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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Ангеловський Микола Олексійович*
академічної групи *125-17-1*
спеціальності *125 Кібербезпека*
спеціалізації[1]
за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи приватного підприємства ТОВ «BeerWineShop»*

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

Рецензент				

Нормоконтролер	ст.викл. Тимофєєв Д.С.			

Дніпро

2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В. І.
«_____»_____ 20 ___ року

ЗАВДАННЯ
На кваліфікаційну роботу ступеня бакалавра

студенту ***Ангеловський Микола Олексійович*** **академічної групи** ***125-17-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***
спеціалізації[1] _____
за освітньо-професійною програмою ***Кібербезпека***

на тему ***Комплексна система захисту інформації інформаційно-телекомунікаційної системи приватного підприємства ТОВ «BeerWineShop»***

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

Розділ	Зміст	Термін виконання
Розділ 1	Актуальність питання захисту інформації в ІТС, аналіз нормативно-правової бази в сфері захисту інформації, підстави для створення КСЗІ.	29.03.2021
Розділ 2	Обстеження фізичного середовища ІТС, обстеження обчислювальної системи, обстеження інформаційного середовища, аналіз загроз та вразливостей, вибір профілю захищеності.	03.05.2021
Розділ 3	Економічна доцільність використання розробленої КСЗІ, економічна ефективність впровадження її елементів в ІТС на ОІД	04.06.2021

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

Дата видачі завдання: 08.01.2021р.

Дата подання до екзаменаційної комісії: 09.06.2021р.

Прийнято до виконання _____ Ангеловський М.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 105 с., 3 рис., 23 табл., 12 додатків, 14 джерел.

Об’єкт дослідження: інформаційна-телекомунікаційна система ТОВ «BeerWineShop».

Мета кваліфікаційної роботи: підвищення рівня захисту інформації в ІТС ТОВ «BeerWineShop».

Методи розробки: спостереження, аналіз, порівняння, опис.

У першому розділі розглянуто питання актуальності впровадження КСЗІ в інформаційно-телекомунікаційну систему приватного підприємства, наведено аналіз нормативно-правової бази в сфері захисту інформації, проаналізований процес обстеження середовища функціонування ІТС, розглянута модель загроз та модель порушника, виконано постановку задачі.

У спеціальній частині наведені загальні відомості про ОІД. Було виконано обстеження фізичного середовища та обчислювального середовища ІТС, проаналізовано технологію обробки інформації, проаналізовані загрози та вразливості, розроблена модель порушника, обрано профіль захищеності, виконано етап розробки КСЗІ та політики безпеки.

В економічному розділі обґрунтована доцільність витрат на розробку КСЗІ, а також проведені розрахунки капітальних та експлуатаційних витрат, оцінено величину можливого збитку від атаки та визначено ефект від впровадження КСЗІ в інформаційну безпеку.

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

РЕФЕРАТ

Пояснительная записка: 105 с., 3 рис., 23 табл., 12 прилож., 14 источников.

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

Цель квалификационной работы: повышение уровня защиты информации в ИТС ООО «BeerWineShop».

Методы, используемые при разработке: наблюдение, анализ, сравнение, описание.

В первом разделе рассмотрены вопросы актуальности внедрения КСЗИ в информационно-телекоммуникационную систему частного предприятия, приведен анализ нормативно-правовой базы в сфере защиты информации, проанализированный процесс обследования среды функционирования ИТС, рассмотрена модель угроз и модель нарушителя, выполнена постановка задачи.

В специальной части приведены общие сведения про ОИД. Было выполнено обследование физической среды и вычислительной среды ИТС, проанализирована технология обработки информации, проанализированы угрозы и уязвимости, разработана модель нарушителя, выбран профиль защищенности, выполнен этап разработки КСЗИ и политики безопасности.

В экономическом разделе обоснована целесообразность затрат на разработку КСЗИ, а также проведены расчеты капитальных и эксплуатационных расходов, оценено величину возможного ущерба от атаки и определен эффект от внедрения КСЗИ в информационную безопасность.

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

ABSTRACT

Explanatory note: 105 p., 3 figures, 23 tables, 12 supplements, 14 sources.

Object of study: information and telecommunication system of «BeerWineShop» LLC.

The purpose of the qualification work: increasing the level of information protection in the ITS of «BeerWineShop» LLC.

Methods that were used: observation, analysis, comparison, description.

The first part of the study examines the relevance of the introduction of CIPS in the information and telecommunications system of a private enterprise, provides an analysis of the regulatory framework in the field of information protection, analyzed the process of examining the environment for the functioning of ITS, considered a threat model and a model of an intruder, and completed the formulation of the problem.

The main part of the study provides general information about OIA. A survey of the physical environment and the computing environment of the ITS was carried out, the information processing technology was analyzed, threats and vulnerabilities were analyzed, a model of the intruder was developed, a security profile was selected, the stage of development of the CIPS and security policy was completed.

In the economic part substantiates the feasibility of costs for the development of the CSIS, as well as calculations of capital and operating costs, estimates the amount of possible damage from an attack and determines the effect of introducing CIPS into information security.

INFORMATION AND TELECOMMUNICATION SYSTEM, INFORMATION SECURITY, OBJECT OF INFORMATION ACTIVITY, MODEL OF THREATS, COMPREHENSIVE INFORMATION PROTECTION SYSTEM.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

БД – база даних;

ДТЗС – допоміжні технічні засоби і системи;

ЖМД – жорсткий магнітний диск;

ЗУ – Закон України;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІС – інформаційна система;

ІТ – інформаційні технології;

ІТС – інформаційно-телекомунікаційна система;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КПП – контрольно пропускній пункт;

КСЗІ – комплексна система захисту інформації;

КСІБ – комп’ютерна система інформаційної безпеки;

НД ТЗІ – нормативний документ в галузі технічний захист інформації.

НСД – несанкціонований доступ;

ОЗУ – оперативний запам'ятовуючий пристрій;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ОТЗ – основні технічні засоби;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ПІБ – прізвище, ім'я, по батькові;

ПК – персональний комп'ютер;

ПО ДФ ПАТ – профспілкова організація дніпропетровської філії публічне акціонерне товариство;

ППКОП – прилад приймально – контрольний охоронно – пожежний;

СКУД – система контролю та управління доступом;

ТОВ – товариство з обмеженою відповідальністю;

ТП – трансформаторна підстанція;

ТТ – торгівельна точка;

ФОП – фізична особа підприємець;

CIPS – comprehensive information protection system;

HDD – hard disk drive;

ITS – information and telecommunication system

LLC – limited liability company;

OIA – object of information activity;

USB – universal serial bus.

ЗМІСТ

ВСТУП

Значним кроком суспільства, що охопив більшість сфер діяльності, такі, як економічна, науково-технічна, сфера культури та освіти, став крок до глобальної інформаційної революції, у рамках якої відбувалося стрімке входження суспільства в інформаційний етап його розвитку – інформатизацію.

Інформатизація сприяє задоволенню інформаційних потреб громадян та суспільства на основі використання інформаційних систем, мереж, ресурсів та інформаційних технологій, основою для побудови яких є сучасна обчислювальна та комунікаційна техніка.

В сучасному світі в кожній інформаційній системі циркулює така інформація, розголошення якої стороннім особам може призвести до значних збитків власнику інформації або навіть припинення функціонування великих підприємств, яким належить ця інформація.

На сьогоднішній день питання, щодо створення комплексної системи захисту інформації на підприємствах та організаціях є особливо актуальним.

З розвитком комерційної та підприємницької діяльності збільшилися спроби несанкціонованого доступу до інформації з обмеженим доступом, що викликало значну потребу у фахівцях з інформаційної безпеки.

Для забезпечення інформаційної безпеки на підприємстві, створюється комплексна система захисту інформації, яка спрямована на забезпечення захисту інформації від розголошення, витоку та НСД.

У роботі було частково змінено інформацію про підприємство на вимогу власника з метою збереження конфіденційності.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

В час, в який ми живемо, питання захисту інформації в ІТС набуло дуже важливого значення. В кожній ІС циркулює така інформація, розголошення якої стороннім особам може призвести до значних збитків власнику інформації або навіть припинення функціонування великого підприємства, до якого належить ця інформація.

Для прикладу можна привести масштабну атаку вірусом «Petya», яким було уражено багато великих компаній, такі як: українські банки, енергетичні компанії, урядові сайти, аеропорти тощо. Такого масштабного вторгнення в сервери компаній наша країна ще не зазнавала. Сума економічних збитків сягала близько 850 млн доларів.

На сьогоднішній день, фахівці у сфері ІТ зазначають, що ситуація з кіберзлочинністю у світі тільки погіршується.

Через зростання рівня інформаційної злочинності, багато підприємств вимушені витрачати чимало грошей на забезпечення ІБ.

Для забезпечення ІБ на підприємстві, створюється КСЗІ, яка спрямована на забезпечення захисту інформації від розголошення, витоку та НСД.

Метою даної кваліфікаційної роботи є обстеження підприємства ТОВ «BeerWineShop», виявлення загроз та вразливостей в ІТС, розробка КСЗІ та політики безпеки для підвищення рівня захисту інформації від реалізації загроз через вразливості.

1.2 Аналіз нормативно-правової бази в сфері захисту інформації

Після входження суспільства в інформаційний етап його розвитку – інформатизацію, на державному рівні почали створюватися закони та нормативні документи (НД) для регулювання інформаційних відносин.

Нормативно-правове забезпечення визначає порядок захисту основних властивостей інформації, таких як: конфіденційності, цілісності та доступності.

Захист інформації в ІТС визначається:

– законами та нормативно-правовим актами України;

– нормативними документами та нормативно-правовими актами системи технічного захисту інформації;

– державними стандартами та нормативними документами зі стандартизації.

Нормативні документи, які використовуються в одному підприємстві або ІТС, включають в себе особливості та умови технології обробки інформації в даному підприємстві або ІТС. Документи розробляються власником компанії.

На даний момент в Україні існує доволі багато нормативно-правових документів, які стосуються інформації та її безпеки. Основою для забезпечення безпеки інформації в Україні є Конституція України, Закони України та нормативно-правові акти (наведені нижче).

Згідно з Законом України (ЗУ) «Про інформацію» [1] статті 1, інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

Згідно з ЗУ «Про інформацію» [1] статті 20 пункту 1, за порядком доступу інформація поділяється на відкриту інформацію та ІзОД. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до ІзОД.

Згідно з ЗУ «Про інформацію» [1] статті 21, ІзОД – інформація з обмеженим доступом. Інформація, яка становить державну, або іншу передбачену законом таємницю, до яких відноситься службова, таємна та конфіденційна інформація.

Згідно з ЗУ "Про доступ до публічної інформації" [2] статті 7, конфіденційною є інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Згідно з ЗУ «Про захист персональних даних» [3] статті 2, персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

Згідно з ЗУ «Про захист персональних даних» [3] статті 5 пункту 1, об’єктами захисту є персональні дані.

Згідно з ЗУ «Про захист персональних даних» [3] статті 10 пункту 2, використання персональних даних володільцем здійснюється у разі створення ним умов для захисту цих даних. Володільцю забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними.

Згідно з ЗУ «Про захист інформації в ІТС» [4]:

– статті 4, порядок доступу до інформації, перелік користувачів та їх повноваження в роботі з цією інформацією визначається власником інформації;

– статті 5, власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом. Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі;

– статті 8, умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством;

– статті 9, відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Відповідно до Цивільного Кодексу України «Поняття комерційної таємниці» [5] статті 505 пункту 1 та пункту 2:

– комерційна таємниця – інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом

адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію;

– комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Відповідно до НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [6], АС на підприємстві відповідає критеріям 3 класу. Клас «3» — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

1.3 Об’єкт інформаційної діяльності

Відповідно до НД ТЗІ 1.6-005-2013 «Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці» [7]

пункту 3, ОІД – інженерно-технічна споруда (приміщення), транспортний засіб, де здійснюється озвучення та/або обробка технічними засобами інформації з обмеженим доступом.

1.4 Підстави для створення КСЗІ

В ІТС відділу центру з обробки замовлень ТОВ «BeerWineShop» оброблюється конфіденційна інформація, яка належить до ІзОД, комерційна таємниця, персональні дані та відкрита інформація.

Відповідно до НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [8], комплексна система захисту інформації (КСЗІ) – сукупність організаційних заходів і інженерних заходів, апаратно-програмних засобів, які забезпечують захист інформації в ІТС. 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.

Відповідно до [8], необхідно провести обстеження середовища функціонування середовища ІТС за такими складовими:

- фізичне середовище;
- середовище обчислювальної системи;
- інформаційне середовище;
- середовище користувачів.

На підставі проведеного обстеження розроблюється ПБ інформації в ІТС та приймається рішення про необхідність створення моделі КСЗІ. Також, розроблюється модель загроз та модель порушника, аналізується можливість керування ризиками. Далі, формуються рекомендації, вимоги, правила та обмеження щодо використання захищених технологій обробки інформації в ІТС.

Створення та впровадження КСЗІ допомагає знизити економічні витрати підприємства у разі реалізації потенційних загроз, які визначені на етапі аналізу моделі загроз та моделі порушника.

1.5 Модель загроз та вразливостей. Модель порушника

Відповідно до НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [9], загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Відповідно до НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» [10] пункту 4.2.2, 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.

Відповідно до [10] пункту 4.2.4, 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, об-

ладнання, 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 не-

вірними 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.

Відповідно до [10] пункту 4.2.5, 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, заземлення, охоронної сигналізації, вентиляції та ін.);

– порушення режимів функціонування АС (обладнання і ПЗ);

– впровадження і використання комп'ютерних вірусів,

– 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 (роздруківок, 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;

– 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).

Розробка моделі загроз для інформації та моделі порушника є основою для проведення аналізу можливих ризиків і формування вимог до КСЗІ.

Відповідно до [10] пункту 4.4, модель порушника – це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії тощо.

Порушник розглядається як особа, яка може одержати НСД до роботи з включеними до складу ІТС засобами. Модель порушника повинна визначати:

– можливі цілі порушника та їх градація за ступенями небезпечності для ІТС та інформації, що потребує захисту;

– категорії персоналу, користувачів ІТС та сторонніх осіб, із числа яких може бути порушник;

– припущення про кваліфікацію порушника;

– припущення про характер його дій.

Відповідно до [10] пункту 4.4.1, метою порушника можуть бути:

– отримання необхідної інформації у потрібному обсязі та асортименті;

– мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

– нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

1.6 Політика безпеки інформації на підприємстві

Відповідно до [10] пункту 5.1, під ПБ інформації 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.

Відповідно до [10] пункту 5.2, під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники.

1.7 Постановка задачі

У наш час використання інформаційних технологій набирає все більше обертів. Питанням кібербезпеки в Україні займаються різні відомства: Державна служба спеціального зв'язку і захисту інформації, Міністерство внутрішніх справ, Служба безпеки України, Національний банк. Кожне з цих відомств вживає заходи для організації безпеки і веде щомісячну статистику відповідних показників, однак їхня діяльність охоплює лише окремі сфери відповідальності.

Дивлячись на важливість забезпечення ІБ підприємства необхідно виконати обстеження фізичного середовища ІТС, обчислювальної системи та інформаційного середовища, середовища користувачів, проаналізувати вірогідні загрози та вразливості ІТС підприємства, скласти модель загроз та модель порушника, розробити КСЗІ та політики безпеки для підвищення рівня захисту інформації підприємства та економічно обґрунтувати доцільність її реалізації.

1.8 Висновок

Перший розділ кваліфікаційної роботи описує актуальність впровадження КСЗІ інформаційно-телекомунікаційної системи приватного підприємства. В розділі наведено головні нормативно-правові документи в сфері захисту інформації. Проаналізовано принцип та процес побудови КСЗІ для підприємства.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про ОІД

ІТС належить: ТОВ «Beerwineshop».

Дата реєстрації підприємства: 25.04.2011р.

Підприємство розташовано за адресою: 49000, Дніпропетровська обл., місто Дніпро, Індустріальний район, проспект Слобожанський, будинок 121Б.

Діяльність підприємства: роздрібна торгівельна мережа з продажу слабоалкогольних напоїв та закусок. ТТ розташовані в п’яти містах України (Київ, Одесса, Дніпро, Харків, Запоріжжя). Клієнти можуть сформувати замовлення особисто в магазині, або онлайн – через офіційний сайт підприємства. Замовлення, які сформовано онлайн, оброблюються операторами в усній формі в програмі 1С:Підприємство 8. Кількість штатних робітників: 12.

Графік роботи: працює 7 днів на тиждень. З 9:00 до 24:00 години.

На рис. 2.1 зображена організаційна структура підприємства:

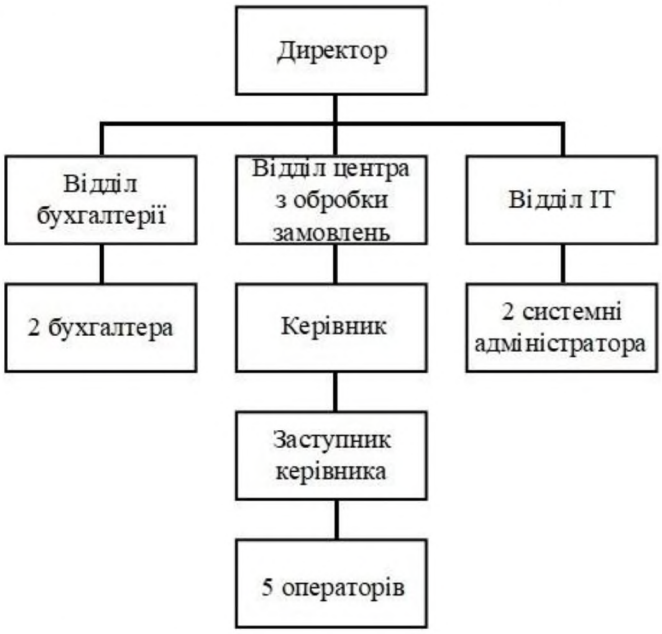

Рисунок 2.1 – Організаційна структура підприємства

2.2 Обстеження фізичного середовища ІТС

2.2.1 Опис ситуаційного плану ОІД

Об'єктом інформаційної діяльності (ОІД) є орендоване приміщення (цокольний поверх) у ФОП Перлина О. О. для підприємства ТОВ «Beerwineshop».

ОІД розташований на цокольному поверсі чотирьох поверхової будівлі.

Ситуаційний план ОІД наведений на рис. Б.1 у Додатку Б. Умовні позначення до ситуаційного плану ОІД наведені на рис. Б.2 у Додатку Б.

Фундамент будівлі виконаний з використанням залізобетонних паль з перетином 0,3х0,3 м, довжиною 12 м та залитий армованим бетоном товщиною 0,7 м. Несучі стіни будівлі збудовані з білої цегли зовні та газобетону з середини, між цеглою та газобетоном присутній утеплювач з базальтової вати, товщина несучих стін 0,65 м. Внутрішні (міжкімнатні) стіни збудовані з газобетону, товщина внутрішніх стін 0,3 м. Між поверхами розташовані бетонні конструкції (плити), товщиною 0,3 м. Дах будівлі виконаний з металочерепиці, завтовшки 0.005 м.

Будівля, в якій розташовано ОІД, з півночі, заходу та півдня огороджена парканом з бетонних плит заввишки 1,5 м.

Територія будівлі впорядкована та асфальтована. Центральний вхід знаходиться зі східної сторони, запасні виходи знаходяться з південної сторони на кожному поверсі (від першого до третього). На поверху 1-3 розташовані офіси інших підприємств. Всі кімнати будівлі орендуються одним власником для офісів.

Будівля оснащена металопластиковими вікнами з подвійним склопакетом. На центральному вході встановлені дві однакові металопластикові вхідні двері – з потрійним склопакетом, розміри 2 × 1,2 м. Замок на перших вхідних дверях – обладнано системою контролю доступу (контролер та зчитувач Seven CR-772M та електромагнітний замок – ML-280 з силою утримання 280 кг), замок на другій двері – врізаний циліндровий (штифтовий).

З західної сторони будівлі розташоване місце паркування транспортних

засобів, а за парканом житлові будинки та вулиця Радищева. На сході знаходиться одноповерхова автомобільна заправна станція та проспект Слобожанський.

Перелік та характеристика всіх будівель та споруд, які розташовані біля ОІД наведено в табл. 2.1. Характеристика та відстань прилеглих вулиць до ОІД наведено в табл. 2.2.

Таблиця 2.1 – Характеристика будівель та споруд

Найменування	Кількість поверхів	Адреса	Напрям відносно ОІД	Відстань до ОІД, м
1. Адміністративна будівля	4	Проспект Слобожанський, будинок 121Б	-	ОІД
2. Адміністративна будівля	2	Проспект Слобожанський, будинок 121А	Південь	20
3. Адміністративна будівля	2	Проспект Слобожанський, будинок 122	Північ	47
4. Житловий будинок	2	Вул. Радищева, будинок 58	Північно-західний	65
5. Житловий будинок	1	Вул. Радищева, будинок 59	Захід	78
6. Житловий будинок	2	Вул. Радищева, будинок 60	Захід	40
7. Житловий будинок	1	Вул. Радищева, будинок 61	Захід	71
8. Житловий будинок	1	Вул. Радищева, будинок 62	Захід	48

Продовження таблиці 2.1 – Характеристика будівель та споруд

Найменування	Кількість поверхів	Адреса	Напрям відносно ОІД	Відстань до ОІД, м
9. Житловий будинок	2	Вул. Радищева, будинок 63	Захід	85
10. Житловий будинок	1	Вул. Радищева, будинок 64	Південно - західний	62
11. Житловий будинок	2	Вул. Радищева, будинок 65	Південно - західний	100
12. Житловий будинок	2	Вул. Радищева, будинок 66	Південь	101
13. Житловий будинок	2	Вул. Радищева, будинок 67	Південно - західний	150
14. Адміністра-тивна будівля	1	Проспект Слобожанський, будинок 120	Схід	79

Таблиця 2.2 – Характеристика та відстань прилеглих вулиць до ОІД

Назва вулиці/проспекту	Ширина вулиці/проспекту, м	Відстань до ОІД, м
Просп. Слобожанський	10,5	36
Вул. Радищева	5	61

Контрольована зона (КЗ) – обмежена периметром будівлі.

На центральному вході в будівлю встановлений КПП з постом цілодобової охорони. Охоронці на вахті – співробітники приватної охоронної фірми «Сокіл», з якою ТОВ «Beerwineshop» уклало договір надання послуг з цілодобової охорони будівлі. Охоронці працюють згідно зовнішніх організаційно-розпорядчих документів охоронної фірми, згідно договору. За добу пост охорони змінюється 2 рази, всього 4 охоронці.

Приміщення будівлі обладнанні охоронною та пожежною системою

сигналізації, яка підключена до ППКОП, який встановлений на КПП. Зовні будівля обладнана системою відеоспостереження, зображення виводиться на екран моніторів, які знаходяться на КПП охоронця. Відео з камер спостереження записується та зберігається на сервері охорони (S3), резервна копія відео-файлів резервуються двічі на день, кожні 12 годин на жорсткий диск HDD2, термін зберігання відео-файлів на сервері та жорсткому диску становить 30 днів.

У робочій час (8:00 - 00:00) режим КЗ забезпечується завдяки сил служби цілодобової охорони з використанням системи відеоспостереження та контролю доступу (на вхідних дверях встановлена система контролю доступу через магнітну картку, яка попередньо програмується та видається охоронцем працівникам закладу, журнал записів виданих магнітних карток знаходиться в охоронця в столі та в електронному вигляді на сервері охорони (S3)).

Відвідувачі, які не мають магнітної картки, можуть зайти тільки за згодою охоронця, який зафіксує ПІБ (згідно документу, який посвідчує особу) та час відвідування. Згода на прохід, або відвідування будівлі для людини, яка не є внутрішнім працівником компанії та не має магнітної картки, надається тільки у разі, якщо охоронця попередив директор підприємства, або керівник.

У не робочій час (00:00 - 08:00) режим КЗ забезпечується силами служби цілодобової охорони з використанням системи відеоспостереження та охоронної сигналізації.

Доступ електриків, техніків, сантехніків в будівлю до комунікаційних систем надається за попередньою заявою від власника об’єкта. Прибиральниця є робітником приватної фірми «Cleanroom» з якою ТОВ «Beerwineshop» уклало договір про надання послуг з прибирання. Прибиральниця має обмежений доступ до ОІД та виконує свою роботу тільки в присутності співробітника компанії.

До будівлі підключені такі системи комунікації:

– система електропостачання підприємства підключена до ТП «Золоті ключі» №10, трьох фазним вводом 0,4 кВ, підземними комунікаціями. ТОВ «Beerwineshop» не має прямих договірних відносин з оператором розподілу електричної енергії, оскільки орендує приміщення у ФОП Надєїін О.М. ТП

знаходиться за межами КЗ та має сторонніх споживачів. Ввід в будівлю знаходиться на цокольному поверсі, кімната №7;

– система водопостачання, підключена до міської системи централізованого водопостачання підземними комунікаціями, пластиковими трубами, що виходять за межі КЗ. ТОВ «Beerwineshop» не має прямих договірних відносин з оператором міської системи централізованого водопостачання, оскільки орендує приміщення у ФОП Надєїін О.М. З'єднання проходить через цокольний поверх в кімнаті №4;

– система каналізації, підключена до міської системи централізованого водовідведення підземними комунікаціями, пластиковими трубами, що виходять за межі КЗ. ТОВ «Beerwineshop» не має прямих договірних відносин з оператором міської системи централізованого водовідведення, оскільки орендує приміщення у ФОП Надєїін О.М. З'єднання проходить через цокольний поверх в кімнаті №4;

– система мережі Інтернет підключена за допомогою оптично-волокнистого кабелю, обладнання від провайдеру ПО ДФ ПАТ «Укртелеком». Кабель прокладено до будівлі підземними комунікаціями. ТОВ «Beerwineshop» має прямі договірні відносини з провайдером інтернету ПО ДФ ПАТ «Укртелеком» та працює згідно укладеного договору про надання телекомунікаційних послуг. Ввід у будівлю знаходиться на цокольному поверсі в кімнаті №10;

– система охоронної сигналізації, забезпечується силами служби цілодобової охорони, пристроями СКУД на вхідних дверях з центральної сторони будівлі та зовнішніми камерами відеоспостереження Green Vision GV-040-GHD-H-COS20-20 1080P по периметру КЗ.

2.2.2 Опис генерального плану:

Генеральний план ОІД наведений на рис. В.1 у Додатку В. Генеральний план з позначенням пожежної та охоронної сигналізації наведений на рис. В.2 у Додатку В. Умовні позначення до генеральних планів ОІД наведено на рис. В.3 у

Додатку В.

Площа ОІД – 83,9 м^2.

Приміщення підприємства знаходиться на нульовому (цокольному) поверсі:

– підлога з середини залита бетоном, на який встановлена дерев'яна підлога з утеплювачем з базальтової вати та вкрита лінолеумом, товщина дерев'яної підлоги з лінолеумом 0,2 м;

– стіни та стеля з середини зашпакльовані трьома шарами цементної штукатурки, завтовшки 0,015 м;

– два вікна, що виходять на захід – металопластикові з подвійним склопакетом, з функцією відкриття, розміри 0,6×0,8 м;

– підвісна стеля зроблена з мінерального волокна, товщина 0,006 м;

– висота від підлоги до стелі – 1,5 м;

– міжкімнатні двері – подвійні металопластикові з подвійним склопакетом, розміри 2×1,2 м;

– замки на міжкімнатних дверях – врізані циліндрові (штифтовані).

Призначення кімнат та доступ до них наведено у табл. Г.1 у Додатку Г.

Особливості кімнат:

– кімнати №1,2 … 5 не зачиняються на ключ;

– ключі від кімнат №6 та кімнати №7 знаходяться у директора в сейфі, який розташований в кімнаті №13;

– ключі від кімнати №8 знаходяться в керівника та заступника керівника, який зачиняє кімнату після закінчення робочого дня операторів, або назначає старшого оператора для передачі ключа, також, ключі від кімнати носять при собі директор та системні адміністратори. Запасний ключ знаходиться у директора в сейфі, який розташований в кімнаті №13;

– ключі від кімнати №9 та кімнати №10 носять при собі системні адміністратори. Кімнати зачиняються на ключ системними адміністраторами після закінчення їх робочого дня. Запасні ключі знаходиться у директора в сейфі,

який розташований в кімнаті №13;

– ключі від кімнати №11 знаходяться у бухгалтерів. Бухгалтери зачиняють кімнату на ключ після закінчення їх робочого дня. Запасний ключ знаходиться у директора в сейфі, який розташований в кімнаті №13;

– ключі від кімнати №12 знаходяться у директора та бухгалтерів. Бухгалтери або директор зачиняють кімнату на ключ після закінчення їх робочого дня. Запасний ключ знаходиться у директора в сейфі, який розташований в кімнаті №13;

– ключі від кімнати №13 знаходяться у директора. Кімната зачиняється на ключ директором після закінчення його робочого дня. Запасний ключ знаходиться у директора в сейфі, який розташовано в кімнаті №13;

– магнітні картки від СКУД знаходяться в охоронця на КПП та у директора в сейфі, який розташований в кімнаті №13;

Після закінчення робочого дня всіх працівників відділів, охоронець встановлює під охорону ОІД.

В будівлі присутні такі системи комунікацій:

– система освітлення, кімнати відділу освітлюються за допомогою люмінесцентних ламп фірми Philips;

– система опалення, приміщення будівлі опалюються за допомогою електроконвекторів фірми Atlantic;

– система вентиляції, приточно-витяжна з системою кондиціювання;

– система пожежної сигналізації, встановлені автоматичні димові; сповіщувачі фірми Артон СПД-3.2, ручні пожежні сповіщувачі фірми Артон SPR-1, сигнальні світлові пристрої Сирена ОС3-5, прилад приймально – контрольний охоронно – пожежний (ППКОП) Лунь-11;

– система охоронної сигналізації, встановлені пасивні інфрачервоні датчики руху фірми Crow SWAN QUAD, магнітно-контактні датчики на відкриття дверей та вікон фірми Електрон ЕСМК-7ЕП, тривожна кнопка фірми Електрон IPTC, датчики на розбиття скла фірми Crow GBD2, камери

відеоспостереження фірми Green Vision GV-040-GHD-H-COS20-20 1080P;

– всі пристрої заземлені на спільний замкнутий контур, що виходить за межі ОІД;

– кабель мережі Інтернет – екранована кручена пара стандарту UTP 4x2x0,5 5e.

ППКОП розташований на КПП на першому поверсі біля центрального входу, кабелі системи пожежної та охоронної сигналізації проходять до ППКОП з кімнати №7 цокольного поверху.

Архівна шафа, в якій зберігаються друковані документи, які відносяться та не відносяться до ІзОД, розташована в кімнаті №11. Права доступу до шафи та документів в ній встановлені директором відділу.

Сейф, в якому зберігаються друковані документи, що відносяться до ІзОД, магнітні картки від СКУД, розташований в кімнаті №13. Права доступу до сейфу та документів в ньому встановлені директором відділу.

Сейф, в якому зберігаються ЖМД HDD1 та HDD2, розташований в кімнаті №10. Права доступу до сейфу та документів в ньому встановлені директором відділу.

2.3 Обстеження обчислювальної системи

Канал зв’язку в межах корпоративної мережі забезпечується одним провайдером ПО ДФ ПАТ «Укртелеком», який надає послуги з підтримки відомчої телекомунікаційної мережі у відповідності до договору між ТОВ «BeerWineShop» та ПО ДФ ПАТ «Укртелеком».

ІТС являє собою мережу типу «пасивна зірка». В основі мережі лежить комутатор (К1), усі пристрої, а саме: 3 сервера (S1 – сервер для роботи 1С; S2 – сервер для файлів, документів, резервних копій; S3 – сервер для відео файлів з камер відеоспостереження), 14 персональних комп’ютерів (ПК1, ПК2 … ПК14), з'єднуються за допомогою даного комутатора крученою парою, комутатор (К1) під’єднаний до маршрутизатора (М1), який в свою чергу підключений між локальною мережею та мережею Інтернет. Принтер П1 та П2 використовуються

для друку документів різних видів важливості, з'єднані з комутатором (К1) крученою парою. ЖМД HDD1 та HDD2 використовуються для резервного зберігання інформації, з'єднані з персональним комп'ютером (ПК9) USB кабелем типу B. Маршрутизатор (М1) включає в себе апаратний брандмауер для захисту від НСД.

Структурна схема обчислювального середовища ІТС представлена на рис.2.2.

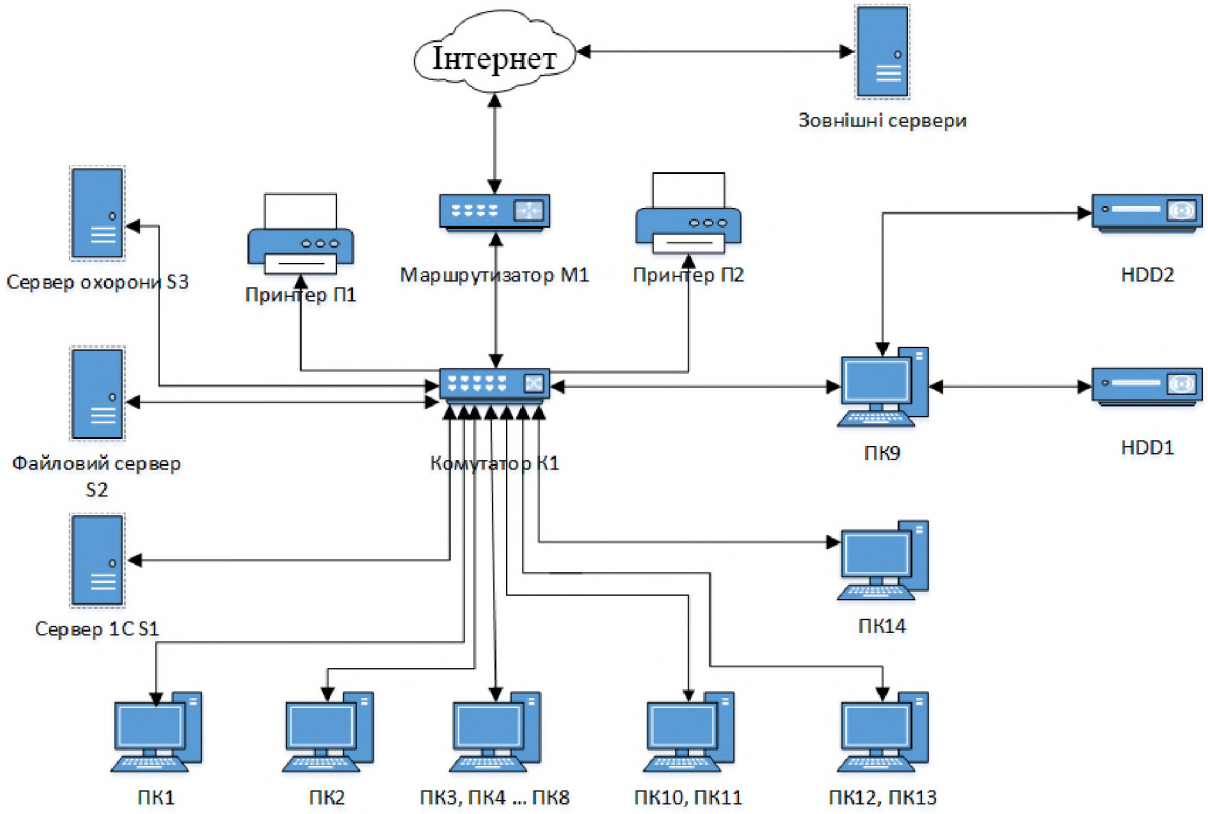

Рисунок 2.2 – Структурна схема обчислювального середовища ІТС

ІТС являє собою мережу типу «пасивна зірка». В основі мережі лежить комутатор (К1), усі пристрої, а саме: 3 сервера (S1 – сервер для роботи 1С; S2 – сервер для файлів, документів, резервних копій; S3 – сервер для відео файлів з камер відеоспостереження), 14 персональних комп'ютерів (ПК1, ПК2 … ПК14), з'єднуються за допомогою даного комутатора крученою парою, комутатор (К1) під'єднаний до маршрутизатора (М1), який в свою чергу підключений між локальною мережею та мережею Інтернет. Принтер П1 та П2 використовуються для друку документів різних видів важливості, з'єднані з комутатором (К1)

крученою парою. ЖМД HDD1 та HDD2 використовуються для резервного зберігання інформації, з'єднані з персональним комп'ютером (ПК9) USB кабелем типу B. Маршрутизатор (M1) включає в себе апаратний брандмауер для захисту від НСД.

До серверів (S1, S2, S3) підключені джерела безперебійного живлення, які підтримують задану якість вихідної напруги у разі відсутності вхідної напруги за рахунок використання енергії акумуляторних батарей. Енергії акумуляторних батарей в середньому вистачає на 2 години автономного живлення серверів.

Через ІТС проходить інформація різних категорій конфіденційності, цілісності та доступності. Локальна комп'ютерна мережа має доступ до мережі Інтернет для забезпечення взаємодії через комп'ютерну мережу з ТТ підприємства, зовнішнім сервером корпоративної пошти Outlook корпорації Майкрософт та зовнішнім сервером хостинг-провайдеру «Hostingroup».

Кожен користувач має власний обліковий запис, пароль від якого встановлює та видає системний адміністратор, після першого входу до облікового запису користувачу потрібно змінити пароль на свій особистий.

Корпоративна пошта Outlook від корпорації Майкрософт, якою користуються працівники для обробки звернень клієнтів, обміну та передачі електронних документів, розташована на зовнішньому сервері. Звернення клієнтів, обмін та передача документів відбувається у незашифрованому вигляді.

Сайт компанії розташований зовнішньому сервері хостинг-провайдеру «Hostingroup», з яким був укладений договір надання послуг з цілодобової підтримки працездатності сайту.

Перелік ОТЗ наведений у табл. Ґ.1 у Додатку Ґ.

Перелік ДТЗС наведений у табл. Д.1 у Додатку Д.

Характеристика складу апаратних засобів ОТЗ наведена у табл. Е.1 у Додатку Е.

Перелік ПЗ встановленого на ОТЗ наведений у табл. Є.1 у Додатку Є.

2.4 Обстеження інформаційного середовища ОІД

Власником інформації є ТОВ «Beerwineshop». В ІТС відсутня таємна та службова інформація, а також інформація, яка становить державну таємницю та є власністю держави.

Інформація підприємства зберігається у вигляді електронних документів, які створені за допомогою пакету прикладних програм Microsoft Office 2016 Pro Plus, Adobe Acrobat Pro DC, 1С:Підприємство 8, або у роздрукованому вигляді. Електронні документи зберігаються на ПК, серверах та флеш накопичувачах. Резервна копія документів зберігається на ЖМД, які в свою чергу знаходяться в сейфі в кімнаті №10. Роздруковані документи, які містять або не містять ІзОД зберігаються в сейфі в кімнаті №13, або архівній шафі кімнати №11 та кімнати №13. Електроні документи, які містять ІзОД та циркулюють в межах офісу для передачі даних з одного ПК на інший, зберігаються на незареєстрованих флеш накопичувачах в сейфі кімнати №13.

Доступ до сейфів, архівних шаф та документів в них, мають працівники, які мають доступ до кімнат в яких знаходяться названі вище об’єкти, див. табл. 2.3.

ІзОД має велику цінність для компанії, її втрата та передача може нанеси суттєвих матеріальних збитків для компанії.

Класифікація інформації, яка циркулює на ІТС наведена в табл. 2.4. Вимоги до захисту інформації встановлено власником підприємства згідно внутрішніх нормативно-правових актів.

Інформація зберігається в системі у форматах: *.img, *.png, *.doc, *.docx, *.pdf, *.xls, *.ppt, *.pptx, *.txt, *.mp3, *.mp4, *.cf, *.cfu, *.cfe, *.dt, *.epf, *.1cd, *.log, *.lgf, *.lgp, *.elf, *.cdn, *.mxl, *.efd, *.mft, *.grs, *.geo, *.st, *.pff, *.pfl ,*.ini.

Імпорт та експорт інформації в ІТС відбувається шляхом:

– копіювання інформації на флеш накопичувач для передачі її іншому користувачу ІТС підприємства, який має повноваження для роботи з цією інформацією;

– передачі або отримання інформації електронною поштою;

– сканування та друку документів;

– передачі або отримання кур’єром на паперовому носії.

Таблиця 2.3 – Класифікація інформації, яка циркулює на ІТС

Вид інформації що циркулює	Правовий режим	Режим досту-пу	Доступ мають	Вимоги до захисту	Місце зберігання
1	2	3	4	5	6
1. Внутрішні документи	Конфіден-ційна інформація	ІзОД	Директор, керівник, заступник керівника, бухгалтери, сис. адмін.	К, Ц, Д	сервер 1С (S1), архівна шафа кімната №11, HDD1
2. Організа-ційнорозпо-рядчі документи	Конфіден-ційна інформація	ІзОД	Директор, керівник, бухгалтери, сис. адмін.	К, Ц, Д	ПК14, файловий сервер (S2), архівна шафа кімната №13, HDD1
3.Інформація про працівників	Конфіден-ційна інформа-ція	ІзОД	директор, бухгалтери, керівник, заступник керівника, сис. адмін.	К, Ц, Д	ПК14, файловий сервер (S2), сейф кімната №13, HDD1

Продовження таблиці 2.3 – Класифікація інформації, яка циркулює на ІТС

1	2	3	4	5	6
4. Інформація про послуги компанії	Відкрита інформація	Відсутній, не потребує захисту	Всі працівники	Ц, Д	Зовнішній сервер, HDD1
5. Асортимент товару	Відкрита інформація	Відсутній, не потребує захисту	Всі працівники	Ц, Д	Зовнішній сервер, HDD1
6. Інформація про клієнтів та замовлення клієнтів	Конфіденційна інформація	ІзОД	Директор, керівник, заступник керівника, оператори, сис. адмін.	К, Ц, Д	Сервер 1С (S1), HDD1
7. Фінансова звітність	Комерційна таємниця	ІзОД	Директор, керівник, заступник керівника, бухгалтери, сис. адмін.	К, Ц, Д	ПК12, ПК13, сервер 1С (S1), архівна шафа, кімната №11, HDD1

Продовження таблиці 2.3 – Класифікація інформації, яка циркулює на ІТС

1	2	3	4	5	6
8. Журнал інвентаризації технічних засобів	Комерційна таємниця	ІзОД	Директор, керівник, сис. адмін.	К, Ц, Д	ПК10, ПК11, файловий сервер (S2),HDD1
9. Журнал інвентаризації охоронних засобів	Комерційна таємниця	ІзОД	Директор, керівник, охоронці, сис. адмін.	К, Ц, Д	ПК14, файловий сервер (S2), сервер охорони (S3), сейф кімнати №10, HDD1, HDD2
10. Записи з камер відеоспостереження	Комерційна таємниця	ІзОД	Директор, охоронці, сис. адмін.	К, Ц, Д	Сервер охорони (S3), HDD2
11. Зовнішні документи	Конфіденційна інформація	ІзОД	директор, бухгалтери, сис. адмін.	К, Ц, Д	Файловий сервер (S2), сейф кімната №13, HDD1

Продовження таблиці 2.3 – Класифікація інформації, яка циркулює на ІТС

1	2	3	4	5	6
12. Архів звернень та скарг клієнтів	Конфіден-ційна інформа-ція	ІзОД	директор, керівник, заступник керівника, оператори, сис. адмін.	К, Ц, Д	Файловий сервер (S2), HDD1
13. Пакети оновлення ОС Microsoft Windows 10 Professional	Відкрита інформація	Відсу-тній, не потре-бує захисту	Всі працівники	Ц, Д	Зовнішній сервер
14. Паролі від облікових записів	Конфіденці йна інформація	ІзОД	системні адміністратори	К, Ц, Д	Пам'ять користувача , записи на листку, реєстр ОС Windows
15. Правила розмежуванн я доступу	Конфіденці йна інформація	ІзОД	Директор, системні адміністратори	Ц, Д	HDD1

Визначення вимог до захисту конфіденційної, цілісної та доступності інформації наведено в табл. 2.4.

Таблиця 2.4 – Вимоги до захисту інформації

Вид інформації що циркулює	Рівень конфіденційності	Рівень цілісності	Рівень доступності
1. Внутрішні документи	КЗ	ЦЗ	ДЗ

Продовження таблиці 2.4 – Вимоги до захисту інформації

Вид інформації що циркулює	Рівень конфіденційності	Рівень цілісності	Рівень доступності
2. Організаційно-розпорядчі документи	К2	Ц2	Д3
3. Інформація про працівників	К3	Ц3	Д2
4. Інформація про послуги компанії	К1	Ц3	Д4
5. Асортимент товару	К1	Ц3	Д4
6. Інформація про клієнтів та замовлення клієнтів	К3	Ц3	Д2
7. Фінансова звітність	К3	Ц4	Д4
8. Журнал інвентаризації технічних засобів	К2	Ц3	Д3
9. Журнал інвентаризації охоронних засобів	К2	Ц3	Д3
10. Записи з камер відеоспостереження	К2	Ц5	Д4
11. Зовнішні документи	К3	Ц4	Д4
12. Архів звернень та скарг клієнтів	К2	Ц2	Д2
13. Пакети оновлення ОС Microsoft Windows 10 Professional	К1	Ц4	Д3
14. Паролі від облікових записів	К4	Ц3	Д5
15. Правила розмежування доступу	К1	Ц2	Д2

Інформація класифікована згідно рівням властивостей, які описані нижче:

Рівні конфіденційності:

– К1 – рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;

– К2 – рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К3 – рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К4 – рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;

– К5 – критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності:

– Ц1– рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;

– Ц2 – рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;

– Ц3 – рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

– Ц4 – рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;

– Ц5 – критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

– Д1– рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;

– Д2 – рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;

– Д3 – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

– Д4 – рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;

– Д5 – критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

2.5 Технологія обробки інформації в ІТС

Внутрішні документи зберігаються в електронному вигляді на сервері 1С (S1) підприємства. Внутрішні документи – документи, які створені в межах підприємства ТОВ «BeerWineShop». До внутрішніх документів належать: авансові звіти працівників, табель обліку відпрацьованого часу, прибуткові ордери. Внутрішні документи формуються в 1С:Підприємство 8 директором, бухгалтером, або керівником. Доступ до внутрішніх документів мають: директор, керівник, заступник керівника, бухгалтери, системні адміністратори. За необхідністю внутрішні документи друкуються через принтер П1 та П2, зберігаються в паперовому вигляді в архівній шафі, яка знаходиться в кімнаті №11. Резервна копія електронних документів створюється автоматично двічі на день (кожні 12 годин) та зберігається у не зашифрованому вигляді на ЖМД HDD1 в сейфі кімнати №10.

Організаційно-розпорядчі документи зберігаються в електронному вигляді на ПК14 – директора та на файловому сервері (S2) підприємства. Організаційно-розпорядчі документи – документи, які містять розпорядження на здійснення певної операції. До організаційно-розпорядчих документів належать: накази про прийняття та звільнення з роботи та довіреність на отримання матеріальних цінностей. Організаційно-розпорядчі документи створюються директором та бухгалтерами. Доступ до організаційно-розпорядчих документів мають: директор, керівник, бухгалтери, системні адміністратори. За необхідністю

організаційно-розпорядчі документи друкуються через принтер П1 та П2, зберігаються в паперовому вигляді в архівні шафі кімнати №13. Резервна копія електронних документів створюється автоматично двічі на день (кожні 12 годин) та зберігається у не зашифрованому вигляді на ЖМД HDD1 в сейфі кімнати №10.

Інформація про працівників (персональні дані) зберігається в електронному вигляді на ПК14 – директора та на файловому сервері (S2) підприємства. Інформація вноситься до системи керівником та системним адміністратором під чай працевлаштування нового працівника. Доступ до інформації мають: директор, бухгалтери, керівник, заступник керівника, системні адміністратори. За необхідністю інформація про працівників друкується через принтер П2 та зберігається в паперовому вигляді в сейфі кімнати №13. Резервна копія електронних документів створюється автоматично двічі на день (кожні 12 годин) та зберігається у не зашифрованому вигляді на ЖМД HDD1 в сейфі кімнати №10.

Інформація про послуги компанії розташована на зовнішньому сервері хостинг-провайдера «Hostingroup», для перегляду доступна за посиланням на офіційному сайті підприємства у відкритому доступі в мережі Інтернет. Інформація про послуги компанії редагується системними адміністраторами за розпорядженням директора. Резервна копія електронних документів створюється автоматично двічі на день та зберігається у не зашифрованому вигляді на ЖМД HDD1 в сейфі кімнати №10.

Асортимент товару розташований на зовнішньому сервері хостинг-провайдера «Hostingroup», для перегляду доступний за посиланням на офіційному сайті підприємства у відкритому доступі в мережі Інтернет. Редагується системними адміністраторами за розпорядженням директора або керівника. Резервна копія електронних документів створюється автоматично двічі на день та зберігається у не зашифрованому вигляді на ЖМД HDD1 в сейфі кімнати №10.

Інформація про клієнтів та замовлення клієнтів зберігається в базі даних (БД) замовлень клієнтів в програмі 1С: Підприємство 8 на сервері 1С (S1) підприємства. Доступ до інформації про клієнтів мають: директор, керівник,

заступник керівника, оператори, системні адміністратори. БД складається з персональних даних клієнтів, таких як: ПІБ, номер телефону, дата народження, а також з такої інформації, як історія замовлень, адреси доставок. При оформлені замовлення клієнтом через сайт компанії, замовлення автоматично потрапляють у базу даних замовлень в 1С: Підприємство 8, як «нове» замовлення. Кожному замовленню присвоюється особистий порядковий номер. Кожне «нове» замовлення оброблюється оператором. Оператор перевіряє наявність товарів в магазині, який вказав клієнт, для отримання замовлення, якщо товари присутні, замовлення переадресовується до магазину в БД замовлень в 1С: Підприємство 8 через мережу Інтернет, якщо товари відсутні в магазині, оператор надсилає Short Message Service (SMS) повідомлення клієнту через сторонній онлайн сервіс розсилки SMS, який знаходиться за посиланням на сайті. Резервна копія електронних документів створюється автоматично двічі на день та зберігається у не зашифрованому вигляді на ЖМД HDD1 в сейфі кімнати №10.

Фінансова звітність формується та зберігається в електронному вигляді на ПК12 та ПК13 – бухгалтерів, а також зберігається на сервері 1С (S1) підприємства. Доступ до фінансової звітності мають директор, керівник, заступник керівника, бухгалтери, системні адміністратори. За необхідністю фінансова звітність друкується на принтері П2, зберігається в паперовому вигляді на робочих місцях директора та бухгалтера, або в архівній шафі кімнати №11. Резервна копія електронних документів створюється автоматично двічі на день та зберігається у не зашифрованому вигляді на ЖМД HDD1 в сейфі кімнати №10.

Журнал інвентаризації технічних засобів формується та зберігається в електронному вигляді на ПК10, ПК11 – ПК системних адміністраторів, зберігається на файловому сервері (S2) підприємства. Доступ до журналу інвентаризації технічних засобів мають: директор, керівник, системні адміністратори. За необхідністю журнал інвентаризації технічних засобів друкується через принтер П1 та П2, зберігається в паперовому вигляді в архівній шафі в кімнати №13. Резервна копія електронних документів створюється автоматично двічі на день та зберігається у не зашифрованому вигляді на ЖМД

HDD1 в сейфі кімнати №10.

Журнал інвентаризації охоронних засобів формується та зберігається в електронному вигляді на ПК14 – директора, а також на файловому сервері (S2) та сервері охорони (S3) підприємства. Доступ до журналу інвентаризації охоронних засобів мають: директор, керівник, охоронці, системні адміністратори. За необхідністю журнал інвентаризації охоронних засобів друкується через принтер П2, зберігається в паперовому вигляді в сейфі кімнати №13. Резервна копія електронних документів створюється автоматично двічі на день та зберігається у не зашифрованому вигляді на ЖМД HDD1 та HDD2 в сейфі кімнати №10.

Записи з камер відеоспостереження зберігаються в електронному вигляді на сервері охорони (S3). Доступ до записів з відеокамер мають: директор, охоронці та системні адміністратори. Резервна копія відеозаписів створюється автоматично двічі на день та зберігається у не зашифрованому вигляді на ЖМД HDD2 в сейфі кімнати №10.

Зовнішні документи зберігаються в електронному вигляді на файловому сервері (S2) підприємства. Зовнішні документи – документи, які створені за межами підприємства ТОВ «BeerWineShop», отримуються від інших підприємств та організацій електронною поштою Outlook або кур'єром «Нової Пошти». До зовнішніх документів належать: рахунки фактури, платіжні доручення, постанови, угоди, виписки банків. Кожен документ реєструється бухгалтером у бланку уніфікованої форми. Доступ до зовнішніх документів мають: директор, бухгалтери. За необхідністю внутрішні документи друкуються через принтер П1 та П2, зберігаються в паперовому вигляді в сейфі кімнаті №13. Резервна копія електронних документів створюється автоматично двічі на день (кожні 12 годин) та зберігається у не зашифрованому вигляді на ЖМД HDD1 в сейфі кімнати №10.

Архів звернень та скарг клієнтів зберігається в електронному вигляді на файловому сервері (S2). Звернення та скарги клієнтів створюються клієнтами та надсилаються на корпоративну пошту Outlook, після чого оброблюються операторами та зберігаються в архів, який розташовано на файловому сервері

(S2). Відповіді на звернення клієнти отримують у вигляді SMS повідомлення. Доступ до звернень мають: директор, керівник, заступник керівника, оператори, системні адміністратори. Резервна копія архіву створюється автоматично двічі на день та зберігається у не зашифрованому вигляді на ЖМД HDD1 в сейфі кімнати №10.

Пакети оновлення ОС Microsoft Windows 10 Professional надходять від веб-вузла компанії Microsoft. Оновлення з зовнішнього сервера завантажується автоматично при підключені ПК до мережі Інтернет. ОС Microsoft Windows 10 Professional підключається до веб-вузла компанії Microsoft і перевіряє наявність оновлень для конкретної комбінації компонентів операційної системи. Якщо оновлення доступно, воно завантажується і повідомляє про це за допомогою значка в області повідомлень, після чого встановлюється при перезагрузці, вимкненні або ввімкненні ПК. Доступ до зміни параметрів оновлення мають тільки системні адміністратори.

Паролі від облікових записів зберігаються у кожного користувача особисто. У пам'яті користувача, у вигляді записів на листку та у реєстру Windows. Для кожного нового користувача, системним адміністратором створюється окремий обліковий запис, пароль від якого надається адміністратором. Виданий адміністратором пароль повинен бути змінений під час першої авторизації.

Правила розмежування доступу кожного користувача до окремого виду інформації, створюються та редагуються директором з системним адміністратором. Резервна копія правил розмежування доступу оновлюється тільки у разі внесення змін та зберігається у не зашифрованому вигляді на ЖМД HDD1 в сейфі кімнати №10.

У разі необхідності директор може запросити та переглянути будь-яку інформацію та документи компанії.

Схему інформаційних потоків ІТС представлено на рис 2.3.

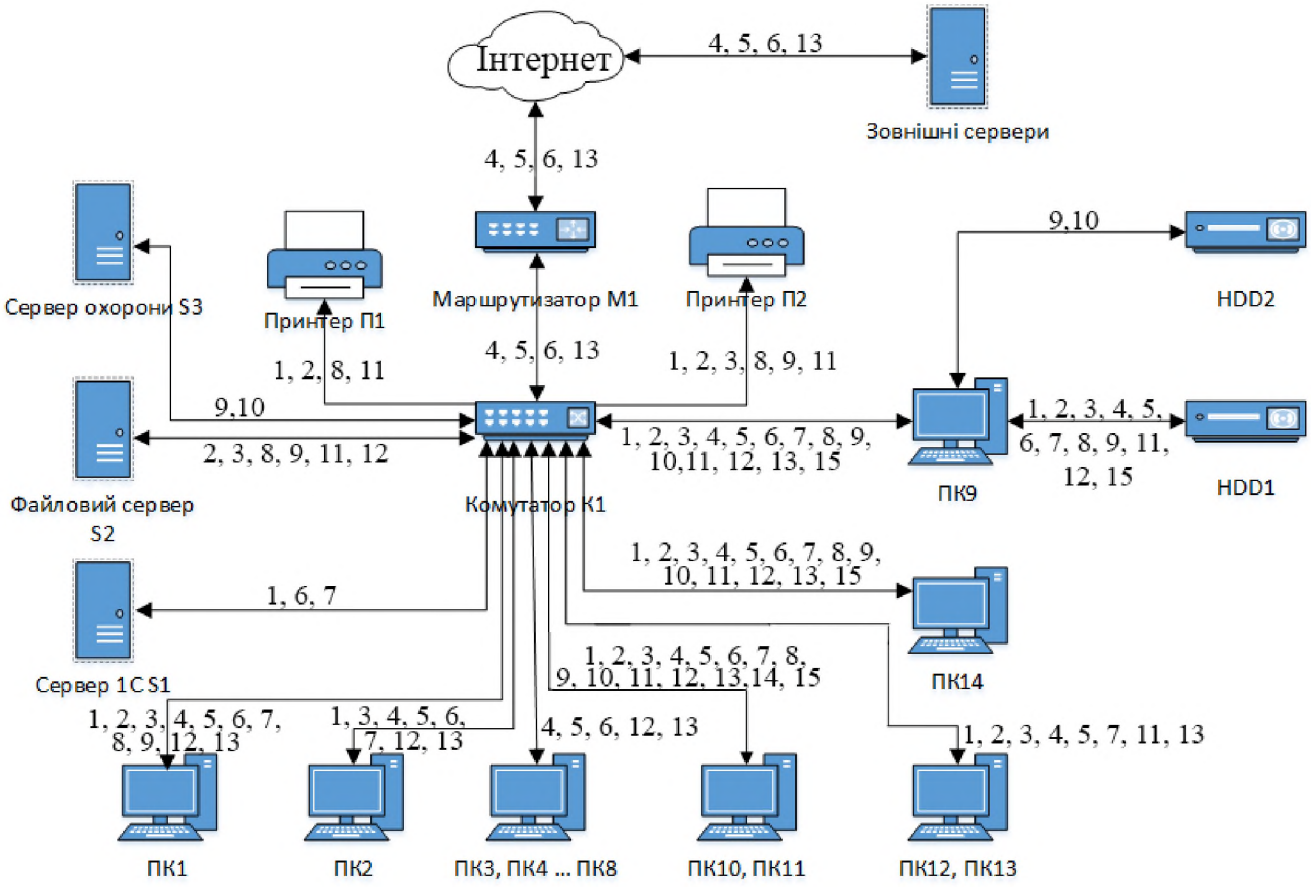

Рисунок 2.3 – Схема інформаційних потоків ІТС

2.6 Середовище користувачів ОІД

Користувачі ІТС мають різний рівень доступу до інформації. Рівень доступу залежить від посади, яку займає працівник і його посадових обов'язків. Обов'язки кожного працівника зазначені в посадових інструкціях відповідно до посади, яку він займає.

Внутрішні працівники – директор, керівник, заступник керівника, оператори, бухгалтери, системні адміністратори.

Позаштатні працівники – прибиральниці, охоронці, електрик, сантехнік, персонал Інтернет провайдеру, можуть перебувати в ОІД лише під наглядом внутрішніх працівників організації.

Рівень кваліфікації працівників підприємства наведено у табл. 2.5.

Таблиця 2.5 – Рівень кваліфікації працівників

Посада, робоче місце	Місце в системі	Кількість працівників на посаді	Рівень кваліфікації	Стаж на підприємстві
1	2	3	4	5
Директор ПК14	Користувач	1	Високо-кваліфікований робітник	5 років
Керівник ПК1	Користувач	1	Кваліфікований робітник	5 років
Заступник керівника ПК2	Користувач	1	Кваліфікований робітник	2 роки
Оператори ПК3, ПК4 … ПК8	Користувач	6	Кваліфікований робітник	5 років, 4 роки 3,5 роки 1 рік 0,5 року 0,1 року
Бухгалтери ПК12, ПК13	Користувач	2	Кваліфікований робітник	5 років 1 рік
Сис. адмін ПК9, ПК10, ПК11	Адміністратор	2	Високо-кваліфіковані робітники	5 років 3 роки

Обов’язки директора:

– контроль за всіма робочими процесами;

– вирішення юридичних питань, які пов’язані з діяльність компанії;

– керування персоналом (керівником, заступником керівника, операторами, бухгалтерами, системними адміністраторами);

– взаємодія з іншими відділами підприємства;

– ведення інвентаризаційної документації відділу центра з обробки замовлень;

– розробка посадових інструкцій, внутрішніх документів;

– складання угод про співпрацю з іншими компаніями.

Обов’язки керівника:

– здійснення набору та навчання персоналу (заступника керівника, операторів);

– керування персоналом (заступником керівника, операторами);

– ведення інвентаризаційної документації;

– проводження додаткових зборів для поліпшення знань заступника керівника;

– аналіз роботи відділу центра з обробки замовлень;

– формування графіку для заступника керівника.

Обов’язки заступника керівника:

– керування персоналом, а саме операторами;

– здійснення навчання персоналу, а саме операторів;

– проводження додаткових зборів для поліпшення знань операторів;

– аналіз роботи операторів;

– приймати участь у розробці посадових інструкцій, внутрішніх документів;

– формування графіку для операторів;

– у разі необхідності, виконувати роль оператора.

Обов’язки оператора:

– обробка замовлень від клієнтів;

– робота з архівом звернень та скарг від клієнтів;

– відправка SMS з відповіддю на звернення, чи скаргу;

– підтримка зв’язку з магазинами мережі через ПЗ Jitsi.

Обов’язки бухгалтера:

– ведення бухгалтерського обліку;

– складання звітів про фінансовий стан компанії та витрат за певний проміжок часу;

– планування бюджету для забезпечення роботи КЦ з урахуванням витрат на персонал, обладнання та технічну підтримку;

– видача заробітної плати працівникам за відпрацьовані години.

Обов'язки системного адміністратора:

– адміністрування локальної обчислювальної мережі;

– адміністрування ІТС, розмежування доступу користувачів до інформації згідно політики безпеки підприємства;

– контроль функціонування інформаційної системи;

– здійснення інсталяції та налаштування ПЗ;

– технічна підтримка відділу центру з обробки замовлень, обробка заяв про несправності технічних засобів;

– вирішення технічних проблем у найкоротший термін;

– контроль за ІБ організації;

– встановлення, налаштування і підтримка працездатності серверів;

– автоматизація підготовки та збереження резервних копій даних на зовнішні ЖМД (HDD1 та HDD2), їх періодичне знищення та оновлення;

– встановлення та оновлення апаратного та програмного забезпечення;

– створення, видалення та зміна прав доступу облікових записів користувачів;

– проводження планового технічного обслуговування та антивірусних заходів ПК.

Матриця розмежування доступу працівників до інформації наведена у табл. 2.6.

Таблиця 2.6 – Матриця розмежування доступу

Інформа-ція	Користувач					
	Директор	Керівник	Заступник керівника	Оператор	Бухгалтер	Сис. Адмін.
1	ЧРВДПС	ЧРДПС	ЧДП	–	ЧРДПС	ЧРВДПС
2	ЧРВДПС	ЧДП	–	–	ЧРДПС	ЧРВДПС
3	ЧРВДПС	ЧДП	ЧРВДПС	–	ЧДП	ЧРВДПС
4	ЧРВДПС	ЧДП	ЧДП	ЧДП	ЧДП	ЧРВДПС
5	ЧРВДПС	ЧРДП	ЧДП	ЧДП	ЧДП	ЧРВДПС
6	ЧРВДПС	ЧРВДПС	ЧРВДПС	ЧРДС	–	ЧРВДПС
7	ЧРВДПС	ЧДП	ЧДП	–	ЧРДПС	ЧРВДПС
8	ЧРВДПС	ЧДП	–	–	–	ЧРВДПС
9	ЧРВДПС	ЧДП	–	–	–	ЧРВДПС
10	ЧРВП	–	–	–	–	ЧРВП
11	ЧРВДП	–	–	–	ЧРДП	ЧРВДП
12	ЧРВДП	ЧРДП	ЧРДП	ЧРДП	–	ЧРВДП
13	–	–	–	–	–	ЧРВ
14	–	–	–	–	–	С
15	ЧРВДПС	–	–	–	–	ЧРВДПС

Операції з файлами: Ч – читання; Р – редагування; В – видалення; Д – друкування; П – передача (імпорт, експорт); С – створення;

Цифрами від 1 до 12 позначено інформацію згідно таблиці 2.5.

2.7 Модель порушника

Порушник – особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби, здійснила спробу виконати операції, які призвели

або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Відносно до ІТС порушників поділяють на: внутрішніх (користувачі, які отримали право доступу до інформації в системі), або зовнішніх (сторонні особи).

Відповідно до [10] пункту 4.4, модель порушника – це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії тощо.

Для побудови моделі порушника використовуються усі можливі категорії, ознаки та характеристики порушників для більш точного їх аналізу (рівень загрози кожної з них оцінюється за 4-бальною шкалою). Складемо модель внутрішнього порушника табл. 2.7 та модель зовнішнього порушника табл. 2.8.

Таблиця 2.7 – Модель внутрішнього порушника

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
1	2	3	4	5	6	7	8
Директор	ПВ3	М2	К2	З1	Ч3	Д4	15
	3	2	2	1	3	4	
Керівник	ПВ2	М2	К2	З1	Ч3	Д2	12
	2	2	2	1	3	2	
Заступник керівника	ПВ2	М2	К1	З1	Ч3	Д2	11
	2	2	1	1	3	2	
Оператор	ПВ2	М2	К1	З1	Ч3	Д2	11
	2	2	1	1	3	2	

Продовження таблиці 2.7 – Модель внутрішнього порушника

1	2	3	4	5	6	7	8
Бухгалтер	ПВ2	М1	К1	З1	Ч3	Д2	10
	2	1	1	1	3	2	
Системний адміністратор	ПВ3	М1	К4	З1	Ч4	Д4	17
	3	1	4	1	4	4	

Таблиця 2.8 – Модель зовнішнього порушника

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Прибиральниця	П32	М1	К1	З1	Ч1	Д1	7
	2	1	1	1	1	1	
Охоронець	П35	М3	К1	З1	Ч4	Д2	16
	5	3	1	1	4	2	
Електрик, технік, сантехнік	П32	М3	К1	З1	Ч4	Д4	17
	2	3	1	1	4	4	
Відвідувачі компанії	П31	М3	К2	З1	Ч3	Д1	11
	1	3	2	1	3	1	
Конкуренти компанії	П34	М3	К3	З4	Ч3	Д1	18
	4	3	3	4	3	1	
Хакери	П33	М3	К4	З4	Ч3	Д1	18
	3	3	4	4	3	1	

Визначення специфікацій моделей порушників наведено у табл.2.9.

Таблиця 2.9 – Внутрішні та зовнішні порушники

Позначення	Визначення категорії	Рівень загрози
Внутрішні порушники по відношенню до ІТС		
ПВ1	Технічний персонал, який обслуговує будови та приміщення , в яких розташовані компоненти ІТС	1
ПВ2	Персонал, який обслуговує технічні засоби ІТС (техніки)	2
ПВ3	Користувачі (оператори) ІТС	2
ПВ4	Адміністратори ІТС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
Зовнішні порушники по відношенню до ІТС		
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4
ПЗ5	Співробітники служби безпеки	4

Специфікація моделі порушника за мотивами здійснення порушень наведена у табл.2.10.

Таблиця 2.10 – Специфікація моделі порушника за мотивами здійснення порушень

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

Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС наведена у табл.2.11.

Таблиця 2.11 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загрози
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту наведена у табл.2.12.

Таблиця 2.12 – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	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

Специфікація моделі порушника за часом дії наведена у табл.2.13.

Таблиця 2.13 – Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загрози
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

Специфікація моделі порушника за місцем дії наведена у табл. 2.14.

Таблиця 2.14 – 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 ІТС	4

З останніх таблиць можемо зробити висновок, що найбільшу загрозу, яка має відношення до проблеми захисту інформації, в моделі внутрішнього порушника становить системний адміністратор та директор, в моделі зовнішнього порушника становить охоронець, електрик, технік, сантехнік, конкуренти компанії та хакери. Тому організація роботи цих осіб повинна бути найбільш контрольованою, оскільки вони є основними потенційними порушниками безпеки інформації.

2.8 Аналіз загроз та вразливостей в ІТС

Джерела загроз для безпеки інформації поділяються на:

– стихійні загрози (спричинені природними катаклізмами);

– антропогенні загрози (спричинені діяльністю людини);

– техногенні загрози (спричинені, через недосконаліть технічних та програмних засобів).

За природою походження джерела загроз поділяються на:

– природні (спричинені природними явищами, які не залежать від людини);

– штучні (спричинені діяльністю людини). Поділяють на навмисні, які направлені на порушення конфіденційності, цілісності та доступності інформації, а також поділяють на ненавмисні, які викликані помилками в апаратно-програмному забезпечені та діях персоналу

Джерелами загроз інформації виступають: люди, апаратно-програмні засоби та середовище, яке оточує ІТС та її компоненти, які можуть впливати на інформацію, як ззовні (зовнішні джерела загроз), так і з середини ІТС (внутрішні джерела загроз).

Перелік загроз та вразливостей для даної ІТС, наведений у табл. 2.15. В таблиці 2.15 не розглядаються загрози витоку інформації через перехоплення побічних електромагнітних випромінювань і наведень, акустоелектичних перетворень інформаційних сигналів та оптичні канали витоку.

Таблиця 2.15 – Перелік загроз та вразливостей

Вид загрози	Вразливості, що призведуть до реалізації загроз
Природні загрози	
Виникнення пожежі, або підтоплення	– недотримання норм пожежної безпеки персоналом підприємства, використання несправного обладнання; – розташування об’єкта на лівому березі м.Дніпро.
Антропогенні загрози	
Втрата засобів розмежування доступу (паролів від облікових записів та магнітних карток від СКУД)	– людський фактор (неуважність); – неналежне зберігання паролів від облікових записів та магнітних карток від СКУД.

Продовження таблиці 2.15 – Перелік загроз та вразливостей

Вид загрози	Вразливості, що призведуть до реалізації загроз
Несанкціоноване ознайомлення з ІзОД позаштатними працівниками за рахунок візуально-оптичного каналу	– відсутність належного догляду за зовнішніми працівниками.
Несанкціонований друк та копіювання ІзОД на сторонні зовнішні носії	– відсутність коректного розмежування доступу до інформації та «квот»; – відсутність шифрування інформації.
Використання неліцензійного ПЗ	– витік інформації через встановлення неліцензійного системного чи апаратного ПЗ.
Несанкціоновані дії по відношенню до інформації (модифікація, видалення, дублювання)	– відсутність шифрування інформації.
Ненавмисне розголошення конфіденційної інформації або інформації, що становить комерційну таємницю	– недостатній рівень підготовки персоналу з питань безпеки; – відсутність організаційних методів захисту від розголошення інформації; – людський фактор (неуважність) .

Продовження таблиці 2.15 – Перелік загроз та вразливостей

Вид загрози	Вразливості, що призведуть до реалізації загроз
Навмисне або ненавмисне зараження ПЗ комп'ютерними вірусами або шкідливими програмами через електронну пошту, флеш накопичувачами або мережу Інтернет	– людський фактор (неуважність); – вільний доступ до мережі Інтернет; – ненадійне антивірусне ПЗ; – відсутність політики використання зовнішніх носіїв; – вільний доступ до мережі інтернет.
Передача або копіювання конфіденційної інформації на електронну пошту або хмарне сховище, передача її онлайн меседжами	– відсутність коректного розмежування доступу та «квот». – вільний доступ до мережі Інтернет; – відсутність організаційних методів захисту від розголошення інформації; – відсутність протоколювання подій.
Ненавмисні помилки користувачів ІТС при роботі з ПЗ	– людський фактор (неуважність).
Відмова в роботі поштового сервісу	– використання сторонньої корпоративної пошти Outlook для отримання зовнішніх документів, звернень та скарг.
Відмова в роботі хостинг-сервера або несанкціонована модифікація інформації на ньому	– використання стороннього хостинг-сервера для сайту.

Продовження таблиці 2.15 – Перелік загроз та вразливостей

Вид загрози	Вразливості, що призведуть до реалізації загроз
Повторне використання об’єктів	– відсутність автоматизованого очищення оперативної пам’яті або ЖМД від інформації, яка зберігається від іншого користувача.
Втрата доступу до інформації	– відсутність автоматизованого відкату до попереднього БД технологічної інформації у попередній стан у разі технічного збою.
Модифікація журналу подій	– відсутність захисту журналу подій.
Техногенні загрози	
Відмова роботи мережі Інтернет або Інтернет обладнання	– відсутність резервного каналу зв’язку мережі Інтернет.
Збій або відмова системи електроживлення	– відсутність у доступній близькості іншого резервного джерела електричної енергії (другого вводу).
Хакерські атаки	– вимкнення оновлення антивірусного ПЗ.
Зношення носіїв інформації (ЖМД)	– втрата інформації через зношення носіїв інформації (ЖМД).

Для оцінювання рівня ймовірності реалізації загрози використаємо таке ранжування:

– 1 низька;

– 2 середня;

– 3 висока.

Для оцінювання рівня збитків від реалізації загрози використаємо таке ранжування:

– 1 низький;

– 2 середній;

– 3 високий.

Ймовірність реалізації загроз визначено експертним методом, на основі аналізу статистичних даних. Модель загроз наведено у табл. 2.16.

Таблиця 2.16 – Модель загроз

Вид загрози	Ймовір-ність	Рівень збитків	Рівень загрози		
			К	Ц	Д
Виникнення пожежі, або підтоплення	1	3	–	+	+
Втрата засобів розмежування доступу	3	2	+	+	+
Несанкціоноване ознайомлення з ІзОД позаштатними працівниками за рахунок візуально-оптичного каналу	1	2	+	–	–
Несанкціонований друк та копіювання ІзОД на сторонні зовнішні носії	3	2	+	–	–
Використання неліцензійного ПЗ	3	3	+	+	+
Несанкціоновані дії по відношенню до інформації (модифікація, видалення, дублювання)	2	3	+	+	+
Ненавмисне розголошення конфіденційної інформації або інформації, що становить комерційну таємницю	1	2	+	–	–
Навмисне або ненавмисне зараження ПЗ комп'ютерними вірусами або шкідливими програмами через електронну пошту, флеш накопичувачами або мережу Інтернет	3	2	+	+	+

Продовження таблиці 2.16 – Модель загроз

Вид загрози	Ймовір-ність	Рівень збитків	Рівень загрози		
			К	Ц	Д
Передача або копіювання конфіденційної інформації на електронну пошту або хмарне сховище, передача її онлайн меседжами	2	3	+	–	–
Ненавмисні помилки користувачів ІТС при роботі з ПЗ	2	1	–	+	+
Відмова в роботі поштового сервісу	2	1	+	–	–
Відмова в роботі хостинг-сервера або несанкціонована модифікація інформації на ньому	1	2	–	+	+
Повторне використання об’єктів	2	2	+	+	+
Втрата доступу до інформації	1	3	+	+	+
Модифікація журналу подій	1	3	+	+	+
Відмова роботи мережі Інтернет або Інтернет обладнання	2	2	–	–	+
Збій або відмова системи електроживлення	2	2	–	+	+
Хакерські атаки	2	2	+	+	+
Зношення носіїв інформації	1	2	–	+	+

Проаналізувавши загрози, можемо зробити висновок, що найбільш небезпечними загрозами для компанії є:

– втрата засобів розмежування доступу;

– несанкціонований друк та копіювання ІзОД на сторонні зовнішні носії;

– несанкціоновані дії по відношенню до інформації (модифікація, видалення, дублювання);

– навмисне або ненавмисне зараження ПЗ комп'ютерними вірусами або шкідливими програмами через електронну пошту, флеш накопичувачами або мережу Інтернет;

– передача або копіювання конфіденційної інформації на електронну пошту або хмарне сховище, передача її онлайн меседжами;

– повторне використання об'єктів;

– втрата доступу до інформації;

– модифікація журналу подій;

– хакерські атаки.

Реалізація даних загроз може призвести до повної або часткової втрати інформації, її пошкодженню або підміни. Таким чином, підприємство може понести фінансових втрат. Присутня необхідність забезпечення підвищених вимог до конфіденційності, цілісності та доступності.

2.9 Вибір профілю захищеності

Проаналізувавши модель загроз ІТС, можемо зробити висновок, що на підприємстві присутні загрози для всіх властивостей інформації. Відповідно до [6], для даного підприємства було обрано профіль захищеності 3.КЦД.1. Відповідно до [6], 3.КЦД.1 – функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка оброблюється в даній АС.

Автоматизована система являє собою організаційно-технічну систему, що об'єднує ОС, фізичне середовище, персонал і оброблювану інформацію.

АС підприємства – відноситься до АС «3» класу з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації.

Відповідно до НД ТЗІ 2.5-004-99 [11], функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів:

– конфіденційність – загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності.

– цілісність – загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності;

– доступність – загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності;

– спостереженість – ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості.

Беручі до уваги характеристики існуючою ІТС та згідно вимог до властивостей інформації, Відповідно до НД ТЗІ 2.5-005-99 [6], для даної АС обрано 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-1, НЦ-2, НТ-3}

Опис вимог до профілю захищеності ІТС наведено у табл. 2.17.

Таблиця 2.17 – Вимоги до профілю захищеності ІТС

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
Конфіден-ційності	Довірча конфіденційність	КД-2 (базова довірча конфіденційність)
Конфіден-ційності	Адміністративна конфіденційність	КА-2 (базова адміністративна конфіденційність)
	Повторне використання об'єктів	КО-1 (повторне використання об'єктів)
	Конфіденційність при обміні	КВ-2 (базова конфіденційність при обміні)

Продовження таблиці 2.17 – Вимоги до профілю захищеності ІТС

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
Цілісності	Довірча цілісність	ЦД-1 (мінімальна довірча цілісність)
	Адміністративна цілісність	ЦА-2 (базова адміністративна цілісність)
	Відкат	ЦО-1 (обмежений відкат)
	Цілісність при обміні	ЦВ-2 (базова цілісність при обміні)
Доступності	Використання ресурсів	ДР-1 (квоти)
	Відновлення після збоїв	ДВ-1 (ручне відновлення)
Спостере-женості	Реєстрація	НР-2 (захищений журнал)
	Ідентифікація і автентифікація	НИ-2 (одиночна ідентифікація і автентифікація)
	Достовірний канал	НК-1 (однонаправлений достовірний канал)
	Розподіл обов'язків	НО-1 (виділення адміністратора)
	Цілісність комплексу засобів захисту	НЦ-2 (КЗЗ з гарантованою цілісністю)
	Самотестування	НТ-3 (самотестування в реальному часі)

Опис кожного критерія обраного профіля:

КД-1, КД-2. Мінімальна, базова довірча конфіденційність. **Не реалізовано**. Потоками інформації від незахищених об'єктів до користувачів вже керує адміністратор.

КА-2. Базова адміністративна конфіденційність. **Умовно реалізовано.** В КЗЗ ІТС присутні апаратно-програмні засоби, для розмежування доступу між користувачами, групами користувачів та їх обліковими записами до певних каталогів файлової системи на ЖМД сервера. Каталоги файлової системи містять як ІзОД так і відкриту інформацію, яка потребує захисту. Розмежування доступу

до IP в ОС Microsoft Windows 10 Professional виконується системним адміністратором через процедуру керування доменами. Але розмежування доступу до периферійних пристроїв, а саме принтерів (П1, П2) відсутнє. Принтери підключені до комутатора (К1), всі користувачі знаючи IP адресу та модель принтеру можуть до нього під ’єднатися. Також відсутнє розмежування доступу користування флеш носіями. Кожен користувач має привілеї для імпорту та експорту інформації з флеш накопичувача. Необхідні умови виконуються: НО-1, НИ-1.

КА-3, КА-4. Повна, абсолютна адміністративна конфіденційність. **Не реалізовано.** Дана політика не може відноситися до всіх об’єктів КС.

КО-1. Повторне використання об’єктів. **Не реалізовано**. Сегменти оперативної пам’яті ПК не форматуються та залишаються доступними для іншого користувача у разі виходу з облікового запису. При завершені роботи система не форматує жорсткий диск на якому працював користувач. Тож, гарантувати те, що вся інформація стає повністю недоступною неможливо. Дана політика не може відноситися до всіх об’єктів КС. Необхідні умови відсутні.

КВ-1, КВ-2. Мінімальна, базова конфіденційність при обміні. **Не реалізовано**. Захист від НСД та ознайомлення зі змістом інформації, яка зберігається на ЖМД сервера або ЖМД для резервного копіювання відсутній. Для захисту інформації необхідно реалізувати її шифрування та розшифрування криптографічними ключами. Використання програмного шифрування файлів при виконанні резервного копіювання, передачі їх через флеш накопичувач не реалізоване.

ЦД-1. Мінімальна довірча цілісність. **Не реалізовано**. Потоками інформації від незахищених об’єктів до користувачів вже керує адміністратор.

ЦА-2. Базова адміністративна цілісність. **Умовно реалізовано.** В КЗЗ ІТС присутні апаратно-програмні засоби, для розмежування доступу між користувачами, групами користувачів та їх обліковими записами до певних каталогів файлової системи на ЖМД сервера. Каталоги файлової системи містять як ІзОД так і відкриту інформацію, яка потребує захисту. Розмежування доступу

до IP в ОС Microsoft Windows 10 Professional виконується системним адміністратором через процедуру керування доменами. Але розмежування доступу до периферійних пристроїв, а саме принтерів (П1, П2) відсутнє. Принтери підключені до комутатора (К1), всі користувачі знаючи IP адресу та модель принтеру можуть до нього під ’єднатися. Також відсутнє розмежування доступу користування флеш носіями. Кожен користувач має привілеї для імпорту та експорту інформації з флеш накопичувача. Необхідні умови виконуються: НО-1, НИ-1. Необхідні умови виконуються: НО-1, НИ-1.

ЦА-3, ЦА-4. Повна, абсолютна адміністративна цілісність. **Не реалізовано**. Дана політика не може відноситися до всіх об’єктів КС.

ЦО-1. Обмежений відкат. **Умовно реалізовано.** В ІТС апаратно-програмни засобами реалізоване автоматичне резервне копіювання інформації на ЖМД (HDD1, HDD2), резервне копіювання відбувається кожні 12 годин, згідно налаштувань в FreeFileSync. Відповідальність за резервне копіювання, згідно політики безпеки, несе системний адміністратор. Автоматизований відкат БД технологічної інформації у попередній стан у разі, якщо в послідовності виконання операцій, які зв’язані з встановлюванням захисту на каталог ЖМД виник технічний збій, не реалізований. Необхідні умови виконуються: НИ-1.

ЦВ-1. Мінімальна цілісність при обміні. **Не реалізовано**. В КЗЗ ІТС відсутня можливість виявлення фактів несанкціонованої модифікації інформації, яка зберігається на ЖМД серверів та ЖМД для резервного копіювання, а також факту її видалення або дублювання.

ДР-1. Квоти. **Не реалізовано**. В КЗЗ ІТС не реалізована послуга для запобігання захоплення користувачами надмірного обсягу ресурсів ЖМД комп’ютера.

ДВ-1. Ручне відновлення. **Реалізовано**. В результаті відмови КС або переривання обслуговування через відключення електропостачання, виходу з ладу одного з компонентів ІТС, випадкове натиснення кнопки вимкнення ПК, чи сервера в ІТС, системний адміністратор приводить КС до нормального функціонування, або стану з обмеженими умовами функціонування в режимі

ручного відновлення. Під час виконання ручного відновлення, деякий час КС може бути недоступний. Необхідні умови виконуються: НО-1.

ДВ-2, ДВ-3. Автоматизоване, вибіркове відновлення. **Не реалізовано**. В КЗЗ ІТС відсутні автоматизовані процедури та апаратно-програмні засоби для повернення КС до нормального функціонування.

НР-1. Зовнішній аналіз. **Реалізовано.** Журнал подій **в** ОС Microsoft Windows 10 Professional реєструє події, що мають безпосереднє відношення до ІБ. Журнал подій містить інформацію про дату, час, місце, тип та успішність, чи не успішність кожної зареєстрованої події. Необхідні умови виконуються: НИ-1.

НР-2. Захищений журнал. **Не реалізовано**. Вбудовані функції ОС Microsoft Windows 10 Professional не дозволяють захистити журнал подій від НСД або редагування.

НИ-2. Одиночна ідентифікація і автентифікація. **Реалізовано**. Реалізовано за допомогою стандартних засобів автентифікації та ідентифікації ОС Microsoft Windows 10 Professional – для користування АС необхідно спочатку ввести пароль доступу до облікового запису за допомогою клавіатури підключеної через USB, а саме – автентифікуватися. Необхідні умови виконуються: НК-1.

НИ-3. Множинна ідентифікація і автентифікація. **Не реалізовано**. Автентифікація проходить тільки одним захищеним механізмом.

НК-1. Однонаправлений достовірний канал. **Реалізовано**. Автентифікація користувача за допомогою захищеного механізму. Пароль для автентифікації вводиться через клавіатуру підключену через USB. При взаємодії користувача з КЗЗ організаційними шляхами гарантується, що в клавіатурі відсутні закладні пристрої (клавіатура розбиралася для перевірки системним адміністратором), купівля клавіатури створювалася методом «нецільової поставки». Пароль завдовжки 14 латинських та численних знаків, з великими там малими символами, вірогідність вводу правильного паролю, користувачем, який його не знає, сходиться до мінімуму. Необхідні умови відсутні.

НК-2. Двонаправлений достовірний канал. **Не реалізовано**. Зв'язок з використанням достовірного каналу не може ініціюватися КЗЗ. Обмін з

використанням достовірного каналу, що ініціює КЗЗ, не може бути однозначно ідентифікований як такий і відбутися тільки після позитивного підтвердження готовності до обміну з боку користувача.

НО-1. Виділення адміністратора. **Реалізована**. Політика розподілу обов'язків, що реалізується КЗЗ, визначає ролі адміністратора, звичайного користувача і притаманні їм функції. Реалізовано за допомогою внутрішніх систем розподілу обов'язків та політикою безпеки ОС Microsoft Windows 10 Professional. Необхідні умови виконуються: НИ-1.

НО-2. Розподіл обов'язків адміністраторів. **Не реалізовано**. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. В системі два адміністратори мають однакові привілеї системного адміністратора.

НЦ-1. КЗЗ з контролем цілісності. **Не реалізовано.** У разі порушення цілісності будь-якого з компонентів, в КЗЗ не реалізовано автоматичне відновлення окремого компонента, повідомлення про неправомірні дії адміністратора та можливість переведення КС до стану, з якого повернути її до нормального функціонування може тільки системний адміністратор.

НЦ-2. КЗЗ з гарантованою цілісністю. **Не реалізовано**. Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів, що не реалізовано.

НТ-3. Самотестування в реальному часі. **Реалізовано.** КЗЗ здатне виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Power-On Self-Test – самотестування при включенні. Перевірка апаратного забезпечення комп'ютера, яка виконується при його включенні. Виконується програмами, що входять в BIOS материнської плати. В процесі штатного функціонування відбувається: перевірка оновлення на останню версію встановленої ОС, оновлення баз та сигнатур встановленого антивіруса, перевірка цілісності реєстру, перевірка цифрових підписів сайтів, перевірка на програми шкідники у реальному часі. Необхідні умови виконуються: НО-1.

Г-2. Критерія гарантії. КЗЗ повинен реалізувати політики безпеки. Всі його компоненти повинні бути чітко визначенні.

2.10 Розробка КСЗІ

Заходи, які представлені в КСЗІ, спрямовані на зниження ризиків від реалізації загроз через вразливості ІТС, або повне виключення загроз, які проаналізовані в табл. 2.15 та табл. 2.16. В першу чергу необхідно ввести заходи для зниження рівня ймовірності реалізації загрози, що допоможе знизити рівень збитків від реалізації загрози або взагалі виключити загрозу зі списку можливих.

Для забезпечення ІБ використаємо апаратно-програмні засоби. Всі апаратно-програмні входять до списку дозволених ЗУ «Про Положення про технічний захист інформації в Україні» [12], затвердженого указом Президента України від 27 вересня 1999 року №1229.

На вибір засобу антивірусного захисту для впровадження зменшення рівня загроз вплинули такі фактори, як:

– вартість не повинна перевищувати середню вартість в сегменті;

– стабільна робота;

– надійність;

– своєчасне оновлення антивірусної бази;

– вплив на швидкість роботи;

– споживання ресурсів (оперативної пам’яті та процесора);

– функціональність;

– простота налаштування;

– наявність тестового періоду для впровадження в ІТС;

–відгуки користувачів на офіційних сайтах програмних засобів анти-вірусного захисту;

– термін дії повинен бути не менше ніж 6 місяців з моменту розробки КСЗІ.

В табл. 2.18 представлені програмні засоби антивірусного захисту, які мають експертний висновок про відповідність до вимог технічного захисту інформації.

Таблиця 2.18 – Програмні засоби антивірусного захисту

Назва продукту	Призначення	Термін дії день.місяць.рік.
Програмний комплекс антивірусного захисту «Avast Business Antivirus» версії 19.X.Y виробництва компанії AVAST Software s.r.o.	Відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Програмний комплекс антивірусного захисту «Avast Business Antivirus» версії 19». Технічні вимоги щодо захисту інформації від несанкціонованого доступу», сукупність яких визначається функціональним профілем захищеності {КА-2, ЦА-1, ЦО-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2}	Дійсний з 27.03.2019 до 27.03.2022
Програмний продукт антивірусного захисту ESET Endpoint Antivirus для Windows (EEA) версії 7.x виробництва компанії «ESET»	Відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Програмний продукт антивірусного захисту ESET Endpoint Antivirus для Windows (EEA) версії 7.x з системою централізованого керування антивірусним захистом корпоративних мереж ESET Security Management Center версії 7.x.»	Дійсний з 12.07.2019 до 12.07.2022

Продовження таблиці 2.18 – Програмні засоби антивірусного захисту

Назва продукту	Призначення	Термін дії день.місяць.рік.
Програмне забезпечення антивірусного захисту інформації «Zillya! Антивірус для Бізнесу» версії 1.1.xxxx.y виробництва ТОВ «ОЛАЙТІ СЕРВІС»	Відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Програмне забезпечення антивірусного захисту інформації «Zillya! Антивірус для Бізнесу». Технічні вимоги за критеріями технічного захисту інформації»	Дійсний з 28.05.2020 до 28.05.2023

Програмні засоби захисту інформації, які представлені в таблиці рекомендовані та дозволені державною службою спеціального зв'язку та захисту інформації України.

Антивірус «Zillya! Антивірус для Бізнесу» має привабливу середню вартість на ринку, але користується поганими відгуками, через нестабільну роботу та малу антивірусну базу.

Якщо обирати між антивірусами «Avast Business Antivirus» та «ESET Endpoint Antivirus». «ESET Endpoint Antivirus» гарантує, що сканування ваших шкідливих програм працює на вас. Функція "Idle Scanning" працює тільки в сплячому режимі або в режимі екранної заставки, що означає, що вона вам не завадить. Функція "Download Scans" перевіряє файли у міру їх завантаження, зупиняючи їх, якщо виявлена загроза. Технологія фільтрації електронної пошти та захисту від фішингу допомагає вам безпечно користуватися службами обміну повідомленнями. З іншого боку, Avast включає в себе широкий спектр

інструментів кібербезпеки – деякі за додаткову плату - які захищають вас від численних загроз. Функція «Пісочниця» означає, що нове ПЗ запускається в безпечному середовищі Avast, щоб уникнути прихованого зараження. Функція «Файловий шредер» повністю видаляє непотрібні файли, тому кіберзлочинці не зможуть отримати до них доступ. Сховище паролів забезпечує безпеку всіх ваших паролів, а протокол «Безпечний Wi-Fi» забезпечить захист вашого з'єднання.

Дивлячись на ринкову вартість, функціональність та відгуки про програмні засоби захисту інформації в мережі Інтернет, для забезпечення безпеки інформації від загрози ненавмисного або навмисного зараження ПЗ комп'ютерними вірусами, або шкідливими програмами через електронну пошту, сторонні зовнішні носії або мережу Інтернет було обрано програмний продукт антивірусного захисту «ESET Endpoint Antivirus».

Для захисту конфіденційної інформації від витоку, розмежування обов'язків для користувачів та груп користувачів, розмежування доступу користувачів до обраних каталогів інформації, контролю за виведенням інформації на друк, блокуванню USB портів системних блоків від використання незареєстрованих зовнішніх носіїв, контролю за використанням дискового простору користувачами (квот), контролю цілісності і самотестування комплексу при старті, відновлення функціонування комплексу після збоїв виявлення підозрілих дій в мережі Інтернет, економії коштів для відновлення файлів, шифрування даних, в табл. 2.19 запропоновано наступні програмні засоби захисту обігу файлів.

Таблиця 2.19 – Програмні засоби захисту обігу файлів

Назва продукту	Призначення	Термін дії день.місяць.рік.
Система захисту інформації ЛОЗАТМ-1, версія 4.X.Y виробництва ТОВ «Науково-дослідний інститут «Автопром»	Відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених в технічному завданні «Система захисту інформації ЛОЗАТМ-1, версія 4.X.Y. Технічне завдання. Редакція 4».	Дійсний з 02.04.2020 до 02.04.2023
Програмний продукт захисту інформації Safetica Full DLP версії 9.x, виробництва компанії Safetica Technologies (Чехія)	Відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Програмний продукт захисту інформації Safetica Full DLP версії 9.x. Технічні вимоги».	Дійсний з 24.01.2020 до 24.01.2023

Продовження таблиці 2.19 – Програмні засоби захисту обігу файлів

Назва продукту	Призначення	Термін дії день.місяць.рік.
Засіб технічного захисту інформації від несанкціонованого доступу «Комплекс «Гриф» версії 4» розробки ТОВ Інститут комп'ютерних технологій	Відповідає вимогам нормативних документів з технічного захисту інформації в обсязі функцій, зазначених у документі «Засіб технічного захисту інформації від несанкціонованого доступу «Комплекс «Гриф». Версія 4. Технічне завдання UA.21541987.00025-01 90 01».	Дійсний з 08.10.2020 до 08.10.2023

Програмні засоби представлені в табл. 2.20 було проаналізовано, для обраного профілю захищеності та реалізації всіх вимог до нього, до уваги було взято засіб технічного захисту інформації від НСД комплекс «Гриф» версії 4. Комплекс «Гриф» версії 4 у порівнянні з іншими комплексами представленими у табл. 2.20 забезпечує реалізацію необхідних послуг:

– КА-2, ЦА-2, комплекс дозволяє системному адміністратору розмежувати доступ користувачів до:

1) Каталогів та файлів на ЖМД, що містять ІзОД;

2) Системного та прикладного ПЗ;

3) Периферійних пристроїв (принтерів та флеш накопичувачів).

(на відміну від системи захисту інформації ЛОЗАТМ-1 та програмного продукту захисту інформації Safetica Full DLP версії 9.х.);

– КО-1, послуга реалізується шляхом очищення оперативної пам'яті ПК перед виділенням його іншому користувачу. Також сегменти ЖМД очищуються

від файлів попереднього користувача, для уникнення можливості доступу до них наступним користувачем;

– КВ-1, КВ-2, комплекс забезпечує захист від несанкціонованого ознайомлення зі змістом інформації, яка зберігається на ЖМД сервера або ЖМД для резервного копіювання, шляхом впровадження механізмів "прозорого" розшифрування / шифрування даних в момент їх читання / запису і реалізації відповідної схеми управління криптографічними ключами. В якості алгоритму шифрування / розшифрування даних використовується алгоритм гамування зі зворотним зв'язком, встановлений ДСТУ 7624: 2014 "Інформаційні технології;

– ЦО-1, комплекс забезпечує можливість автоматизованого здійснення відкату БД у попередній стан у разі, якщо в послідовності виконання операцій, які зв’язані з встановлюванням захисту на каталог ЖМД виник технічний збій;

– ЦВ-1, комплекс забезпечує можливість виявлення фактів несанкціонованої модифікації інформаційних об'єктів, яка зберігається на ЖМД серверів та ЖМД для резервного копіювання, а також факту її видалення або дублювання;

– НР-2, комплекс дозволяє забезпечити захист журналу подій від НСД, редагування та видалення;

– НЦ-1, комплекс дозволяє автоматично переводити систему в стан, з якого її може вивести тільки системний адміністратор у разі виявлення несанкціонованих дій по відношенню до інформації.

2.11 Розробка матриці доступу

Під час обстеження ОІД, була наведена табл. 2.6 розмежування доступу користувачів до інформації, після проведення аналізу загроз та вразливостей було визначено, що користувачі мають надлишкові права доступу до операцій з файлами, що є джерелом загрози для підприємства. Тож, відповідно до політики безпеки розмежування доступу дана матриця була переглянута у табл. 2.20 для виключення випадків наявності надлишкових прав у користувачів.

Таблиця 2.20 – Запропонована матриця розмежування доступу

Інформація	Користувач					
	Директор	Керівник	Заступник керівника	Оператор	Бухгалтер	Сис. Адмін.
1	ЧРВДПС	ЧРДПС	ЧД	–	ЧРДПС	П
2	ЧРВДПС	ЧД	–	–	ЧРДПС	П
3	ЧРВДПС	ЧД	ЧРВДПС	–	ЧД	П
4	ЧРВДПС	ЧДП	ЧДП	ЧП	ЧДП	ЧРВДПС
5	ЧРВДПС	ЧРДП	ЧДП	ЧП	ЧДП	ЧРВДПС
6	ЧРВДПС	ЧРДПС	ЧРДПС	ЧРС	–	ЧРВДПС
7	ЧРВДП	ЧДП	ЧДП	–	ЧРДПС	П
8	ЧРВДПС	ЧД	–	–	–	ЧРВДПС
9	ЧРВДПС	ЧД	–	–	–	ЧРВДПС
10	ЧП	–	–	–	–	ЧРВП
11	ЧРВДП	–	–	–	ЧРДП	П
12	ЧРВДП	ЧРДП	ЧРДП	ЧРП	–	ВП
13	–	–	–	–	–	ЧВП
14	–	–	–	–	–	РВПС
15	ЧРВДПС	–	–	–	–	ЧРВПС

Операції з файлами: Ч – читання; Р – редагування; В – видалення; Д – друкування; П – передача (імпорт, експорт); С – створення;

Цифрами від 1 до 12 позначено інформацію згідно таблиці 2.5.

2.12 Розробка політики безпеки

Відповідно до НД ТЗІ 1.1-003-99 [9], ПБ інформації – сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

Беручи до уваги те, що в ІТС оброблюється ІзОД, для зниження ризиків реалізації загроз через вразливості та досягнення необхідного рівня захищеності

інформації необхідно розробити політики безпеки за мінімальних затрат і допустимого рівня обмежень на технологію обробки цієї інформації в ІТС.

Розробимо політики безпеки для зниження ймовірності реалізації загроз, наведених в табл.2.17.

2.12.1Політика розмежування прав доступу до інформації

Політика розмежування прав доступу до інформації відноситься до кожного користувача ІТС

Мета політики безпеки.

Відповідно до НД ТЗІ 1.4-001-2000 [10], повинні виконуватися наступні правила:

– кожен користувач повинен мати свій унікальний логін і пароль до облікового запису. Паролі створюються та видаються користувачам системним адміністратором. Після отримання паролю, користувачу, при першій авторизації до облікового запису, необхідно змінити пароль на свій особистий, який відповідає параметрам унікальності, необхідною довжиною (12 символів), містить латинські літери верхнього (A-Z) та нижнього (a-z) регістру, складається з використанням цифр (0-9), не повторює ім'я облікового запису, не складається з символів (~!@#$%^&*-+='|\() {} []:;"' <>,.? /);

– кожний користувач закріплюється за одним робочим місцем та несе відповідальність за його працездатність. Перед використанням ІТС користувач повинен ознайомитися з посадовими інструкціями та правилами компанії, про що поставити свій підпис, що свідчить про ознайомлення з політикою безпеки та про те, що користувач зобов'язується виконувати встановлені цим документом правила;

– для виключення випадків неавторизованого доступу до інформації, документів та інших ресурсів, керування механізмами захисту здійснюється системним адміністратором за розпорядженням директора;

– відповідальність за створення резервний копій несе системний адміністратор;

– пароль від облікового запису кожного користувача в ІТС повинен змінюватися кожні 42 дні (або раніше, у випадку втрати або розголошення). Якщо користувач підозрює, що його пароль дізналися, необхідно негайно повідомити про це системного адміністратора та змінити пароль.

2.12.2Політика антивірусного захисту

Політика антивірусного захисту включає в себе інструкції та правила застосування антивірусного ПЗ для користувачів ІТС для уникнення випадків зараження ПЗ комп'ютерними вірусами.

Правила для користувачів ІТС:

– перед початком роботи в системі, користувачеві необхідно переконатися, що антивірусна програма увімкнена та має активовану ліцензію.

– заборонено завантажувати файли з невідомих чи підозрілих джерел;

– заборонено відкривати та переглядати файли, що прикріпленні до електронного листа в Outlook, яке надійшло від підозрілого або ненадійного джерела. Користувачу необхідно одразу видалити даний електронний лист;

– у разі виникнення сумнівів з надійності файлу, необхідно просканувати його на наявність вірусів.

– відповідальність за дотримання та виконання правил захисту від зараження ОТЗ або ДТЗ покладається на всіх користувачів ІТС.

Правила для системного адміністратора:

– регулярно (кожні три місяці) перевіряти всі комп'ютери, зовнішні ЖМД та флеш носії в ІТС на наявність вірусів через антивірусну програму в ІТС. Якщо системний адміністратор запідозрить, що в ІТС наявні віруси, перевірку приладів, які відносяться до ОТЗ та ДТЗ необхідно повести раніше запланованої;

– у випадку, якщо вірус уразив одну або більше зі встановлених програм, знищення вірусу виконується шляхом видалення файлу вірусу та ураженої програми на диску використовуючи встановлене антивірусне ПЗ. Після видалення файлу вірусу та ураженої програми на диску необхідно відновити роботу програми, використовуючи резервну копію і ще раз виконати перевірку на

наявність вірусів через встановлене антивірусне ПЗ.

– відповідальність за проведення заходів захисту інформації в ІТС на наявність вірусів та програм шкідників покладається на системних адміністраторів ІТС.

2.12.3 Політика використання флеш накопичувачів для передачі даних між ПК та ЖМД для резервних копій в ІТС

Політика використання флеш накопичувачів та ЖМД для резервних копій в ІТС регламентує використання в ІТС тільки зареєстрованих носіїв інформації для максимального виключення випадків несанкціонованого копіювання інформації та зараження ПЗ.

Зареєстровані флеш накопичувачів використовуються для циркуляції та передачі інформації в межах ІТС, а також для встановлення ОС та ПЗ. ЖМД використовуються для зберігання резервних копій інформації. Флеш накопичувачі та ЖМД реєструються в КЗЗ системним адміністратором. Доступ до зареєстрованих флеш накопичувачів та ЖМД має системний адміністратор та директор.

Правила використання зареєстрованих флеш накопичувачів та ЖМД:

– повинні зберігатися в зачиненому сейфі, використовуватися тільки за призначенням та тільки уповноваженими особами на це, а саме системними адміністраторами та директором;

– повинні бути записані в перелік інвентаризаційної відомості;

– заборонено передавати носії інформації іншим користувачам ІТС для будь-який цілей;

– дозволено використовувати зареєстровані флеш накопичувачі для копіювання ІзОД з одного комп'ютера до іншого, при умові, якщо перший та другий є складовими ІТС;

– інформація на зареєстрованих флеш накопичувачах та ЖМД повинна зберігатися у зашифрованому вигляді;

– відповідальність за зберігання флеш накопичувачів та ЖМД покладається

на директора.

2.13 Висновок до другого розділу

В спеціальній частині кваліфікаційної роботи наведені загальні відомості про підприємство. Було виконано обстеження фізичного середовища ІТС, обчислювальної системи, інформаційного середовища. Проаналізовано технологію обробки інформації, середовище користувачів ОІД, загрози та вразливості, модель порушника, обрано профіль захищеності, виконано етап розробки КСЗІ та політики безпеки.

Відповідно до проведеного аналізу, було запропонована матриця розмежування доступу, антивірусне ПЗ та засіб технічного захисту інформації від НСД для впровадження КЗСИ та політики безпеки.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічного розділу є розрахунок капітальних витрат на придбання та запровадження складових КСЗІ, розрахунок річних експлуатаційних витрат на утримання та обслуговування функціонування КСЗІ, визначення річного економічного ефекту від впровадження КСЗІ, визначення та аналіз показників економічної ефективності від впровадження КСЗІ.

Економічно доцільним слід вважати, якщо витрати на забезпечення ІБ не перевищують збитків від реалізації загрози через вразливості.

3.1 Визначення витрат на розробку КСЗІ

Трудомісткість розробки КСЗІ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки). Розрахунок проводиться за формулою (3.1):

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

$$t=24+16+16+20+12+14+17=119 \text{ годин;}$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку КСЗІ, становить 24 годин;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації, становить 16 годин;

$t_{а}$ – тривалість процесу аналізу ризиків, становить 16 годин;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту, становить 20 годин;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації, становить 12 годин;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації, становить 14 годин;

$t_{д}$ – тривалість документального оформлення КСЗІ, становить 17 годин;

3.2 Розрахунок витрат на створення елементів КСЗІ

Витрати на розробку КСЗІ $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки КСЗІ $З_{мч}$. Розрахунок проводиться за формулою (3.2):

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

$$К_{рп} = 19873 + 1042{,}44 = 20915{,}44 \text{ грн;}$$

Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою (3.3):

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

$$З_{зп} = 119 * 167 = 19873 \text{ грн;}$$

де t – загальна тривалість розробки КСЗІ, годин;

$З_{іб}$ – середньогодинна заробітна плата спеціаліста з ІБ з нарахуваннями, складає 167 грн/годину.

Вартість машинного часу для розробки КСЗІ на ПК визначається за формулою (3.4):

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

$$З_{мч} = 119 * 8{,}76 = 1042{,}44 \text{ грн;}$$

де t – трудомісткість розробки КСЗІ на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою (3.5):

$$С_{мч} = P * t_{нал} * С_е + \frac{Ф_{зал} * Н_а}{F_р} + \frac{K_{лпз} * Н_{апз}}{F_р}, \text{ грн;} \quad (3.5)$$

$$С_{мч} = 0,7 * 2 * 1,68 + \frac{13571 * 0,5}{1920} + \frac{11070 * 0,5}{1920} = 2,35 + 3,53 + 2,88 = 8,76 \text{ грн;}$$

де Р – встановлена потужність ПК, становить 0,7кВт (два блоки живлення по 350 Вт);

$t_{нал}$ – кількість задіяних робочих станцій при розробці КСЗІ, було задіяно 2 робочі станції;

$С_е$ – тариф на електричну енергію, 1,68 грн/кВт*година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, (комп'ютер введений в експлуатацію 2 місяці тому, первісна вартість становить 14805грн, мінімальний термін корисного використання – 24 місяці.)

Накопичена амортизація: $14805 * 2/24 = 1234$ грн;

$Ф_{зал} = 14805 - 1234 = 13571$ грн;

$Н_а$ – річна норма амортизації на ПК (річна норма амортизації визначається діленням 100% на кількість років корисного використання);

$Н_а = (100\%)/2 = 5\%$;

$Н_{апз}$ – річна норма амортизації на ліцензійне ПЗ, частки одиниці, становить 5%;

$K_{лпз}$ – вартість ліцензійного ПЗ, становить 11070 грн;

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

$F_р$= 1920;

У табл. 3.1 наведений перелік ліцензійного ПЗ, що планується для закупівлі та впровадження в КСЗІ. Вартість вказана за ліцензію терміном на 12 місяців. Вартість подовження ліцензії на 12 місяців для комплексу «Гриф» версії 4 складає 800 грн, для ESET NOD32 Antivirus 4060 грн.

Таблиця 3.1 – Вартість ПЗ що планується для закупівлі

Назва	Вартість, грн
Комплекс «Гриф» версії 4	7010
ESET NOD32 Antivirus	4060
Загальна сума:	11070

У табл. 3.2 розраховано первісну вартість комплекту ПК для розрахунку залишкової вартості ПК на поточний рік.

Таблиця 3.2 – Первісна вартість комплекту ПК

Назва комплектуючого	Комп'ютерні комплектуючі	Вартість нового комплектуючого, грн
Процесор	Intel Core i3-7100 (Kaby Lake)	4393
Материнська плата	MSI H310M PRO-VDH Plus	1493
Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	1599
Оперативна пам'ять	HyperX DDR4-2666МГц 8 Гб	1486
Блок живлення	GameMax VP-350 350W	668
Корпус	Aerocool Split-A-BK-v1 Black	999
Монітор	Logitech K120	299
USB клавіатура	Philips 227E	3599
USB миша	Logitech M100	269
Загальна сума:		14805

Планується використання комп'ютерів, які вже закуплені та встановлені на підприємстві, тому додаткових витрат на закупку обладнання не виникає.

3.3 Розрахунок капітальних (фінансових) витрат

Капітальні (фіксовані) витрати на проектування та впровадження системи ІБ розраховують за формулою (3.6):

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

$$К = 20915{,}44 \ + 11\,070 + 0 + 0 + 6400 + 0 = 38385{,}44, \text{грн};$$

де $К_{рп}$ – витрати на розробку КСЗІ, становлять 20915,44 грн;

$К_{зпз}$ – вартість закупівлі ліцензійного основного й додаткового ПЗ, становить 11 070 грн;

$К_{пз}$ – вартість створення основного й додаткового ПЗ, ПЗ не створюється;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, планується використання вже існуючих;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, становить 6400 тис. грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, становить 0 грн, питанням встановлення обладнання та налагодження системи інформаційної безпеки займаються системні адміністратори;

3.4 Розрахунок річних експлуатаційних витрат

Річні поточні (експлуатаційні) витрати на функціонування системи ІБ розраховуються за формулою (3.7):

$$С = С_{в} + С_{к} + С_{ак}, \quad (3.7)$$

$$С = 4860 + 152684{,}86 + 800 = 158344{,}86 \text{ грн};$$

де $С_{в}$ – витрати на оновлення й модернізацію системи ІБ;

$С_{в} = \ 290 * 14 + 800 \ = \ 4860$ грн;

Вартість подовження ліцензії на 12 місяців для комплексу «Гриф» версії 4 складає 800 грн, для ESET NOD32 Antivirus 4060 грн.

$С_{ак}$ – витрати викликані активністю користувачів системи, що складають 800 грн.

$С_к$ – це витрати на керування системою ІБ, розрахунок відбувається за наступною формулою (3.8):

$$С_к = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос}; \quad (3.8)$$

$$С_к = 6400 + 5535 + 99198 + 21823{,}56 + 19\,353{,}6 + 0 + 374{,}7;$$

$$С_к = 152\,684{,}86 \text{ грн};$$

де $С_н$ – це витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо, становлять 6400 грн;

$С_а$ – річний фонд амортизаційних відрахувань. Використовуються лише програмні засоби, термін корисного використання програмних засобів 2 роки.

$С_а = 11\,070/2 = 5535$ грн;

$С_з$ – це річний фонд заробітної плати інженерно–технічного персоналу, що обслуговує систему інформаційної безпеки , визначається за формулою (3.9):

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

$$С_з = (360720 + 36072) * 0{,}25 = 99\,198\text{ , грн};$$

де $З_{осн}$ – основна заробітна складає 30060 грн на місяць, відповідно 360 720 грн на рік;

$З_{дод}$ – додаткова заробітна складає 10% від 30060 грн на місяць, відповідно 36072 грн на рік.

Виконання інженерно-технічних робіт з налаштування комплексу «Гриф» версії 4 потребує залучення спеціаліста ІБ на 0,25 ставки.

Ставка ЄСВ з 01.01.2016 для всіх категорій платників складає 22%.

$С_{єв}$= 99 198*0,22 = 21 823,56 грн;

$С_{ел}$ – це вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року, визначається за формулою (3.10):

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

$$С_{ел} = 6 * 1920 * 1.68 = 19\ 353{,}6 \text{ грн;}$$

де Р – встановлена потужність апаратури інформаційної безпеки, 0,35 Вт для одного ПК, для всього комплексу враховуються всі 14 ПК та 3 сервери, тобто 6 кВТ;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки складає 1920 год;

$Ц_е$ – тариф на електроенергію, 1,68 грн/кВт годин;

$С_о$ – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування та сертифікацію обслуговуючого персоналу, сторонні організації не залучуються;

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються за даними організації або у відсотках від вартості капітальних витрат, що складає 1% від суми капітальних інвестицій:

$$С_{тос} = 37470{,}76 * 0{,}01 = 374{,}7 \text{ грн;}$$

3.5 Оцінка величини збитку

Можливо виділити такі види збитку, що можуть вплинути на ефективність КСІБ:

– порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);

– порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);

– порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);

– порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

Для розрахунку вартості збитку від атаки можна застосувати наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

$t_{П}$ – час простою вузла корпоративної мережі внаслідок атаки, 1 години;

$t_{В}$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 4 години;

$t_{ВИ}$ – час повторного введення загубленої інформації співробітниками атакованого вузла корпоративної мережі, 3 години;

$З_{с}$ – заробітна плата співробітників атакованого вузла корпоративної мережі, 179340 грн на місяць;

$Ч_{о}$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 2 особи;

$Ч_{с}$ – чисельність співробітників атакованого вузла корпоративної мережі, 9 осіб;

О – обсяг продажів атакованого вузла корпоративної мережі, 8725742 грн. на рік;

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

i – число атакованих вузлів корпоративної мережі, 1 вузол;

n – середнє число атак на рік, 7 атак.

Упущена вигода від простою атакованого вузла корпоративної мережі визначається за формулою (3.11):

$$U = П_{п} + П_{в} + V; \quad (3.11)$$

де $П_{п}$ – оплачувані втрати робочого часу та простої співробітників

атакованого вузла корпоративної мережі, грн;

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

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

Втрати від зниження продуктивності співробітників атакованого вузла корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки, визначаються за формулою (3.12):

$$П_п = \frac{\sum З_с}{F} * t_П; \quad (3.12)$$

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

Розрахунок витрат на заробітну плату співробітників за місяць з нарахуванням ЄСВ наведено в табл. 3.3.

Таблиця 3.3 – Розрахунок витрат на заробітну плату співробітників за місяць з нарахуванням ЄСВ

Посада	Кількість співробіт-ників, осіб	Місячна заробітна плата, грн	Витрати на заробітну плату, грн	Єдиний соціальний внесок, грн	Витрати на заробітну плату з урахуванням ЄСВ, грн
1	2	3	4	5	6
Директор	1	17000	17000	3740	20740
Бухгалтер	2	12500	25000	5500	30500
Керівник	1	14000	14000	3080	17080

Продовження таблиці 3.3 – Розрахунок витрат на заробітну плату співробітників за місяць з нарахуванням ЄСВ

1	2	3	4	5	6
Заступник керівника	1	12500	12500	2750	15250
Оператор	5	9500	47500	10450	57950
Системний адміністратор	2	15500	31000	6820	37820
Загальна сума:					179340

Відповідно до формули (3.12), втрати від зниження продуктивності співробітників атакованого вузла, становлять:

$$П_п = \frac{179340}{176} * 1 = 1018{,}98 \text{ грн};$$

Витрати на відновлення працездатності вузла корпоративної мережі включають кілька складових, визначаються за формулою (3.13):

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

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

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

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

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$, визначаються за формулою (3.14):

$$П_{ви} = \frac{\sum З_с}{F} * t_{ви}; \quad (3.14)$$

$$П_{ви} = (179340/176) * 3 = 3056{,}93 \text{ грн};$$

Витрати на відновлення вузла корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати системних адміністраторів, розраховується за формулою 3.15:

$$П_{пв} = \frac{\sum З_о}{F} * t_в; \quad (3.15)$$

$$П_{пв} = \frac{37820}{176} * 4 = 859{,}54 \text{ грн};$$

де $З_о$ – місячна заробітна плата системних адміністраторів з нарахуванням єдиного соціального внеску, грн на місяць.

Визначимо вартість відновлення працездатності вузла корпоративної мережі за формулою (3.13):

$$П_в = 3056{,}93 + 859{,}54 + 0 = 3916{,}47 \text{ грн};$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла корпоративної мережі визначаються виходячи із середньо годинного обсягу продажів і сумарного часу простою атакованого вузла корпоративної мережі, визначаються за формулою (3.16):

$$V = \frac{О}{F_г} * (t_п + t_в + t_{ви}); \quad (3.16)$$

$$V = \frac{8725742}{2080} * (1 + 4 + 3) = 33560{,}55 \text{ грн};$$

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

Визначимо упущену вигоду від простою атакованого вузла корпоративної

мережі за формулою (3.11):

$$U = 1018{,}98 + 3916{,}47 + 33560{,}55 = 38496 \text{ грн.}$$

Таким чином, загальний збиток від атаки на вузол корпоративної мережі організації складе, визначимо за формулою (3.17):

$$\text{B} = \sum_{\text{i}} * \sum_{\text{n}} * \text{ U}; \quad (3.17)$$
$$\text{B} = 1 * 7 * 38496 = 269472 \text{ грн};$$

3.6 Загальний ефект від впровадження системи ІБ

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки визначається за формулою (3.18):

$$E = \text{B} * \text{R} - \text{C}; \quad (3.18)$$
$$E = 269472 * 0{,}7 - 158344{,}86 = 30285{,}54 \text{ грн};$$

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

R – очікувана ймовірність атаки на вузол корпоративної мережі, частки одиниці;

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

3.7 Визначення та аналіз показників економічної ефективності системи ІБ

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломної роботи, здійснюється на основі визначення та аналізу наступних показників:

1) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

2) термін окупності капітальних інвестицій T_o.

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

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на вузол корпоративної мережі.

Коефіцієнт повернення інвестицій ROSI визначається за формулою (3.19):

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

$$ROSI = \frac{30285,54}{38385,44} = 0,79, \text{ частки одиниці;}$$

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

К – капітальні інвестиції, що забезпечили цей ефект, тис. грн

Проект визначається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції, визначається за формулою (3.20):

$$ROSI > \frac{N_{\text{деп}} - N_{\text{інф}}}{100}, \text{ частки одиниці;} \quad (3.20)$$

$$0,79 > \frac{10\% - 5\%}{100}, \text{ частки одиниці;}$$

$$0,79 > 0,05, \text{ частки одиниці;}$$

де $N_{\text{деп}}$ – річна депозитна ставка, 10%;

$N_{\text{інф}}$ – річний рівень інфляції, 5%;

Останнім пунктом розрахування витрат на реалізацію КСЗІ буде прорахунок терміну окупності, який представляє собою час, необхідний для окуплення встановлених систем ІБ і впровадження політик. Термін окупності розраховується за формулою (3.21):

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

$$T_o = \frac{1}{0{,}79} = 1{,}27 \text{ року.}$$

3.8 Висновок

Відповідно до отриманих даних під час розрахунку економічної частини, капітальні витрати на проектування та впровадження системи ІБ становлять – 38385,44 грн, експлуатаційні витрати на функціонування системи ІБ – 158344,86 грн. Відповідно до розрахунків, створені елементи КСЗІ є доцільними з економічної точки зору.

Загальний збиток від атак на вузол корпоративної мережі організації склав 269472 грн. Загальний ефект від впровадження системи ІБ склав 30285,54 грн. Відповідно до коефіцієнту ROSI, який становить 0,79 частки одиниці – створені елементи КСЗІ є цілком доцільними. Термін окупності елементів КСЗІ становить 1,27 року.

ВИСНОВКИ

У першому розділі розглянуто питання актуальності впровадження КСЗІ в інформаційно-телекомунікаційну систему приватного підприємства, наведено аналіз нормативно-правової бази в сфері захисту інформації, дано визначення поняттю ОІД, проаналізований процес обстеження середовища функціонування ІТС, розглянута модель загроз та модель порушника, дано визначення поняттю політика безпеки та виконано постановку задачі

В спеціальній частині кваліфікаційної роботи наведені загальні відомості про ОІД. Представлена організаційна структура підприємства. Було виконано обстеження фізичного середовища ІТС. Виконане обстеження обчислювального середовища та інформаційних потоків. Проаналізовано технологію обробки інформації та вимоги до її захисту. Проаналізовано середовище користувачів ОІД та наведена матриця розмежування доступу користувачів до інформації. Були виявлені загрози та вразливості для інформаційної безпеки, розроблена модель загроз та модель порушника, обрано профіль захищеності, виконано етап розробки КСЗІ та політики безпеки, а саме визначені програмні засоби (антивірусне ПЗ та засіб технічного захисту інформації від НСД), які рекомендовані для впровадження в ІТС підприємства.

Відповідно до проведеного аналізу, була запропонована нова матриця розмежування доступу користувачів до інформації, через те, що користувачі мають надлишкові права доступу до операцій з файлами, що є джерелом загрози для підприємства.

В економічному розділі було обґрунтовано доцільність витрат на розробку КСЗІ, а також проведені розрахунки капітальних та експлуатаційних витрат, оцінено величину можливого збитку від атаки, визначено ефект від впровадження КСЗІ для ІБ, а також проаналізована економічна ефективність системи захисту інформації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про інформацію» [Електронний ресурс] – №2657-XII – 02.10.1992 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12#Text\.

2. Закон України «Про доступ до публічної інформації» [Електронний ресурс] – №2939-VI – 13.01.2011 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

3. Закон України «Про захист персональних даних» [Електронний ресурс] – №524-IX – 04.03.2020 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

4. Закон України «Про захист інформації в ІТС» [Електронний ресурс] – №1170-VII – 27.03.2014 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

5. Цивільний Кодекс України «Поняття комерційної таємниці» [Електронний ресурс] – №611 – 09.08.1993 – Режим доступу до ресурсу: https://legalexpert.in.ua/komkodeks/gk/79-gk/867-505.html.

6. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [Електронний ресурс] – №172 – 15.10.2008 – Режим доступу до ресурсу: https://tzi.ua/assets/files/НД-ТЗІ-2.5-005--99.pdf.

7. НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці» [Електронний ресурс] – №215 – 15.04.2013 – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.6-005-2013.pdf

8. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [Електронний ресурс] – №806 – 28.12.2012 – Режим доступу до ресурсу: https://tzi.com.ua/downloads/3.7-003-2005.pdf.

9. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [Електронний ресурс] – №22 – 28.04.1999 – Режим доступу до ресурсу: https://tzi.ua/assets/files/1.1_003_99.pdf.

10. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» [Електронний ресурс] – №806 – 28.12.2012 – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.4-001-2000.pdf.

11. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [Електронний ресурс] – №806 – 28.12.2012– Режим доступу до ресурсу: https://tzi.ua/assets/files/НД-ТЗІ-2.5-004-99.pdf.

12. Закон України «Про Положення про технічний захист інформації в Україні» [Електронний ресурс] – №1229-IXIX – 04.05.2008 – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1229/99#Text.

13. 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.

14. Методичні вказівки до виконання економічної частини дипломного проекту /Упоряд.: Д. П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019. – 16 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних позначень	2	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1. Стан питання. Постановка задачі	9	
6	А4	Розділ 2. Спеціальна частина	59	
7	А4	Розділ 3. Економічний розділ	14	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А. Відомість матеріалів кваліфікаційної роботи	2	
11	А4	Додаток Б. Ситуаційний план ОІД	2	
12	А4	Додаток В. Генеральний план ОІД	3	
13	А4	Додаток Г. Призначення кімнат та доступ до них	2	
14	А4	Додаток Ґ. Перелік ОТЗ	6	
15	А4	Додаток Д. Перелік ДТЗС	8	
16	А4	Додаток Е. Характеристика складу апаратних засобів ОТЗ	4	
17	А4	Додаток Є. Перелік ПЗ встановленого на ОТЗ	1	

Продовження ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
18	А4	Додаток Ж. Акт категоріювання об’єкта	1	
19	А4	Додаток З. Перелік документів на оптичному носії	1	
20	А4	Додаток И. Відгук керівника економічної частини	1	
21	А4	Додаток І. Відгук керівника кваліфікаційної роботи	1	

ДОДАТОК Б. Ситуаційний план ОІД

Рисунок Б.1 – Ситуаційний план ОІД

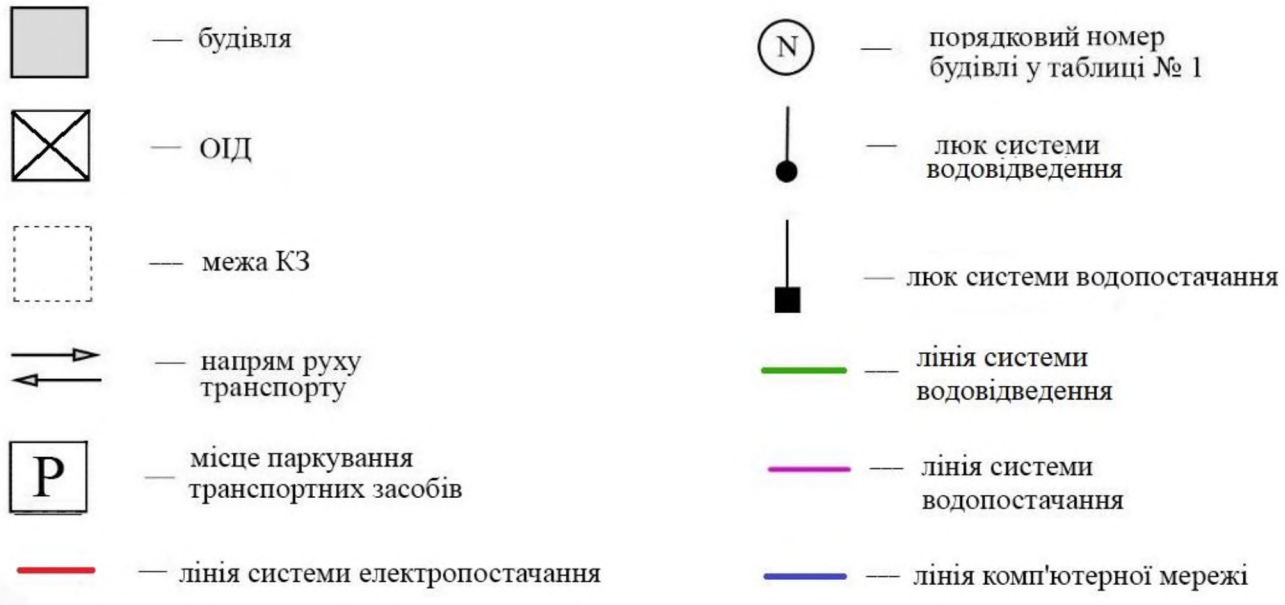

Рисунок Б.2 – Умовні позначення до ситуаційного плану ОІД

ДОДАТОК В. Генеральний план ОІД

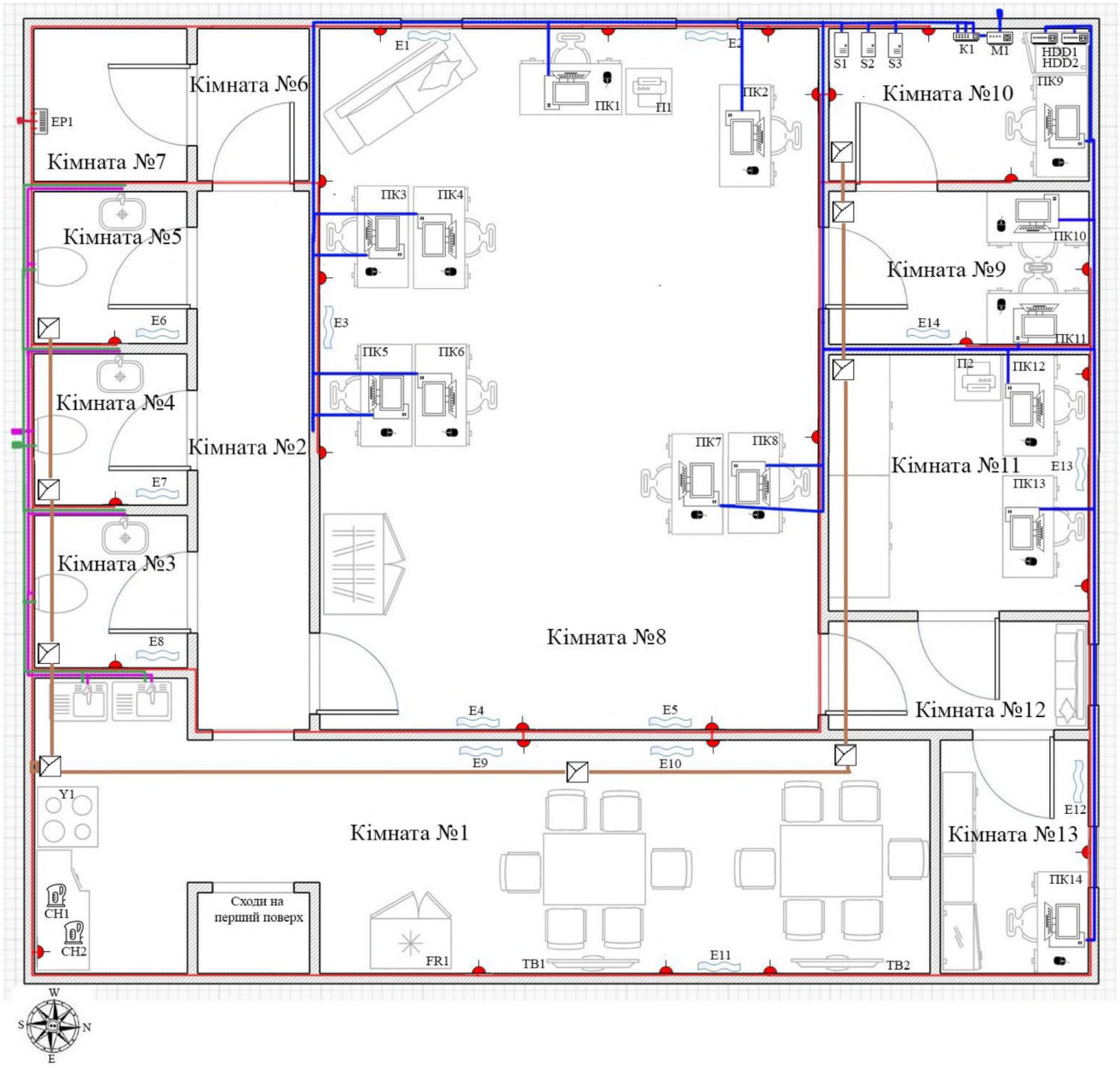

Рисунок В.1 – Генеральний план ОІД

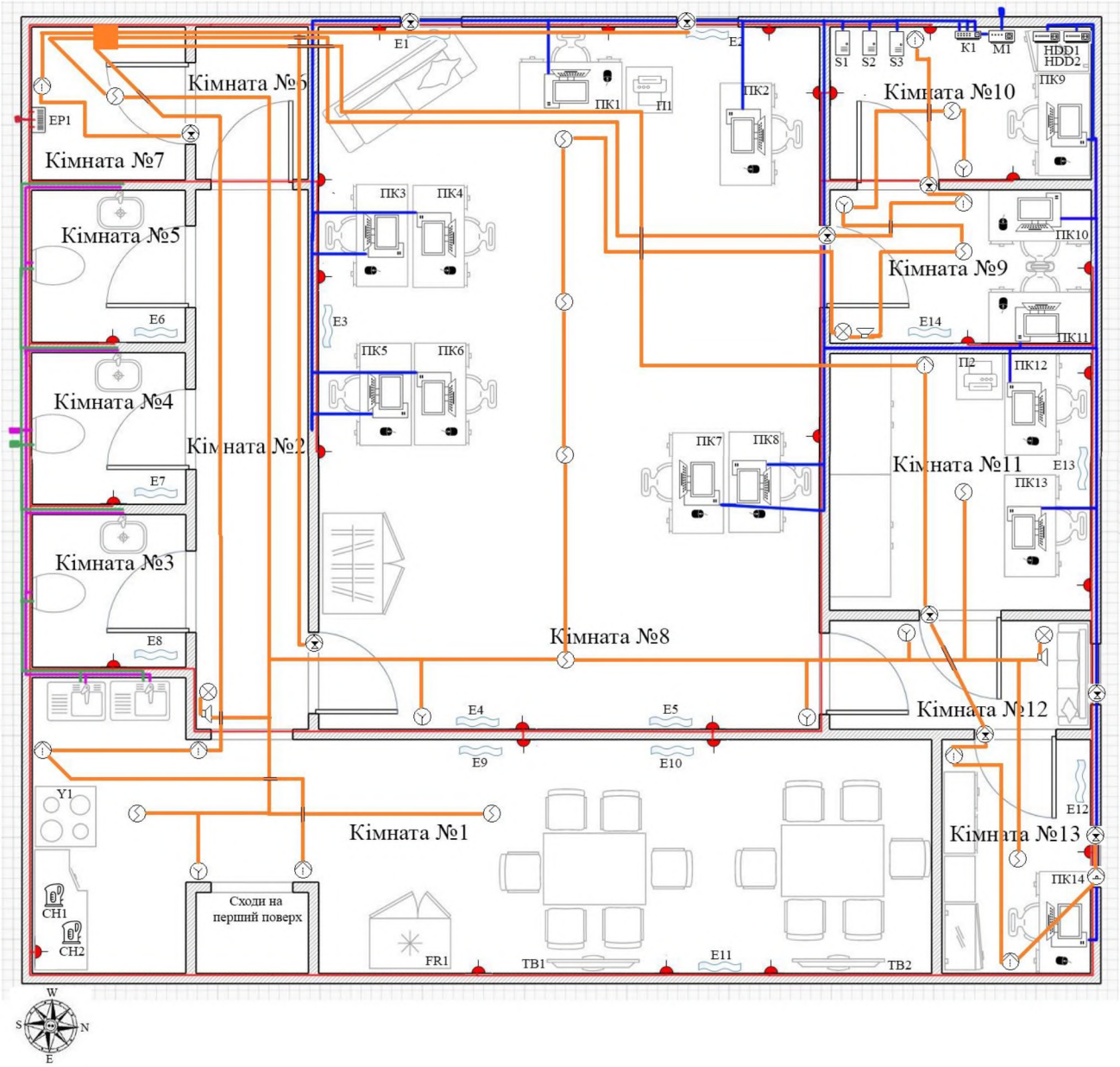

Рисунок В.2 – Генеральний план ОІД. Система пожежної та охоронної сигналізації

Рисунок В.3 – Умовні позначення до генеральних планів ОІД

ДОДАТОК Г. Призначення кімнат та доступ до них

Таблиця Г.1 – Призначення кімнат та доступ до них

№ кімнати	Призначення	Мають доступ без нагляду	Мають доступ під наглядом
Кімната №1	кімната відпочинку та прийому їжі	внутрішні працівники компанії	зовнішні працівники
Кімната №2	коридор	внутрішні працівники компанії, зовнішні працівники	–
Кімната №3	санвузол	внутрішні працівники компанії, зовнішні працівники	–
Кімната №4	санвузол	внутрішні працівники компанії, зовнішні працівники	–
Кімната №5	санвузол	внутрішні працівники компанії, зовнішні працівники	–
Кімната №6	коридор	директор, керівник, системний адміністратор	зовнішні працівники
Кімната №7	щитова будівлі	директор, керівник, системні адміністратори	зовнішні працівники
Кімната №8	робочі місця керівника, заступника керівника, операторів	внутрішні працівники компанії	зовнішні працівники

Продовження таблиці Г.1 – Призначення кімнат та доступ до них

№ кімнати	Призначення	Мають доступ без нагляду	Мають доступ під наглядом
Кімната №9	робочі місця системних адміністраторів	директор, системні адміністратори	керівник, заступник керівника, зовнішні працівники
Кімната №10	серверна	директор, системні адміністратори	позаштатні працівники
Кімната №11	бухгалтерія	директор, системні адміністратори, бухгалтери	керівник, заступник керівника, оператори, зовнішні працівники
Кімната №12	коридор	директор, системні адміністратори, бухгалтери	Керівник, зовнішні працівники
Кімната №13	робоче місце директора	директор	керівник, заступник керівника, оператори, системні адміністратори, бухгалтери зовнішні працівники

ДОДАТОК Ґ. Перелік ОТЗ

Таблиця Ґ.1 – Перелік ОТЗ

Назва	Марка	Модель	Серійний номер	Розміщення	Відстань до границі КЗ, м
1	2	3	4	5	6
Монітор до ПК1	Philips	227E	82BE54846Y84	Кімната 8, на столі	1,5
Монітор до ПК2	Philips	227E	28BE25453Y65	Кімната 8, на столі	1,8
Монітор до ПК3	Philips	227E	52BE39687Y52	Кімната 8, на столі	4
Монітор до ПК4	Dell	SE2416H	12TT86354A69	Кімната 8, на столі	4
Монітор до ПК5	Philips	227E	52BE34587Y96	Кімната 8, на столі	5
Монітор до ПК6	Philips	227E	82BE56897Y53	Кімната 8, на столі	5
Монітор до ПК7	LG	24MK600M	52UA78569C45	Кімната 8, на столі	4,3
Монітор до ПК8	Philips	227E	45BE82356Y87	Кімната 8, на столі	3,8
Монітор до ПК9	Philips	227E	25BE69854Y85	Кімната 10, на столі	1,3
Монітор до ПК10	Philips	227E	58BE26583Y56	Кімната 9, на столі	1,5

Продовження таблиці Г.1 – Перелік ОТЗ

1	2	3	4	5	6
Монітор до ПК11	Dell	SE2416H	45TT83658A56	Кімната 9, на столі	1,5
Монітор до ПК12	Philips	227E	65BE38212Y35	Кімната 11, на столі	1,5
Монітор до ПК13	LG	24MK600M	56UA99753C54	Кімната 11, на столі	1,5
Монітор до ПК14	LG	24MK600M	45UA68783C65	Кімната 13, на столі	1,3
Системний блок (ім'я в ІТС - ПК1)	HP	290 G1 MT	92FF54846Y58	Кімната 8, на підлозі	1,5
Системний блок (ім'я в ІТС - ПК2)	HP	290 G1 MT	38FF25453Y39	Кімната 8, на підлозі	1,8
Системний блок (ім'я в ІТС - ПК3)	HP	290 G1 MT	92FF39687Y15	Кімната 8, на підлозі	4
Системний блок (ім'я в ІТС - ПК4)	HP	290 G1 MT	32FF86354A12	Кімната 8, на підлозі	4
Системний блок (ім'я в ІТС - ПК5)	HP	290 G1 MT	92FF34587Y32	Кімната 8, на підлозі	5
Системний блок (ім'я в ІТС - ПК6)	HP	290 G1 MT	82FF56897Y52	Кімната 8, на підлозі	5

Продовження таблиці Г.1 – Перелік ОТЗ

1	2	3	4	5	6
Системний блок (ім'я в ІТС - ПК7)	HP	290 G1 MT	22FF78569C41	Кімната 8, на підлозі	4,3
Системний блок (ім'я в ІТС - ПК8)	HP	290 G1 MT (8PG31EA)	75FF82356Y69	Кімната 8, на підлозі	3,8
Системний блок (ім'я в ІТС - ПК9)	HP	290 G1 MT (8PG31EA)	35FF69854Y53	Кімната 10, на підлозі	1,3
Системний блок (ім'я в ІТС - ПК10)	HP	290 G1 MT (8PG31EA)	88FF26583Y52	Кімната 9, на підлозі	1,5
Системний блок (ім'я в ІТС - ПК11)	HP	290 G1 MT (8PG31EA)	65FF83658A87	Кімната 9, на підлозі	1,5
Системний блок (ім'я в ІТС - ПК12)	HP	290 G1 MT (8PG31EA)	75FF38212Y48	Кімната 11, на підлозі	1,5
Системний блок (ім'я в ІТС - ПК13)	HP	290 G1 MT (8PG31EA)	56FF99753C48	Кімната 11, на підлозі	1,5
Системний блок (ім'я в ІТС - ПК14)	HP	290 G1 MT (8PG31EA)	35FF68783C45	Кімната 13, на підлозі	1,3

Продовження таблиці Г.1 – Перелік ОТЗ

1	2	3	4	5	6
USB клавіатура до ПК1	Logitech	K120	7847MR13C88	Кімната 8, на столі	1,5
USB клавіатура до ПК2	Logitech	K120	2598MR18C53	Кімната 8, на столі	1,8
USB клавіатура до ПК3	Logitech	K120	3659MR14C54	Кімната 8, на столі	4
USB клавіатура до ПК4	Logitech	K120	4578MR15C78	Кімната 8, на столі	4
USB клавіатура до ПК5	Logitech	K120	3895MR16C89	Кімната 8, на столі	5
USB клавіатура до ПК6	Logitech	K120	2548MR17C45	Кімната 8, на столі	5
USB клавіатура до ПК7	Logitech	K120	7898MR18C42	Кімната 8, на столі	4,3
USB клавіатура до ПК8	Logitech	K120	3658MR19C89	Кімната 8, на столі	3,8

Продовження таблиці Г.1 – Перелік ОТЗ

1	2	3	4	5	6
USB клавіатура до ПК9	Logitech	K120	4879MR20C47	Кімната 10, на столі	1,3
USB клавіатура до ПК10	Logitech	K120	6989MR58C386	Кімната 9, на столі	1,5
USB клавіатура до ПК11	Logitech	K120	2564MR58C485	Кімната 9, на столі	1,5
USB клавіатура до ПК12	Logitech	K120	8978MR36C886	Кімната 11, на столі	1,5
USB клавіатура до ПК13	Logitech	K120	9658MR98C897	Кімната 11, на столі	1,5
USB клавіатура до ПК14	Logitech	K120	3256MR63C668	Кімната 13, на столі	1,3
Маршрутизатор (ім'я в ІТС - М1)	Mikrotik	CRS125-24G-1S-2HnD-IN	AADEF080BBE9	Кімната 10, на полиці	1
Комутатор (ім'я в ІТС - К1)	TP-LINK	TP-LINK T2500-28TC	BAYEU721UYH2	Кімната 10, на полиці	1

Продовження таблиці Г.1 – Перелік ОТЗ

1	2	3	4	5	6
Сервер (ім'я в ІТС - S1)	Dell	PowerEdge T410	PRUT5RQT97JE	Кімната 10, на підлозі	1
Сервер (ім'я в ІТС - S2)	Dell	PowerEdge T410	AC2D9748C2C6	Кімната 10, на підлозі	1
Сервер (ім'я в ІТС - S3)	Dell	PowerEdge T410	MJWSZ8ZIUQQN	Кімната 10, на підлозі	1
Принтер (ім'я в ІТС - П1)	Canon	I-SENSYS LBP162dw	197BA75A26BE	Кімната 8, на тумбі	1,5
Принтер (ім'я в ІТС - П2)	Canon	I-SENSYS LBP162dw	5FB1656C86461	Кімната 11, на тумбі	2
ЖМД (ім'я в ІТС – HDD1)	Western Digital	My Book 6TB WDBBGB0060HBK-EESN 3.5 USB 3.0	6GGLXTBH44CB	Кімната 10, в сейфі	1
ЖМД (ім'я в ІТС – HDD2)	Western Digital	My Passport 5TB WDBPKJ0050BBK-WESN 2.5" USB 3.0	SHLJS48RGMEB	Кімната 10, в сейфі	1

ДОДАТОК Д. Перелік ДТЗС

Таблиця Д.1 – Перелік ДТЗС

Назва	Марка	Модель	Серійний номер	Розміщення
USB миша до ПК1	Logitech	M100	8978LP13C882	Кімната 8, на столі
USB миша до ПК2	Logitech	M100	5369LP18C538	Кімната 8, на столі
USB миша до ПК3	Logitech	M100	2856LP14C548	Кімната 8, на столі
USB миша до ПК4	Logitech	M100	4588LP15C785	Кімната 8, на столі
USB миша до ПК5	Logitech	M100	4698LP16C897	Кімната 8, на столі
USB миша до ПК6	Logitech	M100	4587LP17C453	Кімната 8, на столі
USB миша до ПК7	Logitech	M100	5687LP18C422	Кімната 8, на столі
USB миша до ПК8	Logitech	M100	8578LP19C898	Кімната 8, на столі
USB миша до ПК9	Logitech	M100	6975LP20C478	Кімната 10, на столі
USB миша до ПК10	Logitech	M100	8757LP58C386	Кімната 9, на столі
USB миша до ПК11	Logitech	M100	2757LP58C485	Кімната 9, на столі
USB миша до ПК12	Logitech	M100	8213LP36C886	Кімната 11, на столі

Продовження таблиці Д.1 – Перелік ДТЗС

Назва	Марка	Модель	Серійний номер	Розміщення
USB миша до ПК13	Logitech	M100	4587LP98C897	Кімната 11, на столі
USB миша до ПК14	Logitech	M100	7857LP63C668	Кімната 13, на столі
Флеш пам'ять USB	Transcend	JetFlash 700 16GB	2157LP66C895	Кімната 10, в сейфі
Флеш пам'ять USB	Transcend	JetFlash 700 16GB	3787LP65C098	Кімната 10, в сейфі
Електроконвектор (ім'я в ІТС - Е1)	ATLANT IC	F17 Essential 1500W	YCA59NF85PSK	Кімната 8, на стіні
Електроконвектор (ім'я в ІТС – Е2)	ATLANT IC	F17 Essential 1500W	LVG5WRXAG8KO	Кімната 8, на стіні
Електроконвектор (ім'я в ІТС – Е3)	ATLANT IC	F17 Essential 1500W	FKH2V8QLSGAQ	Кімната 8, на стіні
Електроконвектор (ім'я в ІТС – Е4)	ATLANT IC	F17 Essential 1500W	V1EFFDJC7TC9	Кімната 8, на стіні
Електроконвектор (ім'я в ІТС – Е5)	ATLANT IC	F17 Essential 1500W	53K6HR0RGX1J	Кімната 8, на стіні
Електроконвектор (ім'я в ІТС – Е6)	ATLANT IC	F17 Essential 1500W	JJZP9BTSY7A4	Кімната 5, на стіні

Продовження таблиці Д.1 – Перелік ДТЗС

Назва	Марка	Модель	Серійний номер	Розміщення
Електроконвектор (ім'я в ITC – E7)	ATLANT IC	F17 Essential 1500W	HV8CAO9R7X2D	Кімната 4, на стіні
Електроконвектор (ім'я в ITC – E8)	ATLANT IC	F17 Essential 1500W	GRJZU0H7JIVJ	Кімната 3, на стіні
Електроконвектор (ім'я в ITC – E9)	ATLANT IC	F17 Essential 1500W	PP6CT479A6JE	Кімната 1, на стіні
Електроконвектор (ім'я в ITC – E10)	ATLANT IC	F17 Essential 1500W	ARGOA0LYBXCA	Кімната 1, на стіні
Електроконвектор (ім'я в ITC – E11)	ATLANT IC	F17 Essential 1500W	WWVTH7UB7KD0	Кімната 1, на стіні
Електроконвектор (ім'я в ITC – E12)	ATLANT IC	F17 Essential 1500W	HRICYUEM54K9	Кімната 13, на стіні
Електрокон-вектор (ім'я в ITC – E13)	ATLANT IC	F17 Essential 1500W	YNW1WCWMQPTR	Кімната 11, на стіні
Електрокон-вектор (ім'я в ITC – E14)	ATLANT IC	F17 Essential 1500W	LWC4IO81817N	Кімната 9, на стіні
Електрочайник (ім'я в ITC – CH1)	PHILIPS	Viva Collection HD9355/90	0ZHWCSSUVLQP	Кімната 1, на столі
Електрочайник (ім'я в ITC – CH2)	PHILIPS	Viva Collection HD9355/90	23KGZFIM7AO3	Кімната 1, на столі

Продовження таблиці Д.1 – Перелік ДТЗС

Назва	Марка	Модель	Серійний номер	Розміщення
Плита електрична (ім'я в ІТС – Y1)	GEFEST	ЭП Н Д 5140 0031	B3WPE2R9TNZE	Кімната 1, на підлозі
Пожежний датчик диму	Артон	СПД-3.2	1A5AUVVPQGVI	Кімната 1, на стелі
			UWEOCJ9SPVIM	Кімната 1, на стелі
			7KJ53XPUXGE9	Кімната 7, на стелі
Пожежний датчик диму	Артон	СПД-3.2	FPPEKKIID0MA	Кімната 8, на стелі
			MG7NRUG3Q8S2	Кімната 8, на стелі
			OG8DDWA4PNS2	Кімната 8, на стелі
			6DQNYGY6X1UJ	Кімната 8, на стелі
			4NSMVNPXT70P	Кімната 9, на стелі
Пожежний датчик диму	Артон	СПД-3.2	4E8B09R7Z2AJ	Кімната 10, на стелі
			92S3HPAOHWBO	Кімната 11, на стелі
Кнопка пожежної тривоги	Артон	SPR-1	V0M3Z64N4KBO	Кімната 1, на стіні
			R4R0AWQGK3LJ	Кімната 8, на стіні
			6XPFJ2WCWFLH	Кімната 8, на стіні
			DYU6HSOCKU9S	Кімната 12, на стіні
			61E049FMNQI2	Кімната 9, на стіні
			WXNGEW0O7E9N	Кімната 10, на стіні

Продовження таблиці Д.1 – Перелік ДТЗС

Назва	Марка	Модель	Серійний номер	Розміщення
Сигнально світловий сповіщувач	Сирена	Лунь-11	2MRPW6I90VQB	Кімната 2, на стіні
			FSMJKVEKU03B	Кімната 12, на стіні
			5N3CMSCV686C	Кімната 9, на стіні
Датчик інфрачервоний (пасивний)	Crow	Swan QUAD	SEY6MR26Y3OL	Кімната 1, на стіні
			YGQQ8K6ZHHDN	Кімната 1, на стіні
			ZXRFBI337YK5	Кімната 1, на стіні
			Z4NJ0DZQB1V5	Кімната 7, на стіні
			U1Y61XCQ95PB	Кімната 13, на стіні
			WSTGBW2ME1C8	Кімната 13, на стіні
			WYEQ97ZUIC9M	Кімната 11, на стіні
			E4KZCT8B9IIX	Кімната 9, на стіні
			3T6897G44JBG	Кімната 10, на стіні

Продовження таблиці Д.1 – Перелік ДТЗС

Назва	Марка	Модель	Серійний номер	Розміщення
Датчик інфрачервоний (пасивний)	Crow	Swan QUAD	WSTGBW2ME1C8	Кімната 13, на стіні
			WYEQ97ZUIC9M	Кімната 11, на стіні
			E4KZCT8B9IIX	Кімната 9, на стіні
			3T6897G44JBG	Кімната 10, на стіні
Магнітно-контактний датчик	Електрон	ЕСМК-7ЕП	48OIDYD93XUD	Кімната 7, на дверях
			ZE3NZR2MRQYR	Кімната 8, на дверях
			6RUY3JJ8GG99	Кімната 8, на вікні
			YKQHFKG5CZ1W	Кімната 8, на вікні
			XC994R20K49R	Кімната 11, на дверях
			KTSH5OATRRT0	Кімната 13, на дверях
			OMQU2ZX1Z2NC	Кімната 13, на вікні

Продовження таблиці Д.1 – Перелік ДТЗС

Назва	Марка	Модель	Серійний номер	Розміщення
Магнітно-контактний датчик	Електрон	ЕСМК-7ЕП	G89OKIYPM5RW	Кімната 10, на дверях
			Z2YGLKH6VS6H	Кімната 9, на дверях
Датчик на розбиття скла	Crow	GBD2	L1SVGN63X432	Кімната 13, біля вікна
ППКОП	Лунь	11	3P5IRNYVABAW	На КПП
Панель СКУД	Seven	CR-772M	XF8KWG7VFNBJ	На центральних вхідних дверей
Зовнішня камера відеоспостереження (ім'я в ІТС – CAM14)	Green Vision	GV-040-GHD-H-COS20-20 1080P	TFOART3HNG4J	Зі східної сторони будівлі
Зовнішня камера відеоспостереження (ім'я в ІТС – CAM15)	Green Vision	GV-040-GHD-H-COS20-20 1080P	TR7Z7EWTCZZ3	Зі східної сторони будівлі
Зовнішня камера відеоспостереження (ім'я в ІТС – CAM16)	Green Vision	GV-040-GHD-H-COS20-20 1080P	TPBFK53REPJN	З південної сторони будівлі
Зовнішня камера відеоспостереження (ім'я в ІТС – CAM17)	Green Vision	GV-040-GHD-H-COS20-20 1080P	AVD122EUQFCE	З західної сторони будівлі
Зовнішня камера відеоспостереження (ім'я в ІТС – CAM18)	Green Vision	GV-040-GHD-H-COS20-20 1080P	W986455NT38A	З західної сторони будівлі

Продовження таблиці Д.1 – Перелік ДТЗС

Назва	Марка	Модель	Серійний номер	Розміщення
Зовнішня камера відеоспостереження (ім'я в ІТС – CAM19)	Green Vision	GV-040-GHD-H-COS20-20 1080P	5S2MOKRAKKD2	З південної сторони будівлі
Джерело безпере-бійного живлення	APC	Back-UPS 900W/1600VA	AAZYEIARU9NL	Кімната №10 біля сервера (S1)
Джерело безпере-бійного живлення	APC	Back-UPS 900W/1600VA	R2RNVKTZLNCK	Кімната №10 біля сервера (S2)
Джерело безпере-бійного живлення	APC	Back-UPS 900W/1600VA	GQKSGQ9ZM3T0	Кімната №10 біля сервера (S3)

ДОДАТОК Е. Характеристика складу апаратних засобів ОТЗ

Таблиця Е.1 – Характеристика складу апаратних засобів ОТЗ

Ім'я в ІТС	Назва обладнання	Характеристика	Серійний номер
1	2	3	4
ПК1	Процесор	Intel Core i3-7100 (Kaby Lake)	WMO0FZ43DHDB
	Материнська плата	MSI H310M PRO-VDH Plus	14OOSCSFDWE9
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	TA3Y8ZKSKWUC
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	MU8YV6TPHXON
ПК2	Процесор	Intel Core i3-7100 (Kaby Lake)	Q8LQEL2H6GR2
	Материнська плата	MSI H310M PRO-VDH Plus	N5K37R92XBGF
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	LQWENX1DUECJ
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	JVH44VAWQNMY
ПК3	Процесор	Intel Core i3-7100 (Kaby Lake)	GEMOJQFHQVJ7
	Материнська плата	MSI H310M PRO-VDH Plus	4XC5ZYQOPOK6
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	9SWR5SZ9410C
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	VLYVM8OL496A

Продовження таблиці Е.1 – Характеристика складу апаратних засобів ОТЗ

1	2	3	4
ПК4	Процесор	Intel Core i3-7100 (Kaby Lake)	5FL5WAOGCTOT
	Материнська плата	MSI H310M PRO-VDH Plus	L2FM8ORHDYX5
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	I36HWNVXNP0P
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	SRAN7A7YG3YT
ПК5	Процесор	Intel Core i3-7100 (Kaby Lake)	RHGWDJATCWQ4
	Материнська плата	MSI H310M PRO-VDH Plus	BBQEFHI58KWK
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	B1SJG4MSSUKT
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	IMW84J8QRPQF
ПК6	Процесор	Intel Core i3-7100 (Kaby Lake)	4J4VOHTT94ZR
	Материнська плата	MSI H310M PRO-VDH Plus	1YQ85COPSXLQ
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	7FGGQB1U9S0W
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	U7EQHJOSGKR6
ПК7	Процесор	Intel Core i3-7100 (Kaby Lake)	Y2O8GOPK8259
	Материнська плата	MSI H310M PRO-VDH Plus	8WLPW6E6BMX6
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	IZ9EW4KGKODD
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	XAZKBJPR4N1E

Продовження таблиці Е.1 – Характеристика складу апаратних засобів ОТЗ

1	2	3	4
ПК8	Процесор	Intel Core i3-7100 (Kaby Lake)	VNO7LU45GW8O
	Материнська плата	MSI H310M PRO-VDH Plus	RTJJB8LRONW5
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	I4FG6KLNASV7
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	9BSXGIMJHCX3
ПК9	Процесор	Intel Core i3-7100 (Kaby Lake)	0VD82XSNP8N3
	Материнська плата	MSI H310M PRO-VDH Plus	RTJJB8LRONW5
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	L4SABYKXYGZ4
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	HQUFVF94TYUA
ПК10	Процесор	Intel Core i3-7100 (Kaby Lake)	YQ5KB2NIVPNC
	Материнська плата	MSI H310M PRO-VDH Plus	71GLKCQASHVH
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	AMHK68EIOW1I
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	ICI02OYHQJVN
ПК11	Процесор	Intel Core i3-7100 (Kaby Lake)	SSQE39F7HOL4
	Материнська плата	MSI H310M PRO-VDH Plus	EZ6T8BO3LPGQ
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	DSVGGWKGTW2B
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	1BZD322T2O2U

Продовження таблиці Е.1 – Характеристика складу апаратних засобів ОТЗ

1	2	3	4
ПК12	Процесор	Intel Core i3-7100 (Kaby Lake)	9X26K51HMODF
	Материнська плата	MSI H310M PRO-VDH Plus	FJZ2TFFZYZ2Z
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	AV7AFMF0S1PU
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	33I0WBE5QW60
ПК13	Процесор	Intel Core i3-7100 (Kaby Lake)	8BQ48S2UTRUQ
	Материнська плата	MSI H310M PRO-VDH Plus	WNQ45CMP2WZ4
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	JH5S1L8QRHG9
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	T0SOJ1735QCQ
ПК14	Процесор	Intel Core i3-7100 (Kaby Lake)	ZX5RDH0NXVLP
	Материнська плата	MSI H310M PRO-VDH Plus	EK87FQM76U43
	Твердотільний накопичувач	Samsung 870 Evo-Series 250Гб	7UMAWS7R1GEI
	Оперативна пам’ять	HyperX DDR4-2666МГц 8 Гб	4T86II7WWW71
S1	Процесор	Intel Core i3-8100	7U14MFZKM4M0
	Материнська плата	Asus WS C246 Pro	6SR05K08CGV5
	Жорсткий диск	Western Digital DC HC510 10TB	23XWPSC9FSDV

Продовження таблиці Е.1 – Характеристика складу апаратних засобів ОТЗ

1	2	3	4
S1	Оперативна пам’ять	2 планки HyperX DDR4 3200МГц 16 Гб	4W57ZGZ8U8MJ
			2U00MFZKM8M9
S2	Процесор	Intel Core i3-8100	71T5XQ6F0L9N
	Материнська плата	Asus WS C246 Pro	2FOOB2PC8QBD
	Жорсткий диск	Western Digital DC HC510 10TB	G112696ONHEJ
	Оперативна пам’ять	2 планки HyperX DDR4 3200МГц 16 Гб	B68PL2V0746D
S3	Процесор	Intel Core i3-8100	3H1SQ92DTTFX
	Материнська плата	Asus WS C246 Pro	R2W05QQOEM50
	Жорсткий диск	Western Digital DC HC510 10TB	6JMVUOTSDD5I
	Оперативна пам’ять	2 планки HyperX DDR4 3200МГц 16 Гб	BM6W17F4T1CR

ДОДАТОК Є. Перелік ПЗ встановленого на ОТЗ

Таблиця Є.1 – Перелік ПЗ встановленого на ОТЗ

Назва	Тип	Ліцензія	Де встановлено
Microsoft Windows 10 Professional 19042.804 (build 20H2) x64	Системне	Комерційна	ПК1, ПК2, … ПК14
Пакет програм Microsoft Office 2016 Pro Plus 16.0.5080.1000	Прикладне	Комерційна	ПК1, … ПК14
WinRAR 6.00 Final	Прикладне	Безкоштовно	ПК1, … ПК14
Google Chrome 86.0.4240.198	Прикладне	Безкоштовно	ПК1, … ПК14
Adobe Acrobat Pro DC 2021.001.20142	Прикладне	Безкоштовно	ПК1, … ПК14
FastStone Image Viewer 7.0	Прикладне	Безкоштовно	ПК1, … ПК14
Opera 74.0.3911.160	Прикладне	Безкоштовно	ПК1, … ПК14
Jitsi 2.10.5550	Прикладне	Безкоштовно	ПК1, … ПК14
Windows Defender (Захисник Windows) 4.18.1907.4	Прикладне	Безкоштовно	ПК1, … ПК14
Microsoft Edge 89.0.774.45	Прикладне	Безкоштовно	ПК1, … ПК14
TeamViewer 15.16.8.0	Прикладне	Безкоштовно	ПК1, … ПК14
1С:Підприємство 8.2.18.102	Прикладне	Комерційна	ПК1, ПК2, … ПК14, S1

Продовження таблиці Є.1 – Перелік ПЗ встановленого на ОТЗ

Назва	Тип	Ліцензія	Де встановлено
Microsoft Windows Server 2012 Essentials x64 12.201.125.154	Прикладне	Комерційна	S1, S2, S3
FreeFileSync 11.10	Прикладне	Комерційна	ПК9

ДОДАТОК Ж. ФОРМА ТА ЗМІСТ АКТА КАТЕГОРІЮВАННЯ ОБ’ЄКТА

Прим. №___

ЗАТВЕРДЖУЮ
Директор установи-власника
(розпорядника, користувача) об’єкта
директор Щур Г.П.
(посада, підпис, ініціали, прізвище)
09.05.2021
М.П. _____

АКТ
категоріювання приміщення ТОВ «BeerWineShop»

1. Підстава для категоріювання _____
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
_____
зміна ознаки, за якою була встановлена категорія об'єкта тощо;
_____
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

2. Вид категоріювання _____первинне_____
(первинне, чергове, позачергове)
_____
__
(у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється _____
(обробка інформації технічними засобами та/або озвучування інформації)

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті
_____конфіденційна інформація_____
(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації"; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія _____4 категорія_____

Голова комісії: _____ Гумов О.Л.
(підпис) (ініціали, прізвище)
Члени комісії: _____ Ледін С.Д.
(підпис) (ініціали, прізвище)
09.05.2021

ДОДАТОК З. Перелік документів на оптичному носії

1. Кваліфікаційна_робота_Ангеловський_125-17-1.docx
2. Презентація_ Ангеловський_125-17-1.pptx

ДОДАТОК И. Відгук керівника економічної частини

Відгук керівника економічного розділу:

Керівник розділу _____ Пілова Д.П.
(підпис) (ініціали, прізвище)

ДОДАТОК І. Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу студента групи 125-17-1 Ангеловського М.О. на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи приватного підприємства ТОВ «BeerWineShop»»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 128 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на підвищення рівня захисту інформації в ІТС ТОВ «BeerWineShop».

При виконанні роботи автор продемонстрував рівень теоретичних знань і практичних навичок. На основі аналізу нормативно-правової бази в сфері захисту інформації, процесу обстеження середовища функціонування ІТС, розглянута модель загроз та модель порушника, в ній а також сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому було виконано обстеження фізичного середовища та обчислювального середовища ІТС, проаналізовано технологію обробки інформації, загрози та вразливості, розроблена модель порушника, обрано профіль захищеності, виконано етап розробки КСЗІ та політики безпеки.

Практична цінність роботи полягає в тому, що запропоновані рішення знизять ризики реалізації зафіксованих загроз та вразливостей до мінімуму.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Ангеловський М.О. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,

к.т.н., доцент **О.В. Герасіна**