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 *Чемеріса Максима Костянтиновича*

академічної групи *125-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Обгрунтування методів моніторингу та оцінки захищеності інформації в інформаційно-комунікаційній системі підприємства.*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	ас. Олішевський І.Г.			
розділів:				
спеціальний	проф. Гусєв О.Ю.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер				

Дніпро
2023

ЗАТВЕРДЖЕНО:

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

«_____»_____2023 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Чемерісу Максиму Костянтиновичу*** **академічної групи** ***125-19-2***

(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека та захист інформації*

(код і назва спеціальності)

на тему ***Обгрунтування методів моніторингу та оцінки захищеності інформації в інформаційно-комунікаційній системі підприємства***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 № 350-с

Розділ	Зміст	Термін виконання
Розділ 1	ОБСЛІДУВАННЯ ІТС. АНАЛІЗ ЗАГРОЗ	
Розділ 2	СПЕЦІАЛЬНА ЧАСТИНА	
Розділ 3	ЕКОНОМІЧНА ЧАСТИНА	

Завдання видано _____ **Олішевський І.Г.**

(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ **Чемеріс М.К**

(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 83 ст., 8 рис., 17 табл., 6 додатків, 13 джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система ТОВ “Lantechnics”.

Предмет розробки: створення комплексної системи захисту інформації інформаційно-телекомунікаційної системи ТОВ “Lantechnics”.

Мета кваліфікаційної роботи: розробка рішень щодо захисту від загроз інформаційної безпеки в інформаційно-телекомунікаційної системі ТОВ “Lantechnics”.

У першому розділі обгрунтовано необхідність створення КСЗІ, надано загальні відомості про об’єкт, виконаний акт обстеження об’єкту інформаційної діяльності. Визначений перелік джерел загроз, перелік властивостей та перелік актуальних для ІТС загроз.

У другому розділі описано існуючий профіль захищеності та вибраний новий профіль захищеності підприємства. Також були розроблені рішення, щодо захисту підприємства від актуальних загроз.

В третьому розділі були розраховані витрати на впровадження та підтримку заходів, щодо забезпечення інформаційної безпеки підприємства.

Практична значимість роботи полягає у розробці та впровадженні комплексної системи захисту інформації.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ВРАЗЛИВОСТІ, ІНФОРМАЦІЙНА БЕЗПЕКА.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІТС – інформаційно-технічна система;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КС – комп’ютерна система;

КСЗІ – комплексна система захисту інформації;

ОІД – об’єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ТОВ – товариство з обмеженою відповідальністю;

ЗМІСТ

ВСТУП

Розвиток промислового виробництва призвів до появи великої кількості нових знань. Разом з тим виникла необхідність частину таких знань приховувати від конкурентів, захищати їх. Інформація сьогодні стала продуктом і товаром, який можна купувати, продавати, обмінювати. Захистом інформації називають забезпечення неможливості доступу до інформації сторонніх осіб (несанкціонований, нелегальний доступ) та несумисного або недозволеного використання, зміни чи руйнування інформації.

За сучасних умов, особливо під час роботи в мережах, існує постійна небезпека псування або втрати інформації. Захист інформації слід здійснювати в кількох напрямах. По-перше, це захист від випадкових чинників, тобто неправильних дій користувача, виходу з ладу апаратури. По-друге, це захист від злочинних дій, що полягають у розкритті конфіденційності (секретної) інформації, у несанкціонованому доступі до інформаційних ресурсів. Ці завдання виконують служби безпеки, які забезпечують цілісність та надійність даних, контроль доступу до інформації і захист від збоїв апаратури.

Одним із методів забезпечення інформаційної безпеки підприємства є створення комплексної системи захисту інформації (КСЗІ). Комплексна система захисту інформації – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. Організаційні заходи є обов'язковою складовою побудови будь-якої КСЗІ. Інженерно-технічні заходи здійснюються в міру необхідності.

Мета цієї роботи полягає в створенні КСЗІ для того, щоб захистити ІТС від існуючих в ньому загроз. Спочатку відбувається обстеження ІТС, а саме: обстеження фізичного середовища, обчислювальної системи, інформаційного середовища, середовища користувачів. Відбувається аналіз загроз інформації та вразливостей. Пропонується функціональний профіль відповідно до НД

ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» та НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». Потім вказуються організаційні заходи, проектні рішення і модернізація політики безпеки з метою захисту від існуючих в ІТС загроз.

РОЗДІЛ 1. ОБСЛІДУВАННЯ ІТС. АНАЛІЗ ЗАГРОЗ

1.1 Загальні відомості про ІТС

Об’єктом інформаційної діяльності було вибрано товариство з обмеженою відповідальностью **“Lantechnics”.** Lantechnics - один з провідних розробників та постачальників програмного забезпечення в Україні. ІТС знаходиться за адресою: м. Дніпро, вул. Ярослава Мудрого 10, фірма № 5. Будівля, де розташована організація – трьохповерхова.

Графік роботи організації з понеділка по п’ятницю з 8:00 до 16:00. Дві перерви в період з 11:00 до 12:00 та 15:00 до 15:30. При спрацюванні системи сигналізації на виклик приїжджає охоронна фірма “Гуард”.

Організаційна структура наведена на рисунку 1. Підприємство ТОВ «Lantechnics» складається з 9 працівників, а саме:

- Директор;
- Менеджер;
- Системний адміністратор;
- Помічник системного адміністратора;
- Бухгалтер;
- Секретар;
- Системний програміст;
- Веб-програміст;
- Прикладний програміст.

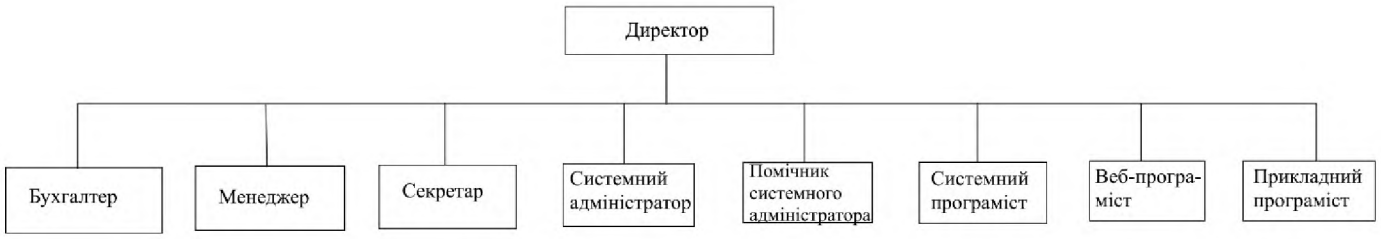


Рисунок 1.1 – Організаційна структура ТОВ «Lantechincs»

1.2 Обгрунтування необхідності створення КСЗІ

Відповідно до чинного законодавства України і вимог окремих нормативних документів Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та Закону України "Про захист персональних даних" обов'язковому захисту інформації підлягає: інформація, що є власністю держави, або інформація з обмеженим доступом, вимоги по захисту якої встановлені законом, в т.ч. персональні дані громадян.

Власник підприємства вирішив створити КСЗІ, тому що в ІТС обробляється інформація з обмеженим доступом, циркулює інформація про клієнтів, робітників, а там присутні персональні дані.

1.3 Обстеження ІТС

Відповідно до НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці», згідно пункту 5.16 «Об’єктам, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, встановлюється четверта (IV) категорія.» Тому ІТС, що розглядається встановлюється четверта категорія, так як на підприємстві циркулює інформація з обмеженим доступом, яка обробляється технічними засобами та не становить державної таємниці.

1.3.1 Обстеження фізичного середовища ІТС.

Бізнес центр знаходиться між такими будівлями: житловий будинок, комерційна будівля, виробнича будівля, житловий будинок, на півночі та півдні присутня автомобільна стоянка. З півночі до автомобільної стоянки проходить грунтова дорога, також на півночі простягається паркан. Бізнес центр, в якому знаходиться об’єкт інформаційної діяльностізбудований з керамічних і газобетонних блоків, має 3 поверха.

Комунікації технічних систем, які підключені до будівлі з об'єктом інформаційної діяльності наступні: системи опалення, водопостачання, електропостачання, пожежної та охоронної сигналізації, комп'ютерної мережі. Ситуаційний план наведено у додатку В.

Задній двір з заходу на північ огорожений міцним і високим парканом. З парадного входу присутня вахта з черговим охоронцем, зайти в будівлю можливо по паперовому пропуску, який необхідно пред'явити охоронцю. У таблиці 1 наведений перелік об'єктів, розташованих навколо будівлі, у якій знаходиться ІТС.

Таблиця 1.1 – Характеристика будівель, що знаходяться поруч з ІТС

№	Назва	Адреса	Відстань до ІТС, м	Кількість поверхів
1	Торговий центр	Вул.Ярослава Мудрого, 15	115 м.	5
2	Комерційна будівля	Вул.Ярослава Мудрого, 20	150 м.	1
3	Бізнес центр	Вул.Ярослава Мудрого, 22	105 м.	6
4	Житловий будинок	Вул.Ярослава Мудрого, 24а	110 м.	1
5	Культова споруда	Вул.Ярослава Мудрого, 25	65 м.	2
6	Торговий центр	Вул.Ярослава Мудрого, 28	67 м.	5
7	Житловий будинок	Вул.Ярослава Мудрого, 32	70 м.	1
8	Адміністративна будівля	Вул.Ярослава Мудрого, 33а	75 м.	1
9	Бізнец центр	Вул.Ярослава Мудрого, 35	60 м.	3
10	Житловий будинок	Вул.Ярослава Мудрого, 37а	60 м.	7
11	Торговий центр	Вул.Ярослава Мудрого, 39	50 м.	6
12	Виробнича будівля	Вул.Ярослава Мудрого 12б	30 м.	4
13	Житловий будинок	Вул.Ярослава Мудрого, 15б	27 м.	4

Продовження таблиці 1.1

14	Торговий центр	Вул.Ярослава Мудрого, 18а	60 м.	6
15	Комерційна будівля	Вул.Ярослава Мудрого, 44	15 м.	1
16	Житловий будинок	Вул.Ярослава Мудрого, 6	14 м.	4
17	Бізнес центр	Вул.Ярослава Мудрого, 10	ІТС	3
18	Виробнича будівля	Вул.Ярослава Мудрого, 13	70 м.	4
19	Торговий центр	Вул.Ярослава Мудрого, 13б	70 м.	5
20	Житловий будинок	Вул.Ярослава Мудрого, 12а	7 м.	5
21	Культова споруда	Вул.Ярослава Мудрого, 48	20 м.	9

ІТС знаходиться в північній стороні бізнес-центра, на другому поверсі. Елементи та лінії технічних систем, які проходять через контрольовану зону, наступні: охоронна та пожежна сигналізація, комп'ютерна мережа, освітлення та електропостачання, опалення (наведено у додатку Г).

За межі КЗ виходять лінії електропостачання, комп'ютерної мережі та опалення. На поверсі присутня електрична щитова, яка в свою чергу підключається до щитової в приміщенні номер три, звідки виходять лінії системи електропостачання та освітлення. З'єднання розеток між собою виконано паралельно.

ІТС складається з 6-х кімнат. Площа офісу – 30 квадратних метрів. Стіни ІТС зроблені з газобетону, товщина стін - 300 мм, міжкімнатні перегородки - 150 мм. Стеля і підлога зроблені з бетону, товщина – 15 см. Висота від підлоги до підвісної стелі – 2,7 м. Підвісна стеля зроблена з алюмінію, товщина рейок – 10 см. 6 міжкімнатних пластикових дверей, на яких встановлена засувка під циліндр. Товщина дверей 80 мм. В приміщення можна потрапити через вхідні

металеві двері, на які встановлений накладний замок товщиною 80 мм. В ІТС шість вікон, як виготовлені з склопластику. Товщина вікна 2,5 см.

1.3.2 Основні та допоміжні технічні засоби

Серед основних технічних засобів виділяються наступні: комп'ютери, принтери, роутер, комутатор, сервер, повний перелік можна оглянути в таблиці №1.2 (додаток Ґ) – відомість основних технічних засобів.

Серед допоміжних технічних засобів слід виділити сповіщувачі диму, розбиття скла, пасивні інфрачервоні сповіщувачі, магнітоконтактні сповіщувачі, клавіатури, мишки. Можна помітити, що сповіщувач розбиття скла не встановлений в приміщенні номер 2 (кабінет директора). Повний перелік наведено в таблиці 1.3 та 1.4 (додаток Ґ).

1.3.3 Обчислювальна система ІТС

На підприємстві використовуються персональні комп'ютери, принтери, комутатор, роутер, сервер. Комп'ютери з'єднуються з роутером через вай-фай адаптер та користувачі мають доступ в інтернет. Характеристика технічних засобів відображена в таблиці 1.5 (додаток Ґ).

Виявлено, що апаратне забезпечення PC №5 та PC №7 є застарілим, та не не відповідає системним вимогам програм, які на ньому використовуються.

Взаємозв'язок між технічніми засобами(комп'ютери, принтери, сервер, комутатор, роутер) вказано на рисунку 1.2.

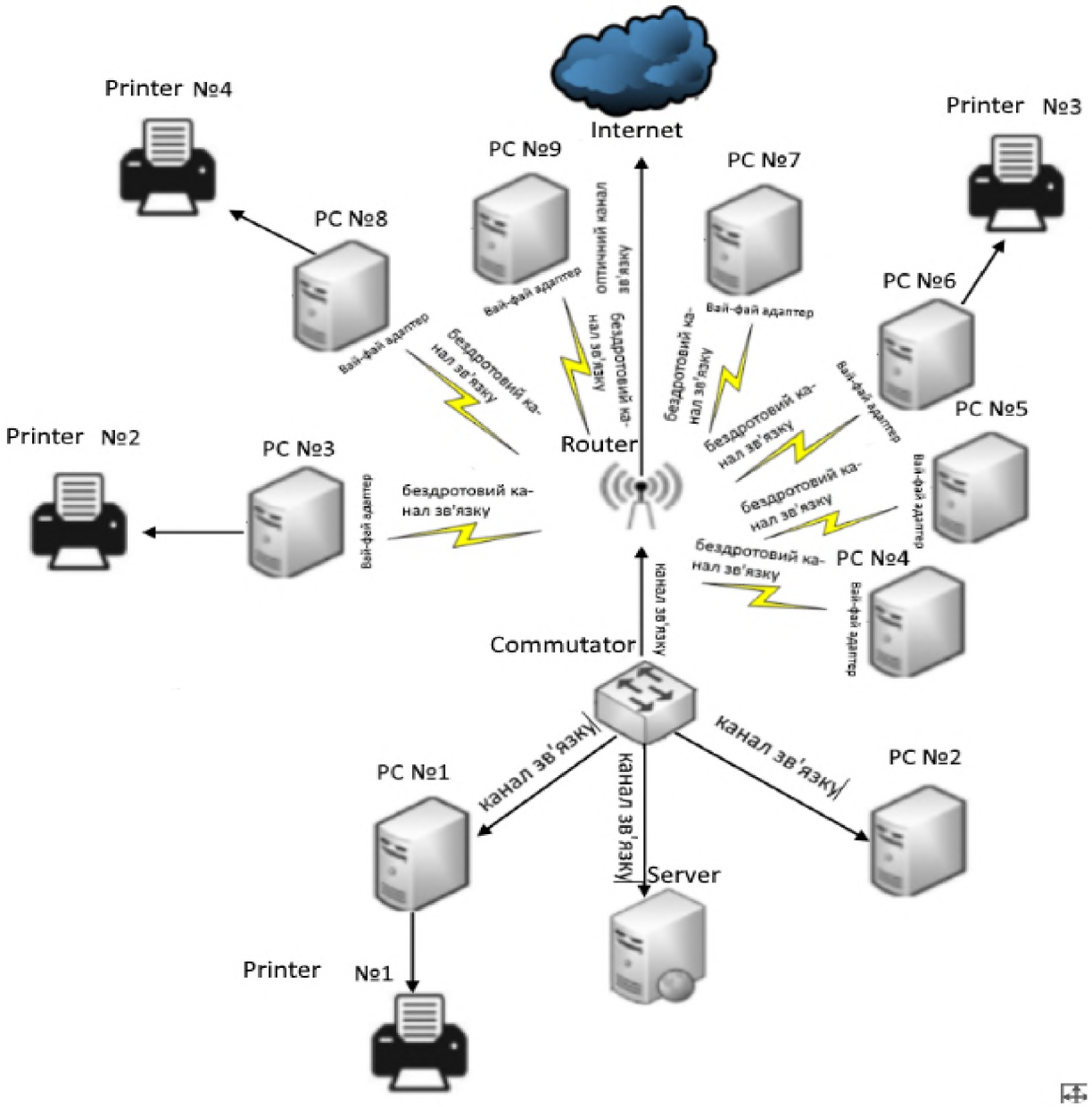


Рисунок 1.2 – схема корпоративної мережі компанії

Програмне забезпечення, яке встановлене на всіх комп'ютерах наведене в таблиці 1.6 (додаток Ґ).

1.3.4 Опис середовища користувачів

Персонал підприємства включає в себе наступних працівників: системного адміністратора, помічник системного адміністратора, бухгалера, директора, програміста, інженера-програміста, прикладного програміста, Секретаря і менеджера.

Системний адміністратор працює за персональним комп'ютером №1 та сервером, використовує принтер №1. Чим займається: підтримує правильну роботу комп'ютерної техніки і програмного забезпечення, а також відповідає за інформаційну безпеку організації. Установлює і обслуговує комп'ютерну та офісну техніку. Забезпечує безпомилкову роботу системного програмного забезпечення. Установлює, налаштовує і оновлює офісне та прикладне ПЗ. Займається налаштуванням сервера

Помічник системного адміністратора працює за персональним комп'ютером №2. Чим займається: підтримує та налаштовує роботу сервера компанії, комп'ютерів співробітників і орг. техніки. Підтримує мережеву інфраструктуру компанії та допомагає в роботі системному адміністратору. Під час обстеження виявлено, що цей співробітник малокваліфікований.

Бухгалтер працює за персональним комп'ютером №3 та використовує принтер №3. Чим займається: документально веде фінансово-господарський облік підприємства, веде фінансову документацію компанії, складає бюджет організації і звітів про доходи та витрати. Також фахівець займається нарахуванням заробітної плати.

Директор працює за персональним комп'ютером №4. Чим займається: керує виробничо-господарською діяльністю компанії. Відповідальний за ефективне використання майна підприємства, за наслідки прийнятих рішень, фінансово-господарські результати діяльності товариства.

Системний програміст працює за персональним комп'ютером №5 та використовує принтер №2. Чим займається: розробляє операційні системи та оболонки для баз даних, а також вирішує інші подібні завдання.

Веб-програміст працює за персональним комп'ютером №6. Чим займається: створює сайти, програми для управління системами сайтів або інтернет-магазинів.

Прикладний програміст працює за персональним комп'ютером №7. Чим займається: створює програмне забезпечення для вирішення різних завдань (редактори, ігри, бухгалтерські програми, CRM-системи).

Секретар працює за персональним комп'ютером №8 та використовує принтер №4. Чим займається: Здійснює контроль за виконанням працівниками підприємства виданих наказів та розпоряджень, Виконує роботу з підготовки засідань і нарад, які проводить керівник, Відповідає на телефонні дзвінки, фіксує і передає службову інформацію керівнику, організовує проведення телефонних переговорів керівника.

Менеджер працює за персональним комп'ютером №9. Чим займається: забезпечує виконання організацією її основного призначення(в більшій частині впровадженні програмного забезпечення), проектує і встановлює взаємодію між окремими операціями і діями, виконуваними в організації.

1.3.5 Інформаційне середовище ІТС

В ІТС присутня інформація про клієнтів, інформація про працівників, результат розробки ПЗ, бухгалтерський звіт, технічна документація до програмного забезпечення та обладнання, реклама готового продукту, накази директора, інформація про замовлення товару.

Результат розробки ПЗ, ця інформація є готовим продуктом. Розроблюють цю інформацію системний програміст, веб-програміст та прикладний програмісти за допомогою персональних комп'ютерів. Зберігається ця

інформація в електронному вигляді на сервері, та в паперовому вигляді на робочому місці директора в шухляді стола, доступ до якого має тільки директор.

Інформація про працівників. Інформація зберігається на сервері в електронному вигляді та в паперовому вигляді в столі директора, оброблюється за допомогою персональних комп'ютерів, зберігається секретарем або директором.

Інформація про клієнтів. Інформація зберігається на сервері та на персональних комп'ютерах, оброблюється за допомогою персональних комп'ютерів , зберігається секретарем, менеджером або директором.

Бухгалтерські звіти. Обробкою цієї інформації займається бухгалтер та окрім нього доступ до неї має директор; бухгалтер та директор може копіювати цю інформацію, а зберіганням займається директор та бухгалтер на своїх персональних комп'ютерах.

Технічна документація до програмного забезпечення та обладнання. Використовують цю інформацію системні адміністратори та директор, зберігається на персональних комп'ютерах та в паперовому вигляді.

Реклама готового продукту. Обробкою цієї інформації займається веб-програміст, відповідальний за коректне донесення менеджер. Розміщається на сайті підприємства. Зберігається на сервері.

Накази директора. Ця інформація є прямим розпорядженням директора, яку отримують всі працівники. Зберігається в електронному та паперовому вигляді на робочих місцях всіх працівників.

Інформація про замовлення товару. Приймає цю інформацію менеджер та доповідає директору. Зберігається директором та менеджером в електронному варіанті на персональних комп'ютерах та сервері.

Режим доступу, правовий режим, рівні захисту інформації більш детально наведено в таблиці 6.

Інформація з обмеженим доступом не озвучується.

На підприємстві відсутній облік зовнішніх носіїв інформації. Тобто, хто завгодно з персоналу може використовувати зовнішні носії інформації для копіювання або завантаження інформації з персональних комп'ютерів.

Таблиця 1.7 – Інформація, що циркулює на об'єкті

№	Назва	Рівень захисту К Ц	Д		Вид представлення	Режим доступу	Правовий режим
1	Результат розробки ПЗ	К4	Д4	Ц4	Електронна, паперова	Обмежений доступ	Конфі-денційна
2	Інформація про клієнтів	К2	Д3	Ц3	Електронна	Відкрита	—
3	Інформація про працівників	К2	Д2	Ц2	Електронна, паперова	Обмежений доступ	Конфі-денційна
4	Технічна документація	К2	Д2	Ц2	Електронна, паперова	Обмежений доступ	Конфі-денційна
5	Бухгалтерські звіти	К1	Д2	Ц2	Електронна	Обмежений доступ	Конфі-денційна
6	Реклама готового продукту	К1	Д2	Ц2	Електронна	Відкрита	—
7	Накази директора	К1	Д2	Ц3	Електронна, паперова	Обмежений доступ	Конфі-денційна
8	Інформація про замовлення товару	К2	Д3	Ц3	Електронна, паперова	Обмежений доступ	Конфі-денційна

Рівні властивостей інформації:

Рівень конфіденційності

К1 – мінімальна конфіденційність. Якщо не буде реалізований цей рівень для інформації, компанія зазнає збитків, якими можна знехтувати у разі втрати конфіденційності інформації.

К2 – базова конфіденційність. Якщо не буде реалізований цей рівень для інформації, компанія зазнає незначних збитків у разі втрати конфіденційності інформації.

К3 – середня конфіденційність. Якщо не буде реалізований цей рівень для інформації, компанія зазнає середніх збитків у разі втрати конфіденційності інформації.

К4 – повна конфіденційність. Якщо не буде реалізований цей рівень для інформації, компанія зазнає максимальних збитків у разі втрати конфіденційності інформації.

Рівні цілісності

Ц1 – мінімальна цілісність. Якщо не буде реалізований цей рівень для інформації, компанія зазнає збитків, якими можна знехтувати у разі втрати цілісності інформації.

Ц2 – базова цілісність. Якщо не буде реалізований цей рівень для інформації, компанія зазнає незначних збитків у разі втрати цілісності інформації.

Ц3 – середня цілісність. Якщо не буде реалізований цей рівень для інформації, компанія зазнає середніх збитків у разі втрати цілісності інформації.

Ц4 – повна цілісність. Якщо не буде реалізований цей рівень, для інформації компанія зазнає максимальних збитків у разі втрати цілісності інформації.

Рівень доступності

Д1 – мінімальна доступність. Якщо не буде реалізований цей рівень для інформації, компанія зазнає збитків, якими можна знехтувати у разі втрати доступності інформації.

Д2 – базова доступність. Якщо не буде реалізований цей рівень для інформації, компанія зазнає незначних збитків у разі втрати доступності інформації.

Д3 – середня доступність. Якщо не буде реалізований цей рівень для інформації, компанія зазнає середніх збитків у разі втрати доступності інформації.

Д4 – повна доступність. Якщо не буде реалізований цей рівень для інформації, компанія зазнає максимальних збитків у разі втрати доступності інформації.

На рисунку 1.3 зображена схема інформаційних потоків.

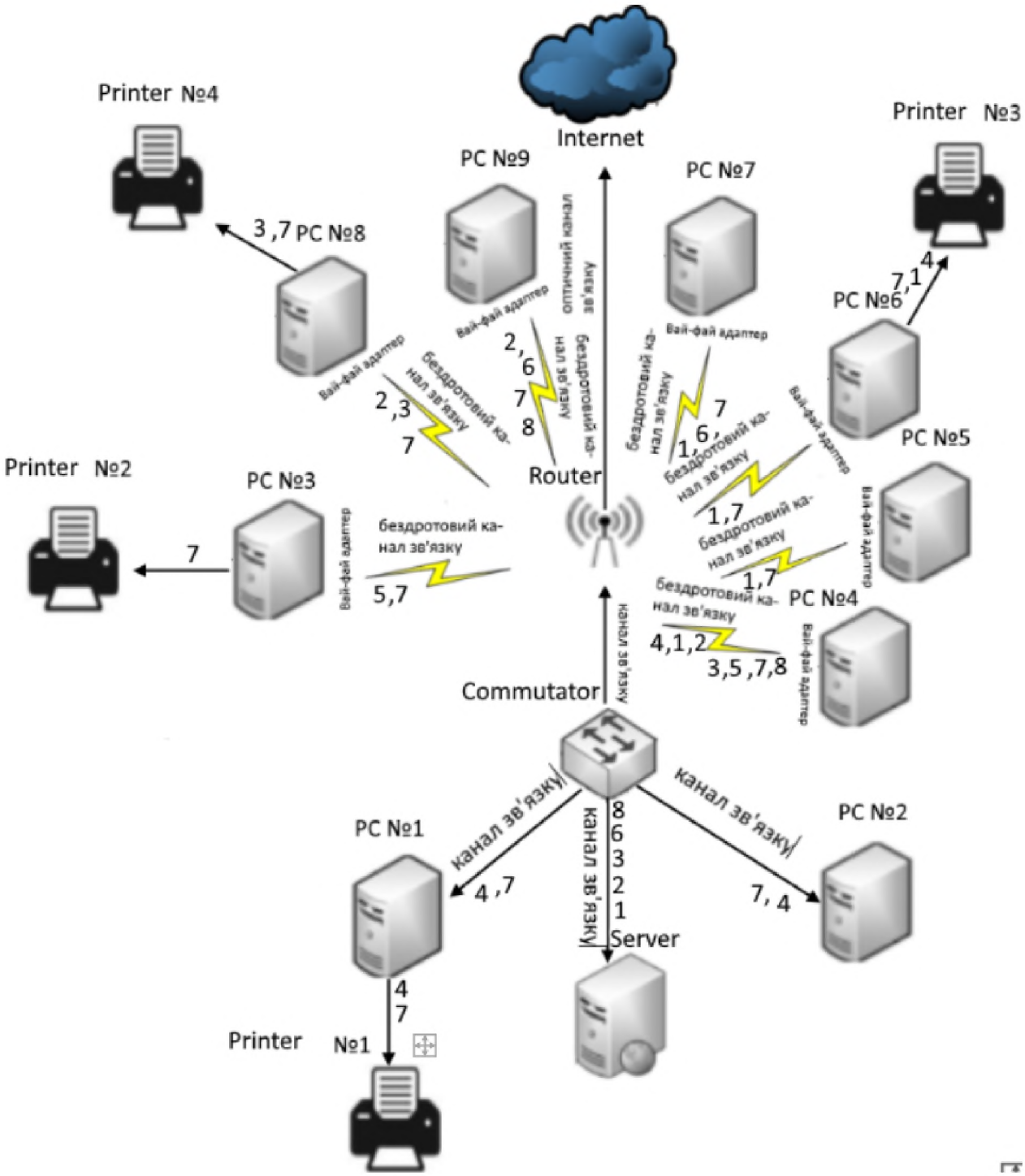


Рисунок 1.3 – Інформаційні потоки на підприємстві

У таблиці 1.8 та 1.9 наведено матриця розмежуваня доступу до інформації в ІТС.

Таблиця 1.8 – матриця розмежування доступу до інформації в ІТС

Користувач	Інформація					Чи може керувати КСЗІ	Рівень кваліфакації	Ресурси
	Результ.розроб. ПО	Інф. Про прац.	Інф. про клієнтів	Бухгалтерські звіти	Технічна документація			
Системний адміністратор	R	R	R	-	R,W,C,S,P,D	+	Вис.-квал.	РС№1
Поміч. систем. адм.	R	R	R	-	R,W,C,S,P,D	-	Мало-кваліф.	РС№2,printer№1
Бухгалтер	-	R,W,C,S,P	R,W,C,S,P	R,W,C,S,P,D	R,S	-	Кваліфіков.	РС№3, printer№3
Директор	R,D,C,S,P	R,W,C,S,P,D	R,W,C,S,P,D	R,C,D,S,P	R,W,C,S,P,D	+	Кваліфіков.	РС№4
Системний програміст	R,W,S,P,D	R	-	-	R,S	-	Вис.-квал.	РС№5, printer№2
Веб-програміст	R,W,S,P,D	R	-	-	R,S	-	Вис.-квал.	РС№6
Прикладний програміст	R,W,S,P,D	R	-	-	R,S	-	Вис.-квал.	РС№7
Секретар	-	R,W,C,S,P	R,W,C,S,P	-	R,S	-	Мало-кваліф.	РС№8, printer№4
Менеджер	R	R	R,W,C,S,P,D	-	R,S	-	Кваліфіков.	РС№9

Таблиця 1.9 – матриця розмежування доступу до інформації в ІТС(2)

Користувач	Інформація			Чи може керувати КСЗІ	Рівень кваліфікації	Ресурси
	Реклама готового продукту	Накази директора	Інформація про замовлення товару			
Системний адміністратор	R,S,C,S	R,S	R	+	Висококваліфіков.	PC№1
Помічник сис. Адміністратора	R,S,C,S	R,S	R	-	Малокваліфіков.	PC№2,printer№1
Бухгалтер	R	R,S	R	-	Кваліфікований	PC№3, printer№3
Директор	R,W,D, C,S, P	R,W,D, C,S, P	R,W,D,C ,S, P	+	Висококваліфіков.	PC№4
Системний програміст	R	R,S	R	-	Висококваліфіков.	PC№5, printer№2
Веб-програміст	R,W,D, C, S, P	R,S	R	-	Висококваліфіков.	PC№6
Прикладний програміст	R	R,S	R	-	Висококваліфіков.	PC№7
Секретар	R,S,C,S	R,S	R	-	Малокваліфіков.	PC№8, printer№4
Менеджер	R,W,D, C, S, P	R,S	R,W,S,C ,P	-	Кваліфікований	PC№9

R – читання;

W – запис;

D – видалення;

C – копіювання;

S – зберігання;

P – друкування;

1.4 Аналіз загроз інформації, що циркулює на ІТС

1.4.1 Аналіз джерел загроз

1.Техногенні:

- Сервер;
- Персональні комп’ютери;
- Неякісне апаратне забезпечення (РС №5 та РС №7);

2. Антропогенні

2.1.Внутрішні:

- Директор;
- Системний адміністратор;
- Помічник системного адміністратора;
- Бухгалтер;
- Системний програміст;
- Прикладний програміст;
- Веб-програміст;
- Менеджер;
- Секретар;

2.2. Зовнішні:

- Конкуренти;
- Злочинці(крадії) ;

3. Стихійні:

- Пожежа;
- Повінь;

Рівні, що були використанні при ранжуванні джерел загроз:

К1 – визначає ступінь доступності до захищаємого об’єкта:

- 1 – антропогенне джерело загроз не має доступу до технічних засобів і програм; об'єкт захисту розташовується на значній відстані від джерел техногенних загроз; на об'єкті відсутні передумови виникнення стихійних джерел загроз.
- 2 – антропогенне джерело загроз має дуже обмежену можливість доступу до технічних засобів і програм; об'єкт захисту розташовується на відстані від джерела техногенних загроз, що виключає можливість його прямого впливу; об'єкт захисту знаходиться поза межами зони дії природних катаклізмів, проте на об'єкті є передумови виникнення стихійних джерел загроз.
- 3 – антропогенне джерело загроз має обмежену можливість доступу до програмних засобів в силу введених обмежень у використанні технічних засобів; техногенні загрози завдають не істотний вплив на об'єкт захисту; об'єкт захисту знаходиться в зоні дії природних катаклізмів, але довгий час не було жодного випадку, проте на об'єкті є передумови виникнення стихійних джерел загроз.
- 4 – антропогенне джерело загроз має можливість опосередкованого доступу до технічних і програмних засобів обробки інформації, що захищається; об'єкти захисту розташовані в безпосередній близькості від джерел техногенних загроз; об'єкт захисту розташований в зоні, в якій багаторічні спостереження вказують на можливість прояву природних катаклізмів.
- 5 – антропогенне джерело загроз має повний доступ до технічних і програмних засобів обробки інформації, що захищається; об'єкти захисту самі містять джерела техногенних загроз; об'єкт захисту розташований в зоні дії природних катаклізмів.

К2 – визначає ступінь кваліфікації і привабливість здійснення діянь для антропогенних джерел; наявність необхідних умов (для техногенних та стихійних джерел):

- 1 – відсутністя можливість будь-якого використання програм, інформація не представляє інтерес для джерела загрози; інформація не представляє інтерес для джерела загрози.
- 2 – обмежується можливістю запуску завдань / програм з фіксованого набору, інформаційні ресурси містять інформацію, яка при її накопиченні і узагальненні протягом певного періоду може завдати шкоди організації; відсутні передумови для реалізації передбачуваної події.
- 3 – враховується можливість створення і запуску користувачем власних програм з новими функціями з обробки інформації, інформаційні ресурси, містять інформацію, розголошення якої може завдати шкоди окремим особам; існують об'єктивні причини на самому об'єкті або в його оточенні, що перешкоджають реалізації загрози.
- 4 – визначається можливість управління функціонуванням мережею, тобто впливом на базове програмне забезпечення, її склад і конфігурацію; захищені інформаційні ресурси містять інформацію, яка може бути використана для отримання вигоди на користь джерела загрози або третіх осіб; умови сприятливі для реалізації загрози, проте довгострокові спостереження не припускають можливості її активізації в період існування і активної діяльності об'єкта захисту;
- 5 – визначається всім обсягом можливостей суб'єктів, які здійснюють проектування і ремонт технічних засобів; інформаційні ресурси містять інформацію, яка може завдати непоправної шкоди і привести до краху організації, що здійснює захист; умови сприятливі або можуть бути сприятливі для реалізації загрози.

КЗ – це ступінь неперебірності наслідків прояви загрози (фатальність):

- 1 – результати прояву загрози не можуть вплинути на діяльність об'єкта захисту.

- 2 – результати прояви загрози можуть призвести до часткового руйнування ІТС, які не потребують великих витрат на його відновлення.
- 3 – результати прояви загрози можуть призвести до часткового руйнування ІТС і до значних витрат на відновлення.
- 4 – результати прояву загрози можуть призвести до середнього руйнування об'єкта і до значних витрат на відновлення.
- 5 – результати прояви загрози можуть призвести до повного руйнування ІТС.

Після того, як джерелам загроз, а точніше їх критерію буде надано оцінка від 1 до 5, вираховується коефіцієнт К(неб) за допомогою формули:

К(неб) =(К1*К2*К3)/125

де 125 максимальне число добутку показників К.

У таблиці 1.10 наведено ранжування загроз.

Таблиця 1.10 – Ранжування загроз

№	Джерело загрози	К1	К2	К3	К(неб)
1	Директор	5	3	3	0,360
2	Системний адміністратор	5	4	3	0,480
3	Помічник системного адміністратора	5	3	3	0,360
4	Менеджер	4	2	2	0,128
5	Веб-програміст	5	3	3	0,360
6	Прикладний програміст	4	3	3	0,288
7	Системний програміст	4	3	3	0,288
8	Бухгалтер	4	2	2	0,128
9	Секретар	4	2	2	0,128
10	Сервер	5	3	3	0,360
11	Персональні комп’ютери	5	3	2	0,240
12	Неякісне апаратне забезпечення	5	3	3	0,360
13	Конкуренти	2	4	5	0,320
14	Злочинці(крадії)	2	4	5	0,320
15	Пожежа	2	2	2	0,064
16	Повінь	2	2	2	0,064

1.4.2 Аналіз вразливостей

Провівши обстеження ІТС, можна сказати, що можливі такі вразливості:

1.Суб'єктивні:

- Порушення режиму інсталяції та завантаження програмного забезпечення(а точніше відсутність)
- Помилкові дії помічника системного адміністратора, в процесі налаштування сервера.
- Відсутня політика реалізації резервного копіювання.
- Неправильне зберігання паперових носіїв інформації.

2.Об'єктивні:

- Недостатній контроль за приміщенням №2(кабінет директора);
- Технічні канали витоку інформації;
- Пряма зона перегляду видимості об'єкту.

3. Випадкові:

- Збій в роботі;
- Пошкодження систем життєзабезпечення.

Рівні, що були використанні при ранжуванні джерел загроз:

К1 – наслідки реалізації угрози, які потім можливо буде усунути:

- 1 – наслідки, якими можна знехтувати;
- 2 – незначні наслідки;
- 3 – середні наслідки;
- 4 – значні наслідки;
- 5 – максимальні наслідки.

К2 – зручність (можливість) використання уразливості джерелом загроз:

- 1 – вразливість неможливо використати або потрібно дуже багато часу та зусиль щоб її реалізувати.

- 2 – потрібні спеціальні умови та обладнання, але її дуже тяжко використати.
- 3 – необхідні спеціальне обладнання та певні умови.
- 4 – порушнику необхідні знання та деяке обладнання, щоб використати цю вразливість.
- 5 – вразливість може використати будь-хто.

К3 – визначає кількість елементів об'єкта, яким характерний та чи інша уразливість:

- 1 – 1 елемент;
- 2 – 3-4 елемента;
- 3 –5-10 елементів;
- 4 –10-15 елементів;
- 5 – більше 15 елементів.

Ранжування поданих вразливостей наведено у таблиці 1.11.

Таблиця 1.11 – Ранжування вразливостей

№	Вразливість	К1	К2	К3	К(неб)
1	Порушення режиму інсталяції та завантаження програмного забезпечення(а точніше відсутність)	4	4	3	0,384
2	Помилкові дії помічника системного адміністратора, в процесі налаштування сервера.	5	4	2	0,320
3	Відсутня політика реалізації резервного копіювання.	4	4	3	0,384
4	Неправильне зберігання паперових носіїв інформації.	4	4	3	0,384
5	Недостатній контроль за приміщенням №2(кабінет директора)	4	5	2	0,320
6	Технічні канали витоку інформації	3	1	2	0,048
7	Пряма зона перегляду видимості об’єкту	1	1	1	0,008
8	Збій в роботі	4	4	3	0,384

9	Пошкодження систем життєзабезпечення	1	1	1	0,008

1.4.3 Аналіз актуальних загроз

Перелік вразливостей:

- В1 – Порушення режиму інсталяції та завантаження програмного забезпечення(а точніше відсутність)
- В2 – Помилкові дії помічника системного адміністратора, в процесі налаштування сервера.
- В3 – Відсутня політика реалізації резервного копіювання.
- В4 – Неправильне зберігання паперових носіїв інформації.
- В5 – Недостатній контроль за приміщенням №2(кабінет директора).
- В6 – Збій в роботі.
- В7 – Пряма зона перегляду видимості об’єкту.
- В8 – Технічні канали витоку інформації.
- В9 – Пошкодження систем життєзабезпечення.

Перелік джерел загроз:

- Д31 – Директор;
- Д32 – Системний адміністратор;
- Д33 – Помічник системного адміністратора;
- Д34 – Веб-програміст;
- Д35 – Сервер;
- Д36 – Персональні комп’ютери;
- Д37 – Неякісне апаратне забезпечення(РС №5,РС№7);
- Д38 – Конкуренти;
- Д39 – Злочинці(крадії);
- Д310 – Менеджер
- Д311 – Прикладний програміст
- Д312 – Системний програміст
- Д313 – Бухгалтер

- Д314 – Секретар
- Д315 – Пожежа
- Д316 – Повінь

Для визначення актуальних загроз були поєднанні актуальні джерела загроз та актуальні вразливості. Коефіцієнт небезпеки було визначено за формулою:

$$К(неб) = К(неб(дж.з.)) * К(неб(вр));$$

У таблиці 1.12 наведено взаємозв'язок вразливостей та джерел загроз.

Таблиця 1.12 – взаємозв'язок вразливостей та джерел загроз

	Вразливості								
Джерела загроз	В1	В2	В3	В4	В5	В6	В7	В8	В9
Д31	0,1382	-		0,1382	-	-	-	-	-
Д32	0,1843	-	-	-	-	-	-	-	-
Д33	0,1382	-	-	-	-	-	-	-	-
Д34	0,1382	-		-	-	-	-	-	
Д35	-	0,1152	0,1382	-	-	-	-	-	
Д36	-	-		-	-	0,092	-	-	
Д37	-	-		-	-	0,1382	-	-	
Д38	-	-		-	-	-	0,002	0,015	
Д39	-	-		-	0,1024		-	-	
Д310	-	-		-	-	--	-	-	
Д311	0,1105	-		-	-	-	-	-	
Д312	0,1105	-		-	-	-	-	-	
Д313	-	-		-	-	-	-	-	
Д314	-	-		-	-	-	-	-	
Д315	-	-		-	-	-	-	-	0,0005
Д316	-	-		-	-	-	-	-	0,0005

Враховуючи пороговий коефіцієнт 0,1, актуальними загрозами можна вважати наступні:

1. На сервері зберігається інформація з обмеженим доступом(та відсутня реалізація резервного копіювання), а в обов'язки помічника системного адміністратора входить налаштування серверу, але цей працівник мало-кваліфікований, то він може допустити помилкові дії при роботі з ним, в той час, коли системний адміністратор не проконтролює ці дії(залишить без нагляду та відійде). Виникає загроза:

- Втрата або пошкодження інформації, із-за помилкових дій при налаштуванні сервера помічником системного адміністратора (В2Д35, В3Д35).

2. Із-за того, що на підприємстві відсутній режим інсталяції та завантаження програмного забезпечення(тобто будь-хто з персоналу може використовувати зовнішні носії інформації для взаємодії з своїм персональним комп'ютером, який знаходиться на робочому місці, то виникає загроза:

- Ураження комп'ютерної системи вірусами (В1Д31, В1Д32).

3. Також із-за цієї вразливості виникає ще одна загроза:

- Несанкціоноване копіювання інформації на зовнішні носії (В1Д33, В1Д34).

4. Із-за недостатнього контроля за приміщенням №2 (кабінет директора) виникає загроза:

- Викрадення або знищення інформації, технічного обладнання в приміщенні №2 (В5Д39).

Це можливо із-за того, що в приміщенні №2 відсутній сповіщувач розбиття скла. порушник міг прокрастися через вікно в неробочий час, та викрасти (знищити) технічне обладнання або інформацію в паперовому вигляді в шухляді стола, або електронному вигляді на персональному комп'ютері.

- 5.Порушення доступності та цілісності інформації на РС №5 та РС№7 (В6Д37).

Це можливо із-за того, що компоненти персонального комп'ютера застарілі та характеристики на відповідають системним вимогам програм, які використовуються на ньому, та й при цьому всьому відсутня реалізація резервного копіювання.

- 6. Втрата паперових носіїв інформації (кабінет директора) (В4Д31).

Це можливо із-за не правильного зберігання паперових носіїв інформації з обмеженим доступом, а саме в шухляді стола.

В таблиці 1.13 наведена класифікація актуальних загроз за їх впливом на властивості інформації.

Таблиця 1.13 – Класифікація актуальних загроз за їх впливом на властивості інформації

№	Актуальна загроза	Властивості інформації, що порушуються		
		К	Ц	Д
1	Втрата або пошкодження інформації, із-за помилкових дій при налаштуванні сервера помічником системного адміністратора	-	+	+
2	Ураження комп'ютерної системи вірусами	-	+	+
3	Несанкціоноване копіювання інформації на зовнішні носії	+	-	-
4	Викрадення або знищення інформації, технічного обладнання в приміщенні №2	+	+	+
5	Порушення доступності та цілісності інформації на РС №5 та РС№7	-	+	+
6	Втрата паперових носіїв інформації(кабінет директора)	+	+	+

1.4.4 Модель порушника

Розглянемо модель порушника. У таблиці 1.14 наведено категорії порушників, які можуть бути.

Таблиця 1.14 – Категорії порушників, визначених у моделі

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

У таблиці 1.15 (додаток Ґ) наведена специфікація моделі порушника.

У таблиці 1.16(додаток Ґ) наведено модель порушника.

У таблиці 1.17 наведено модель внутрішнього порушника

Таблиця 1.17 модель внутрішнього порушника політики безпеки інформації:

Категорія порушника “ПВ”	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Системний адміністратор	ПВ4	М1	К4	З1	Ч4	Д4	17
Помічник сис.адмін.	ПВ4	М1	К2	З1	Ч4	Д3	14
Бухгалтер	ПВ3	М1	К1	З1	Ч3	Д3	10
Директор	ПВ3	М3	К2	З2	Ч3	Д4	16
Системний програміст	ПВ3	М1	К3	З1	Ч3	Д2	12
Веб програміст	ПВ3	М1	К3	З1	Ч3	Д2	12
Прикладний програміст	ПВ3	М1	К3	З1	Ч3	Д2	12
Секретар	ПВ3	М1	К1	З1	Ч3	Д2	10
Менеджер	ПВ3	М1	К1	З1	Ч3	Д3	11

1.5 Висновок

У першому розділі була зібрана наступна інформація:

- Загальні відомості про об’єкт;
- Необхідність створення КСЗІ;

Проведено обстеження ІТС, а саме:

- Фізичне середовища ІТС;
- Обчислювальна система ІТС;
- Середовище користувачів;
- Інформаційне середовище;

На основі отриманих даних були проаналізовані можливі загрози інформації, а саме:

- Джерела загроз;
- Вразливості;
- Актуальні загрози.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Існуючий стан захищеності.

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

«Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС».

Під час обстеження ІТС, було вияснено що ІТС багатокористувачева та розподілена (передача інформації через інтернет), то зроблено висновок, що дана АС відноситься до 3 класу.

Існуючий профіль захищеності:

{НО-1, КД-2, КО-1, ЦД-1, НИ-2,ЦВ-1, НК-1, НТ-2,НЦ-1}

Рекомендований профіль захищеності:

Взято з 3.КЦ.1 та додані послуги, які потрібно реалізувати.

{НО-1, КД-2, КО-1, ЦД-1, ДВ-1,ЦВ-1, НИ-2, НК-1, НЦ-1, НТ-2,НР-2,ЦО-1, КВ-1, ДВ-1, ДР-1}

Відповідно до НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу».

НО-1.Виділення адміністратора.

Ця послуга дозволяє відсікти помилкові дії користувача або адміністратора. Відбувається розподіл окремо на роль адміністратора і звичайного користувача і притаманні їм функції. Ця послуга виконується в системі через вбудовані засоби Windows.

КД-2. Базова довірча конфіденційність.

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

Ця послуга виконується в системі, так як відбувається розмежування доступом на підставі доступу користувача і захищеного об’єкта. В системі всі

користувачі мають свої права доступа до об’єктів та КЗЗ визначає конкретних користувачів або групи користувачів, які мають право одержувати інформацію від об’єкта.

КО-1. Повторне використання об’єктів.

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

Ця умова виконується в системі, так як всі користувачі перед завершенням роботи з ПК, закривають всі програми, процеси. Використовується для цього диспетчер задач або командний рядок.

ЦД-1. Мінімальна довірча цілісність.

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

Ця послуга реалізована, тому що кожний користувач авторизується у своїй системі та працює з тією інформацією, що належить його домену. Користувач може реалізувати обмеження на доступ до об’єктів, що належить його домену з боку інших користувачів.

ДВ-1. Ручне відновлення

«Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування».

Після відмови КС, до нормального функціонування її може повернути тільки адміністратор, або користувачі, які мають відповідні повноваження. Послуга не реалізована. Пропонується реалізація на рівні “Відновлення системи”. Якщо відбувся збій, системний адміністратор повинен запускати комп’ютерну систему в захищеному режимі та використовувати функцію відновлення системи.

НИ-2. Одиночна ідентифікація і автентифікація

«Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача (фізичної особи), який намагається одержати доступ до КС».

Послуга реалізована. Перед тим, як розпочати роботу з ПК всі користувачі здійснюють вхід в свій обліковий запис, шляхом введення логіна та пароля.

НК-1. Однонаправлений достовірний канал

«Дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається)».

Ця послуга реалізована, так як в процесі входу в обліковий запис відбувається перевірка пароля, що набирається із клавіатури. Потрібно для того, щоб КЗЗ зрозумів, що це користувач.

ЦВ-1. Мінімальна цілісність при обміні.

Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Реалізується за допомогою використання протоколу електронної пошти.

НЦ-1. КЗЗ з контролем цілісності.

Політика цілісності КЗЗ визначає склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ. Послуга реалізована, в системі існують програми для перевірки цілісності файлів, такі як Exat file.

НТ-2. Самотестування при старті

«Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС».

Ця послуга реалізована, так як при старті системи є звернення до апаратної частини, до жорсткого диска, перевірка цілісності.

НР-2. Захищений журнал

Реєстрація дозволяє контролювати небезпечні для КС дії. Журнал реєстрації повинен містити інформацію про кожну зареєстровані подію, також журнал повинен визначати хто саме з користувачів активує ту чи іншу дію.

Журнал повинен контролювати системний адміністратор або відповідальний за інформаційну безпеку підприємства.

Послуга не реалізована, далі в КСЗІ описана реалізація.

ЦО-1. Обмежений відкат

«Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути захищений об'єкт до попереднього стану».

Якщо відбувається збій програмного або апаратного забезпечення, або користувачі допускають помилку, ця послуга гарантує відновлення захищеного об’єкту до попереднього стану. Далі Пропонується реалізація цієї послуги з-за допомогою політики резервного копіювання.

КВ-1. Мінімальна 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».

Ця послуга не застосована, але так як на підприємстві використовують електронну пошту для передачі інформації незахищене середовище, то далі пропонується використання протоколу TLS для відправлення пошти.

ДР-1. Квоти

Ця послуга дозволяє користувачам керувати використання послуг і ресурсів. Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу. Не реалізована, необхідно реалізувати за допомогою засобів Active Directory.

2.2 Створення комплексної системи захисту інформації

Комплексна система захисту інформації(КСЗІ) являє собою сукупність організаційних і технічних заходів, апаратних і програмних засобів, які забезпечують захист інформації в інформаційно-телекомунікаційних системах: на автономних робочих станціях і в комп’ютерних мережах. Головною метою створення КСЗІ є досягнення максимальної ефективності

захисту за рахунок одночасного використання всіх необхідних ресурсів, методів і засобів, що виключають несанкціонований доступ до інформації, та створення умов обробки інформації відповідно до чинних нормативно-правових актів України у сфері захисту інформації: Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації» та «Про захист персональних даних».

Відповідно до НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»:

«Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. » Для даної ІТС була створена політика безпеки інформації, яка описана далі. Також було запропоновані організаційні та проектні рішення, щодо забезпеченню захисту інформації.

Враховано те, що усунення вразливостей приведе до мінімізації появи загрози, тому

1.Загроза викрадення або знищення інформації, технічного обладнання в приміщенні №2 вирішується на організаційному рівні, а саме:

— посилення контролю за кабінетом директора.

Відсутність сповіщувача розбиття скла, дає можливість зловмиснику(крадію) в не робочий раз прокрастися в приміщення №2 через вікно, та викрасти:

- Інформацію з обмеженим доступом;
- Технічне обладнання, а саме персональний комп’ютер.

Щоб запобігти цьому, було прийняте рішення:

1) Керівництво “Lantechnics” повинно придбати сповіщувач розбиття скла Astra (IO-329-5);

2) Встановити сповіщувач на вікно з правого боку в приміщенні №2.

Ці дії мінімізують появу загрози викрадення інформації з обмеженим доступом,технічного обладнання шляхом проникнення крадіїв в приміщення №2 через вікно. В тому випадку, якщо вікно розіб'ють, спрацює сигналізація, та група бистрого реагування прибуде на виклик. Це дозволить запобігти крадіжки інформації , якщо охорона вчасно знешкодить порушника.

2. Загроза несанкціонованого копіювання інформації на зовнішні носії вирішується створенням політики обліку зовнішніх носіїв інформації.

Політика обліку зовнішніх носіїв інформації.

Мета політики: створення обліку зовнішніх носіїв інформації, для того, щоб запобігти загрозу несанкціонованого копіювання інформації на зовнішні носії співробітниками підприємства.

Область застосування: політика застосовується для всіх працівників підприємства "Lantechnics".

Зміст політики:

— Працівникам підприємства дозволяється використовувати знімні носії інформації, які стоять на обліку, використання всіх інших знімних пристроїв необхідно заборонити. Обліком зовнішніх носіїв займається системний адміністратор. Кожному співробітнику "Lantechnics" видають по одному USB-накопичувачі.
— Вранці працівники отримують свій зовнішній носій, а в кінці робочого дня повертають. Факт видачі та повернення фіксує системний адміністратор в електронній таблиці або спеціальному журналі, де вказано який саме працівник отримав та повернув носій(посада, прізвище, час).
— Зовнішній носій потрібно використовувати тільки для своїх прямих обов'язків. Забороняється зберігати, копіювати інформацію, яка не стосується області розробки ТОВ "Lantechnics".

— Для зберігання зовнішніх носіїв необхідні придбати сейф, наприклад ВС-15К. Сейф потрібно встановити в приміщенні №4. Відповідальним за зберігання зовнішніх носіїв призначити системного адміністратора.
— Для фізичної реалізації цієї політики, системний адміністратор повинен використовувати технологію Active Directory. Для цього потрібно виконати наступні дії: зайти в розділ GPO, конфігурація комп'ютера, адміністративні шаблони, система, доступ до знімних запам'ятовуючих пристроїв та прописати відповідний код зовнішнього носія(що дозволений відповідно до цієї політики, який використовує той чи інший працівник на цьому комп'ютері). Завдяки цьому. при підключенні зовнішнього незареєстрованого носія відбудеться його блокування.

3. Загроза порушення доступності та цілісності інформації на РС №5 та РС№7.

Технічне обладнання в РС №5 та РС №7 є застарілим, та не відповідає вимогам програм, які використовуються на ньому. За персональним комп'ютером №5 працює системний програміст, а за №7 прикладний програміст, всі вони беруть участь в розробці ПЗ, а саме інформації про готовий продукт з обмеженим доступом, їх праця є особливо важливою для ТОВ "Lantechnics", виходячи з цього не потрібно допустити, щоб їхні персональні комп'ютери дали збій. Прийнято рішення оновити апаратне забезпечення РС №5 та РС№7, для цього потрібно замовити:

— Процесор – 2 одиниці (наприклад Intel Core i5-9600K);
— оперативну пам'ять –2 одиниці (наприклад TEAM Elite Plus Red 8 GB);
— Відеокарта –2 одиниці (наприклад PALIT GeForce GTX 1660 Ti);
— твердотільний накопичувач –2 одиниці (SSD APACER AS510S Pro II 256GB).

Складанням персональних комп'ютерів повинен зайнятися системний адміністратор зі своїм помічником. Материнську плату, блок живлення, корпус використовувати ті самі.

4. Для усунення загрози ураження системи комп'ютерними вірусами потрібно дотримуватися політики облік зовнішніх носіїв інформації та створити політику антивірусного захисту.

Політика антивірусного захисту.

Мета політики: захист комп'ютерних системи від розповсюдження шкідливого програмного забезпечення.

Область застосування: політика застосовується для всіх працівників підприємства "Lantechnics".

Зміст політики:

— На всіх персональних комп'ютерах установлене не ліцензійне антивірусне програмне забезпечення, а саме 360 total security. Потрібно використовувати антивірус, який має експертний висновок про відповідність до вимог технічного захисту інформації, що вказано на сайті державної служби спеціального зв'язку та захисту інформації України.
— Керівництво ТОВ "Lantechincs" потрібно придбати програмний продукт антивірусного захисту ESET Endpoint Antivirus для Windows (EEA) версії 7, так як він має позитивний експертний висновок до 12.07.2022 року.

Інструкції системному адміністратору:

— Системний адміністратор повинен установити нове антивірусне програмне забезпечення на всіх персональних комп'ютерах, які використовуються персоналом.
— Займатися оновленням антивірусного програмного забезпечення, як тільки виходять нові версії цього продукту.
— Обмежити доступ користувачів для налаштування антивірусних компонентів ESET Endpoint.
— Завжди вирішувати проблеми, які пов'язані з комп'ютерними вірусами в кожного співробітника.

— Запланувати централізоване сканування робочих станцій в неробочий час (досить раз в тиждень ввечері).

Інструкції всім іншим користувачам:

— Не відкривати підозрілі сайти;

— Не відкривати вкладення до повідомлень електронної пошти, отримане від невідомих джерел. Такі вкладення повинні відразу видалятися.

— Сканувати носії інформації на наявність вірусів.

5. Співробітники використовують електронну пошту для передачі інформації з обмеженим доступом між собою. Наприклад, менеджер може відправляти веб програмісту свої пропозиції з приводу реклами товару, системний програміст та прикладний програміст взаємодіють між собою з приводу розробки програмного забезпечення. Для цього вони використовують знімні носії та електрону пошту.

Політика електронної пошти

Мета політики: надати інструкції правильного користування електронною поштою та забезпечити захист об’єктів від несанкціонованого ознайомлення під час експорту/імпорту повідомлень електронною поштою.

Область дії: політика застосовується для всіх працівників підприємства “Lantechnics”.

Зміст політики:

Для того, щоб забезпечити неможливість несанкціонованого ознайомлення з повідомленнями, які передаються електронною поштою необхідно шифрувати повідомлення. Наприклад, цього можна досягти завдяки використання пошти Gmail, адже там за замовчуванням використовується протокол TLS.

TLS - це протокол, який забезпечує шифрування електронної пошти для її захисту. Щоб з'єднання було безпечним, протокол TLS повинні використовувати як відправник, так і одержувач пошти.

Інструкції користувачам:

— При відправці повідомлень електронною поштою використовувати Gmail.
— Забороняється використовувати електронну пошту Gmail для своїх особистих цілей, які не пов’язані зі своїми обов’язками та бізнесом підприємства.
— Не відкривати вкладення електронної пошти Gmail. Навіть якщо лист прийшов від знайомого джерела і в кінці листа присутній напис «Повідомлення не містить вірусів. Перевірено антивірусом» або щось подібне, це не дає гарантій, що лист не містить вірус. Цей лист міг відправити вірус, який потрапив комп'ютер цього провіреного джерела. Всі вкладення, які приходять по електронній пошті необхідно спочатку зберегти на жорсткий диск, перевірити антивірусом і, переконавшись у безпеці, відкривати отриманий файл.
— Не дозволяється використовувати робочу пошту Gmail для реєстрації на сайтах, які не пов’язані з бізнесом підприємства.

6. Загроза втрати паперових носіїв інформації можлива через не правильне зберігання документів, а саме в шухляді стола. Звичайно при такому розкладі, документи дуже легко загубляться. Щоб такого не сталося, потрібно:

1) Придбати сейф(наприклад, FEROCON БС-15К.7035);

2)Встановити сейф у кабінеті директора(приміщення №2).

Відповідальним за зберігання документів призначити директора. Заборонити зберігання документів, на яких надрукована інформація з обмеженим доступом в шухлядах стола, на робочому місці. Всі ці документи, повинні бути в сейфі, відсортовані.

В кінці робочого дня всі працівники повинні здати паперові носії інформації з обмеженим доступом секретарю, той в свою чергу під наглядом директора, складає їх в сейф по відділах до яких вони відносяться.

Забороняється виносити документи з інформацією з обмеженим доступом за межі підприємства, якщо попередньо не домовитися з директором.

7. Політика резервного копіювання

Мета політики: для запобігання втрати інформації з обмеженим доступом внаслідок збою програмного, апаратного забезпечення або помилок персоналу, необхідно створити політику реалізації програмного забезпечення.

Область дії: резервне копіювання поширюється на важливу інформацію з обмеженим доступом(наприклад: результат розробки ПЗ, інформація про замовлення товару).

Зміст політики: для реалізації політики резервного копіювання необхідно придбати зовнішні usb накопичувачі, наприклад дві одиниці Transcend StoreJet 25M3S 500GB. Копії будуть зберігатися на двох носіях, це підвищує безпеку інформації.

Відповідальним за резервне копіювання назначити системного адміністратора. Рекомендується використовувати засоби active directory або програму Handy backup(30 днів безкоштовно, потім потрібно придбати ліцензію).

Резервне копіювання необхідно проводити двічі на тиждень або після оновлення інформації. Пріоритет для резервного копіювання має інформація з обмеженим доступом, яка є критичною для підприємства, тобто та, збитки від якої є великі. Після цього резервне копіювання реалізується для всієї іншої інформації з обмеженим доступом.

Якщо відбувся збій в персональному комп'ютері потрібно запустити вбудоване відновлення системи. Для перевірки стану жорстких дисків використовувати програмне забезпечення "Viktoria".

8. Політика контролю за діями користувачів

Мета політики: політика призначена для відстеження дій користувачів і системних подій

Область застосування: політика поширюється на системного адміністратора.

Зміст політики: для відстеження дій користувачів і системних подій необхідно застосувати засоби active directory. Відповідальний за це системний адміністратор.

Інструкції для системного адміністратора:

— Системний адміністратор повинен фіксувати дії користувачів, такі як успішні і невдалі входи в систему.
— Системний адміністратор повинен проглядати накази директора для кожного користувача. В журналі аудиту можливо слідкувати за діями типу "успіх" і / або "відмова". Тобто для кожного співробітника ставиться своє завдання і фіксується системним адміністратором в журналі, коли користувач успішно завершить своє завдання, в журналі створиться відповідний запис "успіх".
— Необхідно переглянути розмежування доступу, щоб кожний співробітник мав доступ до тієї інформації, яку необхідно обробляти відповідно до його обов’язків. Для цього потрібно створити події при доступі до певних об'єктів з включеним аудитом (наприклад, відкриття, читання і т.д.)
— Необхідно добавити теки в яких обробляється інформація з обмеженим доступом до журналу аудиту. Якщо користувач захоче видалити цю папку, створиться відповідний запис.
— Про всі небажані дії користувачів необхідно відразу доповісти директору.

9. Загроза втрати або пошкодження інформації, із-за помилкових дій при налаштуванні сервера помічником системного адміністратора вирішується наступними діями:

— Так як помічник системного адміністратора малокваліфікований то цю людину необхідно відправити на курси підвищення кваліфікації, наприклад – тематичні семінари. Обсяг занять від 72 до 100 годин. Якщо в день займатися по 5 годин, то за 2 тижня ці курси будуть пройдені.

— Після того, як помічник повернеться, системний адміністратор повинен перевірити якість отриманого знання в усній та практичній формі та доповісти про результат директору.
— Потім потрібно тимчасово (2 тижня) допустити помічника до роботи з сервером в супроводі системним адміністратором для контролювання його дій.
— Якщо помічник допустить помилки при налаштуванні, необхідно переглянути його обов'язки та обмежити доступ помічника системного адміністратора від сервера.

2.3 Висновок

В другому розділі було проаналізовано існуючий функціональний профіль захищеності та обрані додаткові критерії захищеності, необхідні для підвищення інформаційної безпеки. Здійснено розробку наступних організаційних та проектних рішень: заміна комплектуючих для персональних комп'ютерів, купівля сповіщувача розбиття скла, двох сейфів, підвищення кваліфікації для помічника системного адміністратора.

Створені розділи політики безпеки, а саме: облік зовнішніх носіїв інформації, резервне копіювання, антивірусний захист,політика електронної пошти, контроль за діями користувачів.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Метою розрахунків є економічне обґрунтування доцільності впровадження комплексної системи захисту інформації. Щоб з'ясувати це, необхідно визначити розмір капітальних та експлуатаційних витрат на заходи і засоби інформаційної безпеки, вірогідні втрати від реалізації загроз інформації, визначити величину відвернених втрат, та на основі цього, розрахувати термін окупності капітальних інвестицій та коефіцієнт повернення інвестицій.

3.1 Розрахунок капітальних витрат

Капітальні витрати – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

За методикою Gartner Group до фіксованих (капітальних) варто відносити наступні витрати:

– вартість розробки проекту інформаційної;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– витрати на первісні закупівлі апаратного забезпечення;

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання, програмного забезпечення та налагодження системи інформаційної безпеки);

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Розрахунок вартості розробки КСЗІ здійснюється з використанням двох показників – трудомісткості розробки КСЗІ і витрат на її розробку.

Трудомісткість буде розраховуватися за формулою:

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

де $t_{тз}$ – тривалість складання технічного завдання на розробку КСЗІ складає 12 год.;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації складає 15 год.;

ta – тривалість процесу аналізу ризиків 5 год.;

tвз – тривалість визначення вимог до заходів, методів та засобів захисту 5 год.;

tозб – тривалість вибору основних рішень з забезпечення безпеки інформації 5 год.;

tовр – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації 11 год.;

tд – тривалість документального оформлення політики безпеки 7 год.

$$t = 12+15+5+5+5+11+7 = 60 \text{ годин}$$

3.2 Розрахунок витрат на створення елементів КСЗІ

Витрати на розробку елементів КСЗІ

Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки КСЗІ З мч:

$$Крп = Ззп + Змч; \quad (3.2)$$

$$Крп = 9360 + 156 = 9516 \text{ грн.};$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) і визначається за формулою:

$$Ззп = t * Зіб \text{ грн.}; \quad (3.3)$$

$$Ззп = 60 * 156 = 9360 \text{ грн};$$

де t - загальна тривалість розробки політики безпеки, годин;

Зіб - средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

60 - годин на розробку елементів КСЗІ;

156 - заробітна плата грн/годину;

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

$$Змч = t * Смч, \text{ грн.} \quad (3.4)$$

Змч = 60 * 2,6 = 156 грн.

де t - трудомісткість розробки КСЗІ на ПК, годин;

Смч - вартість 1 години машинного часу ПК, грн./година.

Смч = Р * tнал * Се + (Фзал * На)/Fр + (Клпз * Напз)/Fр, грн. (3.5)

Смч =0,5 * 1 * 1,68 +(20*0,4)/2112 + (5000*0,5)/2112= 2,6 грн/год.,

де Р - встановлена потужність ПК, кВт; Р – 0,5 кВт

tнал – кількість задіяних роб.станцій при створенні КСЗІ; tнал – 1;

Се – тариф на електричну енергію, грн/кВт година; Се – 1,68 грн/кВт год;

Фзал – залишкова вартість ПК на поточний рік, грн.; Фзал – 20 грн;

На – річна норма амортизації на ПК, частки одиниці; На – 0,4;

Напз – річна норма амортизації на ліцензійне програмне забезпечення,частки одиниці; Напз – 0,5;

Клпз – вартість ліцензійного програмного забезпечення, грн.; Клпз – 5000 грн

Fр – річний фонд робочого часу (за 40-годинного робочого тижня Fр = 2112).

3.3 Капітальні (фіксовані) витрати.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

К = Кпр + Кзпз + Кпз + Каз + Кнавч + Кн, (3.6)

К = 6300+6728+36353+1000 = 50381 тис. грн.

де Кпр – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн; сторонні організації не залучалися, коефіцієнт не враховано.

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис.грн; необхідно придбати ESET Endpoint Antivirus для 9 ПК. Ціна однієї ліцензії 700 грн, 700 * 9 = 6300 грн.

Крп – вартість розробки політики безпеки інформації,тис. грн; – 6 728 грн.

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів,тис. грн; сповіщувач розбиття скла Astra (IO-329-5) – 233 грн. Intel Core i5-9600K(2 одиниці) – 14 000 грн. TEAM Elite Plus Red 8 GB(2 одиниці) – 2000 грн. PALIT GeForce GTX 1660 Ti(2 одиниці) – 16 000 грн. SSD APACER AS510S Pro II 256GB(2 одиниці) – 3 000 грн. Сейф FEROCON БС-15К.7035 – 560 грн. Сейф ВС-15К – 560 грн.

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн; курси підвищення кваліфікації для помічника системного адміністратора – 1000 грн.

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн. Не враховано.

3.4 Розрахунок експлуатаційних витрат

Експлуатаційні витрати - це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі. Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = Св + Ск + Сак, \text{ тис. грн.}, \quad (3.7)$$

$$С = 129552 + 6300 = 135852 \text{ грн.},$$

Де Св – upgrade-відновлення системи інформаційної безпеки;оновлюється ПЗ ESET Endpoint Antivirus для 9 пк, ціна однієї ліцензії 700 грн, тому

Св = 9 * 700 = 6300 грн.

Сак - витрати, викликані активністю користувачів системи інформаційної безпеки;Сак – 0 грн.

Ск - витрати на керування системою в цілому, складають:

$$Ск = Сн + Са + Сз + Сєв + Сел + Со + Стос, \text{ грн}, \quad (3.8)$$

$$Ск = 1000+10150+490+79200+17424+21288= 129552 \text{ грн},$$

де Сн – витрати на навчання адміністративного персоналу й кінцевих користувачів; Сн – 1000 грн;

$$Са=6300/2+14000/5+16000/5+2000/5+3000/5=10150.$$

Со – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування; Со – 0 грн;

Стос – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки, визначається у відсотках від вартості капітальних витрат (1-3%); Стос – 490 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, складає:

$$Сз = Зосн + Здод, грн., \quad (3.9)$$

$$Сз = 6000*12 + 600*12 = 79200 грн.,$$

Де Зосн, Здод – основна і додаткова заробітна плата відповідно, грн. на рік.

$$Сєв = 79200*0,22 = 17424;$$

Зосн – 6000 грн на місяць, Здод – 10 відсотків від Зосн, тому Здод – 600 грн.

Сел – вартість електроенергії, визначається

$$Сел = Р * Fр * Це, грн.; \quad (3.10)$$

$$Сел = 6 * 2112 * 1,68 = 21288 грн.$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;(Р = 6 кВт)

Fр – річний фонд робочого часу системи інформаційної безпеки; (Fр = 2112 год.)

Це – тариф на електроенергію, грн/кВт*годин; (Це = 1,68 грн/кВт за год.)

3.5 Оцінка величини збитку

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

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

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

– порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);

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

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = Пп + Пв + V, \quad (3.11)$$

$$U = 500+19318+18560 = 38378 \text{ грн.}$$

Де Пп - оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн; Пп – 500грн.;

Пв - вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн; Пв – 19318 грн.;

V - втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн. V – 18560 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:

$$Пп = (\Sigma Зс/F)*tп, \text{ грн.}, \quad (3.12)$$

$$Пп = (11000/176)*8 = 500,$$

де Зс – загальна кількість витрат на заробітну плату співробітників за місяць, Зс – 11000 грн;

F – місячний фонд робочого часу, F – 176 год.;

tп – час простою внаслідок атак, tп – 8 год.

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

$$Пв = Пви + Ппв + Пзч, \quad (3.13)$$

де Пви – витрати на повторне уведення інформації, грн.;

Ппв – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

Пзч – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу тви:

$$Пви = (ΣЗс/F)*тви, \quad (3.14)$$

$$Пви = (11000/176)*20 = 1250 грн.;$$

Витрати на відновлення вузла або сегмента корпоративної мережі Ппв визначаються часом відновлення після атаки тв і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$Ппв = (ΣЗо/F)*тв \quad (3.15)$$

де Зо = заробітна плата системного адміністратора, 6000 грн на місяць;

F – місячний фонд робочого часу (при 40–а годинному робочому тижні становить 176 ч.);

тв = 20 годин повторного введення загубленої інформації унаслідок атаки;

$$Ппв =(6000/176)*20 = 681 грн;$$

Пзч – вартість заміни устаткування або запасних частин складає 17000 грн.

$$Пв = 1250 + 681 + 17000 = 18931 грн.;$$

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

$$V = (O/Fr)*(tп +тв+тви), \quad (3.16)$$

$$V= (60000/2112)*(8+20+20) = 18560 грн.;$$

де О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, О – 600000 грн у рік;

Fг – річний фонд часу роботи організації; Fr – 2112 год.

tп – час простою вузла унаслідок атаки; tп – 8 год.;

тви = час відновлення після атаки персонало, що обслуговує корпоративну мережу; тви – 24 год.;

tв = час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі; tв – 24 год.

Таким чином, загальний збиток від атаки складе:

$$B= \Sigma i \, \Sigma n*U, \quad (3.17)$$

$$B=4*3*38378= 460536 \text{ грн.}$$

де і – кількість атакованих вузлів; і – 5;

n – кількість прогнозованих атак на рік; n – 5 ;

3.6 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B * R - C \quad (3.18)$$

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

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

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

$$E= 460536*0,5 – 135852 = 94416 \text{ грн.};$$

3.7 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

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

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

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн. Коефіцієнт повернення інвестицій ROSI:

$$ROSI = 94416/50381=1,87$$

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

$$To = K/E = 1/ROSI = 1/1,87 = 0,53 = 193 \text{ днів.}$$

3.8 Висновок

Згідно з отриманими даними під час розрахунку економічної частини капітальні затрати становлять 50381 грн, експлуатаційні - 135852 грн. Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації склав 460536 грн. Загальний ефект від впровадження системи інформаційної безпеки склав 94416грн. Згідно с коефіцієнтом ROSI який становить 1,87 - створені елементи політики безпеки є цілком доцільними. Термін окупності елементів політики безпеки становить 193 робочих днів.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було виконано обстеження об'єкта інформаційної діяльності відповідно до НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційнотелекомунікаційній системі», обґрунтовано необхідність створення КСЗІ для підприємства "Lantechnics". На підставі зібраних даних була розроблена модель загроз, модель порушника, вразливості, та визначені актуальні загрози.

Профіль захищеності було вибрано відповідно до НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» та НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». З метою захисту від загроз інформаційній безпеці підприємств були розробленні організаційні та проектні рішення, такі як: заміна комплектуючих для персональних комп'ютерів, купівля сповіщувача розбиття скла, двох сейфів, підвищення кваліфікації для помічника системного адміністратора.

Були розроблені розділи політики безпеки, а саме: облік зовнішніх носіїв інформації, резервне копіювання, антивірусний захист,політика електронної пошти, контроль за діями користувачів. Доцільність використання даних рішень було обґрунтовано у економічній частині кваліфікаційної роботи.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».
2. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».
3. 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».
4. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».
5. НД ТЗІ 3.7-001-99 « Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі».
6. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».
7. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».
8. НД ТЗІ 1.1-005-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення».
9. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
10. Закон України «Про інформацію».
11. Закон України «Про захист персональних даних».
12. Закон України «Про державну таємницю».
13. Закон України «Про доступ до публічної інформації».

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ ДИПЛОМНОЇ РОБОТИ

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	28	
6	А4	2 Розділ	13	
7	А4	3 Розділ	9	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	7	
14	А4	Додаток Ґ	9	
15	А4	Додаток Д	1	
15	А4	Додаток Е	1	

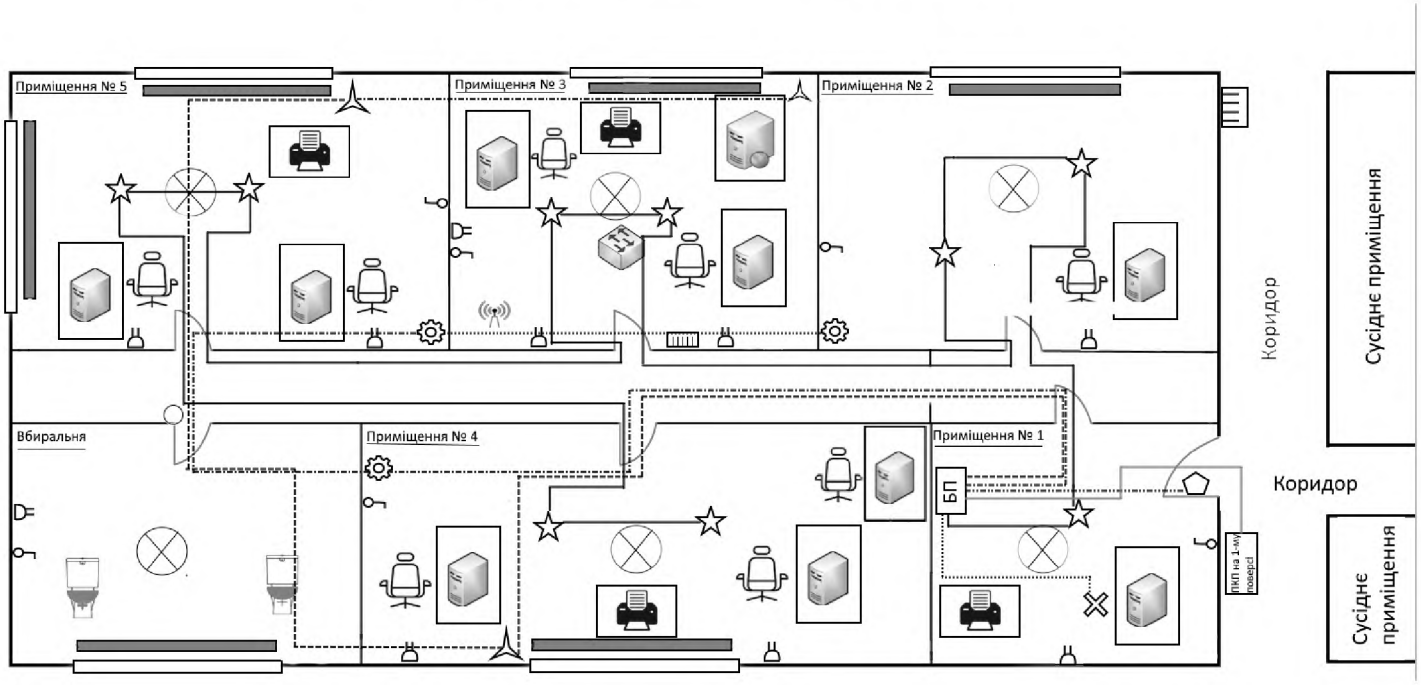
ДОДАТОК Б. ПЕРЕЛІК МАТЕРІАЛІВ НА ОПТИЧНОМУ НОСІЇ

— Презентація Чемеріс.ppt

— Диплом Чемеріс.doc

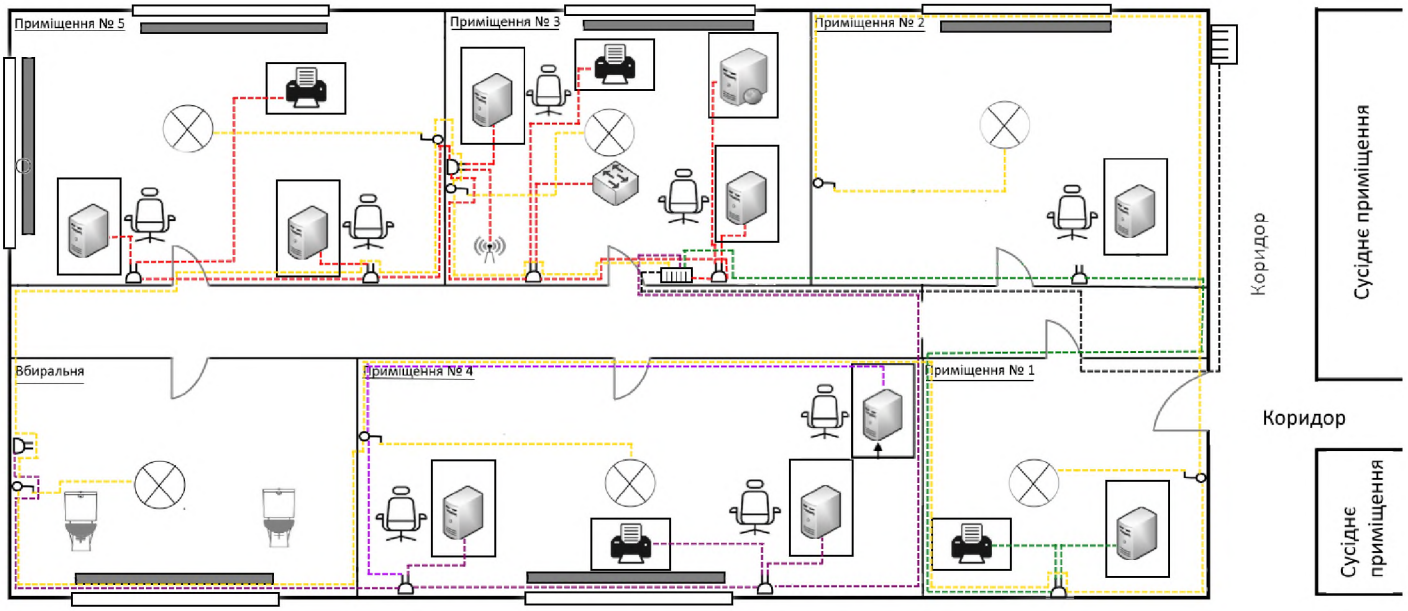
ДОДАТОК В. СИТУАЦІЙНИЙ ПЛАН ТОВ “Lantechincs”

ДОДАТОК Г. ГЕНЕРАЛЬНИЙ ПЛАН ТОВ “Lantechnics”



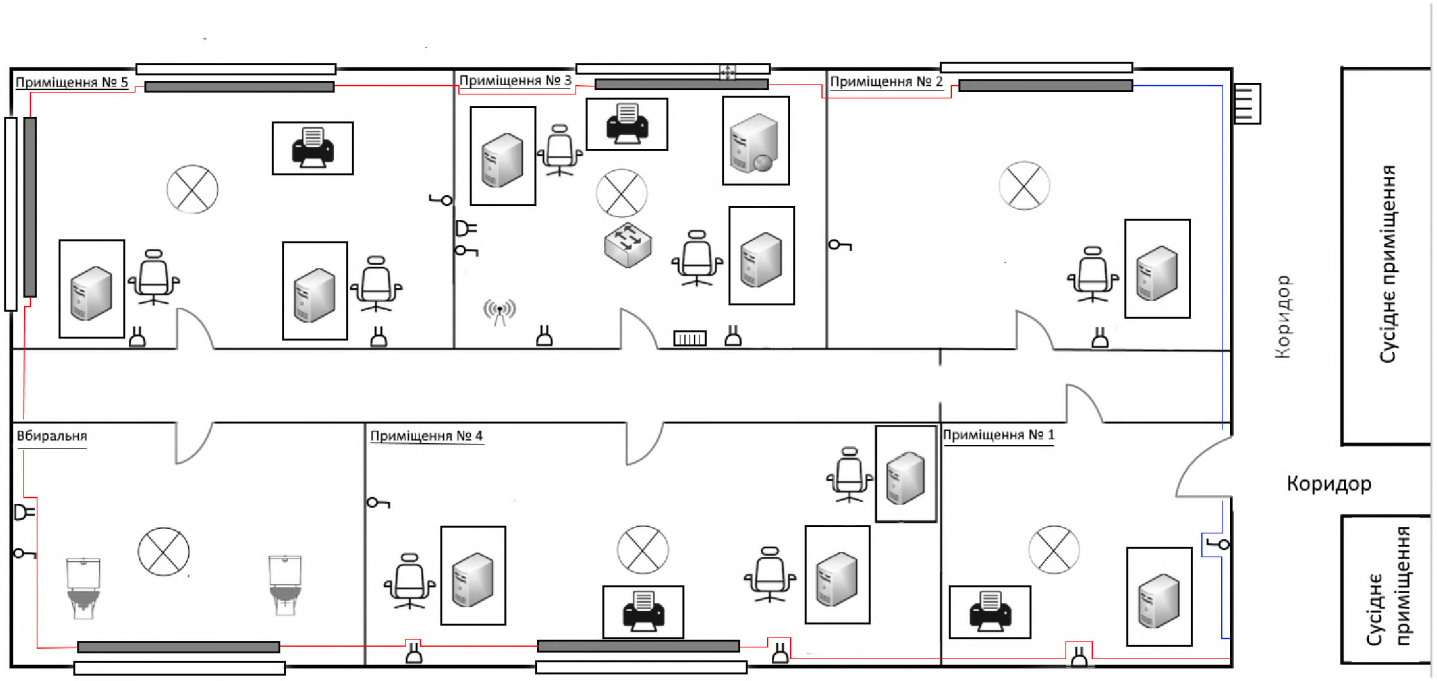
ПОЖЕЖНА ТА ОХОРОННА СИГНАЛІЗАЦІЯ СИГНАЛІЗАЦІЯ

ДОДАТОК Г. ГЕНЕРАЛЬНИЙ ПЛАН ТОВ “Lantechnics”



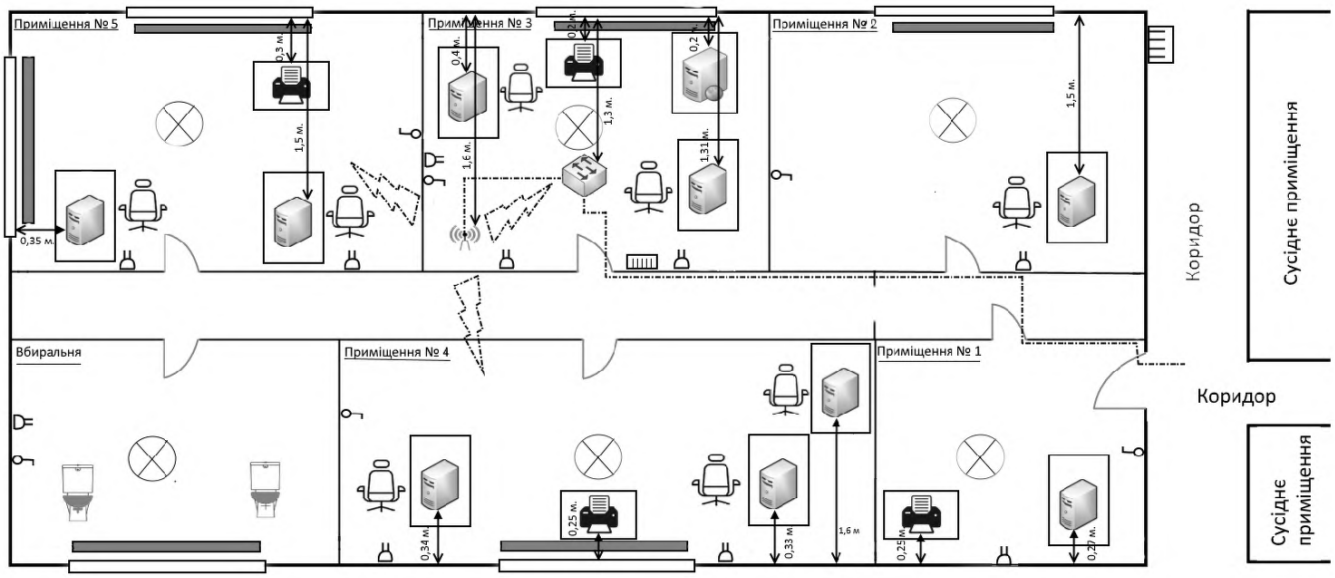
СИСТЕМА ОСВІТЛЕННЯ ТА ЕЛЕКТРОПОСТАЧАННЯ

ДОДАТОК Г. ГЕНЕРАЛЬНИЙ ПЛАН ТОВ “Lantechnics”



СИСТЕМА ОПАЛЕННЯ

ДОДАТОК Г. ГЕНЕРАЛЬНИЙ ПЛАН ТОВ “Lantechnics”



СИСТЕМА КОМП’ЮТЕРНОЇ МЕРЕЖІ

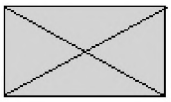
ДОДАТОК Г. УМОВНІ ПОЗНАЧЕННЯ

Ситуаційний план підприємства:

-- межа КЗ

-- номер будівлі

-- будівля

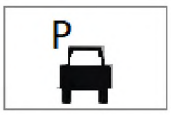


-- територія ОІД

-- паркан

-- трансформаторна підстанція

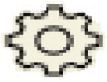
-- напрямок руху автомобілів



-- парковка автомобілів

-- система опалення

система водопостачання



-- розподільний щит

Позначення, які використовуються на всіх 4-х схемах генерального плану:


- персональний комп'ютер


- робоче місце


- принтер


- офісна люстра


- Web сервер


- Комутатор


- Роутер


- подвійна розетка


- вимикач освітлення


- вікно


- батарея опалення


- електрична щитова офісу


- електрична щитова поверху

Лінії системи опалення:

надходження гарячої води по трубам

- вихід холодної води по трубам

Лінії системи комп’ютерної мережі:

- бездротовий канал зв'язку

- лінія системи комп'ютерної мережі

- відстань до границі ОІД

Лінії систем освітлення та електропостачання:

- лінії системи освітлення(всі приміщення)
- лінії системи електропостачання (приміщення № 3, 5)
- лінії системи електропостачання (прміщення № 1, 2, 3)
- лінії системи електропостачання (приміщення № 3,4, вбиральня)
- лінія з'єднання щитової на поверху та офісної)

Лінії систем охоронної і пожежної сигналізації

лінія системи пожежної сигналізації

- Лінії систем охоронної сигналізації

сповіщувач диму

сповіщувач розбиття скла

інфрачервоний пасивний сповіщувач

кнопка тривоги

магнітоконтактний сповіщувач

ДОДАТОК Ґ. ТАБЛИЦЯ 1.2 – ВІДОМІСТЬ ОСНОВНИХ ТЕХНІЧНИХ ЗАСОБІВ

№	Назва	Назва в ІТС	Марка	Серійний номер	Модель	Розміщення	Відстань до границі ІТС
1	Системний блок	PC №1	Немає	123433	Відсутня	Приміщення №3, на підлозі	0,4м.
2	Системний блок	PC №2	Немає	456734	Відсутня	Приміщення №3, на підлозі	1,31м.
3	Системний блок	PC №7	Немає	234589	Відсутня	Приміщення №4, на підлозі	1,6 м.
4	Системний блок	PC №4	Немає	231568	Відсутня	Приміщення №2, на підлозі	1,5м.
5	Системний блок	PC №5	Немає	124680	Відсутня	Приміщення №4, на підлозі	0,33м.
6	Системний блок	PC №6	Немає	683216	Відсутня	Приміщення №4, на підлозі	0,34м.
7	Системний блок	PC №3	Немає	994357	Відсутня	Приміщення №5, на підлозі	1,5м.
8	Системний блок	PC №9	Немає	370427	Відсутня	Приміщення №5, на підлозі	0,35м.
9	Системний блок	PC №8	Немає	288064	Відсутня	Приміщення №1, на підлозі	0,27м.
10	Монітор до PC	Немає	Philips	345672	245E1S/00/01	Приміщення №3, на столі	0,4м.
11	Монітор до PC	Немає	Acer	234569	ED242QRAbidpx	Приміщення №3, на підлозі	1,31м.
12	Монітор до PC	Немає	AOC	645378	24G2U5/BK	Приміщення №4, на столі	1,6м.
13	Монітор до PC	Немає	Dell	157435	Dell SE2416H	Приміщення №2, на столі	1,5м.
14	Монітор до PC	Немає	Samsung	279552	S24E650PL (LS24E65UPL)	Приміщення №4, на столі	0,33м.
15	Монітор до PC	Немає	BenQ Zowie	222246	XL2411P (9H.LGPLB.Q)	Приміщення №4, на столі	0,34м.
16	Монітор до PC	Немає	LG	632747	29WL500-B	Приміщення №5, на столі	1,5м.
17	Монітор до PC	Немає	Asus	225636	VG259Q (90LM053)0-B01370)	Приміщення №5, на столі	0,35м.
18	Монітор до PC	Немає	Samsung	235795	S24R350	Приміщення №1, на столі	0,27м.
19	Принтер	Printer №1	Samsung Xpress	354353	Xpress SL-M2020	Приміщення №3, на столі	0,2м.
20	Принтер	Printer №2	Samsung Xpress	575676	Xpress SL-M2020	Приміщення №4, на столі	0,25м.

Продовження таблиці 1.2

21	Принтер	Printer №3	Samsung Xpress	345322	Xpress SL-M2020	Приміщення №5, на столі	0,3м.
22	Принтер	Printer №4	Samsung Xpress	234234	Xpress SL-M2020	Приміщення №1, на столі	0,25м.
23	Комутатор	Commutator	TP-LINK	235423	TL-SF1005D	Приміщення №3, на столі	1,3м.
24	Роутер	Router	TP-LINK	654732	TL-WR841N	Приміщення №3, на столі	1,6м.
25	Сервер	Server	ARTLINE	534522	R25 v12 (R25v12)	Приміщення №3, на столі	0,2м

ДОДАТОК Ґ. ТАБЛИЦЯ 1.3 – ВІДОМІСТЬ ДОПОМІЖНИХ ТЕХНІЧНИХ ЗАСОБІВ

№	Назва	Назва в ІТС	Марка	Серійний номер	Модель	Розміщення	Відстань до границі ІТС
1	Клавіатура до РС	Немає	MSI Interceptor	845617	DS4100 USB UKR	Приміщення №3, на столі	0,38м.
2	Клавіатура до РС	Немає	MSI Interceptor	112345	DS4100 USB UKR	Приміщення №3, на підлозі	1,35м.
3	Клавіатура до РС	Немає	MSI Interceptor	435345	DS4100 USB UKR	Приміщення №4, на столі	1,6м.
4	Клавіатура до РС	Немає	MSI Interceptor	345346	DS4100 USB UKR	Приміщення №2, на столі	1,54м.
5	Клавіатура до РС	Немає	MSI Interceptor	234234	DS4100 USB UKR	Приміщення №4, на столі	0,30м.
6	Клавіатура до РС	Немає	Esperanza Wired	275644	EGK601 Iluminated	Приміщення №4, на столі	0,30м.
7	Клавіатура до РС	Немає	Esperanza Wired	345345	EGK601 Iluminated	Приміщення №5, на столі	1,55м.
8	Клавіатура до РС	Немає	Esperanza Wired	225643	EGK601 Iluminated	Приміщення №5, на столі	0,38м.
9	Клавіатура до РС	Немає	Esperanza Wired	275734	EGK601 Iluminated	Приміщення №1, на столі	0,29м.
10	Мишка до РС	Немає	HP	345345	X220 USB Black	Приміщення №3, на столі	0,35м.
11	Мишка до РС	Немає	HP	234532	X220 USB Black	Приміщення №3,на підлозі	1,34м.

Продовження таблиці 1.3.

12	Мишка до PC	Нема є	HP	364579	X220 USB Black	Приміщення №4, на столі	1,6м.
13	Мишка до PC	Нема є	HP	224355	X220 USB Black	Приміщення №2, на столі	1,57м.
14	Мишка до PC	Нема є	HP	568678	X220 USB Black	Приміщення №4, на столі	0,33м.
15	Мишка до PC	Нема є	HP	567567	X220 USB Black	Приміщення №4, на столі	0,33м.
16	Мишка до PC	Нема є	HP	457453	X220 USB Black	Приміщення №5, на столі	1,54м.
17	Мишка до PC	Нема є	HP	687684	X220 USB Black	Приміщення №5, на столі	0,36м.
18	Мишка до PC	Нема є	HP	234234	X220 USB Black	Приміщення №1, на столі	0,26м.

ДОДАТОК Ґ. ТАБЛИЦЯ 1.4 – ВІДОМІСТЬ ДОПОМІЖНИХ ТЕХНІЧНИХ ЗАСОБІВ(2)

№	Назва	Розміщення	Марка	Модель	Серійний номер
1	Пасивний інфрачервоний сповіщувач	Приміщення №4, на стелі в лівому куту	Satel	APMD-150	235445
2	Пасивний інфрачервоний сповіщувач	Приміщення №5, на стелі в правому куту	Satel	APMD-150	524526
3	Пасивний інфрачервоний сповіщувач	Приміщення №2, на стелі в лівому куту	Satel	APMD-150	235745
4	Сповіщувач диму	Приміщення №1, на стелі	Аврора-01	ИП 212-141	345246
5	Сповіщувач диму	Приміщення №4, на стелі	Аврора-01	ИП 212-141	235452
6	Сповіщувач диму	Приміщення №4, на стелі	Аврора-01	ИП 212-141	245345
7	Сповіщувач диму	Приміщення №5, на стелі	Аврора-01	ИП 212-141	245256
8	Сповіщувач диму	Приміщення №5, на стелі	Аврора-01	ИП 212-141	678673
9	Сповіщувач диму	Приміщення №3, на стелі	Аврора-01	ИП 212-141	245882
10	Сповіщувач диму	Приміщення №3, на стелі	Аврора-01	ИП 212-141	245856
11	Сповіщувач диму	Приміщення №2, на стелі	Аврора-01	ИП 212-141	568556

12	Сповіщувач д.	Приміщення №2, на стелі	Аврора-01	ИП 212-141	658463

Продовження таблиці 1.4

13	Сповіщувач розбиття скла	Приміщення №4, зверху на вікні	Астра	ІО-329-5	457955
14	Сповіщувач розбиття скла	Приміщення №5, зверху на вікні	Астра	ІО-329-5	468657
15	Сповіщувач розбиття скла	Приміщення №3, зверху на вікні	Астра	ІО-329-5	568563
16	Кнопка тривоги	Приміщення №1, під столом	Aritech	3045-W	835685
17	Магнітоконтактний сповіщувач	Приміщення №3, заверху дверей	Орбита	СМК-1	569939

ДОДАТОК Ґ. ТАБЛИЦЯ 1.5 – ХАРАКТЕРИСТИКА ТЕХНІЧНИХ ЗАСОБІВ

№	Назва	Назва в ІТС	Відповідальний	Характеристика	Серійний номер
1	Персональний комп'ютер	РС№1	Системний адміністратор	Материн. плата: MSI B450 ,AM4,2x DDR4 Процесор: AMD Ryzen 3 3200G, 3,6 (4,0 Turbo) ГГц, 12 нм, 4 ядра, 65 Вт. Операт. пам'ять:HyperX DDR4-3200, 8 gb Жорсткий диск: Western Digital , 500Gb	123131 454353 486732 867864
2	Персональний комп'ютер	РС№2	Помічник сис.адміністратора	Материн. плата: Asus TUF B450-Pro, AM4, 4 x DDR4 Процесор: AMD Ryzen 3 2200G, 3,5 (Turbo 3,7) ГГц ,14 нм,4 ядра, 65вт. Операт. пам'ять: HyperX DDR4-3200, 8 gb Жорсткий диск: Mediamax 500 gb	235797 867867 457397 124554
3	Персональний комп'ютер	РС№3	Бухгалер	Материн. плата: Gigabyte GA-A320M, AM4, 2 x DDR4 Процесор: Intel Core i3-8100 3.6GHz,8GT,s,6MB, 4 ядра. Операт. пам'ять: HyperX DDR4-3200, 8 gb Жорсткий диск: i.norys 500 gb	236848 567535 457587 457245
4	Персональний комп'ютер	РС№4	Директор	Материн. плата:AMD a 320,AM4,2x DDR4 Процесор: AMD Ryzen 5 2600 (3.4 - 3.9 ГГц), 12 нм, DDR4, 65 Вт. Операт. пам'ять:HyperX DDR4-3200, 4GB, Жорсткий диск: Western Digital , 500Gb	457986 457325 856867 385676

5	Персональний комп'ютер	PC№5	Системний програміст	Материн. плата: Gigabyte GA-A320M, AM4, 2 x DDR4 Процесор: Intel Core I5-6500, 2,8 GHz,,8GT,s,6MB, 4 ядра Відеокарта: Palit nVidia GeForce GTX 1050, 1290 МГц, 4gb, GDDR5 Операт. пам'ять: Kingston DDR3-1600 4096MB Жорсткий диск: Mediamax 500 gb	546754 234543 234663 345645 375463

Продовження таблиці 1.5

6	Персональний комп'ютер	PC№6	Веб програміст	Материн. плата: : MSI B450 ,AM4,2x DDR4 Процесор: Intel Core i5-9400F 2.9GHz,8GT,s,9MB Відеокарта: Palit nVidia GeForce GTX 1050, 1290 МГц, 4gb, GDDR5 Операт. пам'ять: HyperX DDR4-3200, 8GB. Жорсткий диск: i.norys 500 gb	436456 567567 347456 456457 867567
7	Персональний комп'ютер	PC№7	Прикладний програміст	Материн. плата: : MSI B450 ,AM4,2x DDR4 Процесор: Intel Core I5-6500, 2,8 GHz,,8GT,s,6MB, 4 ядра Відеокарта: Palit nVidia GeForce GTX 1050, 1290 МГц, 4gb, GDDR5. Операт. пам'ять: HyperX DDR4-3200 4 GB Жорсткий диск: Western Digital , 500Gb	546346 545654 457454 457356 756756
8	Персональний комп'ютер	PC№8	Секретар	Материн. плата:AMD a 320,AM4,2x DDR4 Процесор: AMD Ryzen 5 2600 (3.4 - 3.9 ГГц), 12 нм, DDR4, 65 Вт. Операт. пам'ять:HyperX DDR4-3200, 8GB Жорсткий диск: Mediamax 500 gb	457532 435764 465478 458765
9	Персональний комп'ютер	PC№9	Менеджер	Материн. плата: Asus TUF B450-Pro, AM4, 4 x DDR4 Процесор: Intel Core i3-9100 3.6GHz,8GT,s,6MB Операт. пам'ять: Kingston DDR4-1600 8GB Жорсткий диск: i.norys 500 gb	457453 435675 568678 457577
10	Комутатор	Commutator	Сис. адмін	ЧС5 x Fast Ethernet (10/100 Мбит/с), 350 Вт	353467
11	Роутер	Router	Сис. адмін	4 порта 10/100M LAN (типа RJ45),1 порт 10/100M WAN (типа RJ45), DoS, SPI Firewall	437535
12	Сервер	Server	Сис. адмін	4 ядра, 3.5 - 4.7 ГГц,32 ГБ, HDD: 2 x 1ТБ SSD: 2 x 250 ГБ	457567
13	Принтер	Printer №1	Поміч.сис.адмін.	Лазерная печать, 600x3600 dpi, Wi-Fi, Ethernet, Встроенный модуль 10/100/1000Base-TX Ethernet, Gigabit.	345765
14	Принтер	Printer №2	Системнийпрограміст	Лазерная печать, 600x3600 dpi, Wi-Fi, Ethernet, Встроенный модуль 10/100/1000Base-TX Ethernet, Gigabit.	345123

15	Принтер	Printer №3	Бухгалтер	Лазерная печать, 600x3600 dpi, Wi-Fi, Ethernet, Встроенный модуль 10/100/1000Base-TX Ethernet, Gigabit.	436967
16	Принтер	Printer №4	Секретар	Лазерная печать, 600x3600 dpi, Wi-Fi, Ethernet, Встроенный модуль 10/100/1000Base-TX Ethernet, Gigabit.	454364

ДОДАТОК Ґ. ТАБЛИЦЯ 1.6 – ВІДОМІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

№	Назва	Де встановлена	Опис	Вид	Ліцензія
1	Windows 10 (версия 1903)	PC№1,PC№2, PC№3, PC№4, PC№5, PC№6, PC№7, PC№8, PC№9	Операційна система для персональних комп'ютерів і робочих станцій, розроблена корпорацією Microsoft.	Системне	+ OEM
2	Microsoft Word (версія 2016)	PC№1,PC№2, PC№3, PC№4, PC№5, PC№6, PC№7, PC№8, PC№9	Текстовий процесор, призначений для створення, перегляду і редагування текстових документів	Прикладне	Корпоративна
3	Microsoft Excel (версія 2016)	PC№1,PC№2, PC№3, PC№4, PC№5, PC№6, PC№7, PC№8, PC№9	програма для роботи з електронними таблицями, створена корпорацією Microsoft	Прикладне	Корпоративна
4	Microsoft PowerPoint (версія 2016)	PC№1,PC№2, PC№3, PC№4, PC№5, PC№6, PC№7, PC№8, PC№9	Програма підготовки презентацій і перегляду презентацій	Прикладне	Корпоративна
5	WinRar (версія 5.80)	PC№1,PC№2, PC№3, PC№4, PC№5, PC№6, PC№7, PC№8, PC№9	Програма для архівування файлів і зміни їх розміру	Системне	shareware
6	Microsoft Project (версія 2019)	PC№1,PC№2, PC№3, PC№4, PC№5, PC№6, PC№7, PC№8, PC№9	програма управління проектами	Прикладне	Корпоративна
7	Google Chrome (версія 80.0.3987.149)	PC№1,PC№2, PC№3, PC№4, PC№5, PC№6, PC№7, PC№8, PC№9	браузер, що розробляється компанією Google	Прикладне	безкоштовна

8	Adobe Acrobat(версія 15.0)	РС№1,РС№2, РС№3, РС№4, РС№5, РС№6, РС№7, РС№8, РС№9	Програма редназначена для створення і перегляду електронних публікацій в форматі PDF.	Прикладне	Електронна
9	Adobe Photoshop (версія 2014.0.0)	РС№5, РС№6, РС№7	багатофункціональний графічний редактор	Прикладне	Shareware
10	360 total security (верс ія 10.60.1314)	Всі РС	програма яка захист робочих станцій від вірусів	Системне	–

Продовження таблиці 1.6

11	The KMPlayer(*64 X*)	РС№1,РС№2, РС№3, РС№4, РС№5, РС№6, РС№7, РС№8, РС№9	Програма для відтворення відео файлів.	Прикладне	Безкоштовн а
12	1С:Бухгалте рия(версія 8)	РС№3	програма для автоматизації бухгалтерського обліку	Прикладне	Корпоратив на
13	Microsoft Visual Studio 2019(версія 16.0.2)	РС№5, РС№6, РС№7	інтегроване середовище розробки програмного забезпечення і ряд інших інструментальних засобів.	Прикладне	комерційна
14	Delfi(версія XE2)	РС№5, РС№6, РС№7	програма для написання прикладного програмного забезпечення	Прикладне	Комерційна
15	Notepad++ (в ерсія 7.8.5)	РС№5, РС№6, РС№7	вільний текстовий редактор	Прикладне	безкоштовн а
16	Eclipse(версі я 4.15.0)	РС№5, РС№6, РС№7	вільна інтегроване середовище розробки модульних кроссплатформенних додатків	Прикладне	Безкоштовн а
17	Microsoft SQL Server(версія 15.0)	РС№5, РС№6, РС№7	система керування базами даних (РСУБД)	Прикладне	Комераційн а
18	Exat file	РС№1,РС№2	Програма для перевірки цілісності файлів	прикладне	–

ДОДАТОК Ґ. ТАБЛИЦЯ 1.15 – СПЕЦИФІКАЦІЯ МОДЕЛІ ПОРУШНИКА

За мотивами здійснення порушень

Позначення	Мотив порушення Рівень загроз	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов'язок (ПЗ4)	4
За рівнем кваліфікації та обізнаності щодо ІТС		
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3

Продовження таблиці 1.15

К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4
За показником можливостей використання засобів та методів подолання системи захисту		
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4
За часом дії		
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	4
За місцем дії		
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

ДОДАТОК Ґ. ТАБЛИЦЯ 1.16 – МОДЕЛЬ ПОРУШНИКА

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Системний адміністратор	ПВ4	М1	К4	З1	Ч4	Д4	17
	3	1	4	1	4	4	
	ПЗ4	М4	К3	З4	Ч4	Д4	23
	4	4	3	4	4	4	
Поміч.системн.адміністратора	ПВ4	М1	К2	З1	Ч4	Д3	14
	3	1	2	1	4	3	
	ПЗ4	М4	К3	З2	Ч4	Д3	20
	4	4	3	2	4	3	
Бухгалтер	ПВ3	М1	К1	З1	Ч3	Д3	10
	2	1	1	1	3	3	

	ПЗ4	М4	К2	З2	Ч3	Д2	19

Продовження таблиці 1.16

	4	4	2	2	3	2	
Директор	ПВ3	М3	К2	З2	Ч3	Д4	16
	2	3	2	2	3	4	
	ПЗ4	М4	К2	З3	Ч4	Д4	21
	4	4	2	3	4	4	
Системний програміст	ПВ3	М1	К3	З1	Ч3	Д2	12
	2	1	3	1	3	2	
	ПЗ4	М4	К3	З2	Ч3	Д2	18
	4	4	3	2	3	2	
Веб-програміст	ПВ3	М1	К3	З1	Ч3	Д2	12
	2	1	3	1	3	2	
	ПЗ4	М4	К3	З2	Ч3	Д2	18
	4	4	3	2	3	2	
Прикладний програміст	ПВ3	М1	К3	З1	Ч3	Д2	12
	2	1	3	1	3	2	
	ПЗ4	М4	К3	З2	Ч3	Д2	18
	4	4	3	2	3	2	
Секретар	ПВ3	М1	К1	З1	Ч3	Д2	10
	2	1	1	1	3	2	
	ПЗ4	М4	К2	З2	Ч3	Д2	11
	4	4	2	2	3	2	
Менеджер	ПВ3	М1	К1	З1	Ч3	Д3	11
	2	1	1	1	3	3	
	ПЗ4	М4	К2	З2	Ч3	Д2	11
	4	4	2	2	3	2	

ДОДАТОК Д. ВІДГУКИ КЕРІВНИКІВ РОЗДІЛІВ

В І Д Г У К

на кваліфікаційну роботу студента групи 125-19-2 Чемеріс М.К

на тему: «Обгрунтування методів моніторингу та оцінки захищеності інформації в інформаційно-комунікаційній системі підприємства.»