)f для окремої вразливості можна визначити як відношення добутку вищенаведених показників до максимального значення (125):

$$\text{Кнб\_в} = \frac{(\text{К1}*\text{К2}*\text{К3})}{125}, \tag{1.2}$$

Нижче в табл. 1.24 виконано ранжування вразливостей.

Таблиця 1.25 – Ранжування вразливостей

№	Вразливість	(К1)і	(К2)і	(К3)і	(Кнб_в)і
A.I.a	Побічні випромінювання елементів технічних засобів	2	1	5	0,08
A.I.b	Побічні випромінювання кабельних ліній технічних засобів	2	1	5	0,08
A.I.c	Нерівномірне споживання струму електроживлення	1	1	4	0,032
A.II.a	Апаратні закладки встановлювані в приміщеннях	4	2	2	0,128
A.II.b	Апаратні закладки встановлювані в технічних засобах	4	1	2	0,064
A.II.c	Шкідливе програмне забезпечення	4	3	4	0,384
A.III.a	Наявність прямої видимості об’єктів	5	4	4	0,64
A.III.b	Відсутність режиму доступу до ОІД	3	4	4	0,384
A.III.c	Використання глобальних інформаційних мереж	2	4	4	0,256
B.I.a	Помилки при інсталяції та завантаженні ПЗ	2	2	3	0,096
B.I.b	Помилки при експлуатації ПЗ	3	3	3	0,216
B.I.c	Помилки при вводі даних	2	2	3	0,096
B.II.a	Порушення режиму доступу до технічних засобів	4	5	4	0,64
B.II.b	Порушення режиму використання інформації	4	4	4	0,512
C.I.a	Відмови та несправності технічних засобів що обробляють інформацію	4	3	3	0,288
C.I.b	Збій операційних систем та СУБД	3	3	3	0,216
C.I.c	Збій прикладних програм	3	3	3	0,216
C.I.d	Збій антивірусних програм	3	2	3	0,144
C.II.a	Ушкодження стін та перекриття будівель	5	3	3	0,36
C.II.b	Ушкодження корпусів технологічного обладнання	4	3	4	0,256

Всі вразливості, з Кнб_в > 0,144 ми будемо враховувати в подальшій роботі, всі Кнб_в що < 0,144 враховані не будуть, так як для нас вони не актуальні.

Виявлення актуальних загроз:

Складається матриця взаємозв'язку джерел загроз і вразливостей, з якої визначаються можливі наслідки реалізації загроз (атаки) і обчислюється коефіцієнт небезпеки цих атак як добуток коефіцієнтів небезпеки відповідних загроз і джерел загроз, визначених раніше. Матрицю наведено в табл. 1.28.

При цьому передбачається, що коефіцієнти які менші ніж 0,1, в майбутньому не будуть враховані через малу ймовірність їх реалізації на об’єкті. Визначені актуальні загрози наведено в табл. 1.26.

Таблиця 1.25 – Класифікація актуальних загроз

№	Джерело загрози	Вразливість	Наслідки реалізації загрози	(Кнб_д)і	(Кнб_в)і	(Кнб_з)і
1	I.A.3	A.II.c	Спотворення або втрата інформації	0,46	0,384	0,177
2		A.III.a	Розкриття інформації		0,64	0,29
3		A.III.b	Несанкціоноване проникнення та розприття інформації		0,384	0,177
4		A.III.c	Порушення конфіденційності інформації		0,256	0,118
5	I.B.2	B.I.b	Втрата інформації	0,288	0,216	0,06
7		B.II.a	Порушення конфіденційності інформації		0,64	0,185
8		B.II.b	Порушення конфіденційності інформації		0,512	0,147

Продовження таблиці 1.25

№	Джерело загрози	Вразливість	Наслідки реалізації загрози	(Кнб_д)і	(Кнб_в)і	(Кнб_з)і
10	I.B.3	B.I.b	Втрата інформації	0,64	0,216	0,138
12		B.II.a	Порушення конфіденційності інформації		0,64	0,4
13		B.II.b	Порушення конфіденційності інформації		0,512	0,32
15	II.B.1	C.I.a	Порушення доступності інформації	0,36	0,288	0,1
16	II.B.2	C.I.b	Порушення доступності інформації	0,36	0,216	0,08
17		A.II.c	Спотворення або втрата інформації		0,384	0,138
18	II.B.3	C.I.c	Порушення доступності інформації	0,36	0,216	0,08
19		A.II.c	Спотворення або втрата інформації		0,384	0,138
20	III.A.1	C.II.a	Втрата інформації	0,24	0,36	0,08
21		C.II.b	Втрата інформації		0,256	0,06
22	III.A.2	C.II.a	Втрата інформації	0,36	0,36	0,13
23		C.II.b	Втрата інформації		0,256	0,09

Таблиця 1.26 – Актуальні загрози

№	Джерело загрози	Вразливість	Наслідки реалізації загрози	(Кнб_д)і	(Кнб_в)і	(Кнб_з)і
1	I.A.3	A.II.c	Спотворення або втрата інформації	0,46	0,384	0,177
2		A.III.a	Розкриття інформації		0,64	0,29
3		A.III.b	Несанкціоноване проникнення та розприття інформації		0,384	0,177
4		A.III.c	Порушення конфіденційності інформації		0,256	0,118
5	I.B.2	B.II.a	Порушення конфіденційності інформації	0,288	0,64	0,185
6		B.II.b	Порушення конфіденційності інформації		0,512	0,147
7	I.B.3	B.I.b	Втрата інформації	0,64	0,216	0,138
8		B.II.a	Порушення конфіденційності інформації		0,64	0,4
9		B.II.b	Порушення конфіденційності інформації		0,512	0,32
10	II.B.1	C.I.a	Порушення доступності інформації	0,36	0,288	0,1
11	II.B.2	A.II.c	Спотворення або втрата інформації	0,36	0,384	0,138
12	II.B.3	A.II.c	Спотворення або втрата інформації	0,36	0,384	0,138
13	III.A.2	C.II.a	Втрата інформації	0,36	0,36	0,13

1.6 Об’єкти захисту

Об’єкти захисту в системі, було розділено на окремі групи.

Група 1:

– Організаційно-розпорядча інформація;

– Дані про клієнтів;

– Інвентарізаційні дані;

– Договори закупки товару;

– Замовлення клієнта;

– Бухгалтерська звітність;

– Матеріали для реклами;

– Дані про вартість товарів та ремонт;

– Дані про співробітників;

– Логістичні дані.

Група 2:

– Системне та прикладне програмне забезпечення, що використовується в системі.

Група 3:

– Технічні засоби обробки інформації.

Група 4:

– Облікові записи користувачів.

1.7 Формування профілю захищеності

Після проведеної роботи з обстеження середовищ функціонування, аналізу можливих загроз та порушників було обрано стандартний функціональний профіль захищеності в КС з деякими змінами, що входить до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації згідно з НД ТЗІ 2.5-005-99:

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

1.8 Висновки до Розділу 1

У першому розділі було:

– описано основні відомості по підприємству;

– обґрунтовано необхідність створення КСЗІ;

– проведено обстеження середовищ функціонування (фізичне середовище, обчислювальне середовище, інформаційне середовище та середовище користувачів);

– розроблено модель порушника та модель загроз;

– сформовано профіль захищеності на основі визначених актуальних загроз.

Для системи підприємства «GetApple» є обґрунтована необхідність створення КСЗІ. Для цього необхідно проаналізувати сформований профіль захищеності та впровадити необхідні проектні рішення.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Аналіз критеріїв

Аналіз критеріїв викладених в профілі захищеності згідно з НД ТЗІ 2.5-004-99 [7] та рівень на якому реалізовано на даний момент вказаний профіль захищеності в системі:

КД-2 (Базова довірча конфіденційність) – в системі, яка реалізує послугу довірча конфіденційність на рівні КД-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес).

Реалізація даної послуги допоможе уникнути порушення режиму використання інформації.

Політика даної послуги поширюється на:

– Група 1.

– Група 4.

Послуга реалізовується за допомогою системних механізмів, де користувач може встановити атрибути доступу до власних об’єктів.

КА-2 (Базова адміністративна конфіденційність) – послуга адміністративна конфіденційність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів.

Реалізація даної послуги допоможе уникнути порушення режиму використання інформації.

Політика даної послуги поширюється на:

– Група 2.

– Група 4.

Послуга реалізовується за допомогою системних механізмів, де користувач може встановити атрибути доступу до власних об’єктів.

КО-1 (Повторне використання об'єктів) – КС забезпечує послугу повторне використання об'єктів, якщо перед наданням користувачеві або процесу в розділювальному об'єкті не залишається інформації, яку він містив, і скасовуються попередні права доступу до об’єкта.

Реалізація даної послуги допоможе уникнути порушення режиму використання інформації.

Політика даної послуги поширюється на:

– сегменти оперативної пам’яті.

Послуга реалізується за рахунок обнулення вмісту оперативної пам’яті. Реалізовано механізми, що дають змогу операційній системі, коли процес завершується, звільняти виділену для нього область в пам'яті. Операційна система забезпечує обнулення (запис нулів) областей пам'яті, які були виділені для використання процесом.

КВ-2 (Базова конфіденційність при обміні) – послуги захисту інформації при обміні (конфіденційність при обміні, цілісність при обміні, ідентифікація і автентифікація при обміні, автентифікація відправника і автентифікація одержувача) дозволяють забезпечити безпеку обміну інформацією між такими КЗЗ через незахищене середовище. Реалізація даної послуги на рівні КВ-2 дозволяє керувати засобами експорту і імпорту об'єктів і додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від витоку інформації при підключенні несанкціонованих користувачів.

Реалізація даної послуга допоможе зменшити вразливість системи через використання глобальних інформаційних мереж.

Політика даної послуги поширюється на:

– Група 1;

– Група 2;

– Група 4.

Послуга реалізовується за допомогою встановленого VPN.

ЦД-1 (Мінімальна довірча цілісність) – на даному рівні користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів.

Реалізація даної послуги допоможе уникнути порушення режиму використання інформації.

Політика даної послуги поширюється на:

– Група 1;

– Група 2;

– Група 4.

Послуга реалізовується за допомогою системних механізмів, де користувач може встановити атрибути доступу до власних об’єктів.

ЦА-2 (Базова адміністративна цілісність) – ця послуга дозволяє адміністратору чи спеціально авторизованому користувачу керувати потоками інформації від користувачів і процесів до захищених об'єктів. Дозволяє адміністратору або спеціально авторизованому користувачу, може накладати обмеження на доступ до об'єктів з боку процесів і груп процесів.

Реалізація даної послуги допоможе уникнути порушення режиму використання інформації.

Політика даної послуги поширюється на:

– Група 1;

– Група 2;

– Група 4.

Послуга реалізовується за допомогою системних механізмів, де користувач може встановити атрибути доступу до власних об’єктів.

ЦО-1 (Обмежений відкат) – дозволяє відновлюватися після помилок користувача, збоїв програмного забезпечення або апаратури і підтримувати цілісність баз даних, додатків, побудованих на транзакціях і т. ін. Даний рівень дозволяє авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Реалізація даної послуги допоможе зменшити вразливість системи після помилок при експлуатації ПЗ.

Політика даної послуги поширюється на:

– технологічна інформація;

– послідовність дій.

Послуга частково реалізовується за допомогою механізмів наявних в системному програмному забезпеченні.

ЦВ-2 (Базова цілісність при обміні) – дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Реалізація даної послуги на рівні ЦВ-2 додатково дозволяє керувати засобами експорту і імпорту об'єктів і додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від модифікації інформації у разі підключенні несанкціонованих користувачів.

Реалізація даної послуги допоможе зменшити вразливість системи через використання глобальних інформаційних мереж.

Політика даної послуги поширюється на:

– Група 1;

– Група 2;

– Група 4.

Послуга реалізовується за допомогою встановленого VPN.

ДР-1 (Квоти) – дана послуга дозволяє керувати використанням послуг і ресурсів користувачами. Всі захищені об'єкти КС (наприклад, дисковий простір, тривалість сеансу, час використання центрального процессора і т. ін.) повинні ідентифікуватись і контролюватись диспетчером доступу шляхом накладення обмежень на максимальний обсяг даного ресурсу, що може бути виділений користувачу.

Реалізація даної послуги допоможе контролювати використання дискового простору користувачами.

Політика даної послуги поширюється на:

– дисковий простір;

– Група 4.

Послуга реалізовується за допомогою встановленого механізму надання квот в операційній системі.

ДС-1 (Стійкість при обмежених відмовах) – стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій чи КС в цілому) після відмови її компоненту.

Реалізація даної послуги допоможе зменшити вразливість системи при відмові, несправності компоненту системи, після застосування шкідливого програмного забезпечення до компонентів системи, при помилках в експлуатації ПЗ.

Політика даної послуги поширюється на:

– Група 2.

– Група 3.

Послуга частково реалізовується, так як вся робота відбувається на віддаленому сервері, то в разі виходу з ладу одного компоненту робота зможе продовжуватись.

ДЗ-2 (Обмежена гаряча заміна) – ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів.

Реалізація даної послуги допоможе зменшити вразливість системи при відмові, несправності компоненту системи, після застосування шкідливого програмного забезпечення до компонентів системи..

Політика даної послуги поширюється на:

– Група 2.

Послуга реалізовується, тому при заміні деякого програмного забезпечення система зможе продовжити функціонувати. Наприклад, при відмові ПЗ для віддаленого доступу, передбачено використання іншого доступного ПЗ.

ДВ-1 (Ручне відновлення) – дана послуга забезпечує повернення КС до відомого захищеного стану після відмови або переривання обслуговування.

Реалізація даної послуги допоможе зменшити вразливість системи при відмові, несправності компоненту системи, після застосування шкідливого програмного забезпечення до компонентів системи.

Політика даної послуги поширюється на:

– Група 2;

– Група 3.

Послуга не реалізовується, в системі не передбачено механізмів для повернення системи до нормального функціонування.

НР-2 (Захищений журнал) – реєстрація дозволяє контролювати небезпечні для КС дії.

Реалізація даної послуги допоможе уникнути порушення режиму використання інформації.

Перелік подій, що реєструються:

– факти входу/ виходу або спроби входу/ виходу в/ з ОС користувачів будь-яких категорій;

– факти порушення встановлених прав доступу користувачів;

– факти присвоєння/ зміни прав доступу користувачів до захищених ресурсів;

– факти отримання доступу та виконання певних дій або спроби отримання користувачем будь-якої категорії доступу до будь-яких захищених інформаційних об'єктів.

В системі не ведеться реєстрація подій.

НИ-2 (Одиночна ідентифікація і автентифікація) – ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача (фізичної особи), який намагається одержати доступ до КС.

Реалізація даної послуги допоможе уникнути порушення режиму використання інформації, порушення режиму доступу до технічних засобів.

Послуга реалізовується за допомогою створених облікових записів, які потребують підтвердження паролем, при спробі доступу до системи.

НК-1 (Однонаправлений достовірний канал) – дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається).

Реалізація даної послуги допоможе уникнути порушення режиму використання інформації, порушення режиму доступу до технічних засобів. Допоможе зменшити вразливість системи через наявність прямої видимості об’єктів.

Політика даної послуги поширюється на:

– Група 3;

– Група 4.

Послуга не реалізовується, так як в системі є можливість підглянути , підслухати іншим користувачем, та можливість іншим користувачем спробувати ініціюватись в системі.

НО-2 (Розподіл обов'язків адміністраторів) – дана послуга дозволяє знизити ймовірність навмисних або помилкових неавторизованих дій користувача або адміністратора і величину потенційних збитків від таких дій.

Реалізація даної послуги допоможе уникнути порушення режиму використання інформації, порушення режиму доступу до технічних засобів.

Політика розподілу повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора.

Політика не реалізовується, так як в системі передбачена лише одна адміністративна роль.

НЦ-1 (КЗЗ з контролем цілісності) – дана послуга визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами. Для рівня НЦ-1 даної послуги необхідно, щоб КЗЗ мав можливість перевіряти свою цілісність і в разі виявлення її порушення переводити систему в стан, з якого її може вивести тільки адміністратор.

Реалізація даної послуги допоможе зменшити вразливість системи від впливу шкідливого програмного забезпечення, помилок при експлуатації ПЗ.

Послуга не реалізовується так як в системі не використовується антивірусне ПЗ.

НТ-2 (Самотестування при старті) – самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС.

Реалізація даної послуги допоможе зменшити вразливість системи від помилок при експлуатації ПЗ, відмов та несправностей технічних засобів, що обробляють інформацію.

Під час старту та за запитом адміністратора комплекс виконує набір тестів з метою оцінки правильності функціонування своїх критичних функцій (шляхом перевірки цілісності відповідних ПЗ і БД технологічної інформації).

Послуга не реалізовується.

НВ-1 (Автентифікація вузла) – ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Реалізація рівня НВ-1 даної послуги дозволяє виключити можливість несанкціонованого зовнішнього підключення і є необхідною умовою для реалізації високих рівнів послуг конфіденційності і цілісності при обміні.

Реалізація даної послуги допоможе уникнути порушення режиму використання інформації та зменшити вразливість системи через використання глобальних інформаційних мереж.

Політика даної послуги поширюється на:

– комплекс засобів захисту.

Послуга реалізовується за допомогою протоколу SSL/TLS. Протокол надає можливості автентифікації і безпечної передачі даних через інтернет з використанням криптографічних засобів.

2.2 Основні положення політики безпеки

– введення антивірусного захисту на підприємстві;

– створення другої адміністративної ролі – адміністратор безпеки;

– оновлення матриці розмежування доступу;

– забезпечення резервного копіювання;

– створення політики безпеки з порядку використання резервного копіювання.

– створення політики безпеки робочого місця;

– процедура самотестування системи;

– забезпечення резервного живлення.

2.3 Вибір антивірусного програмного забезпечення

Встановлення антивірусного програмного забезпечення для системи допоможе реалізувати послугу НЦ-1 (КЗЗ з контролем цілісності), зменшити ризик відмови компоненту КС через втручання шкідливого програмного забезпечення, що допоможе реалізувати послугу ДС-1 (Стійкість при обмежених відмовах). Варіантами встановлення антивірусу можна виділити такі, як тільки на сервері, або для всіх 11 пристроїв системи.

Для порівняння було обрано три антивіруси:

– ESET Server Security для Microsoft Windows;

– Zillya! Антивірус для Бізнесу;

– AVG Ultimate.

Порівняння наведено в таблиці 2.1.

Таблиця 2.1 – Порівняння антивірусного програмного забезпечення

№	Характеристика	ESET Server Security для Microsoft Windows	Zillya! Антивірус для Бізнесу	AVG Ultimate
1	Версія	10.X	1.1.xxxx.y	24.3

Продовження таблиці 2.1

№	Характеристика	ESET Server Security для Microsoft Windows	Zillya! Антивірус для Бізнесу	AVG Ultimate
2	Вартість	7200грн на 1рік, при встановленні на одному сервері	7300грн на 1 рік за 11 пристроїв	3200грн на 1 рік за 10 пристроїв (максимальна кількість пристроїв по одній підписці)
3	Функціонал	система запобігання вторгненням (HIPS) здійснює моніторинг активності системи; розширений сканер пам'яті; покращення виявлення відомих уразливостей на мережевому рівні; ESET LiveGuard Advanced забезпечує ще один рівень безпеки, використовуючи хмарну технологію пісочниці для виявлення нових загроз; консоль ESET PROTECT – це панель управління	антивірус – дозволяє виявляти та знешкоджувати шкідливе програмне забезпечення; панель адміністратора, що дозволяє налаштовувати і здійнсювати моніторинг всієї системи; антивірусний сервер, який об'єднує клієнтські частини і дозволяє управляти ними через панель адміністратора, поширює оновлення; брандмауер – контролює доступ в мережу; веб фільтр – керує доступом на вказаний централізований список небажаних сайтів	функція "Аналіз поведінки", що надсилає попередження, виявивши підозрілу поведінку; віддалене керування дає змогу централізовано налаштовувати AVG на всіх ПК мережі; Smart Scanner – покращений модуль сканування; CyberCapture – блокує нові загрози за допомогою автоматичного надсиланню підозрілих файлів у лабораторію
4	Централізоване керування	з системою централізованого керування захистом корпоративних мереж ESET PROTECT	панель адміністратора – центр управління всіма Клієнтськими частинами та налаштуваннями Антивірусного сервера	забезпечується централізоване керування з єдиного центру

Продовження таблиці 2.1

№	Характеристика	ESET Server Security для Microsoft Windows	Zillya! Антивірус для Бізнесу	AVG Ultimate
5		-	оновлення антивірусних баз на комп'ютерах організації відбувається централізовано і не вимагає підключення окремих ПК до мережі Інтернет. Всі оновлення ПК в мережі будуть отримувати з серверної частини антивіруса	забезпечується централізоване оновлення з єдиного центру
6	Наявність рекомендації від Держспецзв'язку	+	+	-

Беручи до уваги результати порівняння антивірусів, ESET Server Security дає потужний набір захисних механізмів, але для встановлення на всіх пристроях системи підприємства стає необхідним знаходження додаткового інструменту, так як даний антивірус працює тільки з сервером, такоє можна виділити високу вартість антивірусу.

Антивірус AVG Ultimate є досить дешевим варіантом для встановлення, але за однієї підписки він не може задіяти всі пристрої системи підприємства, що створює додаткові незручності, та має мінус у відсутності позитивного експертного висновку від Держспецзв'язку.

Антивірус «Zillya! Антивірус для Бізнесу» має середню ціну, може задіяти всі пристрої системи та забезпечити централізоване керування та оновлення всіх пристроїв системи від адміністатора.

Прийнято рішення обрати для використання антивірус «Zillya! Антивірус для Бізнесу». Антивірус також за допомогою свого функціоналу забезпечує реалізацію послуги НР-2 (Захищений журнал).

Перелік антивірусів, що мають позитивний експертний висновок, і відповідно обраний антивірус можна переглянути на сайті Центру антивірусного захисту інформації [4].

Відповідальним за оновлення антивірусного програмного забезпечення встановлено адміністратора безпеки. Оновлення має відбуватись кожен день, перед початком робочого процесу. Процес оновлення буде відбуватись згідно Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації [5].

За організацію оновлень для антивірусного програмного забезпечення, що входить до переліку антивірусів з позитивним експертним висновком, приймає відповідальність Адміністрація Держспецзв'язку.

2.4 Реалізація розподілу обов'язків

В системі в даний момент реалізована лише одна адміністративна роль для прожект-менеджера – системний адміністратор.

Дивлячись на наявну матрицю розмежування доступу можна побачити деяку надлишковість, що в свою чергу може призвести до негативних наслідків. Тому було прийняте рішення ввести другу адміністративну роль – адміністратор безпеки.

Адміністратором безпеки вирішено зробити директора підприємства. В обов'язки адміністратора безпеки буде входити створення облікових записів користувачів, перегляд журналу подій.

Відповідно, прожект-менеджеру, окрім ролі системного адміністратора буде надано додаткову роль звичайного користувача. В матрицю розмежування доступу додано тип інформації – програмне забезпечення.

Далі необхідно оновити наявну матрицю розмежування доступу, додати нові облікові записи, записати права доступу та окремим типом інформації зазначено журнал подій, так як з новою роллю адміністратора безпеки з'являється потреба перегляду подій, що відбуваються в системі підприємства.

Оновлена матриця розмежування доступу наведена в табл. 2.2.

Таблиця 2.2 – Оновлена матриця розмежування доступу

№	Інформація	Користувачі								
		Прожект-менеджер		Менеджер з продажу	Спеціаліст колцентру	Директор		Бухгалтер	Логіст	SMM-спеціаліст / Контент-мейкер
		Системний адміністратор	Користувач			Адміністратор безпеки	Користувач			
1	Організаційно-розпорядча	R	RWD	R	R	R	RWD	R	R	R
2	Дані про клієнтів	–	–	RWD	RW	–	RWD	–	–	–
3	Інвентарізаційні дані	–	RWDP	RWDP	–	–	RWD	–	–	–
4	Договори закупки товару	–	–	–	–	–	RWD	–	–	–
5	Замовлення клієнта	–	–	RWD	RW	–	RWD	–	–	–
6	Бухгалтерська звітність	–	–	–	–	–	RWD	RWD	–	–
7	Матеріали для реклами	–	–	–	–	–	RWD	–	–	RWD
8	Дані про вартість товарів та ремонт	–	–	RWD	RW	–	RWD	–	–	–
9	Дані про співробітників	–	RWD	–	–	–	RWD	–	–	–
10	Логістичні дані	–	–	–	–	–	RWD	–	RWD	–
11	Журнал подій	R	–	–	–	RWD	R	–	–	–
12	Програмне забезпечення	RWD	R	R	R	R	R	R	R	R

Позначення:

– R (читання);

– W (запис);

– D (видалення);

– P (друкування).

2.5 Впровадження резервного копіювання

В роботі підприємства використовується велика кількість різної інформації до якої може бути потрібний постійний доступ та втрата якої може привести до сповільнення функціонування робочого процесу. Впровадження резервного копіювання допоможе реалізувати послугу ЦО-1 (обмежений відкат), а також послугу ДВ-1 (ручне відновлення) створивши копію всієї системи, яку відновити матиме змогу лише адміністратор.

Резервне копіювання можна реалізувати у вигляді зовнішнього накопичувача, RAID-масиву або хмарного сховища. в табл. 2.3 наведена порівняльна характеристика цих трьох варіантів.

Таблиця 2.3 – Порівняльна характеристика технологій резервного копіювання

№	Характеристика	RAID-масив	Зовнішній накопичувач	Хмарне сховище
1	Вартість	Потребує високої вартості для купівлі обладнання	Не потребує великих витрат	В залежності від вибору сервісу, рівня бажаного функціоналу може потребувати великих витрат
2	Доступ	Постійний доступ з максимальною швидкістю	Обмежений доступ, можливий тільки при підключенні накопичувача	Повна доступність, але з залежністю від мережі Інтернет

Продовження таблиці 2.3

№	Характеристика	RAID-масив	Зовнішній накопичувач	Хмарне сховище
3	Складність у встановленні та обслуговуванні	Досить складний варіант для встановлення та обслуговування, що потребує професійних навичок. Потребує виділення додаткового місця для встановлення	Досить простий в обслуговуванні. Потребує місця для зберігання накопичувача.	Певна складність при налаштуванні системи. Все зберігається віддалено та не потребує виділення додаткового місця на підприємстві
4	Безпека	Має високу надійність через розподіл даних між кількома дисками	Існує можливість втрати даних в разу пошкодження або втрату накопичувача	Зазвичай має високий рівень захисту даних (шифрування, автентифікація). Потребує правильного вибору постачальника послуг
5	Масштабованість	Легко масштабується встановленням додаткових дисків	Може потребувати купівлі додаткового накопичувача	Легке збільшення обсягу збереження даних, в разі потреби змінюється тарифний план

Беручи до уваги результати порівняння технологій та інформацію про те, що на підприємстві не передбачена робота з зовнішніми накопичувачами, та не передбачена максимальна оперативність, що надає RAID-масив. Також те , що підприємство включає в свій штаб віддалених працівників, робить хмарне сховище більш привабливим тому було вирішено в подальшому використовувати саме цю технологію.

Згідно з Законом України «Про хмарні послуги» [3, с. 12]:

Кабінет Міністрів України встановлює порядок надання хмарних послуг та/або послуг центру обробки даних, пов’язаних з обробкою державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо

захисту якої встановлена законом, що базується на принципах інтероперабельності та збереження конкуренції, і визначає порядок:

– обов'язкового резервного копіювання та збереження резервних копій у незалежних системах;

– передачі даних від користувача хмарних послуг до надавача хмарних послуг та/або послуг центру обробки даних для забезпечення надання хмарних послуг, а також від надавача хмарних послуг до користувача хмарних послуг;

– передачі даних від одного надавача хмарних послуг та/або послуг центру обробки даних до іншого;

– надання інформації, необхідної для оцінювання безпеки мережевих та інформаційних систем надавачів хмарних послуг та/або послуг центру обробки даних, у тому числі документально встановленої політики безпеки.

Згідно рекомендацій наданих Держспецзв'язку, було вирішено використати хмарну технологію з позитивним експертним висновком «GigaCloud».

Розраховується використовувати послугу BAAS (Backup as a Service), іншими словами – резервне копіювання IT-інфраструктури. Сервіс бекапування (BaaS) – це поєднання трьох складових: хмарні сховища GigaCloud, дата-центр рівня Tier III і технологія Veeam Cloud Connect. Завдяки високій експертизі, GigaCloud має статус «золотого партнера» Veeam. Послуга є доступної у декількох варіантах, для нашої системи обирається варіант – послуга бекапування з власної віртуалізованої інфраструктури у хмару GigaCloud [6].

2.6 Політика порядку використання резервного копіювання

Мета: застосування технології резервного копіювання відбувається для уникнення затримок у функціонуванні роботи підприємства, через втрату доступності або спотворення інформації, що використовується.

Галузь застосування: політика порядку використання резервного копіювання застосовується до всіх системних даних та інформації з обмеженим доступом.

Інструкція: на початку кожного робочого дня виконується повне копіювання стану системи зі всіма конфігураціями, за це є відповідальним адміністратор безпеки.

Повинно виконуватись регулярне резервне копіювання два рази на день, та позапланово в разі потреби за рішенням користувача за інкрементним алгоритмом, тобто кожен раз відбувається запис файлів, лише в яких присутні зміни, що були виконані з часу минулого резервного копіювання.

Доступ до резервних копій в хмарному сховищі регулюється адміністратором безпеки.

В разі потреби у відновленні останнього працюючого стану системи, адміністратор безпеки має в ручну виконати відновлення системи.

2.7 Політика безпеки робочого місця

Мета: забезпечити захист інформації від доступу до неї особам, яким не передбачено володіння нею, реалізація послуги достовірного каналу та уникнення прямої видимості об’єктів.

Галузь застосування: політика безпеки робочого місця застосовується до усіх місць де відбувається робота з технічними засобами, що обробляють інформацію з обмеженим доступом.

Інструкція: політика визначає, в якому вигляді працівник повинен залишати своє робоче місце, коли він залишає його без нагляду та у кінці робочого дня. Працівник має дотримуватися наступних правил: персональні комп'ютери повинні вимикатися після закінчення роботи з ними; у разі покидання працівника свого робочого місця, він має заблокувати або вимкнути свій ПК; забороняється доступ та користування ПК працівника сторонніми особами; після закінчення робочого дня працівник підприємства повинен залишати своє робоче місце у чистоті.

Введення користування фільтрами для захисту екрану, які дозволяють бачити екран лише особі, що сидить перед ним прямо, тобто зменшують кут видимості та відповідно ускладнюють перегляд з боку.

Проведення організаційних заходів з навчання персоналу з питань соціальної інженерії, для захисту від методів маніпуляції або обману персоналу з метою отримання доступу до системи.

Відповідальність за реалізацію та контроль покладено на адміністратора безпеки.

2.8 Процедура самотестування системи

В системі вже існує можливість самотестування системи при старті. Це має можливість реалізовуватись за допомогою BIOS. Так як комп'ютер є складним пристроєм, то відповідно недієздатність одного з компонентів призведе до помилок в роботі або до відмови. Тому передбачено процедуру POST – Power-On Self Test.

Для реалізації послуги достатньо активізувати даний механізм в BIOS. Безпосередньо перед запуском при виконанні POST відбувається перевірка та налаштування всього апаратного забезпечення, сюди входить як оперативна пам'ять, процесор, відеокарта, так і драйвери, системні файли.

2.9 Забезпечення резервного живлення

Для запобігання втрати даних та помилок при проведенні операцій при відключенні електроенергії стає необхідним забезпечення системи резервним живленням. Прийнято рішення забезпечити систему не постійним резервним живленням, а створити можливості для коректного завершення робочого процесу за короткий час.

Віддалені працівники працюють з ноутбуків відповідно для них не є за потрібним купівля додаткового обладнання для живлення. На території магазину купівля додаткового обладнання є необхідною для встановлених IMac (4 пристроя) та мережевого обладнання (маршрутизатор та точка доступу з PoE адаптером). В табл. 2.4 розрахована потужність вказаних пристроїв.

Таблиця 2.4 – Розрахунок потужності пристроїв

№	Пристрій	Потужність, Вт	Кількість	Загальна потужність, Вт
1	IMac	101	4	404
2	Маршрутизатор	33	1	33
3	Точка доступу	20	1	32
	PoE адаптер	12	1	

Враховуючи розташування пристроїв на підприємстві прийнято рішення розділити пристрої на декілька груп. Перша група – це IMac, що розташований у торгівельній залі. Друга група – три IMac на складі та мережеве обладнання.

В загальному вирішено придбати два безперебійники. Для першої групи буде достатньо одного безперебійника з невеликою потужністю та щонайменше однією розеткою, якого буде достатньо для того, щоб дати потужність на один IMac, тобто більшу за 101Вт з додатковим запасом. Для порівняння взято три варіанти, які наведені в табл. 2.5.

Таблиця 2.5 – Порівняльна характеристика безперебійників для першої групи

№	Характеристика	UPS EnerGenie Basic	UPS SEVEN PS-7954	UPS 1000VA LED KD1927
1	Вартість	2000грн	1170грн	3000грн
2	Потужність	390Вт	60Вт	600Вт
3	Тип архітектури	лінійно-інтерактивна	резервна	лінійно-інтерактивна
4	Кількість розеток	2	1	4

Беручи до уваги результати порівняння, можна сказати що безперебійник SEVEN PS-7954 буде недостатньо потужним, а безперебійник 1000VA LED KD1927 є більшим дорожчим та надлишково потужним, тому вирішено обрати безперебійник EnerGenie Basic.

Для другої групи згідно з розрахунком потужностей та кількістю пристрої, потрібно обрати безперебійник, який матиме змогу дати потужність більшу за – 368 Вт та з кількістю розеток щонайменше п'яти. Для порівняння взято три варіанти, які наведені в табл. 2.6.

Таблиця 2.6 – Порівняльна характеристика безперебійників для другої групи

№	Характеристика	UPS Ritar U-Smart-1000	UPS Powercom MAC-3000 IEC	UPS Powercom BNT-600A Schuko
1	Вартість	4900грн	30000грн	3500грн
2	Потужність	600Вт	3000Вт	500Вт
3	Тип архітектури	лінійно-інтерактивна	безперервної дії	лінійно-інтерактивна
4	Кількість розеток	8	8	4

Беручи до уваги результати порівняння можна сказати, що безперебійник UPS Powercom MAC-3000 IEC має досить надлишкову високу потужність та велику ціну, а безперебійник UPS Powercom BNT-600A Schuko виявивсь з недостатньою кількістю розеток та з малим додатковим запасом потужності, тому вирішено обрати безперебійник UPS Ritar U-Smart-1000.

Для забезпечення можливості в короткий час мати доступ до мережі Інтернет можна використати 4G LTE USB модем, який завжди буде встановлено в маршрутизатор та буде підключеним до мобільного оператора, та буде працювати як резервний канал для Інтернет, на випадок зникнення основного каналу провайдера.

Серед популярних моделей важко виділити конкретну модель, так як за характеристиками вони є досить схожими, вирішено обрати модем моделі Olax U90H-E, який має зазначену швидкість до 150 Мб/с.

В якості оператора обрано Vodafone, так як в даний час він себе зарекомендував більш надійним серед своїх конкурентів.

Також повинна бути виконана купівля цього модему для кожного з віддалених працівників, щоб у них також була можливість створити резервний канал Інтернет.

При аварійній ситуації, після завершення останньої операції, користувач повинен виконати позапланове резервне копіювання.

2.10 Висновки до Розділу 2

У другому розділі було проведено аналіз визначеного профілю захищеності, з визначенням рівня його реалізації в системі. Наступним кроком було запропоновано проектні рішення, які дозволять виконати реалізацію необхідних послуг безпеки.

Таким чином, при умові впровадження запропонованих процедур та політик безпеки, буде забезпечено заданий профіль захищеності – 3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДС-1, ДЗ-2, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-1, НТ-2, НВ-1 }, що є основою для забезпечення необхідного рівня захисту інформації, яка обробляється в ІКС.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Центральною метою виконання економічного розділу є техніко-економічне обґрунтування доцільності запровадження комплексної системи захисту інформації на підприємстві магазину роздрібної торгівлі «GetApple».

Обґрунтування доцільності впровадження буде роз'яснюватись в подальших пунктах:

1. Розрахунок капітальних витрат на придбання і налагодження головних аспектів системи інформаційної безпеки або витрат, що є пов'язаними з виготовленням апаратури, приладів, програмного забезпечення.

2. Розрахунок річних експлуатаційних витрат на утримання і обслуговування запровадженої комплексної системи захисту інформації.

3. Визначення річного економічного ефекту після введення комплексної системи захисту інформації.

4. Визначення та аналіз показників економічної ефективності запропонованого проектного рішення.

5. Висновок про економічну доцільність введення комплексної системи захисту інформації.

3.1 Обчислення капітальних витрат

Фіксовані (капітальні) витрати здійснюються на етапі створення системи інформаційної безпеки.

3.1.1 Обчислення трудомісткості розробки комплексної системи захисту інформації

Трудомісткість розробки комплексної системи захисту інформації з'ясовується тривалістю кожної робочої операції та встановлюється за наступною формулою:

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

де tтз – час створення технічного завдання;

tв – час розробки концепції безпеки інформації на підприємстві;

tа – час проведення аналізу ризиків від актуальних загроз;

tвз – час формулювання вимог до заходів, методів та засобів захисту;

tозб – час вибору основних рішень з забезпечення безпеки інформації;

tовр – час організації виконання відновлювальних робіт і забезпечення неперервного функціонування підприємства;

tд – час документального оформлення політики безпеки.

Кожна з робочих операцій мають наступні значення часу:

– tтз = 14 годин;

– tв = 13 годин;

– tа = 18 годин;

– tвз = 16 годин;

– tозб = 13 годин;

– tовр = 10 годин;

– tд = 8 годин.

Далі виконується розрахунок трудомісткості розробки комплексної системи захисту інформації за допомогою формули (3.1):

$$t = 14 + 13 + 18 + 16 + 13 + 10 + 8 = 92 \text{ години}$$

3.1.2 Обчислення фінансових витрат на введення комплексної системи захисту інформації

Витрати на впровадження комплексної системи захисту інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для впровадження комплексної системи захисту інформації Змч та встановлюються за наступною формулою:

$$\text{Крп} = \text{Ззп} + \text{Змч}, \quad (3.2)$$

Заробітна плата спеціаліста з інформаційної безпеки включає основну і додаткову заробітну плату та встановлюються за наступною формулою:

$$\text{Ззп} = t \cdot \text{Зіб}, \quad (3.3)$$

де t – час розробки комплексної системи захисту інформації, годин;

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

Час розробки системи становить – 92 години.

Середньогодинну заробітну плату взято в розмірі – 170 гривень.

Розрахуємо заробітну плату спеціаліста з інформаційної безпеки за формулою (3.3):

$$\text{Ззп} = 92 \cdot 170 = 15640 \text{ грн}$$

Вартість машинного часу витраченого при розробці КСЗІ на ПК визначається за наступною формулою:

$$\text{Змч} = t \cdot \text{Смч}, \quad (3.4)$$

де t – трудомісткість розробки КСЗІ на ПК, годин;

Смч – вартість 1 години машинного часу ПК, грн/година.

Трудомісткість розробки КСЗІ на ПК становить – 92 години

Вартість 1 години машинного часу ПК визначається за наступною формулою:

$$\text{Смч} = P \cdot \text{Се} + \frac{\text{Фзал} \cdot Ha}{Fp} + \frac{Клпз \cdot Напз}{Fp}, \text{ грн}, \quad (3.5)$$

де *Р* – встановлена потужність ПК, кВт;

Се – тариф на електричну енергію, грн/кВт · година;

Фзал – залишкова вартість ПК на поточний рік, грн;

На – річна норма амортизації на ПК, частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення, грн;

Fр – річний фонд робочого часу.

В розрахунок береться один ПК потужністю 0,3 кВт.

Тариф на електричну енергію зараз становить – 4,32 грн/кВт·год.

Річний фонд робочого часу, за 40-годинного робочого тижня становить – 1920).

Вартість ліцензійного програмного забезпечення (Zillya! Антивірус для Бізнесу) становить – 7300 грн.

Річна норма амортизації на ПК становить – 0,2.

Річна норма амортизації на ліцензійне програмне забезпечення становить – 0,4.

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання. Первісна вартість ПК становить – 18000 грн, мінімальний термін корисної служби становить – 50 місяців.

$$\text{Фзал} = 18000 - \frac{18000 \cdot 40}{50} = 3600 \text{ грн}$$

Розрахуємо вартість 1 години машинного часу ПК за формулою (3.5):

$$\text{Смч} = 0{,}3 \cdot 4{,}32 + \frac{3600 \cdot 0{,}2}{1920} + \frac{7300 \cdot 0{,}4}{1920} = 3{,}2 \text{ грн}$$

Розрахуємо вартість машинного часу витраченого при розробці КСЗІ за формулою (3.4):

$$Змч = 92 \cdot 3{,}2 = 294{,}4 \text{ грн}$$

Розрахуємо витрати на впровадження комплексної системи захисту інформації за формулою (3.2):

$$Крп = 15640 + 294{,}4 = 15934{,}4 \text{ грн}$$

Визначена таким чином вартість розробки КСЗІ Крп є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = Крп + Кзпз + Каз + Кнавч + Кн, \quad (3.6)$$

де Крп – вартість розробки КСЗІ та залучення зовнішніх консультантів, грн;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), грн;

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, грн;

Кнавч – витрати на навчання технічних фахівців і осблуговуючого персоналу, грн;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, грн.

Вартість закупівель ліцензійного основного й додаткового програмного забезпечення становить – 7300 грн.

Вартість закупівлі апаратного забезпечення в загальній сумі (Два безперебійники – 6900 грн, п'ять модемів – 4000 грн) становить – 10900 грн.

Витрати на навчання технічних фахівців і осблуговуючого персоналу становлять – 6000 грн.

Витрати на встановлення обладнання та налагодження системи становлять – 4000 грн.

Відповідно розрахуємо капітальні (фіксовані) витрати за формулою (3.6):

$$К = 15934{,}4 + 7300 + 10900 + 6000 + 4000 = 44134{,}4 \text{ грн}$$

3.2 Обчислення поточних (експлуатаційних) витрат

Наступним кроком буде обчислення витрат, яких зазнає підприємство під час експлуатації впровадженої комплексної системи захисту інформації.

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = Св + Ск + Сак, \text{ грн}, \quad (3.7)$$

де Св – вартість відновлення й модернізації системи;

Ск – витрати на керування системою в цілому;

Сак – витрати, викликані активністю користувачів системи інформаційної безпеки.

Вартість відновлення й модернізації системи становить – 0, так як всі оновлення є постійними після придбання та не потребують додаткових витрат.

Витрати, викликані активністю користувачів системи інформаційної безпеки також становлять – 0.

Витрати на керування КСЗІ (Ск) складають:

$$Ск = Сн + Са + Сз + Сєв + Сел + Со + Стос, \text{ грн}, \quad (3.8)$$

де Сн – витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи;

Са – річний фонд амортизаційних відрахувань, грн;

Сз – річний фонд заробітної плати інженерно-технічного персоналу, грн;

Сєв – витрати єдиного внеску на загальнообов'язкове соціальне страхування, грн;

Сел – вартість електроенергії, що споживається апаратурою КСЗІ протягом року, грн;

Со – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу, грн;

Стос – витрати на технічне й організаційне адміністрування та сервіс КСЗІ визначаються у відсотках від вартості капітальних витрат, грн.

Витрати на навчання адміністративного персоналу й кінцевих користувачів становлять – 4500 грн.

Річний фонд амортизаційних відрахувань розраховується діленням вартості програмного забезпечення на термін корисного його використання, який становить – 2 роки:

$$Са = \frac{7300}{2} = 3650 \text{ грн}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки (Сз), складає:

$$Сз = Зосн + Здод, \text{ грн} \qquad (3.9)$$

Роботами з інформаційної безпеки займаються прожект-менеджер (системний адміністратор) та директор (адміністратор безпеки), плата за обслуговування системи становить частку 0,2 від їх заробітної плати. Тому користуючись табл. 3.1, розрахуємо річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки за формулою (3.9):

$$Сз = (18000 \cdot 0{,}15 + 40000 \cdot 0{,}15) \cdot 12 = 104400 \text{ грн}$$

З 01.01.2016 року ставка ЄСВ становить – 22%. Таким чином, витрати єдиного внеску на загальнообов'язкове соціальне страхування становлять:

$$Сєв = 104400 \cdot 0{,}22 = 20880 \text{ грн}$$

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

$$Сел = P \cdot Fp \cdot Це, \text{ грн}, \qquad (3.10)$$

де P – встановлена потужність апаратури інформаційної безпеки;

Fp – річний фонд робочого часу КСЗІ;

Це – тариф на електроенергію;

Встановлена потужність становить – 1 кВт.

Річний фонд робочого часу КСЗІ – становить 2288 годин (при 44-х годинному тижні).

Тариф на електроенергію становить – 4,32 грн/кВт·год.

Таким чином вартість електроенергії, що споживається апаратурою КСЗІ протягом року за формулою (3.10):

$$Сел = 1 \cdot 2228 \cdot 4{,}32 = 9625 \text{ грн}$$

Витрати на залучення сторонніх організацій становлять – 0 грн.

Для визначення витрат на технічне й організаційне адміністрування та сервіс КСЗІ необхідно взяти відсоток (5%) від капітальних витрат (К):

$$\text{Стос} = 0{,}05 \cdot 44134{,}4 = 2206{,}72$$

Таким чином витрати на керування КСЗІ (Ск) за формулою (3.8) складають:

$$\text{Ск} = 4500 + 3650 + 104400 + 20880 + 9625 + 2206{,}72 = 145261{,}8 \text{ грн}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки за формулою (3.7) складають:

$$\text{С} = 145261{,}8 \text{ грн}$$

3.3 Оцінка можливого збитку від атаки

Втрачений прибуток через простій атакованого вузла або сегмента корпоративної мережі дорівнює:

$$U = \text{П}_\text{п} + \text{П}_\text{в} + V, \text{ грн}, \qquad (3.11)$$

де $\text{П}_\text{п}$ – оплачувані втрати робочого часу та простої працівників вузла, що було атаковано;

$\text{П}_\text{в}$ – вартість відновлення працездатності сегмента системи;

V – втрати через затримки в функціонуванні системи.

Втрати до яких призвело зниження продуктивності працівників, сегмент системи яких було атаковано, являють собою втрати їх заробітної плати за час простою після проведеної атаки та розраховуються за наступною формулою:

$$П_п = \frac{\sum Зс}{F} \cdot t_п, \text{ грн}, \quad (3.12)$$

де Зс – заробітна плата працівника, сегмент системи якого було атаковано;

F – місячний фонд робочого часу;

tп – час простою сегмента після проведеної атаки.

Місячний фонд робочого часу при 44-х годинному робочому тижні становитиме – 186 годин.

Простій системи буде дорівнювати – 4 години.

Далі в таблиці 3.1 вказано заробітну плату штабу працівників.

Таблиця 3.1 – Перелік заробітної плати

№	Посада	Кількість працівників	Заробітна плата на місяць, грн
1	Прожект-менеджер	1	18000
2	Менеджер з продажу	3	21000
3	Спеціаліст колцентру	2	15000
4	Директор	1	40000
5	Бухгалтер	1	17000
6	Логіст	1	15000
7	SMM-спеціаліст	1	18000
8	Контент-мейкер	1	13000

$$\sum Зс = 214000 \text{ грн}$$

Втрати до яких призвело зниження продуктивності працівників, розраховується за формулою (3.12):

$$Пп = \frac{214000}{186} * 4 = 4602 \text{ грн}$$

Витрати, яких потребує відновлення працездатності сегмента розраховується наступним чином:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн}, \quad (3.13)$$

де $П_{ви}$ – витрати, що необхідні для повторного уведення інформації;

$П_{пв}$ – витрати на відновлення сегменту системи;

$П_{зч}$ – вартість, що потрібна для заміни обладнання

Вартість, що потрібна для заміни обладнання становить – 6000 грн.

Витрати, що необхідні для повторного уведення інформації, розраховуються за наступною формулою:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви}, \text{ грн}, \quad (3.14)$$

де tви – час повторного уведення загубленої інформації працівниками.

Час повторного уведення буде дорівнювати – 2 години:

$$Пви = \frac{214000}{186} \cdot 2 = 2301 \text{ грн}$$

Витрати на відновлення сегменту системи будуть залежати від частки заробітної плати обслуговуючого персоналу (адміністраторів), розраховуються за наступною формулою:

$$Ппв = \frac{\sum Зо}{F} \cdot t_в, \text{ грн}, \quad (3.15)$$

де tв – час відновлення сегменту обслуговуючим персоналом;

Зо – заробітна плата обслуговуючого персоналу.

Час відновлення сегменту буде дорівнювати – 3 години.

Заробітна плата обслуговуючого персоналу буде становити:

$$Зо = 40000 \cdot 0{,}15 + 18000 \cdot 0{,}15 = 8700 \text{ грн}$$

Таким чином витрати на відновлення сегменту системи за формулою (3.15) складуть:

$$Ппв = \frac{8700}{186} \cdot 3 = 140 \text{ грн}$$

Витрати, яких потребує відновлення працездатності сегмента розрахуємо за формулою (3.13):

$$Пв = 2301 + 140 + 6000 = 8441 \text{ грн}$$

Втрати через затримки у функціонування системи розраховуються за наступною формулою:

$$V = \frac{O}{Fr} \cdot (t\text{п} + t\text{в} + t\text{ви}), \text{ грн}, \quad (3.16)$$

де Fr – річний фонд робочого часу підприємства;

О – обсяг продажів атакованого сегменту, грн у рік.

Річний фонд робочого часу становитиме (52 робочих тижні, 6-ти денний робочий тиждень, будні 8-ми годинний робочий день, субота – 4-х) – 2228 годин.

Обсяг продажів атакованого сегменту взято у розмірі – 4500000грн/рік.

Таким чином втрати через затримки у функціонування системи за формулою (3.16) складуть:

$$V = \frac{4\,500\,000 \text{ грн/рік}}{2228 \text{ год}} \cdot (4 + 2 + 3) = 18177 \text{ грн.}$$

Розрахуємо втрачений прибуток від атаки за формулою (3.11):

$$U = 4602 + 8441 + 18177 = 31220 \text{ грн}$$

Загальний збиток від атаки на сегмент розраховується за наступною формулою:

$$B = \sum i \cdot \sum n \cdot U, \text{ грн}, \quad (3.17)$$

де I – число атакованих сегментів;

N – середня кількість атак на рік.

Число атакованих сегментів взято в розмірі – 3.

Середня кількість атак на рік взята в розмірі – 4.

Відповідно загальний збиток згідно формули (3.17) складе:

$$B = \sum 3 \cdot \sum 4 \cdot 31220 = 374640 \text{ грн}$$

3.4 Загальний ефект від впровадження комплексної системи захисту інформації

При знаходженні загального ефекту від впровадження комплексної системи захисту інформації враховуються ризики порушення інформаційної безпеки та розраховується за наступною формулою:

$$E = B \cdot R - C, \text{ грн}, \quad (3.18)$$

де B – загальний збиток після атаки на сегмент, грн;

R – очікувана ймовірність атаки на сегмент, частки одиниці;

C – щорічні витрати на експлуатацію комплексної системи захисту інформації.

Очікувана ймовірність атаки на сегмент взята в розмірі – 0,6

$$E = 374640 \cdot 0{,}6 - 145261{,}8 = 60791 \text{ грн}$$

3.5 Визначення та аналіз показників економічної ефективності комплексної системи захисту інформації

Для визначення економічної ефективності знадобиться спочатку визначити показник ROSI (коефіцієнт повернення інвестицій), за наступною формулою:

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \quad (3.19)$$

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

K – капітальні інвестиції, що забезпечили даний ефект, тис. грн.

$$ROSI = \frac{60791}{44134{,}4} = 1{,}38$$

Проєкт системи інформаційної безпеки є доцільним при умові, що показник ROSI більший ніж величина річної депозитної ставки з урахуванням інфляції:

$$ROSI > \frac{N\text{деп} - N\text{інф}}{100}, \text{ частки одиниці,} \quad (3.19)$$

де Nдеп – річна депозитна ставка, %;

Nінф – річний рівень інфляції, %.

Річна депозитна ставка становить – 16%.

Річний рівень інфляції становить – 5,5%.

$$1{,}38 > \frac{16 - 5{,}5}{100}$$

$$1{,}38 > 0{,}105$$

Наступним розраховується термін окупності капітальних інвестицій То, що показує час який потрібно щоб окупити капітальні інвестиції за рахунок загального ефекту від впровадження системи інформаційної безпеки, за наступною формулою:

$$\text{То} = \frac{\text{К}}{\text{Е}}, \text{ частки одиниці,} \quad (3.20)$$

$$\text{То} = \frac{44134{,}4}{60791} = 0{,}73, \text{що становить} - 9 \text{ місяців}$$

3.6 Висновок до Розділу 3

У третьому розділі було виконано обґрунтування економічної доцільності впровадження КСЗІ на підприємстві «GetApple». При обґрунтуванні виконувались розрахунки наступних значень:

– фіксованих (капітальних) витрат, які здійснюються на етапі створення системи інформаційної безпеки;

– витрат, яких зазнає підприємство під час експлуатації впровадженої комплексної системи захисту інформації;

– коефіцієнта повернення інвестицій ROSI, який склав 1,38, що дозволило встановити доцільність впровадження комплексної системи захисту інформації;

– термін окупності капітальних інвестицій То, який склав 9 місяців, що дозволило встановити час, який потрібно щоб окупити капітальні інвестиції за рахунок загального ефекту від впровадження системи інформаційної безпеки.

ВИСНОВКИ

Основною метою роботи є забезпечення необхідного рівня захисту інформації, яка обробляється в ІКС, за рахунок впровадження КСЗІ.

У першому розділі було виконано:

– опис відомості про підприємство;

– обґрунтування необхідності створення КСЗІ;

– обстеження середовищ функціонування (фізичне середовище, обчислювальне середовище, інформаційне середовище та середовище користувачів);

– розробка моделі порушника та моделі загроз;

– формування профілю захищеності на основі актуальних загроз.

Що дало обґрунтування необхідність створення КСЗІ для системи підприємства «GetApple»

У другому розділі було виконано аналіз сформованого профілю захищеності. Далі було запропоновано проектні рішення, для підвищення рівня безпеки, такі як: матриця розмежування доступу, положення політики безпеки щодо: антивірусного захисту, безпеки робочого місця, резервного живлення та резервного копіювання.

У третьому розділі було виконано обґрунтування економічної доцільності впровадження КСЗІ на підприємстві «GetApple». При обґрунтуванні виконувались розрахунки фіксованих (капітальних) витрат та витрат, яких зазнає підприємство під час експлуатації КСЗІ. Було виконано підтвердження доцільності запропонованих рішень, визначивши коефіцієнт повернення інвестицій ROSI, що дорівнює – 1,38 та термін окупності капітальних інвестицій То, що дорівнює 9 місяців.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР: станом на 4 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 28.05.2024).

2. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Каб. Міністрів України від 29.03.2006 р. № 373: станом на 21 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text (дата звернення: 28.05.2024).

3. Про хмарні послуги: Закон України від 17.02.2022 р. № 2075-IX: станом на 4 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text (дата звернення: 07.06.2024).

4. Центр антивірусного захисту інформації: перелік. URL: https://cazi.gov.ua/uk/verified-releases (дата звернення: 12.06.2024).

5. Про затвердження Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації: Наказ Адмін. Держ. служби спец. зв'язку та зах. інформації України від 26.03.2007 р. № 45: станом на 10 січ. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/z0320-07#Text (дата звернення: 12.06.2024).

6. GigaCloud: бекап у хмарі (BAAS). URL: https://gigacloud.ua/offer/baas (дата звернення: 13.06.2024).

7. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf (дата звернення: 27.06.2024)

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	32	
6	А4	2 Розділ	21	
7	А4	3 Розділ	15	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	
14	А4	Додаток Ґ	2	
15	А4	Додаток Д	1	
16	А4	Додаток Е	1	
17	А4	Додаток Є	2	

ДОДАТОК Б. Ситуаційний план

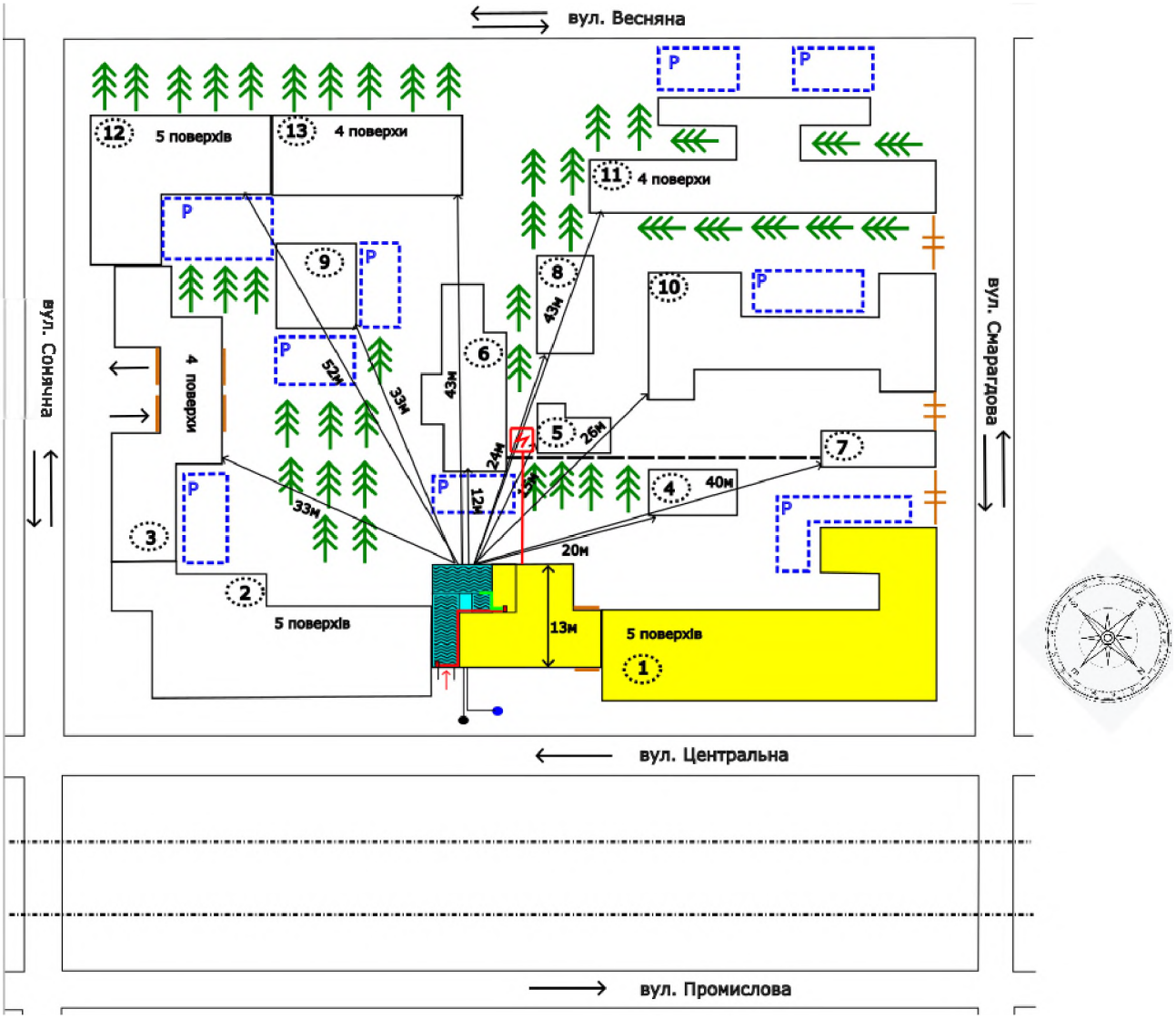

Рисунок Б.1 – Ситуаційний план

Умовні позначення до ситуаційного плану:

- Можливе місце парковки автомобілів
- Зона будівлі в якій знаходиться об’єкт
- Арка
- Ворота
- Дерево
- Вхід
- Трамвайні колії
- Лінія електропостання
- Трансформаторна підстанція
- Контрольована зона
- Прохід всередині приміщення
- Система каналізацій
- Паркан
- Напрям руху
- ОІД
- Електрощитова
- Лінія мережі Інтернет
- Система водопостачання

ДОДАТОК В. Генеральний план

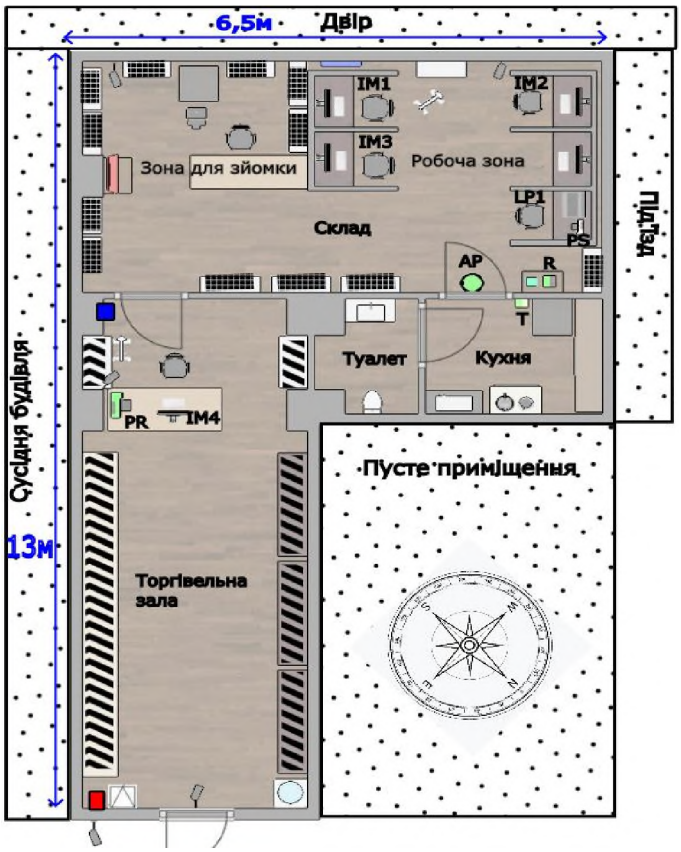

Рисунок В.1 – Генеральний план

Умовні позначення до генерального плану:

	Зона по сусідству з ОІД		Стелаж з технікою для продажу
	Стелаж з технікою готовою на продаж		Кондиціонер
	Обігрівач		Раковина
	Унітаз		Мікрохвильова піч
	Чайник		Кавомашина
	Кулер		POS термінал (**PR**)
	Принтер етикеток (**PS**)		Камера відеоспостереження
	Телевізор		Фотокамера
	iMac (**IM1-IM4**)		Ноутбук (**LP1**)
	Клавіатура		Точка доступу
	PoE адаптер		Маршрутизатор (**R**)
	Абонентський onu термінал (**T**)		Лічильник для води
	Електрощитова		ПКП

ДОДАТОК Г. Перелік допоміжних технічних засобів

Таблиця Г.1 – Перелік допоміжних технічних засобів

№	Назва	Модель	Серійний номер	Розміщення	Відстань до ОТЗ, м
1	Камера відеоспостереження (5 шт.)	IP камера Hikvision DS-2CD1321-I(F)	DS-2CD1234 DS-2CD1235 DS-2CD1236 DS-2CD1237 DS-2CD1238	За межами ОІД, торгівельна зала 2шт., склад 2шт.	6,2, 6, 1, 2,8, 2
2	ПКП	Охоронна централь DSC PC 1616 с клавиатурой PC1555RKZ	BOS-987654	Торгівельна зала, біля вхідних дверей	6
3	Датчик точковий магнітоконтактний	CoVi Security MC-25	ST-DWS-7890	Торгівельна зала, на вхідних дверях	6
4	Датчик об’ємний пасивний інфрачервоний (2 шт.)	Crow SRP-600	AAC123456	Торгівельна зала, склад	1,2, 1,2
5	Пожежний датчик (4 шт.)	Датчик пожежний димовий Артон СПД-3.4	KID-1234-ABCD KID-1234-JSKA KID-1234-XCKB KID-1234-QODI	Торгівельна зона (2 шт.), склад (2 шт.)	4, 2, 2,8, 2,8
6	Тривожна кнопка (2 шт.)	Кнопка тривожна IPTC	SAB-5678-XYZ SAB-5679-XYZ	Торгівельна зала (під столом), кухня (на стіні)	0,3, 0,2
7	Пожежна тривожна кнопка	Сповіщувач пожежний ручний Артон SPR-1	BAY-1234-5678	Торгівельна зала, біля вхідних дверей	6
8	Телевізор	Телевізор Samsung UE-43CU7172	A123B456C7890123	Склад, зона для зйомки, на стіні	3
9	Фотоапарат	Canon EOS R7 + RF-S 18-150 IS STM	1234F56789	Склад, зона для зйомки	1,8

Продовження таблиці Г.1

10	Кондиціонер	SAMSUNG AR09TXHQASINUA	CARR-SAM-987654	Склад	1,2
11	Обігрівач (2 шт.)	Конвектор електричний Ardesto CH-2000MCW	MELC-ARD-123456 MELC-ARD-123457	Торгівельна зала, склад	0,8, 1,3
12	Чайник	Електрочайник Holmer HKS-1510	HK789012A	Кухня	1,8
13	Кавомашина	PHILIPS HD7432/20	PI712012345	Кухня	1,7
14	Мікрохвильова піч	MYSTERY MMW-2013	MY781872345	Кухня	2
15	Кулер	Кулер для води HotFrost D65F	DAI781285LR	Торгівельна зала	6,2
16	PoE адаптер	POE-24-12W-G-WH	DLINK-9876-54321	Склад, на тумбочці	0,2
17	Миша (4 шт.) (до IM1-IM4)	Миша Apple Magic Mouse Bluetooth White (MK2E3ZM/A)	NG-PWR-1234-5670 NG-PWR-1234-5671 NG-PWR-1234-5672 NG-PWR-1234-5673	Склад 3шт., Торгівельна зала	0,1, 0,1, 0,1, 0,1

ДОДАТОК Ґ. Технічні характеристики складу ІКС

Таблиця Ґ.1 – Технічні характеристики складу ІКС

№	Назва	Назва в структурній схемі	Технічні характеристики	Серійний номер
1	Ноутбук	LP1	Процесор – десятиядерний Intel Core i5-1235U (0.9 - 4.4 ГГц)	EKLMNOABC
			оперативна пам'ять – 16 ГБ	EKLMNOBCD
			накопичувач – Kingston SSD, 512 ГБ	EKLMNOCDE
			відеоадаптер – Intel з 4 ГБ пам'яті	EKLMNODEF
2	iMac	IM1-IM4	Процесор – Intel Core i5-7500 із тактовою частотою 3.4 ГГц	C01RL123AC C02RL123AC C03RL123AC C04RL123AC
			оперативна пам'ять – 16 ГБ	C01RL123BC C02RL123BC C03RL123BC C04RL123BC
			накопичувач– Kingston SSD, 256 ГБ	C01RL123DC C02RL123DC C03RL123DC C04RL123DC
			відеоадаптер – AMD Radeon Pro 570 з 4 ГБ пам'яті	C01RL123EC C02RL123EC C03RL123EC C04RL123EC
3	Маршрутизатор	R	Частота роботи Wi-Fi – 5 ГГц + 2.4 ГГц (дводіапазонний); швидкість LAN портів – 1 Гбіт/с; підтримка PoE, підтримка VPN; підтримка протоколів – L2TP, IPsec, DHCP, NAT	LNK123456789
4	Абонентський ONU термінал	T	Швидкість – 1000 Мбіт/с	ABCDEFGH1234
5	Точка доступу	AP	Максимальна швидкість WiFi – до 1300 Мбіт/с; частота роботи Wi-Fi – 2,4 ГГц і 5 ГГц (дводіапазонний); тип живлення – DC, POE; роз'єми – 2 x RJ45, USB	12ABCD345678

Продовження таблиці Ґ.1

6	POS термінал	PR	Процесор – ARM9+ARM7 (450 MIPS+50 MIPS); мережа (LAN) – Dial-up Modem, Ethernet, GPRS; швидкість друку – 60 мм/сек;	IWL220A-ABCDE12345
7	Принтер для етикеток	PS	Швидкість друку – до 152 мм/сек; інтерфейс управління – USB, Ethernet; роздільна здатність – 203dpi	XP0A-AAKDE91917
8	Телевізор	Телевізор	Входи – USB, LAN; частота зміни кадрів – 50 Гц; операційна система – Smart TV	A123B456C7890123
9	Камера відеоспостереження	Камера	Фокусна відстань – фіксована, 4 мм; кут огляду по горизонталі – 90.2°, по вертикалі – 48.6°; мережевий інтерфейс – RJ45 (10M/100M)	DS-2CD1234 DS-2CD1235 DS-2CD1236 DS-2CD1237 DS-2CD1238

ДОДАТОК Д. Перелік документів на оптичному носії

КуцьМО_125-20-1_ПЗ.docx

КуцьМО_125-20-1_ПЗ.pdf

КуцьМО_125-20-1_Презентація.pptx

КуцьМО_125-20-1_Рецензія.pdf

Ситуаційний_план.svg

Генеральний_план.svg

Структурна_схема_ІКС.drawio

ДОДАТОК Е. Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 92б. («відмінно»).

Керівник розділу _____ Дар'я ПІЛОВА

(підпис) (ім'я, прізвище)

ДОДАТОК Є. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
«Комплексна система захисту інформації інформаційно-комунікаційної системи магазину роздрібної торгівлі «GetApple»
студента групи 125-20-1
Куця Максима Олеговича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 89 сторінках та містить 6 рисунків, 35 таблиць, 7 джерел та 8 додатків.

Метою кваліфікаційної роботи є забезпечення заданого рівня безпеки інформації, яка обробляється в ІКС магазину роздрібної торгівлі «GetApple».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: обстеження середовищ функціонування ІКС, розробка моделі порушника, аналіз джерел загроз та вразливостей, визначення актуальних загроз, формування вимог до захисту інформації та розробка проектних рішень їх реалізації.

Запропоновано матрицю розмежування доступу, розроблені положення політики безпеки щодо: антивірусного захисту, резервного копіювання, безпеки робочого місця, резервного живлення та резервного копіювання. Розроблені проектні рішення впровадження антивірусного програмного забезпечення та реалізації резервного електроживлення.

Практичне значення результатів кваліфікаційної роботи полягає у адаптації запропонованих рішень до особливостей магазину роздрібної торгівлі «GetApple».

До недоліків відноситься недостатньо обґрунтована модель загроз та профіль захищеності.

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

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

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

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи, професор Валерій КОРНІЄНКО

Керівник спец. розділу, ст. викладач Олександр КРУЧІНІН