Міністерство освіти і науки України
Національний технічний університет
«Дніпропетровська політехніка»
Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студентки *Іванченко Єлизавети Максимівни*

академічної групи *125-17-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «VIF»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	професор Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент	Зам. директор логістики Крутіков В.М.			

Нормоконтролер	ст. викл. Тимофеев Д.С.			

Дніпро
2021

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

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Іванченко Є. М.* ***академічної групи*** *125-17-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації[1]

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «VIF»*

Затверджую наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021 № 317-с

Розділ	Зміст	Термін виконання
Розділ 1	Обстеження ІТС, аналіз середовищ функціонування	19.04.2021
Розділ 2	Аналіз загроз ІБ ІТС підприємства, розробка проектних рішень щодо реалізації механізмів захисту	28.05.2021
Розділ 3	Обґрунтування економічної доцільності впровадження КСЗІ, розрахунок витрат та ефекту впровадження КСЗІ	10.06.2021

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

Дата видачі завдання: 12.01.2021

Дата подання до екзаменаційної комісії: 08.06.2021

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 95 с., 9 рис., 26 табл., 5 додатків, 17 джерел.

Об’єкт дослідження: інформаційно-телекомунікаційна система ТОВ «VIF».

Мета роботи: підвищення рівня захисту інформації та розробка рекомендацій в ІТС ТОВ «VIF».

Методи розробки: спостереження, аналіз, опис.

У першому розділі наведені загальні дані про підприємство, виконане обстеження фізичного середовища, інформаційного середовища, середовища користувачів та обчислювальної системи. На підставі зібраних даних була розроблена модель порушника та модель загроз. Визначені актуальні загрози та їх вразливості.

У другому розділі був обраний профіль захищеності і розроблені проектні рішення щодо реалізації механізмів захисту, яке включало в себе: розподіл повноважень, щодо адміністрування інформаційно-телекомунікаційної системи, запропоновані правила розмежування доступу, запропоновані засоби реалізації контролю за діями користувачів.

У третьому розділі доведена доцільність використання КСЗІ, визначена економічна ефективність її впровадження в інформаційно-телекомунікаційну систему та визначений коефіцієнт повернення інвестицій ROSI.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ, ПРОЕКТНІ РІШЕННЯ

РЕФЕРАТ

Объяснительная записка: 95 с., 9 рис., 26 табл., 5 приложений, 17 источников.

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

Цель работы: повышение уровня защиты информации и разработка рекомендаций в ИТС ООО «VIF».

Методы разработки: наблюдение, анализ, описание.

В первом разделе приведены общие данные о предприятии, выполнено обследование физической среды, информационной среды, среды пользователей и вычислительной системы. На основании собранных данных была разработана модель нарушителя и модель угроз. Определены актуальные угрозы и их уязвимости.

Во втором разделе был избран профиль защищенности и разработаны проектные решения по реализации механизмов защиты, которое включало в себя: распределение полномочий, относительно администрирования информационно-телекоммуникационной системы, предложены правила разграничения доступа, предложены средства для осуществления контроля за действиями пользователей.

В третьем разделе доказана целесообразность использования КСЗИ, определена экономическая эффективность ее внедрения в информационно-телекоммуникационную систему и определен коэффициент возврата инвестиций ROSI.

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННАЯ СИСТЕМА, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, ЭКОНОМИЧЕСКАЯ ЦЕЛЕСООБРАЗНОСТЬ, ПРОЕКТНЫЕ РЕШЕНИЯ

ABSTRACT

Executive: 95 pages., 9 fig., 26 table, 5 annexes, 17 sources

Object of research: information and telecommunication system of VIF LLC.

Purpose: to increase level of information protection and development of recommendations in ITS LLC "VIF".

Development methods: observation, analysis, description.

The first section provides general information about the company, performed a survey of the physical environment, information environment, user environment and computer system. Based on the collected data, a model of the violator and a model of threats were developed. Current threats and their vulnerabilities have been identified.

The second section selected the security profile and developed design solutions for the implementation of protection mechanisms, which included: distribution of rights for the administration of information and telecommunications system, proposed rules for delimiting access, proposed means of implementing control over user actions.

The third section proves the feasibility of using CIPS, determines the economic efficiency of its implementation in the information and telecommunications system and determines the rate of return on investment ROSI.

COMPREHENSIVE INFORMATION PROTECTION SYSTEM, OBJECT OF INFORMATION ACTIVITY, INFORMATION AND TELECOMMUNICATIONS SYSTEM, MODEL OF THREATS, DISTRICT, MODEL

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система;

ВТК – відділ технічного контроля;

ДТЗС – допоміжні технічні засоби та системи;

ЗЕД – зовнішня економічна діяльність;

ЗУ - закон України;

ІБ - інформаційна безпека;

ІзОД – Інформація з обмеженим доступом;

ІТС - інформаційно-телекомунікаційна система;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КС – комп'ютерна система;

КСЗІ - комплексна система захисту інформації;

НСД - несанкціонований доступ;

ОІД - об'єкт інформаційної діяльності;

ОС - обчислювальна система;

ПБ - політика безпеки;

ПЗ – програмне забезпечення;

ТЗІ - технічні засоби інформації;

ТОВ – товариство з обмеженою відповідальністю.

ЗМІСТ

ВСТУП

Проблеми кібербезпеки в бізнесі залишаються малозрозумілими і слабо враховуються. Однак наслідки кібератак, технічних збоїв або людської недбалості можуть серйозно вплинути на діяльність організації. Для захисту від цих ризиків необхідно мати засоби безпеки.

За статистикою 80% організацій пережили хоча б одну кібератаку за останні дванадцять місяців. Кіберризик не слабшає, а стає все більш значним. Цифрова трансформація і її наслідки (зростання залежності від інструментів, взаємозв'язок інформаційних систем, повсюдне поширення зберігання даних в хмарі і т.д.) породили цілий ряд нових ризиків, проти яких компанії недостатньо озброєні. Що стосується кіберзахисту, то занадто багато організацій як і раніше покладаються на непрацюючі системи та індивідуальні рішення, в той час як загроза стала глобальною. Необхідно терміново усвідомити ризики і впровадити передові методи (технологічні та людські) для підвищення рівня кібербезпеки компаній.

Інциденти, що стосуються інформаційної безпеки є другим за ступенем побоювання ризиком для організацій, випереджаючи стихійні лиха. Тому що IT-інциденти часто призводять до переривання або уповільнення діяльності через все більш помітний взаємозв'язок між нею та IT-системами. Підводячи підсумки, можна сказати, що чим більше компанія залежить від цифрових пристроїв, тим більше центральними стають питання кібербезпеки.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості щодо ТОВ «VIF»

Об’єктом інформаційної діяльності (далі ОІД) є ТОВ «VIF».

ТОВ «VIF» - приватне підприємство, що виробляє шкіряну та шкіргалантерейну продукцію та реалізує її через магазини «BAGS etc» та «BAGS etc Showroom».

За формою власності ТОВ «VIF» комерційна організація, зареєстрована як товариство з обмеженою відповідальністю, на основі приватної власності статутний капітал якої 77 604,00 грн. Підприємство було зареєстровано 14.11.1997.

ТОВ «VIF» має такі види діяльності:

- 15.12 Виробництво дорожніх виробів, сумок, лимарно-сідельних виробів зі шкіри та інших матеріалів;
- 14.19 Виробництво іншого одягу й аксесуарів;
- 46.49 Оптова торгівля іншими товарами господарського призначення;
- 77.33 Надання в оренду офісних машин і устаткування, у тому числі комп'ютери;
- 77.39 Надання в оренду інших машин, устаткування та товарів. н. в.;
- 77.40 Лізинг інтелектуальної власності та подібних продуктів, крім творів, захищених авторськими правами;
- 78.30 Інша діяльність із забезпечення трудовими ресурсами;
- 95.22 Ремонт побутових приладів, домашнього та садового обладнання;
- 95.29 Ремонт інших побутових виробів і предметів особистого вжитку;
- 46.90 Неспеціалізована оптова торгівля;
- 47.19 Інші види роздрібної торгівлі в неспеціалізованих магазинах;
- 47.25 Роздрібна торгівля напоями в спеціалізованих магазинах;
- 47.29 Роздрібна торгівля іншими продуктами харчування в спеціалізованих магазинах;
- 47.72 Роздрібна торгівля взуттям і шкіряними виробами в спеціалізованих магазинах;

- 47.78 Роздрібна торгівля іншими невживаними товарами в спеціалізованих магазинах;
- 49.41 Вантажний автомобільний транспорт;
- 52.29 Інша допоміжна діяльність у сфері транспорту;
- 56.10 Діяльність ресторанів, надання послуг мобільного харчування;
- 56.30 Обслуговування напоями;
- 68.20 Надання в оренду й експлуатацію власного чи орендованого нерухомого майна;
- 77.12 Надання в оренду вантажних автомобілів;
- 32.99 Виробництво іншої продукції, н. в. і. у.

Підприємство функціонує 5 днів на тиждень (з понеділка по п'ятницю). Графік роботи з 8:00 до 17:00, з перервою на обід з 13:00 до 14:00. У період обідньої перерви організація не займається основною діяльністю, служба охорони зокрема 2 особи, які пропускають людей на територію фірми, обідають по черзі.

Працівники являють собою ключовий ресурс продуктивності підприємства для реалізації проектів та ідей компанії. Кількість працівників на досліджуваному підприємстві складає 204 осіб.

Рисунок 1.1 Організаційна структура підприємства

1.2 Обґрунтування необхідності створення КСЗІ

З метою необхідного осмислення чинників захисту інформації в компанії, а також об’єктів захисту, проведемо дослідження нормативно-правових актів, спираючись на які, можуть утворюватися умови захисту з метою конкретних видів інформації.

При побудові комплексної системи захисту інформації в компаніях слід визначити відповідні нормативні документи. Данні документи регламентують, а також встановлюють процедуру захисту властивостей інформації (конфіденційність, цілісність та доступність), а також регламентують порядок ефективної нейтралізації небезпек через введення єдиної системи захисту інформації; встановлюють правила та зобов'язання, а також відповідальність персоналу, діяльність якого пов'язана з інформаційною безпекою.

Згідно ЗУ «Про інформацію» інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

Відповідно до законодавства України і нормативних документів Закону України «Про захист інформації» обов’язковому захисту підлягає інформація з обмеженим доступом та інформація, що містить персональні дані громадян. Для забезпечення заходу інформації в системі створюється КСЗІ.

Спираючись на Закон України «Про захист персональних даних» об’єктами захисту є персональні дані. Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою.

Згідно ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством. Процедура доступу до даних, перелік користувачів та їх

можливості щодо даної інформації формуються власником інформації. Обов'язок за надання захисту інформації в системі покладається на власника системи.

Визначимо клас автоматизованої системи. Згідно НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» АС на підприємстві «VIF» відноситься до АС класу «3», що являє собою розподілений багатомашинний багатокористувачевий комплекс, що обробляє інформацію різних категорій конфіденційності.

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». Категоріювання може бути первинним, черговим або позачерговим. Категоріювання здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об’єкті. Об'єктами категоріювання є об'єкти інформаційної діяльності, в тому числі об'єкти ЕОТ. Об’єкти, яким встановлено відповідну категорію, вносяться до Переліку категорійованих об’єктів, який ведеться власником (розпорядником, користувачем) об’єктів інформаційної діяльності ОІД, що розглядається встановлюється категорія IV (четверта) оскільки на об'єкті обробляється інформація з обмеженим доступом, що не становить державної таємниці.

Спираючись на НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» у якому визначено порядок проведення робіт і комплексу взаємоузгоджених заходів із впровадження КСЗІ, необхідно провести обстеження функціонування ІТС за такими складовими: фізичне середовище, середовище обчислювальної системи, середовище користувачів та середовище інформації, що обробляється даною системою. Якщо в ІТС обробляються інші види інформації, то вимоги цього нормативного документа суб’єкти системи ТЗІ можуть

використовувати як рекомендації. За результатами обстеження середовищ функціонування ІТС затверджується перелік об'єктів захисту і починається етап створення КСЗІ. Він передбачає собою:

- визначення завдань щодо захисту інформації в ІТС, мету створення КСЗІ, варіанти визначення задач захисту та основні напрями забезпечення захисту;
- здійснення аналізу ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначення переліку суттєвих загроз;
- визначення загальної структури та складу КСЗІ, вимог до можливих заходів, методів та засобів захисту інформації, допустимих обмежень щодо застосування певних заходів і засобів захисту.

Простота і контрольованість інформаційної системи: правило простоти і керованості інформаційної системи в цілому встановлює ймовірність формального або неофіційного підтвердження точності здійсненні механізмів захисту. Виключно в простій і керованій системі можливо проконтролювати злагодженість конфігурації різних компонентів і реалізувати централізоване адміністрування.

Для виконання вимог щодо захисту інформації на підприємстві було прийнято рішення про створення КСЗІ.

1.3 Обстеження фізичного середовища ІТС

1.3.1 Опис ситуаційного плану

Офіс та виробництво обстежуваного об'єкту знаходиться за наступною адресою: Україна, м. Дніпро, вул. Мандриківська, 47, п'ятий поверх. Контрольована зона обмежена стінами приміщення. Дах плоский, покритий єврорубероїдом.

Об'єкт знаходиться в п'ятиповерховій будівлі, розташованій на вулиці із високим рівнем руху. Вхід до основної будівлі без перепусток. Споруда має сходові прогони, через які можна дістатися до будь-якої поверхні. Також у будівлі є ліфт, який працює лише по перепусткам.

Відвідувачі мають право перебувати на території підприємства за певних обставин. Процедура пропуску візитера на підприємство проходить наступним чином. На вхідній двері встановлена камера та зв'язок з службою безпеки. Гість, має назвати прізвище та ім'я людини, до якої він прийшов. Служба безпеки викликає співробітника до дверей, який проводить візитера до свого робочого місця. Коли гість буде покидати підприємство, співробітник має проводити його назад до дверей. Випадкові відвідувачі не зможуть потрапити на територію підприємства.

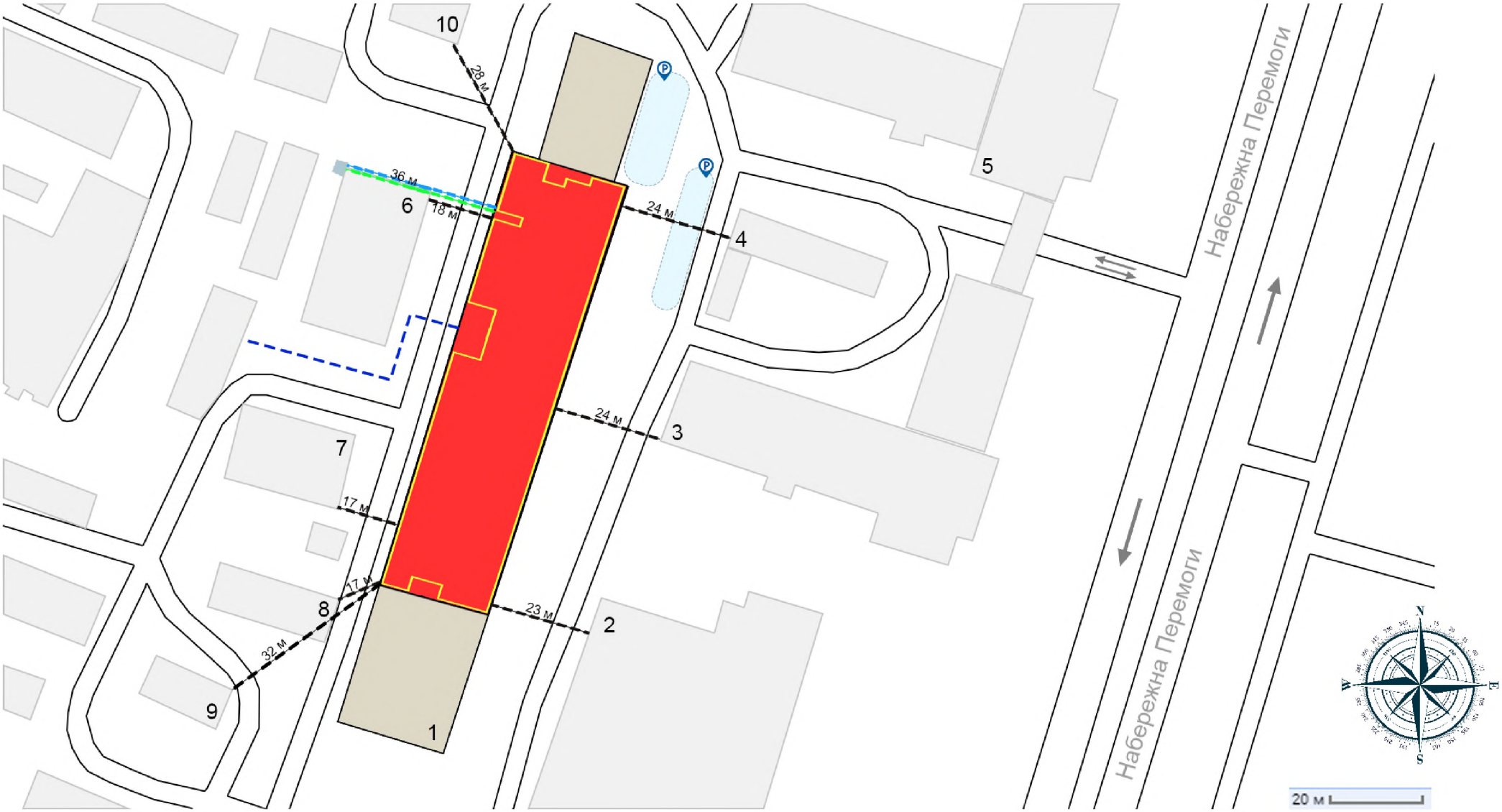
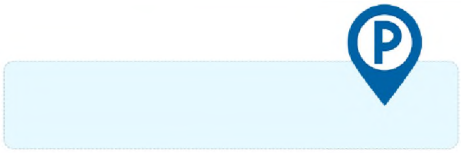


Рисунок 1.2 Ситуаційний план

Таблиця 1.1 – Умовні позначення ситуаційного плану

Позначка	Умовне позначення
	Сусідні будівлі
	Межа будівлі, в якій знаходиться ОІД
	Межа ОІД
	Місце паркування автомобілів
	Напрямок руху автомобілів
	Трансформаторна підстанція
	Межа КЗ
	Лінія системи електроживлення
	Інтернет
	Лінія системи водопостачання

У спорудженні розташовані такі підприємства:

- СТО Ремарк – 1 поверх;
- Магазин автозапчастин Inter Cars Ukraine – 1 поверх;
- Магазин «Чайна лавка» – 2 поверх;
- Печать «Дніпро» – 2 поверх;
- Кафе Бістро – 2 поверх;
- Офіси інших компаній – 3 та 4 поверхи.

Таблиця 1.2 – Характеристики будівель та споруд

№	Найменування	Кількість поверхів	Адреса	Відстань від ОІД
1	Адміністративна будівля	5	Мандриківська, 47	0 м
2	УДХТУ (спортивний комплекс)	3	Набережна Перемоги 40а	23 м
3	НТУ «ДП»	4	Набережна Перемоги 38б	24 м
4	Господарський корпус	1	Набережна Перемоги 38б	24 м
5	НМетАУ	4	Набережна Перемоги 38а	34 м
6	Автосервіс	2	Набережна Перемоги 38а/1	18 м
7	Склад	1	Набережна Перемоги 38а/2	17 м
8	Склад	1	Набережна Перемоги 38а/3	17 м
9	Склад	1	Набережна Перемоги 38а/4	32 м
10	НТУ «ДП», 9 корпус	4	Мандриківська, 45	28 м

Територія навколо будівлі асфальтована. Ширина доріг навколо споруди у якій розташований ОІД, та дороги, що є заїздом, дорівнює 2,5 метри. Основний заїзд до будівлі відбувається з вул. Набережна Перемоги, яка знаходиться на відстані 115 м, з шириною проїжджої частини – 20 м.

На території присутні такі види комунікації, як лінії електропередачі, водопостачання, комп'ютерної мережі.

1.3.2 Опис генерального плану

Висота стель – 6 м. Площа ОІД – 3240 м^2.

Зовнішні стіни будівлі – залізобетонні (0.35м). Внутрішні стіни на підприємстві – цегляні (65мм).

34 (по 17 с двох сторін будівлі) вікна розміром 4м·3м – дерев'яні вкриті матовою плівкою. Мають пластикові горизонтальні жалюзі. У кожному вікні відчиняється кватирка розмірами 0.3м·0.4м, що знаходиться внизу вікна.

Вхідні двері металеві 1.3м·2.1м з двома врізними металевим замком.

Підлога представляє собою плиту міжповерхового перекриття, звукоізолюючий шар, армуючий шар та гідроізолюючий шар , на який покладено керамічну плитку.

Міжкімнатні одностворчаті двері мають розміри одного полотна 70см·200см, виконані з зрощеного масива сосни, кожна з міжкімнатних дверей має один врізний замок.

Система електроживлення (освітлення): мережа 220В; автономний агрегат електроживлення відсутній; світильники з LED лампами. Підключена до трансформаторної підстанції знаходиться за межами КЗ.

Системи сигналізації:

- пожежна – димовий сповіщувач СПД 3;
- охоронна – складається з пасивних інфрачервоних датчиків руху (Pyronix KX10DTP) у кількості 8 штук та камер відеоспостереження (Dahua) у кількості – 18 штук.

На таблиці наведена інформація про системи комунікацій, та життєзабезпечення.

Таблиця 1.3 – Системи комунікацій

Система комунікацій	Спосіб підключення
Система електроживлення	Підключено до трансформаторної станції на вул. Гагаріна, розподільний щиток розташований в будівлі на першому поверсі.
Система водопостачання	Підключено до міського водоканалу, котрий виходить за межі КЗ.

Продовження таблиці 1.3 – Системи комунікацій

Система комунікацій	Спосіб підключення
Система каналізації	Підключена до міської системи каналізації, кота виходить за межі КЗ.
Заземлення	Усі прилади заземлені на спільний контур заземлення, котрий є замкненим і виходить за межі КЗ.
Система вентиляції	Приточно-витяжна
Система опалення	Відсутня

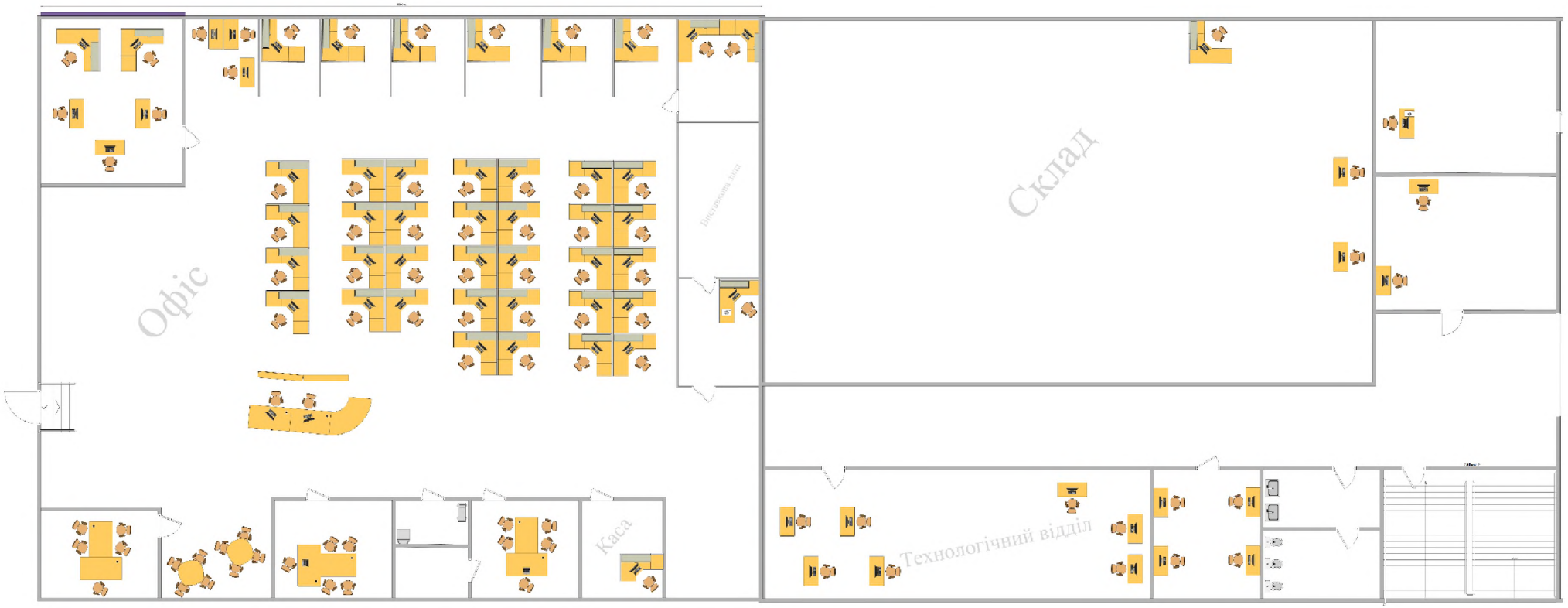


Рисунок 1.3 Генеральний план ч.1

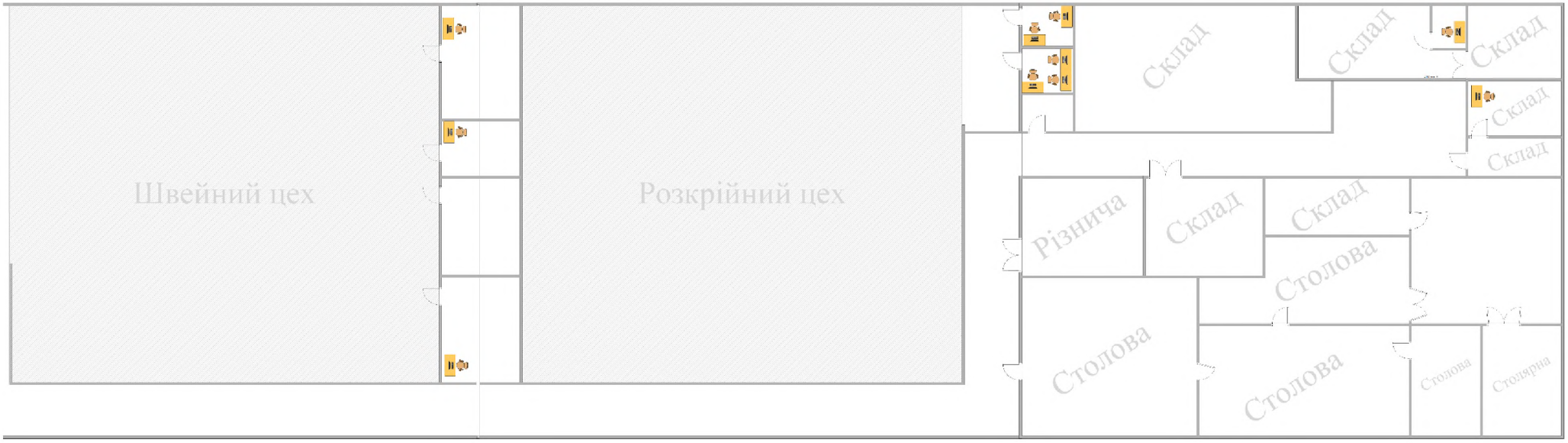


Рисунок 1.4 Генеральний план ч.2

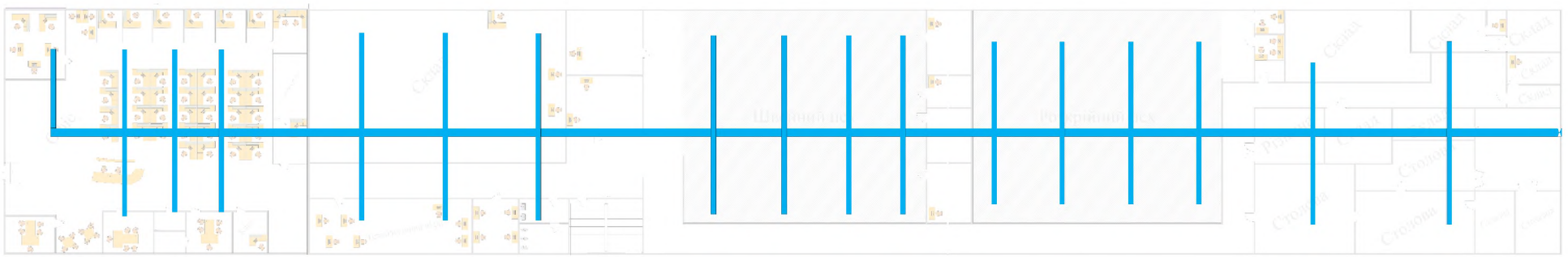


Рисунок 1.5 Генеральний план. Системи вентиляції

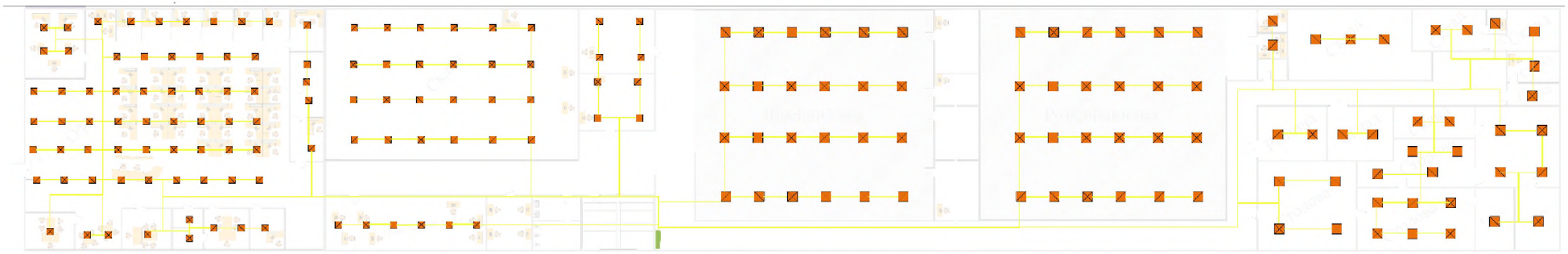


Рисунок 1.6 Генеральний план. Лінії системи електропостачання та освітлення

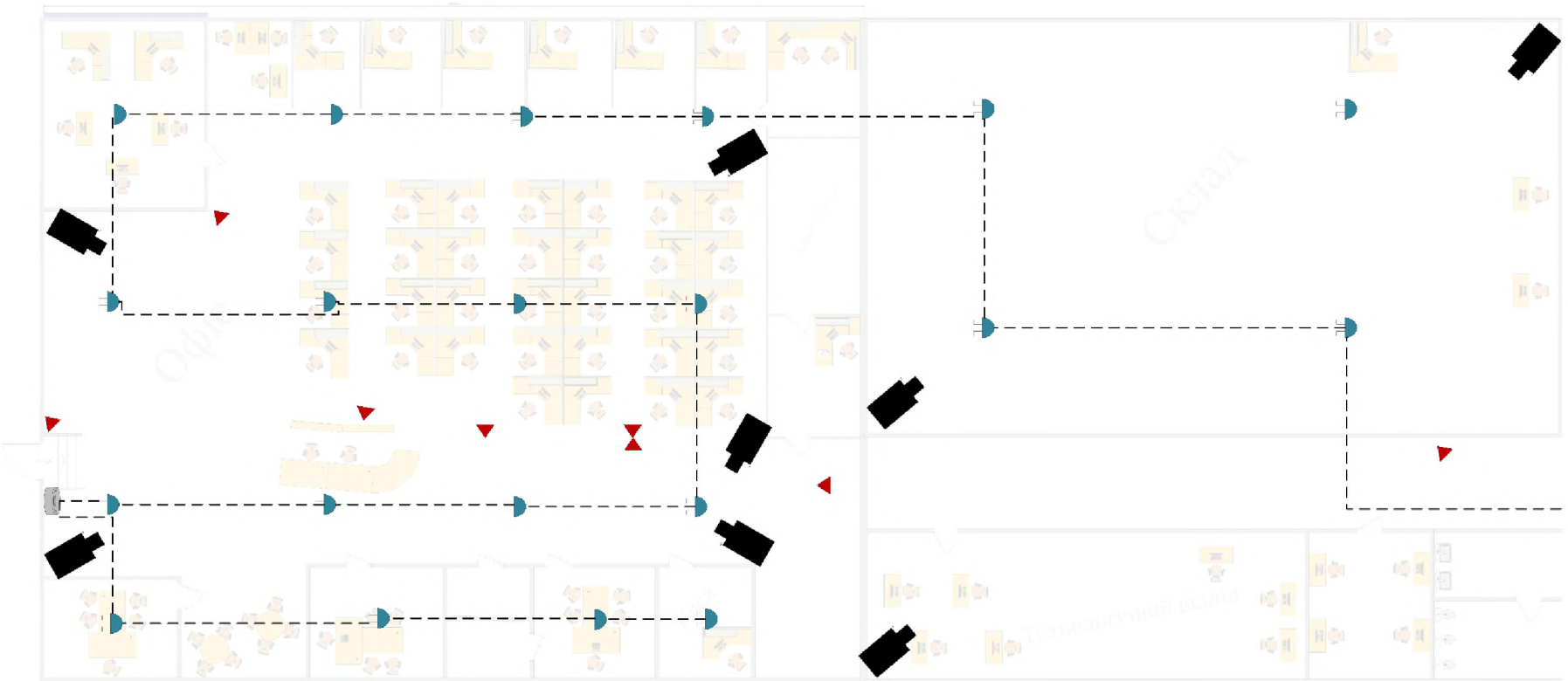


Рисунок 1.7 Генеральний план. Лінії системи охоронної та пожежної сигналізації. Ч. 1

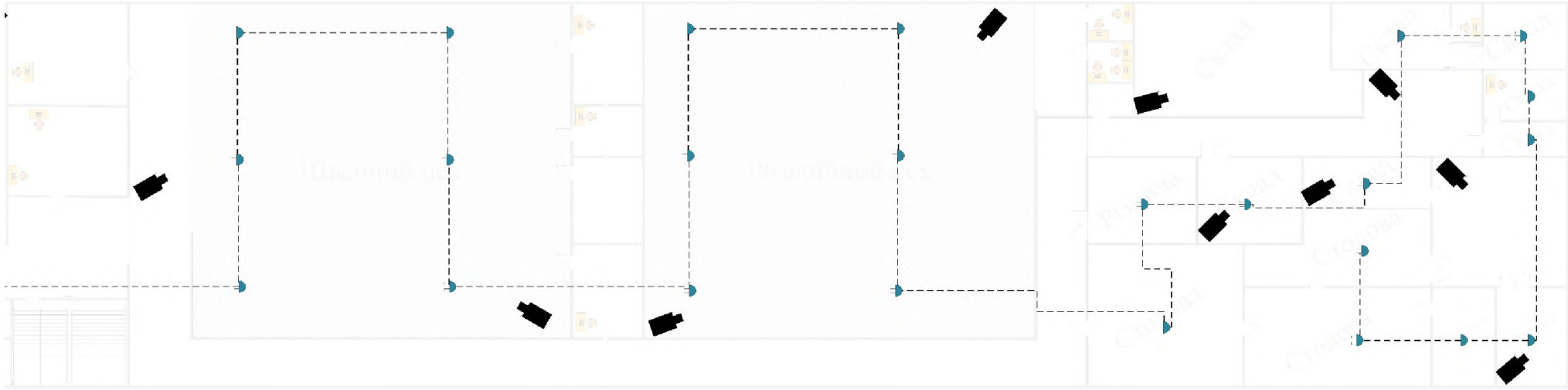


Рисунок 1.8 Генеральний план. Лінії системи охоронної та пожежної сигналізації. Ч. 2

Автоматизована система налічує у собі 78 комп'ютерів (46 станцій в офісі, 2 – в IT відділі, 1 - в касі, 12 - у технологічному відділі, 3 - у швейному цеху, 8 - у розкрійному цеху, 6 - на складі), 2 ноутбуки (офіс, кабінети директорів), 10 серверів (IT відділ), 4 комутатори (IT відділ), маршрутизатор (IT відділ). АС має доступ до мережі Інтернет, провайдером якої є «Фрегат». Перелік основних технічних засобів наведено у таблиці 1.4. Позначення у таблиці 1.4 відповідає наступним назвам: РС – робоча станція, N – ноутбук, S – сервер, M – маршрутизатор, K – комутатор, МО – монітори, ММ – маніпулятор миша, КЛ – клавіатура, ПР – принтер.

Таблиця 1.4 – Перелік ОТЗ

№	Познач.	Марка	Модель	Серійний номер	Розміщення	Відстань до границі КЗ, м
1	PC-1	ARTLINE	Business B25 v26	3CFOBY	Офіс, опенспейс	0,5
2	PC-15			PNSZ16	Офіс, опенспейс	0,5
3	PC-16			3IOSE5	Офіс, опенспейс	0,7
4	PC-17			7H49J0	Офіс, опенспейс	0,7
5	PC-18			W2BX4M	Офіс, опенспейс	0,3
6	PC-19			MN82BI	Офіс, опенспейс	0,7
7	PC-20			BH61DT	Офіс, опенспейс	0,3
8	PC-26			EU9CB3	Офіс, опенспейс	0,7

Продовження таблиці 1.4 – Перелік ОТЗ

№	Познач.	Марка	Модель	Серійний номер	Розміщення	Відстань до границі КЗ, м
9	PC-27	ARTLINE	Business B25 v26	0OSVYW	Офіс, опенспейс	0,3
10	PC-28			U2Q6CX	Офіс, опенспейс	1
11	PC-29			6I9GC5	Офіс, опенспейс	1
12	PC-30			Q7BUI4	Офіс, опенспейс	2
13	PC-44			DZCLNK	Тех. відділ	1,5
14	PC-46 – PC-48	Everest	Home 4070	27VKT6-27VKT8	IT-відділ	0,2
15	PC-49	ARTLINE	Business B25 v26	RYJT4H	Каса	0,5
16	PC-50			PSJ4AU	Тех. відділ	0,5
17	PC-61			SOY9AQ	Тех. відділ	0,7
18	PC-62			Q51TAL	Тех. відділ	0,7
19	PC-67			9YPU06	Тех. відділ	0,7
20	PC-68			2KU7X6	Розкрійний цех	0,2
21	PC-70			8TCXFK	Склад	0,2
22	PC-73			S7XI8R	Склад	0,7
23	N-1 – N-2	Apple MacBook Pro	MXK62	96IY7E	Офіс (кабінети директорів)	0,2
24	S1-S10		Business R24	FPR9Y4-FPR9Z3	IT-відділ	1

Продовження таблиці 1.4 – Перелік ОТЗ

№	Познач.	Марка	Модель	Серійний номер	Розміщення	Відстань до границі КЗ, м
25	М-1	TP-LINK	Archer AX11000	AX9503	IT-відділ	0,4
26	К-1 – К-4	MikroTik	CRS326-24G-2S+RM	BT7WP1-BT7WP4	IT-відділ	0,4
27	МО-1 – МО-24	Dell	E2420H	J1E5K8-J1E5N4	Офіс, тех. відділ, IT-відділ, каса, склад, розкрійний цех	Від 0,2 до 1
28	ММ-1 – ММ-24	A4Tech	N-301	86YMF7-86YMH3	Офіс, тех. відділ, IT-відділ, каса, склад, розкрійний цех	Від 0,2 до 1
29	КЛ-1 – КЛ-24	Logitech	K120	1A6NV8-1A6NX8	Офіс, тех. відділ, IT-відділ, каса, склад, розкрійний цех	Від 0,2 до 1
30	ПР-1 – ПР-10	Canon	i-SENSYS MF3010	Z5ELM6-Z5ELN4	Офіс	3-5

Таблиця 1.5 – Перелік ДТЗС

№	Назва	Марка	Модель	Серійний номер	Розміщення
1	X-1	SHARP	SJ-T1227M5W-UA	45QNKD	Офіс
2	MX-1	PANASONIC	NN-ST251WZPE	X6KT24	Офіс
3	CC-1 – CC-18	Dahua	DH-HAC-HDW1000RP-S3	79AZB2-79AZC9	Офіс
4	ІЧД-1 ІЧД-8	Pyronix	KX10DTP	W3C7HO	Офіс
5	PC-2 – PC-14	ARTLINE	Business B25 v26	UFISJP	Офіс
6	PC-21 – PC-25			WVBT79	Офіс
7	PC-31 – PC-43			IM6VYT	Офіс
8	PC-45			4YISX7	Офіс
9	PC-51– PC-60			7SH8BX	Тех. відділ
10	PC-63 – PC-66			JR7YNZ	Тех. відділ
11	PC-71 – PC-72			NQSKYG	Розкрійний цех
12	PC-74 – PC-78			D5TAIE	Склад

Позначки у таблиці 1.5: Х – холодильник, МХ – мікрохвильова піч, СС – камери відеоспостереження, ІЧД – інфрачервоний датчик, РС – робоча станція.

1.4 Обстеження обчислювальної системи

Структурна схема обчислювальної системи на підприємстві являє собою локальну систему з виходом до мережі Інтернет. В центрі мережі знаходиться комутатор, через який усі користувачі системи мають доступ до Інтернету. Така технологія називається «пасивна зірка». Увесь зв'язок між користувачами та сервером відбувається через комутатор. Також до складу обчислювальної системи входять принтери.

Локальна мережа створена для забезпечення внутрішніх потреб підприємства. Для забезпечення взаємодії з іншими організаціями всі робочі станції мають доступ до мережі Інтернет.

Уся інформація міститься на серверах, які розподілені на відділи. Сервери з позначенням S1-S4 мають відношення до офісу, S5 – IT-відділ, S6-S8 – швейний цех та розкрійний цех, S9 - технічний відділ, S10 - склади.

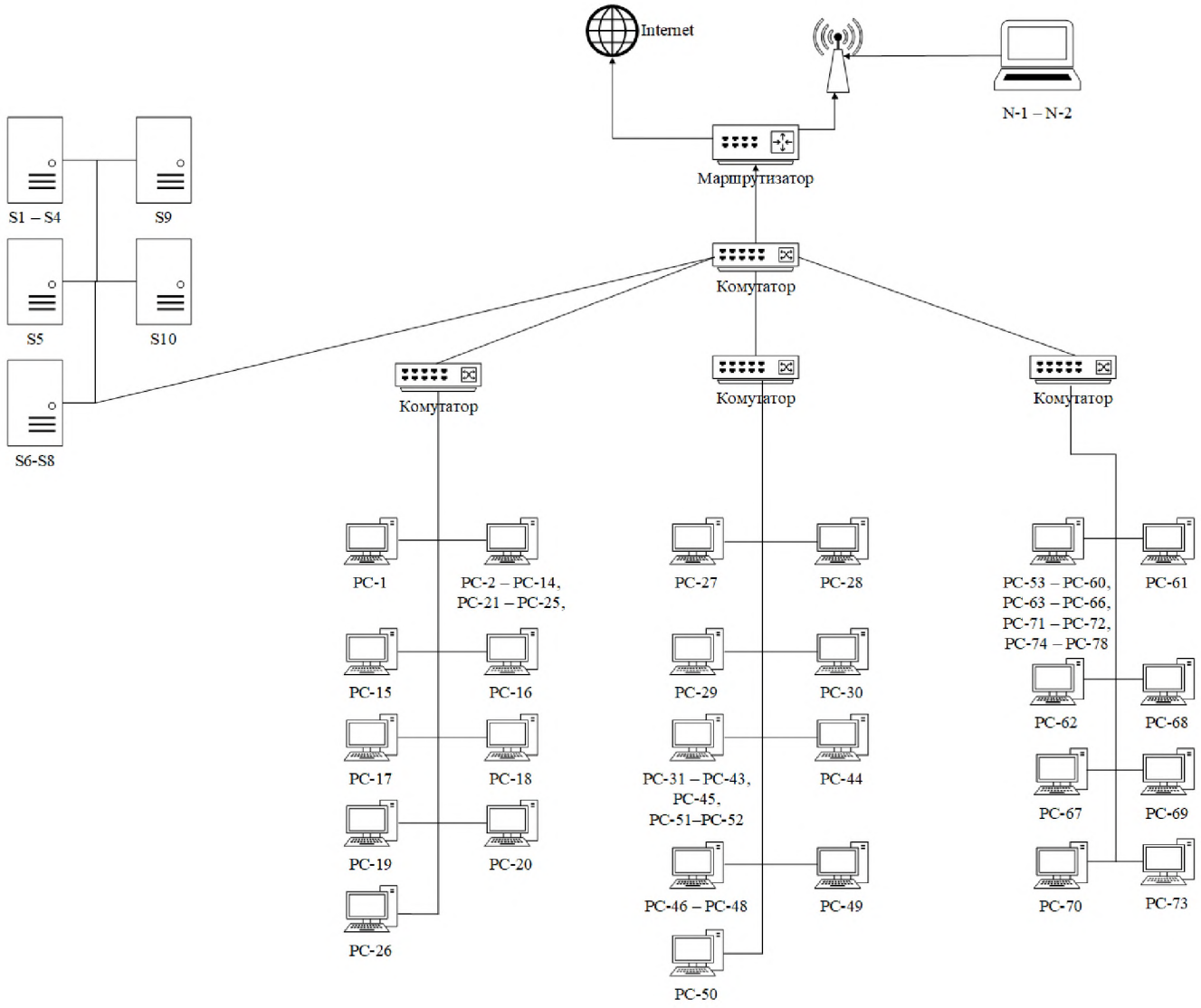


Рисунок 1.9 Структурна схема

Також наглядно у таблиці 1.6 перераховано програмне забезпечення, встановлене на всіх ПК, які використовують співробітники ТОВ «VIF».

Таблиця 1.6 – Характеристики апаратного забезпечення ОС

№	Позначення та назва	Характеристика
1	PC-1 – PC-48 Робочі станції в офісі	Intel Pentium Gold G6400 (4.0 ГГц) RAM 4 ГБ SSD 120 ГБ Intel UHD Graphics 610 Windows 7

Продовження таблиці – Характеристики апаратного забезпечення ОС

№	Позначення та назва	Характеристика
2	PC-47 – PC-48 Робоча станція в IT-відділі	Intel Core i5-9400F (2.9 - 4.1 ГГц) RAM 16 ГБ HDD 1 ТБ + SSD 240 ГБ nVidia GeForce GTX 1650, 4 ГБ
3	PC-49 Робоча станція в касі	Intel Pentium Gold G6400 (4.0 ГГц) RAM 4 ГБ SSD 120 ГБ Intel UHD Graphics 610 Windows 7
4	PC-50 – PC-61 Робочі станції у технічному відділі	
5	PC-62 – PC-65 Робочі станції у швейному цеху	
6	PC-66 – PC-72 Робочі станції у розкрійному цеху	
7	PC-73 - PC-78 Робочі станції на складах	
8	N-1 – N-2 Робочі станції в офісі	Intel Core i5-8257U RAM 8 ГБ SSD 256 ГБ Intel Iris Plus Graphics 645

Таблиця 1.7 – Перелік ПЗ в ІТС

№	Назва	Тип	Ліцензія	Місце встановлення
1	ОС Windows 7 Enterprise x64	Операційна система	Commercial	PC-1 – PC-78
2	1С:Підприємство	Спеціалізоване	Commercial	PC-1 – PC-78
3	Microsoft Word	Прикладне	Corporative	PC-1 – PC-78 N-1 – N-2

Продовження таблиці 1.7 – Перелік ПЗ в ІТС

№	Назва	Тип	Ліцензія	Місце встановлення
4	Microsoft Excel	Прикладне	Corporative	PC-1 – PC-78 N-1 – N-2
5	Adobe Acrobat Reader	Прикладне	Free	PC-1 – PC-78 N-1 – N-2
6	Google Chrome	Веб-браузер	Free	PC-1 – PC-78 N-1 – N-2
7	Adobe Photoshop	Прикладне	Не ліцензійне	PC-10 - PC-63
8	Microsoft Remote Desktop	Прикладне	Free	PC-1 – PC-78
9	macOS 11.2	Операційна система	Commercial	N-1 – N-2
10	360 Total Security 10.8.0.1200	Антивірусна програма	Free	PC-1 – PC-78
11	Windows Media Player 12.0.9600.17031	Прикладне	Free	PC-1 – PC-78

1.5 Обстеження інформаційного середовища

В автоматизованій системі відсутня інформація, що є власністю держави чи відомості, які становлять державну таємницю. Правила доступу до інформації розподілено директором. Доступ до ІзОД мають тільки зареєстровані в системі користувачі. В організації циркулює велика кількість персональних даних, як клієнтів так і співробітників.

Таблиця 1.8 – Класифікація інформації, яка циркулює на ІТС

№	Інформація	Опис	Режим доступу	Правовий режим	Вимоги до захисту
1	Персональні дані співробітників	ПІБ співробітників, домашні адреси, номери телефонів	ІзОД	Конфіденційна	К, Ц, Д
2	Дані про товар	Номери товарів, склад товарів	ІзОД	Конфіденційна	Ц, Д
3	Персональні дані клієнтів компанії	ПІБ клієнтів, номери телефонів	ІзОД	Конфіденційна	К, Ц, Д
4	Документація про постачальників	Назва, реквізити постачальників, адреса підприємств	ІзОД	Конфіденційна	К, Ц, Д
5	Звітність бухгалтерії	Інформація щодо фінансової стабільності компанії	ІзОД	Конфіденційна	К, Ц, Д
6	Інформація про надання послуг, контактна інформація	Прайслист компанії, база даних товарів	Відкрита	-	Ц, Д

Продовження таблиці 1.8 – Класифікація інформації, яка циркулює на ІТС

№	Інформація	Опис	Режим доступу	Правовий режим	Вимоги до захисту
7	Сертифікати на продукцію	-	Відкрита	-	Ц, Д
8	Організаційно-розпорядча документація	-	ІзОД	Конфіденційна	К, Ц, Д
9	Облік та реєстрація вхідних та вихідних документів	-	ІзОД	Конфіденційна	К, Ц, Д
10	Дані про матеріали для виробництва	Номери та кольори шкір, підкладок, тощо	Відкрита	-	Ц, Д
11	Статутні документи	Документи, що дозволяють займатись підприємницькою діяльністю	Відкрита	-	К, Ц, Д
12	Стратегічні плани розвитку підприємства	-	ІзОД	Конфіденційна	К, Ц, Д
13	Технологічна інформація	Паролі доступу до об’єкту, тощо	ІзОД	Конфіденційна	К, Ц, Д

Продовження таблиці 1.8 – Класифікація інформації, яка циркулює на ІТС

№	Інформація	Опис	Режим доступу	Правовий режим	Вимоги до захисту
14	Дизайн виробів	-	ІзОД	Комерційна таємниця	К, Ц, Д
15	Договори	Договори між покупцями, постачальниками, тощо	ІзОД	Конфіденційна	К, Ц, Д
16	Технології обробки матеріалів	-	ІзОД	Комерційна таємниця	К, Ц, Д

До інформації, що існує тільки у паперовому вигляді відноситься облік та реєстрація вхідних та вихідних документів. Усі інші види інформації існують як у паперовому так і в електронному вигляді.

На підприємстві циркулює інформація з обмеженим доступом, доступ до якої контролюється розподільним сервером. Також на підприємстві наявні принтери, доступ до яких має чітке розмежування.

Користувачі ТОВ розподілена на робочі групи: адміністратор, користувачі. Розмежування доступу поділяється на основі відділів, в яких працюють співробітники. Кожний співробітник підключається до сервера через Microsoft Remote Desktop під своїм ім’ям та через введення пароля.

Кожен відділ має доступ тільки до певних файлів, програм та інформації. У кожного відділу є свої права і обмеження. Обмін інформацією між відділами здійснюється за допомогою сервера або зовнішніх носіїв.

Таблиця 1.9 – Класифікація властивостей інформації

Рівні/назва	Конфіденційність	Цілісність	Доступність
1	К1 – приносить малозначний в рідкісних випадках	Ц1 – не відображатимуться на роботі системи	Д1 – підприємство не понесе значних збитків, його робота не буде порушена
2	К2 – приносить незначний матеріальний збиток в певних випадках	Ц2 – не приведуть до збою в роботі, наслідки можна запобігти	Д2 – підприємство понесе незначні збитки, його робота не буде порушена
3	К3 – приносить відчутний матеріальний збиток в певних випадках	Ц3 – призведуть до неправильної роботи через деякий час, наслідки можна запобігти	Д3 – підприємство понесе середні збитки, його робота не буде порушена
4	К4 – розголошення призводить до значних матеріальних витрат, якщо не буде вжито заходів	Ц4 – призведуть до неправильної роботи через деякий час, якщо не буде вжито заходів, наслідки не можна запобігти	Д4 – підприємство понесе значні збитки, його робота буде ускладнена
5	К5 – розголошення інформації призведе до краху роботи об’єкта чи до дуже великих матеріальних витрат	Ц5 – призведуть до неправильної роботи системи в цілому, наслідки не можна запобігти	Д5 – підприємство понесе значні збитки, його робота буде неможлива до прийняття радикальних змін

Після визначення властивостей інформації, розподілимо інформацію з таблиці 1.8.

Таблиця 1.10 – Визначення рівнів конфіденційності, цілісності та доступності інформації

Інформація	Конфіденційність	Цілісність	Доступність
Персональні дані співробітників	К3	Ц2	Д2
Персональні дані клієнтів компанії	К3	Ц3	Д3
Документація про постачальників	К2	Ц1	Д2
Звітність бухгалтерії	К4	Ц3	Д3
Організаційно-розпорядча документація	К3	Ц2	Д3
Облік та реєстрація вхідних та вихідних документів	К3	Ц3	Д2
Статутні документи	К2	Ц2	Д2
Стратегічні плани розвитку підприємства	К4	Ц3	Д3
Дані про товар	К1	Ц4	Д4
Технологічна інформація	К4	Ц4	Д4
Дизайн виробів	К3	Ц2	Д2

Продовження таблиці 1.10 – Визначення рівнів конфіденційності, цілісності та доступності інформації

Інформація	Конфіденційність	Цілісність	Доступність
Договори	К2	Ц2	Д2
Технології обробки матеріалів	К4	Ц4	Д3

1.6 Обстеження середовища користувачів

Середовище користувачів та їх обов'язки:

Бухгалтер (4 особи) – безпосередня участь у фінансовій діяльності підприємства, проведення всіх необхідних операцій з бухгалтерського обліку, складання фінансових розрахунків, тощо.

Головний інженер (1 особа) – визначення науково перспективи розвитку підприємства і шляхи реалізації комплексних програм з усіх напрямів удосконалення.

Головний технолог (1 особа) – керування складанням планів упровадження нової техніки і технології, підвищення ефективності виробництва, розробкою технологічної документації.

Дизайнер (6 осіб) – розробка фінального вигляду продукції.

Директор (1 особа) – визначення, формулювання, планування, здійснення і координація всіх видів діяльності підприємства, визначення напрямків розвитку підприємства у всіх аспектах його діяльності.

Диспетчер (1 особа) – керування водіями та поставками виробів.

Зам. директор департаменту HR (1 особа) – оцінка кандидатів під час прийняття на роботу, планування навчання і розвиток персоналу, мотивація, атестація, організація психологічної підтримки тощо

Зам. директор департаменту виробництва (1 особа) – начальник управління з питань розвитку виробництва.

Зам. директор департаменту маркетингу (1 особа) – формування та реалізація маркетингової політики, аналіз ринкового середовища, тощо.

Зам. директор департаменту продажу (1 особа) – розробка планів роботи та продажу на місяць, визначення стратегію розвитку регіону, окремих територій регіону тощо.

Зам. директор логістики (1 особа) – управління складською логістикою і вантажопереробкою, управління транспортною логістикою, тощо.

Інженер-технолог (2 особи) – розробка технологічних нормативів, інструкції, схем збірки, та іншої технологічної документації, внесення змін в технічну документацію у зв'язку з коригуванням технологічних процесів і режимів виробництва.

Керівник роздрібної мережі (1 особа) – здійснення раціональної та ефективної організації збуту продукції підприємства через мережу роздрібних філіалів компанії, здійснює планування, прогнозування і виконання планів продажів філіалами роздрібної мережі компанії.

Консультант Call-центру (17 осіб) – консультування потенційних клієнтів, використовуючи базу даних виробів підприємства.

Маркетолог (15 осіб) – збір та аналіз даних про смакові переваги покупців, збір інформації про продажі, на основі яких аналізується попит, проведення маркетингових досліджень.

Менеджер ЗЕД (5 осіб) – забезпечення стабільного зв’язку підприємства з контрагентами, що знаходяться за кордоном, організація співпраці з ними, а також сприяння поліпшенню ділових стосунків із цими іноземними підприємствами.

Менеджер оптових продаж (1 особа) – керівництво торговими представниками.

Начальник відділу реклами (1 особа) – визначення напрямків і планування рекламних кампаній, формування рекламної стратегії, заснованої на перспективних напрямках подальшого організаційного розвитку, інноваційної та інвестиційної діяльності.

Начальник об'єднаних складів (1 особа) – здійснення контролю прийому товару на склад по якості і кількості, з оформленням відповідних документів.

Начальник розкрійного цеху (1 особа) – контроль за настиланням матеріалу на настилочний комплекс та подальший розкрій на розкрійнім комплексі з установкою оптимальних параметрів.

Начальник складу (1 особа) – керування роботами, які охоплюють прийом, зберігання і відпуск товарно-матеріальних цінностей на складі, їх розміщення з урахуванням найбільш раціонального використання складських площ, полегшення і прискорення пошуку необхідних матеріалів, інвентарю тощо.

Начальник швейного цеху (1 особа) – організація поточного виробничого планування, облік, складання і своєчасне подання звітності про виробничу діяльність цеху, роботу з впровадження нових форм виробництва, поліпшення нормування праці.

Секретар (6 осіб) – виконання робіт по накопиченню, оформленню, обробці усної та письмової інформації, а також організація та прийом відвідувачів, підготовка засідань і нарад.

Системний адміністратор (3 особи) – виконує функції забезпечення справної роботи КС (здійснення технічне обслуговування апаратного і програмного забезпечення, слідкування за станом антивірусного захисту, проведення періодичних перевірок критичних секцій робочих станцій).

Спеціаліст з відбору персоналу (5 осіб) – розробка і підтримка корпоративного стилю компанії, підбір кандидатів на вакантні місця, створення системи заохочення і покарання працівників підприємства.

Фінансовий аналітик (1 особа) – моніторинг ситуації на фінансових ринках, аналіз роботи компанії і конкурентів, регулярне консультування з фінансових питань, а також складання щоденних аналітичних оглядів і звітів.

Для аналізу доцільності прав доступу до інформації усіх працівників підприємства визначимо основні посади та їх дозволи щодо користування інформацією.

Таблиця 1.11 – Матриця керування доступом

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Бухгалтер	-	-	-	ЧТД	ЧРЗВТД	ЧТД	-	ЧЗТД	-	-	ЧТД	-	-	-	-	-
Головний інженер	-	ЧЗТД	-	-	-	-	ЧТД	ЧТД	-	ЧТД	ЧТД	-	-	-	-	-
Головний технолог	-	ЧЗТД	-	-	-	-	ЧТД	ЧТД	-	ЧТД	ЧТД	-	-	-	-	ЧЗТД
Дизайнер	-	ЧЗТД	-	-	-	-	-	-	-	ЧТД	-	-	-	ЧРЗВТД	-	-
Директор	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД
Диспетчер	-	ЧЗТД	-	ЧЗТД	-	ЧЗТД	ЧЗТД	ЧТД	-	ЧЗТД	ЧТД	-	-	-	-	-
Зам. директор департаменту HR	ЧРЗТД	ЧТД	-	-	-	-	-	ЧТД	-	-	ЧТД	-	-	-	-	-
Зам. директор департаменту виробництва	ЧТД	ЧРЗВ	-	-	-	-	ЧРЗТД	ЧТД	-	ЧРЗВТД	ЧТД	-	-	-	-	ЧД

Продовження таблиці 1.11 – Матриця керування доступом

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Зам. директор департа-менту маркетингу	-	ЧЗТД	-	-	-	-	ЧТД	ЧТД	-	-	ЧТД	-	-	Ч	-	-
Зам. директор департа-менту продажу	-	ЧЗТД	ЧРЗВТД	-	ЧТД	ЧРЗВТД	ЧЗТД	ЧТД	-	ЧТД	ЧТД	-	-	-	-	-
Зам. директор логістики	ЧТД	ЧЗТД	-	ЧРЗВТД	ЧТД	-	ЧЗТД	ЧТД	-	ЧЗТД	ЧТД	-	-	-	-	-
Інженер-технолог	-	ЧТД	-	-	-	-	-	-	-	ЧТД	-	-	-	-	-	-
Керівник роздрібної мережі	-	ЧТД	-	-	-	ЧРЗВТД	ЧТД	ЧТД	-	ЧТД	ЧТД	-	-	-	-	-
Консуль-тант Call-центру	-	ЧТД	ЧРЗВТД	-	-	ЧТД	ЧТД	ЧТД	-	ЧТД	-	-	-	-	-	-
Маркето-лог	-	ЧТД	-	-	-	ЧЗТД	-	-	-	-	-	-	-	-	-	-
Менеджер ЗЕД	-	-	-	-	ЧРЗТД	ЧТД	ЧТД	ЧТД	-	-	-	-	-	-	-	-

Продовження таблиці 1.11 – Матриця керування доступом

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Менеджер оптових продаж	-	ЧРЗТД	ЧРЗВТД	ЧЗТД	ЧРЗТД	ЧЗТД	ЧТД	ЧТД	-	ЧТД	ЧТД	-	-	-	-	-
Начальник відділу реклами	ЧТД	-	-	-	-	ЧТД	ЧТД	ЧТД	-	-	ЧТД	-	-	-	-	-
Начальник об'єднаних складів	ЧТД	ЧРЗВТД	-	ЧТД	-	-	ЧТД	ЧТД	-	ЧРЗВТД	ЧТД	-	-	-	-	-
Начальник розкрійного цеху	ЧТД	ЧРЗВТД	-	ЧТД	-	-	ЧТД	ЧТД	-	ЧРЗВТД	ЧТД	-	-	-	-	-
Начальник складу	ЧТД	ЧРЗВТД	-	ЧТД	-	-	ЧТД	ЧТД	-	ЧРЗВТД	ЧТД	-	-	-	-	-
Начальник швейного цеху	ЧТД	ЧРЗВТД	-	ЧТД	-	-	ЧТД	ЧТД	-	ЧРЗВТД	ЧТД	-	-	-	-	-
Секретар	-	-	-	ЧТД	ЧРЗТД	ЧТД	ЧТД	ЧТД	-	-	ЧЗТД	ЧЗТД	-	-	-	-
Системний адміністратор	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД

Продовження таблиці 1.11 – Матриця керування доступом

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Спеціаліст з відбору персоналу	Ч ЗТ Д	-	-	-	-	-	-	Ч Т Д	-	-	-	-	-	-	-	-
Фінансовий аналітик	-	Ч ЗТ Д	Ч Т Д	Ч ЗТ Д	Ч ЗТ Д	Ч ЗТ Д	Ч Т Д	Ч Т Д	-	-	Ч Т Д	Ч Т Д	-	-	Ч	-

Позначення у таблиці 1.11: Ч – читання, Р – редагування, З – збереження, В – видалення, Т – імпорт/експорт, Д – друк. Цифрами від 1 до 12 позначена інформація з таблиці 1.8.

Аналізуючи таблицю 1.11 – Матриця розмежування доступу можна сказати, що у більшості користувачів є надлишкові права.

1.7 Модель порушника

Згідно НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» порушник розглядається як особа, що може одержати доступ до роботи з включеними засобами, що входять до складу КЗ. Модель порушника – це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії тощо, яка використовується сумісно з моделлю загроз для розробки комплексної системи захисту інформації. Модель порушника має визначати наступні фактори:

- можливі цілі порушника, їх градація;
- категорії користувачів (персоналу), ІТС та сторонніх осіб, із числа яких може бути порушник;
- припущення про кваліфікацію порушника;
- припущення щодо характеру дій порушника (за часом, місцем дії та інші).

Метою порушника може бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- внесення зміни в інформаційні потоки у відповідності зі своїми інтересами;

– збирання відомості про систему, тощо.

Вважається, що за своїм рівнем порушник - це фахівець вищої кваліфікації, який має повну інформацію про систему.

Спочатку потенційних порушників можна поділити на зовнішніх та внутрішніх. Зовнішнього порушника можна охарактеризувати як особу (або групу осіб), що не мають допуску до об'єкту. Внутрішні порушники – це особи, що мають допуск до об'єкту (співробітники, персонал, тощо) та безпосередньо мають доступ до взаємодії з інформацією, що циркулює на об'єкті.

Слід зазначити, що всі злочини, в тому числі і комп'ютерні, здійснюються людьми. Користувачі АС є її складовою частиною, необхідним елементом. З іншого боку, саме вони є основною причиною і рушійною силою порушень і злочинів. Таким чином, питання безпеки об'єктів, що знаходяться під охороною - це, по суті, питання людських відносин і людської поведінки.

Внутрішній порушник «ПВ» - варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов'язків.

Зовнішній порушник «ПЗ4» - це вид граничних загроз згідно причини цілеспрямованих несанкціонованих дій з метою модифікації або крадіжки даних.

Графа «Рівень загроз» таблиці 1.12 визначає відносну оцінку можливих збитків, які може створити порушник за умов наявності відповідних характеристик. Рівень збитків характеризується такими категоріями: 1 – незначні, 2 – середні, 3 – значні, але здебільшого припустимі, 4 – дуже значні.

Таблиця 1.12 – Категорія порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загрози
Внутрішні по відношенню до ІТС		
ПВ1	Працівники офісу	3
ПВ2	Працівники технологічного відділу	2
ПВ3	Працівники розкрійного цеху	2
ПВ4	Працівники складу	2
ПВ5	Адміністратори ІТС	4

Продовження таблиці 1.12 – Категорія порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загрози
ПВ6	Технічний персонал, який обслуговує будови та приміщення (прибиральниці, тощо), в яких розташовані компоненти ІТС	2
ПВ7	Керівники різних відділів	2
ПВ8	Директор	4
Зовнішні по відношенню до ІТС		
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водопостачання і таке інше)	2
ПЗ3	Хакери	4
ПЗ4	Агенти конкурентів	4

Таблиця 1.13 – Специфікація моделі порушника за мотивами здійснення порушень

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

Таблиця 1.14 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

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

Таблиця 1.15 – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

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

Таблиця 1.16 – Специфікація моделі порушника за часом дії

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

Таблиця 1.17 – Специфікація моделі порушника за місцем дії

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

Таблиця 1.18 – Модель порушника внутрішнього

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання систем захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Працівники офісу	ПВ1	М2	К2	З2	Ч3	Д2	**14**
	3	2	2	2	3	2	
Працівники технічного відділу	ПВ2	М2	К1	З2	Ч3	Д2	**12**
	2	2	1	2	3	2	
Працівники розкрійного цеху	ПВ3	М2	К1	З2	Ч3	Д2	**12**
	2	2	1	2	3	2	
Працівники складу	ПВ4	М2	К1	З2	Ч3	Д2	**12**
	2	2	1	2	3	2	
Адміністратори ІТС	ПВ5	М3	К4	З3	Ч4	Д4	**22**
	4	3	4	3	4	4	
Технічний персонал	ПВ6	М1	К1	З1	Ч1	Д1	**7**
	2	1	1	1	1	1	
Керівники різних розділів	ПВ7	М3	К3	З3	Ч3	Д3	**17**
	2	3	3	3	3	3	

Продовження таблиці 1.18 – Модель порушника внутрішнього

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання систем захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор	ПВ8	М3	К3	З3	Ч3	Д3	**19**
	4	3	3	3	3	3	

Таблиця 1.19 – Модель порушника зовнішнього

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання систем захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Відвідувачі	ПЗ1	М2	К1	З1	Ч3	Д2	**10**
	1	2	1	1	3	2	
Представники організацій щодо питань технічного забезпечення	ПЗ2	М1	К3	З3	Ч3	Д1	**13**
	2	1	3	3	3	1	

Продовження таблиці 1.19 – Модель порушника зовнішнього

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання систем захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Хакери	ПЗ3	М4	К3	З4	Ч3	Д0	**18**
	4	4	3	4	3	0	
Агенти конкурентів	ПЗ4	М4	К3	З4	Ч3	Д4	**22**
	4	4	3	4	3	4	

Згідно таблиці 1.17 Модель порушника внутрішнього адміністратори ІТС є основною загрозою для системи. Оскільки вони виконують основні функції щодо забезпечення справного функціонування та безпеки інформаційно-телекомунікаційної системи.

Згідно таблиці 1.18 Модель порушника зовнішнього найбільшою небезпекою для системи є агенти конкурентів.

1.8 Модель загроз

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

Загрози конфіденційності (К) – неправомірний поступ до інформації. Ця загроза виникає коли отримано доступ до інформації з обмеженим доступом.

Загроза порушення цілісності (Ц) – являю собою навмисну замінну даних. Вона виникає через випадкові помилки програм чи напрямлені дії сторонніх осіб.

Загроза доступності (Д) – це створення умов, за яких доступ до послуги або інформації буде або заблокований, або можливий протягом певного періоду, який не забезпечить досягнення деяких бізнес-цілей.

Загрози націлені на різні аспекти завдають шкоди інформації, персоналу, обладнанню, процесам тощо. В свою чергу вони можуть поділятися на навмисні, випадкові та природні. Навмисні загрози спровоковані безпосередньо людиною задля своїх корисних цілей або цілей компаній. Випадкові загрози виникають у разі дій або подій які були вчинені ненавмисно і без корисливого наміру. Випадкові загрози природнього характеру розглядаються як окремий вид. Детальні дані наведені в таблиці 1.20.

Таблиця 1.20 – Модель загроз ІТС

№	Вид загрози	Джерело загрози	Вразливість	Порушення	Рівень		Сума загроз
					Ризиків	Загроз	
1. Навмисні загрози (антропогенні та техногенні)							
1.1	НСД сторонніх осіб до ІзОД внаслідок несанкціонованого фізичного доступу до обладнання	Зовнішнє	– Неефективна система охорони – Недостатній контроль за приміщенням – Безвідповідальність приймаючого співробітника	К	2	3	5
				Ц	3	4	7
				Д	2	3	5
1.2	Порушення конфіденційності або цілісності інформації, що зберігається в ІТС, внаслідок навмисних дій уповноваженого користувача	Внутрішнє	– Відсутність функції резервного копіювання – Неправильний підбір персоналу	К	2	4	6
				Ц	2	4	6

Продовження таблиці 1.20 – Модель загроз ІТС

№	Вид загрози	Джерело загрози	Вразливість	Порушення	Рівень		Сума загроз
					Ризиків	Загроз	
1.3	Навмисне виведення з експлуатації систем життєзабезпечення мережі (електроживлення, охоронна і т.д.)	Внутрішнє	– Неефективна система охорони – Недостатній контроль за приміщенням	К	1	2	3
				Ц	2	4	6
				Д	2	4	6
1.4	Впровадження та використання комп'ютерних вірусів, шкідливих програм для порушення безпеки даних	Внутрішнє, зовнішнє	– Неефективність антивірусного ПЗ	К	2	4	6
				Ц	3	3	6
				Д	3	4	7
1.5	Використання зовнішніх носіїв інформації	Внутрішнє	– Недостатній контроль за системою	К	2	3	5
				Ц	2	4	6
				Д	2	4	6

Продовження таблиці 1.20 – Модель загроз ІТС

№	Вид загрози	Джерело загрози	Вразливість	Порушення	Рівень		Сума загроз
					Ризиків	Загроз	
1.6	Використання спеціального програмного забезпечення для здійснення неправомірного доступу	Внутрішнє, зовнішнє	– Недостатній контроль за приміщенням – Неефективна система охорони – Неефективність антивірусного ПЗ	К	2	3	6
				Ц	2	3	6
				Д	2	3	6
1.7	Скачування та запуск додатків з Інтернету	Внутрішнє	– Відсутність квот	К	3	3	6
				Ц	2	3	5
				Д	2	4	6
1.8	Несанкціоноване перехоплення інформації (за допомогою ПЕМВН, підключення до каналів передачі інформації, тощо)	Зовнішнє	– Старе приміщення – Відсутність контролю за мережами за межами підприємства	К	1	4	5
				Ц	2	3	5
				Д	2	4	6

Продовження таблиці 1.20 – Модель загроз ІТС

№	Вид загрози	Джерело загрози	Вразливість	Порушення	Рівень		Сума загроз
					Ризиків	Загроз	
1.9	Одержання технологічної інформації (атрибутів доступу адміністраторів або інших користувачів системи) іншим користувачем ІТС атрибутами доступу для розширювання своїх повноважень	Внутрішнє	– Необізнаність персоналу – Неефективність ідентифікації та автентифікації користувача	К	3	3	6
				Ц	2	3	5
				Д	2	3	5
1.10	Перевищення посадових обов'язків системним адміністратором	Внутрішнє	– Неефективність використання людського ресурсу	К	2	5	7
				Ц	2	5	7
				Д	2	5	7
2. Випадкові загрози							
2.1	Розголошення інформації	Зовнішнє	– Людський фактор	К	3	1	4
				Ц	1	1	2
				Д	1	1	2

Продовження таблиці 1.20 – Модель загроз ІТС

№	Вид загрози	Джерело загрози	Вразливість	Порушення	Рівень		Сума загроз
					Ризиків	Загроз	
2.2	Порушення інформації, внаслідок ненавмисних дій користувачів	Внутрішнє	– Відсутність резервного копіювання	Ц	2	2	4
				Д	2	2	4
2.3	Випадкове зараження системи комп'ютерними вірусами	Внутрішнє	– Необізнаність персоналу – Неякісне антивірусне програмне забезпечення	К	2	4	6
				Ц	2	4	6
				Д	2	4	6
2.4	Випадкове делегування користувачеві привілеїв іншого користувача	Внутрішнє	– Необізнаність персоналу	К	2	3	5
				Ц	2	3	5
				Д	2	3	5

Продовження таблиці 1.20 – Модель загроз ІТС

№	Вид загрози	Джерело загрози	Вразливість	Порушення	Рівень		Сума загроз
					Ризиків	Загроз	
2.5	Надходження фішингових листів на електронну пошту підприємства	Зовнішнє	– Необізнаність персоналу – Неефективність антивірусного ПЗ	К	2	4	6
				Ц	2	4	6
				Д	2	4	6
2.6	Помилки персоналу	Внутрішнє	– Необізнаність персоналу	К	1	1	2
				Ц	2	2	4
				Д	2	2	4
2.7	Збої в роботі програмних та апаратних засобів	Внутрішнє	– Недосконале або нове програмне забезпечення	К	1	2	3
				Ц	2	3	5
				Д	2	3	5
2.8	Використання застарілої версії Windows	Внутрішнє	– Застаріла операційна система	К	2	3	5
				Ц	1	1	2
				Д	1	2	3

Продовження таблиці 1.20 – Модель загроз ІТС

№	Вид загрози	Джерело загрози	Вразливість	Порушення	Рівень		Сума загроз
					Ризиків	Загроз	
3. Стихійні (впливи природних факторів)							
3.1	Стихійні лиха (землетрус, пожежа, тощо)	Зовнішнє	– Наявність легкозаймистих матеріалів – Старе приміщення	Ц	2	5	7
				Д	2	5	7
3.2	Впливи природніх завад (іскріння в електромережах, грозові розряди)	Зовнішнє	– Неякісна електропроводка – Відсутність резервних каналів електроживлення	Ц	2	5	7
				Д	2	5	7

Рівні ризиків та загроз:

- Низький. Оцінюється в 1 бал. Несе за собою незначні збитки.
- Середній. Оцінюється в 3 бали. Несе за собою збитки середніх розмірів.
- Високий. Оцінується в 5 балів. Несе за собою збитки великих масштабів.

Згідно інформації, наведеної у таблиці 1.20 можна зробити висновок, що є необхідність у забезпеченні заходів для підвищення захисту. Актуальними загрозами для ІС є:

- зараження та використання комп'ютерних вірусів, шкідливих програм. Вразливість: використання застарілої версії Windows, надходження фішингових листів на електронну пошту підприємства, використання зовнішніх носіїв інформації. Наслідки: порушення безпеки інформації;
- скачування та запуск додатків з Інтернету. Вразливість: вільне використання Інтернет ресурсів. Наслідки: використання неліцензійного програмного забезпечення;
- випадкове делегування користувачеві привілеїв іншого користувача. Вразливість: неправильне розмежування прав адміністрування, неправильне розмежування прав доступу. Наслідки: отримання співробітниками доступу до ІзОД.
- НСД сторонніх осіб до ІзОД внаслідок несанкціонованого фізичного доступу до обладнання. Вразливість: недостатній контроль за діями відвідувачів. Наслідки: порушення конфіденційності, цілісності та доступності інформації.

1.9 Висновки до 1 розділу

У першому розділі дипломної роботи було розглянуті:

- рід діяльності підприємства;
- фізичне середовище;
- середовище користувачів;
- середовище обчислювальної системи.

Виконаний аналіз правил розмежування доступу матриця доступу, моделі порушника та загроз, проведено їх аналіз та виявлено актуальні загрози. Окрім цього, виконано класифікації інформації, що циркулює на об’єкті.

РОЗДІЛ 2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Оцінка існуючого стану захищеності

На підприємстві застосовується антивірусне програмне забезпечені від компанії Qihoo під назвою 360 Total Security, ліцензія якого є вільного доступу. Оновлення проходять в автоматичному режимі та сканують усі комп'ютери у мережі. Через те, що використовується версія вільного доступу, антивірусна програма не має можливостей «глибокого» сканування. Як висновок можна сказати, що антивірусне ПЗ не є максимально ефективним.

Для входу у систему працівником як логін використовується ім'я та прізвище користувача та унікальний пароль. Існує дві вимоги до паролю: мінімальна довжина не менше 6 символів та не дозволяється використовувати для паролю особисту інформацію (прізвище, дата народження, тощо).

До входу на ОІД потрібно мати персоналізовану картку-перепустку. За допомогою якої в системі реєструється дата та час появи кожного співробітника на початку робочого дня. По закінченню робочого дня кожний працівник має прикласти картку до сканера ще раз, для того щоб система зареєструвала час, коли працівник покинув підприємство.

2.2 Вибір профілю захищеності та визначення рівня гарантій

Операційна система Microsoft Windows 7 відповідає вимогам НД з ТЗІ але через застарілість версії операційної системи неможливо її використання в ІТС. Настійно рекомендується змінити версію операційної системи на Microsoft Windows 10. Відповідає вимогам НД з ТЗІ в обсязі функцій, зазначених у документі "Державна експертиза за критеріями технічного захисту інформації операційної системи Microsoft Windows 10 Professional. Технічні вимоги", що визначаються функціональним профілем: КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1, ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1 з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99 та має Експертний висновок №1027 дійсний з 26.09.2019.

Показник гарантій – це показник рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації. Для КС на ТОВ «VIF» він відповідає показнику Г-2.

Як було зазначено раніше, АС на ТОВ «VIF» відповідає класу «3». Відповідно до НД ТЗІ 2.5-005-99 зі змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу», обрано функціональний профіль захисту системи але з деякими змінами.

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

Згідно з НД ТЗІ 2.5.004-99:

КД-2 – Базова довірча конфіденційність. Стандартна система вибіркового керування доступу дозволяє реалізувати базовий рівень даної послуги. У поточній конфігурації системи, послуга реалізована завдяки спискам контролю доступу. Необхідні умови: КО-1, НИ-1.

КА-2 – Базова адміністративна конфіденційність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу розпоряджатися потоками інформації від захищених об'єктів до користувачів. Реалізована завдяки системним адміністраторам, які надають рівні доступу до об'єктів та мають журнал доступу користувачів різних рівнів до інформації. Необхідні умови: КО-1, НО-1, НИ-1.

КО-1 – Повторне використання об'єктів. Реалізована. Ця послуга гарантує вірне повторне застосування загальних об'єктів, гарантуючи, те що в разі якщо загальний об'єкт призначений новому користувачеві або процесу, він не стане включати ніякої інформації. Через систему розмежування доступу до облікових записів.

КВ-2 – Базова конфіденційність при обміні. Не реалізована. Дана послуга дозволяє захистити об'єкти від несанкціонованого доступу, що міститься в них, при їх експорті/імпорті через незахищену середу.

КВ-1 – Мінімальна конфіденційність при обміні. Реалізована. Стандартними послугами операційної системи Microsoft Windows 10.

ЦД-1 – Мінімальна довірча цілісність. Реалізована. Дана послуга дає можливість користувачеві регулювати інформаційні потоки від імені інших користувачів до захищених об'єктів, що належать його домену. У системі присутня можливість надавати різні рівні доступу. Необхідні умови: НИ-1.

ЦА-2 – Базова адміністративна цілісність. Реалізована. Дана послуга дає можливість адміністратору або особливо уповноваженому користувачу регулювати потоком даних від користувачів до захищених об'єктів. В системі присутні уповноважені особи (системні адміністратори), які можуть керувати потоками інформації.

ЦО-1 – Обмежений відкат. Реалізована. Ця послуга дає можливість уберегти об'єкти від несанкціонованої модифікації інформації, що міститься в них, в період їх експорту/імпорту за допомогою незахищеного середовища. У системі наявна можливість відміни останніх дій (від 50 до 100 у різних програмах) у таких програмах як Microsoft World, Excel, Adobe Photoshop. Необхідні умови: НИ-1.

ДР-1 – Квоти. Не реалізована. Ця послуга дозволяє користувачам керувати використанням послуг та ресурсів.

ДВ-1 – Ручне відновлення. Реалізована. Ця послуга дозволяє повернути КС у відомий захищений стан після відмови або переривання обслуговування, спричинених помилками користувачів, недосконалістю програмного забезпечення або іншими непередбачуваними ситуаціями. Відновлення у відомий захищений стан відбувається завдяки системним адміністраторам. Необхідні умови: НО-1.

НР-2 – Захищений журнал. Реєстрація у журналі подій дає можливість здійснювати контроль за діями, небезпечними для КС. На підприємстві послуга реалізована на рівні НР-5 Аналіз у реальному часі. Інтерфейси моніторингу стану системи дозволяють виявляти та аналізувати несанкціоновані дії у реальному часі. Необхідні умови: НИ-1, НО-1.

НИ-2 – Одиночна ідентифікація і автентифікація. Реалізована. Ідентифікація та автентифікація дозволяють КЗЗ ідентифікувати та перевірити особистість користувача, що намагається отримати доступ до КС. Необхідні умови: НК-1.

НК-1 – Однонаправлений достовірний канал. Ця послуга дає можливість забезпечувати користувачеві можливість безпосередньої взаємодії з КЗЗ. Реалізована, за рахунок вбудованих функцій операційної системи Microsoft Windows 10.

НО-2 – Розподіл обов'язків адміністраторів. Дана послуга зменшує можливість навмисних або помилкових несанкціонованих дій користувача або адміністратора, а також обсяг потенційного збитку від подібних операцій. Умовно реалізована. АС має три особи, що виконують ролі адміністраторів системи. За бажанням власника ІТС можливе розподілення ролей адміністраторів. Необхідні умови: НИ-1.

НЦ-2 – КЗЗ з гарантованою цілісністю. Дана послуга визначає ступінь можливості КЗЗ захищатися та гарантувати свою здатність керувати захищеними об'єктами. Жодна КС не може вважатися захищеною, якщо засоби захисту є об'єктом для несанкціонованого впливу. В зв'язку з цим рівень НЦ-1 даної послуги є необхідною умовою для абсолютно всіх рівнів усіх інших послуг. Реалізована, за рахунок вбудованих функцій операційної системи Microsoft Windows 10.

НТ-2 – Самотестування при старті. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження при ініціалізації КЗЗ. Реалізована, за рахунок вбудованих функцій операційної системи Microsoft Windows 10, а також за допомогою антивирусного программного забезпечення. Необхідні умови: НО-1.

НВ-1 – Автентифікація вузла. Дана послуга дає можливість КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, ідентифікувати і автентифікувати цей КЗЗ з використанням захищеного механізму підтвердження ідентичності. Має виконуватися на підставі затвердженого протоколу автентифікації. Реалізована, за рахунок вбудованих функцій операційної системи Microsoft Windows 10.

НА-1 – Базова автентифікація відправника. Реалізована. Ця послуга дозволяє однозначно встановити відносини між певним об'єктом та певним користувачем, тобто той факт, що об'єкт був створений або відправлений цим користувачем. Кожна облікова запис містить інформацію щодо прізвища та ім’я користувача.

НП-1 – Базова автентифікація отримувача. Реалізована. Дана послуга дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Кожна облікова запис містить інформацію щодо прізвища та ім’я користувача.

2.3 Проектні рішення

2.3.1 Розробка вимог з інформаційної безпеки

Для підприємства ТОВ «VIF» необхідно впровадити ряд правил, які під час робочого процесу забороняють:

- підключати до робочого комп’ютера буд-які зовнішні пристрої (USB, зовнішні жорсткі диски, смартфони, тощо) без письмової згоди адміністратора системи чи директора;
- приносити з собою фотоапарати чи відеокамери усім співробітникам, крім фотографів;
- здійснювати фото/відеозапис документів, екранів моніторів, тощо;
- здійснювати фото/відеозапис товарів без узгодження з начальником відділу, до якого відноситься співробітник;
- приносити та користуватися диктофоном або іншою звукозаписуючою апаратурою;
- використовувати для входу на підприємство перепустку іншого співробітника;
- використовувати для входу у систему обліковий запис іншого співробітника;
- скачувати та встановлювати на робочу станцію стороннє програмне забезпечення;
- залишати на робочому місці нотатки у кінці робочого дня;

— використовувати мережу Інтернет для обміну інформацією розважального характеру;
— відправляти інформацію електронною поштою адресатам, які не мають відношення до інформації;
— відкривати посилання з електронних листів.

2.3.2 Розмежування прав адміністрування

На ОІД є троє осіб, що виконують ролі системних адміністраторів. Рекомендується впровадити розподіл обов'язків між системними адміністраторами на двох адміністраторів системи та адміністратор безпеки.

Адміністратор безпеки володіє усіма правами по впровадженню та налаштуванню КСЗІ, керує обліковими записами співробітників, слідкує за додержанням правил розмежування доступу, вносить зміни до них при зміні посади співробітників, а також при допуску їх до певної інформації.

Системний адміністратор слідкує за справним функціонуванням КС, вирішує технічні проблеми, що можуть виникнути з АС, проводить планові перевірки її компонентів.

Обов'язки адміністратора безпеки мають бути:

– визначення правил щодо використання КС користувачами;
– створення та видалення облікових записів користувачів;
– можливість повернення АС до нормального функціонування при збої;
– періодичне тестування системи на наявність загроз інформаційній безпеці;
– встановлення нового ПЗ або відновлення версій вже існуючого;
– перегляд і аналіз журналу подій;
– узгоджувати модернізацію АС з іншими адміністраторами та директором;
– попередження щодо поширення комп'ютерних вірусів;
– обробляти запит на зміну атрибутів доступу користувачів;
– видання квот користувачам.

2.3.3 Розробка правил розмежування доступу

Під час обстеження ОІД була розглянута матриця розмежування доступу у таблиці 1.11. В результаті її аналізу було визначено, що більшість користувачів мають надлишкові права особливо щодо друку та імпорту/експорту.

Таблиця 2.1 – Нова матриця розмежування доступом

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Бухгалтер	-	-	-	Ч	ЧРЗВТД	Ч	-	ЧЗД	-	-	ЧД	-	-	-	-	-
Головний інженер	-	ЧЗТД	-	-	-	-	ЧД	Ч	-	ЧД	-	-	-	-	-	-
Головний технолог	-	ЧЗТД	-	-	-	-	ЧД	Ч	-	ЧД	-	-	-	-	ЧЗТД	-
Дизайнер	-	ЧЗД	-	-	-	-	-	-	-	ЧТД	-	-	-	ЧРЗВТД	-	-
Директор	ЧРЗВТД	Ч	-	-	ЧД	-	-	ЧРЗВТД	-	-	-	-	-	-	ЧРЗВТД	-
Диспетчер	-	ЧЗ	ЧРЗ	ЧЗТД	-	ЧЗ	ЧЗД	-	-	ЧД	-	-	-	-	-	-
Зам. директор департаменту HR	ЧРЗ	Ч	-	-	-	-	-	Ч	-	-	ЧД	-	-	-	-	-

Продовження таблиці 2.1 – Нова матриця розмежування доступом

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Зам. директор департаменту виробництва	Ч	ЧРЗВТД	-	-	-	-	ЧРЗД	Ч	-	ЧРЗВТД	ЧД	-	-	-	ЧД	-
Зам. директор департаменту маркетингу	-	ЧЗД	-	-	-	-	ЧД	Ч	-	-	ЧД	-	Ч	-	-	-
Зам. директор департаменту продажу	-	ЧЗ	ЧРЗВД	-	-	ЧРЗВТД	ЧЗД	Ч	-	ЧД	ЧД	-	-	-	-	-
Зам. директор логістики	Ч	ЧЗД	-	ЧРЗВТД	-	-	ЧЗД	Ч	-	ЧЗТД	ЧД	-	-	-	-	Ч
Інженер-технолог	-	ЧД	-	-	-	-	-	-	-	ЧД	-	-	-	-	-	-
Керівник роздрібної мережі	-	Ч	-	-	-	ЧРЗВТД	ЧД	Ч	-	Ч	-	-	-	-	-	-
Консультант Call-центру	-	ЧД	ЧРЗВД	-	-	ЧД	ЧД	-	-	Ч	-	-	-	-	-	-
Маркетолог	-	Ч	-	-	-	ЧЗД	-	-	-	-	-	-	-	-	-	-
Менеджер ЗЕД	-	-	-	-	ЧРЗД	ЧД	ЧД	-	-	-	-	-	-	-	-	-

Продовження таблиці 2.1 – Нова матриця розмежування доступом

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Менеджер оптових продаж	-	ЧРЗД	ЧРЗВД	ЧЗД	ЧРЗ	ЧЗД	ЧД	-	-	ЧД	-	-	-	-	-	-
Начальник відділу реклами	Ч	-	-	-	-	ЧД	Ч	Ч	-	-	ЧД	-	-	-	-	-
Начальник об'єднаних складів	Ч	ЧРЗВТД	-	ЧТД	-	-	ЧД	Ч	-	ЧРЗВТД	ЧД	-	-	-	-	-
Начальник розкрійного цеху	Ч	ЧРЗВТД	-	Ч	-	-	ЧД	Ч	-	ЧРЗВТД	ЧД	-	-	-	-	-
Начальник складу	Ч	ЧРЗВТД	-	Ч	-	-	ЧД	Ч	-	ЧРЗВД	ЧД	-	-	-	-	-
Начальник швейного цеху	Ч	ЧРЗВТД	-	Ч	-	-	ЧД	Ч	-	ЧРЗВТД	ЧД	-	-	-	-	-
Секретар	-	-	-	ЧД	ЧРЗД	ЧД	ЧД	ЧТД	ЧД	-	ЧЗТД	ЧЗТД	-	-	-	-
Системний адміністратор	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД	ЧРЗВТД
Спеціаліст з відбору персоналу	ЧЗД	-	-	-	-	-	-	Ч	-	-	-	-	-	-	-	-

Продовження таблиці 2.1 – Нова матриця розмежування доступом

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Фінансовий аналітик	-	Ч З	Ч	Ч З	Ч З	Ч З	Ч	Ч	-	-	Ч	Ч Д	-	-	-	-

Позначення у таблиці 2.1: Ч – читання, Р – редагування, З – збереження, В – видалення, Т – імпорт/експорт, Д – друк. Цифрами від 1 до 12 позначена інформація з таблиці 1.8.

2.3.4 Обґрунтування вибору системи антивірусного захисту

У розглянутій таблиці 1.20 – Модель загроз ІТС було виявлено три загрози, що походять від зараження вірусами, а саме:

— впровадження та використання комп'ютерних вірусів, шкідливих програм для порушення безпеки даних;

— випадкове зараження системи комп’ютерними вірусами;

— надходження фішингових листів на електронну пошту підприємства.

З цієї причини має буте переглянуто встановлене антивірусне ПЗ. Для зміни антивірусного програмного забезпечення були розглянуті такі продукти як: Bitdefender Gravityzone Elite Security, ESET NOD32 Smart Security Business Edition, McAfee, BullGuard Internet Security, Panda Dome Complete.

Таблиця 2.2 – Порівняльна таблиця антивірусного ПЗ

	Bitdefender	ESET NOD32	McAfee	BullGuard	Panda
Пробний період	-	+	+	-	+
Захист у реальному часі	+	+	+	+	+
Видалення шкідливого ПЗ	+	+	+	+	+
Видалення шпигунського ПЗ	+	+	+	+	+
Видалення рекламного ПЗ	+	+	+	+	+

Продовження таблиці 2.2 – Порівняльна таблиця антивірусного ПЗ

	Bitdefender	ESET NOD32	McAfee	BullGuard	Panda
Захист від програм-вимагачів	+	+	-	-	+
Антифішинг	+	+	+	+	+
VPN	+	+	-	-	+
Сканер вразливостей	+	+	+	+	-
Брандмауер	+	+	+	+	+
Цифровий шредер	+	+	+	-	-

Згідно даним наведеним у таблиці 2.2 – Порівняльна таблиця антивірусних ПЗ можна зробити висновок, що найкращою заміною 360 Total Security є ESET NOD32 Smart Security Business Edition. Ліцензія на цей продукт придбається раз на рік та надає повний профіль послуг. Дане антивірусне програмне забезпечення затверджено експертним висновком № 877 згідно переліку засобів ТЗІ від Держспецзв'язку.

2.4 Обґрунтування методів та засобів контролю за діями користувачів

Термін DLP розшифровується як Data Loss Prevention або Data Leakage Prevention - запобігання витокам даних. Відповідно, DLP-системи це програмні та програмно-апаратні засоби для вирішення завдання запобігання витокам даних.

Оскільки системи DLP запобігають витоку конфіденційної інформації, вони повинні мати вбудовані механізми для визначення рівня конфіденційності документа, виявленого в захопленому трафіку. Як правило, є два найпоширеніші методи: аналіз спеціальних маркерів документа та аналіз змісту документа. В даний час другий варіант є більш поширеним, оскільки він стійкий до змін, внесених до документа перед його відправленням, і дозволяє легко збільшити кількість конфіденційних документів, з якими може працювати система.

Стандартні заходи безпеки включають брандмауер, систему виявлення вторгнень та антивірусне програмне забезпечення. Це механізми, що захищають комп'ютери від внутрішніх і зовнішніх атак.

Найчастіше працівники викликають витік інформаційної системи ненавмисно – через неуважність, некомпетентність чи халатність. Втім випадки крадіжки файлів з метою перепродажу конкурентам, помсти або відкриття своєї фірми на підставі унікальної інформації також досить поширені.

Звичайно, жодна DLP-система не може гарантувати безумовний захист від наслідків помилок працівників, однак вона дозволяє значно мінімізувати їх ризики і наслідки, а також гарантувати дотримання положень проекту захисту конфіденційних даних. Система DLP працює за наступним алгоритмам:

- перехоплення інформації (фіксування отримання, відправлення, відкриття файлів);
- аналіз інформації (система визначає, куди спрямований документ, і по налаштованим маркерам визначає характер інформації в ньому, розуміє, що за документ пересилається);
- блокування інцидентів або повідомлення про них.

DLP-система є необхідністю для впровадження, оскільки на ОІД будь-який користувач може використовувати зовнішні носії та має право на імпорт/експорт будь-яких файлів до яких є достатньо повноважень. Так як на підприємстві було обрано використання антивірусного програмного забезпечення від компанії ESET, то для впровадження системи DLP було обрано програмне забезпечення також від ESET, що має назву ESET DLP SAFETICA.

SAFETICA зберігає важливі дані в компанії. До того ж регулює особисті пристрої співробітників, тому в безпечному корпоративному середовищі передача даних з цих пристроїв неможлива. Працівники не можуть передавати важливу інформацію конкурентам або користуватися нею для власних потреб. Захищає важливі дані навіть в разі їх втрати. Весь диск або вибрані файли залишаються зашифрованими і нечитабельним для сторонніх осіб, дозволяє керувати друком та доступом до мережі Інтернет. Створює звіти про всі файлові транзакції, усі веб-

сайти, електронну пошту та веб-пошту, а також обмін миттєвими повідомленнями, принтери, активність на екрані та відстеження натискання клавіш.

Продукт SAFETICA заснований на клієнт-серверній архітектурі. Клієнт SAFETICA на робочих місцях запускає комунікацію з сервером. Разом з клієнтом на робочих станціях запускається агент завантажувача, який призначений для встановлення, оновлення і управління іншими клієнтськими компонентами. Для управління, настройки і відображення отриманих даних використовується консоль управління. Вона дозволяє відображати вихідні дані моніторингу, статистику та діаграми. Дані, отримані з окремих робочих місць, зберігаються на сервері бази даних. База даних також зберігає настройки всіх компонентів SAFETICA.

Програмне забезпечення SAFETICA складається з трьох модулів: аудитор, супервайзер та DLP. Перший модуль – «Аудитор» виявляє потенційно небезпечну поведінку співробітника з самого його початку. Відстежує дії співробітників і виявляє порушників, які намагаються завдати шкоди компанії. Модуль «Супервайзер» – запобігає небажані дії через заборону запуску певних програм, обмеження на відвідування сайтів тощо. Модуль «DLP» - запобігає витік конфіденційної інформації в автоматичному режимі та працює за заздалегідь встановленими правилами для користувачів. Рішення базується на архітектурі «клієнт-сервер». Відомості, що отримуються з окремих елементів комп'ютерної системи та налаштування для усіх компонентів SAFETICA зберігаються на сервері у базі даних.

2.5 Положення щодо режиму перебування на території підприємства

На підприємстві є необхідністю доопрацювання правил відвідування. Як було зазначено у першому розділі відвідувачі мають право перебувати на території підприємства за певних обставин. Процедура прийому відвідувача до компанії полягає в наступному. На вхідних дверях є камера та зв'язок зі службою безпеки. Гість повинен вказати прізвище та ім'я людини, до якої він прийшов. Служба безпеки викликає працівника до дверей, який проводжає відвідувача до його робочого місця. Коли гість залишає компанію, працівник повинен проводжати його назад до дверей.

Ряд нововведень полягає у наступному:

1) Відвідування з незначних причин (передача забутих вдома речей, тощо) має тривати не більш ніж двадцять хвилин.
2) Відвідування представниками інших компаній має відбуватися так, що одна особа із представників служби безпеки або директор має проводити візитера до кабінету директора, опісля тим самим способом його провести до дверей.
3) Про передачу будь-яких речей сторонніми особами співробітникам має бути оповіщена служба безпеки та провести догляд переданих речей.
4) Візитер не має права використовувати персональні комп'ютери співробітників.
5) У випадку, коли відвідувач отримав фізичний доступ до обладнання, приймаючий співробітник може бути підданий під дисциплінарне стягнення вперше, надалі – грошове стягнення.
6) Відповідальність за відвідувача несе співробітник.

2.6 Положення щодо користування КС

Кожен користувач автоматизованої системи має розуміти, що починаючи з першого робочого дня на підприємстві він несе відповідальність за конфіденційність, цілісність та доступність інформації, яка обробляється на присвоєному йому персональному комп'ютері, а також за сам ПК. Правила для використання персонального комп'ютера мають виглядати наступним чином:

1) Співробітник заступаючи на посаду має бути проінформований щодо правил використання ПК, та правил обробки інформації на ньому згідно його посади.
2) Використання будь-яких зовнішніх носіїв заборонено.
3) Не дозволяється самостійно модифікувати персональний комп'ютер, у разі його несправності потрібно звертатися до адміністратора системи.
4) У разі, якщо співробітник бачить, як інший співробітник намагається пошкодити ПК (б'є по ньому, намагається дістати його компоненти, тощо)

потрібно негайно повідомити про це системного адміністратора та службу охорони.

5) Залишати своє робоче місце дозволяється тільки після того, як обліковий запис користувача був заблокований
6) У кінці робочого дня працівник має вимкнути персональний комп'ютер.
7) Якщо під час перевірки системи було виявлено віруси треба повідомити про це адміністратора системи.
8) Відповідальність за своє робоче місце несе співробітник.

2.7 Висновки до 2 розділу

У рамках другого розділу були розглянуті аспекти існуючого стану захищеності, обґрунтований вибір профілю захищеності. Запропоновані такі проектні рішення як:

- призначення відповідального за інформаційну безпеку – адміністратор безпеки;
- розроблена нова матриця доступу, завдяки якій було визначено нові правила розмежування доступу;
- розробка заходів щодо відвідування території підприємства;
- розробка заходів щодо правил користування комп'ютерною системою.

Проте на реалізацію даних політик, механізмів захисту, тощо необхідні ресурси. У наступному розділі буде розглянуто економічні фактори, які впливають на економічне середовище компанії, розраховано витрати на реалізацію представлених правил та КСЗІ та їх підтримку.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Обґрунтування витрат на реалізацію політик безпеки

Метою цього розділу є економічне обґрунтування доцільності впровадження комплексної системи захисту інформації. Для цього обумовлюється економічна ефективність застосування основних результатів, встановлених в процесі роботи.

Економічна доцільність визначається розрахунками:

- капітальних витрат, що потребують розроблені політики безпеки;
- експлуатаційних витрат;
- річного економічного ефекту від впровадження інформаційної політики безпеки.

Річні прибутки підприємства – 32 198 425 грн. Дане підприємство веде свою діяльність з 1997 року. Кількість співробітників та їх посади зазначені у першому розділі, пункті 1.1.

3.2 Розрахунок капітальних витрат

Капітальні витрати розраховуються наступним чином:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н,} \quad (3.1)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, 0 грн.

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового ПЗ, 0 грн.

$К_{навч}$ – витрати на навчання системного адміністратора становлять 1500 грн.

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, відсутня оскільки за розробленими політики безпеки закупівля апаратного забезпечення не є необхідною.

$К_{рп}$ – вартість розробки КСЗІ, 16 448,9 грн.

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, відсутні оскільки не закуповується апаратне забезпечення.

3.2.1 Визначення трудомісткості розробки КСЗІ

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і

закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{\text{тз}} + t_{\text{в}} + t_{\text{а}} + t_{\text{вз}} + t_{\text{озб}} + t_{\text{овр}} + t_{\text{д}} \text{ годин,} \quad (3.2)$$

де $t_{\text{тз}}$ – тривалість складання ТЗ на розробку КСЗІ, 20 годин;

$t_{\text{в}}$ – тривалість розробки концепції безпеки інформації у організації, 15 годин;

$t_{\text{а}}$ – тривалість процесу аналізу ризиків, 14 годин;

$t_{\text{вз}}$ – тривалість визначення вимог заходів, методів та засобів захисту, 27 годин;

$t_{\text{озб}}$ – тривалість вибору основних рішень з забезпечення БІ, 15 годин;

$t_{\text{овр}}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації, 24 годин;

$t_{\text{д}}$ – тривалість документального оформлення ПБ = 15 годин.

Отже, $t = 20 + 15 + 14 + 27 + 15 + 24 + 15 = 130$ годин.

3.2.2 Розрахунок витрат на створення КСЗІ

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

$$К_{\text{рп}} = З_{\text{зп}} + З_{\text{мч}} \quad (3.3)$$

$$З_{\text{зп}} = t \cdot З_{\text{іб}} = 130 \cdot 125 = 16\,250 \text{ грн,} \quad (3.4)$$

де t – загальна тривалість розробки КСЗІ, годин;

$З_{\text{іб}}$ – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/год = 125 грн/год.

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

$$З_{\text{мч}} = t \cdot С_{\text{мч}} = 130 \cdot 1{,}53 = 198{,}9 \text{ грн} \quad (3.5)$$

де t – трудомісткість підготовки документації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{\text{мч}} = Р \cdot t_{\text{нал}} \cdot С_{\text{е}} + \frac{Ф_{\text{зал}} \cdot Н_{\text{а}}}{F_{\text{р}}} + \frac{К_{\text{лпз}} \cdot Н_{\text{апз}}}{F_{\text{р}}} = 1{,}53 \text{ грн;} \quad (3.6)$$

де – Р – встановлена потужність ПК, 0.4 кВт;

$t_{нал}$ – кількість машин на яких розроблюється КСЗІ, 1 шт.;

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

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, 4703 грн;

$Н_а$ – річна норма амортизації на ПК, 0.3 частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, 1100 грн;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, 0.21 частки одиниці;

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

Вартість ПК = 7 785 грн, строк корисної служби = 38 місяці.

Накопичена амортизація = (7 785 · 38)/(8 · 12) = 3082 грн

Залишкова вартість = 7 785 – 3082 = 4703 грн

$$К_{рп} = З_{зп} + З_{мч} = 16\,250 + 198{,}9 = 16\,448{,}9 \text{ грн} \quad (3.7)$$

Таким чином, капітальні витрати на проектування та впровадження КСЗІ становлять:

$$К = 16\,448{,}9 + 1500 = 17\,948{,}9 \text{ грн}$$

3.2.3 Визначення та розрахунок витрат на впровадження технології DLP

$$К_{пу} = З_{зп} + З_{мч} + К_{пз} = 1187{,}5 + 29{,}07 + 1325 = 2\,541{,}57 \text{ грн}, \quad (3.8)$$

де $К_{пу}$ – вартість впровадження технології;

$К_{пз}$ – вартість придбання ліцензійного ПЗ.

Таблиця 3.1 – Трудомісткість впровадження технології DLP

Склад витрат	Трудомісткість, год-осіб	Вартість грн/год	Сума, грн
Встановлення ПЗ	3	62,5	187,5
Налаштування ПЗ	9		562,5
Склад витрат	Трудомісткість, год-осіб	Вартість грн/год	Сума, грн

Продовження таблиці 3.1 – Трудомісткість впровадження технології DLP

Склад витрат	Трудомісткість, год-осіб	Вартість грн/год	Сума, грн
Навчання персоналу	7	62,5	437,5
Всього			1187,5

Вартість машинного часу на впровадження системи DLP на комп'ютері:

$$З_{мч} = t \cdot С_{мч} = 19 \cdot 1{,}53 = 29{,}07 \text{ грн}$$

Вартість $С_{мч}$ – вартість 1 години машинного часу визначена у розділі 3.2.2, формула 3.5 та становить 1,53 грн.

3.2.4 Визначення та розрахунок витрат на переустановлення операційних систем

$$К_{ос} = З_{зп} + З_{мч} + К_{пз} = 1312{,}5 + 32{,}13 + 85\,800 = 87\,144{,}63 \text{ грн}, \quad (3.9)$$

де $К_{ос}$ – витрати на оновлення операційної системи;

$К_{пз}$ – вартість придбання ліцензійного ПЗ.

Таблиця 3.2 – Трудомісткість переустановлення операційних систем

Склад витрат	Трудомісткість, год-осіб	Вартість грн/год	Сума, грн
Встановлення ПЗ	10	62,5	625
Налаштування ПЗ	10		625
Навчання персоналу	1		62,5
Всього			1312,5

Вартість машинного часу на переустановлення операційних систем:

$$З_{мч} = t \cdot С_{мч} = 21 \cdot 1{,}53 = 32{,}13 \text{ грн}$$

Кількість ПК на яких потрібно цю операцію – 78 шт. Вартість ліцензійної операційної системи – 1100 грн.

3.2.5 Визначення та розрахунок витрат на встановлення антивірусного ПЗ

$$К_{аз} = З_{зп} + З_{мч} + К_{пз} = 1437{,}5 + 35{,}19 + 85\,800 = 87\,272{,}69 \text{ грн}, \quad (3.10)$$

де $К_{аз}$ – вартість встановлення антивірусного ПЗ;

$К_{пз}$ – вартість придбання ліцензійного ПЗ.

Таблиця 3.3 – Трудомісткість впровадження встановлення антивірусного ПЗ

Склад витрат	Трудомісткість, год-осіб	Вартість грн/год	Сума, грн
Встановлення ПЗ	7	62,5	437,5
Налаштування ПЗ	9		562,5
Навчання персоналу	7		437,5
Всього			1437,5

Вартість машинного часу на переустановлення операційних систем:

$$З_{мч} = t \cdot С_{мч} = 23 \cdot 1{,}53 = 35{,}19 \text{ грн}$$

Кількість ПК на яких потрібно цю операцію – 78 шт. Вартість ліцензійної операційної системи – 1100 грн.

Таким чином маємо, що сукупні капітальні витрати становитимуть:

$$К = 17\,948{,}9 + 2\,541{,}57 + 87\,144{,}63 + 87\,272{,}69 = 194\,907{,}79 \text{ грн}$$

3.3 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об’єкта проектування за визначений період, що виражені в грошовій формі.

За методикою Gartner Group до поточних (експлуатаційних) витрат:

- вартість модернізації системи ($С_в$);
- витрати на керування системою в цілому ($С_к$);
- витрати викликані активністю користувачів системи ($С_в$);

Під «витратами на керування» системою мають на увазі витрати, пов’язані з керуванням і адмініструванням серверів та інших компонентів системи. До цієї категорії витрат відносяться:

- навчання адміністративного персоналу й користувачів;
- амортизаційні відрахування від вартості апаратного та програмного забезпечення;

- заробітна плата обслуговуючого персоналу;
- аутсорсинг;
- навчальні курси та сертифікація обслуговуючого персоналу;
- технічне й організаційне адміністрування й сервіс.

3.3.1 Розрахунок поточних витрат на оновлення ліцензій антивірусного ПЗ

Поточні витрати на використання програмного забезпечення:

$$С_п = С_л + С_о = 26\,848 + 606{,}52 = 27\,454{,}52 \text{ грн}, \quad (3.11)$$

де $С_п$ – поточні витрати,

$С_л$ – витрати на продовження ліцензії, за одиницю – 1678 грн на 5 персональних комп'ютерів (у системі їх 78);

$С_о$ – витрати на оновлення ПЗ.

Розрахунок витрат на оновлення ПЗ виконується наступним чином:

$$С_о = З_{зп} + З_{мч} = 603 + 3{,}52 = 606{,}52 \text{ грн}, \quad (3.12)$$

Трудомісткість оновлення складає 5 години.

3.3.2 Розрахунок поточних витрат на використання технології DLP

Поточні витрати на експлуатацію технології DLP розраховуються за формулою 3.12:

$$С_п = С_л + С_о = 1325 + 365{,}01 = 1690{,}01 \text{ грн},$$

де $С_п$ – поточні витрати,

$С_л$ – витрати на продовження ліцензії;

$С_о$ – витрати на оновлення ПЗ.

Розрахунок витрат на оновлення ПЗ виконується за формулою 3.13:

$$С_о = З_{зп} + З_{мч} = 361{,}8 + 3{,}21 = 365{,}01 \text{ грн}$$

Трудомісткість оновлення складає 3 години.

Маємо, що поточні витрати на експлуатацію технології DLP складають 1690,01 грн.

$$С = \sum С_п = 27\,454{,}52 + 1690{,}01 = 29\,144{,}53 \text{ грн}$$

3.3.3 Витрати на керування системою інформаційної безпеки

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

$$С = С_н + С_а + С_з + С_{єв} + С_е + С_{ел} + С_о + С_{тос}, \text{ грн} \quad (3.13)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів становлять 3 000 грн.

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

$$С_з = З_{осн} + З_{дод} \text{ грн} \quad (3.14)$$

Основна заробітна плата визначається з місячного окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати. Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 14 000 грн. Фірма готова взяти спеціаліста за 0.3 ставки Додаткова тоді становить – 1260 грн. Маємо:

$$С_з = 14\,000 \cdot 0.3 \cdot 12 + 1260 \cdot 12 = 50\,778 \text{ грн}$$

Статистика ЄСВ для всіх категорій платників з 01.01.2021 становить 22%, тоді маємо:

$$С_{єв} = 50\,778 \cdot 0.22 = 57\,024 \text{ грн}$$

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

$$С_{ел} = P * F_р * Ц_е = 5{,}2 * 1920 * 1{,}68 = 16\,773{,}12 \text{ грн} \quad (3.15)$$

Витрати на технічне та організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються за даними організації або у відсотках від вартості капітальних витрат – 2%.

$$С_{тос} = 27\,277{,}9 \cdot 0.02 = 545{,}5 \text{ грн}$$

Витрати на керування системою інформаційної безпеки становлять:

$$С_к = 3\,000 + 50\,778 + 16\,773{,}12 + 545{,}5 = 71\,096{,}32 \text{ грн}$$

Отже річні поточні витрати в такому випадку складають:

$$С = 71\,096{,}32 + 29\,144{,}53 = 100\,240{,}85 \text{ грн}$$

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

Для розрахунку вартості збитку можна застосовувати таку модель:

Необхідні вхідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 6 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 10 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 13 годин;

$З_о$ – заробітна плата обслуговуючого персоналу, 10 000 грн/міс;

$З_с$ – заробітна плата працівників атакованого вузла або сегмента корпоративної мережі, грн/міс;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 3 особи;

$Ч_с$ – чисельність працівників атакованого вузла або сегмента корпоративної мережі, 78 осіб.

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 500000 грн. у рік;

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

I – число атакованих сегментів корпоративної мережі, 4;

N – середнє число атак на рік, 2.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \tag{3.16}$$

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

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

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

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки. Заробітна плата кожного з них вказана у таблиці 3.4.

Таблиця 3.4 – Заробітна плата працівників компанії

Посада	Кількість працівників, осіб	Місячна заробітна плата, грн	Єдиний соціальний внесок, грн	Витрати на заробітну плату з урахуванням ЄСВ, грн
Бухгалтер	4	8000	1760	39 040
Головний інженер	1	8000	1760	9760
Головний технолог	1	8000	1760	9760
Дизайнер	4	9000	1980	43 920
Директор	1	15000	3300	18 300
Диспетчер	1	7400	1628	9028
Зам. директор департаменту HR	1	8500	1870	10 370
Зам. директор департаменту виробництва	1	8500	1870	10 370
Зам. директор департаменту маркетингу	1	8500	1870	10 370

Продовження таблиці 3.4 – Заробітна плата працівників компанії

Посада	Кількість працівників, осіб	Місячна заробітна плата, грн	Єдиний соціальний внесок, грн	Витрати на заробітну плату з урахуванням ЄСВ, грн
Зам. директор департаменту продажу	1	8500	1870	10 370
Зам. директор логістики	1	8500	1870	10 370
Інженер-технолог	2	8000	1760	19 460
Керівник роздрібної мережі	1	8500	1870	10 370
Консультант Call-центру	17	6300	1368	130 356
Маркетолог	15	6700	1474	122 610
Менеджер ЗЕД	5	7400	1628	45 140
Менеджер оптових продаж	1	7500	1650	9150
Начальник відділу реклами	1	8500	1870	10 370

Продовження таблиці 3.4 – Заробітна плата працівників компанії

Посада	Кількість працівників, осіб	Місячна заробітна плата, грн	Єдиний соціальний внесок, грн	Витрати на заробітну плату з урахуванням ЄСВ, грн
Начальник об'єднаних складів	1	8500	1870	10 370
Начальник розкрійного цеху	1	8500	1870	10 370
Начальник складу	1	8500	1870	10 370
Начальник швейного цеху	1	8500	1870	10 370
Секретар	6	6500	1430	47 580
Системний адміністратор	3	10 000	2200	36 600
Спеціаліст з відбору персоналу	5	8300	1826	50 630
Фінансовий аналітик	1	9100	2002	11 102
Усього:	78			716 506

$$\sum З_с = 716\,506 \text{ грн}$$

$$П_{п} = \frac{\sum З_{с}}{F} \cdot t_{п} = \frac{716\,506}{160} \cdot 6 = 26\,868{,}98 \text{ грн}, \quad (3.17)$$

де F – 160 годин, місячний фонд робочого часу.

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_{в} = П_{ви} + П_{пв} + П_{зч}, \quad (3.18)$$

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

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

$П_{зч}$ – вартість заміни устаткування або запасних частин, 0 грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_{с}$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$.

$$П_{ви} = \frac{\sum З_{с}}{F} \cdot t_{ви} = \frac{716\,506}{160} \cdot 13 = 58\,216{,}11 \text{ грн}, \quad (3.19)$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_{в}$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_{о} \cdot Ч_{о}}{F} \cdot t_{в} = \frac{10\,000 \cdot 3}{160} \cdot 10 = 1875 \text{ грн}, \quad (3.20)$$

$$П_{в} = 58\,216{,}11 + 1875 + 0 = 60\,091{,}11 \text{ грн}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{О}{F_{г}} \cdot (t_{п} + t_{в} + t_{ви}) = \frac{500000}{1920} \cdot (6 + 10 + 13) = 7\,552{,}08 \text{ грн}, \quad (3.21)$$

де F – 160 годин, місячний фонд робочого часу, тоді річний – 1920 грн.

Упущена вигода від пристрою атакованого вузла або сегмента корпоративної мережі, грн у рік:

$$U = 26\,868{,}98 + 60\,091{,}11 + 7\,552{,}08 = 94\,512{,}06 \text{ грн},$$

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

$$B = \sum_i \sum_n U = 2 \cdot 4 \cdot 94\,512{,}06 = 756\,096{,}48 \text{ грн} \quad (3.22)$$

3.5 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн}, \quad (3.23)$$

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці 47%;

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

$$E = 756\,096{,}48 \cdot 0{,}47 - 100\,240{,}85 = 255\,124{,}5 \text{ грн.}$$

3.6 Визначення та аналіз показників економічної ефективності розробки політики інформаційної безпеки

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

$$ROSI = \frac{E}{K} = \frac{255\,124{,}5}{194\,907{,}79} = 1{,}3 \text{ частки одиниці}, \quad (3.24)$$

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

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

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

$$T_0 = \frac{1}{ROSI} = \frac{1}{1{,}3} = 0{,}77 \text{ роки} \quad (3.25)$$

Після перевірки запропонованих рішень, окупність наступить менш ніж за рік.

3.7 Висновки до 3 розділу

Відповідно до проведених розрахунків можна зробити висновок, що для приватного підприємства ТОВ «VIF» розробка комплексної системи захисту інформації є економічно доцільною, оскільки коефіцієнт повернення інвестицій

ROSI складає 1,3 грн. (тобто на кожну вкладену гривню в розробку політики інформаційної безпеки підприємство ТОВ «VIF» матиме 1,3 грн. економічного ефекту). Термін окупності при цьому складе 0,77 року (281 день).

ВИСНОВКИ

У рамках першого розділу роботи було виконано обстеження на ОІД, розглянуто: обчислювальну систему, інформаційне середовище, фізичне середовище, середовище користувачів. Проведено аналіз та оцінку ризиків інформаційної безпеки і виділено значущі загрози. За результатами обстеження на ОІД та аналізу інформаційних ризиків, виділено недосконалості інформаційно-телекомунікаційної системи підприємства. Недоліки можуть спричинити використання вразливостей системи та призвести до завдання збитків підприємству.

У другому розділі згідно з проведеним аналізом загроз з першого розділу, запропоновані до впровадження методи та засоби захисту інформації для забезпечення ефективної роботи всіх складових системи.

Згідно з отриманими даними під час розрахунку економічної частини - капітальні затрати становлять 237848,09 грн, експлуатаційні - 125886,22 грн. Згідно з підрахунками, створені елементи КСЗІ є доцільними з економічної точки зору. Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації склав 12 545 454,5 грн. Загальний ефект від впровадження системи інформаційної безпеки склав 5 770 477,39 грн. Згідно с коефіцієнтом ROSI який становить 24,26 - створені елементи КСЗІ є цілком доцільними. Термін окупності елементів КСЗІ становить 0,04 роки = 14 днів.

ПЕРЕЛІК ДЖЕРЕЛ

1. ТОВ "В.І.Ф." - 25010554 [Електронний ресурс] – Режим доступу до ресурсу: https://opendatabot.ua/c/25010554;
2. Загрози доступності [Електронний ресурс] – Режим доступу до ресурсу: https://pidru4niki.com/18510811/informatika/zagrozi_dostupnosti;
3. КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ ОПЕРАЦІЙНОЇ СИСТЕМИ MICROSOFT WINDOWS 7 ENTERPRISE EDITION SP1 [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.ua/ua/kompleks_zasobv_zahistu_operacjno_sistemi_microsoft_windows_7_enterprise_edition_sp1.html;
4. Compare The Best Antivirus Solutions For Your Devices [Електронний ресурс] – Режим доступу до ресурсу: https://www.antivirusguide.com/best-antivirus/?lp=default&utm_source=google&utm_medium=cpc&sgv_medium=search&utm_campaign=6478205166&utm_content=99672426616&utm_term=antivirus&cid=508925511803&pl=&feeditemid=&targetid=aud-755007040219:kwd-10745101&mt=b&network=g&device=c&adpos=&p1=&p2=&geoid=1012839&gclid=CjwKCAjwqvyFBhB7EiwAER786fnQpERyVIE8fyMI1fob3YVdBYK4P2VkEqmieRQdhis21lcW7oo8ghoCjw0QAvD_BwE;
5. НД ТЗІ 2.5-005-1999. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Київ 1999 р.;
6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.– Київ 1999 р.;
7. Про інформацію: Закон України: [Електронний ресурс] – Режим доступу: http://www.rada.gov.ua;
8. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі НД ТЗІ 3.7-001-99 – Київ 1999 р.;
9. НД ТЗІ 3.7-003 -05 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Порядок проведення робіт із створення КСЗІ в ІТС;

[Електронний ресурс] – Режим доступу до ресурсу: https://pda.litres.ru/vadim-grebennikov-15/kompleksni-sistemizahistu-informaciyi-proektuvannya/chitat-onlayn/page-2;

10. Комплекс засобів захисту операційної системи Microsoft Windows 10 Professional [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.ua/ua/kompleks_zasobv_zahistu_operacjno_sistemi_microsoft_windows_10_professional.html
11. ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [Електронний ресурс] – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106343;
12. DLP-СИСТЕМЫ [Електронний ресурс] – Режим доступу до ресурсу: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/
13. What is Data Loss Prevention [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/
14. Products In Enterprise Data Loss Prevention (DLP) Market [Електронний ресурс] – Режим доступу до ресурсу: https://www.gartner.com/reviews/market/enterprise-data-loss-prevention
15. SAFETICA ПОЛНАЯ ДОКУМЕНТАЦИЯ [Електронний ресурс] – Режим доступу до ресурсу: https://mirror2.esetnod32.ru/manuals/business/dlp/safetica_9.0_userguide_rus.pdf
16. Методичні вказівки до виконання економічної частини дипломного проекту для студентів спеціальності 125 Кібербезпека/ Упоряд.: Д.П. Пілова, доц.,канд. екон. наук. – Дніпро: НТУ «ДП», 2019. – 16с.
17. 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.

ДОДАТОК А. Акт категоріювання

Гриф обмеження доступу
Прим. N _1_

ЗАТВЕРДЖУЮ
Керівник установи-власника
(розпорядника, користувача) об'єкта
___директор_Іродова_А.О._____
(посада, підпис, ініціали, прізвище)
10.05.2021

М. П.

АКТ
категоріювання _____ТОВ «VIF»_____
(найменування об'єкта категоріювання)

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_____
(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, до неї відносяться об’єкти, в яких циркулює службова та конфіденційна інформація, вимога щодо захисту якої встановлена законом_____

Голова комісії _____
(підпис) ____А. О Тирченко ____
(ініціали, прізвище)
Члени комісії: _____
(підпис) _____В. О._Махно_____
(ініціали, прізвище)
___.___.20__

ДОДАТОК Б. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1. Стан питання. Постановка задачі	54	
6	А4	Розділ 2. Спеціальна частина	15	
7	А4	Розділ 3. Економічна частина	9	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А Акт категоріювання	1	
11	А4	Додаток Б Відомість матеріалів кваліфікаційної роботи	1	
12	А4	Додаток В Перелік документів на оптичному носії	1	
13	А4	Додаток Г Відгук керівника спеціального розділу	1	
14	А4	ДОДАТОК Д Відгук керівника економічного розділу	1	

ДОДАТОК В. Перелік документів на оптичному носії

1. Пояснювальна записка Іванченко Є.М.docx
2. Пояснювальна записка Іванченко Є.М.pdf
3. Презентація Іванченко Є.М.pptx

ДОДАТОК Г. Відгук керівника спеціального розділу

В І Д Г У К
на кваліфікаційну роботу студентки групи 125-17-1
Іванченко Єлизавети Максимівни
на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «VIF»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 95 сторінках.

Метою кваліфікаційної роботи є забезпечення заданого рівня безпеки інформації, яка обробляється в ІТС товариства з обмеженою відповідальністю «VIF».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: обстеження середовищ функціонування ІТС, аналіз джерел загроз та вразливостей, виявлення актуальних загроз, формування вимог до рівня захищеності інформації від НСД, розробка проектних рішень та елементів політики безпеки.

Обґрунтовано вибір антивірусного програмного забезпечення та DLP системи.

Практичне значення результатів кваліфікаційної роботи полягає у запропонованих правилах розмежування доступу.

До недоліків роботи можна віднести недостатньо обґрунтований перелік актуальних загроз.

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

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

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

Кваліфікаційна робота заслуговує оцінки «добре».

Керівник кваліфікаційної роботи, професор **Кагадій Т.С.**

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

ДОДАТОК Д. Відгук керівника економічного розділу

Керівник розділу_____доц. Пілова Д.П.