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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Жмака Даніїла Сергійовича*

академічної групи *125-18-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ "DevUA"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл Тимофєєв Д.С.	90	Відмінно	
економічний	к.е.н., доц. Пілова Д.П.	90	Відмінно	

Рецензент				

Нормоконтролер	ст. викл Тимофєєв Д.С.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Жмак Д.С.* **академічної групи** *125-18-3*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ "DevUA"*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022 № 268-с

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Виконати обстеження інформаційно-технологічної системи ТОВ, аналіз середовищ функціонування	06.05.2022
Розділ 2	Провести аналіз загроз ІБ ІТС товариства з обмеженою відповідальністю, розробити проектні рішення щодо реалізації механізмів захисту	27.05.2022
Розділ 3	Обгрунтувати економічну доцільность впровадження КСЗІ, розрахувати витрати та ефективність запровадження КСЗІ	10.06.2022

Завдання видано _____ Кагадій Т.С.
(підпис керівника) (прізвище, ініціали)
Дата видачі завдання: 20.01.2022
Дата подання до екзаменаційної комісії: 09.06.2022

Прийнято до виконання _____ Жмак Д.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 89 с., 6 рис., 27 табл., 6 додатків, 11 джерел.

Об'єкт розробки: інформаційно-телекомунікаційна система ТОВ «DevUA».

Предмет розробки: комплексна система захисту інформаційно-телекомунікаційної системи ТОВ «DevUA».

Мета кваліфікаційної роботи: забезпечення безпеки інформації в інформаційнотелекомунікаційній системі ТОВ "DevUA".

У першому розділі була розгляну інформаційно-телекомунікаційна система підприємства "DevUA", обґрунтована необхідність створення КСЗІ опираючись на нормативно правову базу, виконана постановка задачі.

У другому розділі був оцінений існуючий стан захищеності інформаційно-телекомунікаційної ТОВ "DevUA" і були розроблені проектні рішення, які сприяють підвищенню рівня захищеності інформації товариства.

В економічній частині була розглянута економічна доцільність запровадження комплексної системи захисту інформації і було доведено, що запропоновані проектні рішення є економічно ефективними та будуть мати позитивний економічний ефект на прибутку підприємства.

Практична значимість роботи полягає у розробці комплексної системи захисту інформації, яка мінімізує ризики порушення основних її характеристик (конфіденційність, цілісність, доступність).

МОДЕЛЬ ПОРУШНИКА, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, АКТ ОБСЕЖЕННЯ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНІ ПОТОКИ, МОДЕЛЬ ЗАГРОЗ, ЗАХИСТ ІНФОРМАЦІЇ, ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ.

ABSTRACT

Explanatory note: 89 pages, 6 figures, 27 tables, 6 appendices, 11 sources.

Object of development: information and telecommunication system of “DevUA” LLC.

Subject of development: complex system of protection of information and telecommunication system of LLC “DevUA”.

The purpose of the qualification work: ensuring information security in the information and telecommunication system of “DevUA” LLC.

In the first section the information and telecommunication system of the enterprise “DevUA” was considered, the necessity of creation of integrated information security system based on normative legal base was substantiated, the statement of the task was executed.

In the second section, the current state of security of information and telecommunications LLC "DevUA" was assessed and design solutions were developed that help increase the level of security of information of the company.
In the economic part, the economic feasibility of implementing a comprehensive information security system was considered and it was proved that the proposed design solutions are cost-effective and will have a positive economic effect on the company's profits.

The practical significance of the work is to develop a comprehensive information protection system that minimizes the risks of violating its basic characteristics (confidentiality, integrity, accessibility).

INFRINGEMENT MODEL, INFORMATION SECURITY POLICY, SURVEY ACT, COMPREHENSIVE INFORMATION PROTECTION SYSTEM, INFORMATION FLOWS, INSTITUTION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

НД – нормативний документ

ТЗІ – технічний захист інформації

КСЗІ – комплексна система захисту інформації

ПЗ – програмне забезпечення

КЗ – контрольована зона

ОС – операційна система

ДТЗС – допоміжні технічні засоби та системи

ІТС – інформаційна технологічна система

НСД – несанкціонований доступ

ВП – внутрішній порушник

ЗП – зовнішній порушник

ТОВ – товариство з обмеженою відповідальністю

Зміст

ВСТУП

Об’єкт досліджень: інформаційно-телекомунікаційна система ТОВ “DevUA”.

Предмет досліджень: безпека інформації в інформаційно-телекомунікаційній системі товариства “DevUA”.

Мета дослідження: забезпечення безпеки інформації в інформаційно телекомунікаційній системі ТОВ “DevUA”.

В сучасному світі людство не може уявити собі життя без інформаційних систем та їх використання. Інформаційні системи зустрічаються на кожному кроці, від лікарень до різноманітних організацій, транспортних компаній та державних ресурсів. Разом з ростом кількості організацій та об’ємів даних, які використовують ці організації зростають також ризики різноманітних загроз, які можуть призвести до незворотних наслідків.

Щороку кібератакам піддається величезна кількість організацій у всьому світі. Згідно зі звітом IBM, частка втрат бізнесу у загальних витратах пов'язаних з витоком даних - становить 38%.

Звіт IBM показує, що дані з кожним роком набувають все більшої ваги, та відповідно їх витоки коштують компаніям все більше і більше. В середньому ціна витока даних по всьому світу дорівнює $4,24 млн.

- 38% - частка втрат бізнесу у загальних витратах пов'язаних із витоком даних.
- $180 - ціна одного запису, що містить персонально ідентифіковану інформацію.
- 287 днів в середньому потрібно для виявлення та локалізації витоку даних.
- На 80% скорочуються витрати від витоку даних після впровадження AI та автоматизації безпеки.
- Гібридні IT-інфраструктури скорочують втрати від витоку даних у середньому на $1,19 млн..

Безліч компаній, як мінімум один раз за рік зазнавали зовнішньої атаки або зіштовхувалися з внутрішніми інцидентами інформаційної безпеки. Непідготовлені ресурси незастраховані від необмеженої кількості загроз. Такі загрози нерідко призводять до критичних або навіть незворотних наслідків.

Наявність якісної системи захисту інформації в IT-компаніях повинна бути першочерговою, тому що будь-який витік даних клієнтів або масштабний збій може призвести до катастрофічних наслідків і не лише технічного або матеріального характеру, а також репутаційного та навіть кримінального.

Підводячи підсумки, можна сказати, що в сучасному світі усі сфери людської життєдіяльності, так чи інакше, пов'язані з інформаційними ресурсами та захист цих ресурсів стає однією з першочергових задач.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості щодо ТОВ “DevUA”

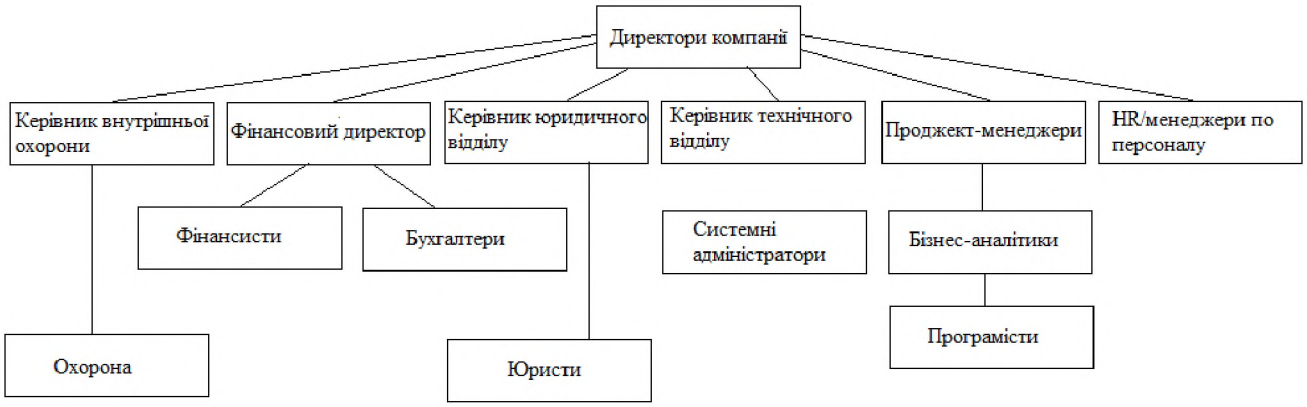
ТОВ “DevUA” – підприємство, що розробляє веб-сервіси та надає їх клієнтам віддалено.

Головний офіс знаходиться на 5 поверсі бізнес-центру “Кудашевський”, за адресою: м. Дніпро, вулиця Барикадна, 16. Підприємство було зареєстровано у 2009 році.

Об’єктом інформаційної діяльності (далі ОІД) є приміщення головного офісу ТОВ “DevUA”.

Функціонує підприємство 5 днів на тиждень. Графік роботи 9:00 – 18:00, з обідньою перервою з 13:00 до 14:00. В компанії зареєстровано 89 робітників.

Рисунок 1.1 Організаційна структура підприємства



1.2 Обґрунтування необхідності створення КСЗІ

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

Згідно зі статтею 21 закону України про “Про інформацію”, інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. Конфіде-

нційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Закон України «Про інформацію» регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» статті 8: інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи порядком, встановленим законодавством.

«Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» затверджені постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 п.16 свідчить про те, що для забезпечення захисту інформації в системі створюється комплексна система захисту інформації, яка призначається для захисту інформації від: витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій; несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів; спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Закон України «Про захист персональних даних» регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист

основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

Закон України «Про державну таємницю» регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

Відповідно до закону України "Про захист інформації в інформаційно-комунікаційних системах" відповідальність за зберігання та захист конфіденційної інформації несе власник системи, до якої належить ця інформація.

Відповідно до НД ТЗІ 2.5-005 -99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" автоматизовану систему ТОВ "DevUA" можна віднести до класу "3", що являє собою розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Згідно з положенням "про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці" НД ТЗІ 1.6-005-2013 об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов'язковому категоріюванню. 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.

Враховуючі, що на об'єкті обробляється інформація з обмеженим доступом, що не становить державної таємниці. Директорами була назначена комісія для категоріювання ОІД і за результатами цього категоріювання була встановлена четверта (IV) категорія. Акт категоріювання наведено в додатку А "Акт категоріювання підприємства".

Керівником компанії було прийнято рішення по створенню КСЗІ, враховуючи наявність великого об'єму персональних даних користувачів, іншої конфіде-

нційної інформації та інформації з обмеженим доступом, було віддано відповідний наказ. Наказ наведено у додатку Б “Наказ про створення КСЗІ”.

1.3 Обстеження фізичного середовища ІТС

Офіс обстежуваного об’єкта знаходиться за адресою: м. Дніпро, вул. Барикадна, 16, третій поверх. Контрольована зона обмежена стінами приміщення. Об’єкт знаходиться в семиповерховій будівлі, яка має свій внутрішній двір з паркінгом. Потрапити на будь-який поверх можливо використовуючи ліфт, в деякі приміщення можна потрапити сходами. Ситуаційний план наведений на рисунку 1.2 нижче.

Будь-яка людина може перебувати на території бізнес-центру, але доступ до приміщень контролюється охороною, яка перебуває на перших поверхах основних входів до будівлі та патрулює територію. Щоб потрапити до приміщень обстежуваного об’єкта, необхідно пройти пункт охорони на першому поверсі, далі піднятися ліфтом до 3 поверху. На поверсі будуть двері із електронною системою пропуску, всі співробітники мають електронні перепустки, аби мати можливість потрапити до приміщення. Також на вході встановленні камери відеоспостереження. Щоб потрапити до приміщення не маючи електронної перепустки, біля дверей є домофон, яким можна звернутися до пункту внутрішньої безпеки, який знаходиться на ресепшені, тоді охорона або адміністратор відчинить двері.

Таким чином можна зробити висновок, що сторонні відвідувачі не мають можливості потрапляння до приміщень компанії.

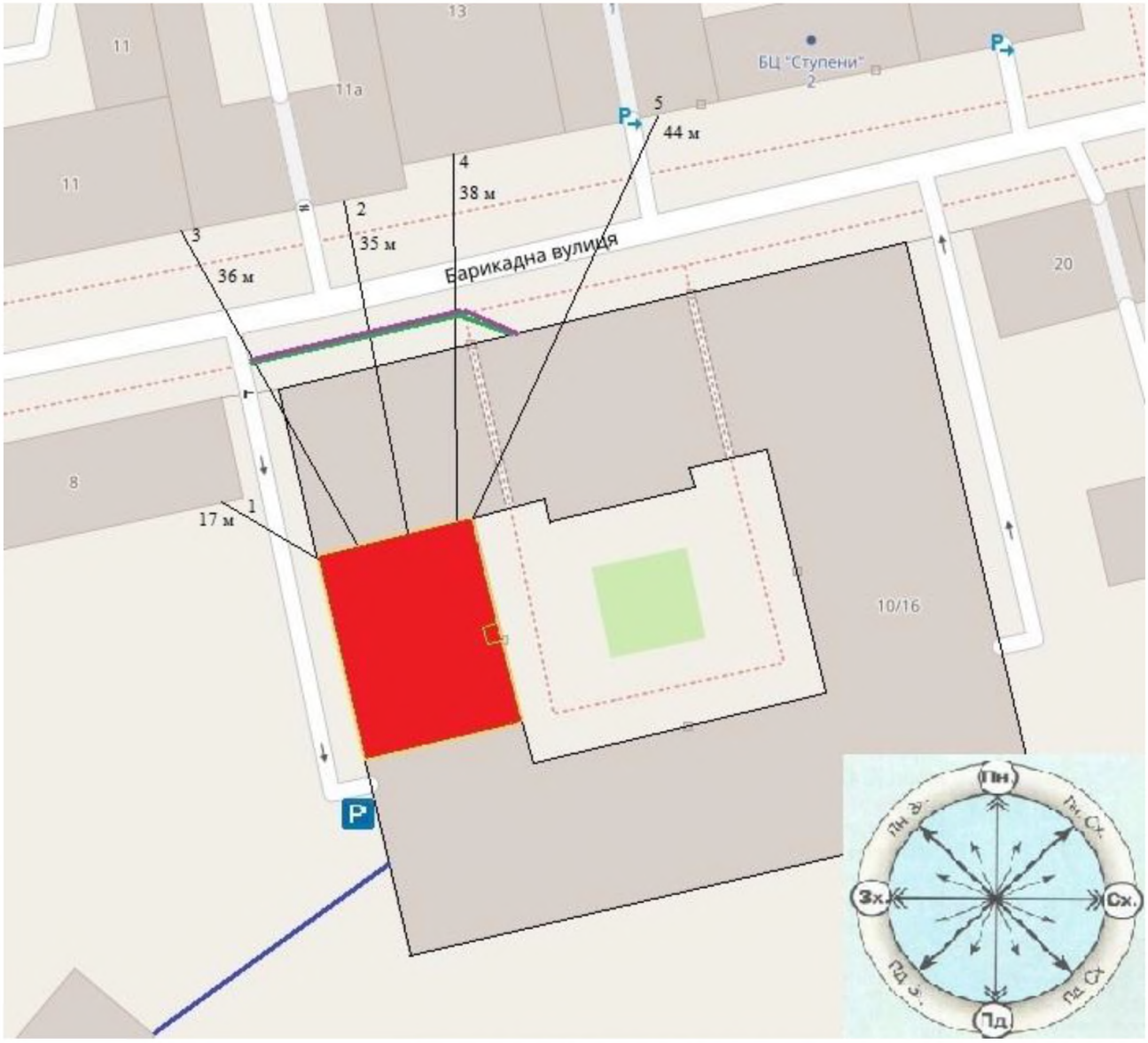


Рисунок 1.2 Ситуаційний план

Таблиця 1.1 – Умовні позначення ситуаційного плану

Позначка	Тлумачення
	Межа КЗ
	Лінія системи водопостачання
	Лінія системи електропостачання
	Інтернет

Продовження таблиці 1.1 - Умовні позначення ситуаційного плану

Позначка	Тлумачення
	Межі будівлі в якій знаходиться ОІД
	Межа ОІД
	Сусідні будівлі
	Паркінг

У будівлі обстежуваного об’єкта розташовані також інші підприємства:

- 1 поверх – Банк “КристалБанк”;
- 2 поверх: Мережа фітнес-клубів “FIT HAUS”;
- 3 поверх: ТОВ “Creative States”, ТОВ “DevUA”
- 4 поверх: Магазин Сільпо, ТОВ “Sitecore”;
- 5 поверх: ТОВ “Epam”;
- 6 поверх: ТОВ “SoftServe”;
- 7 поверх: ТОВ “SoftServe”;

Таблиця 1.2 – Характеристики сусідніх споруд

№	Найменування	Кількість поверхів	Адреса	Відстань від ОІД
1	Адміністративна будівля	3	Барикадна 8	17 м
2	Ресторан Зе Румс	3	Барикадна 11А	35 м
3	Адміністративна будівля	5	Барикадна 11	36 м
4	Адміністративна будівля	3	Барикадна 13	38 м
5	Бізнес центр Ступені	13	Барикадна 15	44 м

Дорога біля будівлі повністю асфальтована. Ширина дороги біля головного входу до території бізнес-центру в якому знаходиться ОІД, дорівнює 4 метри. На території присутні різні види комунікацій, такі як: лінії електромереж, водопостачання та інтернет мережа. В західній частині будівлі знаходиться паркінг.

Висота стелі в офісному приміщені компанії “DevUA” – 4.5 метри. Площа офісних приміщень 519 квадратних метрів. Зовнішні стіни будівлі залізобетонні та обшиті декоративною плиткою, товщина зовнішніх стін – 0.3м., товщина внутрішніх стін – 70мм. Також приміщення містить 28 вікон, вікна розміром 2м*1.5м – пластикові з темним лаком. Вікна закриті метало-пластиковими горизонтальними жалюзями. Кожне вікно можна відчинити на режим провітрювання або повністю.

Основні вхідні двері до приміщень компанії – металеві, товщиною 75мм та розмірами 80см*220см.

Підлога зроблена керамічних плит, які накладені на міжповерхове перекриття зі звуко та гідро ізолюючими шарами.

Двері між приміщеннями компанії пластикові, зі звукоізолюючим шаром, товщина дверей 65мм та розміри 70см*200см.

Система освітлення: мережа 220В, LED лампи розташовані на стелі.

Охоронна система: складається з камер відеоспостереження у кількості 13 штук, пасивних інфрачервоних датчиків руху у кількості 14 штук та протипожежної сигналізації у кількості 20 штук.

Таблиця 1.3 - Системи комунікацій

Система комунікацій	Спосіб підключення
Система каналізації	З'єднана з міською системою каналізацій, яка виходить за межі КЗ
Система електроживлення	Підключена до загальної електромережі
Система вентиляції	Приточно-витяжна
Система опалення	Автономне опалення
Система водопостачання	Підключена до міського водоканалу, який виходить за межі КЗ
Заземлення	Штучне заземлення

Рисунок 1.3 - Генеральний план

Рисунок 1.4 – Системи вентиляції

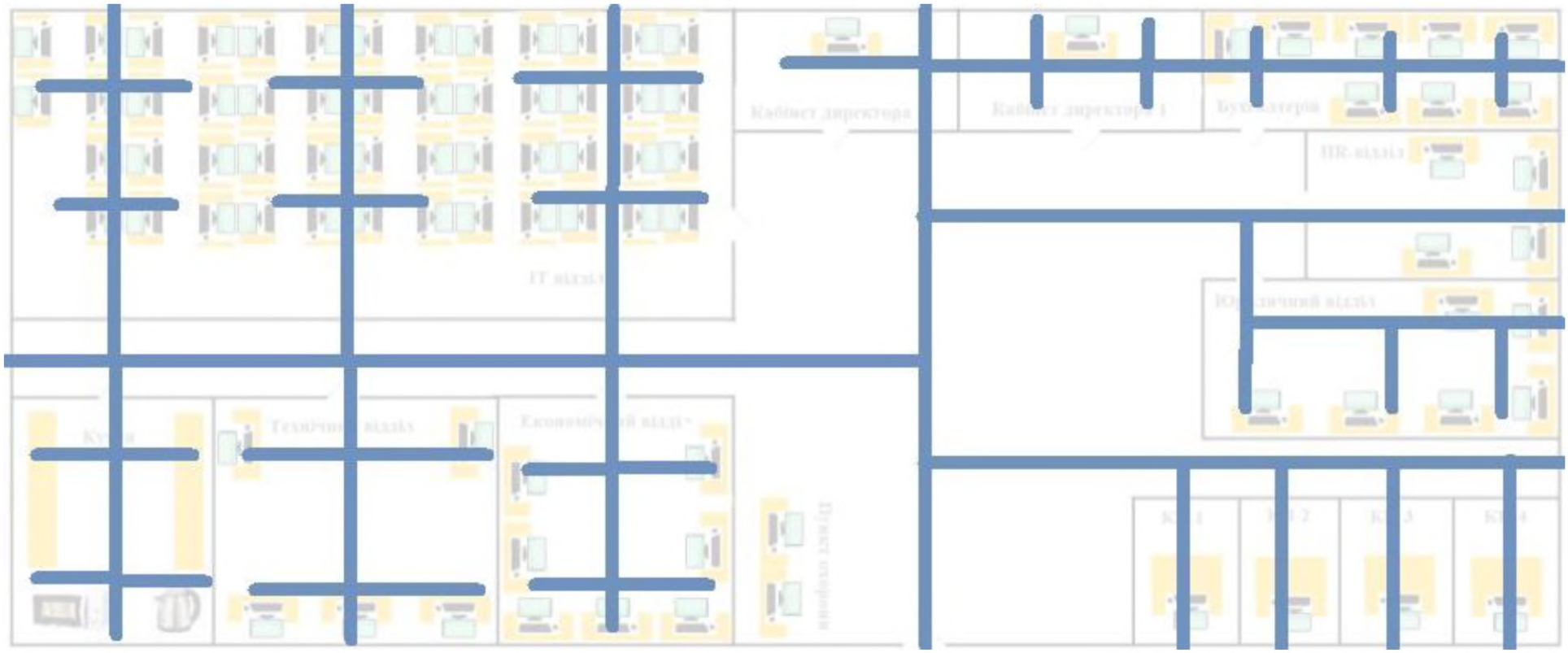
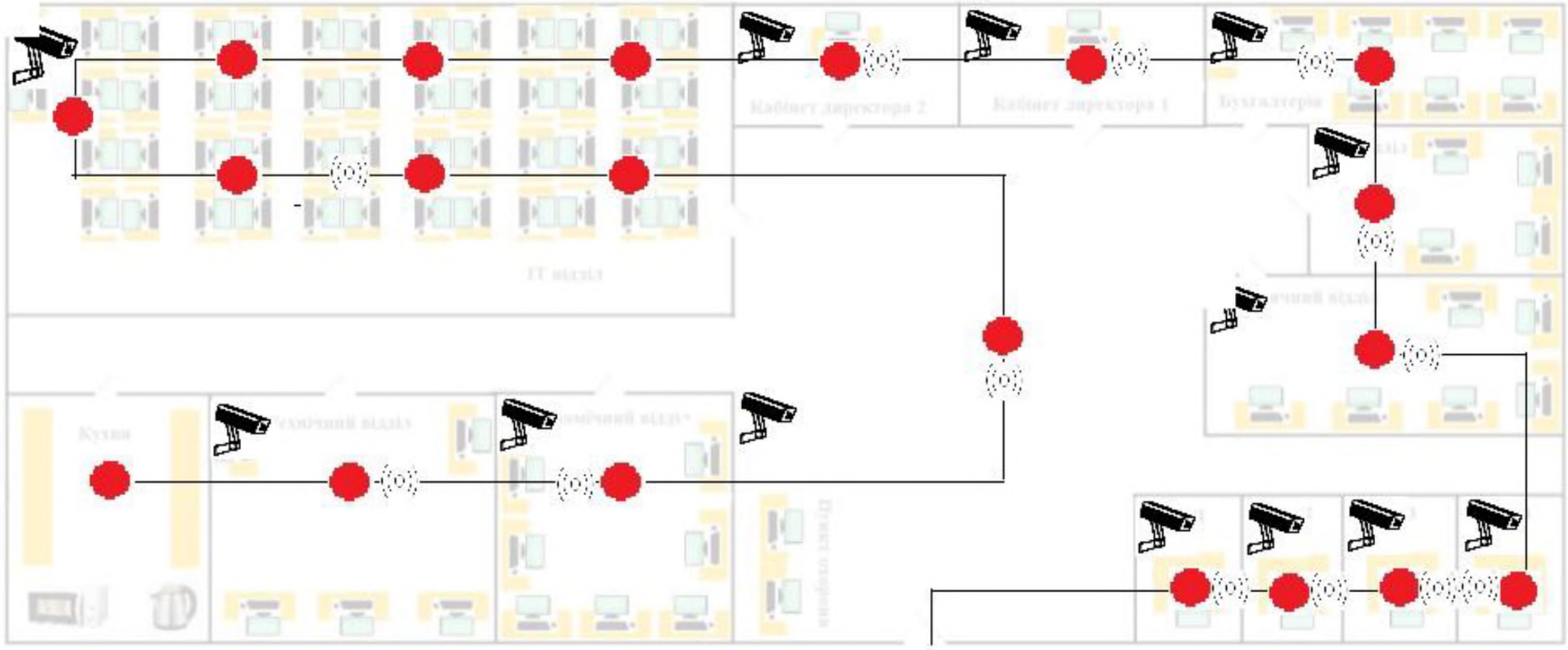


Рисунок 1.5 – Лінії електропостачання та освітлення

Рисунок 1.6 – Охоронні системи



Підприємство складається з таких структурних підрозділів:

- Юридичний відділ – відділ основних бізнес-процесів підприємства, він займається роботою зі справами клієнтів. Також юридичний відділ відповідає за правове забезпечення діяльності організації як суб'єкта господарювання, включаючи правове забезпечення інформаційної безпеки;
- Бухгалтерія - служба, що займається веденням бухгалтерської та податкової звітності, що за сумісництвом виконує функції фінансового відділу, тим самим, розподіляючи фінансові потоки внутрішнього та зовнішнього середовища організації, у тому числі, бухгалтерія фінансує діяльність служби безпеки підприємства;
- Служба внутрішньої охорони – частина служби інформаційної безпеки, яка відповідає за організацію та ведення пропускного режиму на підприємстві та охоронній діяльності. Служба розташована біля входу на територію підприємства.
- Клієнтський відділ – відділ, який організовує взаємодію організації з клієнтами. У клієнтському відділі укладаються бізнес-контракти організації, надаються звіти про виконану роботу клієнтам. Клієнтський відділ веде касові операції з розрахунку з клієнтами;
- Відділ кадрів – виконує функції із забезпечення вакансій на підприємстві, управлінню людськими ресурсами, ведення особових справ працівників та організацією розвитку корпоративної культури, спортивних та інших заходів;
- Серверна - сховище основних баз даних, включаючи персональні дані 2 категорії, та іншу інформацію з грифом суворо конфіденційно. Доступ до серверної мають лише працівники відділу безпеки.
- Технічний відділ – відділ, який безпосередньо виконує основні технічні задачі компанії, працює з проектами клієнтів та розробляє ПЗ.

ІТС включає в себе 79 комп’ютерів(50 в ІТ відділі, 7 в економічному відділі, 5 в юридичному, 2 на пункті охорони, 6 у технічному відділі, 9 у бухгалтерії), 11 ноутбуків(4 у кімнатах перемовин, 2 у кабінетах директорів, 4 в HR-відділі), 2

сервери(Технічний відділ), маршрутизатор(Технічний відділ) та 5 комутаторів (IT відділ, економічний відділ, бухгалтерія, юридичний відділ). АС має доступ до мережі Інтернет, провайдером мережі є “Київстар”. Усі технічні засоби перелічені у таблиці 1.4, позначення в таблиці: РС – робоча станція, Н – ноутбук, С – сервер, К – комутатор, КЛ – клавіатура, КМ – комп’ютерна миша, М – маршрутизатор, ММ – монітор, П - принтер.

Таблиця 1.4 – Перелік технічних засобів

Позначення	Марка	Модель	Серійний номер	Місцезнаходження	Відстань до границі КЗ
PC1 - PC9	Artline	WorkStation W51 (W51v11)	QW1A1 - QW1A9	IT відділ	Від 1 до 8 метрів
PC10 - PC19	Artline	WorkStation W51 (W51v11)	QW1B1 - QW1B9	IT відділ	Від 1 до 8 метрів
PC20 - PC29	Artline	WorkStation W51 (W51v11)	QW1C1 - QW1C9	IT відділ	Від 1 до 8 метрів
PC30 – PC50	Artline	WorkStation W51 (W51v11)	QW1C1 - QW1D1	IT відділ	Від 1 до 8 метрів
PC51 - PC58	Artline	Work Station W31 (W31V03)	AC1B1 - AC1B9	Економічний відділ	Від 1 до 6 метрів
PC59 - PC63	Cobra	Optimal (I64.8.S4.INT.F3838D)	GF1A1 - GF1A7	Юридичний відділ	Від 1 до 7 метрів
PC64 – PC65	Expert	PC Basic (I10100.16.H1S2.INT.A2270)	QQ1A1 - QQ1A2	Пункт охорони	1 м

Продовження таблиці 1.4 – Перелік технічних засобів

Позначення	Марка	Модель	Серійний номер	Місцезнаходження	Відстань до границі КЗ
PC66 - PC71	HP	Z2 G5	GG1A1 - GG1A7	Технічний відділ	Від 1.2 до 5 метрів
PC72 – PC79	Huawei	MateStation S (PUM-WDH9A)	HU1A1 - HU1B1	Бухгалтерія	Від 1.2 до 5 метрів
H1 – H4, H7 – H10	HP	255 G8	NN1A1-NN1A4	HR – відділ, кімнати перемовин	Від 1.6 до 4 метрів
H5 – H6	Apple	MacBook Air M1 13.3	ANA1-AN1A2	Кабінети директорів	2 метри
S1-S2	Artline	Business T65	SA1-SA7	Технічний відділ	4 метри
M1	TP-Link	Archer AX11000	MRSH1	Технічний відділ	6 м
K1	TP-Link	24xRJ-45	KMKM1	Технічний відділ	6 м

Продовження таблиці 1.4 – Перелік технічних засобів

Позначення	Марка	Модель	Серійний номер	Місцезнаходження	Відстань до границі КЗ
К2	TP-Link	24xRJ-45	КМКМ2	Економічний відділ	5 м
К3	TP-Link	24xRJ-45	КМКМ3	Юридичний відділ	4 м
К4	TP-Link	24xRJ-45	КМКМ4	Бухгалтерія	6 м
К5	TP-Link	24xRJ-45	КМКМ5	Технічний відділ	5 м
К6	Cloud Router	Switch Mikrotik (CRS354-48G-4S+2Q+RM)	КМКМ6	ІТ відділ	8 м

Продовження таблиці 1.4 – Перелік технічних засобів

Позначення	Марка	Модель	Серійний номер	Місцезнаходження	Відстань до границі КЗ
КЛ1 – КЛ79	A4tech	FG1010	KLQA1-KLQN5	IT відділ, економічний відділ, юридичний відділ, пункт охорони, технічний відділ, бухгалтерія	Від 1 до 8 метрів
КМ1 – КМ79	A4tech	FG1010	KMQA1-KMQQ9	IT відділ, економічний відділ, юридичний відділ, пункт охорони, технічний відділ, бухгалтерія	Від 1 до 8 метрів
П1-П4	Epson	L1110	PRGF1-PRGF4	Бухгалтерія, юридичний відділ, IT відділ, економічний відділ	Від 7 метрів до 5 метрів

Продовження таблиці 1.4 – Перелік технічних засобів

Позначення	Марка	Модель	Серійний номер	Місцезнаходження	Відстань до границі КЗ
ММ1 – ММ79	Samsung	Curved	M2AP1-M2QM8	ІТ відділ, економічний відділ, юридичний відділ, пункт охорони, технічний відділ, бухгалтерія	Від 1 до 8 метрів

Перелік допоміжних технічних засобів наведено у таблиці 1.5 Позначення у таблиці ДТЗС: Х – холодильник, МХ – мікрохвильова пічка, КВ – камера відеоспостереження, ІЧД – інфрачервоний датчик, ЕЧ – електричний чайник.

Таблиця 1.5 – Перелік допоміжних технічних засобів

Позначення	Марка	Модель	Серійний номер	Місцезнаходження	Відстань до границі КЗ
Х1 - Х3	Vestfrost	CW286W	HW1A1 - HW1A3	Кухня	2 м
МХ1 - МХ2	LG	MS2042DB	MH1A1 - MH1A2	Кухня	2.5 м
КВ1 - КВ22	Hikvision	Turbo DS-2CE16COT-IRF (3.6)	KA1A1 - KA1F9	ІТ відділ, економічний відділ, вхід, юридичний відділ, бухгалтерія, коридор, HR - відділ	Від 1.2 до 8 метрів
ІЧД1 - ІЧД12	Electrum	D-SM-1422	IS1D1 - IS1F2	ІТ відділ, економічний відділ, вхід, юридичний відділ, бухгалтерія, коридор	Від 1.2 до 12 метрів
ЕЧ1-ЕЧ2	Liberton	LEK-1803	EC2A1 - EC2A2	Кухня	1.2 м

1.4 Обстеження обчислювальної системи

Всі пристрої об’єднані в одну локальну обчислювальну мережу . ІТС складається з комп’ютерів та інших електронних пристроїв, що підключені до центрального вузла(комутатора) та утворюють мережу. Також всі комп’ютери мають окремий вихід до мережі інтернет. Схема ІТС зображена на рисунку 1.3, для зруч-

ності сприйняття робочі станції об’єднані у групи, але потрібно зазначити, що кожна робоча станція підключена до комутатора окремо. Ноутбуки підключені до маршрутизатора за допомогою Wi-Fi. PC64 і PC65 підключені напряму до маршрутизатора, без виходу на об’єднуючий комутатор. Сервери об’єднані між собою і мають окремі виходи на основний комутатор.

Для потреб підприємства, не пов’язаних з комерційною діяльністю клієнтів, була також створена локальна мережа.

Інформація, яка обробляється на підприємстві, зберігається на серверах. Перший сервер виконує функції контролеру доменів, а другий відповідає за резервне копіювання:

- S1 – виконує функції контролеру доменів. Контролер домену здійснює автентифікацію користувача в домені, тобто дозволяє йому входити в мережу за допомогою однієї і тієї ж пари логін-пароль з будь-якого включеного до домену комп'ютера, на якому це не заборонено політиками безпеки або локальними налаштуваннями.
- S2 – виконує функції резервного копіювання.

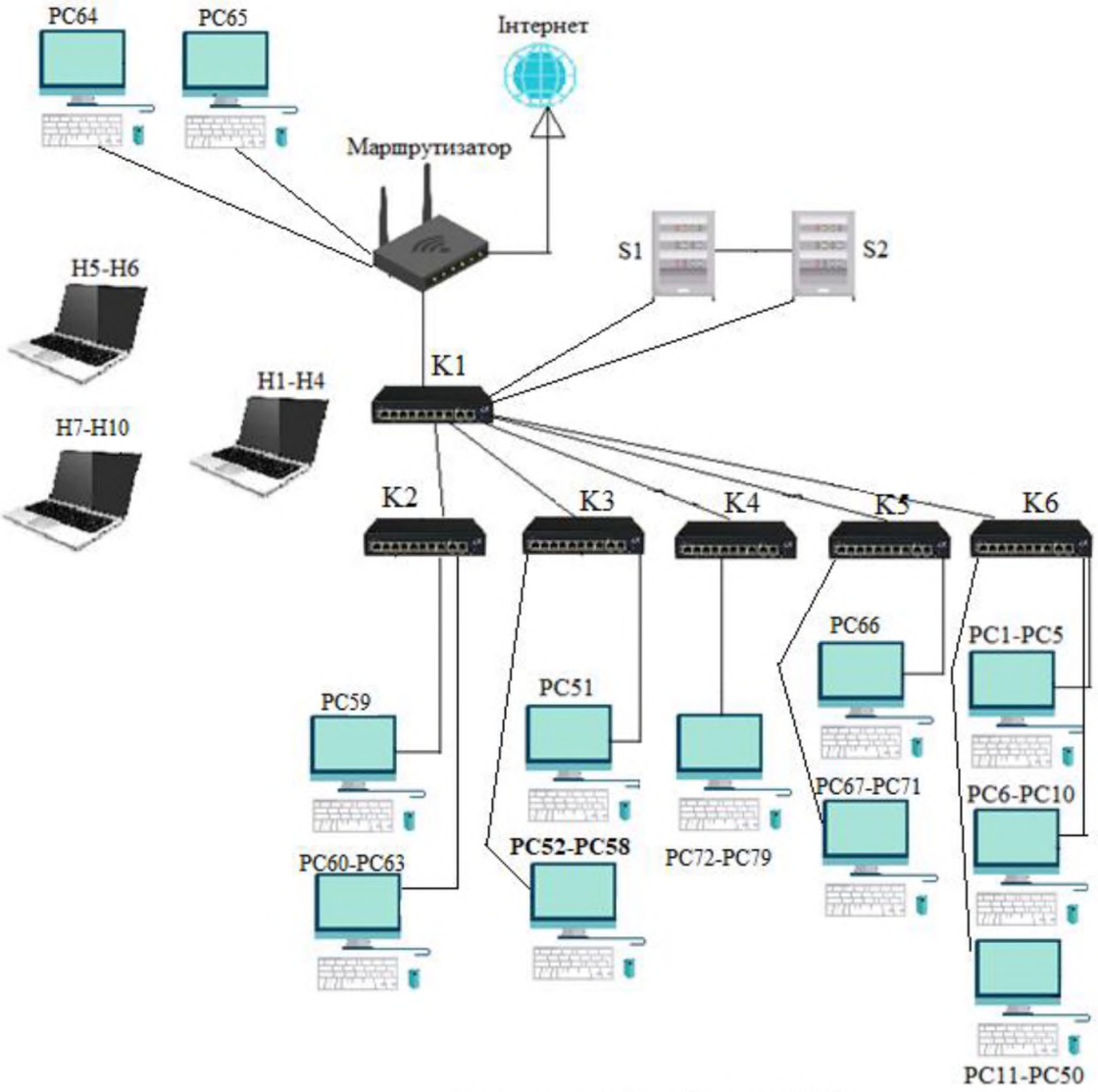


Рисунок 1.3 – Схема ІТС

Таблиця 1.6 – характеристики робочих станцій

Позначення та короткий опис робочих станцій	Характеристики
PC1 – PC50, IT відділ	Intel Core i5-11400F (2.6 – 4.4 ГГц), SSD 1000 ГБ, NVIDIA Quadro P620, RAM 16 ГБ
PC51 – PC58, економічний відділ	Intel Core I3-9100F (3,6 – 4.2 ГГц), SSD 120 ГБ + HDD 2 ТБ, NVIDIA GeForce GT 720 2 ГБ, RAM 8 ГБ
PC59 – PC63, юридичний відділ	Pentium G6400 (4 ГГц), SSD 480 ГБ, Intel UHD Graphics 610, RAM 8 ГБ

Продовження таблиці 1.6 – характеристики робочих станцій

Позначення та короткий опис робочих станцій	Характеристики
PC64 – PC65, пункт охорони	Intel Core i3-10100 (3.6 – 4.0 ГГц), SSD 240 ГБ + HDD 1000 ГБ, Intel UHD Graphics 630, RAM 16 ГБ
PC66 – PC71, технічний відділ	Intel Core i7-10700 (2.9 – 4.8 ГГц), SSD 512 ГБ, Intel UHD 630, RAM 16 ГБ
PC72 – PC79, бухгалтерія	AMD Ryzen 4600G (3.7 – 4.2 ГГц), SSD 256 ГБ, AMD Radeon Graphics, RAM 8 ГБ
H1 – H4, кімнати перемовин	AMD Ryzen 3 3250U (2.6 – 3.5 ГГц), SSD 256 ГБ, AMD Radeon Graphics, RAM 8 ГБ
H5 – H6, кабінети директорів	Apple M1 PRO, SSD 256 ГБ, Apple M1 Graphics, RAM 16 ГБ
H7 – H10, HR-відділ	AMD Ryzen 3 3250U (2.6 – 3.5 ГГц), SSD 256 ГБ, AMD Radeon Graphics, RAM 8 ГБ

Таблиця 1.7 – Програмне забезпечення в ІТС

Назва	Тип	Тип ліцензії	Об'єкти, які використовують ПЗ
Windows 10 x64 PRO 2018	ОС	Commercial	PC41 – PC65, PC72 – PC79
Ubuntu 20.04.4 Desktop (64-bit)	ОС	Free	PC1 – PC40, PC66 – PC71
Atom 1.60.0	Прикладне	Free	PC1 – PC40
Adobe Photoshop CC 2021 v22.5.6.749	Прикладне	Commercial	PC41 – PC50

Продовження таблиці 1.7 – програмне забезпечення в ІТС

Назва	Тип	Тип ліцензії	Об'єкти, які використовують ПЗ
Avast	Антивірусне ПЗ	Free	РС41 – РС65, РС72 – РС79
Office 365	Прикладне	Commercial	РС1 – РС79, Н1 – Н4, Н7 – Н10
Google Chrome x64	Браузер	Free	РС1 – РС79, Н1 – Н4, Н7 – Н10
Adobe Acrobat Reader DC 2018.009.20044	Прикладне	Commercial	РС1 – РС79, Н1 – Н4, Н7 – Н10
Safari 5.1.7	Браузер	Free	Н5 – Н6
Windows Server 2012 R2	ОС	Commercial	S1-S2

1.5 Обстеження інформаційного середовища

В ІТС обробляється великий обсяг інформації, такої як: данні про клієнтів та користувачів сервісів клієнтів; персональні данні робітників; стратегічні плани компанії; інформація про системи захисту, які використовуються підприємством; звітність компанії та інше. Класифікація такої інформація наведена у таблиці 1.8, позначки вимог до захисту: К – конфіденційність, Ц – цілісність, Д – доступність.

Таблиця 1.8 – Класифікація інформації, яка обробляється в ІТС

Інформація	Опис	Правовий режим	Режим доступу	Вимоги до захисту

Інформація	Опис	Правовий режим	Режим доступу	Вимоги до захисту
Персональні данні співробітників	ПІБ, документи, контактні данні, інформація про попередні місця роботи	Конфіденційна	ІзОД	К, Ц, Д

Продовження таблиці 1.8 – Класифікація інформації, яка обробляється в ІТС

Інформація	Опис	Правовий режим	Режим доступу	Вимоги до захисту
Персональні данні клієнтів	ПІБ, контактні данні	Конфіденційна	ІзОД	К, Ц, Д
Персональні данні користувачів клієнтських сервісів	ПІБ, контактні данні, інші данні користувачів	Конфіденційна	ІзОД	К, Ц, Д
Інформація, про продукти клієнтів	Данні про продукт, технології, які використовуються, підключені сервіси	Конфіденційна	ІзОД	К, Ц, Д
Контракти з клієнтами	-	Конфіденційна	ІзОД	К, Ц, Д

Технологічна інформація	Секретні коди доступів до баз данних та інших сервісів	Конфіденційна	ІзОД	К, Ц, Д
Документи підприємства	Юридичні документи підприємства	Конфіденційна	ІзОД	К, Ц, Д

Продовження таблиці 1.8 – Класифікація інформації, яка обробляється в ІТС

Інформація	Опис	Правовий режим	Режим доступу	Вимоги до захисту
Інформація про розвиток та плани розвитку компанії	-	Конфіденційна	ІзОД	К, Ц, Д
Договори зі співробітниками	Контракти зі співробітниками компанії	Конфіденційна	ІзОД	К, Ц, Д
Економічні звіти	-	Конфіденційна	ІзОД	К, Ц, Д
Статистична звітність	-	Відкрита	-	Ц
Інформація про конфігурацію ІТС	-	Конфіденційна	ІзОД	К, Ц, Д

Плани приміщень та систем захисту підприємства	Будь-які данні про системи захисту підприємства, які можуть призвести до потенційних загроз	Конфіденційна	ІзОД	К, Ц, Д

Інформація, яка циркулює в ІТС зберігається в електронному вигляді, але також наявні документи, які зберігаються тільки в паперовому вигляді. До інформації, яка зберігається на папері відноситься: установчі документи підприємства; документи, які регулюють трудові взаємовідносини (трудові книжки, заяви щодо прийому на роботу та звільнення, трудові контракти та інше); документи про взаємовідносини з клієнтами (договори купівлі/продажу послуг, прихідні та розхідні накладні, акти виконаних робіт); офіційна ділова кореспонденція; документи перевірок офіційними державними установами; документи, що підтверджують право власності на різні активи.

Користувачі АС поділені на робочі групи, щодо доступу до інформації. Існуючі групи: адміністратор, користувач. Усі відділи мають доступ тільки до певних видів інформації, яка необхідна для виконання роботи.

Обмін інформацією виконується через сервер та зовнішні носії, такі як: хмарні сховища, системи контролю версій та інші. Також вся інформація, яка зберігається в електронному вигляді має резервні копії.

Таблиця 1.9 – Рівні критичності інформації за властивостями, що підлягають захисту

Конфіденційність	Цілісність	Доступність
К1 - в деяких випадках може нанести мінімальної шкоди, компанія не понесе матеріальних збитків	Ц1 - не призведе до неправильної роботи системи, будь-які наслідки легко виправити	Д1 - не призведе до проблем в роботі системи, в окремих випадках може призвести до мінімальних збитків

К2 - може призвести до незначних матеріальних збитків	Ц2 - може призвести до мінімальних проблем, але ситуацію легко виправити	Д2 - може призвести до мінімальних локальних проблем, але все легко відновити
К3 - може призвести до значних матеріальних збитків	Ц3 - може призвести до проблем в роботі системи, якщо швидко не виправити	Д3 - може призвести до проблем в роботі системи, ситуацію можна відновити, але компанія може понести збитки

Продовження таблиці 1.9 – Рівні критичності інформації за властивостями, що підлягають захисту

Конфіденційність	Цілісність	Доступність
К4 - призведе до великих матеріальних та репутаційних збитків компанії	Ц4 - може призвести до значних проблем в роботі системи, потрібен час для виправлення наслідків	Д4 - призведе до значних проблем в роботі системи, потрібні ресурси для відновлення та компанія понесе значні збитки
К5 - призведуть до критичних матеріальних та репутаційних збитків	Ц5 - призведе до проблем в роботі системи, наслідки можуть бути критичними і невиправними	Д5 - призведе до незворотних наслідків, компанія понесе дуже великі матеріальні збитки

Після розподілення рівнів виконаємо класифікацію інформації з урахуванням критичності.

Таблиця 1.10 – Класифікація інформації яка обробляється ІТС за властивостями

Інформація	Конфіденційність	Цілісність	Доступність
Персональна інформація робітників	К2	Ц2	Д2

Інформація	Конфіденційність	Цілісність	Доступність
Персональні данні клієнтів	К2	Ц2	Д2
Персональні данні користувачів сервісів, які обслуговує товариство	К5	Ц2	Д3
Інформація, про продукти клієнтів	К4	Ц2	Д2
Контракти з клієнтами	К3	Ц2	Д2

Продовження таблиці 1.10 – Класифікація інформації яка обробляється ІТС за властивостями

Інформація	Конфіденційність	Цілісність	Доступність
Технологічна інформація	К4	Ц4	Д4
Документи підприємства	К3	Ц3	Д3
Інформація про розвиток та плани розвитку компанії	К4	Ц3	Д3
Договори з робітниками	К2	Ц2	Д2
Економічні звіти	К3	Ц3	Д3
Плани приміщень та систем захисту підприємства	К5	Ц5	Д5
Трудові контракти та трудові книжки робітників	К2	-	-
Установчі документи підприємства	-	Ц2	Д2
Документи про взаємовідносини з клієнтами	К4	-	-

Офіційна ділова кореспондце-ння	К2	-	-
Документи перевірок офіцій-ними державними установами	К1	К2	Д2

1.6 Обстеження середовища користувачів

До середовища користувачів потрібно віднести усіх робітників компанії, які взаємодіють з АС, а саме:

- Програмісти (40 осіб) – приймають безпосередню участь в розробці та підтримці проектів клієнтів, реалізують основну діяльність товариства;
- Бізнес-аналітики (5 осіб) – складають бізнес задачі для ІТ відділу, спілкуються безпосередньо з клієнтами компанії для розуміння бізнес-цілей.
- Проджект-менеджери (5 осіб) – керують роботою ІТ відділу та слідкують за процесами виконання проектів.
- Фінансовий директор (1 людина) – головний економіст компанії, керує роботою економічного відділу, створює економічну звітність роботи компанії для директорів, приймає економічні рішення для покращення роботи компанії.
- Економісти (7 осіб) – реалізують економічну діяльність компанії, займаються економічною звітністю та аналізують фінансовий потік в компанії.
- Бухгалтери (8 осіб) – слідкують за зарплатнями та прибутками і витратами компанії, готують звітності для податкової служби.
- Керівник охорони (1 людина) – головна людина у сфері охорони компанії, слідкує за охоронними системами та приймає рішення щодо заходів охорони.
- Охорона (1 людина) – слідкує за системами охорони компанії, відповідає за те, щоб не пропускати на територію товариства сторонніх людей, слідкує за пропускним режимом.

- HR, менеджери по персоналу (4 людини) – приймають рішення щодо прийняття кандидатів на працевлаштування в компанію, проводять співбесіди з кандидатами.
- Директори компанії (2 людини) – головні особи, які займаються керуванням компанії, аналізують звіти та приймають стратегічні рішення щодо розвитку компанії.
- Керівник юридичного відділу (1 людина) – головний юрист компанії, який керує роботою юридичного відділу та приймає юридичні рішення щодо роботи компанії.
- Юристи (6 осіб) – вирішують юридичні питання компанії, її співробітників та займаються безпосередньо юридичними відносинами між клієнтами та товариством.
- Керівник технічного відділу (1 людина) – головний технічний працівник компанії, приймає рішення щодо роботи систем в компанії, керує роботою технічного відділу.
- Системні адміністратори (4 особи) – підтримують роботу всієї системи слідкують за безперебійною роботою технічних засобів.

Для того, щоб можна було проаналізувати права доступу кожного користувача ІТС потрібно створити матрицю керування доступом. Позначення у таблиці 1.11: Ч – читання, Р – редагування, З – збереження, В – видалення, І – імпорт або експорт, Д - друк; числові позначення – інформація наведена в таблиці 1.8 перелічена по одній.

Таблиця 1.11 – Матриця керування доступом

Робітники	1	2	3	4	5	6	7	8	9	10	11
Програмісти	Ч, Д	-	Ч, Р, З, В, І	Ч	-	Ч, Р	-	-	Ч	-	Ч

Робітники	1	2	3	4	5	6	7	8	9	10	11
Бізнес-аналітики	Ч, Д	Ч, Д	-	Ч, Д	Ч, Р, І, З, Д	Ч	Ч	Ч, Р, В, Д	Ч	Ч, Р, З, В, І	Ч
Проджект-менеджери	Ч, Д	-	-	Ч, Д	Ч	Ч	-	-	Ч	-	Ч

Продовження таблиці 1.11 – Матриця керування доступом

Робітники	1	2	3	4	5	6	7	8	9	10	11
Фінансовий директор	Ч, Д	Ч, Д	-	Ч	Ч, Р, З, В, І, Д	Ч	Ч, Р, З, В, І, Д	Ч, Р, З, В, І, Д	Ч	Ч, Р, З, В, І, Д	Ч

Економісти	Ч, Д	-	-	Ч	Ч, Р, З, В, І, Д	Ч	-	Ч, Р, З, В, І, Д	Ч	Ч, Р, З, В, І, Д	Ч
Бухгалтери	Ч, Д	-	-	Ч	Ч, Р, З, В, І	Ч	-	-	Ч	Ч, Р, З, В, І, Д	Ч
Керівник охорони	Ч, Д	-	-	-	-	-	-	-	Ч	-	Ч, Р, З, В, І, Д

Продовження таблиці 1.11 – Матриця керування доступом

Робітники	1	2	3	4	5	6	7	8	9	10	11
Охорона	Ч, Д	-	-	-	-	-	-	-	Ч	-	Ч, Р, З, В, І

HR	Ч, Р, З, В, І, Д	Ч, Р, З, В, І, Д	-	Ч	-	-	-	-	Ч, Р, З, В, І, Д	-	Ч
Директори компанії	Ч, Д	Ч, Р, З, В, І, Д	-	Ч, Д, І	Ч, Р, З, В, І, Д	Ч	Ч, Р, З, В, І, Д	Ч, Р, З, В, І, Д	Ч, Д	Ч, Д	Ч
Керівник юридичного відділу	Ч, Д	Ч, Д	-	Ч	Ч, Р, І, З, Д	Ч	Ч, Р, З, В, І, Д	-	Ч, Р, З, В, І, Д	Ч, Р, З, В, І, Д	Ч

Продовження таблиці 1.11 – Матриця керування доступом

Робітники	1	2	3	4	5	6	7	8	9	10	11

Фінансовий директор	Ч, Д	Ч, Д	-	Ч	Ч, Р, З, В, І, Д	Ч	Ч, Р, З, В, І, Д	Ч, Р, З, В, І, Д	Ч	Ч, Р, З, В, І, Д	Ч
Економісти	Ч, Д	-	-	Ч	Ч, Р, З, В, І, Д	Ч	-	Ч, Р, З, В, І, Д	Ч	Ч, Р, З, В, І, Д	Ч
Бухгалтери	Ч, Д	-	-	Ч	Ч, Р, З, В, І	Ч	-	-	Ч	Ч, Р, З, В, І, Д	Ч
Керівник охорони	Ч, Д	-	-	-	-	-	-	-	Ч	-	Ч, Р, З, В, І, Д

Продовження таблиці 1.11 – Матриця керування доступом

Робітники	1	2	3	4	5	6	7	8	9	10	11

Юристи	Ч, Д	Ч, Д	-	Ч	Ч, Р, І, З, Д	Ч	Ч, Р, З, В, І, Д	-	Ч, Р, З, В, І, Д	Ч, Р, З, В, І, Д	Ч
Керівник технічного відділу	Ч, Д	Ч	Ч	Ч	Ч	Ч, Р, З, В, І	Ч	Ч	Ч	Ч	Ч, Р, З, В, І, Д
Системні адміністратори	Ч, Д	Ч	Ч	Ч	Ч	Ч, Р, З, В, І	Ч	Ч	Ч	Ч	Ч, Р, З, В, І, Д

Проаналізувавши матрицю доступу був виявлений надлишковий доступ у деяких користувачів ІТС.

1.7 Модель порушника

Порушника визначають як особу, яка цілеспрямовано або помилково, маючі злі наміри або ні, виконала операції, які призвели або могли призвести до порушення властивостей інформації, які визначаються політикою безпеки.

Спираючись на НД ТЗІ 1.4-001-2000 “ Типове положення про службу захисту інформації в автоматизованій системі”, у кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка повинна бути адекватна реальному порушнику для даної АС.

Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії та інші.

Модель порушника визначає:

- можливу мету порушника та її градацію за ступенями небезпечності для АС;
- категорії осіб, з числа яких може бути порушник;
- припущення про кваліфікацію порушника;
- припущення про характер його дій.

Метою порушника є:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Виконаємо класифікацію порушників за рівнем можливостей, що надаються їм засобами АС, наприклад, поділити на чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей ведення діалогу з АС, можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- третій рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;
- четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

За рівнем знань про АС усіх порушників класифіковано як порушників, що:

- володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;
- володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;
- володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС;
- володіють інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушників класифіковано як порушників, що:

- використовують виключно агентурні методи одержання відомостей;
- використовують пасивні технічні засоби перехоплення інформаційних сигналів;
- використовують виключно штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;

- використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем здійснення дії класифіковано:

- без одержання доступу на контрольовану територію організації (АС);
- з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АС;
- з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів АС;
- з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);
- з одержанням доступу до засобів адміністрування АС і засобів керування КСЗІ

Відповідно до нормативних документів систем технічного захисту інформації (НД ТЗІ 1.6-003-04, НД ТЗІ 3.7-003-05)

По відношенню до АС порушників розділено на внутрішніх “ВП” (з числа співробітників, користувачів системи), або зовнішніх “ЗП”(сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Таблиця 1.12 – Класифікація внутрішніх порушників за рівнем загрози

Позначення	Категорія порушника	Рівень загрози
ВП1	Працівники ІТ відділу	3
ВП2	Працівники економічного відділу	2
ВП3	Працівники технічного відділу	4
ВП4	Охорона	2
ВП5	HR	1

Продовження таблиці 1.12 - Класифікація внутрішніх порушників за рівнем загрози

Позначення	Категорія порушника	Рівень загрози
ВП6	Директори компанії	3
ВП7	Бухгалтери	2

Таблиця 1.13 – Класифікація зовнішніх порушників за рівнем загрози

Позначення	Категорія порушника	Рівень загрози
ЗП1	Хакери	4
ЗП2	Агенти конкурентів	3
ЗП3	Будь-які відвідувачі	2
ЗП4	Працівники обслуговуючих (комунальних та інших) служб	2

Таблиця 1.14 – Класифікація порушника за його метою та рівнем загрози

Позначення	Мета	Рівень загрози
М1	Безвідповідальність, необачність	2
М2	Корисні цілі	3
М3	Навмисне порушення, професійна задача	4

Таблиця 1.15 – Класифікація порушника за його кваліфікацією та рівнем загрози

Позначення	Кваліфікація порушника	Рівень загрози
К1	Має низький технічний рівень знань, але вміє користуватися ІТС	1
К2	Має середній технічний рівень знань і вміє користуватися ІТС	2

Продовження таблиці 1.15 - Класифікація порушника за його кваліфікацією та рівнем загрози

Позначення	Кваліфікація порушника	Рівень загрози
К3	Має високий рівень знань, має гарні навички програмування та проектування ІТС	3
К4	Професіонал, знає нюанси систем захисту ІТС, має навички розробки систем захисту, знає недоліки та вразливості	4

Таблиця 1.16 – Класифікація порушника за його можливостями використання засобів та методів подолання системи захисту

Позначення	Можливості порушника	Рівень загрози
МП1	Може прикладати непрофесійні і нетехнічні зусилля для реалізації порушення	1
МП2	Може використовувати внутрішні недоліки системи безпеки, прикладати непрофесійні технічні зусилля для реалізації порушення	2
МП3	Може використовувати недоліки системи безпеки у тому числі технічні	3
МП4	Може професійно використовувати спеціальні системи та технічні засоби для реалізації порушення	4

Таблиця 1.17 – Класифікація порушника за часом дії

Позначення	Можливості порушника	Рівень загрози
Ч1	Під час ремонту або відновлення ІТС	1
Ч2	Під час призупинки для модернізації або технічного обслуговування ІТС	2
Ч3	Під час звичайної роботи ІТС	3
Ч4	У будь-який час	4

Таблиця 1.18 – Класифікація порушника за місцем дії

Позначення	Можливості порушника	Рівень загрози
МД1	З внутрішніх приміщень КЗ без доступу до технічного обладнання ІТС	1
МД2	З технічних засобів користувачів ІТС (робітники компанії)	2
МД3	Маючи доступ до технічного обладнання спеціального призначення (архіви, бази данних)	3

Продовження таблиці 1.18 – Класифікація порушника за місцем дії

Позначення	Можливості порушника	Рівень загрози
МД4	Маючи повний доступ до систем обслуговування ІТС	4

Таблиця 1.19 – Модель внутрішнього порушника

Порушник	Класифікація за рівнем загрози	Мета порушення	Кваліфікація порушника	Можливості подолання систем захисту	Можливості за часом	Можливості за місцем	Сума
Працівники IT відділу	ВП1	М2	К3	МП3	Ч3	МД3	
	3	3	3	3	3	3	18
Працівники економічного відділу	ВП2	М1	К1	МП1	Ч3	МД2	
	2	2	1	1	3	2	11
Працівники технічного відділу	ВП3	М2	К4	МП4	Ч4	МД4	
	4	3	4	4	4	4	23
Охорона	ВП4	М2	К2	МП2	Ч3	МД2	
	2	3	2	2	3	2	14
HR	ВП5	М2	К1	М1	Ч3	МД2	
	1	3	1	1	3	2	11

Продовження таблиці 1.19 – Модель внутрішнього порушника

Порушник	Класифікація за рівнем загрози	Мета порушення	Кваліфікація порушника	Можливості подолання систем захисту	Можливості за часом	Можливості за місцем	Сума
Директори компанії	ВП6	М2	К2	К2	Ч3	МД3	
	3	2	2	2	3	3	15
Бухгалтери	ВП7	М2	К1	МП1	Ч3	МД2	
	2	2	1	1	3	2	11

Таблиця 1.20 – Модель зовнішнього порушника

Порушник	Класифікація за рівнем загрози	Мета порушення	Кваліфікація порушника	Можливості подолання систем захисту	Можливості за часом	Можливості за місцем	Сума
Хакери	ЗП1	М3	К3	МП4	Ч3	МД0	
	4	4	3	4	3	0	18
Агенти конкурентів	ЗП2	М3	К3	МП4	Ч3	МД4	
	3	4	3	3	3	4	11

Продовження таблиці 1.20 – Модель зовнішнього порушника

Порушник	Класифікація за рівнем загрози	Мета порушення	Кваліфікація порушника	Можливості подолання систем захисту	Можливості за часом	Можливості за місцем	Сума
Відвідувачі	ЗП3	М2	К1	МП1	Ч3	Д2	
	2	3	1	1	3	2	23
Працівники комунальних та інших служб	ЗП4	М1	К2	МП2	Ч3	МД1	
	2	2	2	2	3	1	14

У таблиці 1.19 була складена модель внутрішнього порушника, за сумарною оцінкою рівня загрози можна побачити, що найбільшу небезпеку становлять працівники технічного відділу, бо мають достатній рівень знань, кваліфікацію, обізнаність і доступ до ІТС. Також потрібно звернути увагу на працівників ІТ відділу, вони мають менший за технічний відділ рівень загроз, але достатній для того, щоб можна було зазначити ризики.

У таблиці 1.20 була складена модель зовнішнього порушника, за сумарною оцінкою рівня загрози можна побачити, що найбільшу небезпеку становлять агенти конкурентів.

1.8 Модель загроз

Перед тим, як виявити найважливіші загрози інформаційній безпеці, варто виділити найважливіші об'єкти, до яких належать:

1. Сервери;
2. Персонал;
3. Автоматизовані робочі місця співробітників, на яких обробляється інформація, що захищається;
4. Системи управління ІТС.

Після проведення обстеження середовищ ІТС необхідно визначити всі можливі потенційні загрози для ІТС.

Після визначення найважливіших об’єктів потрібно визначити всі можливі потенційні загрози для ІТС. Походження таких загроз може бути умисним або випадковим.

До випадкових загроз відносять загрози, які виникають в ІТС незалежно від волі людей, такі як: стихійні лиха, збої, технічні баги, відмови, помилки, побічні впливи та інші. Сутність таких подій визначається таким чином:

- збій - тимчасове порушення працездатності якого-небудь елемента системи, наслідком чого може бути неправильне виконання ним у цей момент своєї функції;

- технічні баги – це помилки в коді, які викликають різні незвичайні аномалії у роботі програм.
- відмова - порушення працездатності якого-небудь елемента системи, що призводить до неможливості виконання нею основних своїх функцій;
- помилка - неправильне (разове або систематичне) виконання елементом однієї або декількох функцій, що відбувається внаслідок специфічного (постійного або тимчасового) його стану;
- побічний вплив - негативний вплив на систему в цілому або окремі її елементи, чиниться будь-якими явищами, що відбуваються всередині системи або у зовнішньому середовищі.

До навмисних загроз відносять загрози, які викликані навмисно за волею конкретної людини або групи людей. Передумови появи загроз можуть бути об'єктивними (кількісна або якісна недостатність елементів системи) і суб'єктивними. До останніх відносяться діяльність розвідувальних органів іноземних держав, промислове шпигунство, діяльність кримінальних елементів, дії недобросовісного персоналу ІТС. Перераховані різновиди передумов інтерпретуються таким чином:

- кількісна недостатність - фізична нестача одного або декількох елементів системи, що викликає порушення технологічного процесу обробки даних і / або перевантаження наявних елементів.
- якісна недостатність - недосконаліть конструкції (організації) елементів системи, в силу цього можуть з'являтися можливості випадкового або навмисного негативного впливу на оброблювану або збережену інформацію.

Модель загроз повинна визначити:

- перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);
- перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об’єктів ІТС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи

ІТС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

Загрози для інформації, що обробляється в ІТС, залежать від характеристик ОС, апаратного складу, програмних засобів, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу.

Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись у моделі загроз, наприклад:

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

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

- дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв’язку, видалення даних, програм тощо);
- ненавмисне пошкодження носіїв інформації;
- неправомірна зміна режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

- неумисне зараження ПЗ комп'ютерними вірусами;
- невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;
- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;
- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;
- неправомірне впровадження та використання заборонених політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення тощо);
- наслідки некомпетентного застосування засобів захисту тощо.

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

- порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);
- порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, кондиціонування тощо.);
- порушення режимів функціонування ІТС (обладнання і ПЗ);
- впровадження та використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;
- використання (шантаж, підкуп тощо) з корисливою метою персоналу ІТС;
- крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);
- несанкціоноване копіювання носіїв інформації;
- читання залишкової інформації з оперативної пам'яті ЕОТ, зовнішніх накопичувачів;

- одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача;
- неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;
- впровадження та використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

Таблиця 1.21 – Модель загроз

Загроза	Тип загрози	Вразливість	Порушення	Рівень ризиків	Рівень загроз	Сума
Навмисні загрози						
Потрапляння до технічних засобів робітників сторонніх людей	Зовнішня	Безвідповідальність працівника. Неуважність охорони та інших працівників	К	2	3	5
			Ц	2	4	6
			Д	2	3	5
Потрапляння сторонніх людей до контролюючого обладнання	Зовнішня	Безвідповідальність працівників. Неуважність охорони та інших працівників	К	1	4	5
			Ц	1	4	5
			Д	1	4	5
Потрапляння до системи шкідливих програм або вірусів	Зовнішня або внутрішня	Недоліки систем безпеки і антивірусного ПЗ	К	3	3	6
			Ц	3	4	7
			Д	3	4	7
Скачування неліцензійного ПЗ з небезпечних сайтів, використання зовнішніх носіїв	Внутрішня	Недоліки правил експлуатації технічних засобів на підприємстві Безвідповідальність працівників	К	2	2	4
			Ц	2	3	5
			Д	2	3	5

Продовження таблиці 1.21 – Модель загроз

Загроза	Тип загрози	Вразливість	Порушення	Рівень ризиків	Рівень загроз	Сума
Навмисні загрози						
Навмисне порушення роботи систем життєдіяльності підприємства (електропостачання, інтернет та інше)	Зовнішня або внутрішня	Недоліки системи безпеки Неуважність охорони	К	2	2	4
			Ц	2	3	5
			Д	2	4	6
Навмисне порушення властивостей безпеки інформації робітником	Внутрішня	Недоліки розподілу повноважень Неефективність підбору персоналу	К	2	4	6
			Ц	2	3	5
			Д	2	3	5

Продовження таблиці 1.21 – Модель загроз

Загроза	Тип загрози	Вразливість	Порушення	Рівень ризиків	Рівень загроз	Сума
Навмисні загрози						
Отримання доступу до каналів передачі інформації (за допомогою ПЕМВН або за допомогою стороннього ПЗ)	Внутрішня або зовнішня	Неуважність охорони Недоліки заходів безпеки на підприємстві	К	1	4	5
			Ц	2	3	5
			Д	2	3	5

Продовження таблиці 1.21 – Модель загроз

Загроза	Тип загрози	Вразливість	Порушення	Рівень ризиків	Рівень загроз	Сума
Випадкові загрози						
Випадкове фізичне пошкодження технічного обладнання або інших носіїв інформації(архів)	Внутрішня	Необережність працівника	К	-	-	-
			Ц	2	3	5
			Д	2	3	5
Випадкове розголошення інформації	Зовнішня	Необережність та неуважність працівника	К	3	4	7
			Ц	1	1	2
			Д	1	1	2
Помилка в роботі системи	Внутрішня	Недостатньо пильний контроль за роботою системи та її конфігурацією *Невчасне та неефективне тестування	К	2	3	5
			Ц	2	3	5
			Д	2	3	5

Продовження таблиці 1.21 – Модель загроз

Загроза	Тип загрози	Вразливість	Порушення	Рівень ризиків	Рівень загроз	Сума
Випадкові загрози						
Помилки в роботі внутрішнього ПЗ	Внутрішня	Використання недосконалого та застарілого ПЗ, а також антивірусного ПЗ	К	2	4	6
			Ц	2	3	5
			Д	2	3	5
Помилки персоналу	Внутрішня	Людський фактор Недостатня компетентність робітників	К	2	3	5
			Ц	2	3	5
			Д	2	3	5
Природні загрози						
Стихійні лиха	Зовнішня	Недосконала пожежна система Недоліки проектування будівлі	К	-	-	-
			Ц	2	4	6
			Д	2	4	6

Продовження таблиці 1.21 – Модель загроз

Загроза	Тип загрози	Вразливість	Порушення	Рівень ризиків	Рівень загроз	Сума
Природні загрози						
Аномальні помилки в роботі мереж (короткі замикання, витік газу і тп)	Зовнішня	Застарілі системи постачання електроенергії Недостатня якість мереж постачання	К	-	-	-
			Ц	1	4	6
			Д	1	4	6

1.9 Висновки до розділу 1

У першому розділі було розглянуто фізичне середовище підприємства, його рід діяльності та плани будівлі та приміщень КЗ. Також була обґрунтована необхідність створення КСЗІ, обстежене фізичне середовище ІТС, обчислювальна система та середовище користувачів. Були виявлені загрози.

Була створена матриця керування доступом користувачів ІТС та був виявлений надлишковий доступ у деяких користувачів.

Було створено модель порушника (зовнішнього та внутрішнього) та модель загроз.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Оцінка існуючого стану захищеності

Для того щоб потрапити на територію підприємства робітники використовують спеціальні картки-перепустки, картка обладнана спеціальним чипом, який зчитується на вході до підприємства для розблокування дверей. Після того як робітник потрапив на територію, він повинен просканувати свою картку-перепустку на пункті охорони для того, щоб система записала данні робітника та час, коли він потрапив на територію підприємства. Таким чином обмежується потрапляння сторонніх людей на територію підприємства.

На підприємстві для захисту від шкідливого ПЗ та вірусів використовується антивірусне ПЗ “Avast” від компанії “Avast Software”, тип ліцензії є безкоштовним, тому деякі функції відключені і антивірусне ПЗ працює не достатньо ефективно. Відключені такі функції як глибоке сканування та VPN, які мають великий вплив на ступінь захищеності системи.

Сервери використовують ОС Windows Server 2012 R2, який має експертний висновок, але його термін дії вже вийшов та система вже не має актуальних оновлень і підтримки зі сторони компанії-розробника.

Для входу в систему користувачі ІТС використовують логін та пароль, які мають свої обмеження. Обмеженнями для логіну встановлені: довжина (5 – 15 символів). Для паролю встановлені обмеження: довжина (8 – 16 символів), 1 велика літера, 1 спеціальний символ.

2.2 Вибір профілю захищеності і визначення рівня гарантій

Для того щоб обрати профіль захищеності потрібно визначити клас автоматизованої системи. Автоматизована система ТОВ “DevUA” була віднесена до 3 класу. Робочі станції використовують ОС Windows 10 Professional та Ubuntu *Pack 18.04.

Ubuntu *Pack 18.04 має експертний висновок зареєстрований в Державній службі спеціального зв'язку та захисту інформації за № 985 від 27.06.19 і № 1133 від 09.07.20 та внесено в "Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом", що дозволяє його використання у системах, де циркулює інформація з обмеженим доступом та персональні дані. Сукупність послуг безпеки, які реалізуються функціональним складом ОС «Ubuntu*Pack» становлять такий профіль захищеності:
3.КЦД."Ubuntu*Pack 18.04/20.04"={КД-2, КА-1, КА-2, КО-1, КВ-2, ЦД-1, ЦА-1, ЦА-2, ЦВ-2, ДР-1, ДЗ-1, ДС-1, ДВ-1, НР-3, НИ-3, НК-1, НО-3, НЦ-2, НТ-3, НВ-2}. Розробником забезпечуються гарантії реалізації послуг безпеки, процесу розробки, постачання та супроводження ОС «Ubuntu*Pack» згідно з умовами гарантій рівня **Г-3**.

Windows 10 Professional також 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.

Відповідно до НД-ТЗІ-2.5-005—99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" ІТС ТОВ "DevUA" можна віднести до класу 3. Клас 3 — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу. Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

Відповідно до вищенаведеного НД-ТЗІ-2.5-005-99 було обрано функціональний профіль захищеності 3.КЦД.2, але були внесені деякі правки:

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

КД-2 (Базова довірча конфіденційність). Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Реалізована системою контролю доступів. НЕОБХІДНІ УМОВИ: НИ-1

КА-2 (Базова адміністративна конфіденційність). Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Реалізована КА-3 (Повна адміністративна конфіденційність) розмежуванням прав користувачів. НЕОБХІДНІ УМОВИ: НО-1, НИ-1

КО-1 (Повторне використання об'єктів). Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу. Реалізована завдяки розмежуванню доступу користувачів до окремих акаунтів

КВ-2 (Базова конфіденційність при обміні). Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Реалізована базовими функціями встановлених ОС. НЕОБХІДНІ УМОВИ: НО-1

ЦД-1 (Мінімальна довірча цілісність). Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Реалізована завдяки розмежуванню рівнів доступу. НЕОБХІДНІ УМОВИ: НИ-1

ЦА-2 (Базова адміністративна цілісність). Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Реалізована ЦА-3 (Повна адміністративна цілісність) завдяки наявності адміністраторів та розмежуванню рівнів доступу користувачів. НЕОБХІДНІ УМОВИ: НО-1, НИ-1

ЦО-1 (Обмежений відкат). Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Реалізована ЦО-2 (Повний відкат) завдяки наявності системи резервного копіювання та налаштуванням відкату в окремих програмних засобах. НЕОБХІДНІ УМОВИ: НИ-1.

ЦВ-2 (Базова цілісність при обміні). Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Не реалізована.

ДР-1 (Квоти). Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Не реалізована.

ДВ-1 (Ручне відновлення). Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Реалізована ДВ-2 (Автоматизоване відновлення) завдяки резервному копіюванню та налаштуванню ОС. НЕОБХІДНІ УМОВИ: НО-1

НР-2 (Захищений журнал). Реєстрація дозволяє контролювати небезпечні для КС дії. Реалізована НР-4 (Детальна реєстрація) завдяки налаштуванню реєстрації небезпечних для інформації подій. НЕОБХІДНІ УМОВИ: НИ-1, НО-1

НИ-2 (Одиночна ідентифікація і автентифікація). Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Реалізована завдяки налаштованій системі ідентифікації і автентифікації користувачів. НЕОБХІДНІ УМОВИ: НК-1

НК-1 (Однонаправлений достовірний канал). Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Реалізована стандартними функціями ОС.

НО-2 (Розподіл обов'язків адміністраторів). Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Реалізована, наявні 2 типи адміністраторів (адміністратор безпеки і звичайний адміністратор), які мають різні обов’язки та реалізують різні функції. НЕОБХІДНІ УМОВИ: НИ-1

НЦ-2 (КЗЗ з гарантованою цілісністю). Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами. Реалізована з використанням стандартних функцій ОС. НЕОБХІДНІ УМОВИ: НР-1, НО-1

НТ-2 (Самотестування при старті). Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Реалізована за допомогою антивірусного ПЗ. НЕОБХІДНІ УМОВИ: НО-1

НВ-1 (Автентифікація вузла). Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Реалізована з використанням стандартних функцій ОС.

2.3 Проектні рішення

ІТС ТОВ “DevUA” підтримують 6 осіб (керівник технічного відділу і 5 системних адміністраторів), для оптимальної ефективності безпеки інформації, було прийнято рішення про розподіл обов’язків системних адміністраторів. Керівник технічного відділу буде виконувати функції адміністратора безпеки, 5 системних адміністраторів будуть виконувати функції адміністраторів системи. Таке рішення має максимально ефективно розподілити права і обов’язки адміністраторів.
Адміністратор безпеки виконує такі функції:

- Встановлює розмежування повноважень користувачів та порядок доступу до інформаційних ресурсів, порядок використання основних та допоміжних технічних засобів та систем.
- Здійснює контроль за виконанням працівниками організації робіт згідно з переліком заходів щодо забезпечення безпеки інформації, веде облік позаштатних ситуацій;
- інформує керівництво та уповноважених працівників служби безпеки про інциденти та спроби несанкціонованого доступу до інформації, елементів

автоматизованих систем управління за результатами функціонування та контролю систем технічного захисту інформації.

- Здійснює адміністрування сервісами та механізмами безпеки автоматизованих систем управління, комплексами та засобами технічного захисту інформації та контролю;
- Припиняє роботи за недотримання встановленої технології обробки інформації та невиконання вимог інформаційної безпеки;
- Готує пропозиції щодо вдосконалення технологічних заходів захисту інформації.
- Контролює роботи з встановлення, модернізації та профілактики апаратних та програмних засобів;
- Створення, облік, зберігання та використання резервних та архівних копій масивів даних та електронних документів.
- Бере участь у роботах із внесення змін до програмно-апаратної конфігурації автоматизованої системи управління та контролює її відповідність вимогам забезпечення безпеки інформації.
- Веде облік носіїв інформації, здійснює їх зберігання, приймання, видачу відповідальним виконавцям, контролює правильність їх використання.

Для забезпечення більшої надійності захисту інформації для товариства потрібно запровадити ряд правил, які будуть регулювати обов'язки, і заборони для робітників.

Робітникам заборонено:

- Виходити до мережі інтернет з робочого пристрою без використання VPN.
- Використовувати робочій профіль та пошту для реалізації своїх особистих потреб (відправляти електронні листи на сторонні адреси, які не пов'язані з робочим процесом, реєструвати робочу електрону пошту на сторонніх сервісах не пов'язаних з робочим процесом та інше).
- Фотографувати або робити відеозаписи робочих процесів не в робочих цілях.

- Використовувати робочі профілі інших робітників для вирішення будь-яких потреб, якщо не було надано відповідний дозвіл.
- Використовувати перепустки інших робітників для потрапляння на територію підприємства.
- Розголошувати конфіденційну і таємну інформацію (інформація про розроблювані проекти, системи захисту інформації на підприємстві, ключі доступу, паролі та інше).
- Знаходитись на території підприємства після закінчення робочого дня, якщо не було дозволу від керівництва компанії.
- Використовувати зовнішні носії для збереження конфіденційної або таємної інформації.
- Використовувати робочі пристрої для реалізації своїх особистих потреб (розваги і тд).
- Встановлювати на робочі пристрої неліцензійне стороннє ПЗ.
- Встановлювати на робочі пристрої ПЗ, яке не відноситься до робочих процесів.
- Випитувати інформацію про робочі процеси у інших робітників.
- Виконувати будь-які дії, які можуть порушити безпеку інформації в АС.

Робітники зобов'язані:

- Підписати NDA (угоду про нерозголошення).
- Виконувати свої обов'язки щодо забезпечення захисту інформації на підприємстві перелічені у списку заборон.

У першому розділі була розглянута існуюча матриця доступу(таблиця 1.11), проаналізувавши її було зроблено висновок, що існує багато надлишкового доступу у деяких користувачів. Було прийнято рішення розробити нову матрицю доступу.

Таблиця 2.1 Нова матриця доступу

Робітники	1	2	3	4	5	6	7	8	9	10	11
Програмісти	Ч	-	Ч, Р, З	Ч	-	Ч	-	-	-	-	Ч
Бізнес-аналітики	Ч	Ч	-	Ч, Д	Ч, Р, І, З, Д	-	-	Ч	-	Ч	Ч
Проджект-менеджери	Ч	-	-	Ч, Д	-	-	-	-	-	-	Ч
Фінансовий директор	Ч, Д	Ч	-	Ч	Ч	-	Ч, Р, З, В, Д	Ч, Р, З, В	-	Ч, Р, З, В, І, Д	Ч
Економісти	-	-	-	Ч	-	-	-	Ч	-	Ч, Р, З, В	Ч
Бухгалтери	-	-	-	Ч	-	-	-	-	-	Ч, Р, З, В, Д	Ч
Керівник охорони	Ч	-	-	-	-	-	-	-	Ч	-	Ч
Охорона	-	-	-	-	-	-	-	-	Ч	-	Ч

Продовження таблиці 2.1 – Нова матриця доступу

Робітники	1	2	3	4	5	6	7	8	9	10	11
HR	Ч, Р, З, В, Д	Ч	-	Ч	-	-	-	-	Ч, Р, З, В, І, Д	-	Ч
Директори компанії	Ч	Ч	-	Ч	Ч, Д	-	Ч, Р, З, В, Д	Ч, Р, З, В	Ч, Д	Ч, Д	Ч
Керівник юридичного відділу	Ч, Д	Ч, Д	-	Ч	Ч, Р, І, З, Д	-	Ч, Р, З, В, Д	-	Ч, Р, З, В, І, Д	Ч, Р, З, Д	Ч
Юристи	Ч	Ч	-	Ч	Ч, Р, З	-	Ч, Р, З, В, І	-	Ч, Р, З, В	Ч, Р, З	Ч

Продовження таблиці 2.1 – Нова матриця доступу

Робітники	1	2	3	4	5	6	7	8	9	10	11
Керівник технічного відділу	Ч	Ч	Ч	Ч	Ч	Ч, Р, З, В	Ч	Ч	Ч	Ч	Ч, Р, З, В, І, Д
Системні адміністратори	Ч	Ч	Ч	Ч	Ч	Ч, Р, З	Ч	Ч	Ч	Ч	Ч, Р, З

У таблиці 2.1 була перероблена матриця доступу користувачів ІТС, більшості користувачів була заборонена можливість друку та імпорту/експорту, наразі за ці функції відповідають керівники відділів. Також були обмежені права доступу до інших функцій, які не є обов'язковими для конкретних типів користувачів.

Як було зазначено раніше, для доступу в систему користувачі використовують логіни і паролі, які мають певні обмеження. Було прийнято рішення вдосконалити обмеження створення та оновлення паролю для покращення рівня безпеки. Також було прийнято рішення про оновлення паролю кожних 3 місяці, таке оновлення має суттєво підвисити рівень безпеки робочих акаунтів користувачів ІТС.

Правила створення/оновлення паролю:

- Мінімальна довжина – 8 символів.
- Обов'язкова наявність, як мінімум, 1 спеціального символу, таких як: "!@#$%&*_-+".
- Обов'язкова наявність, як мінімум однієї великої літери.
- Обов'язкова наявність, як мінімум, 1 цифри.
- Максимальна довжина 32 символи.

- Заборонено використовувати в паролі персональні данні, такі як: фамілія, ім'я, ім'я по батькові, дата народження.
- Заборонено використовувати використані раніше паролі при оновленні.

Як було вказано у підрозділі 2.1 на серверах використовується застаріла версія Microsoft Server 2012 R2, який не має актуальних оновлень та підтримки. Було прийнято рішення оновити ОС на серверах на Microsoft Server 2019 Datacenter, яка має актуальний експертний висновок і належну підтримку з новітніми оновленнями безпеки.

Також на робочі станції ТОВ "DevUA" встановлене безкоштовне антивірусне ПЗ "Avast". Порівняння необхідних функцій антивірусного ПЗ від різних виробників наведена у таблиці 2.2. Було порівняне антивірусне ПЗ ESET Protect MDR, Avast Premium security 21.6.2474.0, Avira 15.0.33.24, Bit Defender 18.14.0.1088. Після аналізу було визначено, що оптимальним антивірусним ПЗ є ESET Protect MDR і антивірусне ПЗ від Bit Defender. Враховуючи аналіз ринку антивірусного ПЗ та вивчення докладу з кібербезпеки від ESET, було прийнято рішення про перехід на платну ліцензію антивірусу ESET Protect MDR для отримання повного функціоналу ПЗ та підвищення рівня безпеки пристроїв та захисту інформації. Така версія антивірусного ПЗ була розроблена, як оптимальне рішення для IT-організацій і має новітні функції для захисту інформації та робочих станцій. ESET Protect MDR має єдину консоль управління безпекою, що дозволяє централізовано керувати системою на всіх робочих станціях та заздалегідь передбачати більшість загроз.

Було прийнято рішення про заборону виходу до мережі інтернет без використання VPN. Для запровадження VPN на робочих станціях буде використовуватися комплект раніше обраного антивірусного ПЗ, який має у своєму функціоналі і VPN.

Таблиця 2.2 Порівняння функцій антивірусного ПЗ

Назва	Наявність версії ПЗ для IT підприємств	Навність влаштованого VPN	Захист в реальному часі	Захист від загроз в інтернеті	Сканування мережі	Захист від програм-вимагачів	Захист від фішингу
Avast Premium security 21.6.2474.0	-	+	+	+	+	+	-
ESET Protect MDR	+	-	+	+	+	+	+
Bit Defender 18.14.0.1088	-	+	+	+	+	+	+
Avira 15.0.33.24	-	-	+	-	+	-	-

Для підвищення надійності запобігання витокам даних компанії було прийняте рішення про впровадження DLP-системи. Під DLP-системами прийнято розуміти програмні продукти, які захищають організації від витоків конфіденційної інформації. Сама абревіатура DLP розшифровується як Data Leak Prevention, тобто запобігання витоку даних.

Подібного роду системи створюють захищений цифровий «периметр» навколо організації, аналізуючи всю вихідну, а часом і вхідну інформацію. Контрольованою інформацією може бути не тільки інтернет-трафік, а й інші інформаційні потоки, такі як: документи, що виносяться за межі захисту контуру безпеки на зовнішніх носіях, роздруковуються на принтері, що відправляються на мобільні носії через Bluetooth та інші системи.

За здатністю блокування інформації, упізнаної як конфіденційна DLP-системи можна поділити на системи з активним та пасивним контролем дій користувача.

Активні DLP-системи вміють блокувати передану інформацію, пасивні, відповідно, такої здатності не мають. Активні системи краще борються з випадковими витоками даних, але при цьому здатні допустити випадкову зупинку бізнес-процесів організації, другі ж безпечні для бізнес-процесів, але підходять тільки для боротьби з систематичними витоками.

В даний час найпопулярнішими розробниками DLP-систем є компанії, які відомі своїми іншими продуктами для забезпечення інформаційної безпеки в організаціях. Це насамперед Symantec, McAffee, TrendMicro і WebSense.

Після аналізу ринку DLP-систем та перегляду тестувань DLP-систем від незалежних експертів було обрано систему Symantec DLP.

DLP Symantec відрізняють зручна консоль управління, гнучка настройка контрольованих каналів та наявність модуля Data Insight, який дозволяє здійснювати аудит файлових сховищ з можливістю створення повідомлень при підвищеній активності користувачів під час роботи з тим чи іншим файловим ресурсом. Крім цього, Symantec DLP має механізм інтелектуального самонавчання Vector Machine Learning, призначений для захисту неструктурованих даних, який більш

ефективний у порівнянні зі звичайним підходом до аналізу документів з цифрових відбитків.

DLP-система Symantec має великий список функцій, але основними, які вплинули на підсумковий вибір були:

- Пошук та аналіз даних. Система шукає місця зберігання та аналізує конфіденційні данні, що зберігаються на портативних та настільних комп'ютерах, серверах, у репозиторіях баз даних, на SharePoint серверах та будь-яких інших мережевих ресурсах організації.
- Контроль за розповсюдженням інформації. Перешкоджає поширенню конфіденційних даних через клієнтські системи, віддалені офіси та комп'ютери кінцевих користувачів.
- Запобігання витоку даних. Контролює інциденти, пов'язані з передачею даних на комп'ютерах користувачів: надсилання листів електронною поштою, миттєві повідомлення, публікації корпоративних даних в інтернеті, копіювання даних на знімні пристрої, виведення на друк, передача факсом, функції копіювання та вставки.
- Політики, оповіщення та блокування. Symantec DLP має універсальні політики та активний захист від витоку конфіденційних даних за межі організації. Також система фіксує, попереджає та автоматично блокує будь-які порушення внутрішніх бізнес-процесів, які можуть призвести до витоку.
- Управління та налаштування. Система має єдину консоль управління DLP Enforce Platform для створення, розгортання та застосування політик запобігання витоку даних, реагування на інциденти, аналізу порушень політик та створення звітів щодо них, а також для виконання завдань з адміністрування системи.

Пакет Symantec Data Loss Prevention також включає моніторинг мобільних пристроїв і мобільної електронної пошти через Symantec DLP for Mobile з Mobile Email Monitor і Mobile Prevent. Мобільний монітор електронної пошти підтримує пристрої Android та iOS і може виявляти, коли співробітники завантажують

конфіденційні корпоративні дані на свої мобільні пристрої за допомогою протоколу Microsoft Exchange ActiveSync.

Symantec Data Loss Prevention for Endpoint використовує модулі Symantec DLP Endpoint Discover і Symantec Endpoint Prevent, які контролюють дані, що використовуються. Ці модулі виконують локальне сканування, виявлення та моніторинг для комп'ютерів macOS, Windows 7, Windows 8 та Windows 10. На кінцевих точках ці модулі також контролюють і керують папками синхронізації хмарного сховища, клієнтами електронної пошти Outlook і Lotus Notes, трафіком протоколів HTTP/HTTPS і FTP, зовнішніми носіями інформації, такими як USB, протокол передачі медіа, CompactFlash і SD-картами, а також eSATA та FireWire для портативних дисків. Модулі також контролюють і керують віртуальними робочими столами, такими як Citrix, Microsoft Hyper-V і VMware.

Функція Cloud File Sync and Share не дозволяє користувачам синхронізувати конфіденційні файли даних з робочої станції на хмарні сховища, такі як Box, Dropbox, Google Drive, Hightail, iCloud і Microsoft OneDrive.

2.4 Висновки до розділу 2

У другому розділі був оцінений існуючий стан захищеності та запропоновані проектні рішення для підвищення рівня захисту інформації. Були розроблені наступні проектні рішення:

- Введення обов'язкових правил заборон і обов'язків користувачів ІТС, який встановлює обмеження при користуванні технічними засобами АС і інформації, яка циркулює в ІТС.
- Оновлення або заміна існуючого ПЗ на новітні версії або на кращі аналоги для отримання повноти функціоналу та підвищення рівню безпеки.
- Оновлено матрицю доступу користувачів ІТС для оптимального розмежування їх прав.

- Введення правил оновлення паролів користувачів, а саме: обов’язкове оновлення паролю кожні 3 місяці; валідація паролю з використанням нових правил.
- Запровадження DLP-системи для мінімізації ризиків витоків даних.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою виконання економічного розділу дипломного проекту є техніко-економічне обґрунтування необхідності запровадження комплексної системи захисту інформації ТОВ “DevUA”.

Економічна доцільність запровадження КСЗІ визначається розрахунком капітальних і експлуатаційних витрат та аналізом очікуваних результатів від впровадження запропонованих проектних рішень.

Підприємство “DevUA” займається розробкою веб-проектів, які віддалено поставляє своїм клієнтам. Річний прибуток підприємства становить – 25 180 220 гривень. Кількість робітників та функції, які вони виконують зазначені у першому розділі.

3.1 Розрахунок трудомісткості запровадження КСЗІ

Трудомісткість розробки комплексної системи захисту інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t= t_{тз}+t_{в}+t_{а}+t_{вз}+t_{озб}+t_{овр}+t_{д}, \text{ год.}, \qquad (3.1)$$

де: $t_{тз}$- тривалість складання технічного завдання на розробку комплексної системи безпеки інформації;

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

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

$t_{в}з$- тривалість визначення вимог до заходів, методів та засобів захисту;

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

$t_{овр}$- тривалість організації виконання відновлюваних робіт і забезпечення неперервного функціонування організації;

$t_{д}$- тривалість документального оформлення комплексної системи захисту інформації.

Відповідно до формули 3.1, трудомісткість розробки політики безпеки інформації дорівнює:

$$t = 22+12+14+24+13+14+12 = 111 \text{ годин.}$$

3.2 Розрахунок капітальних витрат

Капітальні витрати розраховуються за формулою:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н}$$

де: $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення консультантів - 2400 гривень.

$К_{зпз}$ – вартість закупівель ліцензійного основного і додаткового ПЗ.

$К_{рп}$ – вартість розробки комплексної системи захисту інформації – 20217,20 грн;

$К_{аз}$- вартість закупівлі апаратного забезпечення та допоміжних матеріалів. Нового обладнання встановлено не було, тому цей показник не враховуємо.

$К_{н}$ - витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

$К_{навч}$ – витрати на навчання технічних фахівців в обслуговуючого персоналу, витрати на навчання системного адміністратора 1800 грн;

3.3 Розрахунок витрат на запровадження комплексної системи захисту інформації

Розрахунок витрат на створення комплексної системи захисту інформації:

$$К_{рп}=З_{зп}+З_{мч}$$

де: $К_{рп}$ – витрати на створення комплексної системи захисту інформації;

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

$З_{мч}$ – вартість витрат машинного часу, що необхідні для створення комплексної системи захисту інформації.

Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою:

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

де: t – загальна тривалість розробки комплексної системи захисту інформації, годин;

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

Средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить – 180 грн/ годину.

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби та визначається за формулою

$$З_{зп} = 111 * 180 = 19980 \text{ гривень};$$

Вартість машинного часу для запровадження КСЗІ розраховується за формулою:

$$З_{мч} = t * С_{мч} = 111 * 2,13 = 237,20 \text{ гривень}$$

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

Вартість 1 години машинного часу розраховується за формулою:

$$С_{мч} = P \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}$$

$= 2,13$

Де – P – встановлена потужність ПК, 0.6 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, 6908 грн;

$Н_а$ – річна норма амортизацій за ПК, 0.3 частки одиниці;

$К_{лпз}$ – вартість ліцензійного ПЗ, 1420 гривень;

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

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня) $F_р$ = 2420 годин;

Вартість ПК = 14200 гривень, строк корисної служби 48 місяців;

Накопичена амортизація = (14200*48)/(8*12) = 7100 гривень;

Залишкова вартість = 14200 – 7100 = 7100 гривень;

Вартість розробки комплексної системи захисту інформації:

$$К_{рб} = 19980 + 237,20 = 20217,20 \text{ грн.}$$

Капітальні витрати на проектування та запровадження комплексної системи захисту інформації:

$$К = 20217,20 + 2400 + 1800 = 24417,20 \text{ грн.}$$

3.4 Розрахунок витрат на впровадження DLP системи

$К_{пу} = З_{зп} + З_{мч} + К_{пз} = 1250 + 48,99 + 1800 = 3098,99$ грн;

де $К_{пу}$ – вартість запровадження технології,

$К_{пз}$ – вартість впровадження DLP системи

Таблиця 3.1 Трудомісткість впровадження DLP системи

Витрати	Трудомісткість, год-осіб	Вартість грн/год	Сума
Встановлення ПЗ	6	62,5	375
Налаштування ПЗ	12	62,5	750
Навчання персоналу	5	62,5	312
Всього			1437

Вартість машинного часу на впровадження DLP-системи становить:

$$З_{мч} = t*С_{мч} = 23*2,13 = 48,99 \text{ грн.}$$

3.6 Розрахунок витрат на оновлення операційних систем

$К_{пу} = З_{зп} + З_{мч} + К_{пз} = 1250 + 53,25 + 12178 = 13481,25$ грн;

де $К_{пу}$ – вартість запровадження технології,

$К_{пз}$ – вартість придбання операційних систем

Таблиця 3.2 Трудомісткість оновлення ОС для серверів

Витрати	Трудомісткість, год-осіб	Вартість грн/год	Сума
Встановлення ОС	12	62,5	750
Налаштування ОС	12	62,5	750
Навчання персоналу	1	62,5	62,5
Всього			1562,5

Вартість машинного часу на впровадження операційної системи становить:

$$З_{мч} = t*С_{мч} = 25*2,13 = 53,25 \text{ грн.}$$

Кількість серверів на яких потрібно оновити ОС – 2 штуки; Вартість 1 ліцензії – 6089 гривень;

3.7 Розрахунок витрат на встановлення антивірусного ПЗ

$К_{пу} = З_{зп} + З_{мч} + К_{пз} = 1250 + 61,88 + 90850 = 92161,88$ грн;

де $К_{пу}$ – вартість запровадження технології,

$К_{пз}$ – вартість придбання програмного забезпечення

Таблиця 3.3 Трудомісткість запровадження антивірусного ПЗ

Витрати	Трудомісткість,	Вартість	Сума

	год-осіб	грн/год	
Встановлення ПЗ	12	62,5	750
Налаштування ПЗ	12	62,5	750
Навчання персоналу	5	62,5	312,5
Всього			1812,5

Вартість машинного часу на оновлення операційних систем становить:

$$З_{мч} = t*С_{мч} = 29*2,13 = 61,88 \text{ грн.}$$

Кількість РС на яких потрібно встановити антивірусне ПЗ – 79 штуки; Вартість 1 ліцензії – 1150 гривень;

Враховуючи витрати на впроваджені технології сукупні капітальні витрати становитимуть:

$$К = 24417,20 + 3098,99 + 13481,25 + 92161,88 = 133159.32 \text{ гривень;}$$

3.8 Розрахунок експлуатаційних витрат

Поточні витрати розраховуються за формулою:

$С_п = С_л + С_о$

де $С_л$ – це витрати на продовження ліцензії, за одиницю

$С_о$ – витрати на оновлення ПЗ.

Розрахунок витрат на оновлення ПЗ виконується наступним чином:

$С_о = З_{зп} + З_{мч}$

Поточні витрати на використання антивірусного ПЗ:

- Трудомісткість оновлення становить 3 години.
- Витрати на оновлення ПЗ – 375 + 3.48 = 378,48 грн.
- Витрати на подовження ліцензії - (1 одиниця ліцензії для подовження за 5 компьютерів – 1150 гривень). У системі 79 комп'ютерів, тому потрібно придбати 16 ліцензій, що буде коштувати: 16*1150 = 18400.

- Поточні витрати – 18400 + 378,48 = 18773,48 грн.

Поточні витрати на використання DLP системи:

- Трудомісткість оновлення становить 6 годин.
- Витрати на оновлення ПЗ – 750 + 6,29 = 756,29 грн.
- Витрати на подовження ліцензії – 1800 гривень.
- Поточні витрати – 1800 + 756,29 = 2556,29 грн.

Поточні витрати на оновлення операційних систем:

- Трудомісткість оновлення становить 4 години.
- Витрати на оновлення ПЗ – 500 + 3,58 = 503,58 грн.
- Витрати на продовження ліцензії – 6089 гривень.
- Поточні витрати – 6089 + 503,58 = 6592,58 грн.

Поточні витрати – 6592,58 + 2556,29 + 18773,48 = 27922,35 грн.

Поточні витрати на керування системою інформаційної безпеки:

$С_к$- вартість на керування системою в цілому, рахується за формулою:

$$С_к = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос}$$

$С_н$ - витрати на навчання адміністративного персоналу і користувачів, проведення тренінгів, становить 3600 грн;

$С_з$- річний фонд заробітної плати інженерно-технічного персоналу, котрий обслуговує систему ІБ, вираховується за формулою:

$$С_з = З_{осн} + З_{дод}, \ 71928 + 9840 = 81768 \text{ грн}$$

де: $З_{осн}$ – основна заробітна плата, складає 19980 грн на місяць, компанія готова брати спеціаліста за 0.3 ставки, тому на рік буде 19980*0.3*12 = 71928 грн.

$З_{дод}$ - додаткова заробітна плата, складає 820 грн на місяць, на рік буде 9840 грн.

ЄСВ становить 22% від фонду заробітної плати тому:

$$С_{єв} = 71928*22\% = 15824,16 \text{ грн}$$

$$С_з = 71928 + 9840 + 15824 = 97592 \text{ грн}$$

$С_{ел}$- це вартість електроенергії, що споживається апаратурою системи ІБ протягом року, вираховується за формулою:

$$С_{ел} = Р*F_р*Ц_е = 5,2*1920*1,68 = 16773,12 \text{ грн}$$

$С_{тос}$ – це витрати на технічне та організаційне адміністрування та сервіс системи ІБ визначаються за даними організації. Або 1% від суми капітальних витрат – 1331.59 грн.

Таким чином, витрати на керування системою інформаційної безпеки становлять:

$С_к = 3600 + 81768 + 16773,12 + 1331,59 = 103472,71$ грн.

Отже поточні річні витрати будуть становити:

$С = 103472,71 + 27922,35 = 131395.06$ грн.

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

Для того щоб розрахувати вартість можливих збитків від атаки на вузол або сегмент корпоративної мережі будемо використовувати наведену нижче модель:

Необхідні вхідні дані для розрахунку:

- $t_п$ — час простою вузла або сегмента корпоративної мережі внаслідок атаки, 5 годин;
- $t_в$ — час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 8 годин;
- $t_{ви}$ — час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 10 годин;
- $З_о$ — заробітна плата обслуговуючого персоналу, 16 000 грн/міс;
- $З_с$ - заробітна плата працівників атакованого вузла або сегмента корпоративної мережі, грн/міс;
- $Ч_о$ — Чисельність обслуговуючого персоналу (адміністраторів та ін.), 6 осіб;

- $Ч_с$ - Чисельність працівників атакованого вузла або сегмента корпоративної мережі, 86 осіб.
- О - обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 500 тис. грн. у рік;
- $П_{зч}$ — вартість заміни встаткування або запасних частин;
- I — число атакованих сегментів корпоративної мережі, 4;
- N — середнє число атак на рік, 2.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

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. Заробітні плати робітників наведені у таблиці 3.4.

Таблиця 3.4 — Заробітні плати працівників товариства

Посада	Кількість працівників	Місячна ЗП	Єдиний соціальний внесок	Витрати на заробітну плату з урахуванням ЄСВ
Програміст	40	25000	1800	1072000
Бізнес-аналітик	5	20000	1780	108900
Проджект-менеджер	5	17000	2320	96600
Фінансовий директор	1	25000	1780	26780
Економіст	7	14000	2450	115150
Бухгалтер	8	13500	2450	127600
Керівник охорони	1	15000	1780	16780
HR	4	16500	1780	73120
Директор компанії	2	36000	1780	75560

Продовження таблиці 3.4 — Заробітні плати працівників товариства

Посада	Кількість працівників	Місячна ЗП	Єдиний соціальний внесок	Витрати на заробітну плату з урахуванням ЄСВ
Керівник юридичного відділу	1	18000	1600	19600
Юрист	6	20000	1870	131220
Керівник технічного відділу	1	18000	1850	19850
Системний адміністратор	4	12000	1560	54240
Охорона	1	10000	1540	11540
Всього				1948940

$$\sum З_С = 1948940 \text{ грн}$$

$$П_П = \frac{\sum З_С}{F} \cdot t_П = \frac{1948940}{160} \cdot 5 = 60904{,}37 \text{ грн},$$

де F — 160 годин, місячний фонд робочого часу.

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

$$П_В = П_{ВИ} + П_{ПВ} + П_{ЗЧ},$$

де $П_{ВИ}$ — витрати на повторне введення інформації, грн.;

$П_{ПВ}$ — витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{ЗЧ}$, — вартість заміни устаткування або запасних частин, 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 $t_{ВИ}$.

$$П_{ВИ} = \frac{\sum З_С}{F} \cdot t_{ВИ} = \frac{60904{,}37}{160} \cdot 10 = 121808{,}75 \text{ грн},$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{ПВ}$ визначаються часом відновлення після атаки $t_В$ і розміром середньо-годинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ПВ} = \frac{\sum З_О \cdot Ч_О}{F} \cdot t_В = \frac{16000 \cdot 6}{160} \cdot 8 = 4800 \text{ грн},$$

$$П_В = 121808{,}75 + 4800 + 0 = 126608{,}75 \text{ грн}$$

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

$$V = \frac{О}{F_Г} \cdot (t_П + t_В + t_{ВИ}) = 500000/1920 \cdot (5 + 8 + 10) = 5989{,}58 \text{ грн},$$

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

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

U = 60904,37 + 126608,75 + 5989,58 = 193502,7 грн,

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

$$B = \sum i \sum n \cdot U = 4 * 2 * 193502,7 = 1548021,6 \text{ грн},$$

3.10 Загальний ефект від впровадження системи інформаційної безпеки

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

E = B * R - C грн,

де B - загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R — вірогідність успішної атаки на вузол або сегмент корпоративної мережі, частки одиниці 43%;

C — щорічні витрати на експлуатацію системи інформаційної безпеки.

E = 1548021,6*0,43 - 131395.06 = 534254,23 грн.

3.11 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:

$$ROSI = \frac{E}{K} = \frac{534254,23}{133159,32} = 4,01 \text{ частки одиниці},$$

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

K — капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

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

$$T_O = \frac{1}{ROSI} = \frac{1}{4,01} = 0,24 \text{ роки}$$

Після розрахунку загального ефекту від впровадження системи інформаційної безпеки, доведено, що її окупність настане менш ніж за чверть року.

3.12 Висновки до 3 розділу

Після проведення розрахунків економічної доцільності запровадження запропонованої комплексної системи безпеки для підприємства “DevUA” можна стверджувати, що запровадження КСЗІ є економічно доцільним, бо її окупність наступить менш, ніж за чверть року (87 днів), а коефіцієнт повернення інвестицій ROSI буде становити 4,01 гривні.

Таким чином можна сказати, що на кожну інвестовану гривню в комплексну систему захисту інформації товариство буде мати 4,01 гривні економічного ефекту, що доказує абсолютно економічну доцільність рішення.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи було наведено загальні відомості щодо ТОВ “DevUA”, обстежено фізичне середовище ІТС, обчислювальна система, інформаційне середовище та середовища користувачів. Було створено модель порушника і модель загроз. Була обґрунтована необхідність створення КСЗІ.

У другому розділі кваліфікаційної роботи було оцінено існуючий стан захищеності, обрано профіль захищеності і визначено рівень гарантій. Були прийняті конкретні проектні рішення для підвищення рівню безпеки ІТС ТОВ “DevUA”, такі як:

- Оновлення існуючого ПЗ на новітнє і більш ефективне.
- Оновлена матриця доступу користувачів ІТС.
- Оновлення розмежувань доступу адміністраторів в ІТС.
- Запровадження DLP-системи для мінімізації ризиків витоків даних.

У третьому розділі кваліфікаційної роботи було оцінено економічну доцільність запровадження комплексної системи захисту інформації для ТОВ “DevUA”. Було доведено абсолютну економічну доцільність запровадження КСЗІ – економічний ефект становить 4,01 гривні.

ПЕРЕЛІК ПОСИЛАНЬ

1. Кібербезпека бізнесу це не лише технічні заходи [Електронний ресурс] – Режим доступу https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/
2. Скільки втрачає бізнес через виток даних? – Звіт IBM 2021 [Електронний ресурс] – Режим доступу https://denovo.ua/blog/vitok-danyh-v-2021-ibm
3. Необхідність створення комплексної системи захисту інформації (КСЗІ) [Електронний ресурс] – Режим доступу https://tzi.com.ua/neobxdnst-stvorennya-kompleksno-sistemi-zaxistu-nformacz-ksz.html
4. НД ТЗІ 3.7-003 -2005 - Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – [Чинний від 08.11.2005] – К. : ДССЗЗІ, 2005. - №125 – (Нормативний документ системи технічного захисту інформації)
5. Закон України “Про інформацію” [Електронний ресурс] – Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12#Text
6. НД ТЗІ 2.5-005 -99 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – [Чинний від 28.04.1999] – К. :ДСТСЗІ СБУ, 2005. - №22 - (Нормативний документ системи технічного захисту інформації).
7. НД ТЗІ 1.6-005-2013 - Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. – [Чинний від 15.04.2013] – К. :АДССЗЗІУ. - №215 – (Нормативний документ системи технічного захисту інформації).
8. НД ТЗІ 1.4-001-2000 - Типове положення про службу захисту інформації в автоматизованій системі. – [Чинний від 4.12.2000] – К. :ДСТСЗІ СБУ, 2000. - №53 – (Нормативний документ системи технічного захисту інформації).

9. Рейтинг Інтернет-загроз: найактивніші шкідливі програми у травні-серпні 2021 [Електронний ресурс] – Режим доступу https://eset.ua/ua/news/view/912/reyting-internet-ugroz-naiboleye-aktivnyye-vredonosnyye-programmy-v-maye-avguste-2021
10. Як обрати DLP-систему [Електронний ресурс] – Режим доступу https://habr.com/ru/post/440838/
11. Оцінка можливого збитку від атаки(злому) [Електронний ресурс] – Режим доступу https://studopedia.net/9_51106_otsInka-mozhlivogo-zbitku-vId-ataki-zlomu.html

ДОДАТКИ

ДОДАТОК А “Акт категоріювання об’єкта”

Гриф обмеження доступу

Прим. № ___

ЗАТВЕРДЖУЮ

Керівник установи-власника
(розпорядника, користувача) об’єкта

__директор_Червонюк Б.А._____

(посада, підпис, ініціали, прізвище)

____. ____. 20___

АКТ

категоріювання _____ТОВ «DevUA»_____

(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 четвертої категорії відносяться об’єкти, в яких циркулює службова та конфіденційна інформація, вимога щодо захисту якої встановлена законом_____

Голова комісії _____ _____

(підпис) (ініціали, прізвище)

Члени комісії: _____ _____

(підпис) (ініціали, прізвище)

____.____. 20___

ДОДАТОК Б “Наказ про створення КСЗІ”

05.05.2022

ТОВ “DevUA”

Н А К А З

01.05. 2022 №17

Про створення комплексної системи захисту інформації в АС 4

Відповідно до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373, **НАКАЗУЮ:**

1. Створити комплексну систему захисту інформації на об'єкті ЕОТ, призначеної для обробки конфіденційної інформації, у головному офісі ТОВ “DevUA”.

2. Призначити відповідального за створення комплексної системи захисту інформації в автоматизованій системі класу 4 та впровадження заходів із захисту інформації товариства та інформації оброблюваної товариством.

3. Контроль за виконанням цього наказу залишаю за собою.

Головний директор ТОВ “DevUA” **Червонюк Б.А.**

ДОДАТОК В Перелік матеріалів на оптичному носії

Жмак Д С _125_18_3_ПЗ.docx

Жмак Д С_125_18_3_ДМ.pptx

Жмак Д С _125_18_3_ПЗ.pdf

Жмак Д С _125_18_3_ПЗ.p7s

ДОДАТОК Г Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	1 Розділ	56	
5	А4	2 Розділ	15	
6	А4	3 Розділ	13	
7	А4	Висновки	1	
8	А4	Перелік джерел	2	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	
13	А4	Додаток Ґ	1	
14	А4	Додаток Д	1	

ДОДАТОК Ґ Відгук керівника економічного розділу

Відгук керівника економічного розділу:

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

Керівник розділу _____ Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Д Відгук керівника кваліфікаційної роботи

В І Д Г У К
на кваліфікаційну роботу студента групи 125-18-3
Жмака Данііла Сергійовича
на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ "DevUA"»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 99 сторінках.

Метою кваліфікаційної роботи є створення комплексної системи захисту інформації для підприємства "DevUA".

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази у сфері забезпечення кібербезпеки; аналіз фізичного та інформаційного середовищ ІТС; вивчення основних деталей функціонування ІТС підприємства.

Розроблені проектні рішення для підвищення рівня безпеки інформації в ІТС ТОВ "DevUA".

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня захисту інформації підприємства за рахунок запровадження розроблених проектних рішень.

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

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

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

Кваліфікаційна робота заслуговує оцінки «90 - Відмінно».

Керівник кваліфікаційної роботи

Керівник спец. розділу