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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи ступеню бакалавра

студентки *Хмари Милени Володимирівни*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1] _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства «Книш О.А.»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Горєв В. М.			
розділів:				
спеціальний	ст. викл. Саксонов Г.М.			
економічний	к.е.н., доц..Пілова Д. П.			

Рецензент				

Нормоконтролер				

Дніпро

2021

ЗАТВЕРДЖЕНО
завідувач кафедри
безпеки інформації та телекомунікацій
_____д.т.н., проф. Корнієнко В.І.
«_____»_____2021 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенці *Хмарі Милені Володимирівні* **академічної групи** *125-17-2*
спеціальності *125 Кібербезпека*
за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства «Книш О. А.»*
Затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021 № 317-С

Розділ	Зміст	Термін виконання
Розділ 1	*Стан питання. Постановка задачі*	05.04.2021 - 23.04.2021
Розділ 2	*Обстеження фізичного середовища, обчислювальної системи, інформаційного середовища, середовища користувачів, складено модель загроз та модель порушника, розроблено політику безпеки*	26.04.2021 - 21.05.2021
Розділ 3	*Техніко-економічне обґрунтування доцільності впровадження політики безпеки*	24.05.2021 - 08.06.2021

Завдання видано: _____ Саксонов Г. М.
Дата видачі: 01.04.2021
Дата подання до екзаменаційної комісії: _____
Прийнято до виконання: _____ Хмара М. В.

РЕФЕРАТ

Пояснювальна записка: 76 с., 8 рис., 22 табл., 6 додатків, 12 джерел.

Об'єкт дослідження: політика безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства «Книш О. А.».

Мета проекту: підвищення рівня захищеності інформації в ІТС приватного підприємства «Книш О. А.».

Методи розробки: спостереження, аналіз, порівняння, опис.

У першому розділі кваліфікаційної роботи розглянуто стан питання, проведено аналіз нормативно-правової бази, видів інформації та доступу до неї, підстав для створення КСЗІ та політики безпеки.

У другому розділі наведені загальні відомості про підприємство. Виконано обстеження фізичного середовища, обчислювальної системи, інформаційного середовища, середовища користувачів, складено модель загроз та модель порушника, розроблено політику безпеки використання мережі Інтернет, електронної пошти, антивірусного захисту та «чистого столу».

У третьому розділі визначено доцільність впровадження політики безпеки. Були розраховані витрати на розробку політики безпеки, капітальні витрати, експлуатаційні витрати та оцінка можливого збитку від атаки.

Практичне значення роботи полягає у підвищенні рівня захищеності інформації на об’єкті інформаційної діяльності за рахунок аналізу слабких місць та розробки політики безпеки.

Наукова новизна роботи полягає у визначенні загроз безпеки інформації та їх запобіганні.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

РЕФЕРАТ

Пояснительная записка: 76 с., 8 рис., 22 табл., 6 приложений, 12 источников.

Объект исследования: политика безопасности информации информационно-телекоммуникационной системы частного предприятия «Кныш О. А.».

Методы разработки: наблюдение, анализ, сравнение, описание.

Цель проекта: повышение уровня защищенности информации в ИТС частного предприятия «Кныш О. А.».

В первом разделе квалификационной работы рассмотрено состояние вопроса, проведен анализ нормативно-правовой базы, видов информации и доступа к ней, оснований для создания КСЗИ и политики безопасности.

Во втором разделе приведены общие сведения о предприятии. Выполнено обследование физической среды, вычислительной системы, информационной среды, среды пользователей, составлена модель угроз и модель нарушителя, разработана политика безопасности использования сети Интернет, электронной почты, антивирусной защиты и «чистого стола».

В третьем разделе определена экономическая целесообразность внедрения политики безопасности. Были рассчитаны затраты на разработку политики безопасности, капитальные затраты, эксплуатационные расходы и оценка возможного ущерба от атаки.

Практическое значение работы состоит в повышении уровня защищенности информации на объекте информационной деятельности за счет анализа слабых мест и разработки политики безопасности.

Научная новизна работы заключается в определении угроз безопасности информации и их предотвращению.

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ОБЪЕКТ ИНФОРМАЦИОНОЙ ДЕЯТЕЛЬНОСТИ

ABSRACT

Explanatory note: 76 p., 8 pic., 22 tab., 6 applications, 12 sources.

Object of development: information security policy of the information and telecommunications system of the private enterprise "Knysh O. A.".

Development methods: observation, analysis, comparison, description.

The purpose of the project is to increase the level of information security in the private enterprise "Knysh O. A.".

In the first chapter of the qualification work, the state of the issue is considered, the regulatory framework, types of information and access to it, the grounds for creating a comprehensive information security system and a security policy.

The second section provides general information about the company. A survey of the physical environment, computer system, information environment, and user environment was performed, a threat model and an intruder model were compiled, and a security policy for using the Internet, email, antivirus protection, and a "clean table" was developed.

The third chapter defines the feasibility of implementing a security policy. Security policy development costs, capital expenditures, operating costs, and assessment of possible attack damage were calculated.

The practical significance of the work is to increase the level of information security at the information activity facility by analyzing weaknesses and developing a security policy.

The scientific novelty of the work lies in the identification of threats to information security and their prevention.

COMPREHENSIVE INFORMATION SECURITY SYSTEM, SECURITY POLICY, THREAT MODEL, INTRUDER MODEL, INFORMATION SECURITY, OBJECT OF INFORMATION ACTIVITY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

КСЗІ - комплексна система захисту інформації;

ОІД - об'єкт інформаційної діяльності;

ПП – приватне підприємство;

ПБ - політика безпеки;

ІБ - інформаційна безпека;

АС - автоматизована система;

ЕОТ - електронно-обчислювальна техніка;

ЗУ - закон України;

ІТС - інформаційно-телекомунікаційна система;

ОС - операційна система;

ПЗ - програмне забезпечення;

ТЗІ - технічні засоби інформації;

ІзДО - інформація з обмеженим доступом;

К – конфіденційність;

Ц – цілісність;

Д – доступність.

ЗМІСТ

ВСТУП

«Хто володіє інформацією, той володіє світом», – сказав колись Уїнстон Черчіль.

На сьогоднішній день інформація – це найцінніший актив, який відіграє важливу роль у сферах економіки та бізнесу України.

З кожним роком зростає тенденція на впровадження нових комп'ютерних на телекомунікаційних технологій у сфері бізнесу. Суспільство та держава відходять від паперових носіїв інформації та переходять до більш сучасних методів обробки інформації, наприклад - жорсткі диски, сервери, хмарне сховище.

Пропорційно розвитку технологій зростає і потреба в інформаційній безпеці на підприємствах, де обробляється інформація з обмеженим доступом або та, яка становить комерційну тайну.

Спотворення, модифікація, видалення чи просто несанкціонований доступ до конфіденційної інформації може призвести до серйозних наслідків та матеріальних збитків, навіть до краху підприємства.

Тому для забезпечення цілісності, доступності та конфіденційності інформації впроваджується комплексні методи націлені на захисту інформації.

Розробка політики безпеки це однин із етапів побудови КСЗІ. Щоб точніше розробити політику безпеки необхідно визначити можливі загрози, проаналізувати вразливості та слабкі місця в інформаційній системі підприємства. Чим точніше буде створена політика безпеки – тим менша імовірність витоку інформації .

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

З кожним роком кількість кіберзлочинів зростають. Кількість кібератак в 2020 році збільшилася на 51% в порівнянні з 2019 роком; 86% всіх атак були спрямовані на організації. Порівняння кількості інцидентів наведено на рисунку 1.1. Найбільше зловмисників цікавили державні і медичні установи, а також промислові компанії.

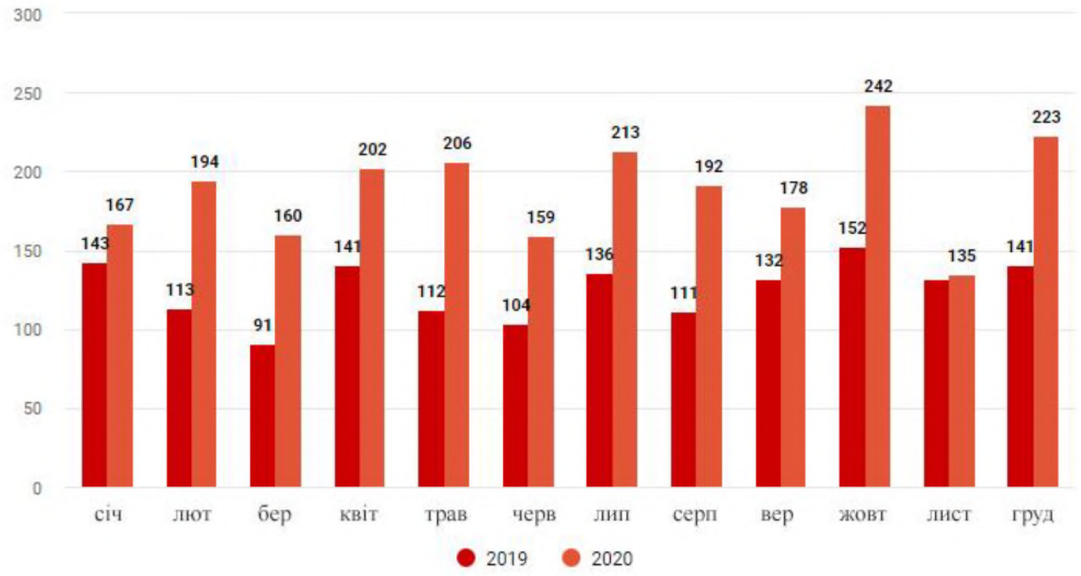


Рисунок 1.1 - Кількість інцидентів в 2019 і 2020 роках

Кількість інцидентів з використанням шкідливого ПЗ збільшилася на 54% в порівнянні з 2019 роком. Серед всіх шкідників, які використовуються в атаках на організації, беззмінним лідером протягом двох років залишаються програми-вимагачі. В інцидентах, спрямованих на приватних осіб, найчастіше фігурували шпигунське ПЗ і банківські трояни.

В атаках на організації основними векторами доставки шкідливого ПЗ залишаються електронна пошта (71%) і компрометація комп'ютерів, серверів та мережевого обладнання (24%), а в атаках на приватних осіб хакери віддають перевагу також електронній пошті і веб-сайтам (по 32%). Типи вкрадених даних наведено на рисунку 1.2.

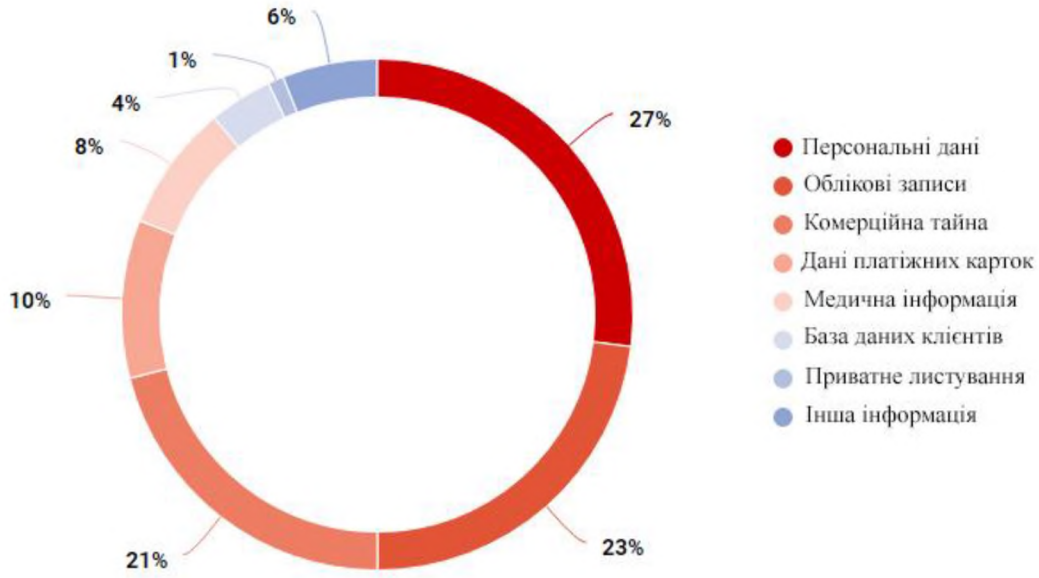


Рисунок 1.2 - Типи вкрадених даних

Оскільки інформація, циркулююча в інформаційній системі, має велику важливість для функціонування підприємства, її витік чи порушення доступу до неї може спричинити значну матеріальну та репутаційну шкоду підприємству, власнику інформації або суб'єкту персональних даних, питання захисту інформації в ІТС є актуальним.

1.2 Аналіз нормативно-правової бази у сфері захисту інформації

Нормативно-правова база в сфері захисту інформації має велику кількість документів, що описують методи збереження інформаційних властивостей, встановлює основні вимоги для розробки політики інформаційної безпеки та етапи побудови комплексної системи захисту інформації.

Згідно Закону України «Про інформацію». Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1].

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Згідно Закону України «Про захист інформації в інформаційно-телекомунікаційних системах». Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації [2].

Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством. У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом.

Згідно наказу «Про затвердження нормативного документа системи технічного захисту інформації НД ТЗІ 1.6-005-2013». Об'єкт інформаційної діяльності - інженерно-технічна споруда (приміщення), транспортний засіб, де здійснюється озвучення та/або обробка технічними засобами інформації з обмеженим доступом [3].

1.2.1 Загальні положення та вимоги з категоріювання

Об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов'язковому категоріюванню [3].

Категоріювання може бути первинним, черговим або позачерговим.

Категоріювання здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об'єкті.

Відповідальність за своєчасність категоріювання та правильність встановлення категорії об'єкта покладається на керівника установи - власника (розпорядника, користувача) об'єкта.

Об'єктами категоріювання є об'єкти інформаційної діяльності, в тому числі об'єкти ЕОТ.

Категоріювання здійснюється за ознакою: ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД.

Об'єктам, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, встановлюється четверта (IV) категорія.

За рішенням розпорядників (користувачів) інформації або за рішенням власників (розпорядників, користувачів) об'єктів, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, об'єктам може встановлюватися III категорія.

Об'єкти, яким встановлено відповідну категорію, вносяться до Переліку категорійованих об'єктів, який ведеться власником (розпорядником, користувачем) об'єктів інформаційної діяльності

1.2.2 Підстави створення КСЗІ

Згідно «Термінології в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 1.1-003-99».

Комплексна система захисту інформації; КСЗІ — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС [4].

Обґрунтування необхідності створення КСЗІ

Згідно «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003 -2005». 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 [5].

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.

1.2.3 Процес обстеження ОІД

Відповідно до «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003 -2005» [5].

Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

Під час виконання цих робіт ІТС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки (далі - середовища функціонування ІТС).

Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

При обстеженні обчислювальної системи ІТС повинні бути проаналізовані й описані:

- загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);
- види і характеристики каналів зв'язку;
- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;

- можливі обмеження щодо використання засобів та ін.

Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням та ін.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту

При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС (дані і програмне забезпечення). Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані види (в термінах об'єктів КС) її представлення в ІТС.

Для кожного виду інформації і типу об'єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи КС (спостережність), яким вони повинні задовольняти.

Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІТС

Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об'єктів, режим доступу до них, можливий 12 вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

При обстеженні фізичного середовища здійснюється аналіз взаємного розміщення засобів обробки інформації ІТС на об'єктах інформаційної

діяльності, комунікацій, систем життєзабезпечення і зв'язку, а також режим функціонування цих об'єктів.

Аналізу підлягають такі характеристики фізичного середовища:

- територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план);

- наявність охорони території та перепускний режим;

- наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІТС;

- режим доступу до компонентів фізичного середовища ІТС;

- вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки;

- наявність елементів комунікацій, систем життєзабезпечення і зв'язку, що мають вихід за межі контрольованої зони;

- наявність та технічні характеристики систем заземлення;

- умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;

- наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

При обстеженні середовища користувачів здійснюється аналіз:

- функціонального та кількісного складу користувачів, їхніх функціональних обов'язків та рівня кваліфікації;

- повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів;

- повноважень користувачів щодо управління КСЗІ;

- рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІТС.

- наявності СЗІ в ІТС

1.2.4 Процес аналізу загроз та побудови моделі порушника

Загроза (threat) — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС [4].

Відповідно до «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003 -2005» [5]. Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз, наприклад:

- зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);
- збої і відмови у роботі обладнання та технічних засобів АС;
- наслідки помилок під час проектування та розробки компонентів АС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);
- помилки персоналу (користувачів) АС під час експлуатації;
- навмисні дії (спроби) потенційних порушників.

Випадковими загрозами суб’єктивної природи (дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

- дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв’язку, видалення даних, програм та ін.);
- ненавмисне пошкодження носіїв інформації;

- неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

- неумисне зараження ПЗ комп'ютерними вірусами;

- невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;

- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

- неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);

- наслідки некомпетентного застосування засобів захисту;

- інші.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

- порушення фізичної цілісності АС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення АС (електроживлення, уземлення, охоронної сигналізації, вентиляції та ін.);

- порушення режимів функціонування АС (обладнання і ПЗ); - впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

- використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів;

- використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;

- крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

- несанкціоноване копіювання носіїв інформації; - читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;

- одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад");

- неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;

- впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

- інші.

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

Для створення моделі загроз необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

1.2.5 Процес створення політики безпеки інформації

Під політикою безпеки інформації (далі - політика безпеки) слід розуміти набір вимог, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо АС, окремого її компонента, послуги захисту, що реалізується системою і т. ін. Політика безпеки інформації в АС є частиною

загальної політики безпеки організації і повинна успадковувати основні її принципи.

Під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. В АС може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

1.3 Постановка задач

Зробити повне обстеження ОІД, згідно нормативно-правових документів описаних у розділі, а саме:

- обстеження фізичного середовища;
- обстеження обчислювальної системи ;
- обстеження інформаційного середовища;
- обстеження середовища користувачів;
- зробити аналіз загроз та вразливостей;
- визначити модель порушника;
- розробити політику безпеки для підприємства;
- зробити економічне обґрунтування впровадження політик безпеки;
- зробити висновки.

1.4 Висновки

Кількість кібератак у 2020 році збільшилася на 54% в порівнянні з 2019 роком, зловмисники найчастіше використовують віруси і трояни, а найпопулярнішим методом поширення і зараження користувачів виступає електронна пошта, тому питання захисту інформації стає більш актуальним.

В розділі наведено перелік основних нормативно-правових документів та наказів у сфері інформаційної безпеки, зазначено основні положення та рекомендації для створення КСЗІ та політики безпеки.

Під час розробки політики безпеки повинно бути проаналізоване фізичне середовище, особливості ОС, технологія обробки інформації, середовище користувачів, моделі порушників і загроз та інші чинники.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про ПП «Книш О. А.»

Об’єктом інформаційної діяльності (далі ОІД) є приватне підприємство «Книш О. А.»

Адреса: 49000, м. Дніпро, вул.. Центральна 2/4.

Специфікація діяльності підприємства: роздрібна торгівля дорослим та дитячим взуттям та одягом.

Графік роботи:

- З понеділка по суботу з 10:00 до 20:00 без перерви;
- У неділю з 10:00 до 19:00 без перерви.

Штат працівників:

- директор - 1 особа;
- креативний директор - 1 особа;
- бухгалтер - 1 особа;
- системний адміністратор - 1 особа;
- старший продавець - 1 особи;
- продавець - 3 особи;
- водій - 1 особа;
- прибиральниця - 1 особа.

2.2 Обстеження фізичного середовища

Об’єктом інформаційної діяльності (далі ОІД) є приватне підприємство «Книш О. А.».

Ситуаційний план наведено на рисунку 2.1.

Підприємство знаходиться на адресою: вул. Центральна 2/4,вхід до ОІД знаходиться на першому поверсі у п’яти поверховій будівлі.

Генеральний план ОІД наведено на рисунку 2.2.

ОІД має два поверхи:

- перший поверх використовується як торгівельний зал, а також складу товару;

- другий поверх призначений для торгівельного залу та складу, а також головного офісу підприємства та бухгалтерії.

Площа ОІД - 164 м^2.

Характеристика складових ОІД:

Висота стель - 400 м; стінні перегородки - 150 мм; стіни зовнішні з цегли - 500 мм.

Вікна (4 шт.) металопластикові, подвійні, з розміром 1500 мм · 2000 мм.

Вхідні двері до магазину - металопластикові, потрійне скло, з розміром отвору 1500 мм · 2000 мм.

Вхідні двері на задньому дворі - металеві з розміром отвору 1000 мм · 2000 мм.

Міжкімнатні двері (4шт.) матеріал - МДФ плити, з розміром 2000 мм · 900 мм.

Підлога на підприємстві – паркет, плитка на складах та у санвузлу.

Контрольована зона (КЗ) обмежена стінами ОІД. Режим КЗ здійснюється за допомогою охоронної системи, постійною відео реєстрацією подій, у неробочий час ОІД вхідні двері закриті на врізний замок та захищенні металевими ролетами. Ключі від ОІД мають лише директор, старший продавець, заступник старшого продавця та бухгалтер.

Підключенні комунікації:

ОІД має доступ до мережі Інтернет, підключення здійснюється оптично-волокнистим кабелем, доступ до Інтернету надає компанія «Фрегат».

Система електроживлення іде від трансформаторної підстанції, яка знаходиться за межами ОІД. Мережа 220В; світильники з LED лампами.

Розташування ліній електромережі та Інтернет кабелю наведено у ДОДАТКУ Б.

Системи каналізації та водопостачання підключені до міських комунальних мереж, які знаходиться за межами ОІД.

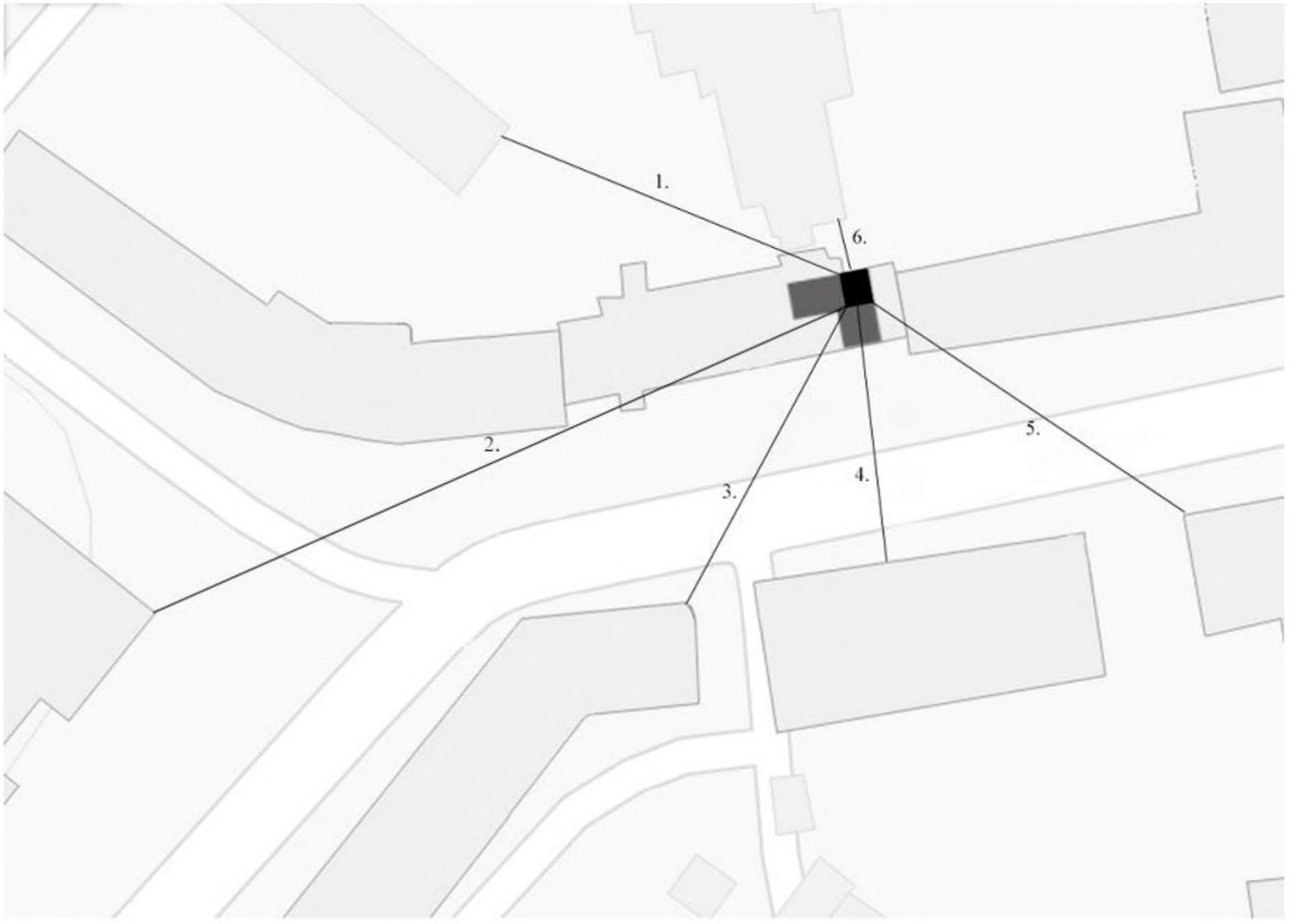
Система опалювання: автономна.

Система заземлення в будівлі відсутня.

Система охорони та сигналізації:

- датчиків диму (7 шт.) на обох поверхах;
- магнітоконтактні датчики на відкриття (6 шт.) на дверях та вікнах;
- інфрачервоні датчики руху (8 шт.);
- камери відеоспостереження (11шт);
- головна централь з клавіатурою.

Розташування охоронної системи та камер відеоспостереження наведено у ДОДАТКУ В.



УМОВНІ ПОЗНАЧЕННЯ:

- будинки
- межа ОІД
- тротуари
- контрольована зона
- дороги
- лінії відстані від КЗ до ближніх будинків

Рисунок 2.1 – Ситуаційний план

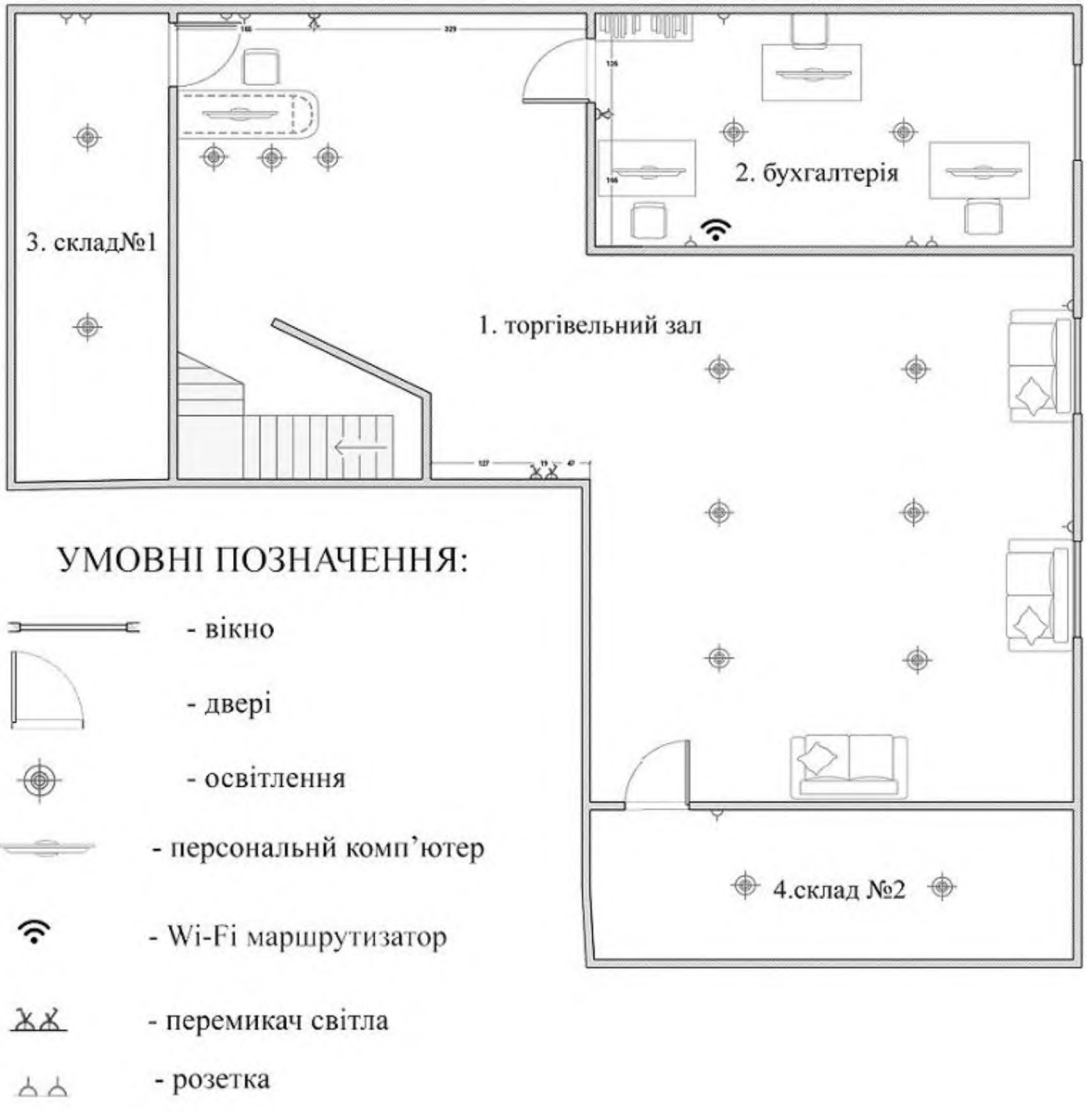
Відстані від КЗ до інших споруд наведено у таблиці 2.1.

Таблиця 2.1 - Відстані інших будівель від КЗ

№	Відстань від КЗ, м	Адреса	Призначення будівлі
1	43	Вул. В'ячеслава Липинського, 1А	Жилий будинок
2	94,7	Просп. Дмитра Яворницького, 50	Торговий комплекс Passage
3	40,6	Вул. В'ячеслава Липинського, 2	Жилий будинок, дрібні магазини
4	30,3	Вул. В'ячеслава Липинського, 4	Жилий будинок,офіси, дрібні магазини
5	48,5	Вул. В'ячеслава Липинського, 6	Жилий будинок,офіси, дрібні магазини
6	17,5	Вул. В'ячеслава Липинського, 1Б	Жилий будинок

1. ОІД, перший поверх

2. ОІД, другий поверх



УМОВНІ ПОЗНАЧЕННЯ:

- вікно
- двері
- освітлення
- персональнй комп'ютер
- Wi-Fi маршрутизатор
- перемикач світла
- розетка

Рисунок 2.2 – Генеральний план ОІД

Розміри приміщень ОІД, м^2:

Перший поверх: торгівельний зал - 35,9 м^2; склад – 17,9 м^2; санвузол – 2,5 м^2.

Другий поверх: торгівельний зал – 69,1 м^2; бухгалтерія – 17 м^2; склад №1 – 10,9 м^2; склад №2 – 11 м^2.

Всього - 164 м^2.

2.3 Обстеження обчислювальної системи ОІД

Обчислювана система поєднує в собі технічні пристрої, що знаходяться в межах ОІД. Підключення до мережі Інтернет забезпечує Інтернет провайдер «Фрегат», який надає послуги відповідно договору.

Обладнання інформаційної системи складається з 4 комп'ютерів, 2 принтерів, Wi-Fi роутера. Перелік основних технічних засобів наведено у таблиці 2.2. Розташування ОТЗ наведено на рисунку 2.4.

Всі компоненти системи маються доступ до Інтернету від Wi-Fi роутера, який підключений до оптоволоконного кабелю провайдера, тобто підключення за топологією відноситься до типу «зірка».

Схема ІТС наведена на рисунку 2.3.

Таблиця 2.2 - Перелік основних технічних засобів

Назва у системі	Кількість	Назва обладнання	Системні характеристики	Місце розташування
ПК1	1	Ноутбук Asus M515DA-EJ228T	Екран 15.6 "(1920x1080) Full HD, AMD Ryzen 5 3500U (2.1 - 3.7 ГГц), RAM 8 ГБ, SSD 256 ГБ, AMD Radeon Vega 8 Graphics	Кабінет директора/ бухгалтерія

Продовження таблиці 2.2

ПК2	1	Ноутбук Acer Aspire 5 A514-54-38SY	Екран 14 "IPS (1920x1080), Intel Core i3-1115G4 (3.0 - 4.1 ГГц), RAM 8 ГБ, SSD 256 ГБ, Intel UHD Graphics	Кабінет директора/ бухгалтерія
ПК3	1	Ноутбук Lenovo G575	Екран 15.6 "(1366x768), AMD E-350 (1.6 ГГц), RAM 4 ГБ, DDR3 1066 МГц, 450 ГБ, AMD Radeon HD 6310.	Торгівельний зал
ПК	1	Ноутбук Lenovo V15-ADA (82C700E9RA)	Екран 15.6 "(1920x1080), AMD Athlon Silver 3050U (2.3 - 3.2 ГГц), RAM 4 ГБ, HDD 500 ГБ , AMD Radeon Graphics	Кабінет директора/ Бухгалтерія
Принтер	2	Лазерне МФУ Samsung SCX 4220	-	Біля каси / бухгалтерія
комп'ю-терна мишка	4	Logitech M170 Wireless	-	Кабінет директора/ бухгалтерія/ торговий зал
Wi-Fi роутер	1	TP-LINK Archer A6	-	Бухгалтерія

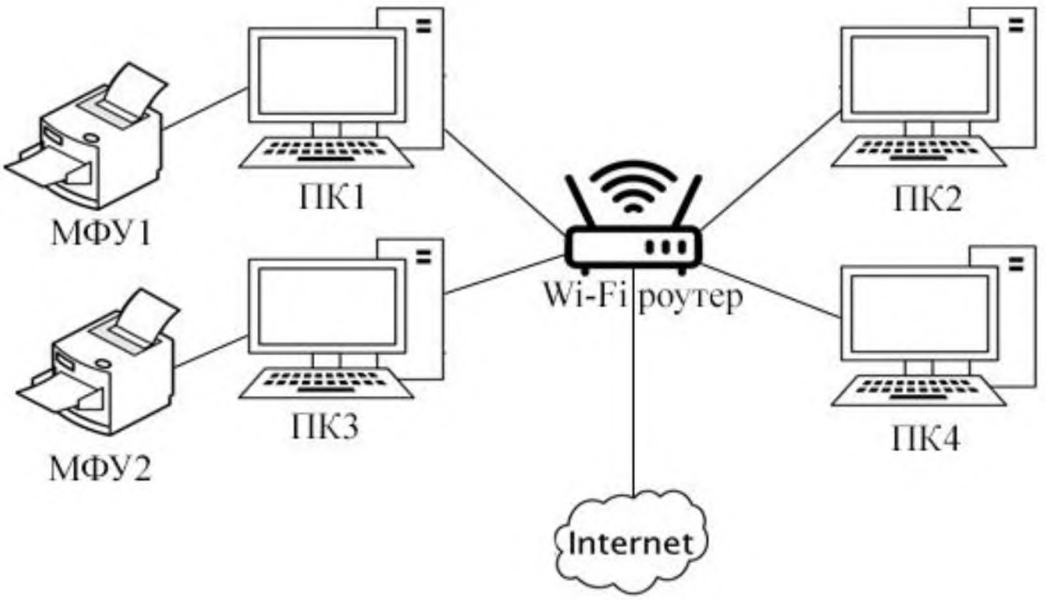


Рисунок 2.3 - Схема ІТС

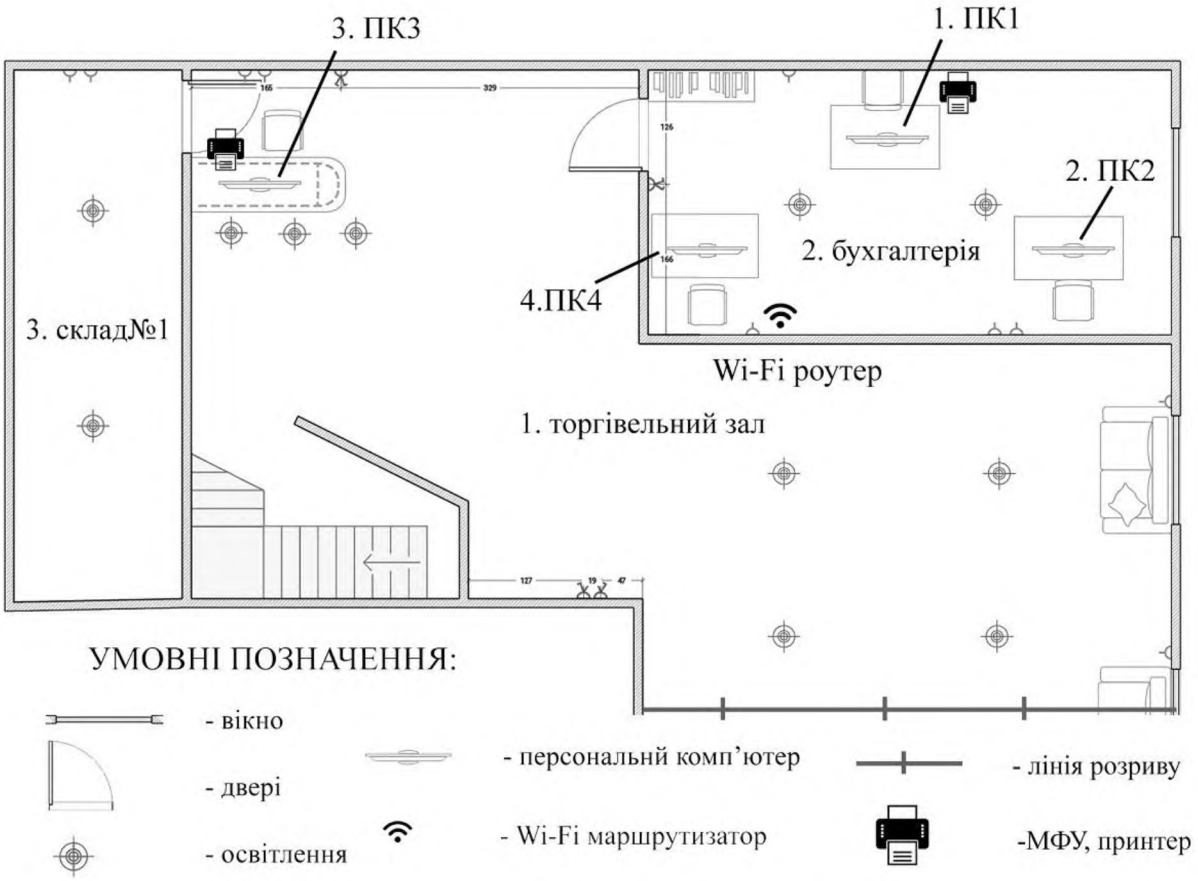


Рисунок 2.4 – Розташування ІТС

Таблиця 2.2 - перелік встановленого програмного забезпечення

Найменування ПЗ	Версія	Місце встановлення	Використовують
ОС Windows 7	Professional x64	ПК1, ПК2, ПК3, ПК4	Всі
Google Chrome	91.0.4472.77		Всі
Microsoft Office 2013	15.0.5345.1002		Всі
Антивірус Eset nod32	14.1.19.0		Всі
Viber	15.4.1.1		Директор, бухгалтер, креативний директор
1С:Предприятие	8.4	ПК1, ПК3, ПК4	Директор, продавець, бухгалтер
Adobe Photoshop	12.0.4	ПК1,ПК2	Креативний директор та головний директор
WinRAR	5.3.12	ПК1, ПК2, ПК3, ПК4	Всі
CCreaner	6/12	ПК1, ПК2, ПК3, ПК4	Всі

2.4 Обстеження середовища користувачів

На ОІД працюють та можуть знаходитись впродовж робочого дня наступні особи:

- директор;
- креативний директор;
- бухгалтер;
- системний адміністратор;
- старший продавець;
- продавець;
- прибиральниця;
- водій;
- прибиральниця.

Посадові обов'язки кожного з працівників наведено у таблиці 2.5.

Організаційна структура підприємства наведена на рисунку 2.5.

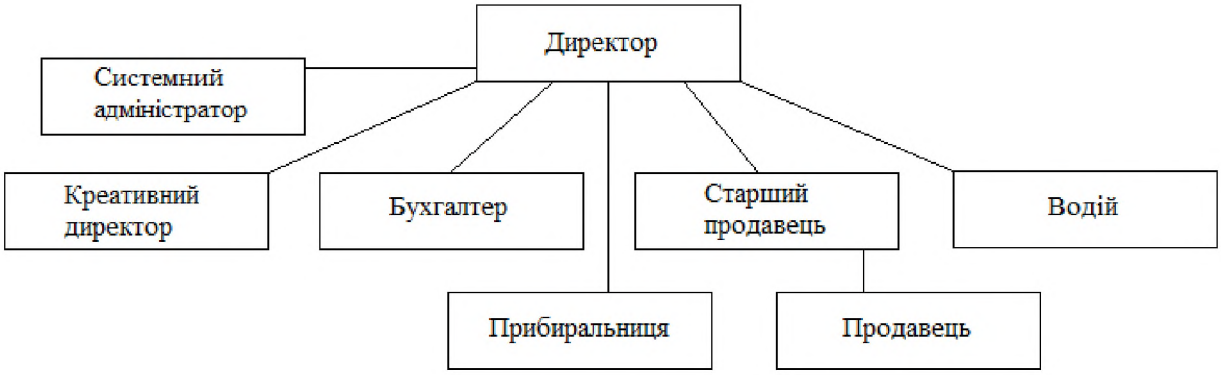


Рисунок 2.5 - Організаційна структура підприємства

Таблиця 2.4 - Підрозділи підприємства

Назва підрозділу	Характеристика підрозділу	Посада
Адміністративний	Управління підприємством. Ведення бухгалтерського обліку та аудиту. Видача заробітної плати.	Директор, бухгалтер.

Продовження таблиці 2.4

Виробничий	Спілкування з клієнтами, підтримка технічних засобів, ведення соціальних мереж.	Креативний директор,сис. адміністратор, продавець.

Таблиця 2.5 - Обов'язки та посади працівників

Посада	Кількість	Підрозділ	Посадові обов'язки
Директор	1	Адміністра-тивний	- контроль робочих процесів та діяльності підприємства; - прийняття рішень та супроводження договорів з постачальниками; - вибір та закуп товару.
Креативний директор	1	Виробничій	- займається рекламою та графічним дизайном; - відповідає на соціальні мережі; - фотографую товар для соціальних мереж та сайтів.
Бухгалтер	1	Адміністра-тивний	- займається фінансовим обліком та аудитом; - складає баланс підприємства; - рахує та видає заробітну плату працівникам компанії.
Продавець	3	Виробничий	- консультування клієнтів компанії щодо товару; - продаж товару; - переоблік товару.

Продовження таблиці 2.5

Системний адміністратор	1	Виробничий	- усунення технічних несправностей, технічна підтримка елементів ІС; - забезпечує розмежування доступу співробітників до інформації згідно політики безпеки; - відповідає за резервні копії даних; - підтримка працездатності мережі; - видалення шкідливого ПЗ та вірусів; - оновлення системи; - підтримка інформаційної безпеки.
Старший продавець	1	Виробничий	- складає графік роботи для продавців та себе; - оформляє замовлення; - працює с касовим апаратом та видає чеки; - оформляє повернення товару та грошей; - вирішує конфліктні ситуації; - продаж товару; - робить переоблік товару.
Прибираль-ниця	1	Виробничий	- прибирання території ОІД.

Продовження таблиці 2.5

Водій	1	Виробничий	- доставка товарів з відділень пошти; - перевезення товарів між складами.

2.5 Обстеження інформаційної системи

На підприємстві інформація зберігається у електронному та паперовому вигляді, власником інформації виступає директор. На ОІД циркулює відкрита інформація та конфіденційна інформація з обмеженим доступом, що не становить державної таємниці, тому ОІД присвоєна четверта (IV) категорія. Класифікація інформації за режимом доступу наведена у таблиці 2.6.

Інформаційна безпека складається з трьох основних вимог - конфіденційності, цілісності та доступності.

Рисунок 2.6 – Складові інформаційної безпеки

Конфіденційність інформації (К) — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом [4].

Цілісність інформації (Ц) — властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом [4].

Доступність (Д) — властивість ресурсу системи, яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний [4].

Таблиця 2.6 - Класифікація інформації за режимом доступу

Вид інформації	Режим доступу	Правовий режим	Вимоги до захисту	Мають доступ
Інформація про послуги та товари	Відкрита	-	Д, Ц	Всі
Інформація про графік роботи	Відкрита	-	Д, Ц	Всі
Персональні дані співробітників	ІзОД	Конфіденційна	К, Д, Ц	Д, Б, СА
Трудові договори	ІзОД	Конфіденційна	К, Д, Ц	Д, Б, СА
Інформація про клієнтів	ІзОД	Конфіденційна	К, Д, Ц	Д, К, КД, СП, П, В
Інформація про постачальників	ІзОД	Конфіденційна	К, Д, Ц	Д, Б, В, СА
База даних замовлень	ІзОД	Конфіденційна	К, Д, Ц	Д, К, КД, СП, П, В

Продовження таблиці 2.6

Інформація про технічне обладнання	ІзОД	Конфіденційна	К, Д, Ц	Д, СА
Накладні на товар	ІзОД	Конфіденційна	К, Д, Ц	Д, К, КД, СП, П, В
Установчі документи підприємства	ІзОД	Конфіденційна	К, Д, Ц	Д, Б, КД, СА
Фінансова звітність	ІзОД	Конфіденційна	К, Д, Ц	Д, К
Паролі для доступу у систему та соц. мереж	ІзОД	Конфіденційна	К, Д, Ц	Д, КР, СА

Список скорочень у таблиці _: Д – директор; КД – креативний директор; Б – бухгалтер; СА – системний адміністратор; СП – старший продавець; П – продавець; В – водій; ПРИБ – прибиральниця.

Таблиця 2.7 - Визначення вимог до рівня конфіденційності , цілісності та доступності інформації.

Вид інформації	Рівень конфіденційності	Рівень цілісності	Рівень доступності
Інформація про послуги та товари	К1	Ц3	Д3
Інформація про графік роботи	К1	Ц3	Д3

Продовження таблиці 2.7

Персональні дані співробітників	К3	К3	Д2
Трудові договори	К3	К2	Д2
Інформація про клієнтів	К3	К2	К2
Інформація про постачальників	К4	К4	К2
База даних замовлень	К2	К4	К4
Інформація про технічне обладнання	К2	К2	К2
Накладні на товар	К2	К4	К3
Установчі документи підприємства	К2	К3	К2
Фінансова звітність	К4	К4	К3
Паролі для доступу у систему та соціальних мереж	К5	К4	К3

Для виявлення рівнів конфіденційності, цілісності і доступності у таблиці 2.7 були використані такі властивості:

Рівні конфіденційності:

К1 – рівень конфіденційності інформації, при якому збитків від витоку конфіденційної інформації не буде;

К2 – рівень конфіденційності інформації, при якому збитки від витоку конфіденційної інформації будуть мінімальні;

К3 – рівень конфіденційності інформації, при якому збитки від витоку конфіденційної інформації будуть відчутними;

К4 – рівень конфіденційності інформації, при якому збитки від витоку конфіденційної інформації будуть значними;

К4 – рівень конфіденційності інформації, при якому збитки від витоку конфіденційної інформації будуть критичними.

Рівні цілісності:

Ц1– рівень цілісності інформації, при якому порушення цілісності не призведе до збитків;

Ц2– рівень цілісності інформації, при якому порушення цілісності призведе до мінімальних збитків;

Ц3– рівень цілісності інформації, при якому порушення цілісності призведе до відчутних збитків;

Ц4– рівень цілісності інформації, при якому порушення цілісності призведе до значних збитків;

Ц5– рівень цілісності інформації, при якому порушення цілісності призведе до критичних збитків.

Рівні доступності

Д1– рівень доступності інформації, при якому порушення доступності не призведе до матеріальних збитків;

Д2– рівень доступності інформації, при якому порушення доступності призведе до мінімальних матеріальних збитків;

Д3– рівень доступності інформації, при якому порушення доступності призведе до відчутних матеріальних збитків;

Д4– рівень доступності інформації, при якому порушення доступності не призведе до значних матеріальних збитків;

Д5– рівень доступності інформації, при якому порушення доступності не призведе до критичних матеріальних збитків.

2.5.1 Технологія обробки інформації

Інформація про послуги, товари та графік роботи знаходитися у відкритому доступі на сайті підприємства, а також соціальних мережах. Редагується системним адміністратором та креативним директором.

Персональні дані співробітників та трудові договори, містять інформацію про паспортні дані, ІНН та місце проживання, зберігаються на комп'ютері бухгалтера та директора, редагуються директором і бухгалтером.

Інформація про клієнтів. Додається до бази старшим продавцем при здійсненні покупцем покупки. Містить таку інформацію, як історія покупок, номер телефону, електронну адресу, ПІБ та дату народження. Зберігається на сервері компанії, редагується системним адміністратором або директором.

Інформація про постачальників. Містить контактну адресу постачальників та банківські рахунки для оплати замовлень. Замовлення на поставки оформлюються директором. База даних знаходиться на комп'ютері директора, редагується та оновляється директором.

База даних замовлень. Замовлення поступають із сайтів та соціальних мереж, приймаються креативним директором, обробляються старшим продавцем. База даних знаходиться на комп'ютері креативного директора та сервері сайту. Інформація із замовлень додається до бази даних клієнтів.

Інформація про технічне обладнання. Містить в собі дані про охорону систему та інше технічне обладнання. Використовуються охоронною компанією та системним адміністратором.

Накладні на товар. Містять список товарів, їх назву, категорію, кількість та розмірну сітку, ціну та інші деталі. Дані зберігаються на комп'ютері бухгалтера та редагуються бухгалтером. За необхідністю друкується старшим продавцем.

Фінансова звітність. Обробляється бухгалтером та директором, формується з даних про замовлення та закупки. Може зберігатися у паперовому вигляді у бухгалтера.

2.6. Модель порушника

Порушник - це користувач, який здійснює несанкціонований доступ до інформації [4].

Ґрунтуючись на особливостях роботи ІТС, потенційний порушник може бути як внутрішнім, наприклад, співробітники, користувачі системи з різним рівнем доступу до ІзОД, так і зовнішнім, наприклад, конкуренти, покупці, відвідувачі, комунальні служби та хакери.

Для створення моделі порушника необхідно виявити його потенційний мотив та класифікувати його за рівнем кваліфікації, відношенню до ІТС, часом та місцем дії. Для класифікації були використані дані із 2.8 – 2.13.

Всі класифікатори порушника наведено у таблицях, у колонках «Рівень загроз» наведено оцінку загрози, де:

1 - Мінімальний;

2 - Середній;

3 - Високий;

4 - Критичний.

Таблиця 2.8- Категорії порушників, визначених у моделі

Позна-чення	Визначення категорії	Рівень загрози
	Внутрішні по відношенню до ІТС	
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1

Продовження таблиці 2.8

ПВ2	Персонал, який обслуговує технічні засоби ІТС (інженери, техніки)	2
ПВ3	Користувачі (оператори) ІТС	3
ПВ4	Адміністратори ІТС, співробітники служби захисту інформації	4
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	5
	Зовнішні по відношенню до ІТС	
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 конкурнтів або закордонних спецслужб «під прикриттям»	4

Таблиця 2.9 - Специфікація моделі порушника за мотивами порушення

Позна-чення	Мотив порушення	Рівень загрози
М1	Безвідповідальність	1
М2	Корисливий інтерес	2

Таблиця 2.10 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позна-чення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1

Продовження таблиці 2.10

К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 2.11 - Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

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

Таблиця 2.12 - Специфікація моделі порушника за часом дії

Позна-чення	Характеристика можливостей порушника	Рівень загрози

Продовження таблиці 2.12

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

Таблиця 2.13 - Специфікація моделі порушника за місцем дії

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

Таблиця 2.14 - Модель внутрішнього порушника

Посада	Категорія	Мотив	Кваліфікація	Подолання системи захисту	За часом дії	За місцем дії	Сума загроз
Директор	ПВ5	М1	К1	31	Ч4	Д4	16
Креативний директор	ПВ3	М1, М2	К2	31	Ч3	Д2	14
Бухгалтер	ПВ3	М1, М2	К1	31	Ч4	Д3	14

Продовження таблиці 2.14

Системний адміністра-тор	ПВ4	М1, М2	К3	31	Ч4	Д4	23
Старший продавець	ПВ3	М1,М2	К1	31	Ч4	Д2	14
Продавець	ПВ3	М1, М2	К1	31	Ч4	Д2	14
Водій	ПВ3	М1	К1	31	Ч1	Д1	8
Прибиральниця	ПВ1	М1	К1	31	Ч4	Д1	12

З таблиці 2.14 можно побачити, що найбільшу суму загроз (23 б.), що має відношення до проблеми захисту інформації становить системний адміністратор. Тому організація роботи цієї особи повинна бути найбільш контрольованою.

Таблиця 2.15 - Модель зовнішнього порушника

Посада	Категорія порушника	Мотив порушень	Рівень кваліфікації	Можливості за часом дії	Можливості за місцем дії
Покупці, відвідувачі	ПЗ1	М2	К1	Ч3	Д2
Представники організацій, що займаються технічним забезпеченням(комунальні служби)	ПЗ2	М2	К1	Ч3	Д2

Продовження таблиці 2.15

Хакери, злочинці	ПЗ3	М2	К4	Ч3	Д2
Конкуренти	ПЗ4	М2	К2	Ч3	Д2

2.7 Модель загроз

Модель загроз - це абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.[4]

Загрози можуть порушувати конфіденційність, доступність та цілісність інформації, наносити збитки персоналу, клієнтам, технічному обладнанню. Загрози можуть бути випадковими, навмисними та природного характеру, також поділяються на внутрішні та зовнішні.

До випадкових відносяться дії спричинені некомпетентність персоналу, збоїв програмного забезпечення, відказу технічного обладнання.

До навмисних відносяться дії авторизованих в системі працівників, які мають корисливий інтерес, хакерами та конкурентами.

До природних відносяться загрози спричинені стихійними лихами, наприклад, аварії, пожар, потоп та інше.

Таблиця 2.16 – Загрози та можливості реалізація.

Загроза	Реалізація	Джерело
Стихійні явища (пожежа, аварії)	- легкозаймисті матеріали; - несправність комунальних систем; - стара будівля.	Зовнішнє
Відмови системи електроживлення	- неякісна чи стара електропроводка; - відсутність електричних запобіжників.	Внутрішнє

Продовження таблиці 2.16

Пошкодження та втрата носіїв інформації в наслідок стихійних загроз	- відсутність резервного копіювання; - відсутність хмарного сховища.	Зовнішнє
Несанкціоноване підключення до технічних засобів	- недосконаліть охоронної системи.	Зовнішнє
Несанкціоноване підключення до каналів зв'язку	- використання застарілих протоколів захисту Інтернет мереж або відсутність захисту зовсім; - використання слабких паролів; - некомпетентність персоналу та розголошення паролів доступу.	Зовнішнє
Читання даних, на екрані чи залишених без догляду роздрукованих документів	- некомпетентність персоналу; - відсутність політики безпеки «чистого» столу та екрану.	Зовнішнє
Зараження системи комп'ютерними вірусами	- відсутність або недосконаліть антивірусного програмного забезпечення; - несвоєчасне оновлення антивірусного ПЗ; - некомпетентність персоналу.	Внутрішнє

Продовження таблиці 2.16

Пошкодження чи втрата носіїв інформації та інформації на них, що спричинені користувачами	- некомпетентність персоналу.	Внутрішнє
Втрата або розголошення паролів доступу у систему	- некомпетентність персоналу.	Внутрішнє
Несанкціоноване внесення змін у ПЗ та технічні засоби	- некомпетентність персоналу; - відсутність або недосконалість розмежування прав користувачів у системі.	Внутрішнє
Вхід у систему недопущених осіб	- недосконалість охоронної системи; - слабкі паролі; - некомпетентність користувачів.	Внутрішнє, зовнішнє
Порушення цілісності інформації через ненавмисні дії користувачів (наприклад, видалення).	- некомпетентність користувачів; - відсутність резервного копіювання;	Внутрішнє
Навмисне копіювання, порушення конфіденційності або цілісності інформації авторизованим користувачем	- недосконале розмежування доступу; - неправильний підбір персоналу; - відсутність журналу подій.	Внутрішнє

Продовження таблиці 2.16

Соціальна інженерія	- низький рівень знать працівників у сфері інформаційної безпеки.	Зовнішнє , внутрішнє

Таблиця 2.17 - Характеристика ймовірностей реалізації загроз

Оцінка ймовірності	Характеристика
1	Практично неможливе, 1%
2	Низька ймовірність, 25%
3	Середня ймовірність, 50%
4	Висока ймовірність, 75%
5	Критична ймовірність, 99%

Таблиця 2.18 - Характеристика рівнів загроз

Оцінка	Характеристика
Оцінка конфіденційності	
0	Конфіденційність не порушується
1	Конфіденційність порушується
Оцінка доступності	
0	Доступність не порушується
1	Доступність порушується
Оцінка цілісності	
0	Цілісність не порушується
1	Цілісність не порушується
Оцінка спостережливості	
0	Спостережливість не порушується
1	Спостережливість порушується

Рівень загрози у таблиці 2.7.4 визначається:

Рівень загрози = (1К+2Ц+3Д+4С) · ймовірність реалізації загрози.

Таблиця 2.19 - Виявлення рівнів загроз для кожної із загроз.

Загроза	Ймовір-ність	Що порушує				Рівень загроз
		1К	2Д	3Ц	4С	
Стихійні явища (пожежа, аварії)	2	0	1	1	1	6
Відмови системи електроживлення	2	0	0	1	1	4
Пошкодження та втрата носіїв інформації в наслідок стихійних загроз	2	0	1	1	0	4
Несанкціоноване підключення до технічних засобів	2	1	0	0	0	2
Несанкціоноване підключення до каналів зв’язку	2	1	0	0	0	2
Читання даних, на екрані чи залишених без догляду роздрукованих документів	4	1	1	0	0	8
Зараження системи комп’ютерними вірусами	4	1	1	1	1	16

Продовження таблиці 2.19

Пошкодження чи втрата носіїв інформації та інформації на них, що спричинені користувачами	3	0	1	1	0	6
Втрата або розголошення паролів доступу у систему	3	1	1	1	1	12
Несанкціоноване внесення змін у ПЗ та технічні засоби	2	0	1	1	1	6
Вхід у систему недопущених осіб	2	1	1	1	1	8
Порушення цілісності інформації через ненавмисні дії користувачів (наприклад, видалення).	3	0	1	1	0	6
Навмисне копіювання, порушення конфіденційності або цілісності інформації авторизованим користувачем	2	1	1	0	0	4

Продовження таблиці 2.19

Соціальна інженерія	3	1	1	1	0	9

Можна зробити висновок, що найбільшу загрозу становить людський фактор при роботі с ІТС, який може призвести до зараження шкідливим програмним забезпеченням та вірусами, розголошення паролів доступу, неправильне використання обладнання та ПЗ та інше.

Відповідно до НД ТЗІ 2.5-005 -99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». ОІД відноситься 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.

Для АС класу 3 обраний наступний профіль захищеності:

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

КД-2. Базова довірча конфіденційність

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації.

КА-2. Базова адміністративна конфіденційність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління.

КО-1. Повторне використання об'єктів

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу

Критерії не встановлюють, коли саме має виконуватися очищення об'єкта. Залежно від реалізованих механізмів можна виконувати очищення об'єкта під час його звільнення користувачем або безпосередньо перед його наданням наступному користувачу.

КВ-2. Базова конфіденційність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Реалізація даної послуги додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від витоку інформації при підключенні несанкціонованих користувачів

ЦД-1. Мінімальна довірча цілісність

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену.

На даному рівні користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Керування правами має грубу вибірковість (на рівні розподілу потоків інформації між групами користувачів). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів.

ЦА-2. Базова адміністративна цілісність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ЦО-1. Обмежений відкат

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат. Якщо система реалізує дану послугу, то її використання має фіксуватись в журналі.

ЦВ-2. Базова цілісність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування

Реалізація даної послуги на рівні ЦВ-2 додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від модифікації інформації у разі підключенні несанкціонованих користувачів.

ДР-2. Квоти

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Квоти використовуються таким чином, щоб гарантувати, що жоден користувач не зможе захопити решту певного ресурсу, дозволяючи виділяти менші обсяги ресурсів, ніж максимальна квота користувача, гарантуючи таким чином іншому користувачеві доступ до розділюваного ресурсу.

ДВ-1. Ручне відновлення

Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Відновлення може вимагати втручання оператора, а для її більш високих рівнів реалізації КЗЗ може

продукувати відновлення працездатності автоматично. Якщо відновлення неможливе, то КЗЗ повинен переводити систему до стану, з якого її може повернути до нормального функціонування тільки адміністратор.

НР-2. Захищений журнал

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень. Реєстрація — це процес розпізнавання, фіксування і аналізу дій і подій, що пов'язані з дотриманням політики безпеки інформації. Використання засобів перегляду і аналізу журналів має бути прерогативою спеціально авторизованих користувачів

НИ-2. Одиночна ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС.. Для підвищення ефективності захисту від специфічних загроз несанкціонованого доступу для найбільш високого рівня даної послуги (НИ-3) вимагається використання комбінації мінімум двох різних типів автентифікації, наприклад, введеного з клавіатури пароля і носимого ідентифікатора.

НК-1. Однонаправлений достовірний канал

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

НО-2. Розподіл обов'язків адміністраторів

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Система, що претендує на включення даної послуги до рейтингу, повинна передусім забезпечувати існування ролей для адміністратора і звичайного користувача (рівень НО-1).

НЦ-2. КЗЗ з гарантованою цілісністю

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами. Для рівня НЦ-2 необхідно, щоб КЗЗ підтримував власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе від зовнішніх впливів. Дана вимога є однією з вимог до реалізації диспетчера доступу.

НТ-2. Самотестування при старті

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ранжируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

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. Рівні даної послуги ранжируються на підставі повноти реалізації.

2.8. Розробка політики безпеки

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 проводити навчання персоналу для підвищення їх обізнаності в сфері інформаційної безпеки;

- регулярно оновляти операційну систему та програмне забезпечення;

- відстежувати ризики та загрози безпеки інформації та вживати дії;

- регулярно проводити технічну діагности обладнання;

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

2.8.1 Політика безпеки використання мережі Інтернет

Опис:

Інтернет став невід'ємною частиною робочого процесу, а також великою загрозою інформаційної безпеки, тому є велика необхідність впровадження правил та інструкцій під час його використання.

Мета політики:

Збільшити рівень інформаційної безпеки підприємства за рахунок введення інструкцій та правил використання мережі 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 системний адміністратор.

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;

- дійснювати 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 штрафні санкції та дисциплінарні міри.

Періодичність та порядок перегляду політики:

Політика безпеки повинна переглядатися щороку директором та системним адміністратором. Але у разі виникнення необхідності можуть бути внесені корективи раніше вказаного терміну

2.8.2. Політика «чистого стола» та «чистого екрану»

Опис:

Політика дає рекомендація для робітників у якому вигляді вони зобов'язані залишати свої робочі місця протягом та вкінці робочого дня.

Мета політики:

Мінімізації ризику неавторизованого доступу або пошкодження документів на паперових носіях, носіїв даних і засобів обробки інформації.

Область дії:

Політика поширюється на всіх працівників компанії.

Відповідальні особи:

За виконання політики безпеки співробітниками відповідальним назначається системний адміністратор та директор.

Інструкція політики:

- застосовувати паролі для входу у систему;

- персональні комп'ютери та принтери повинні бути виключені по закінченню роботи;

- персональні комп'ютери повинні бути заблоковані, якщо протягом деякого часу їх не збираються використовувати;

- паролі та ключі заборонено записувати, залишати на робочому місці, або ховати десь поблизу нього, наприклад під комп'ютером;.

- інформація з обмеженим доступом повинна бути схована у сейф чи шухляду із замком після її використання;

- надруковані документи з важливою або конфіденційної інформацією необхідно вилучати з принтерів.

Відповідальність:

У разі порушення політики працівником будуть застосовані штрафні санкції та дисциплінарні міри відповідно до внутрішніх нормативних документів підприємства.

Періодичність та порядок перегляду політики:

Політика безпеки повинна переглядатися щороку директором та системним адміністратором. Але у разі виникнення необхідності можуть бути внесені корективи раніше вказаного терміну.

2.8.3. Політика безпеки використання електронної пошти

Опис:

Найпоширенішім методом передачі інформації в межах однієї організації виступає електронна пошта, неправильне використання якої може привести до зараження системи вірусами, втрати інформації і зупинки

роботи. Дана політика дає рекомендації та інструкції використання електронної пошти.

Мета політики:

Політика спрямована на мінімізацію загроз інформаційної безпеки під час використання електронної пошти співробітниками для виконання їх посадових обов'язків .

Області дії:

Політика поширюється на всіх працівників компанії, які використовують електрону пошту.

Відповідальні особи:

За виконання політики безпеки співробітниками відповідальним назначається системний адміністратор та директор

Інструкція політики:

- приймати та обробляти письма можна коли відправник є надійним джерелом.

- функція автоматичного завантаження додатків повинна бути виключена

- перед запуском і відкриттям файлів з електронної пошти файли повинні бути просканованні антивірусом.

- при роботі з електронною поштою потрібно використовувати обліковий запис з обмеженими можливостями у системі.

- використання електронної пошти не повинно порушувати закони України та внутрішні нормативні правила компанії.

- при виявленні несправностей, пов’язаних з роботою пошти, необхідно терміново зв’язатися з відповідальними особами.

Відповідальність:

У разі порушення політики працівником будуть застосовані штрафні санкції та дисциплінарні міри відповідно до внутрішніх нормативних документів підприємства.

Періодичність та порядок перегляду:

Політика безпеки повинна переглядатися щороку директором та системним адміністратором. Але у разі виникнення необхідності може бути переглянута раніше вказаного терміну.

2.8.4. Політика безпеки використання антивірусного захисту

Опис:

Дана політика дає рекомендації та інструкції по використанню антивірусних програм і перевірки технічних систем на наявність шкідливого ПЗ.

Мета політики:

Збільшити рівень захищеності ІТС за рахунок використання антивірусних програм

Область дії:

Політика поширюється на всіх працівників компанії, які використовують мають доступ до мережі Інтернет та використовують комп'ютери .

Відповідальні особи:

За виконання політики співробітниками відповідальним назначається системний адміністратор.

Інструкція політики:

- на кожному комп'ютері повинен бути встановлені та налагодженні антивірусні засоби;

- дозволяється використовувати лише ліцензійне антивірусне програмне забезпечення, рекомендоване системним адміністратором;

- встановленням і налаштуванням засобів антивірусного ПЗ займається системний адміністратор;

- антивірусне ПЗ повинно регулярно оновлюватися згідно з виходом оновлень;

- всі файли скачані та отримані із мережі Інтернет перед відкриттям повинні діагностуватися антивірусом;

- системний адміністратор повинен регулярно проводити виморочну повну перевірку комп’ютерів;

- у разі виникнення проблем з антивірусним ПЗ користувачі повинні негайно сповістити системного адміністратора.

Відповідальність:

Відповідальність за виконання інструкцій антивірусного захисту покладається на всіх робітників.

Відповідальність за проведення профілактичних заходів та перевірки системи антивірусним ПЗ покладається на системного адміністратора.

У разі порушення політики можуть бути застосовані штрафні санкції та дисциплінарні міри відповідно до внутрішніх нормативних документів підприємства.

Періодичність та порядок перегляду політики:

Політика безпеки повинна переглядатися щороку директором та системним адміністратором. Але у разі виникнення необхідності можуть бути внесені корективи раніше вказаного терміну.

2.9 Висновки

У другому розділі було проведене повне обстеження ОІД, при обстеженні було виявлено:

- КЗ знаходиться на другому поверсі ОІД;

- обчислювана система включає в себе 4 комп'ютера та підключення до мережі Інтернет від WI-FI роутера;

- підприємство користується послугами охоронної компанії та має надійну охоронну систему;

- підприємство має у своєму штабі адміністратора ІСТ;

- на ОІД циркулює відкрита інформація та конфіденційна інформація з обмеженим доступом;

- обстеження інформаційного середовища показало, що на ОІД є така інформація - бази даних співробітників, клієнтів, постачальників, накладні на товар, фінансові операції; власником інформації виступає директор.

- модель порушника показала, що найбільшу потенційну загрозу становить системний адміністратор;

- модель загроз показала, що найбільшу загрозу в собі несе зараження вірусними програмами та недбалість користувачів.

Для запобігання реалізації загроз було розроблено 4 політики безпеки:

- політика безпеки використання мережі Інтернет;
- політика використання антивірусного програмного забезпечення;
- політика використання електронної пошти;
- політика «чистого» столу.

3 ЕКОНОМІЧНА ЧАСТИНА

Метою виконання економічного розділу кваліфікаційної роботи є техніко-економічне обґрунтування доцільності запровадження політики безпеки підприємства «Книш О. А.».

3.1 Визначення витрат на розробку політики безпеки

Трудомісткість розробки політики безпеки визначається тривалістю кожної робочої операції:

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

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

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

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

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

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

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

$t_{д}$ – тривалість документального оформлення політики безпеки.

Згідно формули (3.1) трудомісткість розробки політики безпеки дорівнює:

$$t = 3 + 3 + 5 + 4 + 4 + 2 + 5 = 26 \text{ год.}$$

Розрахунок витрат на створення політики безпеки:

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

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

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

$З_{мч}$ – вартість витрат машинного часу, що необхідні для створення політики безпеки.

Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою:

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

де t – загальна тривалість розробки політики безпеки, годин;

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

Середньогодинна заробітна плата спеціаліста з інформаційної безпеки становить – 125 грн./год.

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

$$З_{зп} = 26 \text{ год} \cdot 125 \text{ грн} = 3250 \text{ грн.}$$

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 політики безпеки інформації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

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

$$С_{мч} = 0{,}22 \cdot 1 \cdot 1{,}68 + \frac{10000 \cdot 0{,}54}{1920} + \frac{1192{,}40 \cdot 0{,}54}{1920} = 3{,}49 \text{ грн.}$$

де Р – встановлена потужність ПК, 0,44кВт;

$t_{нал}$ – кількість машин на яких розроблюється політика безпеки, 1 машина;

$С_е$ – тариф на електричну енергію, 1,68грн/кВ·год;

$Ф_{зал}$– поточна вартість ПК на початок року, 10000 грн.;

$Н_а$ – річна норма амортизації на ПК, 0,54 частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення,частки одиниці, 0.54 частки одиниці;

$К_{лпз}$– вартість ліцензійного програмного забезпечення, 1192,40грн.;

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

Згідно формули (3.4) вартість 1 години машинного часу ПК дорівнює:

$$З_{мч} = t \cdot С_{мч} = 26 \cdot 3{,}49 = 90{,}74 \text{ грн.}$$

Згідно формули (3.2) витрати на розробку ПБ становлять:

$$К_{рп} = З_{зп} + З_{мч} = 3250 + 90{,}74 = 3340{,}74 \text{ грн.}$$

3.2 Розрахунок (фіксованих) капітальних витрат

Таблиця 3.1 - Перелік придбаного ліцензійного ПЗ

№	Назва	Кількість	Вартість, грн
	Eset NOD32 antivirus	4	1192,40
Всього:			1192,40

Капітальні (фіксовані) витрати на впровадження системи інформаційної безпеки складаються за формулою:

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

$$К = 1192{,}40 + 3340{,}74 + 1500 = 6032{,}74 \text{ грн.}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, стороння організація не наймалась, тому не враховується.

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 1192,40грн.;

$К_{аз}$ – вартість закупівель апаратного забезпечення та допоміжних матеріалів, тис.грн, апаратне забезпечення не куплялось, тому не враховується;

$К_{рп}$ – вартість розробки політики безпеки інформації, 3340,74грн ;

$К_{навч}$ - витрати на навчання технічних фахівців і обслуговуючого персоналу, витрати на навчання системного адміністратора 1500грн.

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, нове апаратне обладнання не купувалося, не враховується оскільки апаратне забезпечення (згідно $К_{аз}$) не куплялося.

3.3 Розрахунок експлуатаційних витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

$$С = С_в + С_к + С_{ак}, \text{ тис. грн.,} \quad (3.7)$$

де $С_в$ - витрати на upgrade-відновлення й модернізацію системи ІБ, вартість програмного забезпечення - 1192,40грн.;

$С_к$ – витрати на керування системою ІБ, грн.;

$С_{ак}$ – витрати викликані активність користувачів:

- пряма допомога й додаткові настроювання – 500грн;
- формальне навчання – 500грн;
- розробка додатків – 500грн;
- робота з даними – 500грн;
- неформальне навчання – 500грн;
- futz-фактор(витрати пов’язані з наслідками некомпетентності користувачів) – 1000грн.

Витрати на керування системою ІБ складають:

$$С = С_н + С_а + С_з + С_{єв} + С_е + С_{ел} + С_о + С_{тос}\text{грн.,} \quad (3.8)$$

де $С_н$ - витрати на навчання адміністративного персоналу й кінцевих користувачів,курсів підвищення кваліфікації, 1500 грн.;

$С_а$- річний фонд амортизаційних відрахувань, визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних

активів(ПЗ); Вартість купівлі ліцензійного ПЗ - 1192,40 грн., мінімальний срок дії користування – 2 роки.

$$С_а = \frac{1192,40}{2} = 596,2 \text{ грн.}$$

$С_з$- річний фонд заробітної плати інженерно-технічного персоналу, 84000 грн/рік ;

$$С_з = С_{осн} + С_{дод}, \text{ грн.,} \quad (3.9)$$

де $С_{осн}, С_{дод}$ – основна і додаткова заробітна плата, грн. на рік.

Додаткова заробітна плата це 8-10% від основної заробітної плати.

Основна заробітна плата системного адміністратора складає 7000 грн. на місяць, тож маємо 84000 грн. на рік.

Додаткова заробітна плата начисляється у розмірі 8% від основної.

$$С_{дод} = 84000 \cdot 8\% = 6720 \text{ грн.,}$$

$$С_з = 84000 + 6720 = 90720 \text{ грн.}$$

$С_{ел}$ – вартість електроенергії, що споживаються апаратурою інформаційної безпеки протягом року, визначається за формулою:

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

Р – встановлена потужність апаратури інформаційної безпеки, 0,22кВт середня потужність одного комп'ютера;

$$Р = 0,22 \text{ кВт} \cdot 4 \text{ компютера} = 0,88 \text{ кВт.}$$

$F_р$ – річний фонд робочого часу системи інформаційної безпеки, ОІД працює кожен день с 10:00 до 20:00, 10 годин на добу;

$$F_р = 365 \text{ днів} \cdot 10 \text{ годин} \cdot 4 \text{ компютера} = 14600 \text{ год.}$$

$Ц_е$ – тариф на електроенергію, 1,68грн/кВт·год.

$$С_{ел} = 0,88 \cdot 14600 \cdot 1,68 = 21584,64 \text{ грн.}$$

$С_о$ – втрати на залучення сторонніх організацій для виконання деяких видів обслуговування. (Сторонні організації не були залучені).

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс систем інформаційної безпеки, визначаються за даними організації або у відсотках від вартості капітальних витрат (1-3%).

$$К=6032,74 \text{ грн.},$$

$$С_{тос} = 6032,74 \cdot 1\% = 60,32 \text{грн.}$$

Отже, витрати на керування системою інформаційної безпеки складають:

$$С_к = 1500 + 596,2 + 90720 + 21584,64 + 60,32 = 114461,16 \text{ грн.},$$

$$С = 1192,40 + 114461,16 + 3000 = 118653,56 \text{ грн.}$$

3.4 Оцінка можливого збитку від атаки на вузол або сегмент корпоративної мережі

Таблиця 3.2 - Заробітна плата працівників

Посада	Кількість працівників	Заробітна плата в місяць, грн.	Заробітна плата помножена на кількість працівників, грн.
Директор	1	20000	20000
Креативний директор	1	11000	11000
Системний адміністратор	1	7000	7000
Бухгалтер	1	11000	11000
Старший продавець	1	9000	9000
Продавець	3	8000	24000

Продовження таблиці 3.2

Водій	1	6000	6000
Прибиральниця	1	3000	3000
Всього:		75000	91000

Місячний фонд робочого часу складає 300 годин. Річний – 3600 годин. Час простою внаслідок атаки 4 години:

Упущена вигода від простою атакованого вузла або сегмента мережі становить:

$$U = П_п + П_в + V, \quad (3.11)$$

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

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

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

Втрати від зниження продуктивності співробітників являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

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

де F – місячний фонд робочого часу (при 70 годинному робочому тижні становить 300 годин);

Зс – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 91000 грн./місяць;

$t_п$– час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин, 5 години ;

$$П_п = \frac{91000}{300} \cdot 5 = 1516{,}66 \text{грн.}$$

Втрати на відновлення працездатності вузла:

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

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

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

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

Витрати на повторне уведення інформації розраховуються за формулою:

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

де F – місячний фонд робочого часу (при 70 годинному робочому тижні становить 300 годин);

Зс – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 91000 грн./місяць;

$t_{ви}$– час повторного введення загубленої інформації співробітниками атакованого вузла, 6 годин.

$$П_{ви} = \frac{91000}{300} \cdot 6 = 1820 грн.$$

Витрати на відновлення вузла або сегмента корпоративних мережі $П_{пв}$ визначаються:

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_{в}\ , \qquad (3.15)$$

де F – місячний фонд робочого часу (при 70 годинному робочому тижні становить 300 годин);

Зо – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн. на місяць, 7000грн;

$t_{в}$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 5 години.

$$П_{пв} = \frac{7000}{300} \cdot 5 = 116{,}66 \text{ грн.},$$

$$П_{в} = 1820+116{,}66 +3000=4936{,}66 \text{ грн.}$$

$П_{зч}$ – вартість заміни устаткування або запасних частин, 3000грн.

Витрати від зниження очікуваного обсягу продажів а час просто:

$$V = \frac{O}{Fr} \cdot (t_{п} + t_{в} + t_{ви})\ , \qquad (3.16)$$

де Fr – річний фонд робочого часу (при 70 годинному робочому тижні становить 3600 годин у рік);

О – обсяг продажів атакованого вузла, 1900000 грн. у рік.

$$V = \frac{1900000}{3600} \cdot (5 + 6 + 5) = 8444{,}44 \text{грн.}$$

Упущена вигода від простою атакованого вузла або сегмента мережі становить:

$$U = 1516{,}66 + 4936{,}66 + 8444{,}44 = 14897{,}76 \text{ грн.}$$

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

$$U = \sum i \sum n\, U, \tag{3.17}$$

де I – число атакованих вузлів, 4 комп'ютера;

N – середнє число атак на рік, 3 рази.

$$U = 14897{,}76 \cdot 4 \cdot 3 = 178773{,}12 \text{ грн.}$$

3.5 Визначення та аналіз показників економічної ефективності

Загальний ефект від впровадження системи інформаційної безпеки розраховується за формулою:

$$\text{E} = \text{B} \cdot R - C, \tag{3.18}$$

де B – Загальний збиток від атаки на вузол корпоративної мережі, грн.;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

$$\text{E} = 178773{,}12 \cdot 0{,}75 - 118653{,}56 = 15426{,}84.$$

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки.

Оцінка економічної ефективності системи захисту інформації здійснюється на основі визначення та аналізу наступних показників:

– сукупна вартість володіння (ТСО);

– коефіцієнт повернення інвестицій ROSI (Return on Investment for Security);

– термін окупності капітальних інвестицій То.

$$ROSI = \frac{E}{К}, \tag{3.19}$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, 15426,84грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, 6032,74грн.

$$ROSI = \frac{15426,84}{6032,74} = 2,55.$$

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

$$Т_о = \frac{К}{Е} = \frac{1}{ROSI}, \text{ років.}, \tag{3.20}$$

$$Т_о = \frac{6032,74}{15426,84} = 0,39 \text{ року (5 місяців).}$$

3.6 Висновки

- Капітальні витрати на впровадження інформаційної політики безпеки складають - 6032,74 грн.;

- Експлуатаційні витрати на впровадження інформаційної політики безпеки складають -118653,56 грн.;

- Можливий збиток від атаки на вузол складає - 178773,12 грн.;

- Загальний ефект від впровадження системи інформаційної безпеки складає - 103773,48грн;

- Термін окупності капітальних інвестицій - 5 місяців.

Тому економічна доцільність впровадження політики інформаційної безпеки обґрунтована і може піти на користь підприємству.

ВИСНОВКИ

Кожного року кількість кібератак зростає, у 2020 році зареєстрованих випадків було на 54% більше ніж попереднього року, відповідно зростає і актуальність питання захисту інформації.

У другому розділі були обстежені фізичні особливості розташування ОІД, середовище користувачів, методи обробки інформації, середовище обчислювальної системи, виявлена модель порушника та загроз.

Із розділів «модель порушника» та «модель загрози» можна дійти висновку, що найбільшу загрозу для ІТС становить не особливості самої ІТС, а дії користувачів, які можуть мати навмисний або ненавмисний характер, наприклад втрата носіїв інформації, розкриття конфіденційної інформації, зараження комп'ютерними вірусами та троянами, використання комп'ютерів не за призначенням. Саме тому виникає необхідність розробки та впровадження політики безпеки, яка буде виступати інструкцією як для користувачів, так і адміністраторів ІТС.

Оскільки найпоширенішим методом зараження комп'ютерними вірусами у 2020 році була електронна пошта, тому була виявлена необхідність розробки політики безпеки використання електронної пошти та антивірусного захисту.

А також беручи до уваги те, що ОІД це магазин, у якому за день можуть бути сотні відвідувачів, з'являється необхідність впровадження політики «чистого» столу та екрану, що представляє собою інструкції про те, як користувачі повинні залишати комп'ютери та друковану інформацію, якщо вони тимчасово їх не використовують.

Із економічного розділу можна зробити висновок, що потенційні збитки від атаки перевищують витрати на розробку політики безпеки, капітальні витрати на покупку ліцензійного програмного забезпечення, а також підтримку роботи політики безпеки протягом року, а термін окупності становить приблизно 5 місяців.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про інформацію». [Чинний, редакція від 16.07.2020]. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». [Чинний, редакція від 04.07.2020] URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

3. Наказ «Про затвердження нормативного документа системи технічного захисту інформації НД ТЗІ 1.6-005-2013» [Прийняття від 15.04.2013] URL: https://zakon.rada.gov.ua/rada/show/v0215519-13#Text

4. Нормативний документ системи технічного захисту інформації «Термінології в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 1.1-003-99». URL: https://tzi.com.ua/downloads/1.1-003-99.pdf

5. Нормативний документ системи технічного захисту інформації «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003 - 2005». URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf

6. Нормативний документ системи технічного захисту інформації «Типове положення про службу захисту інформації в автоматизованій системі». URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf

7. Змістовий модуль 1. Формування вимог до КСЗІ та її завдань. Тема 5. Модель порушника безпеки інформації в ІТС. URL: https://studfile.net/preview/9649925/page:4/

8. Постанова «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [від 29 березня 2006 р. N 373 Київ]. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text

9. Нормативний документ системи технічного захисту інформації «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу НД ТЗІ 2.5-005 -99». URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-005--99.pdf

10. Нормативний документ системи технічного захисту інформації «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99». URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf

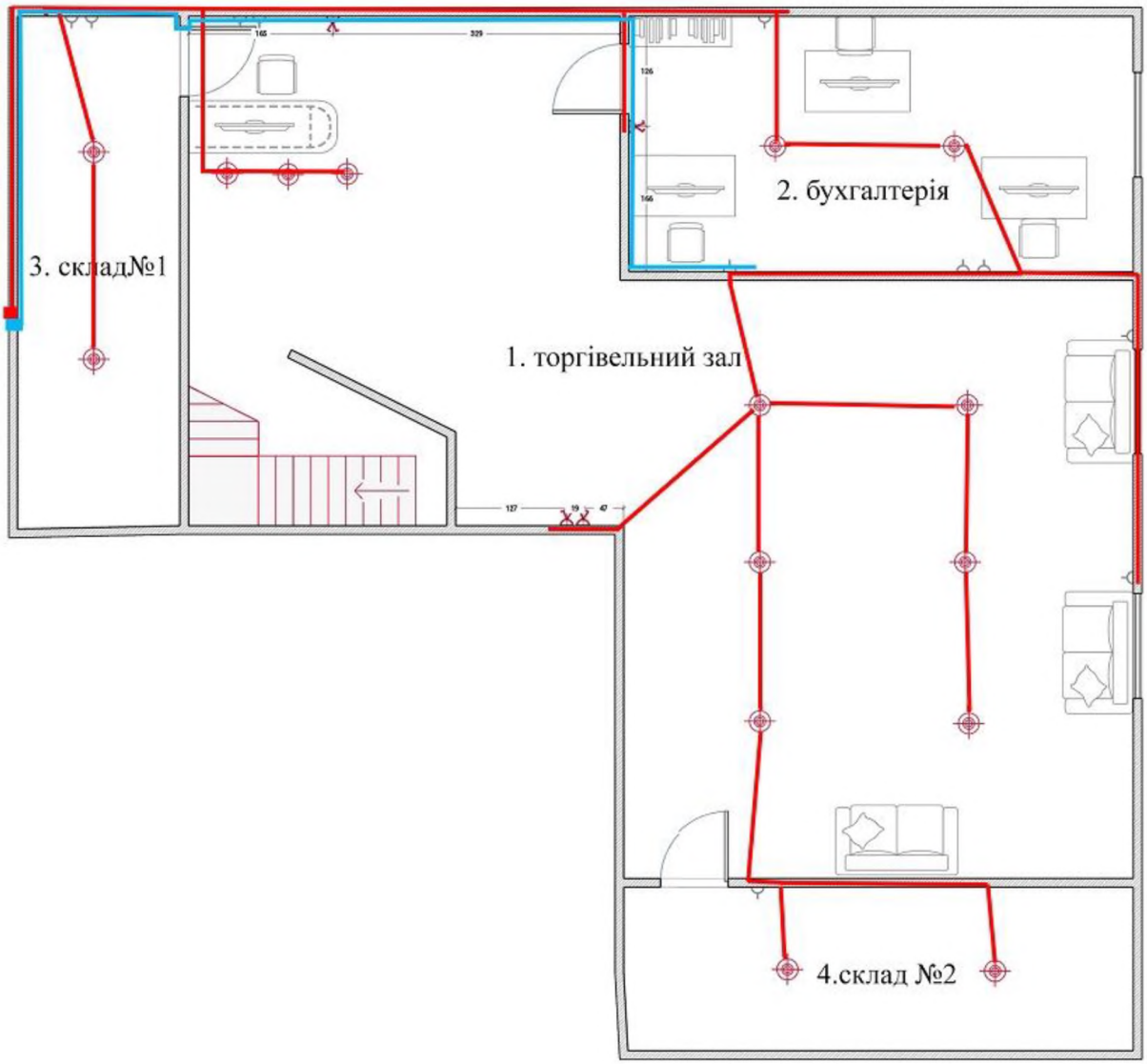
11. Статистика кіберзлочинів за 2020 рік. Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/

12. 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. URL: https://bit.nmu.org.ua/ua/student/diplom/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4_%D0%9A%D0%A0%D0%91_125_2020.pdf

ДОДАТОК А. Відомості матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	11	
6	А4	Спеціальна частина	41	
7	А4	Економічна частина	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	
13	А4	Додаток Д	1	
14	А4	Додаток Е	1	

ДОДАТОК Б. Розташування ліній електромережі та Інтернет



УМОВНІ ПОЗНАЧЕННЯ:

- вікно
- двері
- освітлення
- лінії електропостачання
- вихід ліній електропостачання за межі ОІД
- персональний комп'ютер
- Wi-Fi маршрутизатор
- перемикач світла
- розетка
- лінії інтернет кабелю
- вихід лінії інтернет кабелю за межі ОІД

Рисунок Б.1 - Лінії електромережі та кабелю Інтернет

ДОДАТОК В. Розташування охоронної системи

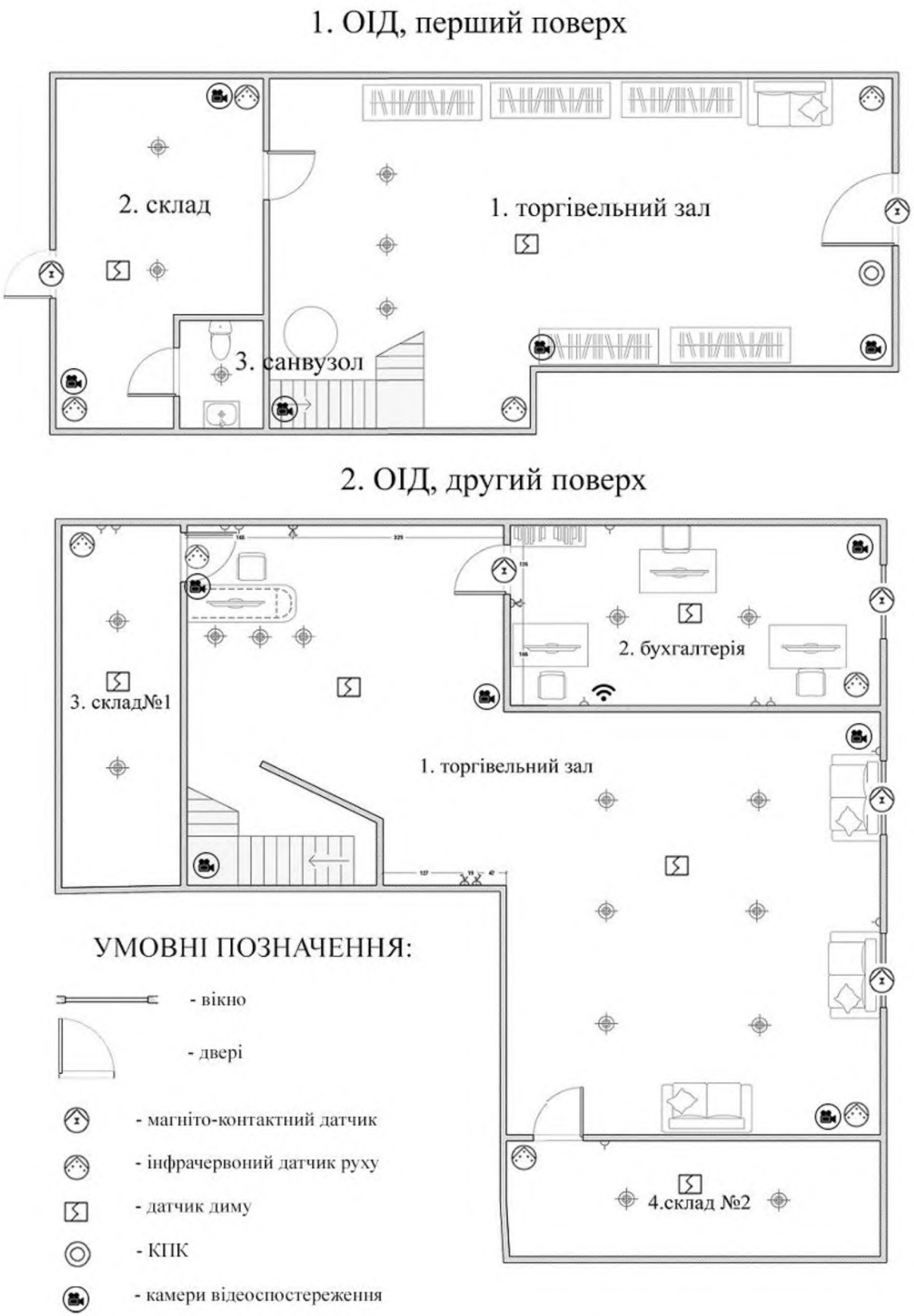


Рисунок В.1 - Датчики охоронної системи

ДОДАТОК Г. Перелік документів на оптичному носії

1 Пояснювальна записка.docx

2 Пояснювальна записка.pdf

3 Презентація.pptx

ДОДАТОК Д. Відгук керівника економічного розділу

Керівник економічного розділу к.е.н.,доц..Пілова Д. П.

Дата: _____ Підпис_____

ДОДАТОК Е. Відгук керівника кваліфікаційної роботи

ВІДГУК

На кваліфікаційну роботу студентки групи 125-17-2

Хмари Милени Володимирівни

На тему: «Політика безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства «Книш О. А.»

Пояснювальна записка складається із вступу, трьох розділів і висновків, викладених на 76 сторінках.

Метою кваліфікаційної роботи є підвищення рівня захищеності інформації в ІТС приватного підприємства «Книш О. А.».

Тема кваліфікаційної роботи безпосередньо відноситься до діяльності бакалавра спеціальності 125 «Кібербезпека».

Для досягнення поставленої мети у кваліфікаційній роботі проводиться: аналіз нормативно-правової бази у сфері інформаційної безпеки, стану питання; обстеження фізичного середовища, обчислюваної системи, середовища користувачів; розробка моделі порушника та загроз.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня захищеності інформації на об’єкті інформаційної діяльності, за рахунок аналізу слабких місць та розробки політики безпеки.

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

За період дипломування Хмара М. В. проявила себе як фахівець, здатний самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи **Горєв В. М.**

Керівник спец. розділу **Саксонов Г.М.**