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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Гузченка Святослава Владиславовича*

академічної групи *125-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-комунікаційної системи магазина роздрібної торгівлі «Shoes City»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Магро В.І.			
розділів:				
спеціальний	ст. викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.	90	відмінно	

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Гузченку С.В.* **академічної групи** *125-19-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-комунікаційної системи магазина роздрібної торгівлі «Shoes City»*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.23 № 350-с

Розділ	Зміст	Термін виконання
Розділ 1	Обстеження ІКС, розробка моделі порушника та загроз	12.04.23 - 26.04.23
Розділ 2	Вибір профілю захищеності. Розробка проектних рішень	27.04.23 – 26.05.23
Розділ 3	Техніко-економічне обґрунтування доцільності впровадження КСЗІ	26.05.23 – 09.06.23

Завдання видано _____ Магро В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 02.04.2023

Дата подання до екзаменаційної комісії: 09.06.2023

Прийнято до виконання _____ Гузченко С.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 82 с., 9 рис., 20 табл., 4 додатки, 17 джерел.

Об’єкт дослідження: інформаційно-комунікаційна система ФОП «Shoes City»

Мета кваліфікаційної роботи: забезпечення необхідного рівня захисту інформації інформаційно-комунікаційної системи підприємства ФОП «Shoes City».

Методи дослідження: опис, аналіз.

В першому розділі представлені загальні відомості про підприємство, обґрунтування необхідності створення КСЗІ, виконано обстеження фізичного середовища, обчислювальної системи, інформаційного середовища та середовища користувачів. Завдяки зібраним даним розроблено модель порушника та модель загроз. Виявлені актуальні загрози та вразливості.

В другому розділі обрано профіль захищеності та запропоновані проєктні рішення щодо реалізації механізмів захисту, що включають в себе: розмежування прав адміністрування в інформаційно-комунікаційній системі, систему антивірусного захисту, засоби фізичного захисту та засоби реалізації контролю за діями користувачів. Також запропоновано впровадження політики безпеки.

В третьому розділі за допомогою економічних розрахунків було обґрунтовано доцільність впровадження КСЗІ в інформаційно-комунікаційну систему підприємства, визначено економічну ефективність та розраховано коефіцієнт повернення інвестицій ROSI.

КОМППЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЛЬНОСТІ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ.

ABSTRACT

Explanatory note: 82 pages, 9 pic., 20 tables, 4 applications, 17 sources.

Object of study: information and communication system of PE «Shoes City»

The purpose of the project: to develop comprehensive information protection system of the information and communication system of PE «Shoes City».

Methods of development: description, observation, survey, analysis and calculation.

The first section presents information about the enterprise, reasoning of necessity to create comprehensive information protection system, examination of physical environment, calculating system environment, information environment and users environment. Based on the collected data, user violator model and model of threats were developed. Current threats and vulnerabilities were discovered.

In the second section the security profile was selected and the following project solutions were proposed: distribution of rights of administration, rules of access delimitation, antivirus protection system, means of physical protection and user means control over users actions. Also the implementation of security policies were proposed.

In the third section expediency of CIPS implementation was justified by using economic calculations, economic efficiency was defined and the rate of return on investments ROSI was calculated.

COMPREHENSIVE INFORMATION PROTECTION SYSTEM, INFORMATION AND COMMUNICATION SYSTEM, OBJECT OF INFORMATION ACTIVITY, MODEL OF THREATS, USER VIOLATOR MODEL, ECONOMIC EXPEDIENCY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІзОД – інформація з обмеженим доступом;

ІКС – інформаційно-комунікаційна система;

ІС – інформаційна система;

ІТ – інформаційні технології;

ІТС – інформаційно-телекомунікаційна 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;

ОТЗ – основні технічні засоби;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

ТЗІ – технічний захист інформації;

ФОП – фізична особа підприємець;

ЗМІСТ

ВСТУП

В наш час більшість підприємств веде свою діяльність в інтернет-просторі. Розміщення в інтернеті власного сайту дає змогу залучити більше клієнтів та створити якісний імідж для компанії, що безумовно допомогає збільшити прибуток. Створення ІКС для підприємства значно спрощує та покращує ефективність його роботи.

Проте діяльність в інтернет-просторі також створює додаткові загрози безпеки інформації для бізнесу. Конкуренти та кіберзлочинці можуть здійснювати кібератаки з ціллю заволодіти конфіденційної інформацією, щоб в подальшому отримати з цього фінансову вигоду. А саме підприємство може зазнати від цього значних втрат, що можуть навіть призвести до припинення його діяльності.

Загалом існує два типи загроз: зовнішні та внутрішні.

До зовнішніх відносяться шкідливе програмне забезпечення, DDoS-атаки, фішинг, ботнети, проникнення в мережу, втрата пристроїв зі збереженими паролями.

До внутрішніх зазвичай відносяться витоки конфіденційної інформації через співробітників чи підрядників та вразливе ПЗ.

Реалізація цих загроз може суттєво вплинути на репутацію підприємства, підірвати довіру клієнтів та завдати йому великих збитків, а якщо це мале підприємство, то і зовсім може зникнути з ринку.

Через це багато підприємств сьогодні більш відповідально ставляться до інформаційної безпеки та приймають відповідні міри. Але на жаль представники малого бізнесу нехтують інформаційною безпекою через неможливість фінансування для впровадження заходів безпеки або через недооцінення можливих загроз та ризиків. Проте за звітом компанії з кібербезпеки Barracuda Networks співробітники невеликих компаній мали справу зі спробами атак з використанням методів соціальної інженерії на 350% частіше, ніж їхні колеги з великих корпорацій.

Щоб запобігти цим загрозам та уникнути їх наслідків потрібно впроваджувати КСЗІ.

Комплексна система захисту інформації є сукупністю організаційних та інженерно-технічних заходів, що спрямовані на забезпечення захисту інформації від розголошення, витоку та несанкціонованого доступу.

КСЗІ є глобальною концепцією безпеки та основою для безпеки інфраструктури підприємства в цілому, що забезпечить його безперервне функціонування.

В кваліфікаційній роботі буде розглянуто магазин роздрібної торгівлі «SHOES CITY».

Актуальність роботи обумовлена стрімким розвитком підприємства, збільшенням кількості співробітників та оброблюваної інформації, що потребує впровадженням надійної системи захисту.

Мета кваліфікаційної роботи підвищення рівня захисту інформації на підприємстві ФОП «SHOES CITY».

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про підприємство

Підприємство ФОП «SHOES CITY» - інтернет-магазин роздрібної торгівлі взуттям. Компанія працює з 2018 року та займається закупівлею брендового взуття оптом через постачальників та продажом його через фізичну точку збуту та через власний інтернет-магазин створений на торгових майданчиках PROM UA, ROZETKA та через соціальну мережу Instagram. Адреса головного офісу: м. Дніпро, вулиця Івана Акінфієва, 1, 2-й поверх(з 9-ти). Підприємство працює з понеділка по суботу 6 днів на тиждень з 9:00 до 19:00.

Компанія на даний момент налічує 10 співробітників.

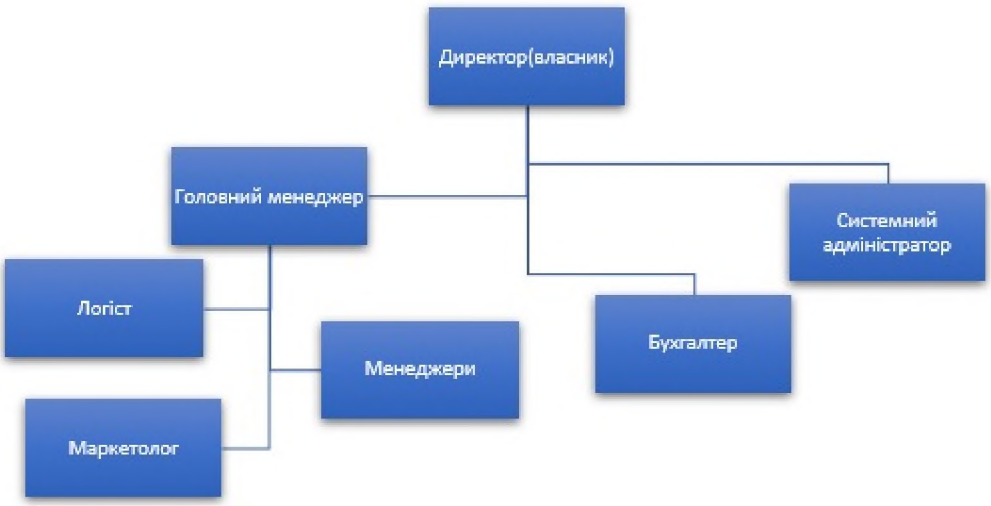


Рисунок 1.1 – Організаційна структура підприємства

1.2 Обґрунтування необхідності створення КСЗІ

Необхідність забезпечення захисту інформації , а саме створення комплексної системи захисту інформації (КСЗІ) в автоматизованих системах 1-ого, 2-ого та 3-ого класу визначається передусім вимогами нормативно-правових документів, таких як НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем» або в окремих випадках рішенням власника інформаційних ресурсів.

Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;
- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;
- оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІТС у разі створення КСЗІ.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.[5]

1.3 Обстеження ІКС

1.3.1 Обстеження фізичного середовища

Опис ситуаційного плану:

Об'єктом інформаційної діяльності є офіс приватного підприємства ФОП «Shoes City» , який розташований в м. Дніпро на вулиці Івана Акінфієва 1. Площа ОІД складає 255 м^2.

Офіс де циркулює інформація з обмеженим доступом(ІзОД) розташований на 1-му поверсі 9-ти поверхової жилої будівлі на перших двох поверхах якої знаходяться офісні приміщення.

Режим допуску до території будівлі забезпечується наступним чином:

- Заїзд на парковку в дворі житлового будинку з вул. Акінфієва вільний.
- Щоб потрапити в будівлю необхідно мати магнітний ключ від дверей домофону.
- Цілодобовий доступ до будівлі житлового будинку мають його мешканці та співробітники компаній, офісні приміщення яких знаходяться на перших двох поверхах.

Режим контрольованої зони(КЗ) забезпечується наступним чином:

- В робочий час вхід до підприємства дозволяється всім співробітникам які знають код від кодового магнітного замку, після того як директор відчинить основний врізний замок. Ключ від основного замка є тільки в директора.
- В неробочий час з 19:00 до 9:00 офіс становиться під централізовану охорону системи сигналізації та закривається на ключ директором.

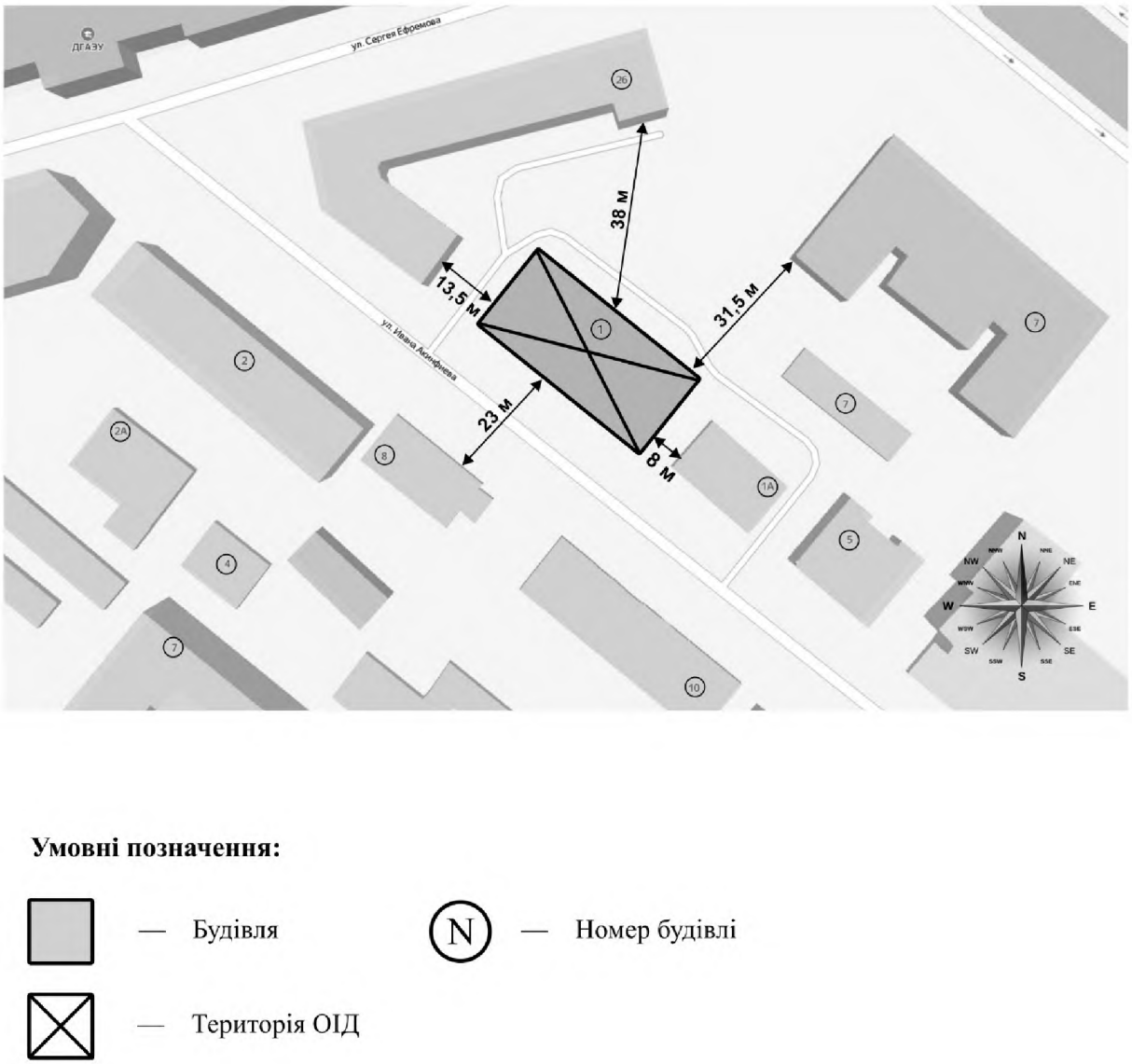
Ситуаційний план ОІД наведений нижче на рисунку 1.2

Навколо будівлі в якій знаходиться ОІД, розміщені наступні об’єкти:

На півночі від ОІД знаходиться 5-ти поверховий житловий будинок, на заході житловий 5-ти поверховий будинок в якому розташована Дитяча музична школа №2 та студія балету, на півдні через дорогу 2-х поверхова офісна будівля, на сході майже прилягає до будинку в якому знаходиться ОІД двоповерхова офісна будівля. На північному сході знаходиться адміністративна 4-х поверхова споруда районної ради Соборного району Дніпра. На південному сході від КЗ розташовано 5-ти поверховий житловий будинок. На південному заході також розташований 5-ти поверховий житловий будинок. Дані наведені в табл. 1.1

Таблиця 1.1 – Характеристика будівель та споруд

Назва будівлі	Адреса	Кількість поверхів	Мінімальна відстань до КЗ
Офісна будівля	вул. Івана Акінфієва, 3	2	8 м
Офісна будівля	вул. Івана Акінфієва, 8	2	23 м
Житловий будинок	вул. Сергія Єфремова, 26	5	13,5 м
Житловий будинок	вул. Івана Акінфієва, 10	5	40 м
Адміністративна споруда	площа Шевченка, 7	4	31,5 м
Житловий будинок	вул. Івана Акінфієва, 2	5	30 м



Умовні позначення:

— Будівля

N — Номер будівлі

— Територія ОІД

Рисунок 1.2 – Ситуаційний план розташування ОІД

Опис генерального плану ОІД:

Стіни будівлі в якій розташовано ОІД зроблені з білої цегли товщиною 400 мм. Перекриття зроблені з використанням залізобетонних плит.

Двері до офісного приміщення також металеві з основним врізним замком та додатковим автоматичним магнітним замком що відчиняється після вводу правильного 4-х значного пін-коду на металевих клавішах що розташовані поряд з дверима. Врізний замок відкриває директор, який першим вранці заходить до офісу. Ключ має тільки він. Інші співробітники потрапляють через пін-код.

В офісі є 3 вікна що виходять у внутрішній двір будівлі та 3 вікна з зовнішнього боку. На кожному вікні встановлені жалюзі. Вікна металопластикові двостулкові 1430 х 1470 мм. Висота стелі – 3м. Підлога виконана з ламінату. До будівлі проведено електричне та водопостачання.

Труби системи опалення проходять під землею до підвалу будівлі, в якому розмежовуються вертикально до інших приміщень.

Лінія системи водопостачання йде по металевій трубі що заходить в будинок, після лічильника йде пластикова труба. Каналізаційні труби з ПВХ.

Розподільна електрощитова знаходиться в підвалі будинку, на кожному поверсі є окрема щитова що розподіляє струм до щитової кожного приміщення.

Елементи системи електропостачання в приміщенні заземлені(йдуть 3 дроти). Підключені до щитової підприємства, яка далі підключена до щитової на поверху будівлі.

Система охоронно-пожежної сигналізації була спроектована та встановлена під замовлення власником приміщення який здає його в оренду. Може працювати дистанційно.

Вентиляційна система – приточно-витяжна з кондиціонером, проведена до кожного приміщення, може як підігрівати так і охолоджувати повітря.

Система опалення складається з металічних радіаторів з пластиковими трубами з вертикальною розводкою що йде з підвального приміщення.

Локальна мережа - це вита пара та оптоволоконне покриття, що прокладені в контрольованій зоні від щитової провайдеру(«Воля»)на першому поверсі та не виходить за його межі.

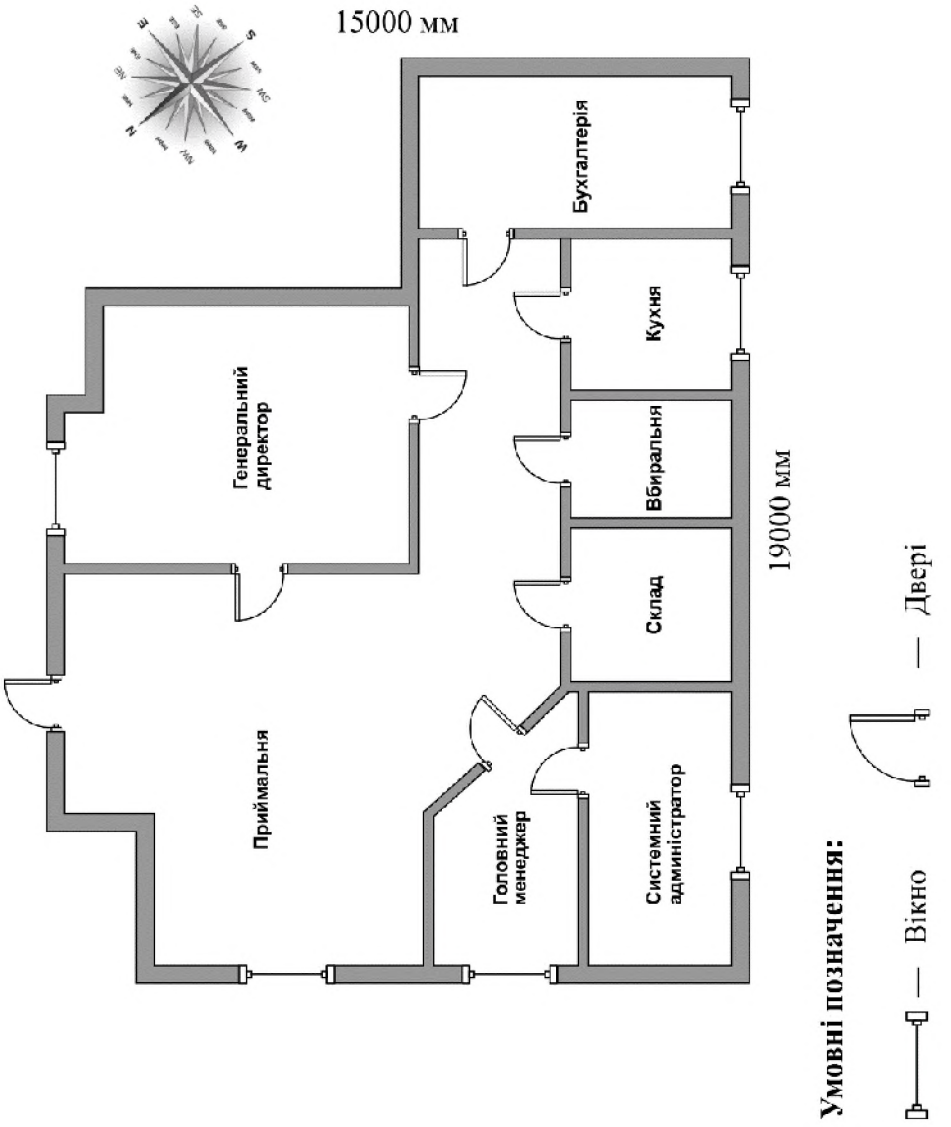


Рисунок 1.3 – Схема приміщення ОІД

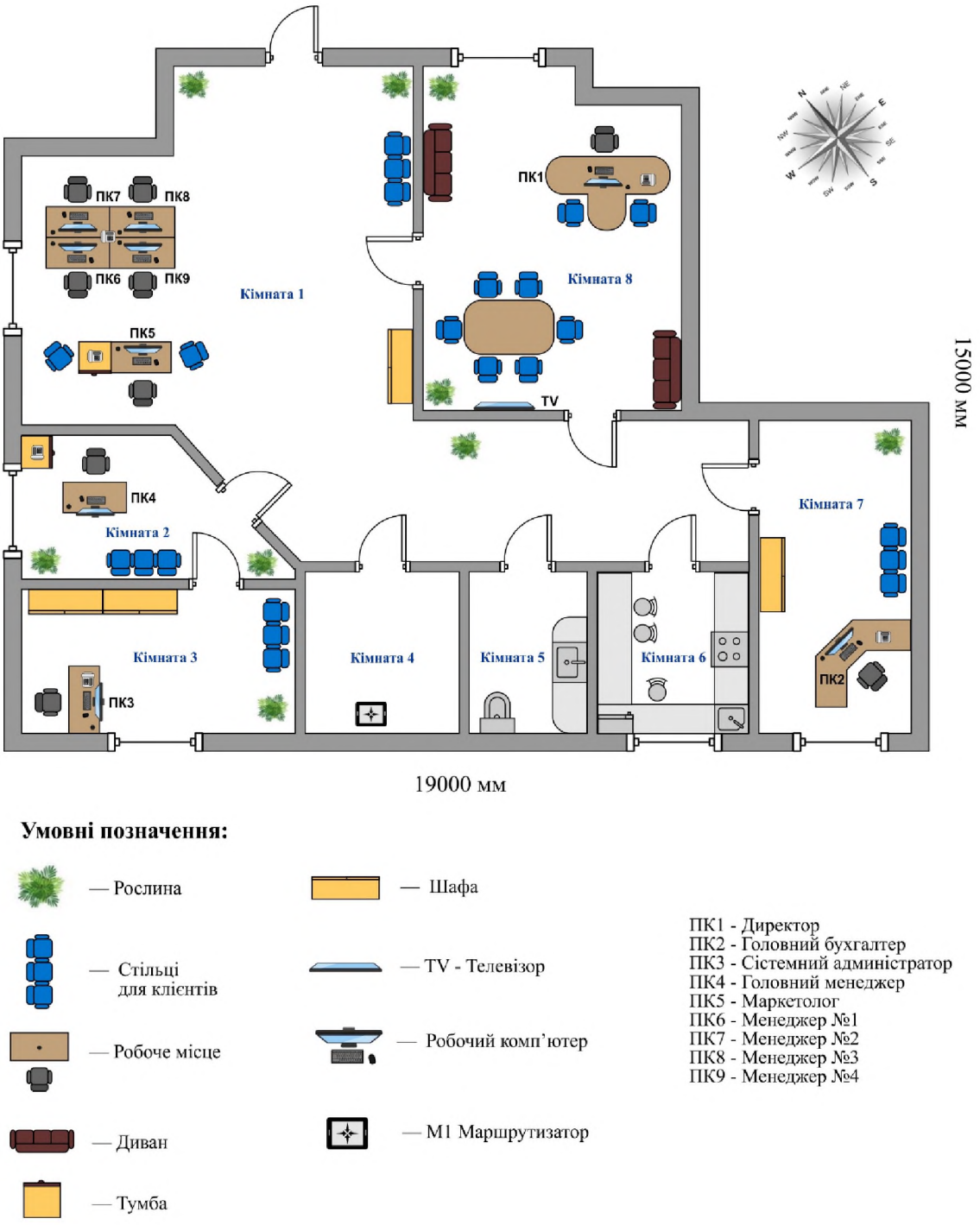


Рисунок 1.4 – Генеральний план ОІД

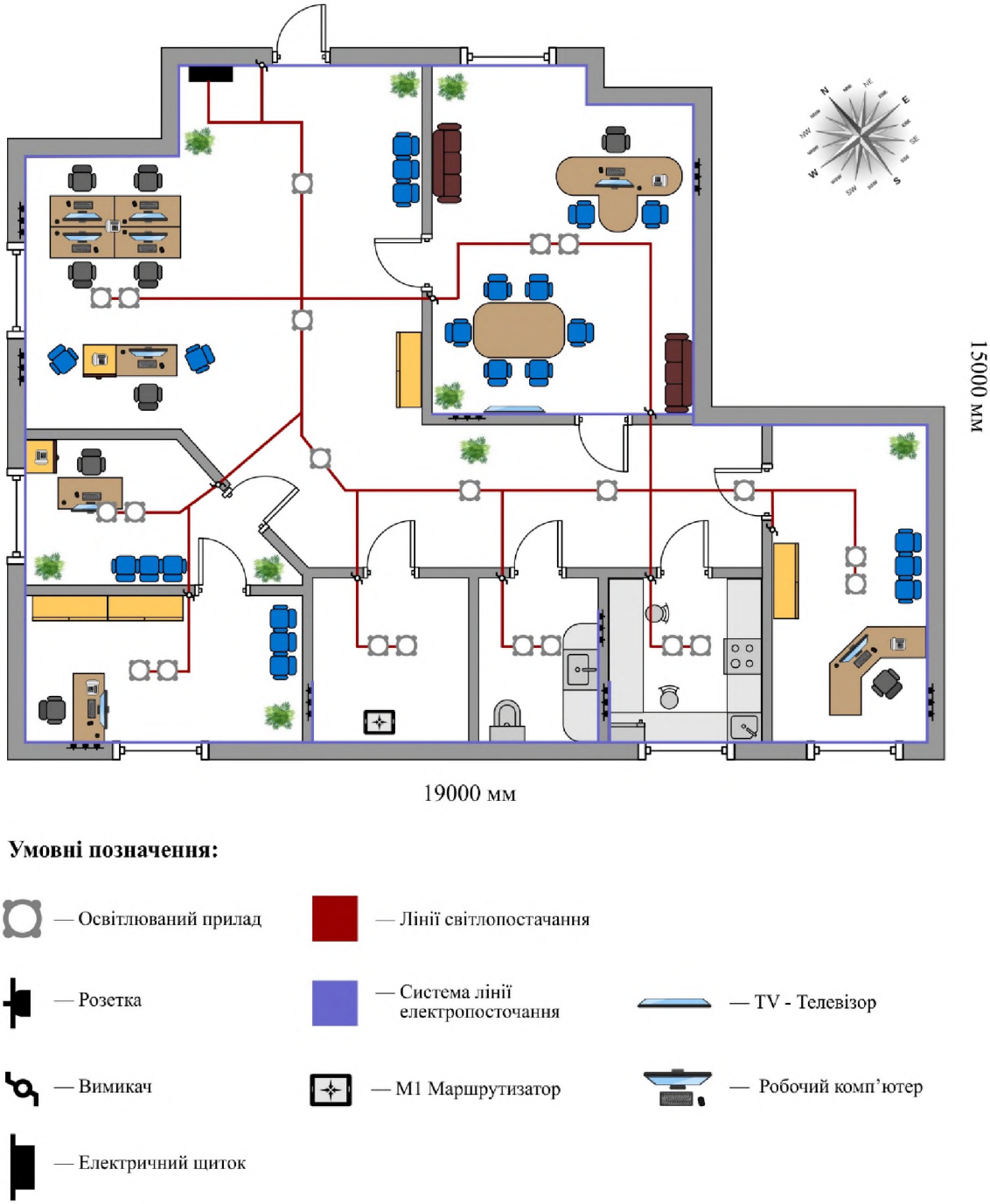


Рисунок 1.5 – Генеральний план ліній електропостачання та освітлення

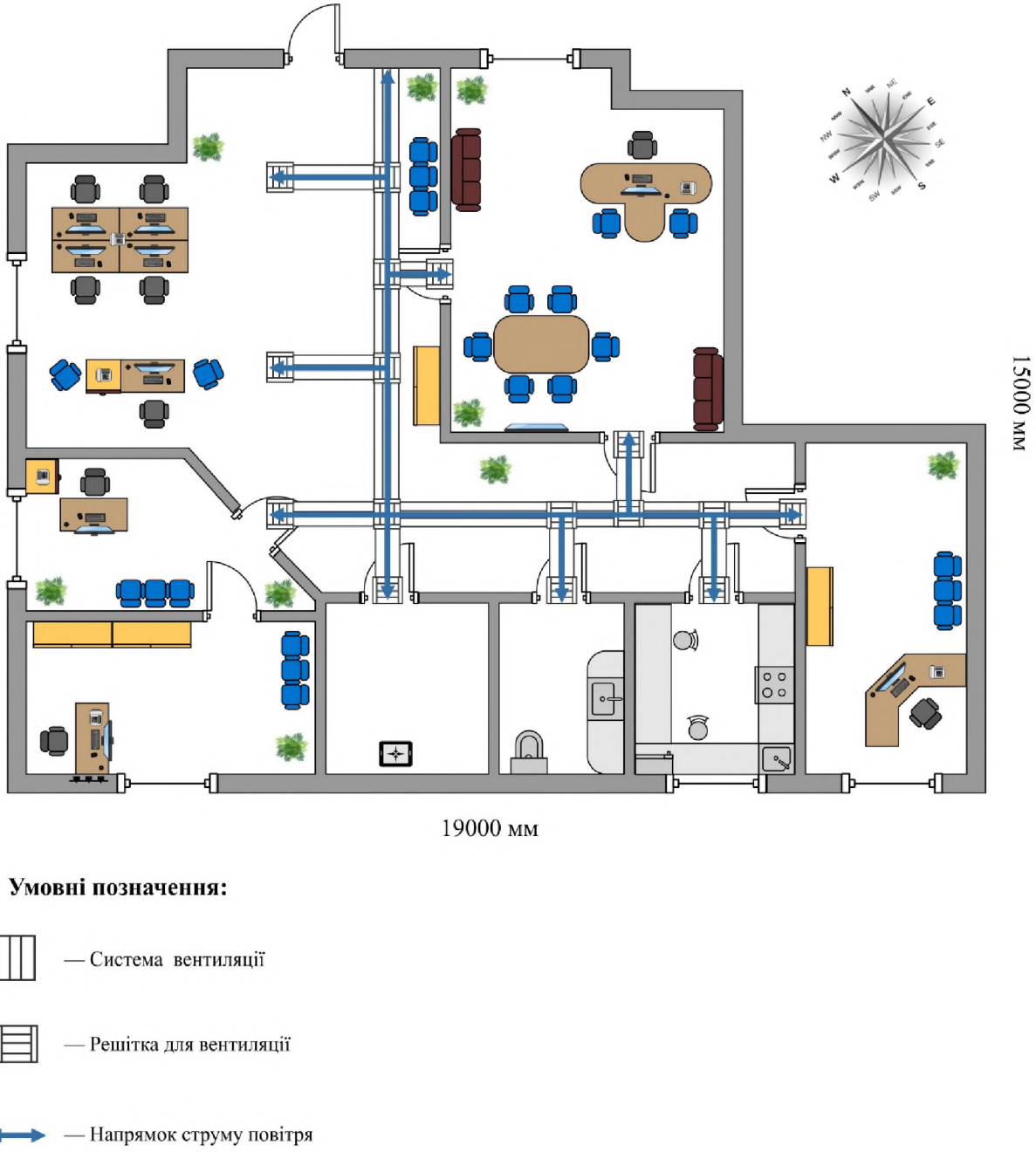


Рисунок 1.6 – Генеральний план ліній системи вентиляції та кондиціювання

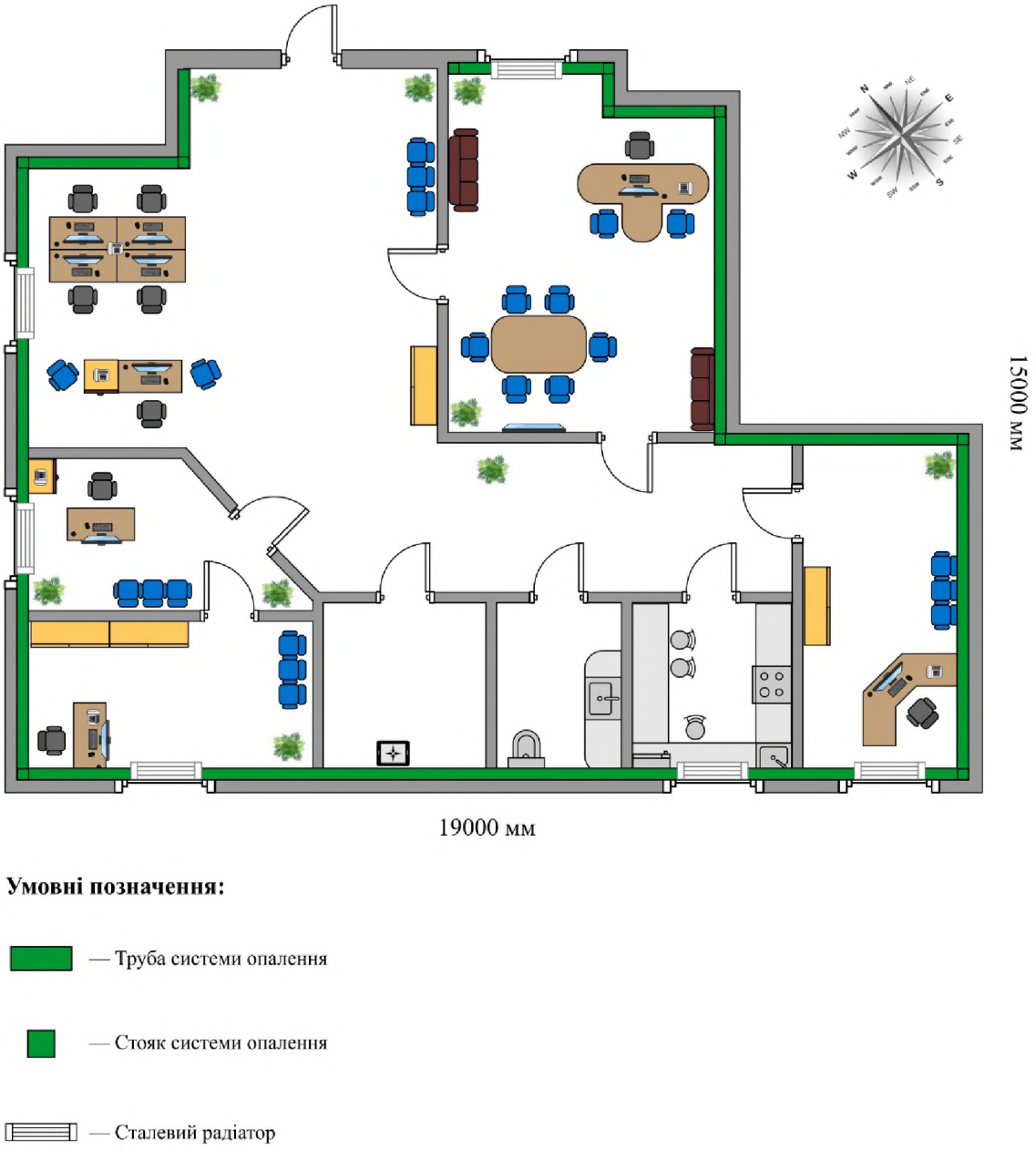
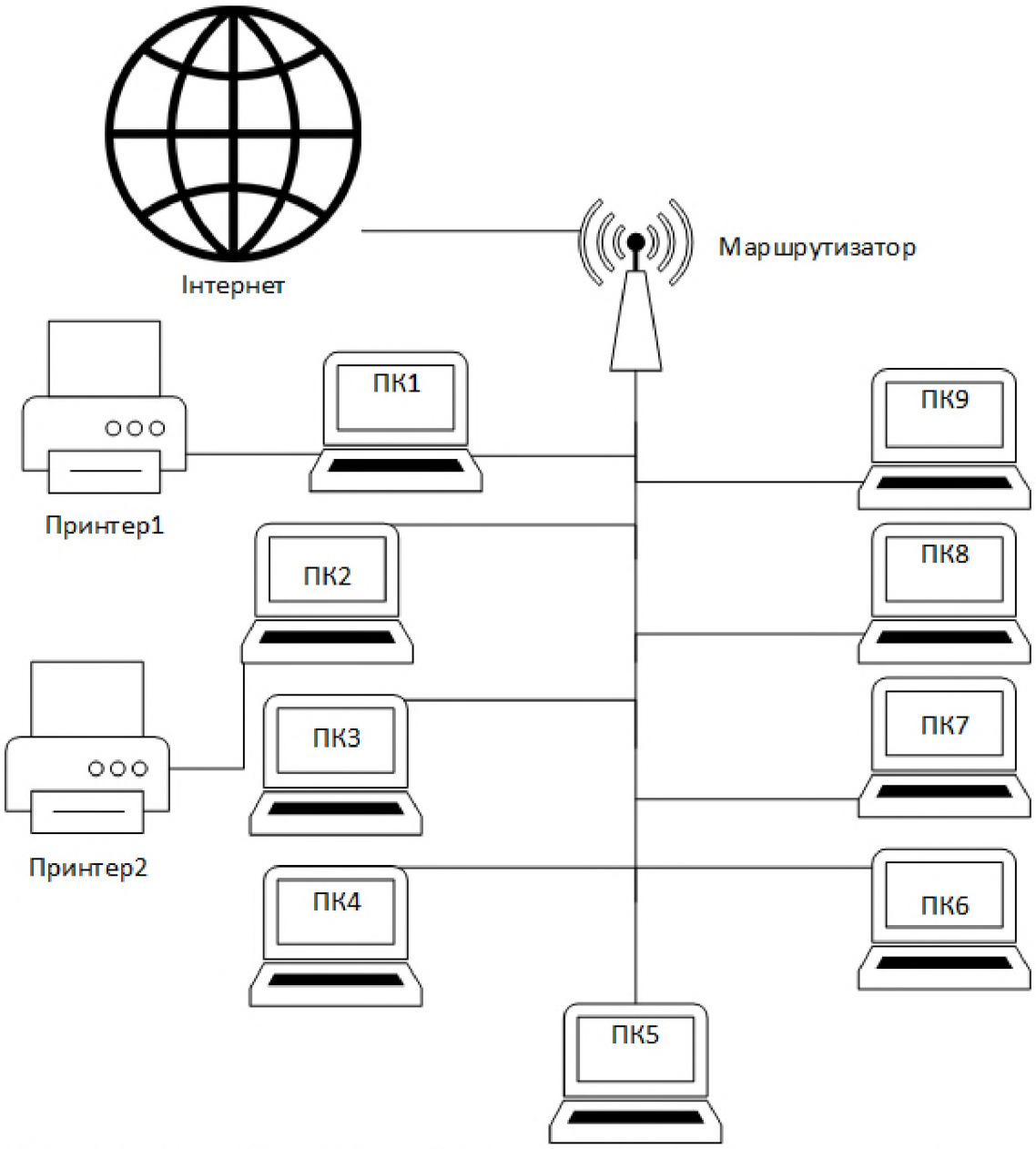


Рисунок 1.7 – Генеральний план системи опалення та водопостачання

1.3.2 Обстеження обчислювальної системи

Автоматизована система налічує у собі 9 комп'ютерів (5 ноутбуків в приймальні, 1 ноутбук – в кабінеті директора, 1 ноутбук – в кабінеті головного менеджера, 1 ноутбук – в кабінеті бухгалтера, 1 ноутбук – в кабінеті системного адміністратора), 1 маршрутизатор розташований в складі та 2 принтери. АС має доступ до мережі Інтернет провайдером якої є «Воля». Локальна мережа бездротова, створена за допомогою роутера та об'єднує всі комп'ютери через Wi-



Fi. Всі комп'ютери об'єднані в робочу групу через локальну мережу.

Рисунок 1.8 – Схема ІКС підприємства

В таблиці 1.2 наведено перелік основних технічних засобів. Кожен співробітник на підприємстві працює зі своїм власним ноутбуком для зручності та мобільності. За потреби директор може за власні кошти придбати співробітнику ноутбук для роботи .

Таблиця 1.2 – Перелік ОТЗ – основних технічних засобів

№	Назва	Марка	Модель	Серійний номер	Розміщення	Відстань до межі КЗ, м
1	ПК1	Apple	MacBook Air 13" M1 8/256GB 2020	FX78431	Кабінет директора	1,5
2	ПК2	HP	250 G8	CH30951	Кабінет бухгалтера	1,5
3	ПК3	LENOVO	ThinkBook 15 G3 ACL	VY34026	Кабінет системного адміністратора	0,5
4	ПК4	Xiaomi	Mi RedmiBook 15 i3/8/256	GH56123	Кабінет головного менеджера	1
5	ПК5	Acer	Aspire 3 A315-35-P9Q4	KN67410	Приймальня	2
6	ПК6	Lenovo	V14 Grey	DL30695	Приймальня	1
7	ПК7	HP	ProBook 455 G7 Silver	QS81074	Приймальня	1

Продовження таблиці 1.2

№	Назва	Марка	Модель	Серійний номер	Розміщення	Відстань до межі КЗ, м
8	ПК8	Apple	MacBook Air 13" 128GB 2018	BJ01347	Приймальня	2
9	ПК9	ASUS	Vivobook Go 15 E510KA-BQ296	KW14804	Приймальня	2
10	Маршрутизатор	TP-Link	ARCHER AX73 AX5400	AX03578	Склад	0,5
11	Принтер 1	Canon	Pixma MG3640S	0515C107AA/ 0515C007	Кабінет директора	0,5
12	Принтер 2	Canon	PIXMA Ink Efficiency E414	1366C009	Кабінет бухгалтера	0,5

Таблиця 1.3 – Перелік допоміжних технічних засобів

№	Назва	Марка	Модель	Серійний номер	Розміщення
1	Телевізор	Xiaomi	43" Xiaomi Mi TV P1 43 Black	XM038167	Кабінет директора

Також у таблиці 1.4 вказано програмне забезпечення яке встановлено на всіх комп'ютерах, що використовують працівники ФОП «Shoes City».

Таблиця 1.4 – Перелік програмного забезпечення в ІКС

№	Назва	Тип	Ліцензія	Місце встановлення
1	ОС Windows 10 pro	Операційна система	Commercial	ПК2-ПК7, ПК9
2	macOS Catalina 10.15.7	Операційна система	Commercial	ПК1, ПК8
3	Microsoft Office 2019	Прикладне	Corporative	ПК2-ПК7, ПК9
4	Google Chrome	Веб браузер	Free	ПК1-ПК9
5	Adobe Photoshop	Прикладне	Commercial	ПК8

1.3.3 Обстеження інформаційного середовища

Кожен день на підприємстві «Shoes City» створюється, обробляється та зберігається інформація різних ступенів важливості та конфіденційності. Це може бути інформація щодо поставки товару, ціна його закупки, фотографії та відео відзнятого товару для його реклами, інформація щодо замовлень клієнтів та їх персональні дані. Пошкодження, витік або розголошення цієї інформації може спричинити різного рівня неприємності для підприємства, в тому числі фінансові збитки та втрата довіри клієнтів.

Перелік інформації що циркулює на підприємстві:

- за способом сприйняття: візуальна та звукова;
- за формою уявлення: текстова, цифрова, графічна та звукова;
- за значенням: актуальна, достовірна, повна та цінна;

- за призначенням: спеціальна, секретна та особиста.

На підприємстві циркулює інформація про клієнтів та постачальників, деталі та кількість замовлень, бухгалтерські звіти, інформація щодо наявності товару та планових закупівель, плани щодо розширення бізнесу. Детальніше в табл. 1.5.

Інформація про клієнтів включає в себе ПІБ замовника, його номер телефону та можливо електронну пошту або акаунт в соцмережі, місто та відділення пошти в якому клієнт буде отримувати товар, реквізити на які клієнт здійснював оплату та суму переказу і скріншот для його підтвердження та номер ТТН(Товарно транспортна накладна) за яким клієнт буде отримувати товар. Ця інформаційна є конфіденційною та не повинна розголошуватись або поширюватись. Зберігається в базі даних та CRM.

Бухгалтерські звіти містять у собі інформацію щодо активів підприємства та його грошового обороту, зарплатні відомості працівників, вартість закупівель товару, а також податкові відомості. Доступ до цієї інформації має обмежена кількість людей.

Плани щодо розширення підприємства створений директором та використовується як інструкція подальших дій для розвитку компанії.

В обстежуваній ІКС не міститься інформація яка є власністю держави чи відомості, що становлять державну таємницю.

Технологія обробки інформації:

Переважна більшість інформації знаходиться на ПК працівників та хмарному сховищі Google Диск на корпоративному Google акаунті підприємства доступ до якого мають всі працівники. Правила доступу до інформації не врегульовані, переглядати та редагувати її можуть всі користувачі системи.

Таблиця 1.5 – Класифікація інформації, що циркулює в ІКС

№	Вид інформації	Порядок доступу	Правовий режим	Вид представлення в ІТС	Вимоги до захисту		
					К	Ц	Д
1	Інформація про клієнтів	Обмежений	Конфіденційна	Графічна, текстова, звукова	К3	Ц2	Д2
2	Інформація про товар	Відкритий	Відкрита	Графічна, текстова, цифрова	К1	Ц2	Д2
3	Звіти бухгалтерії	Обмежений	Конфіденційна	Текстова, числова	К2	Ц3	Д2
4	Документи про закупівлю товарів	Обмежений	Конфіденційна	Графічна, текстова, звукова	К2	Ц2	Д1
5	Наявність товару та його кількість на складі	Відкрита	Відкрита	Текстова, числова, звукова	К1	Ц2	Д2
6	Плани з розширення компанії	Обмежений	Комерційна таємниця	Графічна, текстова, звукова	К3	Ц3	Д3
7	Інформація про об’єкти та системи безпеки	Обмежений	Комерційна таємниця	Графічна, текстова, звукова	К3	Ц3	Д3
8	Рекламні матеріали	Відкритий	Відкрита	Цифрова, графічна, текстова	К1	Ц2	Д2

Продовження таблиці 1.5

№	Вид інформації	Порядок доступу	Правовий режим	Вид представлення в ІТС	Вимоги до захисту		
9	Інформація про постачальників товару	Обмежений	Комерційна таємниця	Цифрова, текстова, числова	К3	Ц3	Д3

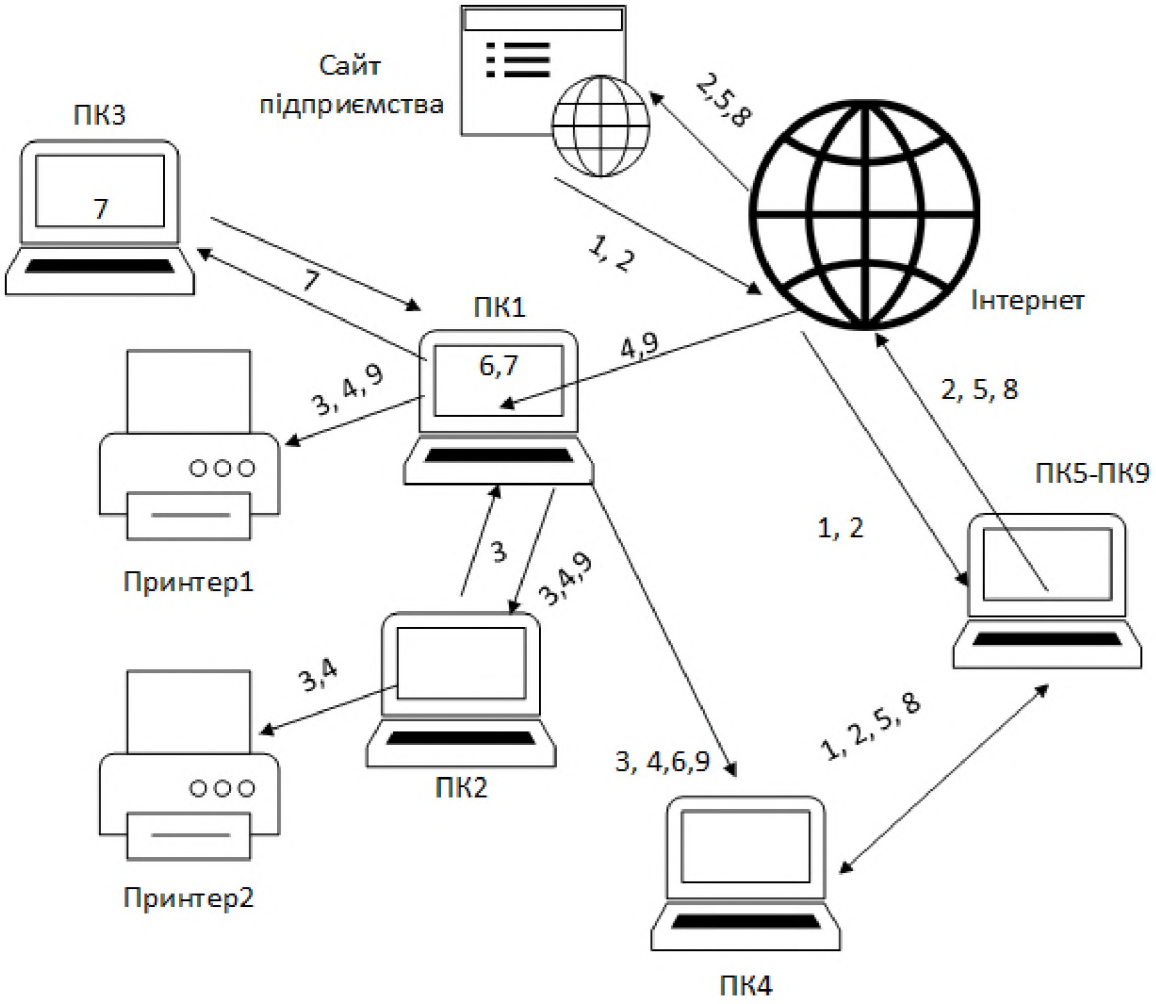


Рисунок 1.9 – Схема інформаційних потоків підприємства

Цифрами 1 – 9 позначена інформація з таблиці 1.5

Таблиця 1.6 – Рівень важливості конфіденційності інформації

Рівень наслідків	Опис
К1	Не призводить до розкриття конфіденційної інформації
К2	Призводить до розкриття окремих даних що відносяться до комерційної таємниці, персональних даних та може спричинити незначні фінансові втрати
К3	Призводить до розкриття окремих даних що відносяться до комерційної таємниці, персональних даних та може призвести до значних фінансових втрат та значно вплинути на репутацію підприємства

Таблиця 1.7 – Рівень важливості цілісності

Рівень наслідків	Опис
Ц1	Не призводить до фінансових втрат
Ц2	Призводить до незначних фінансових втрат та має незначний вплив на репутацію підприємства
Ц3	Призводить до значних фінансових втрат та значно впливає на репутацію підприємства

Таблиця 1.8 – Рівень важливості доступності

Рівень наслідків	Опис
Д1	Не впливає на доступність
Д2	На деякий час впливає на доступність інформації, що може спричинити незначні фінансові та репутаційні втрати
Д3	Унеможливлює користування ресуром на тривалий час на має значні наслідки для підприємства

1.3.4 Обстеження середовища користувачів

Штат працівників та їх службові обов'язки:

Головним на підприємстві є директор(він же і є власник). До його повноважень входить керування всіма відділами підприємства, прийняття рішення щодо закупівлі товару, підписання договорів з постачальниками, створення планів та контроль за їх виконанням.

Задача головного менеджера керувати відділом продаж, вести звітність щодо наявності товару та кількості продаж, корегувати роботу менеджерів, маркетолога та логіста.

Маркетолог налаштовує рекламу для залучення нових клієнтів, та аналізує її ефективність.

Менеджери спілкуються з клієнтами, консультують їх та приймають замовлення по телефону, через сторінку інтернет-магазину або через месенджери в соціальних мережах. Також вносять данні в таблицю продажів та збирають замовлення.

Логіст займається доставкою зібраних замовлень до поштового відділення та їх своєчасною відправкою до клієнтів. Також логіст отримує новий товар від постачальників та доставляє його до підприємства.

Системний адміністратор стежить за обладнанням в офісі підприємства, його вчасним обслуговуванням та оновленням програмного забезпечення.

Бухгалтер складає податкові відомості, вираховую зарплату працівників згідно умов працевлаштування, робить щомісячні звіти підприємства.

Також окрім співробітників підприємства «Shoes City» на території об'єкта інформаційної діяльності(ОІД) задіяний обслуговуючий персонал офісної будівлі:

- прибиральниці, працюють позмінно
- сантехник
- електрик

При потребі цим працівникам може бути наданий доступ до ОІД.

Для аналізу доцільності прав доступу до інформації всіх працівників підприємства визначимо основні їх посади та дозволи щодо користування інформацією в табл. 1.9.

Таблиця 1.9 – Матриця розмежування доступу

	1	2	3	4	5	6	7	8	9
Директор	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д
Головний менеджер	Ч Р З В Т Д	Ч Р З В Т Д	Ч З	Ч З	Ч Р З В Т Д	Ч З	Ч З	Ч Р З В Т Д	Ч Р З В Т Д
Бухгалтер	Ч З	Ч З	Ч Р З В Т Д	Ч З	Ч Р З В Т Д	Ч З	Ч З	Ч З	Ч Р З
Системний адміністратор	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д
Маркетолог	Ч Р З В Т Д	Ч Р З В Т Д	Ч	Ч З	Ч Р З В Т Д	Ч З	Ч З	Ч Р З В Т Д	Ч Р З
Менеджери	Ч Р З В Т Д	Ч Р З В Т Д	Ч	Ч З	Ч Р З В Т Д	Ч З	Ч З	Ч Р З Д	Ч З

Ч – читання, Р – редагування, З – збереження, В – видалення, Т – імпорт/експорт, Д – друк. Цифрами 1 – 9 позначена інформація з таблиці 1.5

1 – інформація про клієнтів, 2 – інформація про товар, 3 – звіти бухгалтерії, 4 – документи про закупівлю товарів, 5 – наявність товару та його кількість, 6 – плани з розширення компанії, 7 – інформація про об’єкти та системи безпеки, 8 – рекламна інформація, 9 – інформація про постачальників товару.

Проаналізувавши таблицю 1.9 можна з впевненістю сказати що в більшості користувачів є надлишкові права.

1.4 Модель порушника

Модель порушника є описом можливих дій порушника, що складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Порушників прийнято поділяти на зовнішніх і внутрішніх.

До внутрішніх відносять співробітників, користувачів інформаційної системи, які можуть наносити шкоду інформаційним ресурсам як ненавмисно, так і навмисно; технічний персонал, який обслуговує будівлі і приміщення (електрики, сантехніки, прибиральниці тощо); персонал, який обслуговує технічні засоби (інженери, техніки).

Зовнішні порушники є сторонніми особами, які знаходяться поза контрольованою зоною організації або не авторизовані для використання даної комп'ютерної системи. Тобто вони не мають в системі облікового запису і відповідно до політики безпеки взагалі не мають права працювати в даній системі. Зовнішніми порушниками можуть бути: відвідувачі, які можуть завдати шкоди навмисно або через незнання існуючих обмежень; кваліфіковані хакери; особи, яких найняли конкуренти щоб отримати необхідну інформацію; порушники пропускного режиму

Модель порушника має визначати такі фактори:

- можливі цілі порушника та їх градація;
- категорії користувачів(персоналу) ІКС та сторонніх осіб, із числа яких може бути порушник;
- припущення щодо кваліфікації порушника;
- пропущення щодо характеру дій порушника(за часом, місцем дії і тд).

Метою порушника може бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;

- внесення зміни в інформаційні потоки у відповідності зі своїми інтересами;
- збирання відомостей про систему, тощо.

Вважається що за своїм рівнем порушник це спеціаліст вищого рівня, що має повну інформацію про ІКС.

Внутрішній порушник «ПВ» – вид мінімальної загрози з причини безвідповідального ставлення до виконання своїх посадових обов'язків.

Зовнішній порушник «ПЗ» – це вид граничних загроз згідно причини цілеспрямованих несанкціонованих дій з метою модифікації або крадіжки даних.

Графа «Рівень загроз» в таблиці 1.10 позначає відносну оцінку можливих збитків, що може створити порушник за умов наявності відповідних характеристик. Рівень збитків характеризується по шкалі від 1 до 4: 1 – незначні, 2 – середні, 3 – значні, але не критичні, 4 – дуже значні.

Таблиця 1.10 – Категорія порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загроз
ПВ1	Обслуговуючий персонал ІКС (Системний адміністратор)	3
ПВ2	Користувачі ІКС	2
ПВ3	Керівники (Головний менеджер, Директор)	4
ПВ4	Персонал без доступу до ІКС (логіст)	1
ПЗ1	Технічний персонал що обслуговує приміщення (електрик, сантехник, прибиральниця)	1
ПЗ2	Відвідувачі (запрошені гості)	1
ПЗ3	Колишні працівники	2
ПЗ4	Хакери (Особи що намагаються отримати НСД до ІКС)	3
ПЗ5	Конкуренти та їх представники (Агенти)	4

Таблиця 1.11 – Специфікація моделі порушника за мотивами здійснення порушень

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

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

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Має низький рівень знань, але вміє працювати з технічними засобами в ІКС	1
К2	Має середній рівень знань та практичні навички роботи з технічними засобами в ІКС та їх обслуговування	2
К3	Має високий рівень знань в сфері програмування та обчислювальної техніки, проектування так експлуатації ІКС	3
К4	Знає структуру, функції та механізми дії засобів захисту інформації в ІКС, їх недоліки та можливості	4

Таблиця 1.13 – Класифікація моделі порушника за показником можливостей використання засобів та методів подолання систем захисту

Позначення	Опис можливостей порушника	Рівень загроз
З1	Може тільки підслуховувати розмови та переглядати документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехоплення без модифікації інформації та компонентів ІКС	2
З3	Використовує тільки штатні засоби та недоліки системи захисту для її подолання та компактні носії інформації які можна непомітно пронести	3
З4	Застосовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІКС, дезорганізації систем обробки інформації	4

Таблиця 1.14 – Класифікація моделі порушника за часом дії

Позначення	Опис можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності ІКС з метою відновлення або ремонту	1
Ч2	Під час призупинення компонентів ІКС з метою технічного обслуговування чи модернізації	2
Ч3	Під час функціонування ІКС чи компонентів системи	3
Ч4	Як в процесі функціонування ІКС так і під час призупинення компонентів системи	4

Таблиця 1.15 – Класифікація моделі порушника за місцем дії

Позначення	Опис місця дії порушника	Рівень загроз
Д1	Всередині приміщення але без доступу до технічних засобів	1
Д2	З робочих місць користувачів ІКС	2
Д3	З доступом у зберігання баз даних, архівів і т.д.	3
Д4	Має доступ в зону керування засобами безпеки ІКС	4

Таблиця 1.16 – Модель порушника

Посада	Категорія порушника	Мотив порушень	Рівень обізнаності щодо ІКС	Можливості подолання систем захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Внутрішні порушники по відношенню до ІКС							
Системний адміністратор	ПВ1	М2	К4	З3	Ч4	Д4	20
	3	2	4	3	4	4	
Бухгалтер	ПВ2	М3	К1	З2	Ч3	Д2	13
	2	3	1	2	3	2	
Менеджери, маркетолог	ПВ2	М3	К1	З2	Ч4	Д2	10
	2	3	1	1	1	2	
Головний менеджер	ПВ3	М2	К2	З2	Ч4	Д3	17
	4	2	2	2	4	3	
Директор	ПВ3	М2	К2	З3	Ч4	Д4	19
	4	2	2	3	4	4	
Логіст	ПВ4	М1	К1	З1	Ч3	Д1	8
	1	1	1	1	3	1	

Продовження таблиці 1.16

Посада	Категорія порушника	Мотив порушень	Рівень обізнаності щодо ІКС	Можливості подолання систем захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Зовнішні порушники по відношенню до ІКС							
Обслуговуючий персонал(прибиральниця, електрик)	ПЗ1	М1	К1	З1	Ч1	Д1	6
	1	1	1	1	1	1	
Відвідувачі	ПЗ2	М2	К1	З1	Ч3	Д1	9
	1	2	1	1	3	1	
Колишні працівники	ПЗ3	М2	К1	З1	Ч4	Д0	10
	2	2	1	1	4	0	
Хакери	ПЗ4	М3	К3	З4	Ч3	Д0	16
	3	3	3	4	3	0	
Конкуренти та їх агенти	ПЗ5	М4	К3	З4	Ч4	Д3	21
	4	3	3	4	4	3	

Як видно за таблиці 1.16 – Модель порушника основну загрозу для системи серед внутрішніх порушників несе системний адміністратор. Оскільки він виконує основні функції щодо забезпечення справного функціонування та безпеки інформаційно-комунікаційної системи. Також велику загрозу може нести директор оскільки на нього покладено багато обов'язків та керування процесами підприємства, але директор водночас є і власником підприємства, тобто в його інтересах не допустити реалізацію загроз через свої необачні дії, тож вірогідність реалізації такого сценарію дуже мала. Крім цього велику кількість загроз можуть спричинити дії головного менеджера, оскільки він має багато повноважень та надлишковий доступ до інформації в системі.

Із зовнішніх порушників найнебезпечнішими є конкуренти та їх агенти.

1.5 Модель загроз

Відповідно до НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» модель загроз є абстрактним формалізованим або неформалізованим описом методів і засобів здійснення загроз. Загалом загрози поділяються на природні(об'єктивні) - викликані впливом на інформаційне середовище природних фізичних процесів або стихійних природних явищ, що не залежать від волі людини та штучні (суб'єктивні) – викликані впливом на інформаційну сферу людини.

Також загрози інформаційної безпеки можуть бути класифіковані за аспектом інформаційної безпеки на який вони спрямовані, а саме:

Загрози конфіденційності(К) – неправомірний доступ до інформації, виникає коли сторонні особи отримують доступ до ІзОД.

Загрози цілісності(Ц) – являють собою навмисну заміну даних. Може виникнути через помилки в програмному забезпеченні чи навмисні дії сторонніх осіб.

Загрози доступності(Д) – являє собою створення умов за яких, за яких доступ до послуги або інформації буде заблокований, або неможлиим на деякий період часу, що не забезпечить досягненню бізнес-цілей.

Суб'єктивні загрози поділяються на випадкові та навмисні.

Нижче наведений перелік основних загроз безпеки інформації:

- збій або відмова в роботі технічних або програмних засобів;
- зміна умов фізичного середовища(пожежа, землетрус, повінь та інші стихійні лиха або аварії);
- помилки персоналу під час експлуатації ІКС;
- навмисні дії порушників;
- наслідки помилок під час проектування та розробки компонентів ІКС(ПЗ, засобів захисту та обробки інформації, тощо).

Випадковими загрозами суб'єктивної природи є помилкові дії персоналу що є ненавмисними, тобто через недбалість, неуважність та незнання. Сюди входить:

- ненавмисне зараження ПК вірусами;
- ненавмисне пошкодження носіїв інформації;
- недбалість при обробці даних: Це включає в себе некоректне збереження, передачу або видалення інформації. Наприклад, співробітник може випадково видалити важливі файли, помилково надіслати конфіденційні дані на невірну адресу електронної пошти або неправильно зберегти інформацію, що може призвести до її втрати;
- неуважність при використанні паролів та ідентифікаторів: це включає в себе вибір слабких паролів, використання одного й того ж пароля для кількох облікових записів або неправильне збереження ідентифікаторів доступу. Такі дії створюють ризик несанкціонованого доступу до системи;
- незнання політик безпеки та процедур: недостатнє розуміння політик безпеки і процедур компанії може призвести до навмисного або ненавмисного порушення заходів безпеки. Наприклад, співробітник може не усвідомлювати важливість захисту конфіденційної інформації або неправильно виконувати процедури резервного копіювання;

- неправильне використання технічних засобів: це може включати в себе неправильне налаштування системи, випадкове видалення або зміну налаштувань, неправильне використання захисних програм або некоректне підключення до мережі;

Усі ці ненавмисні дії персоналу можуть створювати загрози для безпеки інформації в комп'ютерних системах. Для мінімізації таких загроз необхідно надавати належну освіту та навчання персоналу з питань безпеки, розробляти чіткі політики та процедури, а також забезпечувати системи контролю та моніторингу.

Навмисними загрозами суб'єктивного походження є цілеспрямовані дії порушника, що націлені на проникнення в систему та отримання можливості несанкціонованого доступу до ресурсів ІТС або перешкоджання її роботи чи виведення з ладу.

До таких загроз входять:

- виведення з ладу систем забезпечення ІКС(електроживлення, охоронної сигналізації);
- використання персоналу ІКС конкурентами(підкуп, шантаж);
- використання комп'ютерних вірусів, підслуховуючих пристроїв та інших засобів розвідки;
- хакерські атаки: це включає спроби здійснити несанкціонований доступ до системи або мережі шляхом зламу паролів, використання вразливостей програмного забезпечення, перехоплення мережевого трафіку або використання соціальної інженерії;
- внутрішні загрози: це можуть бути дії зловживання довірою або недобросовісні дії з боку внутрішніх співробітників, які намагаються отримати несанкціонований доступ до ресурсів системи, розкрити конфіденційну інформацію або спричинити шкоду системі зсередини;
- викрадення облікових записів: це включає незаконне використання облікових записів користувачів шляхом отримання доступу до їхніх ідентифікаторів та паролів. Зловмисники можуть використовувати ці облікові

записи для отримання доступу до конфіденційної інформації або здійснення шкідливих дій в системі;

- соціальна інженерія: це включає маніпулювання людьми з метою отримання конфіденційної інформації або здійснення несанкціонованого доступу до системи. Це може бути використанням підступних методів переконання або обману, щоб отримати паролі, ідентифікатори доступу або іншу цінну інформацію;
- вандалізм і спам: це включає видалення, пошкодження або зміну даних в системі з метою завдання шкоди або перешкоджання її нормальному функціонуванню. Також входить відправлення небажаних повідомлень (спаму), які можуть перевантажити систему або створити незручності користувачам;
- використання забороненого політикою безпеки ПЗ, що дозволяє отримати доступ до критично важливої інформації(наприклад аналізаторів безпеки мереж)4

Ці загрози вимагають ретельного планування та впровадження заходів безпеки, таких як використання міцних паролів, регулярне оновлення програмного забезпечення, моніторинг активності мережі та розробка політик безпеки для запобігання атакам та виявлення порушень безпеки.

Таблиця 1.17 – Модель загроз ІКС

№	Вид загрози	Джерело загрози	Вразливість	Порушення	Рівень		Сума загроз
					Ризиків	Загроз	
1. Навмисні загрози(антропогенні та техногенні)							
1.1	НСД сторонніх осіб до ІзОД внаслідок фізичного доступу до обладнання	Зовнішнє	Відсутність системи охорони та відеоспостереження; Недостатній контроль за приміщенням	К	2	3	5
				Ц	3	4	7
				Д	2	3	5
1.2	Порушення Конфіденційності або цілісності інформації що зберігається в ІКС, внаслідок навмисних дій уповноваженого користувача	Внутрішнє	Відсутність функції резервного копіювання; Неправильний підбір персоналу	К	2	3	5
				Ц	2	3	5

Продовження таблиці 1.17

№	Вид загрози	Джерело загрози	Вразливість	Порушення	Рівень		Сума загроз
					Ризиків	Загроз	
1.3	Навмисне виведення з експлуатації систем життєзабезпечення мережі(електроживлення, інтернет, сигналізація)	Внутрішнє	Відсутність охоронної системи Відсутність системи відеоспостереження Недостатній контроль за приміщенням	К	1	2	3
				Ц	2	3	5
				Д	2	4	6
1.4	Впровадження та використання комп'ютерних вірусів, шкідливих програм для порушення безпеки даних	Внутрішнє та зовнішнє	Відсутність антивірусного ПЗ	К	3	5	8
				Ц	3	5	8
				Д	3	5	8
1.5	Використання зовнішніх носіїв інформації	Внутрішнє	Відсутність належного контролю за діями користувачів в системі	К	2	2	4
				Ц	2	2	4
				Д	2	2	4

Продовження таблиці 1.17

№	Вид загрози	Джерело загрози	Вразливість	Порушення	Рівень		Сума загроз
					Ризиків	Загроз	
1.6	Використання спеціального ПЗ для здійснення неправомірного доступу	Внутрішнє та зовнішнє	Надлишкові права доступу користувачів в системі Відсутність антивірусного ПЗ	К	2	4	6
				Ц	2	4	6
				Д	2	4	6
1.7	Скачування та запуск додатків з Інтернету	Внутрішнє	Відсутність квот	К	3	4	7
				Ц	2	4	6
				Д	2	3	5
1.8	Перевищення службових повноважень персоналом	Внутрішнє	Надлишкові права доступу користувачів в системі Відсутність належного контролю за діями користувачів в системі	К	3	4	7
				Ц	3	4	7
				Д	2	4	6

Продовження таблиці 1.17

№	Вид загрози	Джерело загрози	Вразливість	Порушення	Рівень		Сума загроз
					Ризиків	Загроз	
2. Випадкові загрози							
2.1	Розголошення інформації стороннім особам	Зовнішнє	Людський фактор	К	2	1	3
				Ц	1	1	2
				Д	1	1	2
2.2	Порушення цілісності та доступності інформації внаслідок ненавмисних дій користувачів	Внутрішнє	Відсутність резервного копіювання	Ц	2	2	4
				Д	2	2	4
2.3	Випадкове зараження системи вірусами	Внутрішнє	Відсутність антивірусного ПЗ Необізнаність персоналу	К	2	5	7
				Ц	2	5	7
				Д	2	5	7
2.4	Надходження фішингових листів на електронну пошту підприємства	Зовнішнє	Необізнаність персоналу Відсутність антивірусного ПЗ	К	2	5	7
				Ц	2	5	7
				Д	2	5	7

Продовження таблиці 1.17

№	Вид загрози	Джерело загрози	Вразливість	Порушення	Рівень		Сума загроз
					Ризиків	Загроз	
2.5	Збої в роботі програмних або апаратних засобів	Внутрішнє	Недосконале або нове ПЗ	К	1	2	3
				Ц	1	1	2
				Д	1	1	2
2.6	Втрата паролів	Внутрішнє Зовнішнє	Відсутність політики безпеки паролів	К	3	4	7
				Ц	3	4	7
				Д	3	4	7
3. Стихійні(впливи природних факторів)							
3.1	Стихійні лиха(землетрус, пожежа тощо)	Зовнішнє	Наявність легкозаймистих матеріалів	Ц	1	5	6
				Д	1	5	6
3.2	Відключення електропостачання або інтернету	Зовнішнє	Неякісна проводка. Відсутність альтернативного джерела живлення	Ц	1	5	6
				Д	1	5	6

Рівні ризиків та загроз:

- Низький. Оцінюється в 1 бал. Несе за собою незначні збитки.
- Середній. Оцінюється в 3 бали. Несе за собою середні втрати.
- Високий. Оцінюється в 5 балів. Призводить до великих збитків.

Проаналізувавши таблицю 1.17 – Модель загроз ІКС, можна зробити висновок що є необхідність у забезпеченні заходів для підвищення захисту.

Актуальними загрозами для інформаційної системи є:

- Навмисне або ненавмисне зараження системи комп'ютерними вірусами, та впровадження шкідливих програм для порушення безпеки даних. Вразливість у відсутності антивірусного ПЗ, надлишкових правах доступу користувачів системи та у відсутності належного контролю за діями користувачів в системі. Наслідками є порушення безпеки інформації.
- Скачування та запуск додатків з Інтернету. Вразливість у вільному використанні інтернет ресурсів. Наслідком є використання неліцензованого програмного забезпечення.
- Перевищення службових повноважень персоналом. Вразливість у надлишкових правах доступу користувачів та у відсутності належного контролю за діями користувачів в системі. Наслідки: отримання несанкціонованого доступу до ІзОД.
- Втрата паролів. Вразливість у відсутності політики безпеки відносно паролів.

1.6 Постановка задачі

Зважаючи на виконані обстеженння, для розробки комплексної системи захисту інформації необхідно обрати профіль захищеності відповідно до потреб системи та розробити проектні рішення для його реалізації.

Розробити положенняполітики безпеки.

Розрахувати економічну доцільність впровадження КСЗІ.

1.7 Висновки до першого розділу

В першому розділі було розглянуто:

- вид діяльності підприємства;
- виконано обстеження фізичного середовища;
- виконано обстеження обчислювальної системи;
- виконано обстеження середовища користувачів.

Окрім цього виконаний аналіз та здійснено класифікацію інформації, що циркулює на підприємстві, розроблено модель можливого порушника та модель загроз ІКС, на основі яких також виявлено актуальні загрози та вразливості в системі.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз існуючого стану захищеності

На підприємстві не впроваджено політику щодо використання антивірусного ПЗ. Кожен співробітник на власний розсуд приймає рішення про використання антивірусного ПЗ, ці процеси не контролюються директором компанії або системним адміністратором. З цього можна зробити висновок, що при безвідповідальних діях працівників підприємства можливе зараження системи вірусами, що призведе до неминучих втрат через відсутність засобів протидії цій загрозі. Тому потребується встановлення на кожний ПК ефективного антивірусного ПЗ та впровадження політики антивірусного захисту в компанії.

Для входу в систему працівниками використовується ім’я та прізвище користувача та унікальний пароль. Вимог до паролю немає, кожен співробітник встановлює його на свій розсуд. Необхідно впровадити політику безпеки паролів.

Також при обстеженні середовища користувачів було виявлено, що у більшості з них є надлишкові права доступу. Потрібно впровадити політику розмежування доступу.

Для входу до об’єкту інформаційної діяльності(ОІД) потрібно зайти в під’їзд жилого будинку та пройти по сходам до дверей офісу на першому поверсі. ввести 4-х значний код від магнітного замку на вхідних дверях підприємства. Також на дверях є врізний замок ключ від якого є тільки в директора.

2.2 Профіль захищеності

Згідно з НД ТЗІ 2.5-005 -99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від

несанкціонованого доступу» досліджувана АС підприємства ФОП «Shoes City» належить до Класу «3» — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу. Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

В межах кожного класу АС класифікуються на підставі вимог до забезпечення певних властивостей інформації. З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю і доступністю. В зв'язку з цим, в кожному класі АС виділяються підкласи. Обстежувана АС відноситься до підкласу «х.КЦД» — автоматизована система, в якій підвищені вимоги до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації.

Для кожного з підкласів кожного класу вводиться деяка кількість ієрархічних стандартних функціональних профілів, яка може бути різною для кожного класу і підкласу АС. Профілі є ієрархічними в тому розумінні, що їх реалізація забезпечує наростаючу захищеність від загроз відповідного типу (конфіденційності, цілісності і доступності). Наростання ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг. [12]

Така класифікація корисна для полегшення вибору переліку функцій, які повинен реалізовувати КЗЗ Обчислювальної системи, проектованої або існуючої АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення КСЗІ АС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків.

Відповідно до обстеження ІКС, аналізу моделі порушника та загроз було обрано наступний профіль захищеності з деякими змінами:

3.КЦД.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦА-1, ЦО-1, ЦВ-1, ДР-1,

ДВ-1, НР-1, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Опис послуг безпеки згідно НД ТЗІ 2.5.004-99:

КД-2 – базова довірча конфіденційність. Політика довірчої конфіденційності, яка реалізується КЗЗ, повинна визначати множину об'єктів ІКС, до яких вона відноситься. КЗЗ надає користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об’єкта.

КО-1 – Повторне використання об’єктів. Перш ніж користувач або процес отримає до свого розпорядження звільнений іншим користувачем чи процесом об’єкт, права доступу встановлені для попереднього користувача або процесу до даного об’єкта будуть скасовані перед тим, як користувач чи процес зможе отримати до свого розпорядження звільнений іншим користувачем чи процесом об’єкт, вся інформація, яка міститься в даному об’єкті, стане недоступною. Реалізовано.

КВ-1 – мінімальна конфіденційність. Реалізована при обміні завдяки стандартному набору послуг ОС Windows 10.

ЦД-1 – Мінімальна довірча цілісність. КЗЗ здійснює розмежування доступу на підставі атрибутів доступу процесу і захищеного об’єкта. Необхідні умови: НИ-1. Реалізована.

ЦА-1 Мінімальна адміністративна цілісність. КЗЗ здійснює розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта. Реалізована.

ЦО-1 – Обмежений відкат. Є автоматизовані засоби, що дозволяють авторизованому користувачу або процесу відкатити чи відмінити певний набір (множину) операцій, виконаних над захищеним об’єктом за деякий проміжок часу. Реалізовано. Необхідні умови: НО-1.

ЦВ-1 – Мінімальна цілісність при обміні. Реалізована при обміні завдяки стандартному набору послуг ОС Windows 10.

ДР-1 – Квоти. Політика використання ресурсів, що реалізується КЗЗ визначає множину об'єктів КС, до яких вона відноситься. Не реалізовано.

ДВ-1 – Ручне відновлення КЗЗ визначає множину типів відмов КС та переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Реалізоване. Необхідні умови НО:1.

НР-1 – Зовнішній аналіз. КЗЗ визначає перелік подій, що реєструються. Дає можливість здійснювати контроль за небезпечними діями. Реалізовано. Необхідні умови НО-1, НИ-1.

НИ-2 – Одиночна ідентифікація і автентифікація. КЗЗ автентифікує користувача із використанням захищеного механізму. Необхідні умови: НК-1. Реалізовано.

НК-1 – Однонаправлений достовірний канал. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем. Реалізована за рахунок вбудованого функціоналу ОС Windows 10.

НО-2 – Розподіл обов'язків адміністраторів КЗЗ розподіляє ролі адміністраторів і звичайного користувача і притаманні їм функції. Реалізовано, є системний адміністратор та адміністратор безпеки.

НЦ-2 – КЗЗ з гарантованою цілісністю. КЗЗ не підтримує домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Не реалізовано.

НТ-2 – Самотестування при старті. КЗЗ не описує властивості КС реалізовані процедури, що можуть використовуватися для оцінки правильності функціонування КЗЗ при старті. Не реалізовано. Необхідні умови НО-1.

НВ-1 – Автентифікація вузла. Підтвердження ідентичності виконується на підставі затвердженого протоколу автентифікації. Реалізована за рахунок вбудованого функціоналу ОС Windows 10.

Щоб реалізувати НЦ-2 потрібно від імені адміністратора у ОС Windows вибрати налаштування "Контроль цілісності". При цьому ОС буде контролювати цілісність системних та програмних файлів шляхом їх можливого змінення, навіть від імені адміністратора. Цей механізм захисту не дає оновлювати ПЗ за вимогою. При необхідності оновити ПЗ, що значить змінити системні та програмні файли, необхідно буде відключити цю функцію в налаштування ОС Windows, після цього провести оновлення ПЗ та відновити дану функцію для контролю цілісності.

Щоб реалізувати НТ-2 потрібно в налаштуваннях BIOS ввімкнути самотестування при старті, але ця функція не є надійною чере, бо вона тестує елементи перед завантаженням системи. Самотестування після запуску ОС можна реалізувати завдяки програмі MSI Afterburner AIDA64. Для цього потрібно встановити її на ПК та налаштувати на самоаналіз при старті, є можливість доповненого тестування у встановлений час та збереження звіту з тестування систем для подальшого аналізу системним адміністратором.

На підприємстві кожен співробітник може увійти у свій обліковий запис з будь-якого ноутбука, який раніше був авторизованим у мережі підприємства.

Вхід до системи дозволяється при спів падінні логіну та паролем. Доступ до даної інформації можливий лише системному адміністратору та директору.

Самотестування системи відбуватиметься при її старті за допомогою BIOS та за вимогою адміністратора спеціальним ПЗ.

Для аналізу системи на захищеність потрібно впровадити використання антивірусних програм та ПЗ, що дозволить в реальному часі слідкувати за інформаційними потоками підприємства. Також для цього в системі підприємства повинен відбуватися моніторинг журналу подій, за яким може слідкувати системний адміністратор або за потреби додатково найнятий спеціаліст з кібербезпеки підприємства.

2.3 Проєктні рішення

2.3.1. Розробка вимог з інформаційної безпеки

Для підприємства ФОП «Shoes City» необхідно впровадити ряд правил, що під час робочого процесу забороняють:

- підключати до робочого комп'ютери будь-які пристрої(USB-накопичувач, смартфон тощо) без згоди на це директора або системного адміністратора;
- використовувати для входу в систему обліковий запис іншого співробітника;
- здійснювати фото або відео зйомку без узгодження з головним менеджером або директором;
- скачувати та встановлювати на робочий ПК стороннє програмне забезпечення;
- використовувати Інтернет для розважальних або власних цілей, що не стосуються робочого процесу;
- відкривати посилання з електронних листів що приходять на електронну пошту;
- ділитися в соцмережах інформацією про підприємство з особами які не мають відношення до цієї інформації;
- переглядати/зберігати інформацію співробітнику доступ та обробка якої не входить в його повноваження.

2.3.2 Розмежування прав адміністрування

На підприємстві є одна особо що виконує роль системного адміністратора. Він слідкує за справним функціонуванням КС, вирішує технічні проблеми, що можуть виникнути з АС, проводить планові перевірки її компонентів.

Рекомендується найняти ще одну особу на посаду адміністратор безпеки. Він буде володіти всіма правами по впровадженню та налаштуванню КСЗІ, керує обліковими записами, вносить зміни до них при зміні посади працівників, а також за необхідності доступу до певної інформації.

Також в його обов'язки має входити:

- слідкування за справним функціонуванням ІКС, вирішувати технічні проблеми, що можуть виникати в процесі її роботи та проводити планові перевірки її компонентів;
- визначення правил щодо користування ІКС користувачами;
- можливість повернути ІКС до нормального функціонування при виникненні збоїв;
- періодичне тестування системи на наявність загроз інформаційної безпеки;
- встановлення та вчасне оновлення на кожному ПК антивірусного ПЗ;
- перегляд та аналіз журналу подій;
- регулярне оновлення існуючого ПЗ та за потреби встановлення нового;
- узгодження модернізації ІКС з директором підприємства;
- оброблення запитів на зміну атрибутів доступу користувачів;
- видання квот користувачам.

2.3.3 Розробка правил розмежування доступу

Під час обстеження середовища користувачів ІКС в таблиці 1.9 було розглянуто матрицю розмежування доступу користувачів. Проаналізувавши дану таблицю було виявлено що більшість користувачів мають небажані надлишкові права. Тому було прийнято рішення про створення правил

розмежування доступу та впровадження адміністративного керування доступом. Дані наведені в табл. 2.1.

Таблиця 2.1 – Нова матриця керування доступом

	1	2	3	4	5	6	7	8	9
Директор	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д	Ч Р З В Т Д
Головний менеджер	Ч Р З В Т Д	Ч Р З В Т Д	Ч З	Ч З	Ч Р З В Т Д	Ч	Ч З	Ч Р З В Т Д	Ч З
Бухгалтер	Ч З	Ч З	Ч Р З В Т Д	Ч З	Ч З Д	-	Ч	Ч З	Ч З
Системний адміністратор	Ч З	Ч З	-	Ч	Ч	-	Ч Р З В Т Д	Ч З	Ч З
Маркетолог	Ч З	Ч Р З Т Д	-	Ч	Ч	-	Ч	Ч Р З В Т Д	Ч З
Менеджери	Ч Р З Д	Ч Р З Т Д	-	-	Ч Р З Т Д	-	Ч	Ч Р З Д	Ч З

Ч – читання, Р – редагування, З – збереження, В – видалення, Т – імпорт/експорт, Д – друк. Цифрами 1 – 8 позначена інформація з таблиці 1.5 1 – інформація про клієнтів, 2 – інформація про товар, 3 – звіти бухгалтерії, 4 – документи про закупівлю товарів, 5 – наявність товару та його кількість, 6 –

плани з розширення компанії, 7 – інформація про об’єкти та системи безпеки, 8 – рекламна інформація, 9 – інформація про постачальників товару.

2.3.4 Обґрунтування вибору системи антивірусного захисту

В розглянутій в першому розділі таблиці Таблиця 1.17 – Модель загроз ІКС було виявлено загрози, що призводять до зараження системи вірусами, а саме:

- впровадження та використання комп’ютерних вірусів, шкідливих програм для порушення безпеки даних;
- випадкове зараження системи вірусами;
- надходження фішингових листів на електронну пошту підприємства.

Ці загрози мають високу ймовірність реалізації через вразливість, що полягає у відсутності антивірусної системи в ІКС та політики антивірусної безпеки. Тому було прийнято рішення встановити антивірусне ПЗ на всі ПК в системі.

В ході аналізу було виявлено що найкращим варіантом буде обрати ESET Endpoint Antivirus для Windows версії 7.3, оскільки ця програма відповідає вимогам нормативних документів із технічного захисту інформації в обсязі функцій, зазначених у документі «Програмний продукт антивірусного захисту ESET Endpoint Antivirus для Windows (EEA) версії 7.X з системою централізованого керування антивірусним захистом корпоративних мереж ESET Security Management Center версії 7.X. Технічні вимоги за критеріями технічного захисту інформації» з рівнем гарантій Г-2 згідно документу "Експертний висновок № 1325 Дійсний з 28 січня 2022 до 28 січня 2025".

2.3.5 Фізичний захист інформації

Під час аналізу можливих загроз та вразливостей в таблиці 1.17 – Модель загроз ІКС було виявлено вразливість що полягає в недостатньому контролі за приміщенням та діями персоналу. Для зменшення даної вразливості директором підприємства було прийнято рішення про впровадження системи відеоспостереження в офісі.

Встановлення системи відеоспостереження значно підвищить інформаційну безпеку на підприємстві за рахунок забезпечення постійного контролю та фіксації дій працівників або можливих відвідувачів, що унеможливить для них непомітне виконання несанкціонованих дій. Слід врахувати що відповідно до ст. 307 Цивільного кодексу України, фізична особа може бути знята на фото-, кіно-, теле- чи відеоплівку лише за її згодою. З даних вимог випливає що відеоспостереження за працівниками в робочий час можливе тільки за згоди особи на його проведення. В іншому випадку це вважається незаконним.

На основі отриманої згоди від працівників директором компанії затверджено встановити камеру в Кімнаті №1 в якій знаходиться найбільша кількість працівників(4 менеджери та 1 маркетолог).

Розташування для камери обрано на шафі в Кімнаті №1 таким чином щоб в зону фіксації потрапляли робочі місця працівників та вхідні двері до офісу.

Доступ до управління камерою та перегляду відео буде доступний тільки директору. Було обрано поворотну бездротову Wi-Fi IP Камеру 3Мп Reolink E1. Вартість її складає 1699 грн.

Характеристики: Поворотний механізм забезпечує огляд по горизонталі на 355° та по вертикалі на 50°. Управління відбувається через спеціальний додаток що можна встановити на смартфон або ПК, спостерігати можна з любої точки де є доступ до інтернету. Також в камеру вбудований датчик руху який вмикає камеру при спрацюванні, що дозволяє вести запис тільки

необхідних моментів. Окрім цього є вбудований мікрофон та динамік що дозволяє записувати та відтворювати звук.

2.4 Політика безпеки підприємства

Політика безпеки повинна розроблятися на основі проведених аналізів стосовно фізичного середовища ОІД, Середовища користувачів, моделі порушників та загроз, технології обробки інформації та інших чинників.

Опис:

Загальні правила безпеки:

- в системі повинне бути розмежування прав доступу. всі користувачі повинні ідентифікуватися системою;

- для доступу у систему повинна використовуватися та ідентифікація та автентифікація користувачів;

- повинні бути встановлені антивірусні програми, а також регулярно проводитися оновлення баз даних вірусів та сигнатур;

- необхідно регулярно проводити навчання персоналу для підвищення їх

обізнаності в сфері інформаційної безпеки;

- регулярне оновлення операційної системи та програмного забезпечення;

- відстеження ризиків та загроз безпеки інформації та вживання відповідних заходів.;

- регулярна технічна діагностика обладнання з метою виявлення несправностей;

при виявленні несправностей необхідно терміново зв’язатися з відповідальними особами.

2.4.1 Політика резервного копіювання

Мета: Забезпечення безперебійності бізнес-процесів підприємства шляхом забезпечення доступності резервних копій даних. Запобігання втраті важливої інформації внаслідок випадкового видалення, пошкодження, хакерських атак або природних катастроф.

Застосування: Політика резервного копіювання повинна застосовуватися до всіх систем та даних, що циркулюють в інформаційній системі підприємства.

Частота резервного копіювання: Регулярне резервне копіювання всіх важливих даних та систем повинно проводитися згідно з визначеним графіком. Рекомендується щоденне резервне копіювання.

Зберігання копій: Резервні копії повинні зберігатися на віддалених і безпечних медіа, відокремлених від основних систем. Рекомендується використовувати зовнішні накопичувачі або хмарні сервіси, наприклад Google Диск.

Перевірка цілісності та відновлення даних: Періодична перевірка цілісності резервних копій для впевненості у їхньому правильному функціонуванні та можливості відновлення даних.

Тестування відновлення: Регулярне проведення тестів відновлення з резервних копій, щоб переконатися у функціональності процесу відновлення та відповідності даних відновленому стану.

Доступ до резервних копій: Доступ до резервних копій повинен бути обмежений і контрольований системним адміністратором підприємства для запобігання несанкціонованому доступу та зміні даних.

Оновлення політики: Політика резервного копіювання повинна переглядатися директором підприємства один раз на рік та оновлюватися регулярно з урахуванням змін в інфраструктурі, технологіях та потребах підприємства.

2.4.2 Політика антивірусного захисту

Мета політики: створити вимоги яким повинні дотримуватися всі користувачі та ПК в ІКС для гарантування ефективного захисту від вірусів.

Область дії: поширюється на всіх працівників компанії

Відповідальність:

Вчасно звантажувати та встановлювати свіжі модифікації антивірусного програмного забезпечення.

Встановленням та налаштування антивірусного ПЗ займається адміністратор безпеки.

Ніколи не відкривати будь-які файли, що торкаються електронної пошти від невідомого та підозрілого джерела. Слід негайно помістити такого роду повідомлення до папки «Видалене», а потім очистити її для остаточного видалення.

Видаляти папку «Спам», ланцюг та інше електронну пошту, що не має атрибутів підприємства згідно з політикою безпеки.

Ніколи не завантажувати файли з невідомих чи підозрілих джерел.

Уникати прямого дискового доступу (читання/запис), за винятком того, що відповідає необхідним діловим вимогам.

Перед використанням завжди сканувати диск/переносний носій/тощо від невідомого джерела або клієнтів на предмет вірусів.

Регулярно дублювати критичні дані і системні конфігурації, зберігати їх в безпечному місці (видалене сховище, хмарне сховище).

Відповідальність за виконання інструкцій антивірусного захисту покладається на всіх співробітників.

2.4.3 Політика використання мережі Інтернет

Мета політики:

Збільшити рівень інформаційної безпеки підприємства за рахунок введення інструкцій та правил користування мережею Інтернет для працівників.

Область дії: Політика поширюється на всіх працівників компанії, що мають доступ до Інтернету у робочий час.

Відповідальні особи: За виконання політики безпеки співробітниками відповідальним назначається адміністратор безпеки.

Інструкція політики:

Користуватися мережею Інтернет дозволяється у випадку:

- приймання та обробки замовлень;

- пошук інформації, яка необхідна для виконанні своїх прямих обов'язків;

- для комунікації з іншими співробітниками компанії.

Забороняється:

- використовувати комп'ютер для особистих цілей;

- грати в комп'ютерні ігри;

- дивитися фільми, серіали та інше;

- скачувати невідомі файли;

- встановлювати невідоме ПЗ;

- вести неузгоджену діяльність від імені компанії;

- передавати конференційну інформацію третім особам;

- здійснювати видалення, модифікацію інформації на сайтах та соціальних мережах компанії;

- переглядати інформацію, яка вважаються незаконною законодавством України.

Відповідальність: У разі порушення політики безпеки працівником будуть застосовані дисциплінарні або штрафні санкції.

Періодичність та порядок перегляду політики: Політика безпеки повинна переглядатися раз на рік директором та адміністратором безпеки.

При необхідності може коректуватися незалежно від цього терміну в залежності від потреб компанії.

2.4 Висновки до другого розділу

В другому розділі було проведено аналіз існуючих систем захисту та вибрано необхідний профіль захищеності відповідно до потреб підприємства. Також було запропоновано проектні рішення, а саме:

- розроблено вимоги з інформаційної безпеки;
- впровадження адміністративного розмежування доступу;
- обрано систему антивірусного захисту;
- впровадження системи відеоспостереження;

Окрім цього також було розроблено політики безпеки:

- політика резервного копіювання;
- політика антивірусного захисту;
- політика використання мережі Інтернет.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Метою виконання економічної частини є техніко-економічне обґрунтування доцільності запровадження комплексної системи захисту. Для цього обумовлюється економічна ефективність застосування основних результатів, встановлених в процесі роботи.

Для визначення економічної ефективності необхідно:

- розрахувати капітальні витрат, що потребує розроблена КСЗІ;
- розрахувати експлуатаційні витрати на утримання і обслуговування КСЗІ;
- визначити річний економічний ефект від впровадження КСЗІ;
- розрахувати коефіцієнт повернення інвестицій ROSI та термін окупності капітальних інвестицій;
- визначити та проаналізувати показники економічної ефективності запропонованих рішень;
- зробити висновок щодо економічної доцільності.

Підприємство ФОП «Shoes City» займається перепродажем брендового взуття через інтернет-магазин та фізичну точку збуту. Річний прибуток підприємства складає 5 000 000 грн.

3.1 Розрахунок капітальних витрат

3.1.1 Розрахунок трудомісткості розробки КСЗІ

Трудомісткість розробки КСЗІ на підприємстві визначається за 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 $t_{тз}$ – тривалість складання технічного завдання на розробку програмного механізму захисту цілісності програмного коду; $t_{тз} = 12$ годин;

$t_{в}$ – тривалість розробки концепції безпеки; $t_{в} = 10$ годин

$t_{а}$ – тривалість аналізу ризиків, пов'язаних з загрозами; $t_{а} = 10$ годин

$t_{вз}$ – тривалість визначення вимог до до заходів методів та засобів захисту; $t_{вз} = 12$ годин;

$t_{озб}$ – тривалість вибору основного рішення з забезпечення безпеки інформації; $t_{озб} = 12$ годин;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації; $t_{овр} = 10$ годин;

$t_{д}$ – тривалість документального оформлення політики безпеки; $t_{д} = 10$ годин.

Розрахуємо трудомісткість розробки КСЗІ за формулою (3.1):

$$t = 12 + 10 + 10 + 12 + 12 + 10 + 10 = 76 \text{ годин.}$$

3.1.2 Розрахунок витрат на створення КСЗІ

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

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

.

Заробітна плата спеціаліста з інформаційної безпеки визначається за формулою:

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

.

де t – загальна тривалість розробки КСЗІ, годин;

$З_{іб}$ – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину. (Середня зарплата 30 000 грн на місяць, приблизно 190 грн за годину при 40 робочих годинах на тиждень)

Розрахуємо зарплату спеціаліста за формулою (3.3):

$$З_{зп} = t*З_{іб} = 190*76 = 14\ 440\ грн$$

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t \cdot С_{мч}, \text{ грн,} \quad (3.4)$$

де t – трудомісткість розробки КСЗІ, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал}*Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р} \text{ грн/година,} \quad (3.5)$$

де P – встановлена потужність ПК, кВт, P = 0,4 кВт;

$t_{нал}$ – кількість задіяних робочих станцій, $t_{нал} = 1$;

$С_е$ – тариф на електричну енергію, грн/кВт*година, $С_е$ = 2,64 грн/кВт*год;

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

$Н_а$ – річна норма амортизації на ПК, частки одиниці, $Н_а = 1/5 = 0.2$;

$Н_{апз}$ – річна норма амортизації на ліцензійне ПЗ, частки одиниці, $Н_{апз}$ = 0.5;

$К_{лпз}$ – вартість ліцензійного ПЗ, грн(ESET Endpoint Antivirus 1850 грн/рік), $К_{лпз} = 1850$ грн;

$F_р$ – річний фонд робочого часу (при 40-годинному робочому тижні),

$F_р$= 1920 год.

Щоб визначити залишкову вартість ПК, треба знайти його накопичену амортизацію. Вартість ПК = 15 000 грн, мінімальний термін корисної служби = 60 місяців, термін використання 30 місяців.

$$Ф_{зал} = 15\,000 – (15\,000 * 40)/60 = 5000 \text{ грн}$$

Отже, вартість 1 години машинного часу за формулою (3.5):

$$С_{мч} = 0.4 \cdot 1 \cdot 2.64 + \frac{5000 \cdot 0.2}{1920} + \frac{1850 \cdot 0.5}{1920} = 2.06 \text{ грн/година;}$$

Вартість витрат машинного часу за формулою (3.4):

$$З_{мч} = t * С_{мч} = 76 * 2,06 = 156,25 \text{ грн.}$$

Витрати на розробку КСЗІ за формулою (3.2) складають:

$$К_{рп} = З_{зп} + З_{мч} = 14\,440 + 156,\,25 = 14\,596,\,25 \text{ грн.}$$

3.1.3 Капітальні (фіксовані) витрати на створення комплексу

Капітальні витрати на впровадження проектних рішень кваліфікаційної роботи розраховуються за формулою складають:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, \text{грн,}$$

(3.6)

де $К_{рп}$ – вартість розробки КСЗІ та залучення для цього зовнішніх консультантів, тис. грн; $К_{рп}$ = 14 596, 25 грн;

$К_{зпз}$ –вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн, $К_{зпз}$ = 1850 грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн; $К_{пз}$ = 0 грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн; $К_{аз}$ = 1700 грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, $К_{навч}$ = 10000 грн;

$К_н$ – витрати на встановлення обладнання та налагодження КСЗІ, грн; $К_н$ = 5000 грн.

Таким чином капітальні витрати на впровадження КСЗІ за формулою (3.6) складуть:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_н = 14\ 596,\ 25 + 1850 + 1700 + 10000 + 5000 = 33\ 146,\ 25грн.$$

3.2 Розрахунок поточних (експлуатаційних) витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, грн,$$

(3.7)

де $С_в$ - вартість відновлення й модернізації системи ($С_в$ = 0);

$С_к$ - витрати на керування системою в цілому;

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

Оскільки до вартості ліцензії програмного забезпечення входить постійне підтримання та оновлення до нових версій – витрати на відновлення й модернізацію не виникають.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{св} + С_{ел} + С_о + С_{тос}, грн,$$

(3.8)

де $С_н$ - витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи, яка складає 6000 грн;

$С_а$ – річний фонд амортизаційних відрахувань; $С_а = К_{зпз} / 2 = 1850 / 2 = 925$;

$С_{єв}$ – витрати єдиного внеску на загальнообов'язкове соціальне страхування, грн;

$С_{ел}$ – вартість електроенергії, що споживається апаратурою КСЗІ протягом року, грн;

$С_о$ – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу, грн; $С_о = 0$ грн;

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс КСЗІ визначаються у відсотках від вартості капітальних витрат – 3%, грн;

$$С_{тос} = К * 0.03 = 33\ 146,\ 25 = 994,38\ грн.$$

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

$$С_з = З_{осн} + З_{дод},\ грн. \qquad (3.9)$$

Оскільки виконання робіт вимагає залучення спеціаліста з інформаційної безпеки, директором було прийнято рішення найняти спеціаліста на 0.2 ставки з додатковим окладом 10%.

$$З_{осн} = 20\ 000 * 0,2 * 12 = 48\ 000\ грн$$

$$З_{дод} = 0.1\ З_{осн} = 4800\ грн$$

Отже, річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки за формулою (3.9), складає:

$$С_з = З_{осн} + З_{дод} = 52800\ грн.$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 52800*0,22 = 11\ 616\ грн.$$

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \ грн., \quad (3.10)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,4 кВт);

$F_р$ – річний фонд робочого часу КСЗІ ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 2,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року за формулою (3.10):

$$С_{ел} = 0,4*1920*2,64 = 2027,52 \ грн.$$

Витрати на керування системою інформаційної безпеки ($С_к$) за формулою (3.8) складають:

$$С_к = 6000+925+994,38+11616+52800+2027,52 = 74\ 362,9 \ грн.$$

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

$$С = 74\ 362,9 \ грн.$$

3.3 Оцінка величини можливого збитку

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі визначається за формулою:

$$U = П_п + П_в + V, \ грн \quad (3.11)$$

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

$П_в$ - вартість відновлення працездатності вузла або сегмента корпоративної мережі, грн;

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

Втрати робочого часу і простою співробітників визначаються за формулою:

$$П_п = \frac{\sum З_с}{F} t_п, \; грн, \qquad (3.12)$$

де $З_с$ – заробітна плата співробітників атакованого вузла чи сегмента корпоративної мережі, грн за місяць;

F – місячний фонд робочого часу, при 40 годинному робочому тижні становить 176 годин;

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

Для визначення заробітної плати атакованого вузла визначимо заробітну плату працівників в таблиці 3.1

Таблиця 3.1 – Заробітна плата працівників з урахуванням ЄСВ

Посада	Кількість працівників	Місячна заробітна плата, грн	Єдиний соціальний внесок, грн	Зарплата з урахуванням ЄСВ, грн
Бухгалтер	1	15000	3300	18300
Головний менеджер	1	20000	4400	24400
Маркетолог	1	14000	3080	17080
Менеджер	4	12000	2640	58560
Системний адміністратор	1	15000	3300	18300

$$\sum З_с = 136\ 640\ грн$$

Визначимо трати робочого часу і простою співробітників за формулою (3.12):

$$П_{п} = \frac{136640}{176} \cdot 2 = 1552,7\ грн$$

Вартість відновлення вузла визначається за формулою:

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

де $П_{ви}$ – витрати на повторне введення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

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

$П_{зч} =$ 5000 грн.

Витрати на повторне введення інформації рахуються за формулою:

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

де $t_{ви}$ – час повторного введення загубленої інформації співробітниками, годин; $t_{ви} = 3$ год.

$$П_{ви} = \frac{136640}{176} \cdot 3 = 2329 \text{ грн}$$

Витрати на повторне введення інформації визначаються за формулою :

$$П_{пв} = \frac{\sum З_{о}}{F} \cdot t_{в},\ грн, \quad (3.15)$$

де $t_{в}$ – час відновлення після атаки персоналом, годин; $t_{в} = 3$ год;

$З_{о}$ - заробітна плата обслуговуючого персоналу, грн.

Заробітна плата системного адміністратора 15 000 грн на місяць і 20 000

грн на 0,2 ставки.

$$П_{пв} = \frac{15000+4000}{176} \cdot 3 = 323{,}86, \textit{ грн},$$

Вартість відновлення вузла вирахуємо за формулою (3.13):

$$\textit{П}_в = 2329 + 323{,}86 + 5000 = 7652{,}86 \textit{ грн.}$$

Витрати від зниження обсягу продажів за час простою визначаються за формулою:

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}), грн, \quad (3.16)$$

де $F_г$ – річний фонд часу роботи організації (52 робочі тижні, 6-ти денний робочий тиждень, 10-ти годинний робочий день); $F_г$ = 3120 годин;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн в рік; О = 5 000 000 грн на рік;

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

$t_в$ – час відновлення після атаки персоналом, годин; $t_в$ = 3 год;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками, годин; $t_{ви}$ = 3 год.

$$V = \frac{5000000}{3120} \cdot (2 + 3 + 3) = 12820{,}5 \text{ грн;}$$

Визначимо збиток від атаки на вузол за формулою (3.11):

$$U = 1552{,}7 + 7652{,}86 + 12820{,}5 = 22026 \textit{ грн}$$

Загальний збиток від атаки на вузол визначається за формулою:

$$В = \sum_i \sum_n U \text{ грн}, \quad (3.17)$$

де І – число атакованих вузлів або сегментів корпоративної мережі, І =1;

N – середнє число атак на рік, N = 5.

$$B = \sum_1 \sum_5 22026 = 110\ 130 \text{ грн}$$

Величина загального збитку повинна бути скорегована на величину збитку, що може бути завдана в результаті дій системного адміністратора та діями співробітників. Для ФОП «Shoes City» такий збиток може складати 80 000 грн. та 40 000 грн відповідно.

$$B = 110\ 130 + 80\ 000 + 40\ 000 = 230\ 130 \text{ грн.}$$

3.4 Загальний ефект від впровадження КСЗІ

З урахуванням ризиків порушення безпеки інформації можна визначити загальний ефект від впровадження КСЗІ за формулою:

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

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

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

С – щорічні витрати на експлуатацію КСЗІ, грн;

$$E = 230\ 130 * 0{,}5 - 74\ 362{,}9 = 40\ 702 \text{ грн.}$$

3.5 Визначення та аналіз показників економічної ефективності КСЗІ

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

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

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

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

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{40\ 702}{33\ 146{,}25} = 1{,}22, \quad \textit{частки одиниці,}$$

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

$$ROSI > (N_{деп} - N_{інф})/100), \quad (3.20)$$

де $N_{деп}$ – річна депозитна ставка, (14,55%);

$N_{інф}$ – річний рівень інфляції, (14,8%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1{,}22 > (14{,}55 - 14{,}8)/100$$

$$1{,}22 > -0{,}0025.$$

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

$$T_o = \frac{К}{E} = \frac{1}{ROSI} \quad (3.21)$$

$$T_o = \frac{1}{1.22} = 0.82 \text{ року, що дорівнює близько 10 місяців}$$

3.6 Висновок

В економічному розділі було проаналізовано основні економічні показники для впровадження КСЗІ та визначено, що запропоноване в кваліфікаційній роботі рішення є доцільним для підприємства ФОП «Shoes City», оскільки коефіцієнт повернення інвестицій ROSI складає 1,22. Термін окупності при цьому складе 0,82 року, що становить приблизно 10 місяців.

ВИСНОВКИ

В першому розділі наведено загальну інформацію про підприємство, обґрунтовано необхідність створення КСЗІ, виконано обстеження ІКС підприємства, а саме: фізичного середовища, середовища обчислювальної системи, інформаційного середовища та середовища користувачів. На основі цих даних було розроблено модель порушника та модель загроз інформаційної безпеки. В результаті було виявлено основні вразливості та недоліки ІКС підприємства ФОП «Shoes City».

В другій частині згідно проведено аналізу потенційних загроз та вразливостей було обрано профіль захищеності та запропоновано проектні рішення для підвищення інформаційної безпеки, до них відносяться: розмежування прав адміністрування, правила розмежування доступу користувачів, вибір системи антивірусного захисту, фізичний захист. Також було визначено необхідні політики безпеки: політика антивірусного захисту, політика резервного копіювання та політика використання мережі Інтернет.

В третьому розділі проведено економічні розрахунки капітальних витрат на впровадження КСЗІ та річних експлуатаційних витрат. Визначено що запропоновані в другому розділі рішення будуть доцільними для підприємства, оскільки коефіцієнт ROSI дорівнює 1.22, а термін окупності склав 0.82 року, що приблизно 300 днів або 10 місяців.

ПЕРЕЛІК ПОСИЛАНЬ

1 Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук - Дніпро: НТУ «ДП», 2020. - 47 с.

2 Методичні рекомендації до економічної частини дипломного проекту зі спеціальності 125 кібербезпека / Упоряд.: Д.П. Пілова - Дніпро: НТУ «ДП»2019.

3 Хакери атакують малі бізнеси втричі частіше за великі [Електронний ресурс] URL: https://www.kliksolutions.com.ua/great-info/hakery-atakuyut-mali-biznesy-vtrychi-chastishe-za-velyki

4 Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text

5 НД ТЗІ 3.7-003-05 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 №806 - Порядок проведення робіт із створення КСЗІ в ІТС

6 НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу - Київ 1999 р.;

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

8 Закон Україні «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 No80-VI // Відомості Верховної Рали України-1994-№80.(Електронний ресурс) Режим доступу до ресурсу: zakon.rada.gov.ua/laws/show/80/94-Bp

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

28.04.1999] - К.: ДСТСЗІ СБУ, 1999-№22 (Нормативний документ системи технічного захисту інформації)

10 НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформацій в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999] - К.: ДСТСЗІ СБУ, 1999-№22 (Нормативний документ системи технічного захисту інформації)

11 НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. [Чинний від 04, 12.2000] - К.: ДСТЗІ СБУ, 2000-№53 (Нормативний документ системи технічного захисту інформації)

12 НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. [Чинний від 28.04.1999] - К.: ДСТСЗІ СБУ, 1999-№22 (Нормативний документ системи технічного захисту інформації)

13 НД ТЗІ 3.6-001-2000 Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. [Чинний від 20.12.2000] - К.: ДСТСЗІ СБУ, 2000-N060 (Нормативний документ системи технічного захисту інформації)

14 ДСТУ 3396.1-96 Захист інформації. Технічний захист. інформації. Порядок проведення робіт.

15 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі НД ТЗІ 3.7-001-99 - Київ 1999 р.;

16 Загрози інформаційної безпеки [Електронний ресурс] Режим доступу до ресурсу: http://www.security.ase.md/publ/ru/pubru91

17 Опис інформаційної безпеки підприємства [Електронний ресурс] - Режим доступу до ресурсу: https://bos.kiev.ua/infosecurity

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	38	
6	А4	2 Розділ	15	
7	А4	3 Розділ	12	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. («відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК В. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-19-2

Гузченко Святослава Владиславовича

на тему: «Комплексна система захисту інформації інформаційно - комунікаційної системи магазину роздрібної торгівлі «Shoes City»»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на_____сторінках.

Метою кваліфікаційної роботи є забезпечення заданого рівня безпеки інформації, яка обробляється в ІКС інтернет-магазину ФОП «Shoes City».

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, розробка проектних рішень та їх реалізації.

Запропоновано матрицю розмежування доступу, розроблено елементи політики безпеки щодо: фізичного захисту, антивірусного захисту, використання мережі Інтернет та резервного копіювання. Обґрунтовано розподіл ролей адміністраторів та вибір засобів антивірусного захисту.

Практичне значення результатів кваліфікаційної роботи полягає у адаптації запропонованих рішень до інтернет-магазину ФОП «Shoes City».

До недоліків відноситься:

- незначні неточності в описі середовищ функціонування КСЗІ;
- недостатньо обґрунтована модель загроз та профіль захищеності;
- відсутність пропозицій щодо налаштувань служб вбудованої КЗЗ.

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

За час дипломування Гузченко С.В. проявив себе фахівцем, здатним достатньо 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, доцент Магро В.І.

Керівник спец. розділу, ст. викладач Кручінін О.В.

ДОДАТОК Г. Перелік документів на оптичному носії

1. Диплом_Гузченко.pdf
2. Диплом_Гузченко.docx
3. Презентація_Гузченко.pptx