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 ***Бовдиря Даніла Євгеновича***

академічної групи ***125-16-1***

спеціальності ***125 Кібербезпека***

спеціалізації[1]

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка підсистеми захисту від несанкціонованого доступу комплексної системи захисту інформації ТОВ «Сфера»***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Святошенко В.О.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Лізунова Т.Л.			

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Бовдирю Данілу Євгеновичу*** **академічної групи** ***125-16-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка підсистеми захисту від несанкціонованого доступу комплексної системи захисту інформації ТОВ «Сфера»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Виконати обстеження інформаційно-телекомунікаційної системи підприємства. Визначити основні загроз інформаційної безпеки.	29.03.2020
Розділ 2	Проаналізувати існуючи засоби захисту інформаційно-телекомунікаційної системи підприємства. Розробити заходи щодо захисту від несанкціонованого доступу до інформації яка циркулює на ОІД.	24.05.2020
Розділ 3	Виконати розрахунок економічних показників, визначити економічну доцільність впровадження системи захисту.	14.06.2020

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

Дата видачі: 08.01.2020р.

Дата подання до екзаменаційної комісії: 15.06.2020р.

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

РЕФЕРАТ

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

Об'єкт розробки: автоматизована система ТОВ «Сфера».

Мета роботи: розробка підсистеми захисту від несанкціонованого доступу автоматизованої системи ТОВ «Сфера».

У спеціальній частині виконано аналіз об'єкта захисту та існуючої системи безпеки, та наведені методи та засоби реалізації підсистеми захисту від НСД.

У роботі наведені:

- технічне завдання на розробку підсистеми захисту від НСД;
- розмежування доступу засобами клієнту Active Directory.

В економічному розділі виконати розрахунок економічної ефективності впровадженої підсистеми захисту від НСД.

Практичне значення роботи полягає в підвищені захисту інформації ТОВ «Сфера», шляхом впровадження підсистеми захисту від НСД.

Розроблена підсистема захисту від НСД призначена для впровадження у АС ТОВ «Сфера», з метою захисту конфіденційної інформації.

ACTIVE DIRECTORY, WINDOWS 2012, АВТОМАТИЗОВАНА СИСТЕМА, НЕСАНКЦІОНОВАНИЙ ДОСТУП, PROXY-СЕРВЕР, ПІДСИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ.

РЕФЕРАТ

Пояснительная записка: ___ стр., __ рис., ___ табл., __ приложений, __ источников.

Объект разработки: автоматизированная система ООО «Сфера».

Цель работы: разработка подсистемы защиты от несанкционированного доступа автоматизированной системы ООО «Сфера».

В специальной части выполнен анализ объекта защиты и существующей системы безопасности и приведены методы и средства реализации подсистемы защиты от НСД.

В работе приведены:

- техническое задание на разработку подсистемы защиты от НСД;

- разграничение доступа средствами клиенту Active Directory.

В экономическом разделе выполнить расчет экономической эффективности внедренной подсистемы защиты от НСД.

Практическое значение работы состоит в повышении защиты информации ООО «Сфера», путем внедрения подсистемы защиты от НСД.

Разработана подсистема защиты от НСД предназначена для внедрения в АС ООО «Сфера», с целью защиты конфиденциальной информации.

ACTIVE DIRECTORY, WINDOWS 2012, АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ, НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, PROXY-СЕРВЕР, ПОДСИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ.

ABSTRACT

Explanatory note: __ p., __ fig., __ tab., __ additions, __ sources.

Object of development: automated system of LLC "Sphere".

Purpose of work: development of the subsystem of protection against unauthorized access of the automated system of LLC "Sphere".

The special part analyzes the object of protection and the existing security system, and describes the methods and means of implementation of the subsystem protection against NMS.

The paper presents:

- Terms of Reference for the development of the subsystem protection against NSD;

- Delimiting access to Active Directory client tools.

In the economic section, calculate the cost-effectiveness of the implemented NMS protection subsystem.

The practical importance of the work is to increase the protection of information of LLC "Sfera" by introducing a subsystem of protection against NSD.

The developed subsystem of protection against NSD is intended for introduction in the AS of Sfera LLC, in order to protect confidential information.

ACTIVE DIRECTORY, WINDOWS 2012, AUTOMATED SYSTEM, UNAUTHORIZED ACCESS, PROXY-SERVER, INFORMATION PROTECTION SUBSYSTEM.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІзОД – інформація з обмеженим доступом;

ІС – інформаційна система;

КЗЗ – комплекс засобів захисту;

КМ – комп’ютерна мережа;

КСЗІ – комплексна система захисту інформації;

НСД – несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ПК – персональній комп’ютер;

ТОВ – товариство з обмеженою відповідальністю.

ЗМІСТ

с.

ВСТУП 11

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ 14

1.1 Загальні відомості про підприємство 14

1.1.1 Організація роботи на підприємстві 14

1.1.2 Ієрархія організації роботи підрозділів на підприємстві 14

1.2.1 Фізичне середовище 15

1.2.1.1 Ситуаційний план 15

1.2.1.2 Генеральний план 18

1.2.1.3 Система охорони 21

1.2.1.4 Пожежна система 21

1.2.1.5 Система опалення 21

1.2.1.6 Система електроживлення та заземлення 21

1.2.2 Обчислювальне середовище 21

1.2.3 Інформаційне середовище 24

1.2.3.1 Перелік програмних засобів встановлених на робочих станціях виробничих підрозділів ТОВ «Сфера» 25

1.2.4 Середовище користувачів 29

1.3 Перелік існуючих елементів захисту інформації на підприємстві 31

1.4 Модель порушника 32

1.5 Аналіз загроз 33

1.6 Постановка задачі. Висновок 34

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА 36

2.1 Технічне завдання 36

2.1.1 Найменування роботи та область застосування 36

2.1.2 Призначення розробки 36

2.1.3 Етапи виконання робіт 36

2.1.3.1 Попередній 36

2.1.3.2 Проектування і розробка 36

2.1.3.3 Проведення випробувань і передача в експлуатацію 37
2.1.4 Економічні показники 37
2.2 Система розмежування доступу до інформації на сервері та робочих станціях підприємства 37
2.2.1 Створення домену 37
2.2.2 Установка Microsoft DNS Server 37
2.2.3 Запуск майстра інсталяції Active Directory 39
2.2.4 Додавання серверів і робочих станцій в домен 40
2.2.5 Налаштування об’єктів Active Directory 42
2.2.5.1 Групові політики 42
2.2.5.2 Структура об'єктів групової політики і їх місце в службі каталогів 43
2.2.5.3 Локальні політики робочої станції 45
2.2.6 Контроль доступу до ресурсів 45
2.2.7 Розмежування доступу до мережі Інтернет 46
2.2.8 Розроблені правила доступу до інформації на підприємстві 48
2.3 Програми для контролю і моніторингу доступу до різних пристроїв вводу, виводу та зберігання інформації 49
2.3.1 Програма FileControl 49
2.3.2 Програма DeviceLock 52
2.4 Програмні засоби захисту інформації 57
2.4.1 Налагодження параметрів мережевого екрана Outpost Firewall 57
2.4.2 Антивірусна програма Eset NOD32 61
2.5 Структура локальної мережі 61
2.6 Висновок 62
РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ 63
3.1 Розрахунок (фіксованих) капітальних витрат 63
3.1.1 Розрахунок поточних витрат 66
3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі 69
3.2.1 Оцінка величини збитку 69
3.2.2 Загальний ефект від впровадження системи інформаційної безпеки 72

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки 72
3.4 Висновок 73
ВИСНОВКИ 75
ПЕРЕЛІК ПОСИЛАНЬ 76
ДОДАТОК А 78
ДОДАТОК Б 79
ДОДАТОК В 87
ДОДАТОК Г 88
ДОДАТОК Д 89

ВСТУП

Інформаційна безпека галузь, що швидко розвивається область інформаційних технологій. Словосполучення інформаційна безпека в різних контекстах може мати різний зміст. Стан захищеності національних інтересів в інформаційній сфері визначається сукупністю збалансованих інтересів особистості, суспільства і держави.

Під інформаційною безпекою розуміють захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятний збиток суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації і підтримуючої інфраструктури.

Разом з тим, захист інформації – це комплекс заходів спрямованих на забезпечення інформаційної безпеки.

З методологічної точки зору правильний підхід до проблем інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем. Загрози інформаційної безпеки – це зворотний бік використання інформаційних технологій.

Кажучи про системи безпеки, потрібно відзначити, що вони повинні не тільки і не стільки обмежувати допуск користувачів до інформаційних ресурсів, скільки визначати і делегувати їх повноваження у спільному вирішенні завдань, виявляти аномальне використання ресурсів, прогнозувати аварійні ситуації та усувати їх наслідки, гнучка адаптуючи структуру в умовах відмов, часткової втрати або тривалого блокування ресурсів.

Не варто, однак, забувати про економічну доцільність застосування тих чи інших заходів забезпечення безпеки інформації, які завжди повинні бути адекватні існуючим загрозам.

Паралельно з розвитком засобів обчислювальної техніки і появою все нових способів порушення безпеки інформації розвивалися і удосконалювалися

засоби захисту. Необхідно відзначити, що більш старі види атак нікуди не зникають, а нові тільки погіршують ситуацію. Існуючі сьогодні підходи до забезпечення захисту інформації дещо відрізняються від існуючих на початковому етапі. Головна відмінність сучасних концепцій у тому, що сьогодні не говорять про якомусь одному універсальному засобі захисту, а мова йде про КСЗІ, що включає в себе:

- інформативно-правової базис захисту інформації;
- засоби, способи та методи захисту;
- органи і виконавців.

Іншими словами, на практиці захист інформації представляє собою комплекс регулярно використовуваних засобів і методів, прийнятих заходів і здійснюваних заходів з метою систематичного забезпечення необхідної надійності інформації, що генерується, зберігається та обробляється на об'єкті АС, а також передається по каналах. Захист повинен носити системний характер, тобто для отримання найкращих результатів всі розрізнені види захисту інформації повинні бути об'єднані в одне ціле і функціонувати в складі єдиної системи, що представляє собою злагоджений механізм взаємодіючих елементів, призначених для виконання завдань по забезпеченню безпеки інформації.

Більш того, КСЗІ призначена забезпечувати, з одного боку, функціонування надійних механізмів захисту, а з іншого – управління механізмами захисту інформації. У зв'язку з цим повинна передбачатися організація чіткої та налагодженої системи управління захистом інформації.

Наведені факти роблять проблему проектування ефективних систем захисту інформації актуальною на сьогоднішній день.

В першому розділі був проаналізований сучасний метод побудови КСЗІ, відповідно до нормативних документів технічного захисту інформації України.

У другому розділі було розглянуто як на основі клієнту Active Directory у Windows в комбінації з програмою DeviceLock, а також з Proxy-сервер Usergate

реалізувати надійний захист від несанкціонованого доступу до конфіденційної інформації на підприємстві ТОВ «Сфера».

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про підприємство

Об’єктом інформаційної діяльності є ТОВ «Сфера» що знаходиться за адресою 51500, Дніпропетровська обл., м. Тернівка, вул. Маяковського 33. Сферою діяльності ОІД є надання клієнтам малих будівельних послуг, ремонтів жилих комплексів, та модернізацією архітектурних споруджень.

ТОВ «Сфера» розробляє проектну документацію і дає гарантії. Підприємство ж самостійно займається і закупівлею матеріалу, хоча для цього і вимагає передоплату. ТОВ «Сфера» може наймати працівників і у інших фірм, якщо на підприємстві не буде спеціалістів потрібних для виконання робіт.

1.1.1 Організація роботи на підприємстві

Внутрішня діяльність ТОВ «Сфера» полягає у безперебійному і безпосередньому виробництві будівельних послуг. Її учасниками є: трудовий колектив в особі працівників і управлінського персоналу, власника (директор).

Зовнішня сторона ТОВ «Сфера» обумовлена відносинами з постачальниками, споживачами продукції (замовниками), партнерами (субпідрядниками), кредиторами, державними органами.

Учасники цього товариства не відповідають за зобов’язання і несуть ризик збитків у межі внесених ними внесків.

Власником ТОВ «Сфера» є директор, він і відповідає за розподіл обов’язків на підприємстві, а також перевіряє виконання робіт в управлінському персоналі, в той час коли управлінський персонал по ієрархії перевіряє роботу трудового персоналу згідно власних повноважень. Також є такі відділи які є відповідальними перед Директором і не виконують ніякої функції керування. Таким чином налагоджено оптимальний робочий процес на підприємстві.

1.1.2 Ієрархія організації роботи підрозділів на підприємстві

Ієрархія організації роботи підрозділів підприємства потрібні для оптимізації виробничого процесу на підприємстві, визначення інформаційних потоків та розподілу обов’язків на підприємстві, схема розподілу обов’язків зображена на рисунку 1.1.

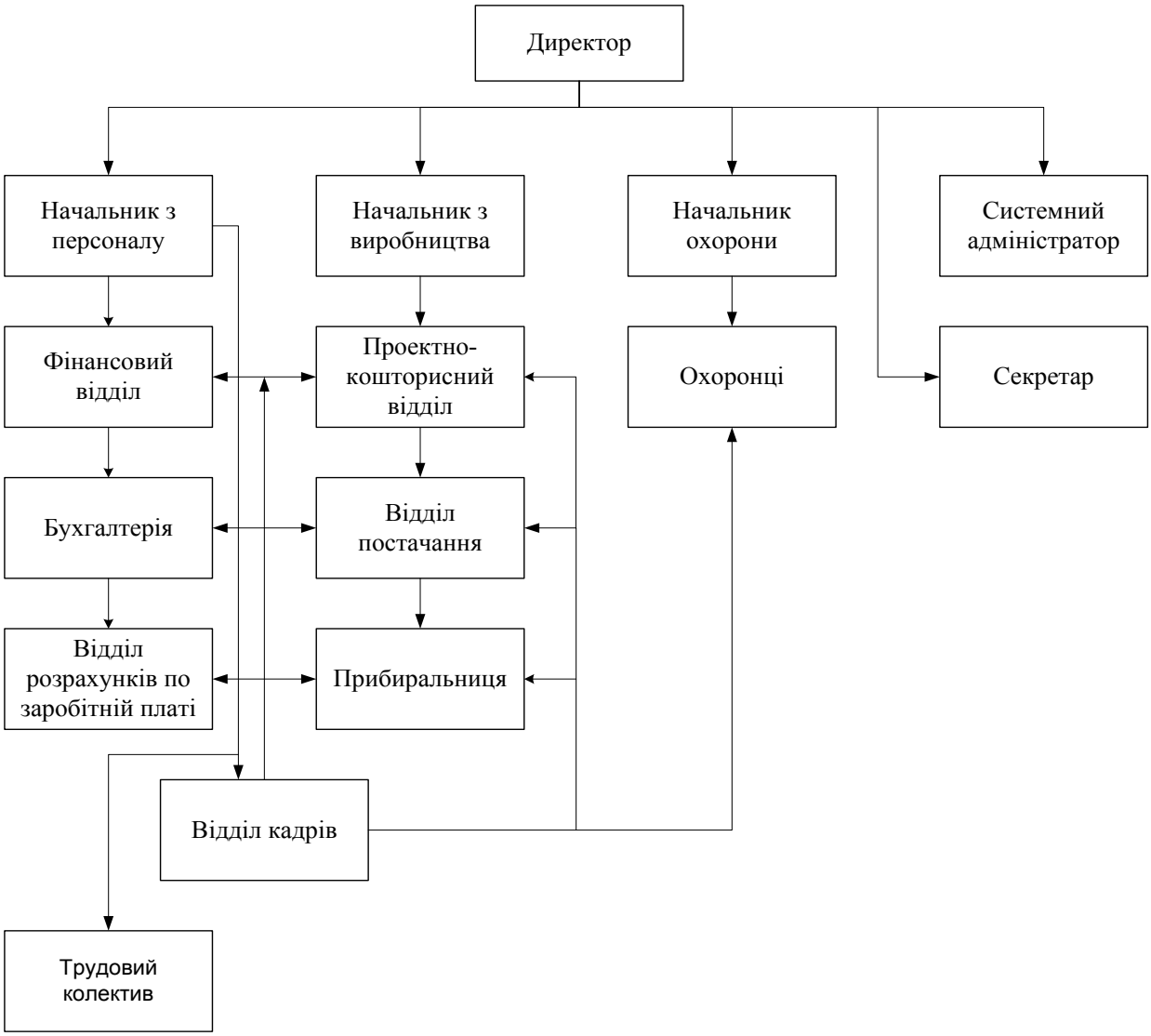


Рисунок 1.1 – Схема організації роботи підрозділів на підприємстві

1.2.1 Фізичне середовище

1.2.1.1 Ситуаційний план

Місцями розміщення стаціонарних чи мобільних засобів технічної розвідки можуть бути декоративні кущі, розташовані за об’їзною дорогою на висоті 0,5-1 метрів на південь від ОІД. Також стаціонарні засоби технічної

розвідки можуть бути встановлені на північ, захід та схід на відстані 150 метрів від ОІД. Ситуаційний план зображене на рисунку 1.2.

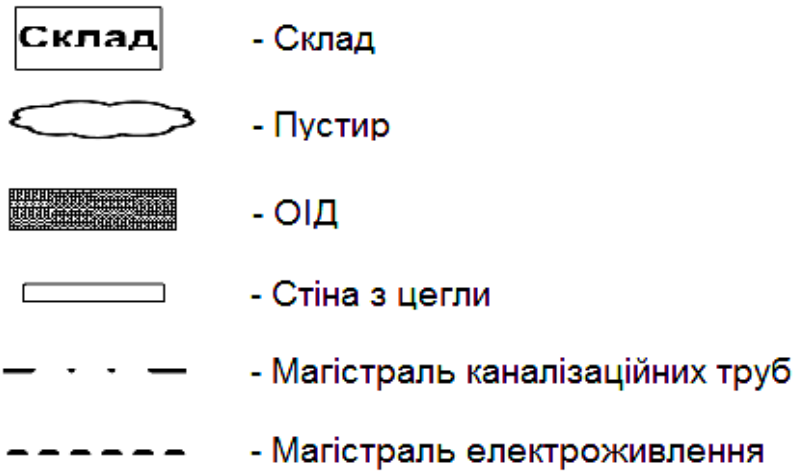
Таблиця 1.1 – Основні характеристики вулиць

№	Назва вулиці	Розташування відносно ОІД	Ширина для проїзду	Ширина пішохідної частини	Інтенсивність руху транспорту	Наявність місць неконтрол. перебування авто
1	Маяковського	південь	15 м.	--	низька	пустир 150 м.
2	Маяковського	схід	30 м.	--	низька	150 м. траси

Таблиця 1.2 – Об’єкти, які оточують ОІД

№	Розташування відносно ОІД	Кількість поверхів	Адреса	Характеристика об’єкта	Відстань від ОІД
1	захід	--	--	--	--
2	схід	1	Маяковського 33а	Цех, належить ТОВ «Сфера»	5 м.
3	північ	--	--	пустир	15 м.
4	південь	--	--	Дорога, відстань до міста 1 км	30 м.

Умовні позначення:



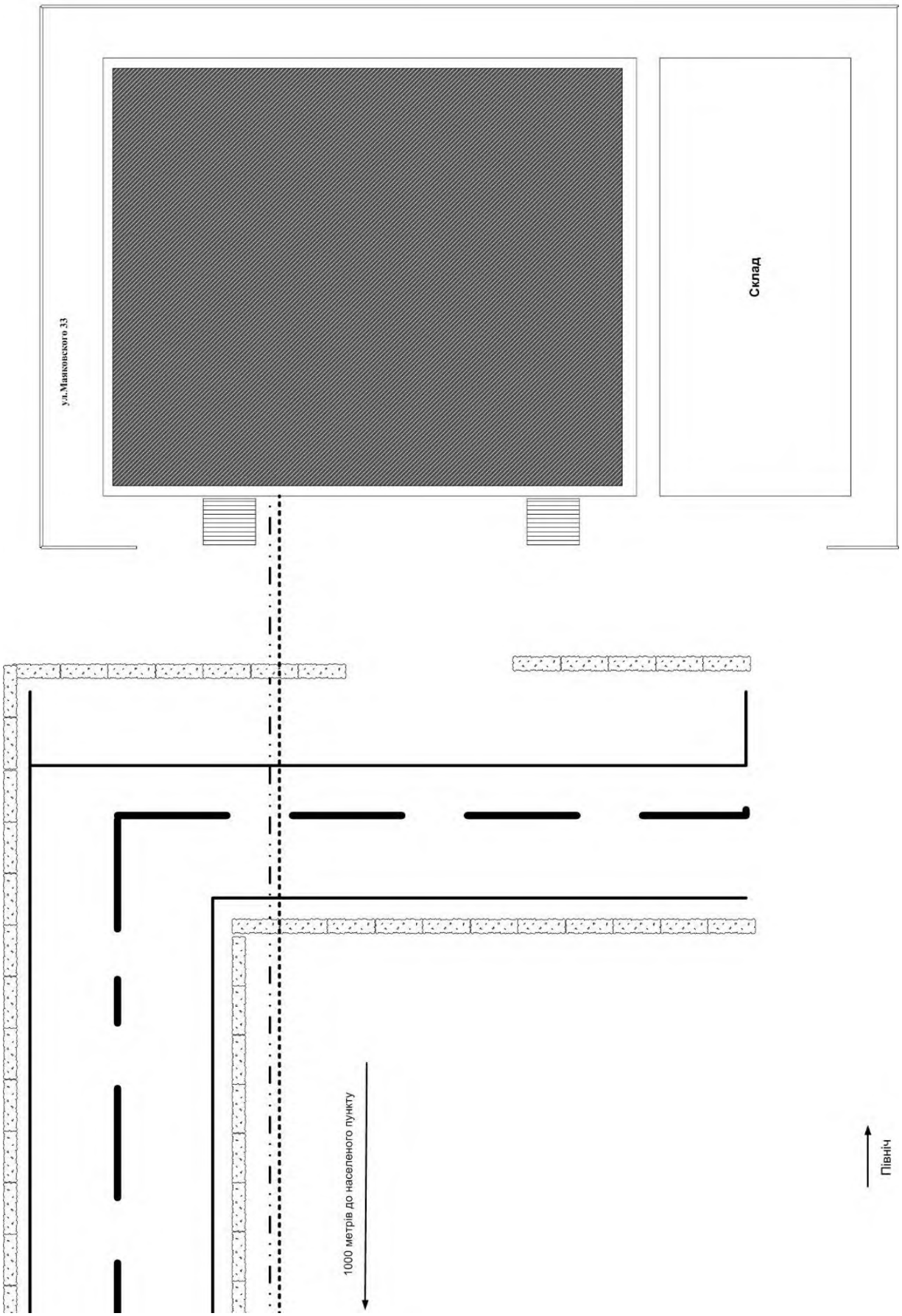


Рисунок 1.2 – Ситуаційний план

1.2.1.2 Генеральний план

Об’єктом інформаційної діяльності є ТОВ «Сфера» що знаходиться за адресою 51500, Дніпропетровська обл., м. Тернівка, вул. Маяковського 33. Сферою діяльності ОІД є надання клієнтам малих будівельних послуг, ремонтів жилих комплексів, та модернізацію архітектурних споруджень.

Організація розміщена у двоповерховій будівлі, яка є власністю ТОВ «Сфера».

Контрольована зона обмежена стінами будівлі та огороджена цеглиною загорожею та знаходиться на другому поверсі. Контроль доступу до КЗ здійснює охоронцями. Кожен працівник має пред’явити спеціальне посвідчення щоб бути допущеним до свого робочого місця. Прийом відвідувачів проводиться лише за записом у спеціально відведений час, кожен відвідувач на вході реєструється та заноситься у спеціальний журнал відвідувань.

Загальна характеристика будівлі:

Фундамент будівлі – залізобетон, стіни – панельні, перекриття у будівлі – цеглові.

Характеристика приміщення де оброблюється ІзОД.

Приміщення має: пожежну сигналізацію, електрику та автономне опалення;

Зовнішня поверхня стін виконані з панельних плит, внутрішня з цегляної укладки та пластикових панелей, зовнішні стени завтовшки 40 см., внутрішні перекриття завтовшки 20 см.

Підлога і стеля кімнати виконані із залізобетонних плит.

Вхідні двері до виділеного приміщення одинарні залізні з вплотнювачами. Останній ремонт зазначених кімнат проводився у 2012 році.

Під час проведення ремонту було демонтовано всі незадіяні електропровідні кабелі, дроти, ланцюги, елементи інженерних комунікацій, що проходили транзитом.

Кількість кімнат:

- Приймальна;

- Кабінет директора;
- Кабінет начальника безпеки;
- Кімната охорони (перший поверх);
- Серверна;
- Кімната адміністратора;
- Кімната начальника з виробництва;
- Кімната начальника з персоналу;
- Кімната проектно-кошторисного відділу;
- Кімната відділу розрахунків по заробітній платі;
- Бухгалтерія;
- Кабінет відділу кадрів;
- Кабінет фінансового відділу;
- Кабінет відділу постачання.

Режимними приміщеннями ОІД є серверна та щитова кімната.

Доступ у серверну кімнату мають начальник безпеки та системний адміністратор. Доступ до серверної кімнати обмежується фізично – згідно діючих посадових інструкцій системного адміністратора та начальника безпеки, двері у серверну кімнату повинні бути зачинені, також у їх обов’язки входить нагляд за доступом у серверну кімнату.

Доступ у щитову кімнату має тільки начальник охорони. Доступ до щитової кімнати обмежується фізично – згідно діючих посадових інструкцій начальника охорони, двері у архівну кімнату повинні бути зачинені. Візуального нагляду за щитовою кімнатою не здійснюється.

Також постійний доступ режимних приміщень мають охорона, прибиральниці, а також разовий доступ мають робітники, що здійснюють необхідні технічні роботи у даному приміщенні. Разовий доступ для технічних працівників можливий тільки за наявністю письмової санкції, затвердженої директором. Прибирання здійснюється тільки у присутності охоронця у спеціально відведений час – щоденно з 8:30-9:00 з понеділка по п’ятницю.

Ключі від серверної знаходяться у начальника охорони та адміністратора. Ключі від щитової кімнати знаходяться у начальника охорони. Дублікати всіх ключів знаходяться у директора та знаходяться у конверті з печаткою та сховані у сейф, що позначає що ключі не використовуються без необхідності. Також ключі які використовують адміністратор та начальник охорони, запечатуються у конверт з печаткою директора, які після закінчення робочого дня ховають у сейф директора.

Будівля знаходиться на відстані 1000 метрів на північ від міста, на відстані 20 метрів від входу знаходиться об'їзна дорога, рух на який мінімальний.

Сусідів будівля не має. З Сходу на відстані 5 метрів знаходиться цех який не підлягає обстеженню у зв'язку з тим що інформація яка підлягає захисту у цій будівлі не циркулює. На першому поверсі будівлі інформація з обмеженим доступом також не обробляється, і у зв'язку з цим обстеження першого поверху не виконується.

Режим роботи організації: кожен день тижня з 8.00 до 17.00, з понеділка по п'ятницю.

Кількість працівників:

- Директор (1 людина);
- Начальник охорони (1 людина);
- Бухгалтерія (2 людини);
- Відділ розрахунків по заробітній платі (2 людини);
- Охоронець (3 людини у зміну);
- Проектно-кошторисний відділ (2 людини);
- Системний адміністратор (1 людина);
- Прибиральниця (1 людина);
- Секретар (1 людина);
- Начальник з виробництва (1 людина);
- Начальник з персоналу (1 людина);
- Відділ постачання (1 людина);

- Фінансовий відділ (2 людини);
- Відділ кадрів (1 людина).

Усі працівники організації працюють з 8.00 до 17.00, окрім охорони. Охорона працює у дві зміни, денну та нічну по одному охоронцю в зміну.

Запис на прийом до директора та складення договору на виконання робіт, здійснюється за попереднім записом у секретаря.

1.2.1.3 Система охорони

Охоронна виконана у вигляді встановлення металевих решіток на вікнах. Охорона будівлі у вечірній та нічний час здійснюється охоронцями. На початку робочого дня кожен охоронець повинен скласти звіт за зміну.

1.2.1.4 Пожежна система

Пожежна сигналізація, виконана з використанням датчиків диму, звуковою сиреною та кнопкою тривоги, встановлених та виведених на пульт пожежної безпеки міської станції пожежників, також виконується обхід ОІД та інших споруд підприємства начальником охорони та складається звіт в кінці робочого дня. Схема розташування датчиків зображено у додатку Б.

1.2.1.5 Система опалення

На підприємстві система опалення автономна у зв’язку з тим що об’єкт знаходиться поза зоною підключення до централізованого опалення. Також встановлено два кондиціонери у кабінеті директора та серверній. Батареї опалення встановлені у всіх кімнатах. Схема опалення зображена у додатку Б.

1.2.1.6 Система електроживлення та заземлення

На підприємстві знаходиться стандартна система електроживлення та система занулення. Перетин проводу 1 мм^2, використовується також 17 розподільних коробок. Встановлено 34 лампи денного світла та 13 розеток. Схема електроживлення та заземлення зображення у додатку Б.

1.2.2 Обчислювальне середовище

На підприємстві ТОВ «Сфера» є п’ятнадцять комп’ютерів, одинадцять принтерів та один сервер.

Опис технічних засобів оброблювання інформації на підприємстві ТОВ «СФЕРА».

1) Комп’ютер директора:

Процесор – AMD Ryzen 5 1600 (3.2 - 3.6 ГГц);

ОЗП – 8 ГБ;

Жорсткий диск - 1 ТБ;

Відео карта - nVidia GeForce GTX 1050 Ti, 4 ГБ;

Записуючий пристрій - DVD-RW;

Монітор - Philips 245E1S/00/01;

Комп'ютерна миша - A4Tech X-710BK USB Black;

Клавіатура - Logitech K120 USB;

Принтер - Canon i-SENSYS MF3010.

2) Комп’ютер секретаря:

Процесор – AMD Ryzen 3 1200 (3.1 - 3.4 ГГц);

ОЗП – 8 ГБ;

Жорсткий диск – 1 ТБ;

Відео карта – nVidia GeForce GTX 1050, 2 ГБ;

Записуючий пристрій - DVD-RW

Монітор - Samsung S24R350;

Комп'ютерна миша - A4Tech X-710BK USB Black;

Клавіатура - Logitech K120 USB;

Принтер - Canon i-SENSYS MF3010.

3) Комп’ютер системного адміністратора:

Процесор - AMD Ryzen 5 3500 (3.6 - 4.1 ГГц);

ОЗП – 16 ГБ;

Жорсткий диск – HDD: 1 ТБ / SSD: 480 ГБ;

Відео карта - nVidia GeForce GTX 1650 Super, 4 ГБ;

Записуючий пристрій - DVD-RW;

Монітор - Samsung S24R350;

Комп'ютерна миша - A4Tech X-710BK USB Black;

Клавіатура - Logitech K120 USB.

4) Інші комп’ютери робітників підрозділів підприємства (12 штук):

Процесор – AMD Ryzen 5 1600 (3.2 - 3.6 ГГц);

ОЗП – 8 ГБ;

Жорсткий диск – 1 ТБ;

Відео карта - nVidia GeForce GTX 1050, 4 ГБ;

Записуючий пристрій - DVD-RW;

Монітор - Samsung S24R350;

Комп'ютерна миша - A4Tech X-710BK USB Black;

Клавіатура - Logitech K120 USB;

Принтери (9 штук) – Принтер - Canon i-SENSYS MF3010.

5) Сервер:

Процесор – Intel Core i7-9700F (3.0 - 4.7 ГГц);

ОЗП – 32 ГБ;

Жорсткий диск – HDD: 2 x 1 ТБ / SSD: 250 ГБ;

Записуючий прістрій - DVD-RW;

Монітор - Samsung S24R350;

Комп'ютерна миша - A4Tech X-710BK USB Black;

Клавіатура - Logitech K120 USB.

6) Комутатор (2 штуки): D-Link DES-1100-16 (16 портів 10/100Мб/с)

7) Модем ADSL модем D-Link DSL-2640U.

8) Структура локальної мережі з виходом у Інтернет

На підприємстві ТОВ «Сфера» встановлено 15 комп’ютерів зв’язані з сервером комутаторами. У свою чергу сервер підключений до мережі Інтернет через ADSL-модем (послуги Інтернет провайдера надає ВАТ Укртелеком). Структура локальної мережі зображено в додатку Б.

Топологія локальної мережі на підприємстві ТОВ «Сфера» - Зірка.

Ця топологія є однією з поширених топологією у світі. Її одночасно легко обслуговувати, а також налаштовувати.

Переваги:

- Вихід з ладу однієї робочої станції не відбивається на роботі всієї мережі в цілому;
- добра масштабованість мережі;
- легкий пошук несправностей і обривів в мережі;
- висока продуктивність мережі (за умови правильного проектування);
- гнучкі можливості адміністрування.

Недоліки:

- вихід з ладу центрального концентратора обернеться непрацездатністю мережі (або сегмента мережі) в цілому;
- для прокладки мережі найчастіше потрібна більше кабелю, ніж для більшості інших топологій;
- кінцеве число робочих станцій в мережі (або сегменті мережі) обмежене кількістю портів в центральному концентраторі.

1.2.3 Інформаційне середовище

Інформаційне середовище – сукупність технічних і програмних засобів зберігання, обробки і передачі інформації.

На території підприємства циркулює як відкрита інформація, так і ІзОД.

До відкритої інформації належать:

1) Інформація про організацію та вид її діяльності;
2) Інформація про вид надаваних послуг та їх вартість;
3) Інформація по усім формам державної звітності;
4) Відомості, необхідні для перевірки нарахування та оплати податків та інших обов’язкових платежів;
5) Відомості про чисельність та склад працівників, їх заробітну платню у цілому, по професіям та посадам, а також інформація про наявність вільних робочих місць;
6) Документи об сплаті податків та обов’язкових платежів

7) Правила та норми, регламентуючі порядок роботи працівників підприємства;

До комерційної таємниці та конфіденційної інформації належать:

1) Дані первинних облікових документів бухгалтерського обліку підприємства;

2) Зміст регістрів бухгалтерського обліку;

3) Зміст внутрішньої бухгалтерської звітності;

4) Проведені та проводимі підприємством угоди, у тому числі договори, їх предмет, зміст, ціна та інші суттєві умови;

5) Відомості про відкриті у кредитних установах розрахункових та інших рахунках, у тому числі у іноземній валюті, про міграцію коштів на цих рахунках, відомості про існуючі вклади в банках, у тому числі у іноземній валюті;

6) Відомості про клієнтів підприємства.

Будь-яка інша інформація, яка згідно з законодавством не може бути віднесена до державної таємниці, може бути віднесена до комерційної таємниці за рішенням директора підприємства.

На підприємстві ТОВ «Сфера» встановлено програмне та апаратне забезпечення для проведення обчислювальної роботи з грошовими операціями, розрахунками на будівельні матеріали та обробку документації внутрішньо виробничого процесу, а також мінімальні засоби антивірусної безпеки.

1.2.3.1 Перелік програмних засобів встановлених на робочих станціях виробничих підрозділів ТОВ «Сфера»

1) Операційні системи

На всіх п’ятнадцятьох (15) комп’ютерах встановлена ліцензійна версія Windows 10, яка є оптимальною операційною системою на користувальному рівні, а також реалізує усі потреби підприємства ТОВ «Сфера».

На сервері встановлена ліцензійна версія Windows Server 2016. Ця операційна система поставляється з передвстановленою оболонкою. NET Framework. Це дозволяє даній системі виступати в ролі сервера додатків для

платформи Microsoft. NET без встановлення будь-якого додаткового програмного забезпечення.

IIS. Для підвищення стабільності стало можливим ізолювати програми один від одного в окремих процесах без зниження продуктивності. Також був створений новий драйвер HTTP.sys для обробки запитів по протоколу HTTP. Цей драйвер працює в режимі ядра, в результаті чого обробка запитів прискорюється.

Безпека. Система тепер встановлюється в максимально обмеженому вигляді, без будь-яких додаткових служб, що зменшує поверхню атаки. У Windows Server також включений програмний міжмережевий екран Internet Connection Firewall.

Інше. У Windows Server є служба тіньового копіювання тому (Volume Shadow Copy Service), яка автоматично зберігає старі версії користувацьких файлів, дозволяючи при необхідності

повернутися до попередньої версії того чи іншого документу.

Ролі. Введено нове поняття - «ролі», на них засновано управління сервером. Простіше кажучи, щоб отримати файл-сервер, необхідно додати роль - «файл-сервер».

2) Програмне забезпечення для обробки документів.

На всіх робочих станціях підприємства ТОВ «СФЕРА» встановлені ліцензійні пакети Microsoft Office Professional 2016.

Компоненти: Access, Excel, Outlook, Outlook і Business Contact Manager, PowerPoint, Publisher, Word.

Спільна робота: Microsoft Office інтегрується зі службами Microsoft Windows SharePoint, забезпечуючи додатки, що дозволяють підвищити продуктивність праці як окремого користувача, так і всього підприємства. Можна працювати над документами разом з допомогою вдосконалених функцій, таких як управління версіями, і більш ефективно проводити збори. Робочі області для зборів у Microsoft Office дозволяють спільно використовувати документи в реальному часі, а система передачі миттєвих

повідомлень забезпечує широкі можливості обміну даними в будь-який час і в будь-якому місці.

3) Антивірусний захист.

На підприємстві ТОВ «СФЕРА» на кожній робочій станції встановлено ліцензійну копію антивірусу ESET NOD32 RU.

Опис: Eset NOD32 - це комплексне антивірусне рішення для захисту в реальному часі від широкого кола загроз.

Підтримка – Windows Server 2012, 2016, Windows 7, 8, 10.

4) Система телефонного зв’язку.

На підприємстві встановлений телефонний росподільний щиток який на пряму з’єднаний з АТС «Укртелеком», відстань до якого 1500 метрів.

На підприємстві ТОВ «Сфера» встановлено одинадцять (10) телефонних апаратів у кожному відділі по одному апарату, а також один у директора і один у секретаря. Схема телефонної мережі зображено у додатку Б.

Даного програмного забезпечення на підприємстві ТОВ «СФЕРА» вистачає для виконання створення, обробки та використання інформації. Але недостатньо для захисту від несанкціонованого доступу і інших загроз її цілісності, доступності й достовірності.

5) Класифікація інформаційної системи та її елементів.

Для зручності подальших посилань на клас категорії введемо буквено-цифрове позначення (літера "Д" означає "доступність", "Ц" - "цілісність", "К" - "конфіденційність", цифри зростають з убуванням значущості критерію).

Класифікація інформаційних об'єктів.

За доступності або наявності:

Д0 - критична інформація (робота суб'єкта буде зупинена);

Д1 - дуже важлива інформація (суб'єкт буде працювати, але короткий час);

Д2 - важлива інформація (суб'єкт може працювати без цієї інформації деякий час, але вона скоро знадобиться);

Д3 - корисна інформація (без інформації можна працювати, але її використання економить ресурс);

Д4 - не суттєва інформація (застаріла або невикористовувані, не впливає на роботу суб'єктів інформація);

Д5 - шкідлива інформація (наявність такої інформації вимагає обробки, а обробка веде перевитрати ресурсів).

За несанкціонованої модифікації або цілісності:

Ц0 - критична інформація (несанкціоноване зміна приведе до неправильної роботи всього підприємства або значної його частини; наслідки такої модифікації незворотні);

Ц1 - дуже важлива інформація (несанкціоноване зміна приводить до невірної роботі всього підприємства або його частини через деякий час, якщо не будуть вжиті деякі дії; наслідки такої модифікації незворотні);

Ц2 - важлива інформація (несанкціоноване зміна призводить до неправильної роботи частини підприємства через деякий час, якщо не будуть вжиті деякі дії; наслідки такої модифікації оборотні);

Ц3 - значима інформація (несанкціоноване зміна позначиться через деякий час, але не призведе до збою в системі; наслідки такої модифікації оборотні);

Ц4 - незначний інформація (несанкціоноване зміна не позначиться на роботі системи).

За розголошенню чи конфіденційності:

К0 - критична інформація (розголошення призведе до краху підприємства або значних матеріальних втрат);

К1 - дуже важлива інформація (розголошення призведе до значних матеріальних втрат, якщо не будуть прийняті які-небудь заходи);

К2 - важлива інформація (розголошення призведе до деяких матеріальним або моральним втрат, можливим непрямим, якщо не будуть вжиті деякі дії);

К3 - значима інформація (приносить моральну шкоду, може бути використана в певний момент);

К4 - незначне інформація (може принести моральний збиток у дуже рідкісних випадках);

К5 - незначний інформація (не впливає на роботу суб'єкта).

Класифікація інформаційної системи та її елементів зображено у таблиці 1.3.

Таблиця 1.3 – Класифікація інформаційної системи та її елементи

№	Найменування	За доступності	За цілісності	За конфіденційності
1	Бухгалтерська інформація (податкові накладні, бухгалтерські звіти, інформація про платежі, про платню)	Д2	Ц2	К1
2	Фінансова інформація	Д1	Ц1	К1
3	Договори та листи замовлення	Д1	Ц2	К1
4	Виробнича інформація по проектах	Д3	Ц3	К3
5	Інформація про клієнтів	Д2	Ц3	К2
6	Інформація про співробітників	Д3	Ц4	К4
7	Інформація про плани підприємства	Д1	Ц2	К1

1.2.4 Середовище користувачів

Середовище користувачів обчислювальної системи підприємства ТОВ «Сфера» є ненадійною відносно загроз зв’язаних з несанкціонованим доступом до інформації що оброблюється на підприємстві, а також може викликати помилки при створенні, обробці, зберіганню та передачі інформації.

Опис середовищ:

На підприємстві усі відділи працюють у однакових середовищах користувачів.

Представляє собою використання операційної системи Windows 10 з її службами та системами захисту інформації. Також використовується Microsoft Office 2016 для створення та обробки документів які потрібні у виробничому процесі підприємства.

Вхід в систему користувачів виконується без вводу «логіну» та «паролю». Обліковий запис має обмежені повноваження, що надає користувачу усіх повноважень щодо створення документів виробничих процесів, їх змінення та зберігання, але не надає прав щодо встановлення та видалення програмного забезпечення.

Уся інформація що обробляється на комп'ютерах користувачів зберігається на жорсткому диску і копіюється на інші комп'ютери та сервер обчислювальної системи підприємства. Такий підхід має достатньо недоліків, а також у разі видалення або змінення є неможливим до відновлення.

- Управління доступом що діє на підприємстві

Матриця управління доступом к оброблювальній інформації на підприємстві (R – читання; A – додавання, з можливістю знищення набранного текста; D – знищення; W – змінення; M – запис.) таблиця 1.4.

Таблиця 1.4 – Матриця управління доступом

Об'єкт							
Суб'єкти	про співробітників підприємства	про поточні операції		бухгалтерський облік		Про грошові платежі	Юридичні дані та документи.
		замовлення	Виконання	Державна звітність	Внутрішній бух. облік		
Системний адміністратор	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M
Фінансовий відділ	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M
Відділ кадрів	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M
Відділ постачання	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M
Директор	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M
Секретар	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M
Бухгалтерія	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M
Відділ розрахунків по заробітній платі	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M
Проектно-кошторисний відділ	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M

Начальник з виробництва	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M	R A D W M

1.3 Перелік існуючих елементів захисту інформації на підприємстві

На підприємстві ТОВ «Сфера» встановлено ліцензійні копії антивірусної програми ESET NOD32 Business Edition на кожен комп’ютер обчислювальної системи підприємства.

Рішення ESET NOD32 Business Edition розроблено для мереж великих і середніх організацій і забезпечує захист файлових серверів і робочих станцій компанії. ESET NOD32 Business Edition забезпечує виявлення і блокування вірусів, троянських програм, черв'яків, шпигунських програм, рекламного ПЗ, фішинг-атак, руткітів і інших інтернет-загроз, які становлять небезпеку для компаній. Незважаючи на мінімальну потребу в ресурсах, дане рішення забезпечує неперевершений рівень про активного захисту, практично не знижуючи продуктивність комп'ютера. ESET NOD32 Business Edition забезпечує підтримку файлових серверів Windows, Novell Netware та Linux / FreeBSD.

Також на сервері підприємства ТОВ «СФЕРА» встановлено ліцензійну копію брандмауера Outpost Firewall Pro, який забезпечує захист від зовнішніх Інтернет – атак.

Основні переваги Outpost Firewall Pro:

- безпечний доступ в Інтернет;
- упереджувальний захист від загроз;
- повна перемога над шпигунським ПЗ;
- безпечне перебування у Інтернеті;
- непробивна самозахист;
- робота з високою продуктивністю;
- потужний захист, яка є простою у використанні.

Встановлене ПЗ на підприємстві забезпечує мінімальний захист системи від поширених Інтернет – атак (троянські програми, черв'яки, шпигунські програми, рекламного ПЗ та інше), але не може забезпечити усіх потреб підприємства.

1.4 Модель порушника

Типи зловмисників, які випадково чи спеціально, діяльністю чи бездіяльністю можуть нанести збитків інформаційній системі ТОВ «Сфера» класифіковані по категоріям та представлені в вигляді таблиці 1.5.

Ймовірності реалізації загроз, які може нанести кожний із виділених груп зловмисників, за 5-бальною шкалою: I - низька; II – незначна; III – середня; IV – вагома; V - висока.

Таблиця 1.5 – Модель порушника

Позначення	Категорія (тип) порушника	Рівень загрози
Внутрішні		
A1	Директор	V
A2	Системний адміністратор	IV
A3	Начальник по персоналу	IV
A4	Працівники організації, що мають доступ до конфіденційної інформації	III
A5	Секретар	II
A6	Начальник охорони, Охоронці	I
A7	Прибиральниця	I
Зовнішні		
B1	Підрядчики, найняті задля виконання тих чи інших робіт	IV
B2	Недобросовісні конкуренти	IV
B3	Відвідувачі	III
B4	Будь-які персони, що знаходяться за межами КЗ	I

1.5 Аналіз загроз

В цій моделі, визначені властивості захищеності інформаційних об’єктів, які можуть бути порушеними – конфіденційність (к), цілісність (ц), доступність (д) та якісна оцінка ймовірності здійснення загроз та рівнів збитків (шкоди) по кожному з видів порушень.

Оцінка збитків що очікуємо:

I – Без ризикова зона – область, у якій випадкові збитки не очікуються.

II – Зона допустимого ризику – область, у межах якої зберігається економічна вигода підприємницької діяльності, тобто випадкові збитки можуть мати місце, але вони менші за очікуваний прибуток від діяльності.

III – Зона критичного ризику – область, з можливістю збитків, які є більшими за очікуваний прибуток, до значення повної розрахункової виручки від підприємницької діяльності.

IV – Зона катастрофічного ризику - область можливих збитків, які за своїм об’ємом є вищими за критичний рівень та можуть досягати значення повного об’єму майнового стану підприємця.

Оцінка вірогідності реалізації ризику проводиться за імовірнісної шкалою: I – велика; II – середня; III – низька. Перелік загроз виконано у вигляді таблиці 1.6.

Д – Доступність; Ц – Цілісність; К – Конфіденційність.

Таблиця 1.6 – Аналіз загроз

Можливі загрози інформації	Модель порушника	Властивість інформації	Оцінка можливих збитків	Оцінка вірогідності реалізації ризику
		К, Ц, Д		
1	2	3	4	5
Загрози, забезпечені технічними засобами				
Відмови у мережі енергопостачання	--	Ц, Д	III	II
Відмови технічних засобів обробки інформації				

Відмови компонентів комп'ютерів	--	Ц, Д	III	I
Відмови принтерів	--	Ц, Д	III	II
Загрози, забезпечені діяльністю суб'єктів				
Викрадення:				
Технічних засобів	А2-7, В1-2, В4	К, Ц, Д	IV	I
Носіїв інформації	А2-7	К, Ц, Д	IV	I
Інформації	А2-7, В1-2	К, Ц, Д	IV	I

Продовження таблиці 1.6

1	2	3	4	5
Модифікація:				
Програмних засобів	А1, А2	К, Ц, Д	IV	II
Даних	А1-7	К, Ц, Д	IV	II
Паролів та правил доступу	А-3	К, Ц, Д	IV	II
Знищення:				
Технічних засобів	А2-7, В1-3	Ц, Д	IV	II
Носіїв інформації	А2-7	Ц, Д	IV	II
Програмного забезпечення	А-2	Ц, Д	IV	II
Інформації	А1-7, В1-2,	Ц, Д	IV	II
Переривання:				
Пропускної здатності каналів зв'язку	А2-7, В1-3	Ц, Д	III	I
Об'ємів вільної операційної пам'яті	А-3	Ц, Д	III	I
Об'ємів вільного дискового простору	А1-7	Ц, Д	III	I
Перехоплення інформації (несанкціоноване)				
За рахунок ПЕМВ від технічних засобів	В1-3	К	IV	I
За рахунок наводок по лініям електроживлення	В1-3	К	IV	I
За рахунок наводок по стороннім провідникам	В1-3	К	IV	I
При підключенні до каналів передачі інформації	В1-3	К	IV	I
За рахунок порушення встановлених правил доступу	А1-7, В1-3	К	IV	II

1.6 Постановка задачі. Висновок

При обстеженні підприємства ТОВ «Сфера» виявлена велика кількість недоліків обчислювальної та інформаційної системи, а також проведено аналіз моделей порушника та складено перелік можливих загроз для конфіденційної інформації на підприємстві.

Таким чином на підставі проведеного аналізу підприємства, згідно державних стандартів, є необхідність створення системи захисту від НСД.

Встановлено, що захисні заходи необхідно починати безпосередньо з організаційних заходів, які, у свою чергу, повинні відповідати державним вимогам щодо забезпечення режиму секретності робіт, що проводяться.

При створенні підсистеми захисту від НСД на підприємстві є необхідним задіяти вже існуючи елементи захисту інформації, а також проаналізувати і встановити нові програмні засоби захисту від НСД.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Технічне завдання

2.1.1 Найменування роботи та область застосування

Об'єкт розробки – автоматизована система ТОВ «Сфера».

Предмет розробки – підсистема захисту від несанкціонованого доступу.

Область застосування – автоматизована система ТОВ «Сфера».

2.1.2 Призначення розробки

Призначення роботи є розробка підсистеми захисту від несанкціонованого доступу автоматизованої системи підприємства, яка дозволить забезпечити підвищення рівня безпеки інформаційних ресурсів товариства з обмеженою відповідальністю «Сфера».

2.1.3 Етапи виконання робіт

2.1.3.1 Попередній

На цьому етапі необхідно:

- проаналізувати можливі загрози безпеки інформації;
- зробити аналіз нормативних документів у сфері інформаційної безпеки;
- вибрати функціональний профіль захищеності і клас АС.

2.1.3.2 Проектування і розробка

На цьому етапі необхідно:

- розробка системи захисту від несанкціонованого доступу;
- створити домен на основі ОС Windows Server;
- налаштувати клієнт Activ Directory;
- розробити правила доступу до інформації;
- провести аналіз існуючих програм розмежування доступу;
- розробка підсистеми розмежування доступу;

- налаштувати існуючі на підприємстві засоби захисту інформації.

2.1.3.3 Проведення випробувань і передача в експлуатацію

На цьому етапі необхідно:

- впровадити розроблені засоби та заходи;
- провести випробування і проаналізувати отримані результати;
- підготувати і передати технічну документацію для впровадження;
- оформити і затвердити акт про передачу на впровадження.

2.1.4 Економічні показники

У даній частині роботи потрібно оцінити витрати та розрахувати економічну рентабельність впровадження підсистеми захисту на підприємстві.

Дана інформація приведена в економічному розділу.

2.2 Система розмежування доступу до інформації на сервері та робочих станціях підприємства

2.2.1 Створення домену

Перший домен в лісі стає вершиною першого дерева в лісі. Домени Active Directory використовують систему імен DNS, наприклад "nttest.SFERA.com".

Налаштування контролера першого домену виконується у два етапи:

1) Установка Microsoft DNS Server.

2) Запуск майстра інсталяції Active Directory.

2.2.2 Установка Microsoft DNS Server

Клієнти Active Directory використовують DNS для пошуку контролерів домену. Microsoft рекомендує використовувати DNS-сервер, який входить до складу Windows 2016 , проте допускається використання і інших серверів DNS, якщо вони задовольняють певним функціональним вимогам[21].

Якщо DNS-сервер встановлено і налаштовано для підтримки домену Active Directory і контролерів цього домену, то можна перейти до наступного етапу. Якщо ні - Microsoft рекомендує встановити DNS на першому контролері домену.

Під час установки може бути виданий запит на встановлення статичної IP-адреси сервера. Сервери DNS вимагають для коректної роботи вказівки як мінімум одного постійного IP-адреси на комп'ютері.

Щоб встановити Microsoft DNS Server необхідно:

1) Ввести логін та пароль, використовуючи локальну обліковий запис адміністратора

2) У меню Start вибрати пункт Settings, а потім - пункт Control Panel.

3) Двічі натиснути по значку Add / Remove Programs.

4) Натиснути кнопку Add / Remove Windows Components.

Буде запущена програма-майстер Windows Components Wizard.

5) Вибираю пункт Networking Services і натискаюь кнопку Details.

6) Встановити під включене положення прапорець поруч із пунктом Dynamic Name Service (DNS).

7) Натиснути кнопку OK, щоб закрити діалогове вікно.

8) Натиснути кнопку Next для встановлення програмного забезпечення сервера DNS.

9) Якщо з'явиться запит з пропозицією вказати статичний IP-адресу, натискаю кнопку OK і виконую наступне:

а) У діалоговому вікні Local Area Connection Properties, яке повинне з'явитися після цього, вибрати пункт Internet Protocol (TCP / IP) і натиснути кнопку Properties.

б) Встановити перемикач в положення Use the following IP address і вказуючи значення в полях IP address, Subnet mask і Default Gateway.

в) Встановити перемикач в положення Use the following DNS server addresses і ввести IP-адресу сервера DNS у полі Primary DNS Server.

г) Натиснути кнопку OK, щоб закрити діалогове вікно Internet Protocol (TCP / IP) Properties.

д) Натиснути кнопку OK, щоб закрити панель Connection configuration.

е) Натиснути кнопку Finish для завершення установки DNS.

10) Закрити вікно Add / Remove Programs. DNS-сервер встановлений.

2.2.3 Запуск майстра інсталяції Active Directory

Підвищення статусу серверів до контролерів домену відбувається за допомогою програми-майстра інсталяції Active Directory, відомої також під назвою DCpromo[10].

Для запуску DCpromo необхідно:

1) У меню Start вибирати пункт Run.

2) Ввести dcpromo та натиснути кнопку OK.

3) Буде запущена програма-майстер DCpromo. Натиснути кнопку Next, щоб продовжити роботу з нею.

4) Якщо з'явиться повідомлення про те, що обраний шлях не належить розділу NTFS і в системі існує тільки розділ FAT, доведеться перетворити його в NTFS. Якщо це повідомлення не з'явиться - пропускаю наступні два пункти.

- Натиснути кнопку OK, щоб закрити вікно повідомлення.
- Натиснути кнопку Cancel, щоб перервати роботу DCpromo.
- У меню Start вибрати пункт Programs, а потім пункт Command Prompt.
- Ввести команду: convert <drive:> / FS: NTFS, де <drive:> - ім'я логічного диска, де встановлена Windows 2016.
- Утиліта Convert повідомить про поточну файлову систему розділу і проінформує про необхідність перезавантаження. Ввести Y та натиснути клавішу Enter.
- Перезавантажити систему. Логічний том буде перетворений в NTFS в процесі завантаження. Зареєструватись і знову запустити DCpromo, прогорнути вікна до вікна System Volume path і продовжити роботу.

5) Вибрати пункт New domain і натискаю кнопку Next.

6) Вибрати пункт Create new domain tree і натискаю кнопку Next.

7) Вибрати пункт Create a new forest of domain trees і натискаю кнопку Next.

8) Ввести повне DNS-ім'я, для свого домену Active Directory, наприклад "nttest.SFERA.com", і натиснути кнопку Next. DCpromo перевіряю, чи не використовується вже введене ім'я.

9) DCpromo запропонує NetBIOS-ім'я домену. Для забезпечення зворотної сумісності з такими клієнтами, як Windows NT 4.0, це ім'я буде використовуватися ними для ідентифікації домену. Використовуйте запропоноване ім'я і натискаю кнопку Next.

10) DCpromo запропонує шлях для розміщення бази даних і файлів журналу Active Directory. Вказати новий шлях, а потім натиснути кнопку Next.

11) DCpromo запропонує шлях до файлу для створення резервної копії системного тому. Вказати новий шлях, а потім натиснути кнопку Next.

12) Якщо з'явиться попередження про те, що DCpromo не може зв'язатися з DNS-сервером для вирішення зазначеного імені, натиснути кнопку OK.

13) Вибрати Yes, щоб DCpromo налаштував для DNS і натиснути кнопку Next.

14) Натиснути кнопку Next для запуску процесу підвищення статусу. Він займе кілька хвилин.

15) Натиснути кнопку Finish.

16) Натиснути кнопку Restart Now, щоб перезавантажити комп'ютер.

2.2.4 Додавання серверів і робочих станцій в домен

На комп'ютерах, що працюють під управлінням Windows 2016 , необхідно налаштувати як мінімум один IP-адрес сервера DNS, щоб вони могли виявити контролер домену в процесі підключення. IP-адреса DNS-сервера може повідомлятися клієнтським системам автоматично за допомогою DHCP або встановлюватися вручну у вікні налаштування мережевих з'єднань[10, 16].

Облікові записи для підключаються комп'ютерів можна створити в домені заздалегідь або в процесі приєднання до домену.

Включення в домен Windows 2016 робочих станцій, що працюють під управлінням Windows, проводиться таким чином.

Щоб приєднати сервер або робочу станцію Windows до домену необхідно:

1) У меню Start вибрати пункт Settings, а потім - пункт Control Panel.
2) Натиснути двічі по значку System.

3) Натиснути на закладці Network Identification.

4) Натиснути кнопку Change, щоб змінити статус членства комп'ютера.

5) У списку Member of вибрати пункт Windows secure domain.

6) У поточному полі введення вказати повне DNS-ім'я домену, до якого приєднати комп'ютер ("nttest.SFERA.com").

7) Натиснути кнопку OK.

8) Ввести ім'я та пароль облікового запису домену, що володіє достатніми привілеями для виконання операції приєднання комп'ютера до домену. Ввести ім'я та пароль користувача, який має повноваження на створення об'єктів у використовуваному за умовчанням контейнері Computers. Повноважень адміністратора домену буде достатньо.

9) Натиснути кнопку OK для відправки імені та пароля.

10) Натиснути кнопку OK.

11) Натиснути кнопку OK, щоб закрити вікно попередження про перезавантаження.

12) Натиснути кнопку OK, щоб закрити панель System.

13) Натиснути кнопку Yes для перезавантаження комп'ютера.

Створюємо загальну папку яка містить такі підпапки:

- Директор_ДОК;
- Начальник_персонал_ДОК;
- Проектно_кошторисний_ДОК;
- Розрахунки_ДОК;
- Бухгалтерія_ДОК;
- Кадри_ДОК;
- Фінанси_ДОК;
- Постачання_ДОК;
- Секретар_ДОК.

Створюємо доменні групи:

- Proekt;
- Cash;

- Buhgalteria;
- Kadri;
- Finans;
- Finanse.

Окремі користувачі:

- DokAdmin;
- Chif;
- Secretary;
- Chif_Kadri;

Усі користувачі та доменні групи, окрім Директора, адміністратора безпеки і системного адміністратора, мають право:

- запис інформації на сервер, згідно своїх прав;
- читання інформації з серверу, згідно своїх прав.

Забороняється:

- видалення інформації на сервері;
- змінення інформації на сервері;
- копіювання інформації з сервера.

Доменній групі – DomainAdmins та користувачеві – Директор, надаються права адміністраторів системи.

2.2.5 Налаштування об’єктів Active Directory

2.2.5.1 Групові політики

Служба каталогів полегшує роботу IT-підрозділу з адміністрування інформаційних ресурсів підприємства. Технології Intellimirror і CCM (Change and Configuration Management - управління змінами і конфігураціями) дозволяють управляти робочими місцями, використовуючи переміщувані профілі і пере направлення каталогів, автономні папки та розповсюдження програм. Багато хто з цих завдань легко виконуються за допомогою групових політик, забезпечуючи при цьому централізоване управління, а також гнучкий механізм настройки і відладки [8-10]. Групові політики дозволяють:

- призначати сценарії запуску, входу і виходу;
- поширювати програмне забезпечення в мережі за допомогою публікації або призначення;
- однозначно визначати набір налаштувань безпеки для віддалених машин;
- визначати політики паролів для користувачів домену;
- конфігурувати параметри Internet Explorer;
- налаштовувати пере направлення окремих папок з профілю користувача;
- накладати обмеження на робочий стіл;
- визначати налаштування таких категорій, як автономні папки, дискові квоти та інші, не винятком є налаштування самих групових політик.

Всі налаштування адміністратор може зробити за допомогою редактора реєстру, але інтуїтивно зрозумілий інтерфейс редактора об'єктів групової політики багато в чому спрощує це завдання.

2.2.5.2 Структура об'єктів групової політики і їх місце в службі каталогів

Об'єкт групової політики (GPO, Group Policy Object) складається з двох частин: конфігурація комп'ютера (Computer Configuration) і конфігурація користувача (User Configuration) вказано на рисунку 2.1. Він є контейнером для груп політик, застосовуваних відповідно до машин і користувачам мережі.

У «Конфігурації комп'ютера» адміністратор може налаштувати параметри безпеки, політики паролів користувачів, параметри аудиту, використання груп з обмеженим доступом (Restricted Groups), параметри реєстру і так далі.

Як вже говорилося, GPO містить у собі два вузли, в яких визначаються специфічні для комп'ютерів і користувачів налаштування. Проте буває, що існують ідентичні налаштування для комп'ютерів і користувачів. Як система «розрулює» їх застосування, буде розказано далі.

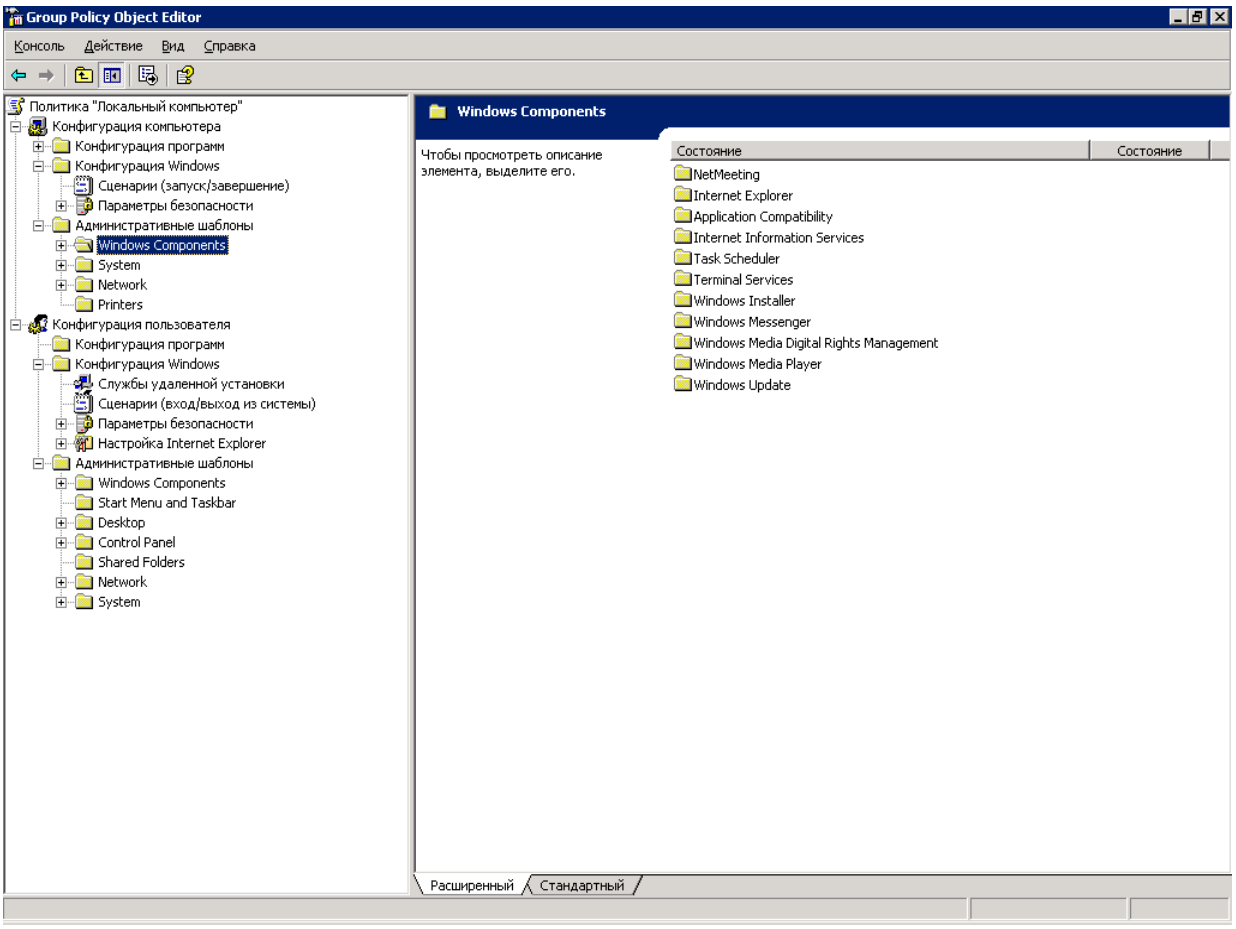


Рисунок 2.1 – Редактор групових політик gpedit.msc

Кожна політика в об'єкті GPO може бути налаштована і немає. У першому випадку вона впливає на об'єкт і може бути в змозі включено / вимкнено, а також приймати значення із зазначенням додаткових параметрів. У другому – політика на об'єкт не впливає.

Об'єкти групових політик зберігаються двома частинами: контейнер групової політики (GPC, Group Policy Container) і шаблон групової політики (GPT, Group Policy Template). Контейнер зберігається безпосередньо в службі каталогів і містить інформацію про властивості, версії, статус і список компонентів. Шаблони GPT знаходяться в каталозі \ Windows \ SYSVOL \ sysvol \ Domain_Name \ Policies \ GUID, де GUID – Глобальний унікальний ідентифікатор об'єкта GPO.

У цій папці містяться адміністративні шаблони (ADM - файли), налаштування безпеки, інформація про доступні додатках та імена сценаріїв з командними рядками.

2.2.5.3 Локальні політики робочої станції

Кожна робоча станція під управлінням операційних систем сімейства Windows має свої локальні політики, та адміністратор домену має можливість редагувати їх. Вони схожі з груповими політиками домену, але застосовуються для всіх локальних користувачів комп'ютера без винятку. Також неможливо налаштувати ряд установок, таких, наприклад, як пере направлення каталогів і встановлення додатків. Незважаючи на це, структура об'єкта локальних групових політик така ж, як і GPO домену. Розміщується він у папці \ Windows \ system32 \ GroupPolicy.

За допомогою команди gpedit.msc ви можете редагувати локальні політики робочої станції. Синтаксис рядка для запуску gpedit.msc для перегляду локальної політики віддаленої машини буде виглядати наступним чином: Gpedit.msc / gpcomputer: ім'я комп'ютера

2.2.6 Контроль доступу до ресурсів

Існує два типи прав, які можна налаштувати на ресурсі. Є NTFS права, а також права на загальний доступ (share permission).

Процес ручного настроювання об'єктів Active Directory аналогічний, але існує майстер (Wizard), який може значно полегшити настройку. Це дуже зручний майстер, тому що існує понад 1000 персональних прав на деякі об'єкти Active Directory, такі як організаційні одиниці. Як встановлювати (частково) права, вказано на рисунку 2.3 [10-12].

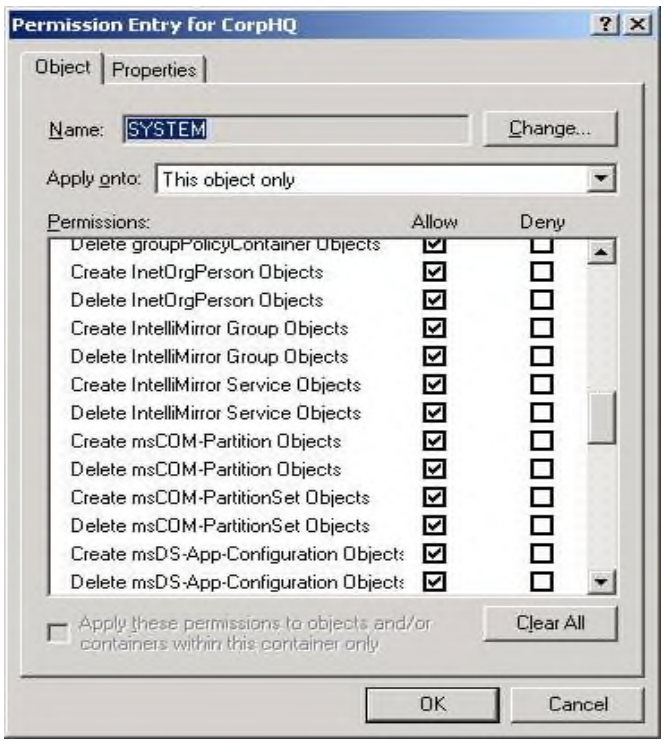


Рисунок 2.2 – Частковий список прав для організаційної одиниці

Для доступу до майстра тиснемо правою кнопкою миші на вузол, який міняємо. З'явиться меню Delegate Control. Після його вибору з'явиться діалогове вікно майстра Delegation of Control Wizard. Цей майстер дозволяє задати "хто" (користувач або група) буде мати "цей" рівень доступу (ці права) для об'єктів в Active Directory.

2.2.7 Розмежування доступу до мережі Інтернет

Я буду використовувати Proxy-сервер Usergate який дає можливість встановлення почтового серверу, розмежування доступу у Інтернет, а також контроль трафіку користувачів обчислювальної системи підприємства «Сфера».

Опис поштового серверу UserGate Mail Server:

- Організація роботи електронної пошти

У числі основних функцій UserGate Mail Server - управління доменами і користувачами, веб-клієнт, підтримка списків розсилки, робота віддаленими обліковими записами, підтримка LDAP, а також гнучка і потужна система правил.

- Безпека:

Для забезпечення безпечного доступу до пошти в програмі реалізована підтримка протоколів SSL, POP3s, SMTPs і IMAPs. У UserGate Mail Server інтегровані модулі антивірусної перевірки листів.

- Антиспам:

Основний модуль захисту від спаму побудований на технології компанії Commtouch, також використовується багатьма відомими виробниками програмних продуктів і апаратних рішень. Робота модуля заснована на Recurrent Pattern Detection, контент-агностичним технології, здатної виявляти і блокувати спам на будь-якій мові. В якості додаткового засобу боротьби зі спамом використовується безкоштовний SpamAssassin, що поєднує велику кількість методів аналізу, розпізнавання і блокування спам-повідомлень.

- Резервне копіювання:

UserGate Mail Server дозволяє серйозно знизити ризик втрати даних, завдяки підтримці процедури резервного копіювання. Програма підтримує резервне копіювання за розкладом, відновлення даних з резервної копії як на тому ж сервері, так і на іншому.

Необхідністю встановлення Proxy-сервер Usergate є створення єдиного кеш-простору його організації дозволить скоротити вхідний трафік і прискорить пошук в Internet документів, вже отриманих ким-небудь із співробітників.

Proxy-сервер UserGate реалізує:

Забезпечення та контроль доступу в мережу Інтернет

Індивідуальний доступ до мережі Інтернет:

- для кожного співробітника компанії адміністратор задає параметри доступу в мережу Інтернет:
- входить і вихідна швидкість з'єднання;
- розподіл ширини Інтернет - смуги;
- дозволені програми (наприклад, можливість використовувати тільки Microsoft Edge як браузер).

Оптимізація роботи співробітників у мережі Інтернет

За статистикою, більше 80% співробітників використовують робочий час в особистих цілях, наприклад, спілкуються з однокласниками, листуються з друзями, скачують музику та фільми. Оптимізувати роботу співробітників допоможе UserGate, обмеживши доступ до непотрібних для роботи сайтам, заборонивши скачування файлів таких розширень, як *. mp3, *. avi та інші.

- Потужна система фільтрації веб-сайтів

Впровадження системи фільтрації веб-сайтів від компанії Bright Cloud значно поліпшило URL-filtering в UserGate. Досить вибрати небажані категорії, наприклад, "Знайомства" та "Ігри" і обмежити до них доступ. Таким чином, не потрібно постійно оновлювати списки небажаних веб-сайтів.

Дані сервери реалізують усі потреби підприємства що до захисту від несанкціонованого доступу у Інтернет, а також іншої інформації яка може зашкодити робото здатності підприємства.

2.2.8 Розроблені правила доступу до інформації на підприємстві

При аналізі інформаційного середовища було виявлено, що до інформації яка є конфіденційною мали доступ усі працівники підприємства.

Під час розробки системи розмежування доступу до інформації що циркулює на підприємстві ТОВ «Сфера» була розроблена нова матриця доступу яка зображена у таблиці 2.1 [6-7].

Таблиця 2.1 – Матриця управління доступом к оброблювальній інформації на підприємстві

Об’єкти							
Суб'єкти	про співробітників підприємства	про поточні операції		бухгалтерський облік		Про грошові платежі	Юридичні дані та документи.
		Замовлення	Виконання	Держ. звітність	Внутр. бух. облік		
Системний адміністратор	D	D	D	D	D	D	D
Фінансовий відділ	--	R	R A W M	R A M	--	R A M	R
Відділ кадрів	--	R	R	--	--	--	R A D W M
Відділ постачання	R	R	R	--	--	--	--

Продовження таблиці 2.1

Об’єкти							
Суб'єкти	про співробітників підприємства	про поточні операції		бухгалтерський облік		Про грошові платежі	Юридичні дані та документи.
		Замовлення	Виконання	Держ. звітність	Внутр. бух. облік		
Директор	R	R	R	R	R	R	R
Секретар	R	R M	R	R	R	R	R
Бухгалтерія	R	R	R	R A D W M	R A D W M	R A D W M	R
Відділ розрахунків по заробітній платі	R	R	R	R A D W M	R	R A D W M	R
Проектно-кошторисний відділ	R	R	R	--	--	--	R
Начальник з виробництва	R	R A D W M	R A D W M	R	--	R	R

Опис значень таблиці:

R – читання; A – додавання, з можливістю знищення набраного тексту; D – знищення; W – змінення; M – запис.

2.3 Програми для контролю і моніторингу доступу до різних пристроїв вводу, виводу та зберігання інформації

2.3.1 Програма FileControl

Основні функції FileControl – відображення підключених до комп'ютера пристроїв, дозвіл / заборона роботи з різними ними і запис операцій з файлами на цих пристроях. За діями користувача стежить спеціальний драйвер стеження, який встановлюється на кожен комп'ютер віддалено, із сервера [11-12, 15].

Управління доступом

FileControl контролює наступні пристрої і порти:

- USB порт і всі пристрої, що підключаються по USB (флешки, зовнішні жорсткі диски, фотокамери, стільникові телефони, mp3 плеєри, та ін), причому окремо від інших управляються USB принтери;
- оптичні DVD приводи;

- зовнішні порти введення-виведення - COM, LPT, інтерфейси Bluetooth і Wi-Fi.

Контроль доступу здійснюється як для комп'ютерів, так і для окремих користувачів Windows. Для пристроїв, доступ до яких має бути дозволений завжди (USB-ключі, сканери, принтери і т.п.), реалізований білий список.

Моніторинг та статистика

FileControl показує USB-пристрої, підключені до комп'ютерів, і веде журнал дій користувачів із зовнішніми накопичувачами інформації. Інформація про час підключення / відключення пристроїв і про те, які файли і коли були прочитані або записані, зберігається в базу даних. За допомогою зручної системи пошуку з фільтрами можна швидко знайти потрібні дані. Також є можливість експортувати ці дані в MS Excel.

Тіньове копіювання файлів

Програма без відома користувачів зберігає в окрему папку на сервері всі файли, які були прочитані з зовнішніх USB-дисків, або записувалися на них.

Простота встановлення та використання

Всі модулі програми містяться в одному дистрибутиві, який встановлюється на сервер в автоматичному режимі. Після цього треба вибрати комп'ютери локальної мережі для встановлення на них драйверів стеження. Це робиться дистанційно - можна вибирати як по одному, вказавши ім'я або IP адреса, так і відразу по кілька, вказавши діапазон IP адрес, або імпортувавши з Active Directory. Також можлива ручна установка драйверів стеження.

Пристрій і принципи роботи FileControl

FileControl складається з чотирьох модулів - всі вони містяться в одному дистрибутиві:

- Серверний

Представляє з себе сервіс, який постійно обмінюється інформацією з драйверами стеження. Встановлюється на сервері офісної локальної мережі дозволяє / забороняє ті або інші дії, зберігає інформацію в базу даних. Управляється за допомогою консолі адміністрування.

- Користувацький

Це драйвер стеження, керуючий доступом безпосередньо на клієнтських комп'ютерах і збирає інформацію про пристрої і файлах. Драйвери стеження встановлюються на комп'ютери локальної мережі дистанційно, через консоль адміністрування. Можлива також ручна установка на кожному комп'ютері.

- Адміністраторський

Панель управління, з якої здійснюється керування сервером FileControl, встановлення та видалення драйверів стеження, а також робота з базою даних.

- База даних

У FileControl інтегрована база даних SQLite. У ній зберігається вся інформація про комп'ютери, пристроях, файлах, і правила доступу. Запити до бази даних здійснюються через консоль адміністрування.

Єдиний спосіб повністю контролювати операції з файлами на зовнішніх пристроях – установка на всіх комп'ютерах локальної мережі драйвера, непомітного для користувачів комп'ютерів. Драйвер стеження FileControl – низькорівневий, що працює на рівні ядра ОС. Він відстежує всі операції запису або читання на знімні пристрої. При спробі запису або читання на пристрій, драйвер стеження перевіряє права доступу і діє відповідно до них, тобто дозволяє або забороняє дію. У той же момент на сервер відправляється інформація про вироблений дії. Установки рівня доступу драйвер стеження отримує з сервера в момент завантаження комп'ютера клієнта, або при зміні їх адміністратором.

Серверна частина FileControl – сервіс, який встановлюється на сервері. Цей модуль служить для збору даних від драйверів стеження і відправлення їм установок прав доступу. Зібрані дані про користувачів, їхніх пристроях, і роботі з файлами на цих пристроях сервіс зберігає в базу даних SQLite.

Панель управління FIleControl – це користувальницький інтерфейс програми. Служить для моніторингу підключених USB пристроїв, зміни прав доступу для користувачів, дистанційної установки драйверів стеження і пошуку

по базі даних. Представляє з себе exe-програма, яка може бути запущено з будь-якого комп'ютера в локальній мережі, а не тільки на сервері.

2.3.2 Програма DeviceLock

За допомогою програми DeviceLock можно [14]:

- Контролювати доступ користувачів і груп до пристроїв (CD / DVD-приводи, змінні накопичувачі, смартфони, жорсткі диски, локальні і мережеві принтери, WiFi, Bluetooth і т.п.) і портам вводу-виводу (USB, FireWire, COM, LPT).
- Дозволяти і забороняти доступ до певних типів файлів незалежно від встановлених на пристрій дозволів. Визначення типів файлів засноване на сигнатурному методі і не залежить від розширення файлу.
- Контролювати доступ користувачів і груп до пристроїв і портам вводу-виводу в залежності від часу та дня тижня.
- Для змінних носіїв, жорстких дисків, CD / DVD-приводів, можна встановлювати тип доступу "тільки читання".
- Застосовувати один набір політик для ситуації коли комп'ютер підключений до мережі й інший набір політик для ситуації, коли комп'ютер не підключений до мережі.
- Здійснювати повнотекстовий пошук по змісту файлів тіньового копіювання і журналів, що зберігаються на DeviceLock Enterprise Server. Повнотекстовий пошук особливо корисний у випадках, коли вам необхідний пошук по змісту документів, що зберігаються в базі даних тіньового копіювання. DeviceLock Search Server може автоматично розпізнавати, індексувати, знаходити і відображати документи безлічі форматів, таких як: Adobe Acrobat (PDF), Архіви (GZIP, RAR, ZIP), Lotus, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, OpenOffice (документи, таблиці та презентації) тощо.
- Встановлювати спеціальні "політики шифрування" для дисків, зашифрованих за допомогою сторонніх засобів шифровки. Використовуючи такі політики, наприклад, дозволити запис тільки зашифрованих даних на

знімні пристрої і заборонити запис незашифрованих даних. DeviceLock виявляє диски, створені продуктами ViPNet SafeDisk, PGP Whole Disk Encryption, DriveCrypt і TrueCrypt (USB-флешки та інші знімні пристрої), а також розпізнає флеш-диски, що підтримують апаратне шифрування даних.

- Захистити диски та змінні носії від випадкового або навмисного форматування.

- Для кожного користувача або групи задати своє "білий" список пристроїв, доступ до яких буде завжди дозволено. Пристрої можна ідентифікувати по моделі і по унікальний серійний номер.

- Ідентифікувати певний CD / DVD-диск на основі записаних на нього даних і вирішити його використання, навіть якщо сам CD / DVD-привод заблокований. Для кожного користувача або групи можна задати свій "білий" список носіїв.

- Надавати тимчасовий доступ до пристроїв за відсутності мережевого підключення до агента. Адміністратор повідомляє користувачеві спеціальний короткий буквено-цифровий код по телефону, який тимчасово розблоковує доступ тільки до потрібного пристрою.

- Протоколювати всі дії користувачів з пристроями і файлами (копіювання, читання, видалення і т.п.). Також можна протоколювати зміни в налаштуваннях DeviceLock, час старту і зупинки агента.

- Для кожного користувача або групи зберігати точну копію даних (тіньове копіювання), копійованих на зовнішні пристрої, що передаються через послідовні і паралельні порти, а також друкованих на локальних і мережевих принтерах. Точні копії всіх файлів і даних зберігаються в SQL-базі даних на сервері.

- Забезпечити необхідний рівень захисту навіть якщо користувачі в мережі мають адміністративні привілеї на локальних комп'ютерах. Коли захист DeviceLock включена, ніхто, крім авторизованих адміністраторів, не може підключатися до агента, зупиняти або видаляти його. Навіть члени локальної

групи Адміністратори (якщо вони не входять до списку авторизованих адміністраторів) не можуть обійти захист.

- Виявляти і блокувати роботу USB і PS/2-кейлогеров.
- За допомогою системи віддаленого управління, забезпечувати доступ до всіх можливих функцій програми з робочого місця адміністратора системи. DeviceLock Management Console представляє з себе оснастку (snap-in) для Microsoft Management Console, зі стандартним інтерфейсом, інтуїтивно зрозумілим будь-якому адміністратору Windows. Крім того, для управління DeviceLock в мережах, де не використовується Active Directory, передбачена додаткова консоль з власним інтерфейсом - DeviceLock Enterprise Manager.
- Керувати через групові політики Windows в домені Active Directory за допомогою стандартної оснащення Group Policy, яка входить до складу Windows. Повна інтеграція у групові політики Windows дозволяє автоматично встановлювати DeviceLock на нові комп'ютери, що підключаються до корпоративної мережі, і здійснювати настройку для нових комп'ютерів в автоматичному режимі.
- Оновлювати налаштування агентів на відключених від мережі комп'ютерах шляхом створення файлів з настройками та передачі їх користувачам, чиї комп'ютери не підключені до мережі і знаходяться поза досяжністю консолей управління. Для запобігання неавторизованих змін в настройках ці файли можуть бути підписані за допомогою електронного цифрового підпису.
- Встановлювати агенти з зумовленими настройками. Агенти можуть бути встановлені на віддалені комп'ютери з уже певними політиками безпеки (налаштуваннями) шляхом розгортання спеціально створеного установчого пакета Microsoft Installer (MSI). Такий MSI-пакет створюється адміністратором за допомогою стандартної консолі управління DeviceLock.
- Централізовано зберігати журнали аудиту та тіньового копіювання. Для централізованого збору та зберігання даних тіньового копіювання і журналів аудиту використовується додатковий компонент - DeviceLock

Enterprise Server. Ви можете встановити кілька примірників DeviceLock Enterprise Server у вашій мережі, щоб рівномірно розподілити навантаження. DeviceLock Enterprise Server використовує SQL-сервер для зберігання даних.

- Контролювати поточний стан агентів на віддалених комп'ютерах. DeviceLock Enterprise Server може періодично опитувати віддалені комп'ютери і зберігати в журнал моніторингу поточний стан, версію та відомості про налаштування кожного агента. Крім того, DeviceLock Enterprise Server порівнює поточні політики безпеки (налаштування) агентів на зазначених адміністратором комп'ютерах з еталонними політиками, збереженими в XML-файл, і записує інформацію про виявлені відхилення в журнал моніторингу. При цьому можлива автоматична заміна поточні політик безпеки на еталонні.

- Формувати графічні звіти на основі даних з журналів аудиту та тіньового копіювання, що зберігаються на сервері.

- Формувати звіти за встановленими настройок і по пристроям (USB, FireWire), які використовують користувачі на своїх комп'ютерах.

- Вибирати комп'ютери безпосередньо зі служб каталогів LDAP (таких як Novell, Open LDAP і т.п.).

- Використовувати потокове стиснення даних аудиту і тіньового копіювання, пересилаються з віддалених агентів на DeviceLock Enterprise Server, для зменшення обсягу переданої по мережі інформації і зниження навантаження на мережу.

- Використовувати автоматичний вибір оптимального сервера. Для передачі даних аудиту і тіньового копіювання, агенти можуть вибирати з своїх списків найбільш швидкі з доступних серверів.

- Використовувати контроль пропускної здатності мережі. DeviceLock може визначати баланс свого мережевого трафіку, дозволяючи вам обмежувати пропускну здатність мережі для даних аудиту і тіньового копіювання йдуть від агентів на DeviceLock Enterprise Server.2.3.3 Порівняльна характеристика програм DeviceLock та FileControl

Програма FileControl здійснює багато функцій блокування оптичних CD і DVD приводів, зовнішніх портів введення-виведення - COM, LPT; інтерфейси Bluetooth та Wi-Fi. Може бути інтегрований у Active Directory, вести тіньове копіювання файлів з носіїв, але цих функцій недостатньо для того щоб здійснювати повноцінний захист.

У той час програма DeviceLock забеспечює повний спектр функцій які виконує програма FileControl, але рівень захищеності який надає програма є набагато більшим. До них відносяться:

- для знімних носіїв можна встановлювати тип доступу "тільки читання";

- можна встановлювати графік користування пристроями вводу, виводу;

- можна призначати файлам типи доступу незалежно від встановлених налаштувань системи.

Відстеження усіх файлів які були скопійовані на сервер програми з розширенням Adobe Acrobat (PDF), Архіви (GZIP, RAR, ZIP), Lotus, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works, OpenOffice (документи, таблиці та презентації) тощо;

Захист файлів від випадкового та навмисного форматування;

Дозволяти доступ до пристроїв вводу-виводу користувачам або групам і створювати «білі списки» для них. Пристрої можна ідентифікувати по моделі і по унікальним серійним номерам;

Забезпечити необхідний рівень захисту навіть якщо користувачі в мережі мають адміністративні привілеї на локальних комп'ютерах;

Змінення, видалення або надання прав не відповідаючи статуту дозволено тільки авторизованим адміністраторам програми, навіть якщо є інші адміністратори у системі;

Забезпечити необхідний рівень захисту навіть якщо користувачі в мережі мають адміністративні привілеї на локальних комп'ютерах;

Керувати через групові політики Windows в домені Active Directory.

Ґрунтуючись на проведеної зрівняльної характеристиці, є цілком обґрунтований вибір програми DeviceLock для встановлення на сервер підприємства і усі комп’ютери локальної мережі.

При налагоджені системи було досягнуто результату зображеному на рисунку 2.4.

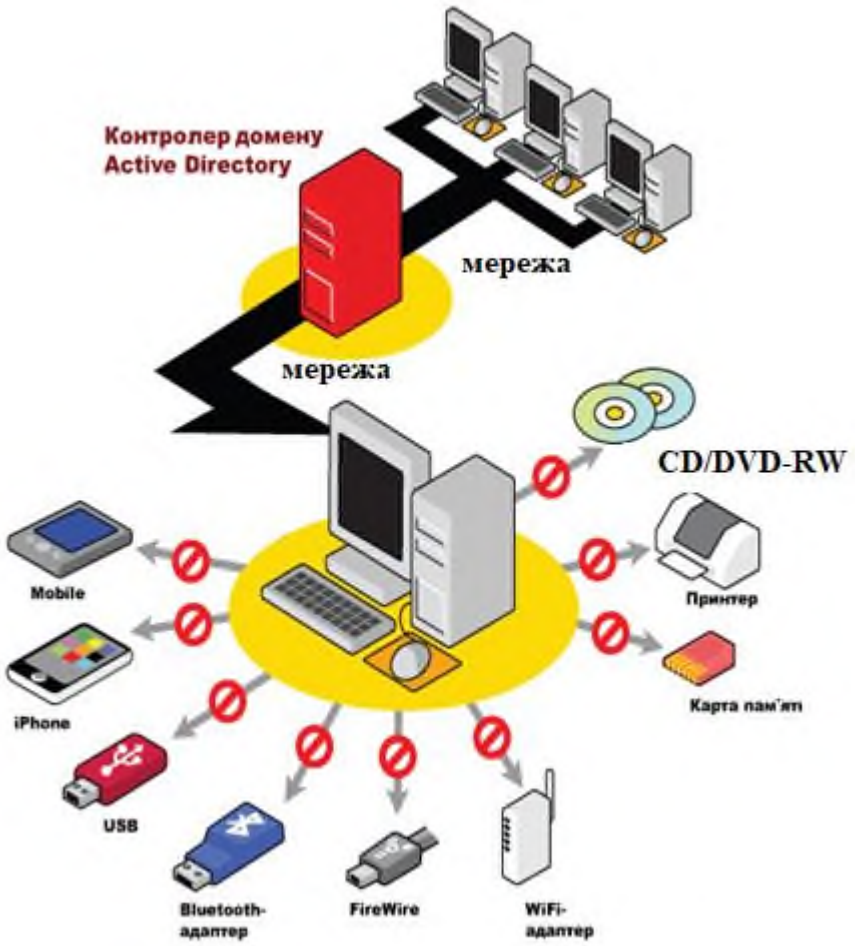


Рисунок 2.3 – Створена система розмежування доступу до пристроїв вводу-виводу

2.4 Програмні засоби захисту інформації

2.4.1 Налагодження параметрів мережевого екрана Outpost Firewall Profesional

Програмний мережевий екран.

Режим завантаження

Outpost Firewall Pro дозволяє контролювати свою поведінку під час запуску системи. Виконую настройку мережевого екрана у режим «блокувати усе» [17].

Заборонені програми

Будь-яка мережева активність додатків, що відносяться до цієї групи, блокується. Рекомендується додавати в цю групу програми, які не потребують доступу в мережу Інтернет, такі як текстові редактори, калькулятори тощо. Додавання програм зображено на рисунку 2.4.

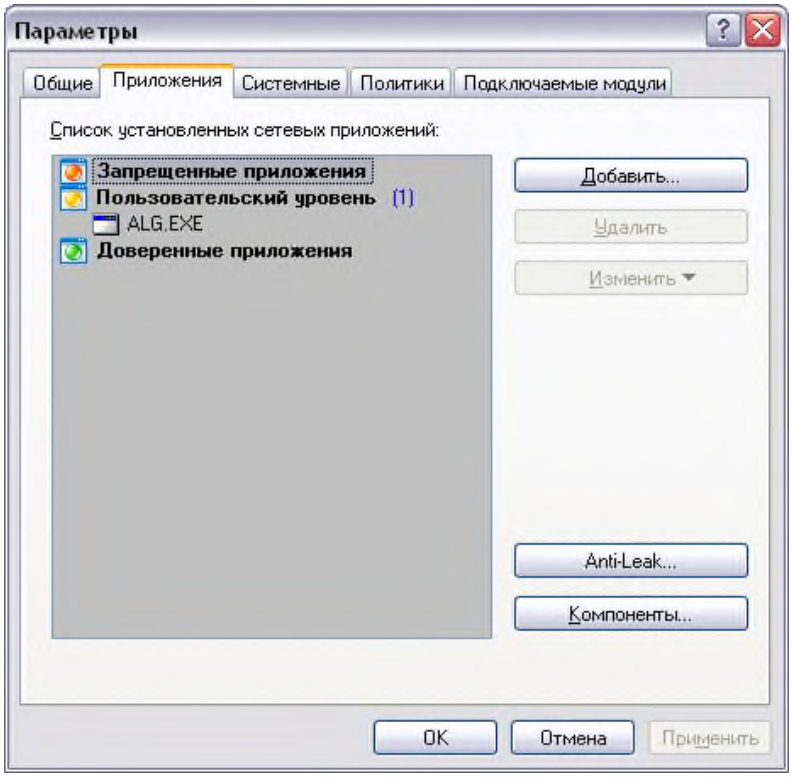


Рисунок 2.4 – Список програмних додатків

Довірені програми

Додатків, що належать до цієї групи, дозволена будь-яка мережева активність. Не рекомендується включати сюди програми.

Є можливість змінити статус програми та процесу, просто перетягнувши їх в потрібну категорію.

Налаштування політики брандмауера

Один з найбільш корисних і важливих параметрів Outpost Firewall Pro – політика брандмауера. Політика задає, яким чином Outpost Firewall Pro буде контролювати доступ вашого комп'ютера до Інтернету або іншої будь-якої мережі, до якої він підключений. Наприклад, політика Блокувати припускає особливо сувору позицію Outpost Firewall Pro, в той час як політика Дозволяти - навпаки, дуже м'яку.

Значок, відповідний кожному з режимів висвічуватиметься в системному лотку як піктограму Outpost Firewall Pro. Поглянувши на значок у системному лотку, ви відразу зможете сказати, в якому режимі працює брандмауер. Налаштування режиму брандмауера зображено на рисунку 2.5.

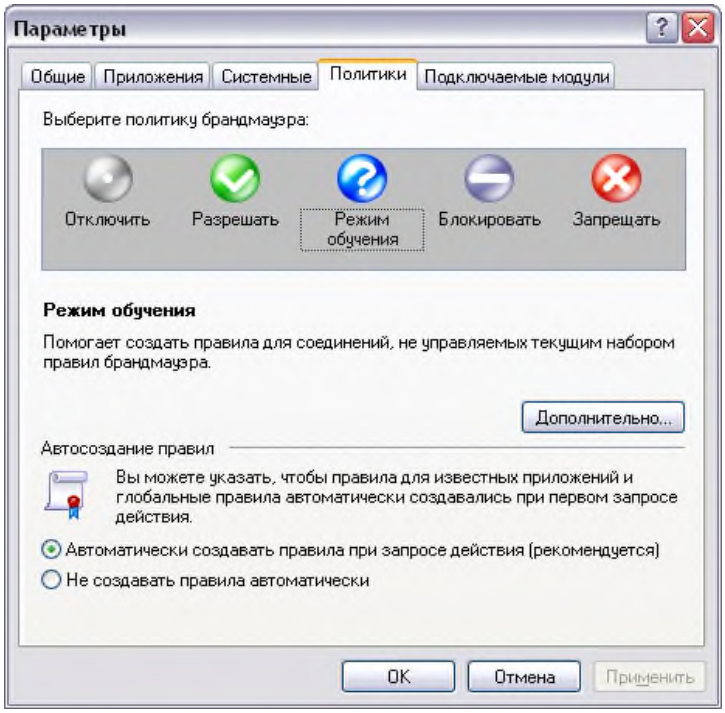


Рисунок 2.5 – Політика безпеки

Запобігання мережевих атак

Одним з найважливіших аспектів захисту за допомогою брандмауера є фільтрація вхідних пакетів, що використовується для контролю вхідної активності та блокування хакерів і шкідливих програм при їх спробі атакувати ваш комп'ютер.

Модуль Детектор атак виявляє, запобігає та повідомляє вас про всі можливі атаки на вашу систему з Інтернету і локальної мережі, до якої підключений комп'ютер. Модуль переглядає вхідні дані і визначає їх законність або за допомогою порівняння контрольних сум з відомими атаками, або виробляючи аналіз поведінки. Це дозволяє виявляти не лише відомі типи атак, такі як сканування портів, Відмова від обслуговування (Denial of Service, DoS-атаки), атаки класів 'short fragments' і 'my address' і багато інших, але також і майбутні загрози.

Блокування атакуючого

Після виявлення атаки Outpost Firewall Pro може змінювати свою поведінку, щоб автоматично захистити вас від можливих майбутніх атак з цієї адреси. Для цього встановіть прапорець Блокувати атакуючого на і всі дані з атакуючого комп'ютера будуть блокуватися протягом вказаного проміжку часу. За замовчуванням це 5 хвилин

Також можливо блокувати всю підмережа, до якої належить адреса атакуючого комп'ютера, вибравши параметр Блокувати підмережа атакуючого.

Захист від Ethernet-атак

Коли дані пересилаються по мережі з одного комп'ютера на інший, зразок комп'ютера розсилає ARP-запит для визначення MAC-адреси по IP-адресою цільового комп'ютера. Тим часом відправлення широкомовного повідомлення і відповіддю з Ethernet-адресою дані можуть піддаватися підміну, крадіжку чи несанкціонованому перенаправлення третій особі.

Завдяки контролю Ethernet-і Wi-Fi-з'єднань, модуль Детектор атак також виявляє і запобігає деякі Ethernet-атаки, такі як підробка IP-адреси (IP spoofing), сканування ARP, ARP-флуд та інші, захищаючи вашу систему від вторгнень з локальної мережі. Щоб вказати налаштування виявлення Ethernet-атак, виберіть вкладку Ethernet властивостей модуля.

Я використав даний мережевий екран тому що він вже встановлений на усіх комп’ютерах підприємства, але не був налагоджений відповідно до вимог інформаційної безпеки. Після налагодження програми Outpost Firewall Pro

виконує захист від мережевих атак на локальну систему підприємства ТОВ «Сфера», а також попереджає їх.

2.4.2 Антивірусна програма Eset NOD32

Опис програми:

Eset NOD32 – це комплексне антивірусне рішення для захисту в реальному часі від широкого кола загроз [20].

Підтримка - ОС Windows 7, 8, 10, Windows Server 2016.

- Проактивний захист і точне виявлення загроз. Антивірус ESET NOD32 розроблений на основі передової технології ThreatSense. Ядро програми забезпечує проактивне виявлення всіх типів загроз і лікування заражених файлів (у тому числі, в архівах) завдяки широкому застосуванню інтелектуальних технологій, поєднанню евристичних методів і традиційного сигнатурного детектування.

- Host Intrusion Prevention System (HIPS). Удосконалена система захисту від спроб зовнішнього впливу, здатних негативно вплинути на безпеку комп'ютера. Для моніторингу процесів, файлів і ключів реєстру HIPS використовується сполучення технологій поведінкового аналізу з можливостями мережного фільтра, що дозволяє ефективно детектувати, блокувати і запобігати подібним спроби вторгнення.

- Висока швидкість роботи. Робота Антивірусу ESET NOD32 не відбивається на продуктивності комп'ютера - сканування і процеси відновлення відбуваються практично непомітно для користувача, не навантажуючи систему.

- Зручність. Антивірус ESET NOD32 розроблений за принципом мінімального навантаження на систему і займає не більше 44 Мб пам'яті.

- Простота використання. Компактний і інтуїтивно зрозумілий користувальницький інтерфейс, мінімальні звернення до користувача при роботі роблять використання ESET NOD32 простим і зручним.

2.5 Структура локальної мережі

Після усіх налаштувань системи та проведених робіт по розмежуванню доступу до всієї інформації була змінена архітектура мережі на підприємстві ТОВ «Сфера» яка зображена на рисунку 2.6. Було налаштоване надійне розмежування доступу до інформації на рівні клієнта Active Directory та програми контролю (блокування) пристроїв вводу, виводу інформації, яка циркулює у обчислювальної системі підприємства ТОВ «Сфера».

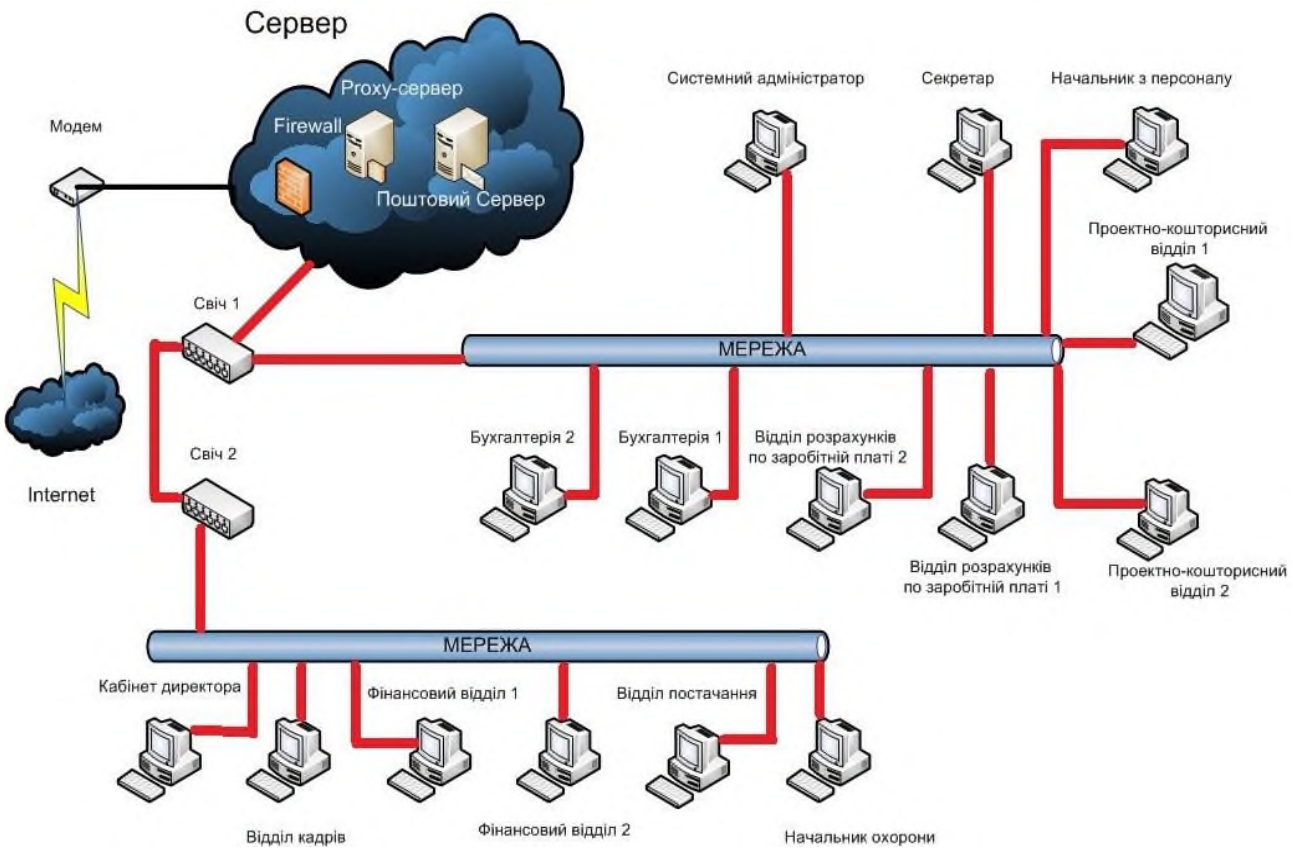


Рисунок 2.6 – Структура мережі після впроваджених заходів

2.6 Висновок

При виконанні технічного завдання було налаштовано систему розмежування доступу на сервер та комп’ютери обчислювальної системи за рахунок клієнту Active Directory у Windows 2016 в комбінації з програмою DeviceLock та існуючих засобів захисту інформації на підприємстві, що забезпечило надійний захист від НСД, як в середині підприємства, так і зовні.

Таким чином дана система захисту від НСД є надійною, актуальною, а також економічно вигідною для підприємства.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Розробка заходів щодо захисту від несанкціонованого доступу до інформації, яка циркулює на ОІД, потребує визначення витрат та показників економічної ефективності, що дозволить визначити економічну доцільність запропонованих заходів. Тому метою економічного розділу є обґрунтування економічної доцільності впровадження системи захисту інформації на підприємстві. З цією метою необхідно виконати наступні розрахунки:

– капітальні витрат 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 на підприємстві

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

– тривалість складання технічного завдання на розробку політики безпеки інформації, $t_{тз}$=4 годин;

– аналіз можливих загроз безпеки інформації, $t_{аз}$=14 годин;

– аналіз нормативних документів у сфері інформаційної безпеки, $t_{нд}$=8 годин;

– обрання функціонального профілю захищеності і класу АС, $t_{пз}$=10 годин;

– розробка системи захисту від несанкціонованого доступу, $t_{знд}$=18 годин;

– створення домену на основі ОС Windows Server, $t_{знд}$=3 години;

– налаштування клієнт Activ Directory, $t_{к}$=5 годин;

– розробка правила доступу до інформації, $t_{рпд}$=12 годин;

– аналіз існуючих програм розмежування доступу, $t_{апрд}$=6 годин;

– розробка підсистеми розмежування доступу, $t_{рпрд}$=8 годин;

– налаштування існуючих на підприємстві засобів захисту інформації $t_{нзз}$=8 годин;

– впровадження розроблених засобів та заходів, $t_{врз}$=4 години;

– проведення випробування і аналіз отриманих результатів, $t_{вар}$=4 години;

– підготування технічної документації для впровадження, $t_{техд}$=3 години;

– оформлення і затвердження акту про передачу на впровадження, $t_{оа}$=2 години.

Отже,

$$t = t_{тз}+ t_{аз}+ t_{нд}+ t_{пз}+ t_{знд}+ t_{знд}+ t_{к}+ t_{рпд} +t_{апрд}+ t_{рпрд}+ t_{нзз}+ t_{врз}+ t_{вар}+ t_{техд}+ t_{оа}=$$

$$= 4+14+8+10+18+3+5+12+6+8+8+4+4+3+2= 109 \text{ годин.}$$

Розрахунок витрат на розробку системи захисту інформації на підприємстві

Витрати на розробку системи захисту інформації на підприємстві Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 25070 + 345,53 = 25415,53 \text{ грн.}$$

$$З_{зп} = t\ З_{пр} = 109*230 = 25070 \text{ грн.}$$

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:

$$З_{мч} = t*С_{мч} = 109*3,17 = 345,53 \text{ грн.}$$

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

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = 0,6 \cdot 2 \cdot 1,64 + \frac{5400 \cdot 0,2}{1920} + \frac{4100 \cdot 0,3}{1920} = 3,17 \text{ грн.}$$

На всіх п’ятнадцятьох (15) комп’ютерах ТОВ «Сфера» встановлена ліцензійна версія Windows 10, яка є оптимальною операційною системою на користувальному рівні, а також реалізує усі потреби підприємства. На сервері встановлена ліцензійна версія Windows Server 2016. Також на

підприємстві ТОВ «СФЕРА» на кожній робочій станції встановлено ліцензійну копію антивірусу ESET NOD32 RU.

Відповідно до розроблених рекомендації щодо впровадження системи захисту інформації на підприємстві ТОВ «Сфера» планується використання програми DeviceLock, вартістю 2696,70 грн.

Таким чином, капітальні (фіксовані) витрати на створення політики безпеки інформації:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 25415,53+2696,70 = 28112,23 \text{ грн.}$$

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:

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

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

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

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ = 0 грн.).

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 ($С_н$ = 12000 грн.).

Річні амортизаційні відрахування програми DeviceLock, вартістю 2696,70 грн із корисним строком використання 2 роки, за прямолінійним методом нарахування амортизації складуть:

$$С_а = 2696,70 / 2 = 1348,35 \text{ грн.}$$

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 16000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,3 ставки. Отже,

$$С_з = (16000*12 + 16000*12*0,1)*0,3= 63360 \text{ грн.}$$

З 01.01.2019 р. Ставка ЄСВ для всіх категорій платників складає 22%.

$$С_{єв} = 63360*0,22 = 13939,2 \text{ грн.}$$

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=1,2 кВт);

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

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

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

$$С_{ел} = 1,2*1920*1,64 = 3778,56 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% (Стос = 28112,23*0,01=281,12 грн).

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

$$С_к = 12000+1348,35 +63360+13939,2+3778,56+281,12 = 94707,23 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 94707,23 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

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

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

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

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 9000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 12000 грн./міс.;

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

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 14 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 350 тис. грн. у рік;

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

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 28.

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:

$$П_П = \frac{\sum Зс}{F} \cdot t_n = \frac{12000 \cdot 14}{176} \cdot 4 = 3818{,}18 \quad \text{грн},$$

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 $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{12000 \cdot 14}{176} \cdot 3 = 2863{,}64 \text{ грн.}$$

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

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_в = \frac{9000 \cdot 1}{176} \cdot 2 = 102{,}27 \text{ грн.}$$

Витрати на заміни встаткування або запасних частин можуть скласти 1200 грн.

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

$$П_в = 2863{,}64 + 102{,}27 + 1200 = 4165{,}91 \text{ грн.}$$

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:

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

$$V = \frac{350000}{2080} \cdot (4 + 2 + 3) = 1177{,}88 \text{ грн.}$$

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.

$$U = 3818{,}18 + 4165{,}91 + 1177{,}88 = 9161{,}97 \text{ грн.}$$

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

$$B = \sum_i \sum_n U = \sum_1 \sum_{28} 9161{,}97 = 256535{,}2 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.},$$

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (70%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 256535{,}2 * 0{,}7 - 94707{,}23 = 84867{,}41 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

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

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

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{84867,41}{28112,23} = 3,02, \quad \text{частки одиниці,}$$

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, (20%);

$N_{інф}$ – річний рівень інфляції, (14%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$3,02 > (20 - 14)/100 = 3,02 > 0,06.$$

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{3,02} = 0,33, \quad \text{років.}$$

3.4 Висновок

Розробка впровадження системи захисту інформації на підприємстві ТОВ «Сфера» може вважатися економічно доцільною, виходячи зі значення коефіцієнт повернення інвестицій ROSI, що складає 3,02 при величині

економічного ефекту 84867,41 грн. Отримане значення коефіцієнта ROSI перевищує дохідність альтернативного вкладення коштів. Термін окупності при цьому складатиме 0,33 років (біля 4 місяців). Щорічні експлуатаційні витрати реалізацій заходів щодо захисту від несанкціонованого доступу до інформації, яка циркулює на ОІД ТОВ «Сфера» складають 94707,23 грн.

ВИСНОВКИ

При обстеженні підприємства ТОВ «Сфера» виявлена велика кількість недоліків інформаційної системи, а також проведено аналіз моделей порушника та складено список можливих загроз для конфіденційної інформації на підприємстві.

Таким чином на підставі проведеного аналізу підприємства, згідно державних стандартів, є не необхідність створення системи захисту від НСД.

При виконанні технічного завдання було налаштовано систему розмежування доступу на сервер та комп’ютери обчислювальної системи за рахунок клієнту Active Directory у Windows 2012 в комбінації з програмою DeviceLock та існуючих засобів захисту інформації на підприємстві, що забезпечило надійний захист від НСД, як в середині підприємства, так і зовні.

При порівняно невисокому рівні капітальних витрат, більшу частину яких становлять витрати на ліцензійне ПЗ, необхідне для побудови СЗІ мережі, розробка дає великий економічний ефект.

На основі виконаних розрахунків можна сказати, що з економічної точки зору розробка є ефективною та конкурентоспроможною.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про інформацію».

2. НД ТЗІ 3.7-001-99. «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі».

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

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

5. Закон України «Про державну таємницю».

6. Закон України ВР «Про захист інформації в інформаційно-телекомунікаційних системах».

7. Адміністративні шаблони (електрон. ресурс)/ спосіб доступу URL: http://stfw.ru/page.php?id=8724

8. Покрокове керівництво з використання сценаріїв диспетчера сервера (електрон. ресурс)/ спосіб доступу URL: http://www.microsoft.com/rus/windowsserver2012/docs/Server_Manager_Scenarios_in_WS12_Step-by-Step_Guide_ru/index.aspx.

9. Покрокове керівництво по розгортанню служби керування правами Active Directory в экстрамережі (електрон. ресурс)/ спосіб доступу URL: http://www.microsoft.com/rus/windowsserver2012/docs/Deploying_ADRMS_in_Extranet_WS12_Step-by-Step_Guide_ru/Deploying_ADRMS_in_Extranet_WS12_Step-by-Step_Guide_ru_index.aspx.

10. Програма для керування и мониторинга доступу до USB портів та різним приладам для вводу/виводу й зберігання інформації (електрон. ресурс)/ спосіб доступу URL: http://www.filecontrol.ru/.

11. Інтернет ресурс przone (електрон. ресурс)/ спосіб доступу URL: http://www.przone.ru/soft/prog40.html.

12. Інтернет ресурс пожежної служби (електрон. ресурс)/ спосіб доступу URL: http://arsenal01.ru/show/showgood.php?idg=6.

13. Офіціальний сайт програми DeviceLock® (електрон. ресурс)/ спосіб доступу URL: http://www.devicelock.com/ru/dl/.

14. Покрокове керівництво по створенню та розгортанню шаблонів служби керування правами Active Directory (електрон. ресурс)/ спосіб доступу URL: http://www.microsoft.com/rus/windowsserver2008/docs/Creating_and_Deploying_ADRMS_Templates_in_WS08_Step-by-Step_Guide_ru/Creating_and _Deploying_ADRMS_Templates_in_WS08_Step-by-Step_Guide_ru_index.aspx.

15. Програмні продукти agnitum.ru (електрон. ресурс)/ спосіб доступу URL: http://www.agnitum.ru/products/outpost/.

16. Комп'ютерний портал BOARD (електрон. ресурс)/ спосіб доступу URL: http://ru-board.com/new/article.php?sid=174.

17. Інтернет портал Security Lab (електрон. ресурс)/ спосіб доступу URL: http://www.securitylab.ru/contest/212096.php.

18. Портал антивірусу ESET NOD 32 (електрон. ресурс)/ спосіб доступу URL: http://evrokom.com/ESETNOD32RUSBOX_45914.html.

19. Windows 2012 Операційна система. Настройка DNS и Active Directory. Microsoft Windows 2012 Технический обзор.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	3	
5	А4	1 Розділ	22	
6	А4	2 Розділ	27	
7	А4	3 Розділ	12	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Схеми підприємства ТОВ «Сфера»

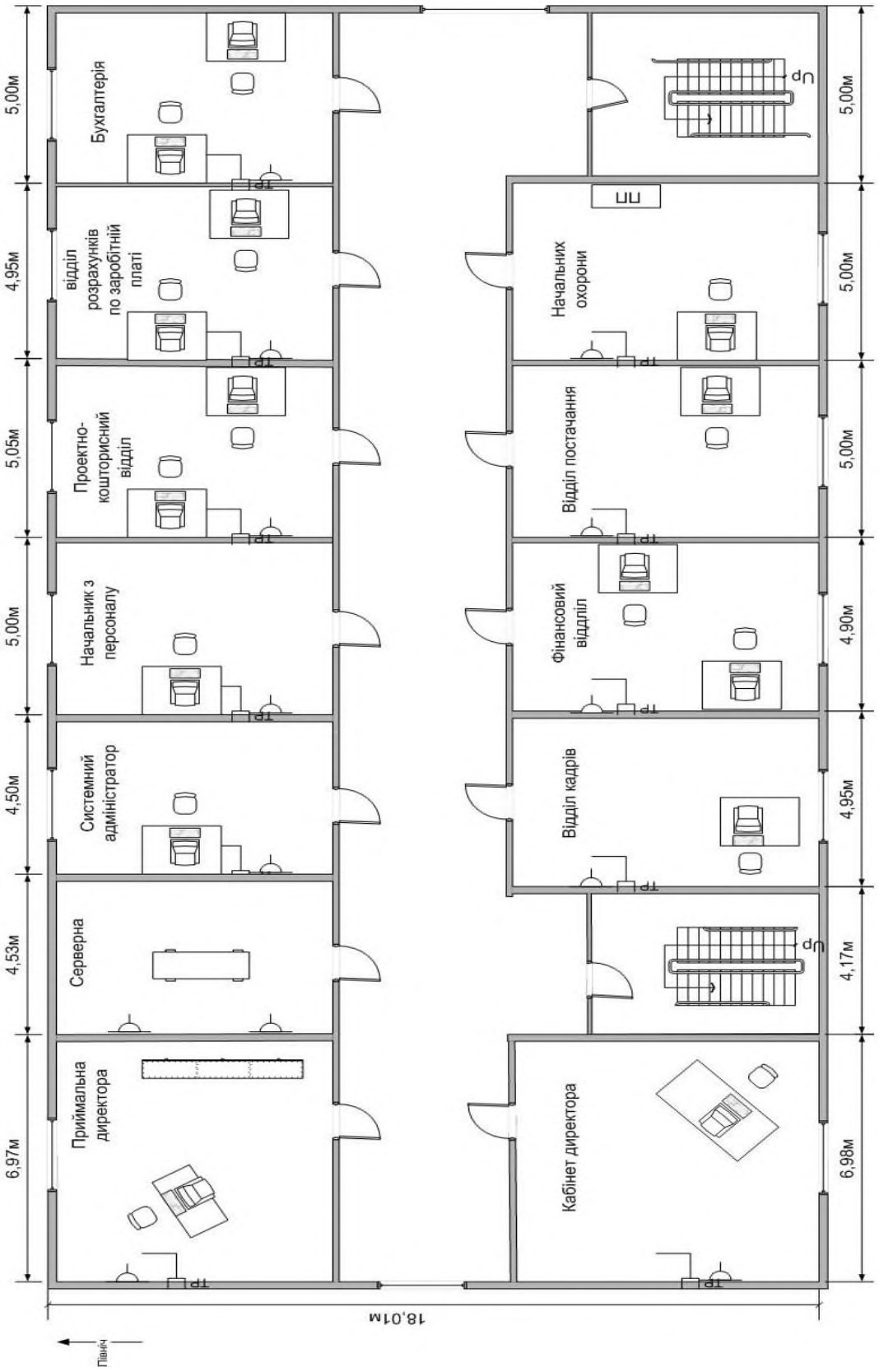


Рисунок 1 – Схема офісу підприємства ТОВ «Сфера»

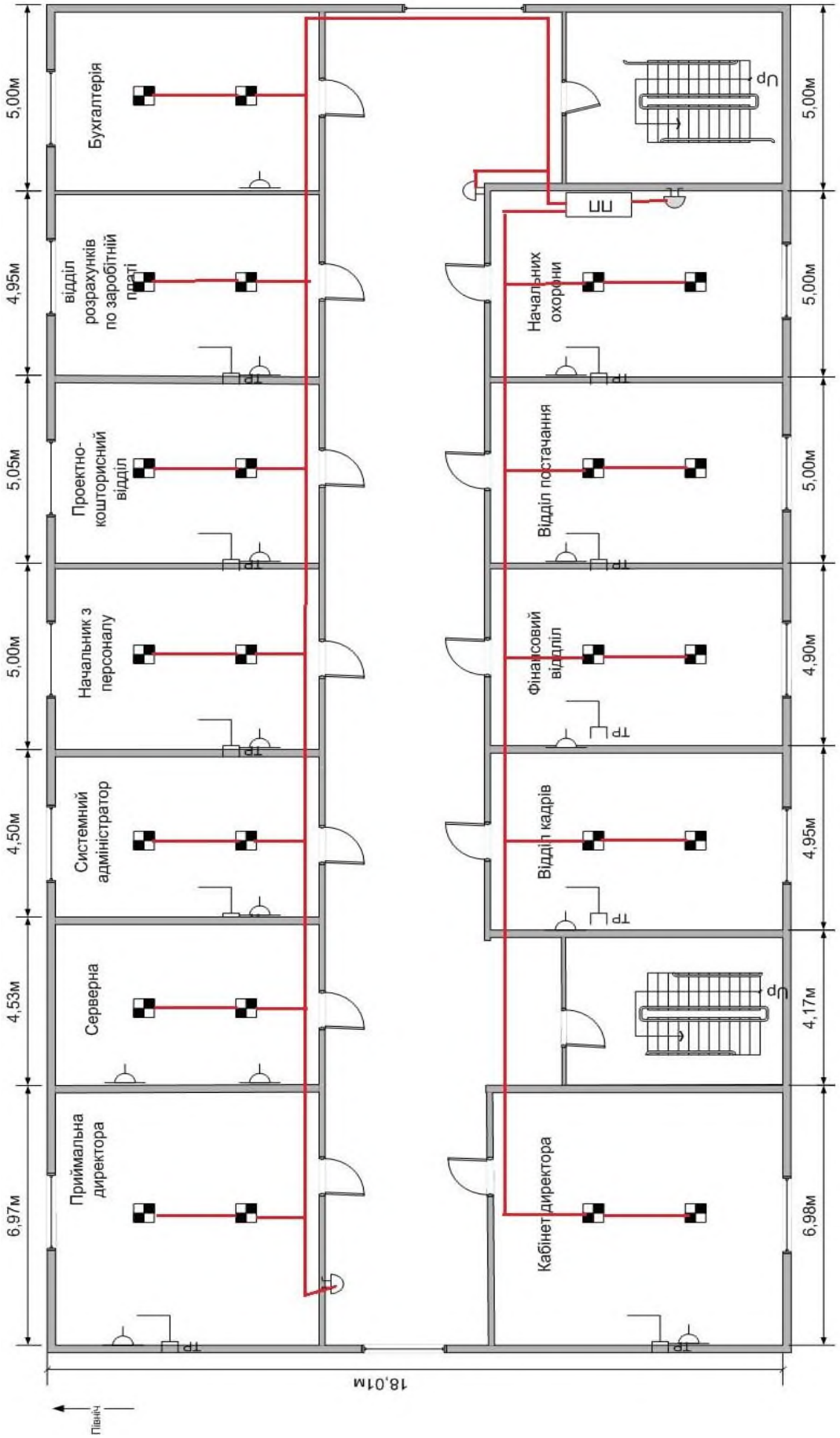


Рисунок 2 - Схема розташування датчиків диму

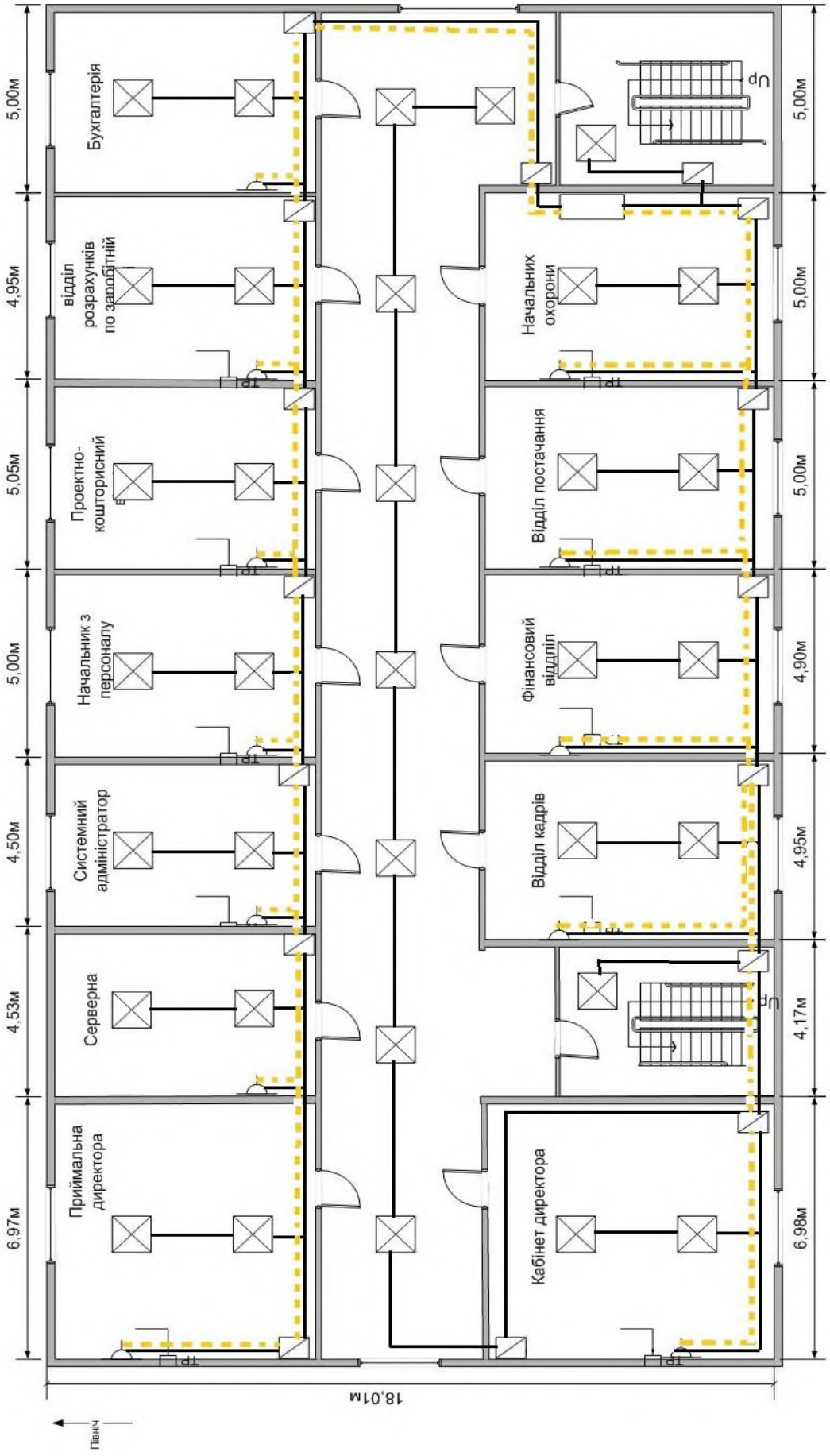


Рисунок 3 - Схема електроживлення та занулення

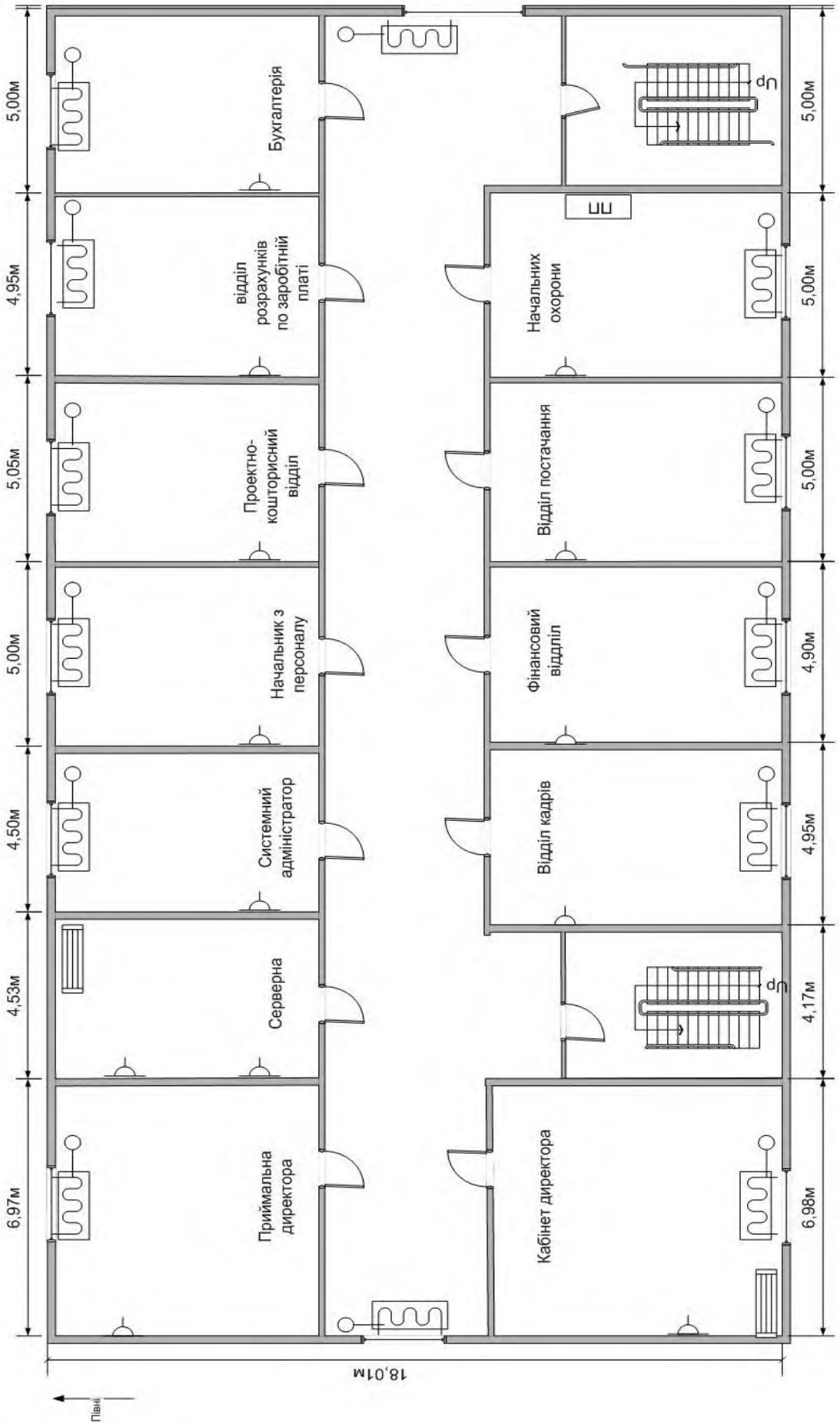


Рисунок 4 - Схема опалення

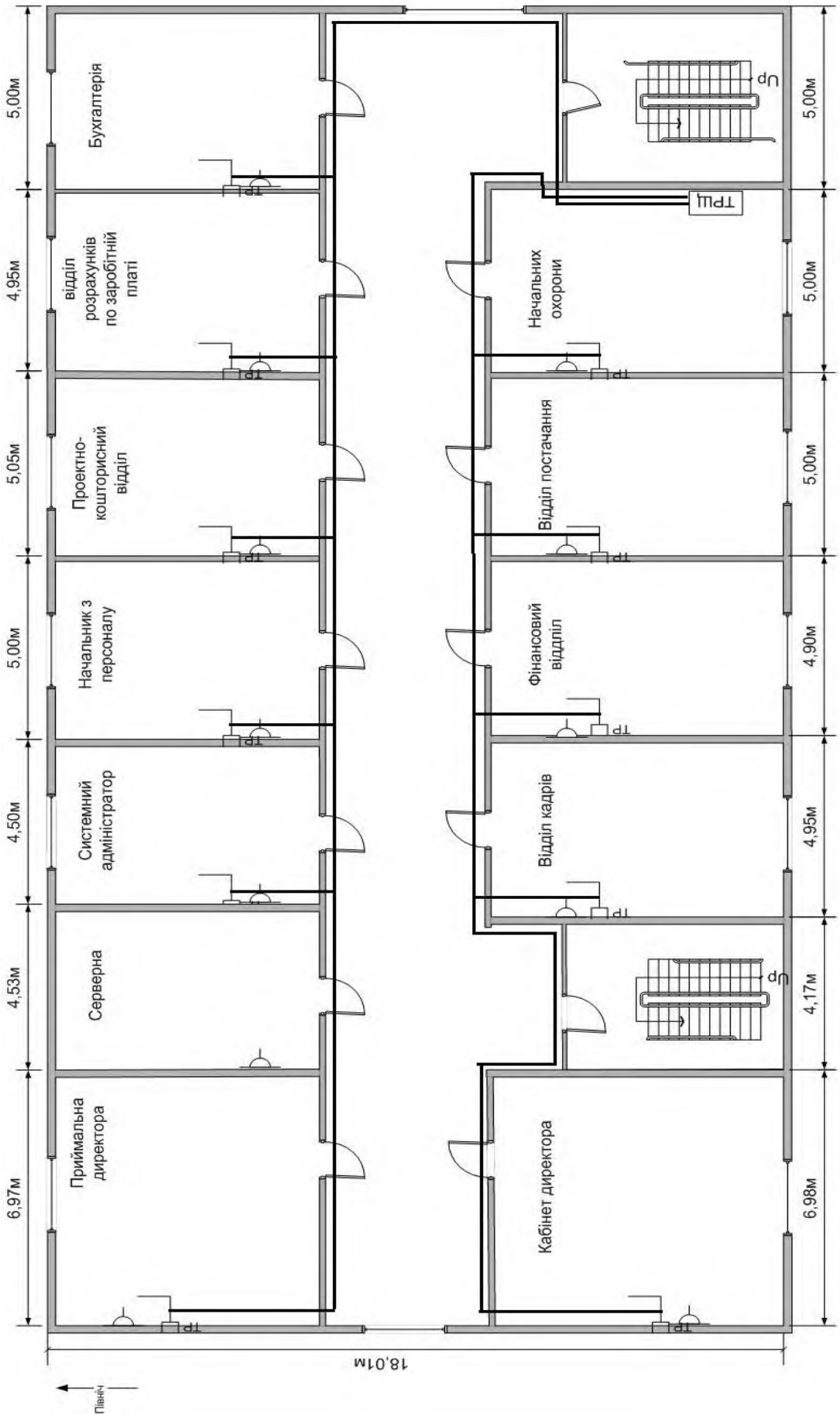


Рисунок 5 - Схема телефонної мережі

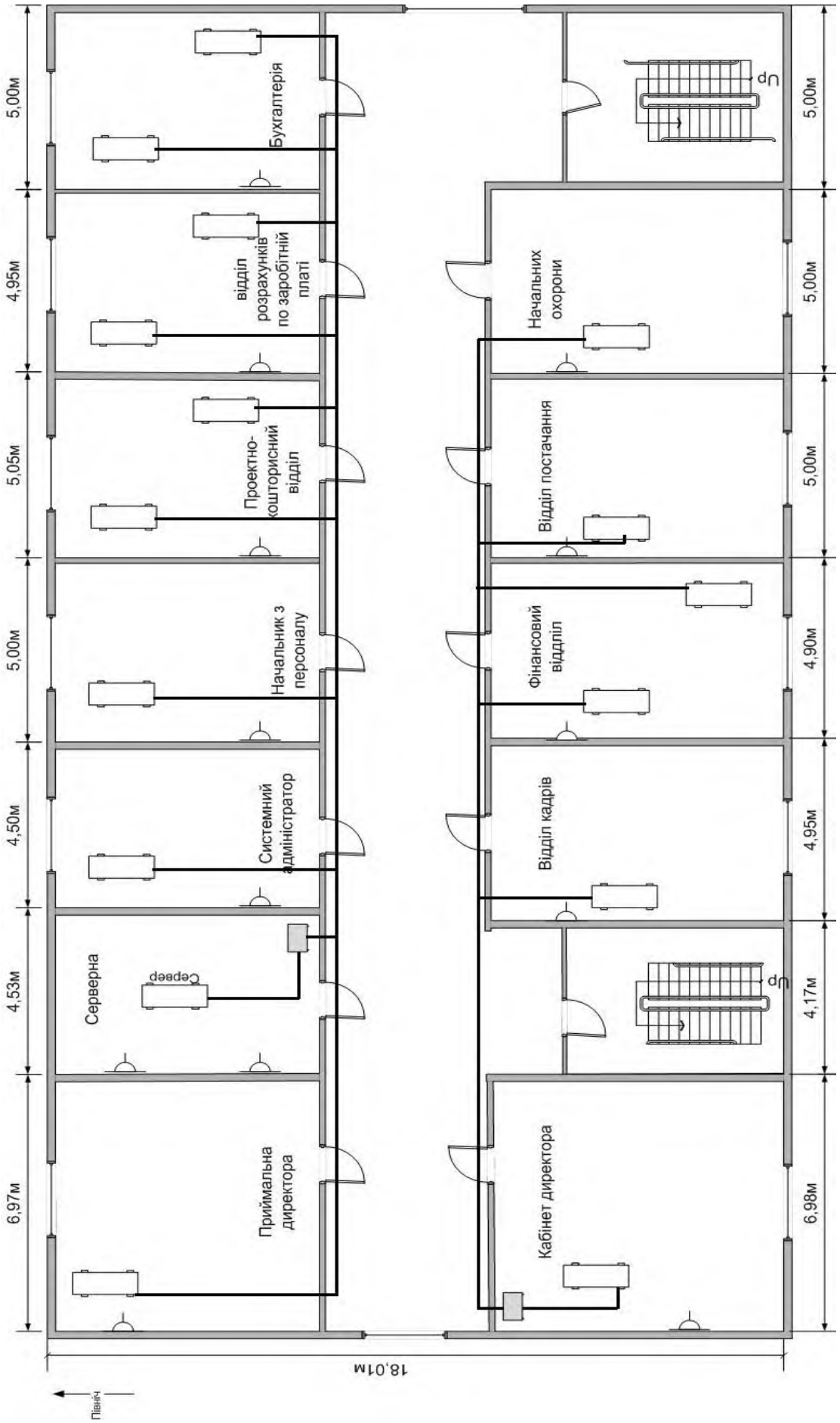


Рисунок 6 - Схема локальної мережі

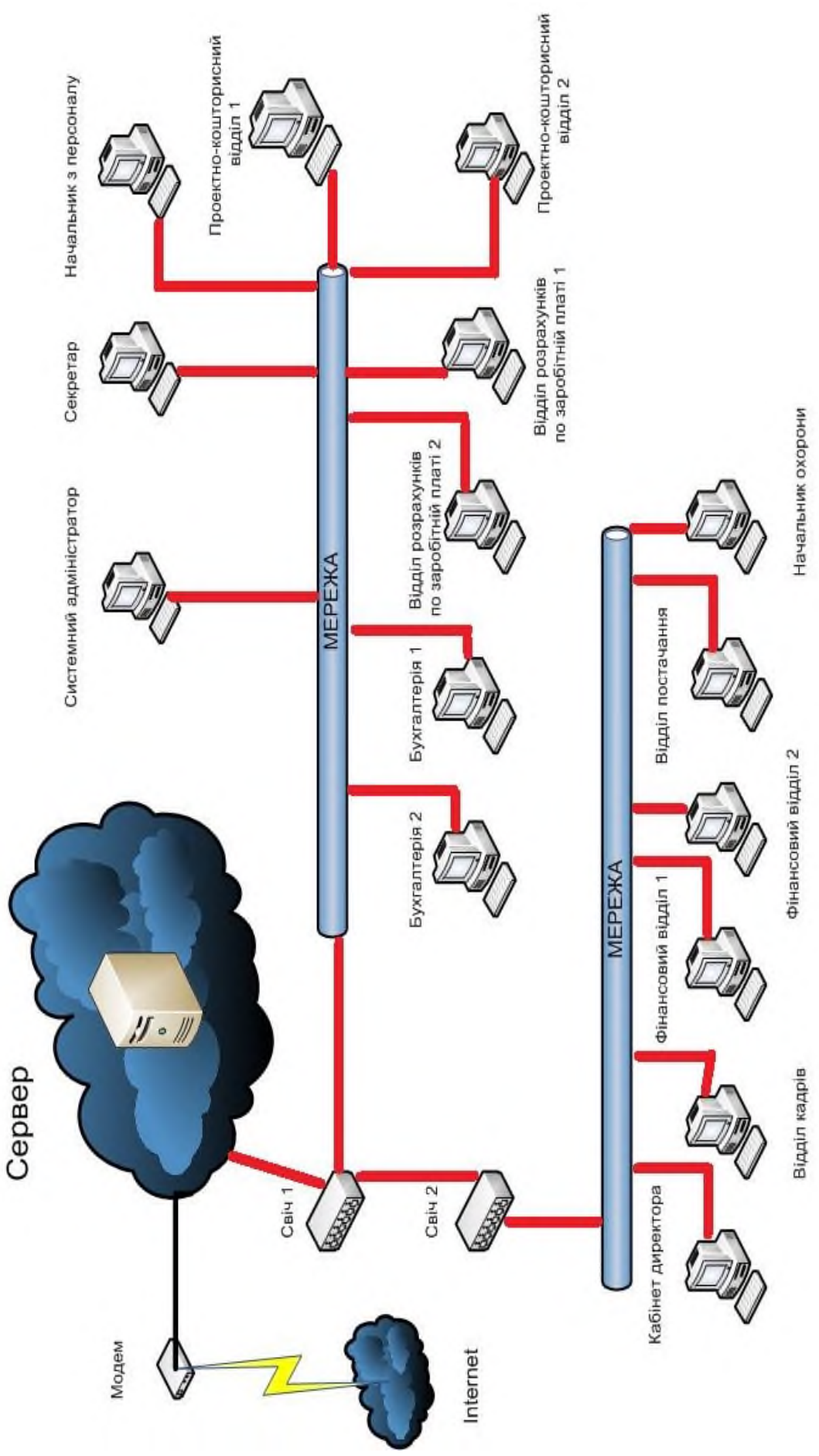


Рисунок 7 - Структура локальної мережі

Умовні позначення:

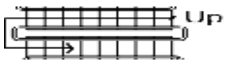

- Батарея опалення


- Кондиціонер

- Протипожежна понель

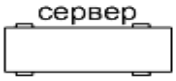
- Стіна

- Двері


- Сходи

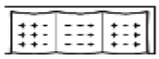

- Стіл


- Комп'ютер



- Сервер


- Вікно


- Меблі

- Телефонний росподільний щиток

- Телефонна розетка


- Люмінісцентна лампа


- Робоча станція


- Стул


- Комутатор (свіч)


- Електрична розетка


- Датчик диму


- Звукова тривога


- Кнопка тривоги


- Розподільна коробка


- Стояк опалення

ДОДАТОК В. 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

16 Додаток Д.doc

Презентація.pptx

ДОДАТОК Г. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Д. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Розробка підсистеми захисту від несанкціонованого доступу
комплексної системи захисту інформації ТОВ «Сфера»
Бовдиря Даніла Євгеновича

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.

Об'єкт розробки: автоматизована система ТОВ «Сфера».

Мета роботи: розробка підсистеми захисту від несанкціонованого доступу автоматизованої системи ТОВ «Сфера».

У спеціальній частині виконано аналіз об'єкта захисту та існуючої системи безпеки, та наведені методи та засоби реалізації підсистеми захисту від НСД.

У роботі наведені:

- технічне завдання на розробку підсистеми захисту від НСД;
- розмежування доступу засобами клієнту Active Directory.

Практичне значення роботи полягає в підвищені захисту інформації ТОВ «Сфера», шляхом впровадження підсистеми захисту від НСД.

Розроблена підсистема захисту від НСД призначена для впровадження у АС ТОВ «Сфера», з метою захисту конфіденційної інформації.

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