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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Соломіна Костянтина Сергійовича*

академічної групи *125-19ск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка системи захисту інформації інформаційно-комунікаційної системи приватного підприємства "Степ 2020"*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Соломіну Костянтину Сергійовичу* **академічної групи** *125-19ск-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка системи захисту інформації інформаційно-комунікаційної системи приватного підприємства "Степ2020"***

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

Розділ	Зміст	Термін виконання
Розділ 1	Розглянути характеристику підприємства, навести структура ІТС, провести категоріювання та обстеження об'єкту	29.03.2022
Розділ 2	Визначити функціональний профіль захищеності автоматизованої системи, побудувати модель загроз та модель порушника, запропонувати та налаштувати програмне забезпечення для забезпечення всіх критеріїв профілю захищеності та нейтралізації загроз інформації в ІТС ПП «Степ 2020»	24.05.2022
Розділ 3	Визначити збитки від атаки на обчислювану мережу та здійснити розрахунок витрат на реалізацію системи захисту інформації комп'ютерної мережи	14.06.2022

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

Дата видачі: 08.01.2022р.

Дата подання до екзаменаційної комісії: 15.06.2022р.

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

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., _ табл., __ додатка, __ джерел.

Мета роботи: розробка системи захисту інформації в інформаційно-комунікаційної системи приватного підприємства " Степ 2020".

У розділі «Стан питання. Постановка задачі» розглянута характеристика підприємства, наведена структура ІТС, проведене категоріювання та обстеження об’єкту.

У спеціальній частині визначений функціональний профіль захищеності автоматизованої системи, побудована модель загроз та модель порушника, запропоноване, встановлене та налаштоване програмне забезпечення для забезпечення всіх критеріїв профілю захищеності та нейтралізації загроз інформації в ІТС ПП «Степ 2020».

В економічному розділі визначені збитки від атаки на обчислювану мережу та здійснено розрахунок витрат на реалізацію системи захисту інформації комп’ютерної мережи.

Впровадження запропонованих засобів та заходів дозволить підвищити рівень інформаційної безпеки на підприємстві.

ІНФОРМАЦІЙНА БЕЗПЕКА, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ЗАГРОЗА, АВТОМАТИЗОВАНА СИСТЕМА, КАТЕГОРІЮВАННЯ, ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ.

ABSTRACT

Explanatory note: ___ pp., ___ pic., ___ table, ___ app, ___ sources.

Purpose: development of a comprehensive information security system in the information and communication system of the private enterprise "Step 2020".

In the section "Status of the issue. Problem statement "the characteristic of the enterprise is considered, the structure of ITS is resulted, the categorization and inspection of object is carried out.

The special part defines the functional security profile of the automated system, builds a threat model and violator model, proposed, installed and configured software to ensure all the criteria of the security profile and neutralize information threats in ITS PE "Step 2020".

The economic section identifies the losses from the attack on the computer network and calculates the cost of implementing a system of information protection of the computer network.

The implementation of the proposed tools and measures will increase the level of information security in the enterprise.

INFORMATION SECURITY, THREAT MODEL, INFRINGEMENT MODEL, THREAT, AUTOMATED SYSTEM, CATEGORY, OBJECT OF INFORMATION ACTIVITY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – Автоматизована система;

БД – База даних;

ДТЗС – Допоміжні технічні засоби;

ЕОМ – Електрона обчислювальна машина;

ЗОТ – Засоби обчислювальної техніки;

ЗУ – Закон України;

ІБ – Інформаційна безпека;

ІзОД – Інформація з обмеженим доступом;

ІБ – Інформаційна безпека;

ІС – Інформаційна система;

ІТС – Інформаційно-телекомунікаційна система.

ІС – Інформаційна система;

КЗ – Контрольована зона;

КЗЗ – Комплекс засобів захисту;

КС – Комп'ютерна система;

КСЗІ – Комплексна система захисту інформації;

ЛОМ – Локальна обчислювальна мережа;

ОІД – Об'єкт інформаційної діяльності;

ПК – Персональний комп'ютер;

ПЗ – Програмне забезпечення;

НСД – Несанкціонований доступ;

GB – Gigabyte;

IP – Internet Protocol;

MB – Megabyte;

USB – Universal Serial Bus.

ЗМІСТ

с.

ВСТУП ... 8

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ ... 9

1.1 Загальні відомості про ПП «СТЕП 2020» ... 12

1.2 Технології передачі даних ... 17

1.3 Фізична середа передачі даних ... 17

1.4 Локальна обчислювальна мережа ... 17

1.5 Визначення класу автоматизованої системи ... 18

1.6 Опис системи ... 18

1.7 Контрольована зона ... 20

1.8 Категоріювання об'єкту ... 20

1.9 Обстеження ІТС «ПП СТЕП 2020» ... 21

1.10 Визначення кількості програмних засобів для виконання робіт ... 31

1.11 Теоретичні відомості про програмний комплекс «Астра» ... 31

1.12 Супровід та оновлення ПЗ ... 32

1.13 Висновок. Постановка задач ... 33

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА ... 34

2.1 Технічне завдання ... 34

2.2 Модель порушника ... 35

2.3 Модель загроз інформації ІТС ПП «СТЕП 2020» ... 37

2.3.1 Види джерел загроз ... 38

2.4 Аналіз ризиків ... 41

2.5 Вибір функціонального профілю захищеності ... 48

2.5.1 Критерії конфіденційності ... 49

2.5.2 Критерії цілісності ... 51

2.5.3 Критерії доступності ... 53

2.5.4 Критерії спостережності ... 54

2.6 Запропоноване програмне забезпечення ... 57

2.6.1 Діагностика носіїв інформації ... 57

2.6.2 Програмний засіб для очищення оперативної пам'яті 61
2.6.3 Базова цілісність при обміні..... 63
2.6.4 Налаштування одно направлений достовірний канал..... 66
2.7 Висновок 68
РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ 69
3.1 Розрахунок (фіксованих) капітальних витрат 69
3.1.1 Розрахунок поточних витрат..... 72
3.2 Оцінка можливого збитку 75
3.2.1 Загальний ефект від впровадження системи інформаційної безпеки..... 78
3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки..... 78
3.4 Висновок 79
ВИСНОВКИ..... 81
ПЕРЕЛІК ПОСИЛАНЬ 82
ДОДАТОК А..... 83
ДОДАТОК Б 84
ДОДАТОК В 85
ДОДАТОК Г 86

ВСТУП

Питанню інформаційної безпеки зараз приділяється величезна увага, існують тисячі публікацій з цієї тематики, присвячені різним аспектам і прикладним питанням захисту інформації, на міжнародному та державному рівнях приділяється багато уваги для забезпечення інформаційної безпеки.

Під інформаційною безпекою розуміють захищеність інформації від випадкових і навмисних впливів природного або штучного характеру, чреватих нанесенням шкоди власникам або користувачам інформації. Вона досягається здійсненням комплексу нормативно-правових, організаційно-технічних, апаратних і програмних заходів і засобів щодо запобігання несанкціонованого розповсюдження (витоку, розкрадання, копіювання), втрати, знищення, спотворення, підробки, блокування інформації.

Проблема забезпечення інформаційної безпеки – комплексна, тому її рішення має розглядатися на різних рівнях: законодавчому, адміністративному, процедурному і програмно-технічному.

Мета заходів щодо забезпечення інформаційної безпеки – скоротити можливий економічний і моральний збиток підприємства, пов'язаний з пошкодженням чи неправомірним використанням інформаційних ресурсів.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

Проблема захисту інформації, взагалі кажучи, має багатовікову історію. Адже навіть наскальні малюнки (не кажучи вже про стародавніх рукописах) є не що інше, як спроба зберегти інформацію про реалії об'єктивного світу. Застосування ж спеціальних заходів з метою збереження інформації в таємниці практикувалося ще в стародавні часи: достовірно, наприклад, відомо, що видатний політичний діяч і полководець Стародавнього Риму Цезар використовував для цих цілей криптографічне перетворення текстів повідомлень (яке увійшло в історію під назвою шифру Цезаря), хоча за сучасними уявленням вельми примітивне.

Але оскільки тут розглядаються питання захисту інформації в автоматизованих системах її обробки, то і ретроспективний аналіз їх походження і розвитку будемо виробляти на глибину реального існування цих систем. У провідних, з точки зору інформатизації, країнах розглянута проблема знаходиться в центрі уваги фахівців і інтенсивна розробляється вже більше 30 років. Досить красномовним свідченням цього уваги може слугувати той факт, що число публікацій по різних аспектах захисту інформації тільки в відкритій пресі обчислюється багатьма тисячами, причому серед них багато десятків - це публікації монографічного характеру. Видаються спеціальні журнали, регулярно проводяться конференції, відповідні дисципліни включені в навчальні плани всіх вузів, що готують фахівців з обчислювальної техніки і її використанню.

На даний час приватна й ділова інформація має комерційну вартість і тому важливою є проблема її захисту від несанкціонованого доступу. Нині спостерігається тенденція до підвищення кількості атак та несанкціонованого доступу, які захоплюють контроль над віддаленою інформаційною системою, копіюють та передають зловмисникам персональні дані, іншу конфіденційну або, навіть, секретну інформацію. Проблема комплексного захисту сучасних інформаційно-комунікаційних систем та мереж інформації стає ще

актуальнішою, якщо мова йде про захист великої кількості оперативної інформації, що обробляється в сучасних комп'ютерних системах.

Інформація – це дані про осіб, предмети, факти, події, явища та процеси незалежно від форми їх подання.

Головною метою будь-якого підприємства є забезпечення конфіденційності, цілісності та доступності циркулюючої інформації.

Метою захисту інформації повинно бути:

- запобігання відтіканню, розкраданню, втраті, перекручуванню, підробці інформації;
- запобігання загрозам державної безпеки, безпеки особистості, суспільства в цілому;
- запобігання несанкціонованим діям зі знищення модифікації, копіювання, блокування інформації; запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні бази даних і системи, забезпечення правового режиму документованої інформації як об'єкта власності;
- збереження конфіденційності документованої інформації згідно з діючим законодавством;
- забезпечення прав суб'єктів в інформаційних процесах при розробці, виробництві та застосуванні інформаційних систем, технологій та засобів їх забезпечення.

У цілому засоби забезпечення захисту інформації в частині запобігання навмисних дій залежно від способу реалізації можна поділити на групи:

- технічні;
- програмні;
- змішані;
- організаційні.

Оскільки тема кваліфікаційної роботи – розробка системи захисту інформації інформаційно-комунікаційної системи, мова буде йти про методи захисту.

Наскільки актуальна проблема захисту інформації від різних загроз, можна побачити на прикладі даних, опублікованих Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

- несанкціонований доступ – 2 %;
- укорінення вірусів – 3 %;
- технічні відмови апаратури мережі – 20 %;
- цілеспрямовані дії персоналу – 20 %;
- помилки персоналу (недостатній рівень кваліфікації) – 55%.

Таким чином, однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор), оскільки вони становлять 75 % усіх випадків.

Загалом, об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації.

Порушник – користувач, який здійснює несанкціонований доступ до інформації

Загроза несанкціонованого доступу – це подія, що кваліфікується як факт спроби порушника вчинити несанкціоновані дії стосовно будь-якої частини інформації в інформаційній системі.

Потенційні загрози несанкціонованого доступу до інформації в інформаційних системах поділяють на цілеспрямовані (умисні) та випадкові. Умисні загрози можуть маскуватися під випадкові шляхом довгочасної масованої атаки несанкціонованими запитами або комп'ютерними вірусами.

Для того, щоб мінімізувати цю шкоду і впроваджують політику інформаційної безпеки, аби проінформувати користувачів про їх обов’язки та санкції, які будуть до них застосовуватись, або визначити що потрібно робити у разі інших форс-мажорних обставин.

Об’єктом обстеження в дипломному проекті є приватне підприємство «Степ 2020». Розробка комплексної системи захисту інформації для кожного підприємства є першочерговою справою, а для компанії, яка має напрям у торгівельній сфері тим паче, оскільки на підприємстві циркулює великий обсяг інформації, що відноситься до конфіденційної інформації та великий об’єм персональних даних клієнтів компанії.

Втрата або НСД до цієї інформації може нанести як матеріальну, так і моральну шкоду.

На основі проаналізованого існуючого стана безпеки інформації, а також побудованих моделі порушника та моделі загроз, буде розроблена комплексна системи захисту інформації інформаційно-телекомунікаційної системи інформаційної безпеки підприємства.

1.1 Загальні відомості про ПП «СТЕП 2020»

Приватне підприємство «СТЕП 2020» компанія яка надає послуги з виготовлення та продажу м’яких меблів. Основною метою є розробка дизайну меблів та їх виготовлення. Центр розробки дизайну меблів розташований за адресом м. Дніпропетровськ, вул. Якова Самарського, 5 (таблиця 1.1).

Таблиця 1.1 – Загальні відомості про організацію

№ П/П	Повна назва	Приватне підприємство «СТЕП 2020»
1	Форма власності	Приватна
2	Поштова адреса	Україна, м. Дніпро, вул. Якова Самарського, 5
3	Кількість персоналу	9 чоловік

Штат працівників:

- Директор – 1 чол.
- Секретар директора – 1 чол.
- Помічник бухгалтера – 1 чол.
- Головний бухгалтер –1 чол.

- Дизайнер – 2 чол.
- Системний адміністратор – 1 чол.
- Головний дизайнер – 1 чол.
- Охорона – 1 чол.

Обов’язки персоналу:

1 Директор - керівник підприємства;

2 Секретар директора – здійснює роботу з організаційно-технічного забезпечення адміністративно-розпорядчої діяльності керівника;

3 Бухгалтер – прийом та видача готівки, оформлення касових документів, видача бланків суворої звітності, здача і отримання грошей в банку, облік касових операцій;

4 Дизайнер – виконує специфічний ряд проектної діяльності, що об'єднує художньо-предметне мистецтво і науково обґрунтовану інженерну практику у сфері індустріального виробництва;

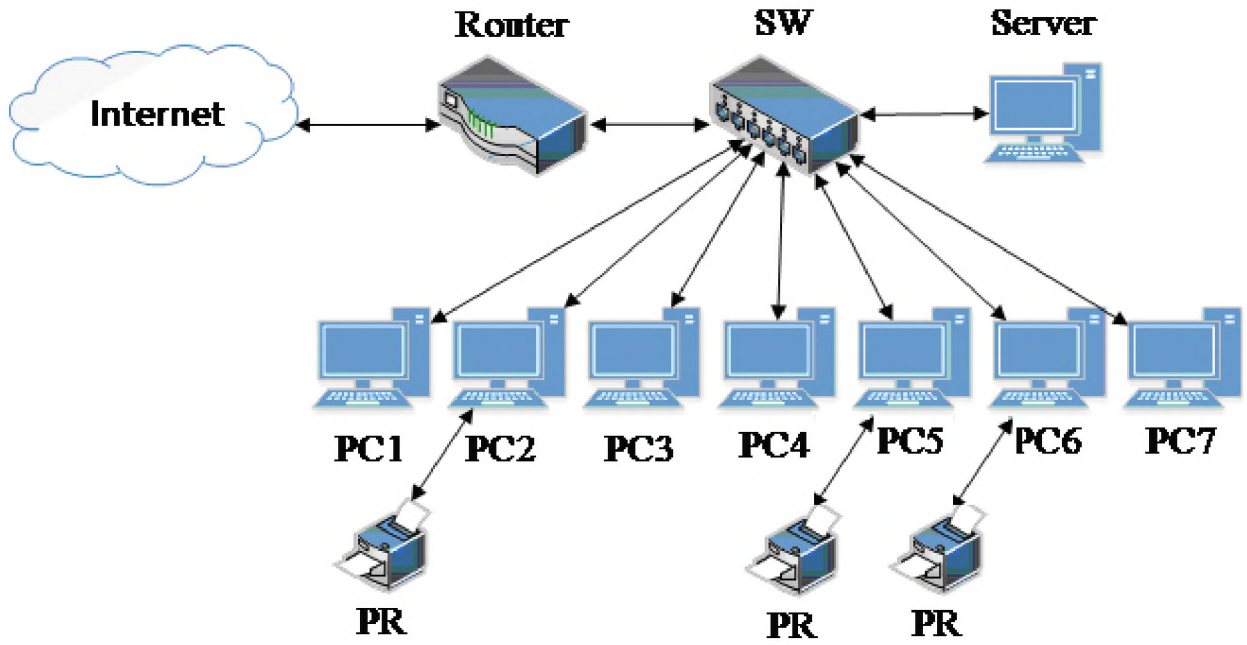
5 Системний адміністратор – виконує роль системного адміністратора та адміністратора безпеки одночасно. Контроль і підтримка працездатності ЛОМ, налаштування мережевого обладнання, інформує керівництво компанії про вразливі місця обчислювальної мережі та ін;

6 Охоронець – охороняє контрольовану зону підприємства від несанкціонованого проникнення з боку третіх осіб;

Об’єкт інформаційної діяльності складається з сервера, який є головним обчислювальним вузлом в ЛОМ, який виконує функцію файлового серверу, робочих станцій та комунікаційного обладнання.

Кожен з комп’ютерів має локальну операційну систему, локальний обліковий запис, антивірусне ПЗ, прикладне ПЗ і спеціалізоване ПЗ.

Узагальнена схема мережі «ПП СТЕП 2020» представлена на рисунку 1.1.



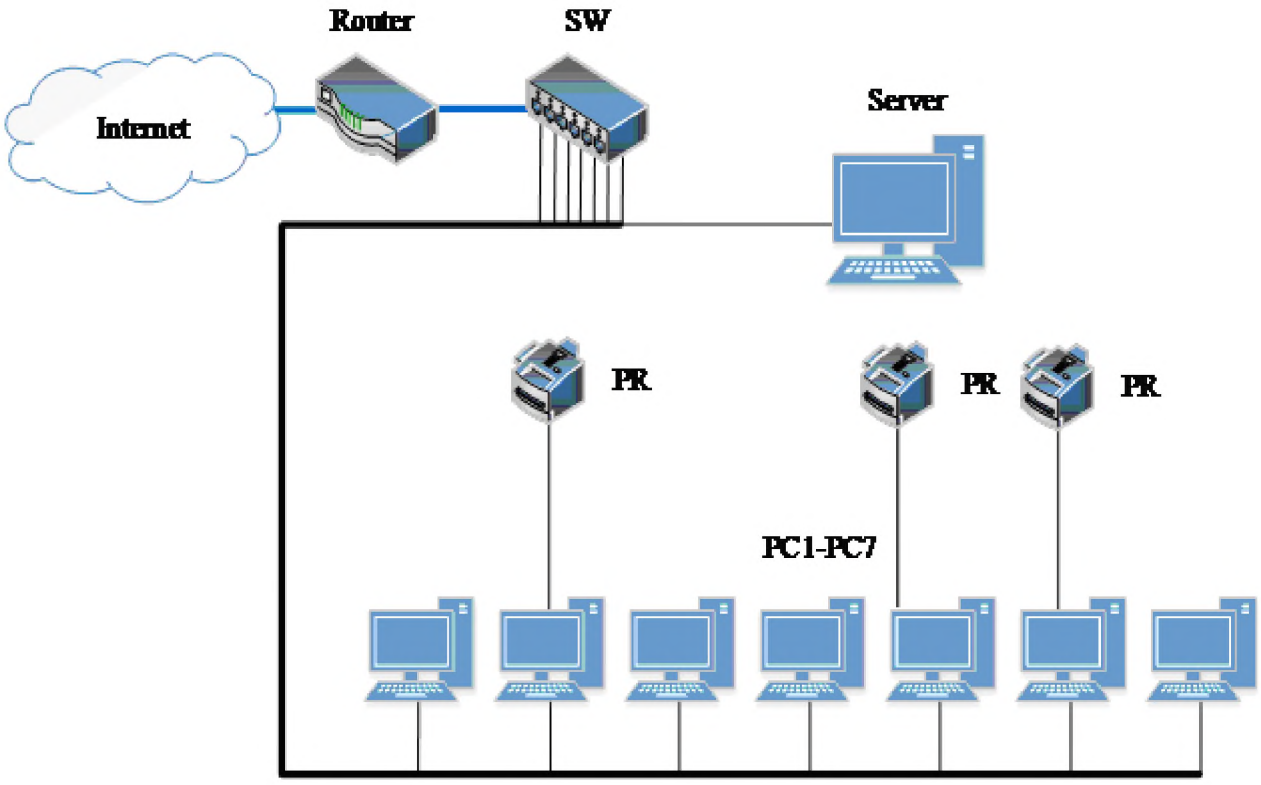
PC 1 – Директор
PC 2 – Секретар директора
PC 3 – Помічник бухгалтера
PC 4 – Головних бухгалтер
PC 5 – Дизайнер №1
PC 6 – Дизайнер №2
PC 7 – Головний дизайнер
SW – Комутатор
Router - Маршрутизатор
PR – Багатофункціональний мережевий пристрій
Server - Системний адміністратор

Рисунок 1.1 – Узагальнена схема мережі «ПП СТЕП 2020»

На всіх ПК є доступ в глобальну мережу Інтернет. ЛОМ (принцип побудови мережі та основні технічні ресурси зображено на рисунку 1.2) організована завдяки кабельної розводки витої пари, топологія зірка, зі швидкістю локального трафіку до 100 Мб/с і шістнадцяти-портового комутатора (залишається дев'ять програмно та апаратно-вільних портів). Для підключення комп'ютерів до мережевого обладнання використовується вита пара CAT 5e. Вихід в глобальну мережу Інтернет здійснюється завдяки маршрутизатору зі швидкістю трафіку 100 Мбит/с.

У кожного комп'ютера свій динамічний IP адрес, назначений маршрутизатором.

Інформаційні потоки: найбільш конфіденційна інформація зберігається на сервері. Також варто відзначити наявність мережевих багатофункціональних пристроїв доступних з любого ПК у мережі при працюючому комп'ютері PC2; PC5; PC6.



PC 1 – Директор
PC 2 – Секретар директора
PC 3 – Помічник бухгалтера
PC 4 – Головних бухгалтер
PC 5 – Дизайнер №1
PC 6 – Дизайнер №2
PC 7 – Головний дизайнер
SW – Комутатор
Router - Маршрутизатор
PR – Багатофункціональний мережевий пристрій
Server - Системний адміністратор

Рисунок 1.2 – Принцип функціонування мережі та основні технічні ресурси

ПЗ, яке потрібно для роботи окремо кожного підрозділу представлено в таблиці 1.2.

Таблиця 1.2 – Програмне забезпечення, встановлене на ПК та сервері

Встановлене програмне забезпечення	PC1	PC2	PC3	PC4	PC5	PC6	PC7	Server
Операційна система								
Microsoft Windows 10	+	+	+	+	+	+	+	-
Windows Server 2019	-	-	-	-	-	-	-	+
Прикладне ПЗ								
Microsoft office 365	+	+	+	+	+	+	+	+
Adobe Acrobat Reader	+	+	+	+	+	+	+	+
Спеціалізоване ПЗ								
Астра конструктор	-	-	-	-	+	+	+	-
Астра розкрій	-	-	-	-	+	+	+	-
Corel Draw	-	-	-	-	+	+	+	-
1С: Підприємство	-	-	+	+	-	-	-	-
Розрахунок заробітної плати в MS Excel	-	-	+	+	-	-	-	-
ПЗ для забезпечення безпеки								
Comodo Internet Security (включає в себе Comodo Firewall)	+	+	+	+	+	+	+	+

Резервне копіювання на підприємстві реалізоване за допомогою програми Acronis Cyber Protect Backup.

1.2 Технології передачі даних

Для передачі даних на фізичному і канальному рівні моделі OSI використовується пакетна технологія Fast Ethernet, що дозволяє передавати дані зі швидкістю 100Мбіт/с. Фізичний інтерфейс – 100TX використовується для передачі даних по одній парі скручених проводів (кручена пари) в кожному напрямку зі швидкістю 100Мбіт/с.

Формує кадр, який далі буде пересилатися через фізичне середовище передачі даних, по прибуттю за призначенням буде підхоплений протоколом TCP/IP. Даний протокол реалізується на рівні обладнання (мережевої карти).

Саме така швидкість забезпечить комфортну роботу всіх користувачів в мережі як між собою так і з сервером.

1.3 Фізична середа передачі даних

Головним фізичним середовищем з передачі даних використовується неекранований 4 жильний кабель типу «вита пара».

Основні характеристики: UTP Cat5e (смуга частот 125 МГц) - 4 жильний кабель, вдосконалена категорія 5, неекранований, швидкість передачі даних - до 100Мбіт/с при використанні двох пар (до 1000Мбіт/с. при використанні чотирьох пар).

Переваги:

- низька вартість;
- висока перешкодостійкість (за рахунок скручених провідників).

Для комутації кабелю до мережевого устаткування (мережева карта, свіч) застосовуються коннектори RJ-45.

1.4 Локальна обчислювальна мережа

Для організації локальної мережі потрібне активне і пасивне мережеве обладнання. До активної відноситься обладнання яке володіє «інтелектуальною» особливістю, наприклад маршрутизатори, комутатори і Wi-Fi маршрутизатори. До пасивного відносяться - кабель, коннектори, патч-кор,

патч-панелі. Для створення локальної мережі кожен комп'ютер повинен володіти мережевою картою.

Для з'єднання робочих місць в мережу застосовуються маршрутизатор та комутатор.

На підприємстві встановлене наступне активне мережеве обладнання:

- комутатор TP-LINK TL-SF1016D 16 портів 10/100 Мбит/с з автопогодженням, с роз'ємами RJ45 (авто-MDI/MDIX);
- маршрутизатор TP-LINK TL-R402M 4 порта LAN 10/100 Мбит/с (Автоматичне визначення/ Auto MDI/ MDIX).

1.5 Визначення класу автоматизованої системи

До того як буде проведено аналіз загроз та буде обґрунтований профіль захищеності необхідно провести класифікацію АС, це робиться згідно НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

Також, спочатку необхідно встановити найвищий гриф секретності інформації яка обробляється в АС – провести категорування, обстеження об'єкту та визначити властивості інформації.

Після того як АС присвоєно класифікаційний рівень, визначаються вимоги до системи безпеки, виходячи з яких приводяться необхідні функціональні послуги та обґрунтовується профіль захищеності. Реалізований профіль захищеності повинен враховувати проведений аналіз загроз, та мінімізувати вірогідність виникнення якоїсь з перерахованих у аналізі загроз загрози.

1.6 Опис системи

АС розташовано в офісі компанії, всім устаткуванням (системний блок, мишка, клавіатура, монітор) присвоєні інвентарні номери.

На ПК реалізовані два облікові записи користувачів:

1) інженер, який виконує обов'язки системного адміністратора;

2) користувач, який працює з програмою середою розробки «Астра Конструктор» та «Астра Розкрій»:

- цей обліковий запис з повними правами є для адміністрування ПК;
- другий з обмеженими правами використовується користувачем програми «Астра Конструктор» та «Астра Розкрій».

Інформація, яка обробляється комп'ютером:

1) відкрита;

2) з обмеженим доступом – конфіденційна (готові проекти).

ІТС - це комп'ютерна мережа, розподілена на порівняно невеликій території в радіусі декількох кілометрів (в межах організації/підприємства, або його підрозділів) і призначена для збору, передачі інформації в межах даної території.

На ПК реалізовані дві облікові записи користувачів з різними правами доступу, На підприємстві є 8 комп'ютерів, які об'єднані між собою в єдину мережу за допомогою мережевого обладнання.

Серед 8 комп'ютерів, 7- робочі станції та один сервер, на якому зберігається вся оброблювана інформація.

На сервері встановлена Windows Server 2019, за допомогою якої і відбувається налаштування інших робочих станцій та встановлення правил розмежування доступу стосовно персоналу, завдяки Active Directory.

Усі комп'ютери входять до єдиного домену "Ustel" і керуються системним адміністратором.

Мережева топологія представляє собою – активну зірку. Оскільки робочі станції об'єднані між собою одним комутатором і керуються сервером.

Нижче приведена таблиця 1.3 з мережевими та фізичними адресами ПК.

Таблиця 1.3 – Мережеві та фізичні адреси обчислюваних засобів

Засіб обчислювальної техніки	IP-адрес	MAC-адрес
ПК1	192.168.1.2	08-00-27-00-5C-6D

ПК2	192.168.1.3	08-00-27-0E-25-B8
ПК3	192.168.1.4	00-DD-88-C7-9A-24
ПК4	192.168.1.5	00-08-A3-BB-CE-04
ПК5	192.168.1.6	00-0D-56-09-FB-D1
ПК6	192.168.1.7	00-12-3f-D4-8D-1B
ПК7	192.168.1.8	40-61-86-E5-3D-E1

1.7 Контрольована зона

Доступ до ПК обмежений і знаходиться під контролем. КЗ обмежене стінами будівлі, територія компанії не огороджена, на дворі можливе неконтрольоване перебування сторонніх осіб.

У будівлі є кімната охоронця та турнікет через який ведеться пропускний режим.

На всіх вікнах будівлі встановлені грати та є пожежна сигналізація.

1.8 Категоріювання об’єкту

Категоріювання на об’єкті проведено відповідно НД ТЗІ 1.6-005-2013.

Категорування проводиться у зв’язку з тим, що система ТЗІ для даного ОІД розробляється і впроваджується вперше, також прийнято рішення про створення КСЗІ.

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

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

Призначена комісія постановила:

1 Серед об’єктів на категоріювання слід виділити наступні загрози: в приміщенні циркулює ІзОД, а саме готовий проект під час обробки, пересилання тощо;

2 В кабінет №1 де циркулює така інформація:

2.1 Інформація в ПЕОМ. За режимом доступу: ІзОД – Гриф конфіденційно;

2.2 Інформація в процесі пересилання на сервер завдяки ЛОМ. За режимом доступу: ІзОД – Гриф конфіденційно.

1.9 Обстеження ІТС «ПП СТЕП 2020»

Обстеження проводиться у зв'язку з тим, що система ТЗІ для даного ОІД розробляється і впроваджується вперше.

Комісія з обстеження розглянула та проаналізувала:

- Схема комп'ютерної мережі (рис. 1.3);
- Генеральний план (рис. 1.4);
- Ситуаційний план (рис. 1.5);
- Схеми електроживлення, освітлення та заземлення;
- Схема опалення та водопостачання;
- Схема пожежної сигналізації;
- План розташування ОТЗ та ДТЗС на ОІД;

Споруда в якій проводилося обстеження окремо розташована, одноповерхова не огороджена на вікнах встановлені грати.

Найближча будівля знаходиться на півночі в 8 метрах, на заході відстань складає 12,5 метрів, на південно-заході до найближчого будинку 11м в і на південно-заході 15м.

У східному напрямку відстань до дороги складає 9,2 метри.

Електроживлення трьох провідне з заземлюючим проводом, підведено від трансформаторної підстанції в щитову, на яку встановлений замок і вона знаходиться під контролем охорони.

Водопостачання та опалення централізоване, підведено з півдня, підключена система радіаторного опалення.

Каналізація підведена з півдня, злив виконується за системою трубних комунікацій.

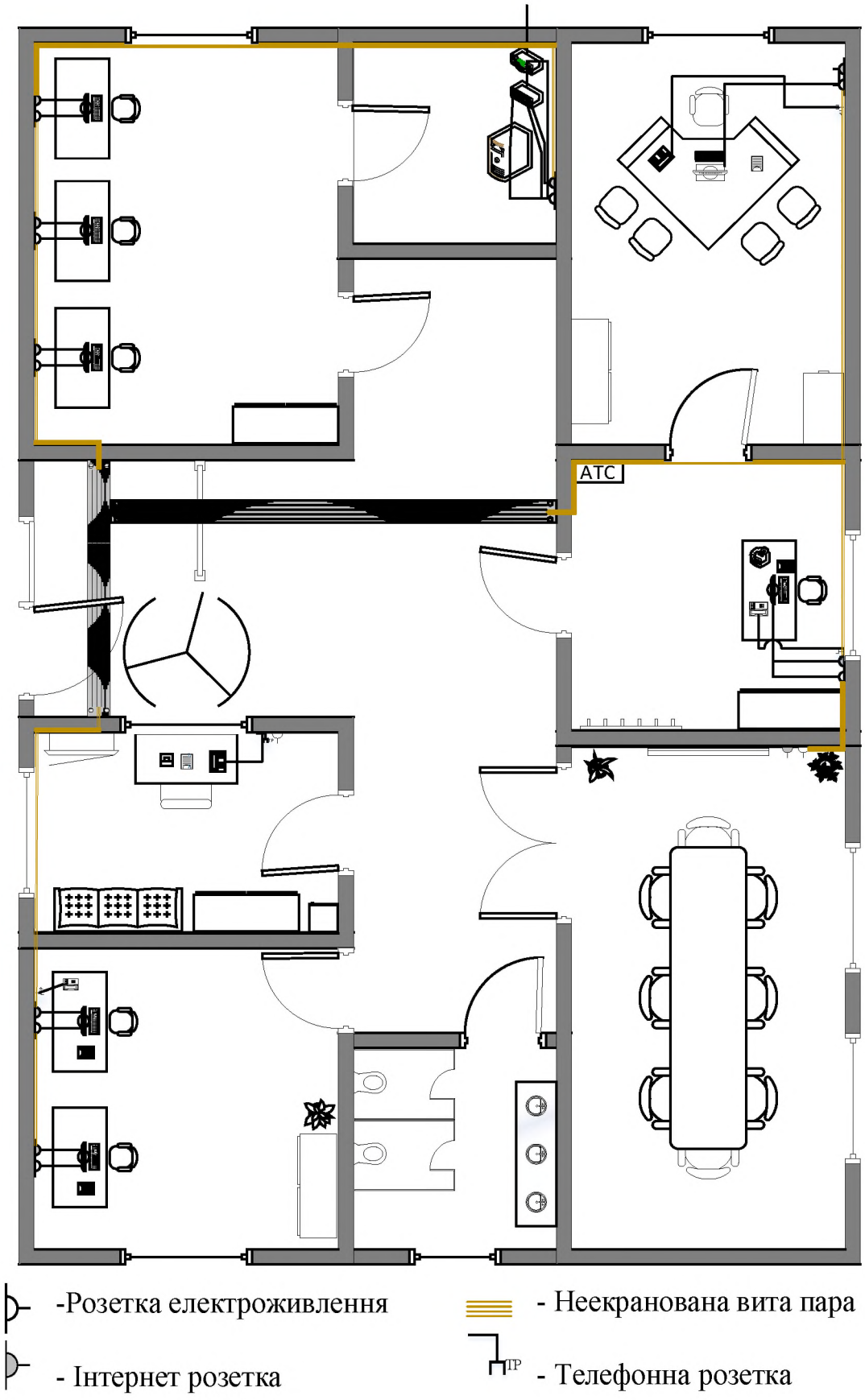


Рисунок 1.3 – Схема комп’ютерної мережі

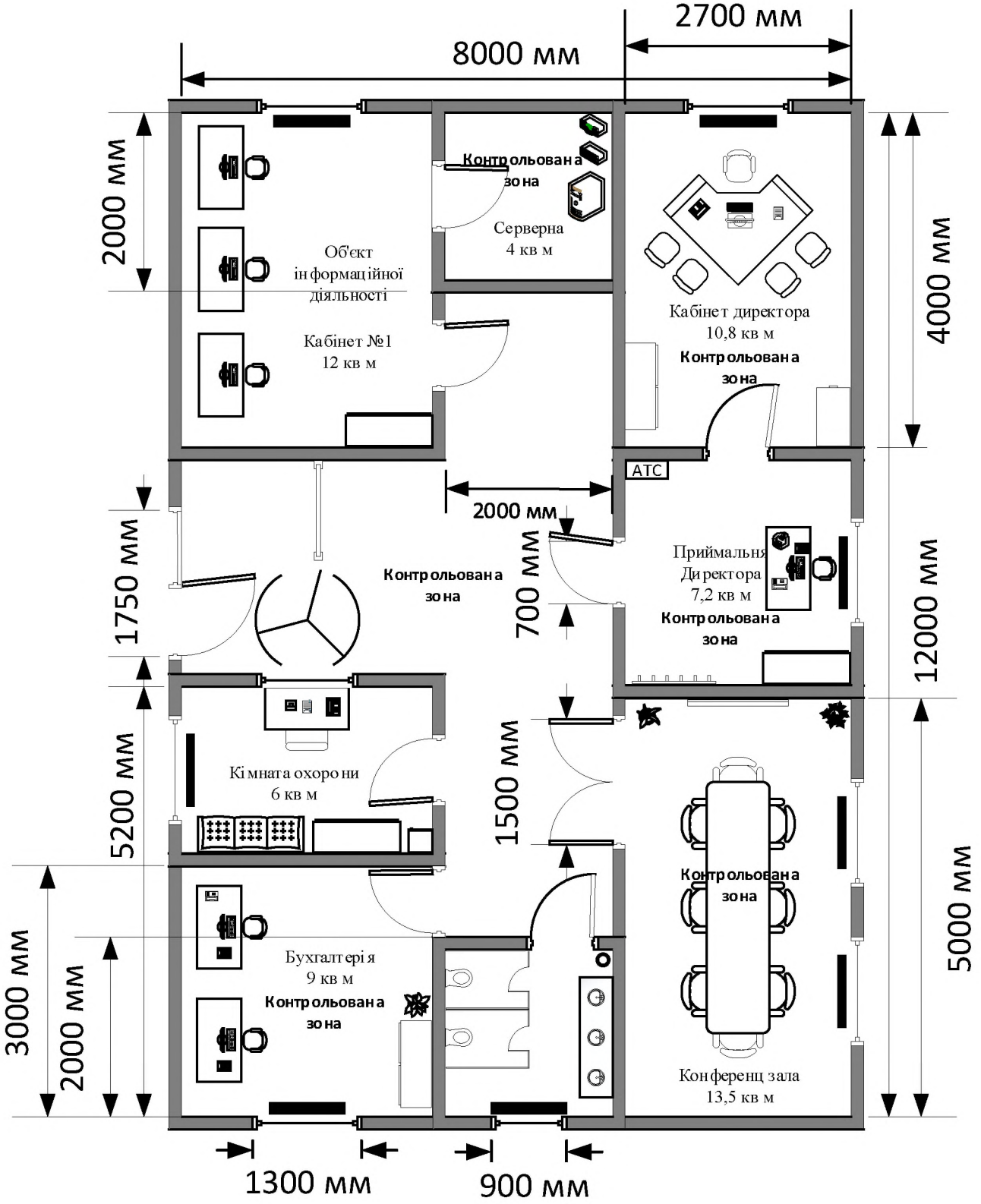


Рисунок 1.4 – Генеральний план

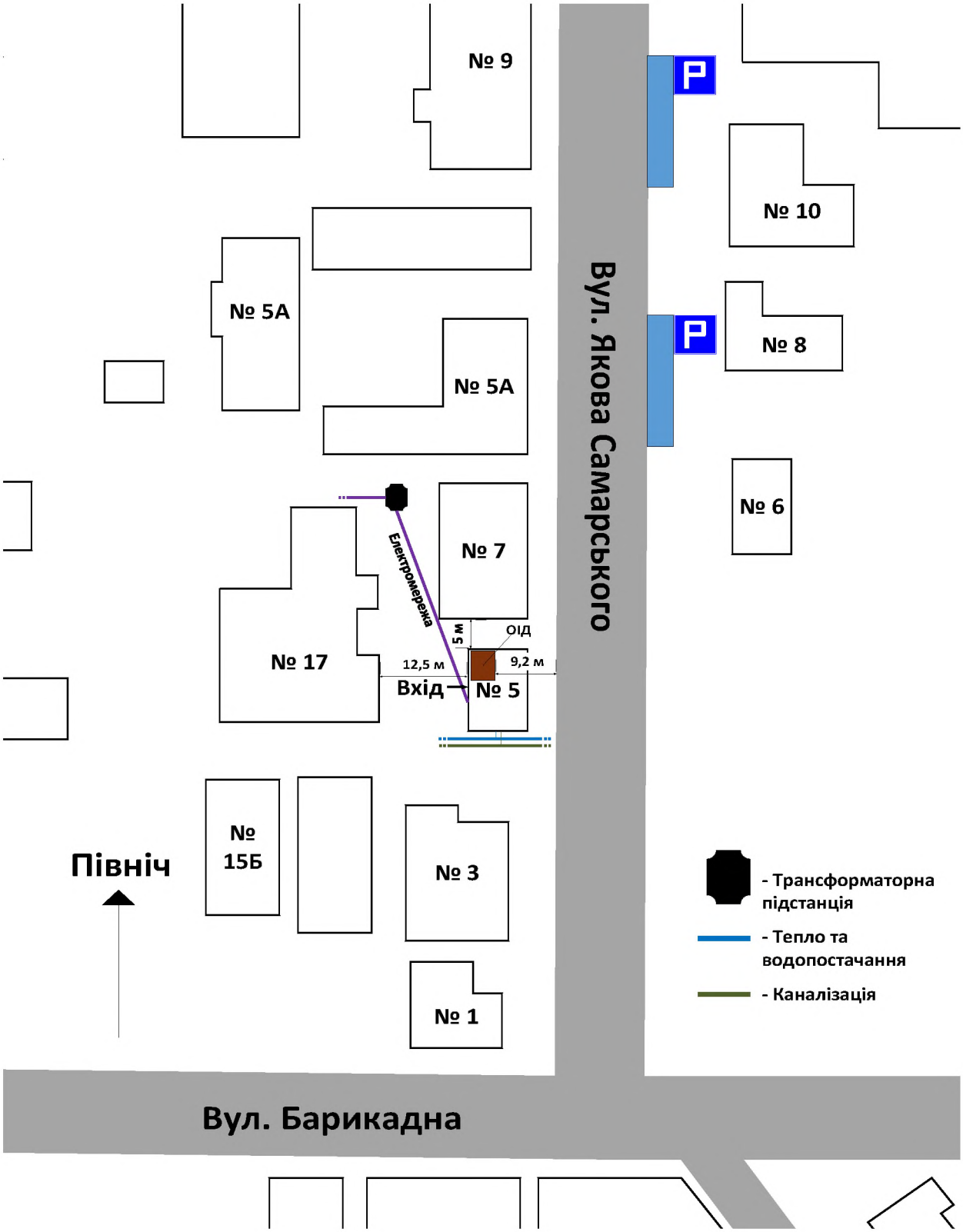
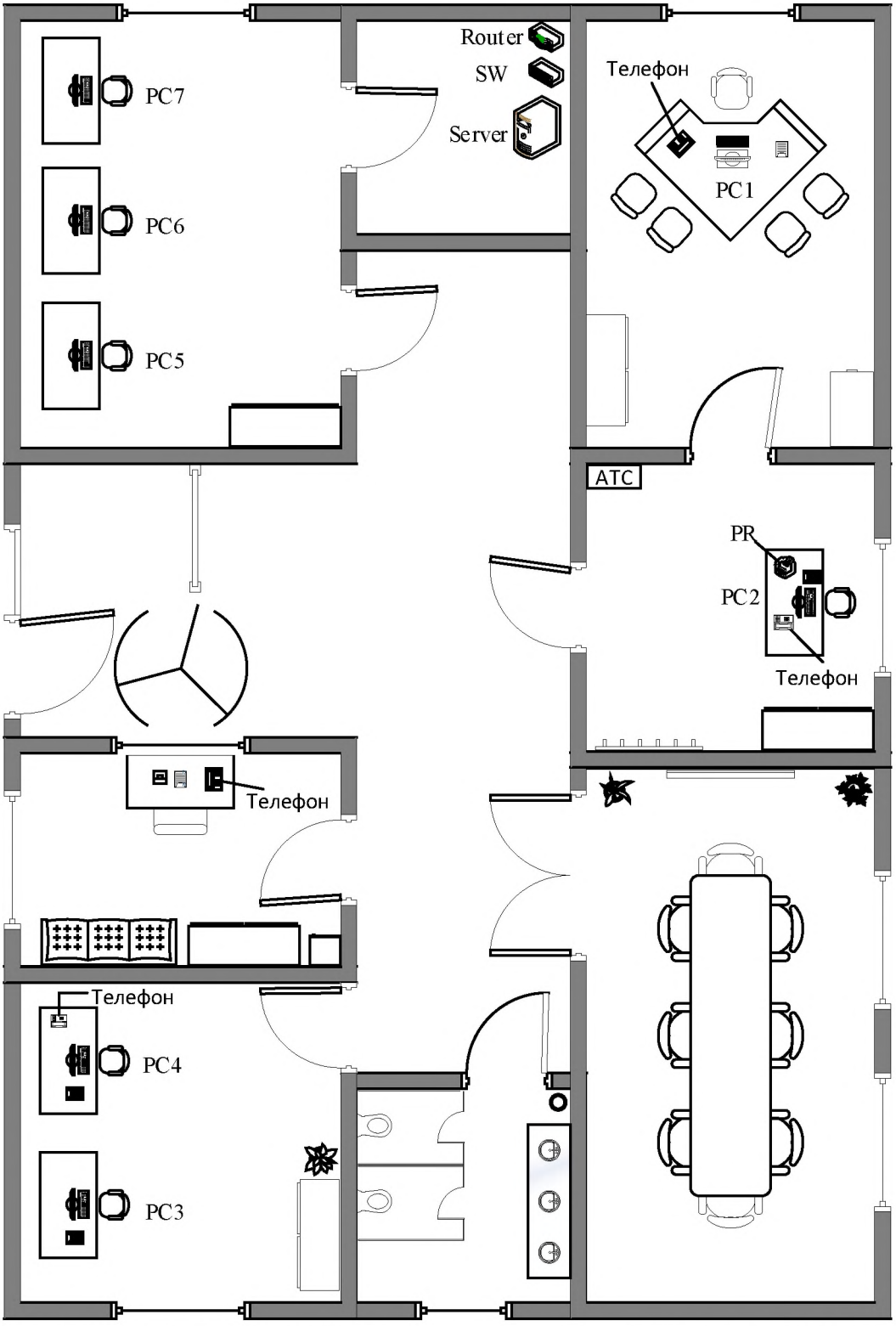


Рисунок 1.5 – Ситуаційний план



PC1-PC7 – Комп'ютери 1-7
SW – Комутатор
Router – Маршрутизатор
Server – Сервер
PR – Багатофункціональний пристрій

Рисунок 1.6 – План розташування ОТЗ та ДТЗ

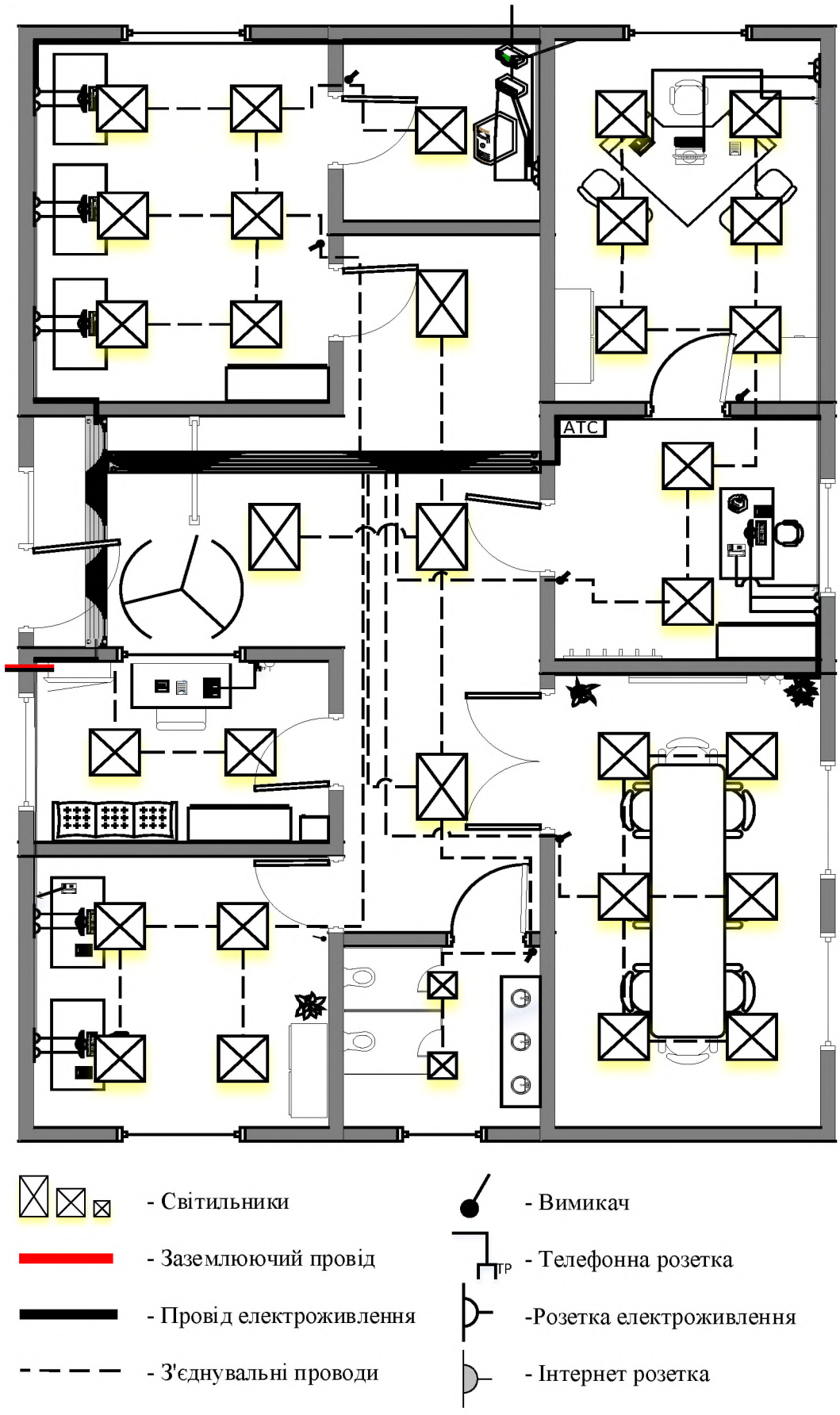


Рисунок 1.7 – Схема електроживлення, освітлення

та заземлення

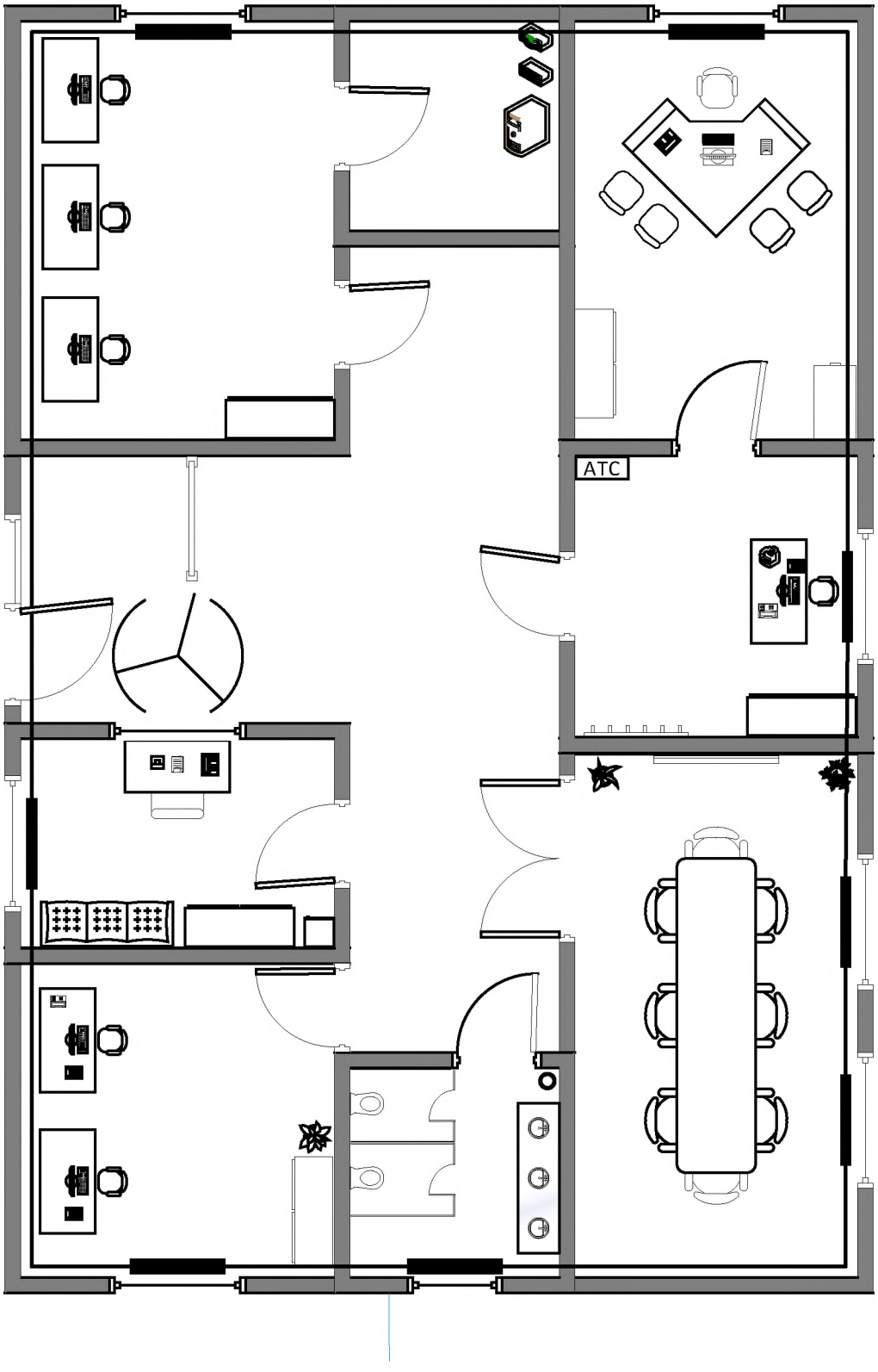
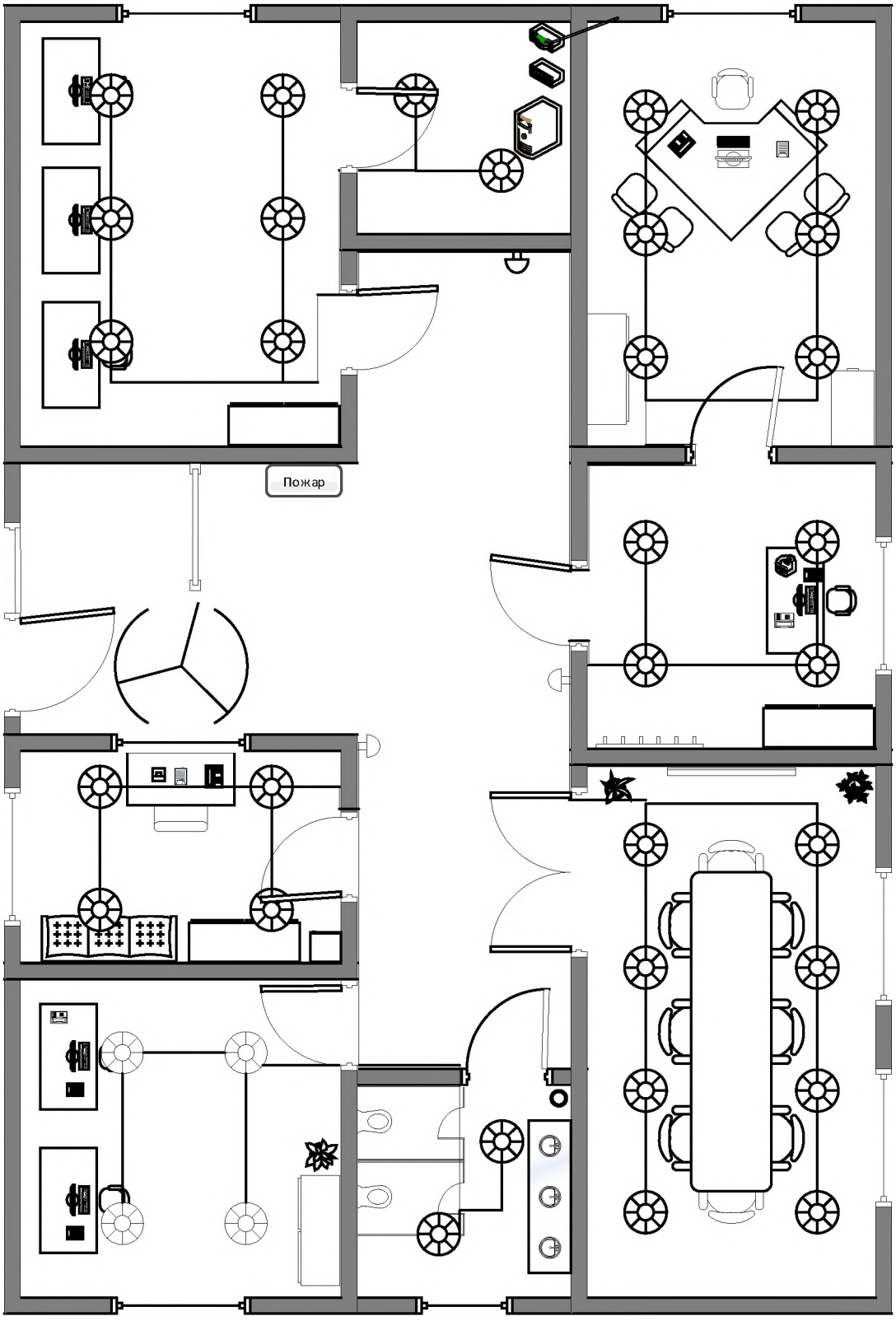


Рисунок 1.8 – Схема опалення та водопостачання



Пожар - Кнопка пожежної тривоги

- Пожежний датчик

- Звуковий оповіщувач

Рисунок 1.9 – Схема пожежної сигналізації

У всій будівлі окрім туалетної кімнати встановлені двостулкові металопластикові вікна розміром 1300*1400 мм, в туалетній кімнаті встановлено вікно розміром 900*900мм.

Також у будівлі встановлені дерев'яні двері товщиною 4 см та розмірами 750*2000 мм. Двері на вході двостулкові металеві розміром 1750*2000 мм, у актовому залі двері двостулкові розміром 1500*2000 мм.

Зовнішні стіни будівлі цегляні товщиною в одну цеглу, внутрішні стіни товщиною в пів цегли.

Штат співробітників складається з директора закладу, секретаря директора, бухгалтерів, дизайнерів, системного адміністратора та охоронця.

Найвищий рівень доступу має директор, нижчий рівень у секретаря.

Рівні доступу до інформації представлені в таблиці 1.5.

Таблиця 1.5 – Рівні доступу

Суб'єкти	Доступ
Адміністрація	Повний доступ
Адміністратор мережі	Підвищений доступ. Налаштування обладнання та ПЗ, створювати документи та встановлювати рівні доступу до документів
Секретар	Створювати акти, оформляти звіти, виводити документацію на друк.
Дизайнери	Можуть вносити і змінювати дані. Розробляють проекти.
Бухгалтери	Переглядати деяку документацію, оформляти звіти.
Охоронець	Не має доступу

Таблиця 1.6 – Основна інформація, яка обробляється у закладі

Інформація	Носій	Режим доступу	Правовий режим	Особи, що мають доступ
Відомості по співробітниках	Електронний та паперовий	Обмежений доступ	Конфіденційна	Адміністрація Бухгалтерія Адміністратор мережі
Проекти	Електронний та паперовий	Обмежений доступ	Конфіденційна	Адміністрація Дизайнери
Бухгалтерські відомості	Електронний та паперовий	Обмежений доступ	Конфіденційна	Адміністрація Бухгалтерія
База клієнтів	Електронний	Обмежений доступ	Конфіденційна	Директор, головний бухгалтер, бухгалтер,

				секретар директора, головний дизайнер
Плани впровадження нового модельного ряду	Електронний та паперовий	Відкритий доступ, за запитом	Відкрита	Всі охочі

Відкрита інформація: Плани впровадження нового модельного ряду, інформація про використання програмного забезпечення, інформація про надання послуг(прайс-лист).

Конфіденційна інформація: персональні дані співробітників і клієнтів компанії, розроблені проекти; бухгалтерські відомості, про укладені договори з клієнтами.

Матриця доступу до інформації приведена в таблиці 1.7.

Таблиця 1.7 – Матриця доступу до інформації

	Відомості по співробітниках	Бухгалтерські відомості	База клієнтів	Проекти	Плани впровадження нового модельного
Директор	c, d, r, w	r	c, d, r, w	r	c, d, r, w
Секретар директора	c, d, r, w	r	c, r, w	-	c, r
Системний адміністратор	-	_	-	-	r
Головний бухгалтер	c, r, w	c, d, r, w	-	-	r
Помічник бухгалтера	c, r, w	c, r, w	-	-	r
Головний дизайнер	-	-	-	c, d, r, w	r
Дизайнер №1	-	-	-	c, d, r, w	c, r
Дизайнер №2	-	-	-	c, d, r, w	c, r

c – створення, d – видалення, r – читання, w – запис.

1.10 Визначення кількості програмних засобів для виконання робіт

На данному підприємстві для роботи дизайнерів використовуються такі програмі засоби як: «Астра Конструктор», «Астра Розкрій» та Corel Draw.

Сімейство програм Астра призначене для конструювання меблів, створення креслень і специфікацій, перевірки розмірів, візуалізації проекту, економного розкрою матеріалів.

Це програма для меблевих фірм і для тих, хто захоплюється виготовленням меблів самостійно для свого будинку. Проектування та виготовлення меблів за індивідуальним замовленням дуже поширене.

Астра Конструктор Меблів – програма, що дозволяє виконувати проектування виробу, викреслювати окремі деталі та зберігати їх у бібліотеці. Працюючи з програмою, можна автоматично перевірити, як стикуються деталі.

Можна «зібрати» на моніторі, а потім і в реальності, нові вироби з деталей, креслення яких збережені в бібліотеці. Комплект розроблені деталі для конкретного виробу - це вихідна інформація для іншої програми - Астра Розкрій.

Астра Розкрій - це програма, призначена для підбору варіантів економного розкрою стандартних листів ДСП, фанери або інших листових матеріалів. У базі даних зберігаються залишки матеріалів, які можуть в подальшому бути використані для іншого замовлення.

Програма передбачає безпосередню роботу в системі наступних типів користувачів:

1 Адміністратор системи;

2 Директора;

3 Головний дизайнер;

4 Дизайнери.

1.11 Теоретичні відомості про програмний комплекс «Астра»

Програмний комплекс «Астра» є найрасповсюдженим ПЗ для розробки дизайну меблів на території України.

Астра – вільне інтегроване середовище. Розвивається і підтримується ТОВ ТЕХНОС.

До сімейства програм Астра входять такі программи як Astra S-Nesting – розкрій диталей довільної форми, Astra Cutting – управління вирізкою на розкрійних станках.

Необхідність в подібному комплексі ПЗ, як «Астра Конструктор» та «Астра Розкрій», виникла сучасними вимогами та спрямоване на швидке, просте, якісне проектування меблів, та підготовки документації для виготовлення меблів.

Проект «Астра» працює з 1999 року. Розробник ТОВ "Технос" Україна.

Програма «Астра конструктор» є у таких версіях як: Професійна версія, стандартна версія, старт версія, домашня версія.

Програма «Астра розкрій» є у таких версіях як: Професійна версія, базова версія, базова версія + модуль розрахунків та обліку залишків.

Для інсталяції (дана програма встановлюється тільки в корінь каталогу C://) ПЗ на демонстраційний термін достатньо завантажити з офіційного сайту astrades24-setup-demo.exe інсталятор програми «Астра конструктор» та astra-nesting-setup5 інсталятор програми «Астра розкрій». Після запуску одного з інсталяторів відкривається стандартне вікно інсталятора, де користувачеві необхідно прийняти ліцензійну угоду, та вибрати компоненти які будуть встановлені. Після встановлення ПЗ ними одразу можна користуватися.

1.12 Супровід та оновлення ПЗ

Програма оновлюється приблизно кожні півтора місяця, немає фіксованої дати, оновлення доповнює, змінює, оптимізує роботу ПЗ та/або виправляє помилки.

Супровід також на високому рівні, є форум, де можна знайти досить багато інформації або задати питання, також можна отримати допомогу по електронній пошті. Підтримка користувачів організована за допомогою кількох міських телефонів, стільникового телефону, електронної пошти, форми зворотного зв'язку на сайті.

1.13 Висновок. Постановка задач

В першій частині роботи було проведено обстеження об’єкта інформаційної діяльності. Проведено категоріювання об’єкта, проаналізовано циркулюючу інформацію та засоби її обробки. На основі отриманої інформації необхідно розробити системи захисту інформації інформаційно-комунікаційної системи приватного підприємства "Степ 2020", розробити модель загроз та модель порушника на їх основі проаналізовані можливі ризики.

В спеціальній частині роботи необхідно вирішити наступні задачі:

- розглянути існуючу систему безпеки;
- розробити модель загроз та модель порушника на їх основі проаналізувати можливі ризики;
- обрати функціональний профіль захищеності;
- запропонувати засоби захисту, що реалізують функціональний профіль захищеності.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Технічне завдання

Найменування і сфера застосування

Найменування: Розробка системи захисту інформації в інформаційно-телекомунікаційній системі приватного підприємства "Степ 2020"

Призначення розробки

Призначення – є розробка підсистеми захисту від несанкціонованого доступу інформаційно-комунікаційної системи підприємства, яка дозволить забезпечити підвищення рівня безпеки інформаційних ресурсів.

Порядок контролю і приймання

Контроль та здавання розробки керівникові роботи здійснюється на підставі оформлення і передачі керівникові пояснювальної записки.

Економічний розділ

У даній частині необхідно привести розрахунки щодо доцільності використання запропонованих засобів та заходів захисту інформаційно-комунікаційної системи підприємства.

Етапи виконання робіт

- проаналізувати можливі загрози безпеки інформації;
- зробити аналіз нормативних документів у сфері інформаційної безпеки;
- обстежити локальну мережу підприємство;
- вибрати функціональний профіль захищеності і клас АС;
- скласти модель порушника;
- скласти модель загроз для підприємства;
- запропонувати заходи щодо запобігання НСД доступу в ІКС підприємства;
- впровадити розроблені засоби та заходи;
- провести випробування і проаналізувати отримані результати;
- підготувати і передати технічну документацію для впровадження;
- розрахувати економічну ефективність розробки;
- передати записку пояснення на рецензування.

2.2 Модель порушника

Порушник – це особа, яка може отримати доступ до роботи з включеними в склад АС засобами. Вона може помилково, унаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби здійснити спробу виконати операції, які можуть призвести до порушення властивостей інформації.

Згідно НД ТЗІ 1.1-003-99, модель порушника – абстрактний формалізований або неформалізований опис порушника. Посилаючись на НД ТЗІ 1.4-001-2000, вона повинна визначати:

– можливу мету порушника та її градацію за ступенями небезпечності для АС;

– категорії осіб, з числа яких може бути порушник;

– припущення про кваліфікацію порушника;

– припущення про характер його дій.

Внутрішні порушники:

– ПВ1 – директор;

– ПВ2 – бухгалтер та його помічник;

– ПВ3 – секретар директора;

– ПВ4 – головний дизайнер;

– ПВ5 – системний адміністратор;

– ПВ6 – дизайнери;

– ПВ7 – охоронець.

Зовнішні порушники:

– ПЗ1 – клієнти;

– ПЗ2 – технічний персонал;

– ПЗ3 – конкуренти.

Класифікація порушників

За рівнем можливостей:

– РМ1 – найнижчий рівень, використовує лише агентурні методи одержання відомостей;

– РМ2 – можливість запуску фіксованого набору програм, що реалізують заздалегідь передбачені функції обробки інформації;

– РМ3 – можливість створення і запуск власних програм з новими функціями обробки інформації;

– РМ4 – повний обсягом можливостей осіб, що здійснюють проєктування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

Рівень знань про АС:

– РЗ1 – володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

– РЗ2 – володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

– РЗ3 – володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проєктування та експлуатації АС;

– РЗ4 – володіють інформацією про функції та механізм дії засобів захисту.

Мета порушника:

– МЕ1 – отримання необхідної інформації у потрібному обсязі та асортименті;

– МЕ2 – мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами;

– МЕ3 – нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

За місцем здійснення дій:

– МД1 – без одержання доступу на контрольовану територію організації (АС);

– МД2 – з одержанням доступу на контрольовану територію;

– МД3 – з одержанням доступу до робочих місць кінцевих користувачів АС;

– МД4 – з одержанням доступу до місць накопичення і зберігання даних.

Модель порушника зображена в таблиці 2.2.

Таблиця 2.2 – Модель порушника

Позначення	Рівень можливостей	Рівень знань	Мета порушника	Місце здійснення дій	Рівень загрози
Внутрішні порушники					
ПВ1	РМ3	РЗ1	МЕ1,МЕ2,МЕ3	МД3,МД4	4
ПВ2	РМ2	РЗ1	МЕ2,МЕ3	МД3	3
ПВ3	РМ2	РЗ1	МЕ3	МД3	2
ПВ4	РМ2	РЗ1	МЕ3	МД3	2
ПВ5	РМ4	РЗ4	МЕ1,МЕ2,МЕ3	МД4	5
ПВ6	РМ2	РЗ1	МЕ1	МД2	3
ПВ7	РМ2	РЗ1	МЕ1	МД3	2
Зовнішні порушники					
ПЗ1	РМ1	РЗ1	МЕ1,МЕ3	МД2	2
ПЗ2	РМ4	РЗ3	МЕ1,МЕ2	МД3,МД4	5
ПЗ3	РМ1	РЗ1	МЕ1,МЕ2,МЕ3	МД2	2

Рівень загрози:

1 – низький;

2 – середній;

3 – високий;

4 – дуже високий;

5 – Критичний.

2.3 Модель загроз інформації ІТС ПП «СТЕП 2020»

Носіями загроз безпеки інформації є джерела загроз. У якості джерел загроз можуть виступати як суб'єкти (особистість), так і об'єктивні прояви.

Причому, джерела загроз можуть перебувати як усередині організації, що захищається, – внутрішні джерела, так і поза неї – зовнішні джерела. Розподіл

джерел на суб'єктивні й об'єктивні виправдане виходячи із приводу провини або ризику збитку інформації. А розподіл на внутрішні й зовнішні джерела виправдане тому, що для однієї й тієї ж загрози методи парирування для зовнішніх і внутрішніх джерел можу бути різними.

Згідно НД ТЗІ 1.1-003-99, модель загроз – абстрактний, формалізований чи неформалізований опис методів і засобів здійснення загроз.

2.3.1 Види джерел загроз

Всі джерела загроз можна розділити на три групи:

- антропогенні;
- техногенні;
- стихійні лиха.

а) антропогенними джерелами загроз безпеки інформації виступають суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини. Тільки в цьому випадку можна говорить про заподіяння збитку. Ця група найбільш велика й становить найбільший інтерес із погляду організації захисту, тому що дії суб'єкта завжди можна оцінити, спрогнозувати й вжити адекватні заходи. Методи протидії в цьому випадку керовані й прямо залежать від волі організаторів захисту інформації.

б) техногенні джерела загроз менш прогнозовані, прямо залежать від властивостей техніки і тому вимагають особливої уваги. Даний клас джерел загроз безпеки інформації особливо актуальний в сучасних умовах.

в) стихійні джерела загроз об'єднують обставини, що становлять непереборну силу, такі обставини, які мають об'єктивний і абсолютний характер, що поширюється на всіх. До непереборної сили в законодавстві і договірній практиці відносяться стихійні лиха або інші обставини, які неможливо передбачити чи неможливо запобігти при сучасному рівні людського знання і можливостей. Такі джерела загроз абсолютно не піддаються прогнозуванню та тому заходи захисту від них повинні застосовуватися завжди. До них відносяться: пожежі; землетрусу; повені; урагани; різні непередбачені обставини; інші форс-мажорні обставини.

Під час розробки моделі загроз були посилання на наступні документи: НД ТЗІ 1.4-001-2000 Типове положення про Службу Захисту Інформації; НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

Модель загроз представлена в таблиці 2.1.

Таблиця 2.1 – Модель загроз

Загрози	Рівень реалізації загрози	Властивість, що порушується	Рівень шкоди
Антропогенні загрози			
Крадіжка ПЕОМ	3	К, Ц, Д	5
Крадіжка носіїв інформації	4	К, Ц, Д	5
Модифікація (ПЗ та інформації)	4	Ц, Д.	5
Електронна інф.			
Паперова форма			
Зовнішні			
Кримінальні структури	3	К,Ц,Д	5
Недобросовісні партнери	3	К	4
Технічний персонал	2	Д, Ц	4
Внутрішні			
Працівники	4	К,Д	3
Другорядний персонал (прибиральниця,охорона)	2	К	1
Техногенні загрози			
Порушення працездатності (системи обробки інформ. носіїв ін.форм.)	3	Д	3
Зовнішні			
Комп'ютерні віруси	5	К, Ц, Д	4
Неякісні ТЗОІ	3	К, Ц, Д	3
Неякісне ПЗ	3	К, Ц, Д	5

Внутрішні			
Вихід із ладу апаратно-програмних засобів	4	Д	4
Збій системи електроживлення	3	Д	4
Стихійні джерела загроз			
Пожежа	3	К, Ц, Д	5
Землетрус	2	К, Ц, Д	5
Повінь	1	К, Ц. Д	5
Ураган	1	К, Ц, Д	5
Нез`ясовані явища	1	К, Ц, Д	5

Рівень реалізації загрози : 1 – 5

1 – низька;

2 – середня;

3 – висока;

4 – дуже висока;

5 – неприпустимо висока.

Роз'яснення до рівня реалізації загрози

1 – рівень загрози низький, практично неможливий (ймовірність у 0-30% випадків);

2 – рівень загрози середній, але в окремих випадках можливий (ймовірність у 30-50% випадків);

3 – загроза висока в 50% випадків;

4 – дуже висока ймовірність виникнення загрози порушення (ймовірність у 50-80% випадків);

5 – неприпустимо висока загроза, неминуча так як ймовірність прямую до 100 (ймовірність у 80-90% випадків).

Рівень шкоди : 1 – 5

1 – низький;

2 – середній;

3 – високий;

4 – дуже високий;

5 – критичний.

Роз'яснення до рівень шкоди:

Критичний та дуже високий - без неї робота суб'єкта зупиняється;

Високий - без неї можна працювати деякий час, але рано чи пізно вона знадобиться;

Середній та низький - без неї можна працювати, але її використання заощаджує ресурси.

2.4 Аналіз ризиків

Важливою характеристикою небезпеки, а точніше мірою можливої небезпеки, є частота, з якою вона може проявлятись або ризик.

Ризик — функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Аналіз ризику — процес визначення загроз безпеці інформації та їх характеристик, слабких сторін КСЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеню їх прийнятності для експлуатації АС.

Ймовірність реалізації загрози (Y):

0,25 – низька; 0,5 – середня; 0,75 – висока; 1 – дуже висока.

Рівень збитків (Q):

1 – низький; 2 – середній; 3 – високий; 4 – дуже високий; 5 – неприпустимо високий.

Рівень ризику (R):

1 – 2 низький;

2 – 3 середній;

3 – 4 високий;

4 – 5 дуже високий.

Аналіз ризиків приведено в таблиці 2.3.

Таблиця 2.3 – Аналіз ризиків

Інформація	Джерело загрози	Загроза	Вразливість	Ймовірність реалізації	Рівень збитків	Рівень ризику	Порушення властивості
Про співробітників і клієнтів компанії	кримінальні структури; недобросовісні партнери; технічний персонал; працівники	несанкціоноване ознайомлення	порушення правил розмежування доступу	0,5	2	R=2*0,5=1	К
	-	крадіжка	залишення паперів, чи носіїв без догляду	0,75	3	R=0,75*3=2,25	К,Ц,Д
	-	комп'ютерні віруси	відсутність антивірусного програмного забезпечення чи його збій	1	3	R=1*3=3	Ц,Д
Про надання послуг (прайс-лист)	клієнти; недобросовісні партнери; працівники	знищення	залишення паперів без догляду	0,5	2	R=0,5*2=1	Ц,Д

Продовження таблиці 2.3

Інформація	Джерело загрози	Загроза	Вразливість	Ймовірність реалізації	Рівень збитків	Рівень ризику	Порушення властивості
Про фінансові операції	кримінальні структури; недобросовісні партнери; технічний персонал; працівники.	неякісне ПЗ неякісні ТЗОІ	помилки програмного коду; збій технічних засобів.	0,25	4	R=0,25*4=1	Ц,Д
	-	модифікація	порушення правил розмежування доступу	0,5	4	R=0,5*4=2	Ц
	-	крадіжка	залишення паперів, чи носіїв без догляду	0,75	5	R=0,75*5=3,75	К,Ц,Д
Правила про розпорядок дня	клієнти; недобросовісні партнери; працівники.	модифікація	порушення правил розмежування доступу.	0,5	2	R=0,5*2=1	Ц

Продовження таблиці 2.3

Інформація	Джерело загрози	Загроза	Вразливість	Ймовірність реалізації	Рівень збитків	Рівень ризику	Порушення властивості
Інформація про укладені договори страхування з клієнтами	кримінальні структури; недобросовісні партнери; технічний персонал; працівники	збій системи електроживлення	пошкоджена проводка; відсутність джерела безперебійного живлення	0,5	5	R=0,5*5=2,5	Ц,Д
	-	пожежа	пошкоджена проводка	0,25	5	R=0,25*5=1,25	Ц,Д
Інформація про використання програмного забезпечення	клієнти; недобросовісні партнери; працівники	модифікація; знищення	слабкі паролі від облікового запису; порушення правил розмежування доступу	0,25	2	R=0,25*2=0,5	Ц,Д

Продовження таблиці 2.3

Інформація	Джерело загрози	Загроза	Вразливість	Ймовірність реалізації	Рівень збитків	Рівень ризику	Порушення властивості
Про рух грошових засобів	кримінальні структури; Недобросовісні партнери; технічний персонал; Працівники	модифікація; крадіжка;	слабкі паролі від облікового запису; залишення паперів, чи носіїв без догляду	0,5	4	R=0,5*4=2	К,Ц,Д
	-	крадіжка ТЗОІ	недбалість охоронців;	0,25	4	R=0,25*4=1	К,Ц,Д
	-	комп'ютерні віруси	відсутність антивірусного програмного забезпечення, чи його збій	1	4	R=1*4=4	Ц,Д

Продовження таблиці 2.3

Інформація	Джерело загрози	Загроза	Вразливість	Ймовірність реалізації	Рівень збитків	Рівень ризику	Порушення властивості
Про заробітну плату	кримінальні структури; недобросовісні партнери; технічний персонал; працівники	модифікація; знищення	порушення правил розмежування доступу; слабкі паролі від облікового запису;	0,75	3	R=0,75*3=2,25	Ц,Д
	-	несанкціонований перегляд;	порушення правил розмежування доступу	0,5	3	R=0,5*3=1,5	К
	-	комп'ютерні віруси	відсутність антивірусного програмного забезпечення, чи його збій	1	4	R=1*4=4	Ц,Д

Продовження таблиці 2.3

Інформація	Джерело загрози	Загроза	Вразливість	Ймовірність реалізації	Рівень збитків	Рівень ризику	Порушення властивості
Про власний капітал	кримінальні структури; недобросовісні партнери; технічний персонал; працівники	модифікація; знищення	слабкі паролі від облікового запису; порушення правил розмежування доступу	0,25	4	R=0,25*4=1	Ц,Д
	-	несанкціонований перегляд	порушення правил розмежування доступу;	0,5	3	R=0,5*3=1,5	К
	-	комп'ютерні віруси	відсутність антивірусного програмного забезпечення, чи його збій	1	4	R=1*4=4	Ц,Д

2.5 Вибір функціонального профілю захищеності

Відповідно НД ТЗІ 2.5-005-99, автоматизована система, що забезпечує функціонування автоматизованої системи приватного підприємства «СТЕП 2020», представляє собою АС 3 класу, тобто розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

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

Згідно з 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. На основі типових умов функціонування і класу системи був обраний наступний стандартний профіль захищеності:

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

Позначення послуг:

1 КД — довірча конфіденційність;

2 КА — адміністративна конфіденційність;

3 КО — повторне використання об'єктів;

4 КВ — конфіденційність при обміні;

5 ЦД — довірча цілісність;

6 ЦА — адміністративна цілісність;

7 ЦО — відкат;

8 ЦВ — цілісність при обміні;

9 ДР — використання ресурсів;

10 ДВ — відновлення після збоїв;

11 НР — реєстрація;

12 НИ — ідентифікація і автентифікація;

13 НК — достовірний канал;

14 НО — розподіл обов'язків;

15 НЦ — цілісність КЗЗ;

16 НТ — самотестування;

17 НВ — автентифікація при обміні.

2.5.1 Критерії конфіденційності

КД-2. Базова довірча конфіденційність:

– політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС;

– КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта користувача, процесу і захищеного об'єкта;

– запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта;

– КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначати конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта;

– КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначати конкретних користувачів і/або групи користувачів, які мають право ініціювати процес;

– права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

Здійснюється за допомогою ActiveDirectory.

КА-2. Повна адміністративна конфіденційність:

– політика адміністративної конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС;

– КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта користувача і захищеного об'єкта користувача, процесу і захищеного об'єкта;

– запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження;

– КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта;

– КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес;

– права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

Здійснюється за допомогою ActiveDirectory.

КО-1. Повторне використання об'єктів:

– політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС;

– перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані;

– перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Після завершення роботи, користувач повинен вимкнути комп'ютер, або скористатися наявним програмним засобом для очищення оперативної пам'яті, в даному випадку – Ainvo Memory Cleaner.

КВ-2. Базова конфіденційність при обміні:

– політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься;

– політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності;

– КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається;

– запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження;

– запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу;

– запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.

Здійснюється за допомогою розмежування прав доступу (групові політики).

2.5.2 Критерії цілісності

ЦД-1. Мінімальна довірча цілісність:

– політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься;

– КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта;

– запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта;

– КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт;

– права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

Здійснюється за допомогою розмежування прав доступу (групові політики).

ЦА-2. Базова адміністративна цілісність:

– політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься;

– КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта;

– запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження;

– КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити: конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт;

– КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес;

– права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

Здійснюється за допомогою розмежування прав доступу (групові політики).

ЦО-1. Обмежений відкат:

– політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься;

– повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Відновлення системи.

ЦВ-2: Базова цілісність при обміні:

– КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається а також фактів його видалення або дублювання;

– запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу;

– запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу;

– запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

Засоби захисту Internet Access Monitor.

2.5.3 Критерії доступності

ДР-1. Квоти:

– політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься;

– політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу;

– запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

Квотування засобами ОС.

ДВ-1. Ручне відновлення:

– політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки;

– повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС;

– після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження;

– повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування.

Відновлення системи.

2.5.4 Критерії спостережності

НР-2. Захищений журнал:

– політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються;

– КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки;

– журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення

користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події;

– КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування;

– адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Використовується вбудований журнал реєстрації Windows.

НИ-2. Одиночна ідентифікація і автентифікація:

– політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ;

– перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен;

– автентифікувати цього користувача з використанням захищеного механізму;

– КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

Реєстрація користувачів відбувається за допомогою ActiveDirectory.

НК-1. Однонаправлений достовірний канал:

– політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ;

– достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

Реалізується за допомогою протоколу аутентифікації Password Access Protocol – доступ по паролю.

НО-2. Розподіл обов'язків адміністраторів:

– політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції;

– політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора;

– функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі;

– користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

На підприємстві є адміністратор, який виконує функції системного адміністратора, та адміністратора безпеки.

НЦ-2. КЗЗ з гарантованою цілісністю:

– політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів;

– КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування;

– повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Реалізується за допомогою серверної операційної системи Windows Server 2019.

НТ-2. Самотестування при старті:

– політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ;

– КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні

виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

Процедура POST (Poweronself-test), Memtest, HDDScan.

НВ-1: Автентифікація вузла:

– політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ;

– КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ з використанням захищеного механізму;

– підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

Мас адреса, ip адреса, підтвердження ідентичності виконується на підставі протоколу Password Access Protocol – доступ по паролю.

2.6 Запропоноване програмне забезпечення

Всі критерії стандартного функціонального профілю захищеності 3.КЦД.2, крім НТ-2; КО-1; ЦВ-2 та НК-1 відбувається за допомогою вже втановленного ПЗ (Comodo Internet Security) або налаштуванням служби Active Directory, за допомогою розмежування прав доступу (групові політики) та при використані інших вбудованих служб до операційної системи Microsoft Windows 10 яка використовується на підприємстві. В свою чергу ОС Windows 10 відповідає вимогам НД з ТЗІ в обсязі функцій, зазначених у документі “Державна експертиза за критеріями технічного захисту інформації.

Таким чином потрібно забезпечити Самотестування при старті (НТ-2), Базову цілісність при обміні даних (ЦВ-2), Повторне використання об'єкту (КО-1) та Однонапрямлений достовірний канал (НК-1) для забезпечення виконання всього функціонального профілю захищеності 3.КЦД.2.

Для здобуття необхідного рівня безпеки та виконання критеріїв профілю захищеності на підприємстві пропонується встановити нове програмне забезпечення.

2.6.1 Діагностика носіїв інформації

Для забезпечення критерію НТ-2 (Самотестування при старті) виконуємо вибір програмного забезпечення HDDScan призначеної для діагностики носіїв інформації та Memtest86+. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

Самотестування, що повинна реалізується у КЗЗ, виконується за допомогою BIOS материнської плати. Це системи POST (Power-On Self-Test) системи само тестування при старті.

HDDScan - це програма для низькорівневої діагностики накопичувачів HDD в операційній системі Windows.

На рисунку 2.2 представлено головне вікно програми HDDScan.

Рисунок 2.2 - Головне вікно програми

На рисунку 2.3 зображено вікно тестів програми HDDScan.

Рисунок 2.3 - Вікно тестів

Це вікно містить чергу всіх тестів, що запускаються програми, а також монітор температури. Менеджер дозволяє видаляти тести з черги, ставити на паузу або зупиняти. Подвійний клік на записи в черзі викликає вікно з інформацією про поточної задачі.

На рисунку 2.4 зображено інформацію про завдання яке виконується.

Рисунок 2.4 - Інформації про завдання

Вікно містить інформацію про тест, дозволяє ставити тест на паузу або зупиняти, а також генерує звіт.

Вкладка Graph містить інформацію залежності швидкості тестування від номера блоку, представлену у вигляді графіка, що представлена на рисунку 2.5.

Рисунок 2.5 - Вкладка Graph

На рисунку 2.6 відображено вміст вкладки Report.

Рисунок 2.6 - Вкладка Report

Вкладка Report містить інформацію про тест і перераховує всі блоки

MemTest86 - утиліта призначена для тестування надійності роботи оперативної пам'яті. При тестуванні оцінюється здатність пам'яті записувати і зчитувати дані.

Рисунок 2.7 містить інформацію про вікно встановлення утіліти MemTest86.

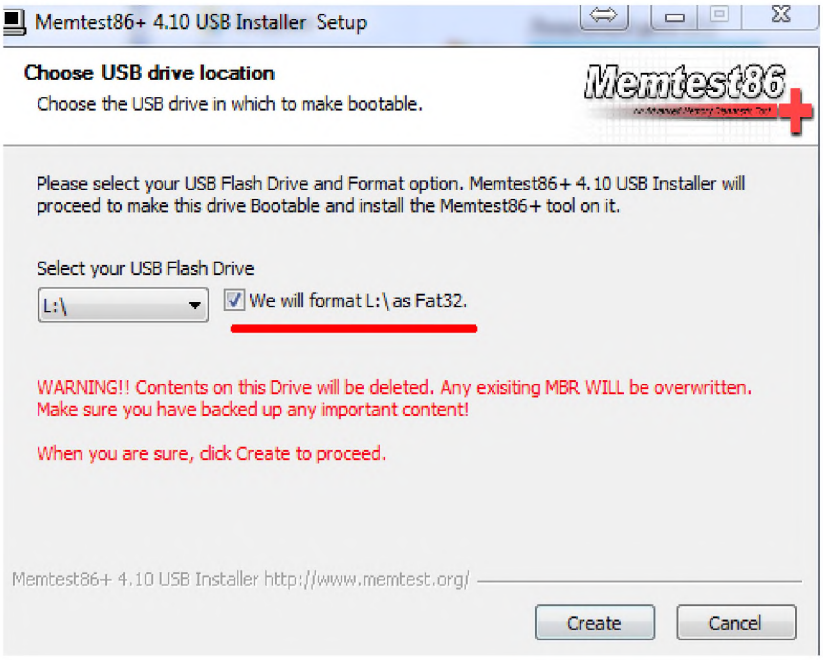


Рисунок 2.7 - Вікна встановлення утиліти MemTest86

Програма тестує оперативну пам'ять циклічно, тобто у неї є декілька тестів (Всього їх дев'ять), які вона ганяє по колу. І як тільки одине коло буде пройдено, то внизу екрана з'явиться повідомлення «***** Pass complete, (no, 1, 2, 10...) errors, press Esc to exit*****».

Якщо по закінченні тесту видається повідомлення, як на рисунку 2.8, показано, що пам'ять не містить несправних блоків.

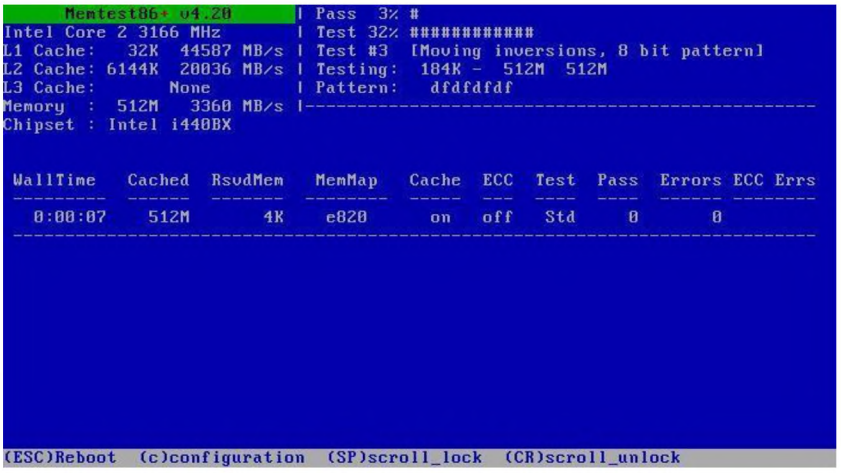


Рисунок 2.8 - Пам'ять не містить несправних блоків

2.6.2 Програмний засіб для очищення оперативної пам'яті

Для повторного використання об'єктів необхідно щоб перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Для цього після завершення роботи, користувач повинен вимкнути комп'ютер, або скористатися наявним програмним засобом для очищення оперативної пам'яті.

Ainvo Disk Cleaner призначений для видалення з жорсткого диска або дисків, якщо їх кілька) непотрібних файлів. До таких файлів відносяться різні тимчасові файли, логи, збережені попередні версії документів, таблиці з ескізами графічних файлів і багато іншого.

Рисунок 2.9 відображає вікно програми Ainvo Disk Cleaner.

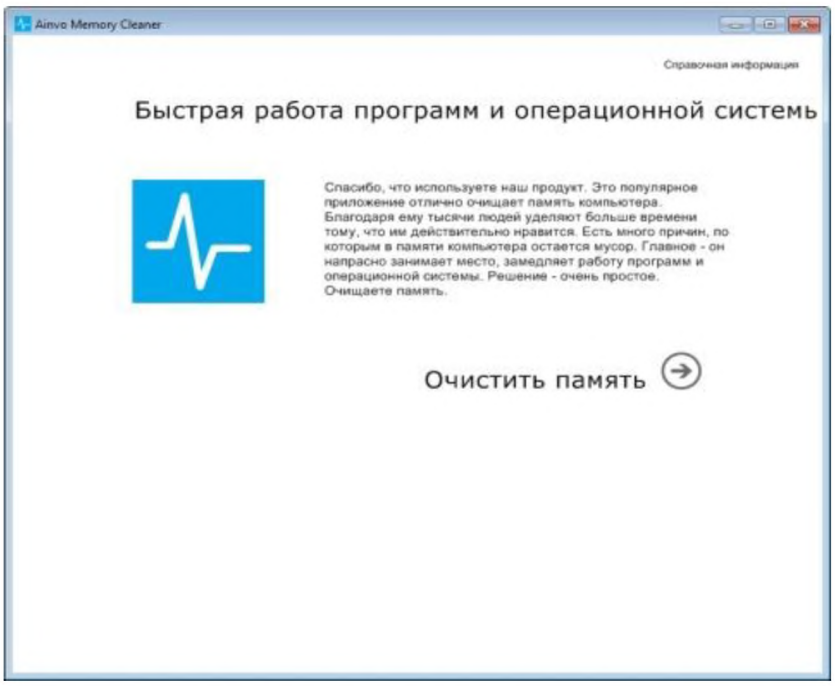


Рисунок 2.9 - Вікно програми Ainvo Disk Cleaner

Очищення пам'яті відбувається абсолютно без участі користувача, якісь настройки повністю відсутні. Весь процес використання полягає в старті програми, натиснення кнопки запуску і одержання звіту, скільки пам'яті вдалося звільнити. Насправді Ainvo Memory Cleaner займається вивантаженням з оперативної пам'яті бібліотек, завантажених туди різними додатками. Справа в тому, що коли ви використовуєте якусь програму, то вона, за потреби, може завантажувати необхідні окремі модулі, що містять необхідний виконуваний код, ресурси, процедури і так далі. На жаль, не всі бібліотеки звільняють пам'ять після завершення роботи основної програми. Також існують універсальні бібліотеки, використовувані різними додатками. Але коли ні одна з них не запущено, пам'ять залишається зайнятою марним модулем. Ainvo Memory Cleaner примусово вивантажує їх з пам'яті, не завдаючи шкоди працюючим програмам.

На рисунку 2.10 зображено вікно очищення пам’яті.

Рисунок 2.10 - Вікно очищення пам'яті

На рисунку 2.12 зображений процес виконання очищення пам’яті.

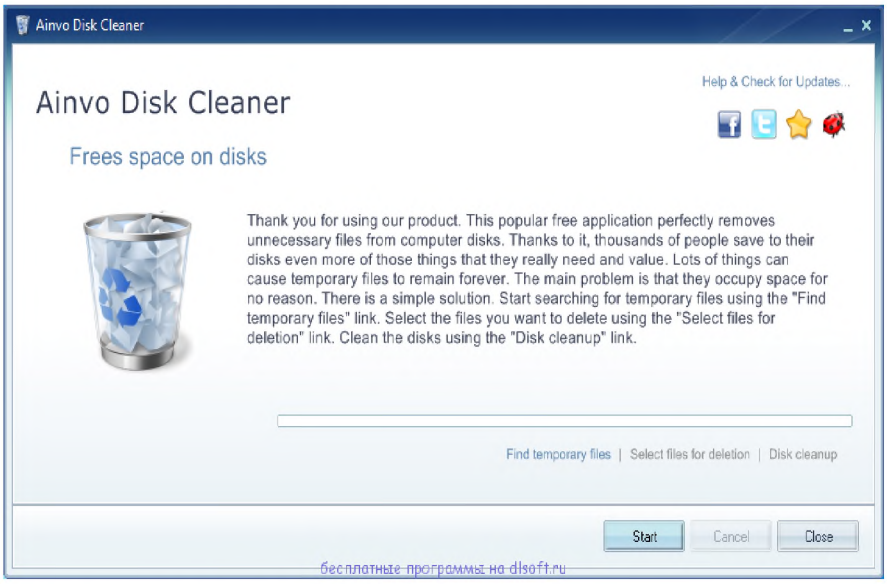


Рисунок 2.10 - Процес виконання очищення пам'яті

2.6.3 Базова цілісність при обміні

Базова цілісність при обміні досягається тоді коли забезпечується можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання це можна від слідити за допомогою ПЗ Internet Access Monitor яке забезпечує облік і контроль Інтернет-трафіку.

У програмі є спеціальний інструмент, який називається "журнал". З його допомогою можна "на льоту" формувати різні фільтри. Фільтри доступні за всіма параметрами, включеним у записи бази даних - по імені користувача, адресою його комп'ютера, протоколу, типом отриманих даних, мережевих адресах, відвідуваних користувачами, типами сайтів, з часу відвідин, використовуваних програм і так далі. Фільтри можуть бути складними, що дозволяє виконувати відбір тільки тієї інформації, яка необхідна для конкретного аналізу.

На рисунку 2.11 відображено журнал програми Internet Access Monitor.

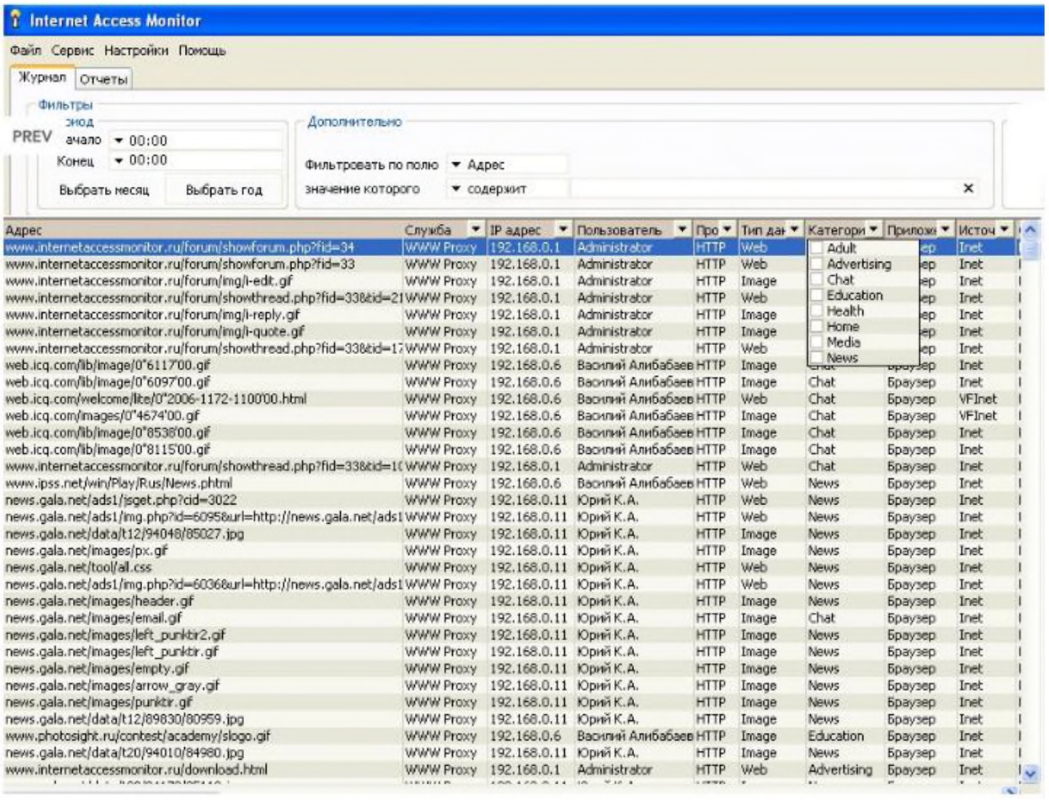


Рисунок 2.11 - Журнал Internet Access Monitor

Найбільш інформативним видом звіту є його уявлення в графічному вигляді. Internet Access Monitor має вбудовані засоби для побудови діаграм, візуалізуючих розподіл трафіку по різних параметрах. Побудова діаграми здійснюється на основі вже сформованого звіту. Для перегляду діаграм необхідно виділити назву будь-якої секції звіту (наприклад, "По днях тижня") і, викликавши правою кнопкою миші контекстне меню, вибрати пункт "Діаграма".

Рисунок 2.12 відображає візуальний розподіл трафіку.

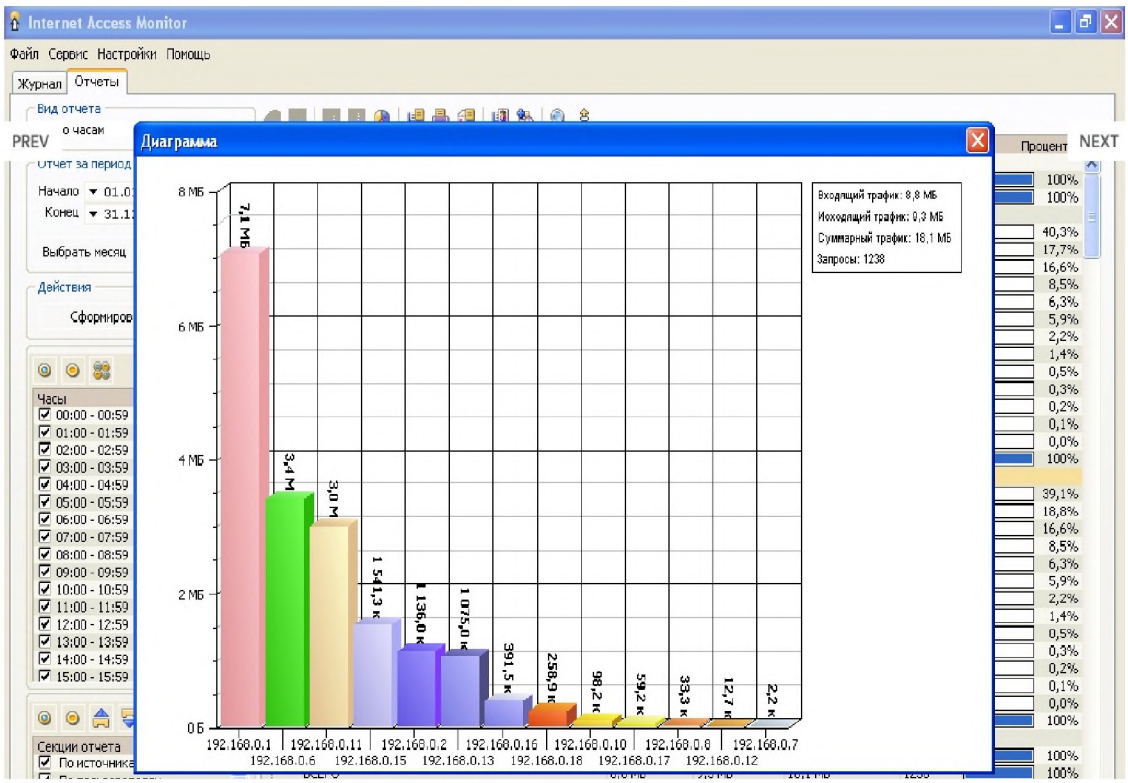


Рисунок 2.12 - Візуалізуючий розподіл трафіку

Рисунок 2.13 відображає розширені налаштування програми Internet Access Monitor.

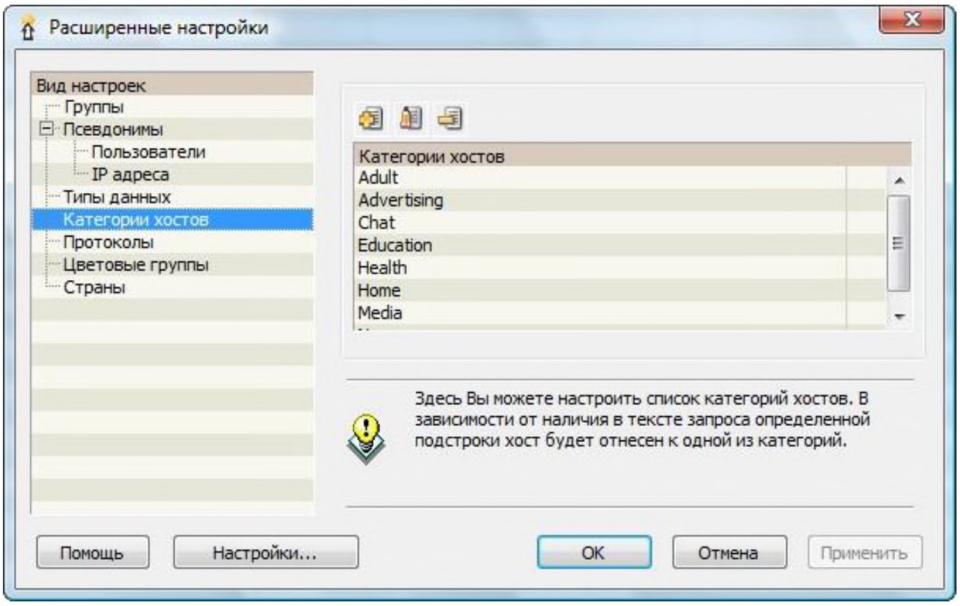


Рисунок 2.13 - Розширені налаштування

Звіт складається з типу звіту, інтервалу часу, об'єкта, за яким будується звіт, розділу. Він дозволяє переглядати інформацію, згрупованому по тому чи іншому ознакою. Для зручності, при використанні одних і тих же форм звітів, можна використовувати шаблони, які створюються і зберігаються самостійно. Підготовлені шаблони можна додавати в планувальник і з їх допомогою формувати звіти за розкладом. І не лише формувати, а й відправляти на електронну адресу або викладати у вигляді файлу в певний каталог.

Рисунок 2.14 відображає звіт виконання програми.

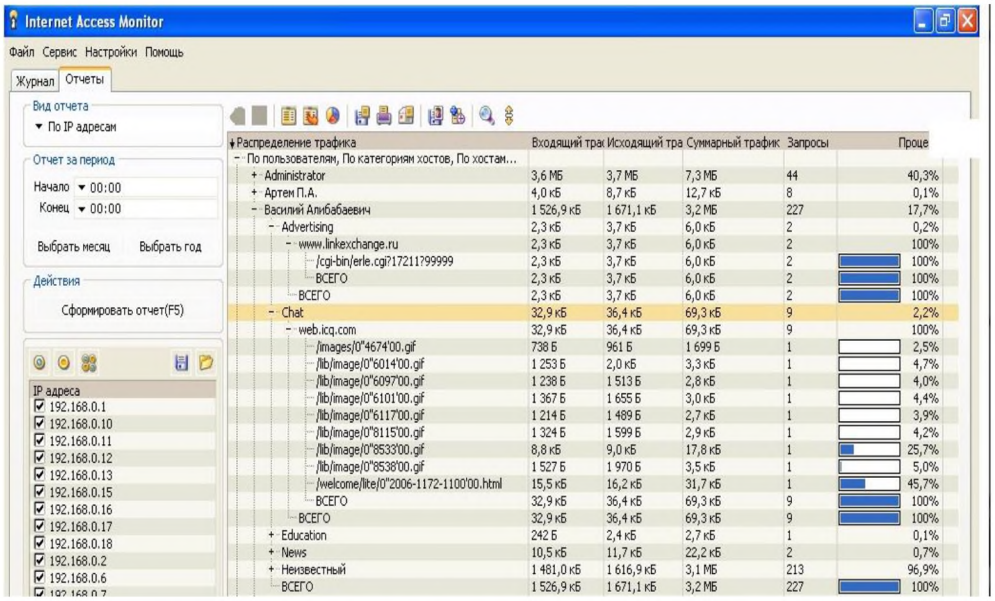


Рисунок 2.14 - Звіт виконання програми

2.6.4 Налаштування одно направлений достовірний канал

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації та виконання критерію профілю захищеності НК-1. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

Реалізується за допомогою протоколу аутентифікації Password Access Protocol – доступ по паролю.

Потрібна настройка, представлена на рис 2.15 активізація функції обмеженого делегування, передбачає використання обмеженого делегування з

допомогою налаштування Trust this user for delegation to specific services only. Ця настройка наказує облікового запису служби (або комп'ютера) запитувати делегування автентифікації тільки службами, зазначеними в списку. У розглянутому нами випадку квитки служби можуть запитуватися лише від імені інших користувачів для SQL Server. Натиснувши кнопку Add, ви повинні відшукати користувача (тобто обліковий запис служби) або комп'ютер, що є хостом служби, для доступу до якої хочете санкціонувати делегування. В даному випадку я вибрав обліковий запис служби SQL Server. Як показано на рис 2.16 вибір служб для здійснення делегування, ви побачите список імен учасників служб Service Principal Name (SPN), визначений виділеного користувача або комп'ютера, де ви можете вибрати служби, для доступу до яких буде виконуватися аутентифікація.

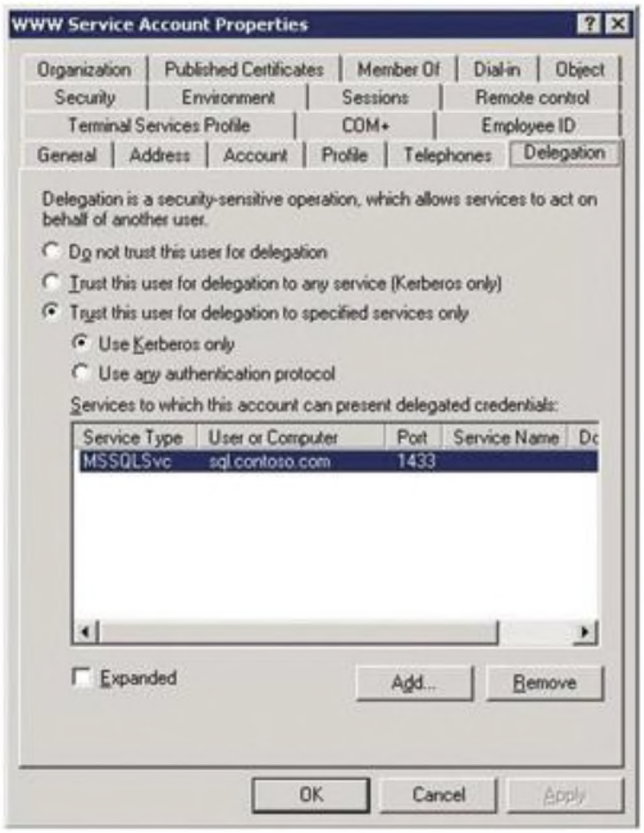


Рисунок 2.15 - Активізація функції обмеженого делегування

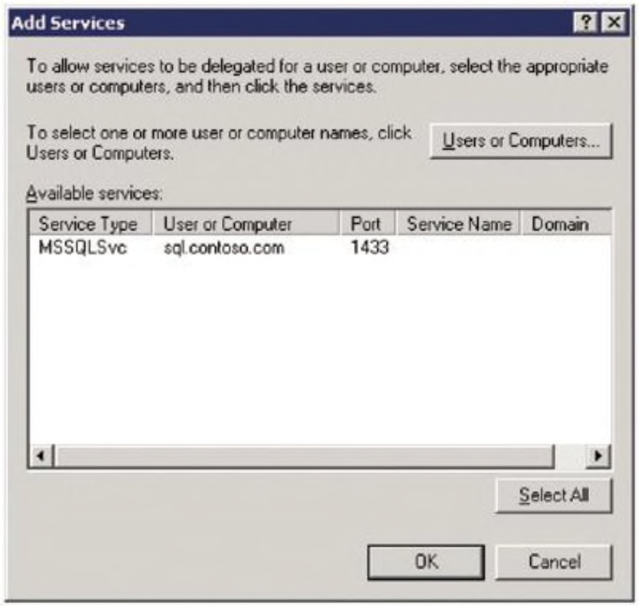


Рисунок 2.16 - Вибір служб для здійснення делегування

2.7 Висновок

В спеціальній частині роботи було проведено обстеження об’єкта інформаційної діяльності, проаналізовано циркулюючу інформацію. Створено модель загроз, модель порушника та проведено аналіз ризиків. Для здобуття необхідного рівня безпеки та виконання критеріїв профілю захищеності на підприємстві пропонується встановити нове програмне забезпечення таким чином буде забезпечуватися виконання усього функціонального профілю захищеності 3.КЦД.2.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даного розділу є обґрунтування економічної доцільності розробки системи захисту інформації інформаційно-комунікаційної системи приватного підприємства "Степ 2020". Для досягнення цієї необхідно здійснити наступні розрахунки: капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення; річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування; річний економічний ефект від впровадження запропонованих заходів; показники економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

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

Витрати на впровадження системи захисту інформації на підприємстві визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки системи захисту інформації інформаційно-комунікаційної системи підприємства

Трудомісткість розробки системи захисту інформації на підприємстві визначається тривалістю кожної робочої операції, до яких належать наступні:

– тривалість складання технічного завдання на розробку системи захисту інформації інформаційно-комунікаційної системи підприємства, $t_{тз}$=9 годин;

– тривалість аналізу нормативних документів у сфері інформаційної безпеки, $t_{нд}$=10 годин;

– тривалість аналізу загроз інформаційній безпеці, $t_{зі}$=16 годин;

– тривалість обрання функціонального профілю захищеності і класу АС, $t_{пз}$=14 годин;

– тривалість розробки системи захисту інформації інформаційно-комунікаційної системи підприємства, $t_{знд}$=40 години;

– тривалість підготування технічної документації для впровадження запропонованих рішень, $t_д$=8 годин.

Отже,

$$t = t_{тз} + t_{нд} + t_{зі} + t_{пз} + t_{знд} + t_д = 9+10+16+14+40+8 = 97 \text{ годин.}$$

Розрахунок витрат на розробку системи захисту інформації інформаційно-комунікаційної системи підприємства

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

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 16102 + 500,52 = 16602,52 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 97*166 = 16102 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

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

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t*С_{мч} = 97*5,16 = 500,52 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = 0,9 \cdot 2 \cdot 1,68 + \frac{4556 \cdot 0,4}{1920} + \frac{7623 \cdot 0,3}{1920} = 5,16 \text{ грн.}$$

При розробці системи захисту інформації інформаційно-комунікаційної системи приватного підприємства "Степ 2020" всі критерії стандартного функціонального профілю захищеності 3.КЦД.2, крім НТ-2; КО-1; ЦВ-2 та НК-1, пропонується здійснювати за допомогою вже встановленого програмного забезпечення та при використані інших вбудованих служб до операційної системи Microsoft Windows 10, яка використовується на підприємстві. Також пропонується встановити нове програмне забезпечення за допомогою використання якого буде забезпечуватися виконання усього функціонального профілю захищеності 3.КЦД.2. Додаткового пропонується встановити наступне таке програмне забезпечення як, Comodo Internet Security, Ainvo Memory Cleaner та Ainvo Disk Cleaner, які розповсюджується безкоштовно. Таким чином, додаткові витрати щодо придбання програмного забезпечення не виникають.

Витрати на навчання технічних фахівців і обслуговуючого персоналу ($К_{навч}$) складатимуть 2800 грн.

Витрати на встановлення обладнання та налагодження системи ($К_н$) інформаційної безпеки складатимуть 6300 грн.

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_н =$$
$$= 16602,52+2800+6300 = 25702,52 \text{ грн.}$$

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

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

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

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

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad грн.$$

де $С_{в}$ - вартість відновлення й модернізації системи;

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки.

Оскільки розробці системи захисту інформації інформаційно-комунікаційної системи приватного підприємства "Степ 2020" використовується вже наявне на підприємстві програмне забезпечення або таке, що розповсюджується безкоштовно, тому додаткові витрати щодо відновлення не виникають.

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи, які складуть 3000 грн.

Оскільки розробку системи захисту інформації інформаційно-комунікаційної системи приватного підприємства "Степ 2020" реалізовано за допомогою використання програмного, яке надається на безкоштовній основі, тому додаткові витрати щодо амортизаційних відрахувань не виникають.

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

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 19600 грн. Додаткова заробітна плата – 8% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,15 ставки. Отже,

$$С_з = (19600*12 + 19600*12*0,08)*0,15 = 38102,4 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2022 р. складає 22%.

$$С_{єв} = 38102,4*0,22 = 8382,53 \text{ грн.}$$

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,1 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1*2*1920*1,68 = 6451,2 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2% ($С_{тос}$ = 23306,28*0,02=466,13 грн).

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

$$С_к = 3000+38102,4+8382,53+6451,2+466,13 = 56402,26 \text{ грн.}$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, виходячи з величини капітальних витрат та середньостатистичних даних щодо активності користувачів. За статистичними даними активність користувачів складає 10%. Тому:

$$С_{ак} = 23306,28*0,1=2330,63 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 56402,26+2330,63 = 58732,89 \text{ грн.}$$

3.2 Оцінка можливого збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Оцінка можливого збитку від атаки на вузол або сегмент мережі

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 2 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 3 години;

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

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 25000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 19600 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особа;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 6 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 422 тис. грн. на рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 900 грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 42.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

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

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

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

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

$$П_п = \frac{\sum З_с}{F} t_п = \frac{19600*6}{176} * 2 = 1336{,}36 \text{ грн},$$

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

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

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

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

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

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

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або

сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с}{F} t_{ви} = \frac{19600*6}{176} * 3 = 2004{,}55 \text{ грн.}$$

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

$$П_{пв} = \frac{\sum З_о}{F} t_в = \frac{25000*1}{176} * 3 = 426{,}14 \text{ грн.}$$

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 2004{,}55+426{,}14+900 = 3330{,}69 \text{ грн.}$$

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

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{422000}{2080} \cdot (2 + 3 + 3) = 1623{,}08 \text{ грн.}$$

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

$$U = 1336{,}36+3330{,}69+1623{,}08= 6290{,}13 \text{ грн.}$$

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

$$B = \sum_i \sum_n U = \sum_1 \sum_{42} 6290{,}13 = 264185{,}46 \text{ грн.}$$

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C$$

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

R – вірогідність успішної реалізації загрози (32%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 246185{,}46*0{,}32 - 58732{,}89 = 20046{,}46 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

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

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

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

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{20046,46}{25702,52} = 0,78 \text{ частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (8%);

$N_{інф}$ – річний рівень інфляції, (6%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,78 > (8 - 6)/100 = 0,78 > 0,02.$$

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

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{0,78} = 1,28 \text{ років.}$$

3.4 Висновок

Таким чином, виходячи з результатів наведених розрахунків, розробку системи захисту інформації інформаційно-комунікаційної системи приватного підприємства "Степ 2020" можна вважати економічно доцільною. Коефіцієнт повернення інвестицій складає 0,78 грн./грн., тобто 0,78 грн. економічного ефекту на 1 грн. капітальних витрат. Дохідність інвестицій у розробку системи захисту інформації інформаційно-комунікаційної системи приватного підприємства "Степ 2020" матиме вищу дохідність, ніж за альтернативного варіанту вкладення коштів. Термін окупності складатиме 1,28 року. Капітальні інвестиції складуть 25702,52 грн., які у разі їх вкладення принесуть економічний ефект величиною 20046,46 грн.

ВИСНОВКИ

В кваліфікаційній роботі було проведено обстеження об’єкта інформаційної діяльності, проаналізовано циркулюючу інформацію. Створено модель загроз, модель порушника та проведено аналіз ризиків. Для здобуття необхідного рівня безпеки та виконання критеріїв профілю захищеності на підприємстві пропонується встановити нове програмне забезпечення таким чином буде забезпечуються виконання усього функціонального профілю захищеності 3.КЦД.2.

В економічній частині було приведено обґрунтування економічної діяльності розробки та впровадження КСЗІ. Розраховано капітальні витрати, витрати на обслуговування та можливі збитки.

Практична цінність роботи полягає у підвищенні рівня захищеності інформації та забезпечення безперервності ведення бізнесу.

ПЕРЕЛІК ПОСИЛАНЬ

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

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

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

4. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

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

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

7. Закон України № 1280-IV«Про телекомунікації»(Електрон. ресурс) / Спосіб доступу: URL: zakon.rada.gov.ua/go/1280-15- Загол. з екрана.

8. Закон України №2938-17 від 13.01.2011р."Про інформацію"//Відомості Верховної Ради України. – 2011. -№ 32, с.313.

9. Рішення НКРЗ №512 від 11.11.2010 «Умови здійснення діяльності у сфері телекомунікацій з надання послуг доступу до Інтернет (Електрон. ресурс) / Спосіб доступу: URL: http://www.nkrz.gov.ua/uk/activities/ruling2/1289571519/print-Загол. з екрана.

10. Закон України № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах»(Електрон. ресурс) / Спосіб доступу: URL: zakon.rada.gov.ua/go/80/94-вр.

11. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. –Изд-во «ДиаСофт», 2011. – 693с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	25	
6	А4	2 Розділ	32	
7	А4	3 Розділ	12	
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	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Розробка системи захисту інформації інформаційно-комунікаційної системи приватного підприємства "Степ 2020"
ст. гр. 125-19ск-1 Соломіна Костянтина Сергійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерел та __ додатка.

Мета роботи: розробка системи захисту інформації в інформаційно-комунікаційної системи приватного підприємства " Степ 2020".

У розділі «Стан питання. Постановка задачі» розглянута характеристика підприємства, наведена структура ІТС, проведене категоріювання та обстеження об'єкту.

У спеціальній частині визначений функціональний профіль захищеності автоматизованої системи, побудована модель загроз та модель порушника, запропоноване, встановлене та налаштоване програмне забезпечення для забезпечення всіх критеріїв профілю захищеності та нейтралізації загроз інформації в ІТС ПП «Степ 2020».

В економічному розділі визначені збитки від атаки на обчислювану мережу та здійснено розрахунок витрат на реалізацію системи захисту інформації комп'ютерної мережи.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник