Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: **Розробка локальної комп'ютерної мережі для м'ясопереробного цеху с.Мшанець Зборівського району Тернопільської області**

Виконав: студентка IV курсу, групи СНзс-42
спеціальності 122 Комп'ютерні науки
(шифр і назва спеціальності)

_____ Осипчук Н.В.
(підпис) (прізвище та ініціали)

Керівник _____ Марценко С.В.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Шимчук Г.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Жаровський Р.О.
(підпис) (прізвище та ініціали)

Тернопіль
2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«__» _____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Осипчук Наталії Вікторівні
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка локальної комп'ютерної мережі для м'ясопереробного цеху с.Мшанець Зборівського району Тернопільської області

Керівник роботи Марценко Сергій Володимирович, к.т.н., доц., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «__» _____ 2021 року № _____

2. Термін подання студентом завершеної роботи 13.06. 2022р.

3. Вихідні дані до роботи Технічне завдання на розробку мережі цеху

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1.Аналіз предметної області. 1.1 Аналіз технічного завдання на розробку локальної комп'ютерної мережі для м'ясопереробного цеху с.Мшанець. 1.2 Огляд хмарних рішень для цифрового документообігу. 1.3 Системи відеоспостереження та моніторингу фізичної активності. 1.4 Організація віддаленого захищеного доступу до ресурсів мережі. 1.5 Використання firewall для захисту локальної мережі. 1.6 Висновки до першого розділу 2. Розробка проекту локальної мережі для м'ясопереробного цеху с.Мшанець. 2.1 Розробка фізичної топології для мережі м'ясопереробного цеху. 2.2 Створення логічної топології для локальної комп'ютерної мережі м'ясопереробного цеху. 2.3 Пропонований набір активного обладнання для цеху. 2.4 Тестування модельованих рішень мережі м'ясопереробного цеху с.Мшанець. 2.5 Висновки до другого розділу. 3. Безпека життєдіяльності, основи охорони праці. Висновки. Список літературних джерел

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Мета та актуальність роботи. 2. Практичне значення результатів. 3. Типи бнадмауерів 4. Модель Cisco для побудови мережі. 5. Планування першого поверху цеху. 6. Планування другого поверху цеху. 7. Аналіз вимог мережі. 8. Схема кабелів цеху. 9. Логічна топологія цеху. 10. Вибір комутатора Cisco. 11. Вибір точки доступу. 12. Модель та тестування мережі 13. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Гурик О.Я., доц. каф. ІМТ		

7. Дата видачі завдання 24 січня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	24.01.2022	*Виконано*
2.	Підбір наукових джерел щодо розробки проекту	04.01.2022-30.01.2022	*Виконано*
	мережі цеху		
3.	Переклад та опрацювання джерел щодо розробки	31.01.2022-06.02.2022	*Виконано*
	проекту мережі цеху		
4.	Виконання дослідження щодо розробки проекту	07.02.2022-13.02.2022	*Виконано*
	Розроблення проекту мережі цеху		
5.	Оформлення розділу «Аналіз предметної області»	14.02.2022-06.03.2022	*Виконано*
6.	Оформлення розділу «Розробка проекту локальної	07.03.2022-03.04.2022	*Виконано*
	мережі для м’ясопереробного цеху с.Мшанець»		
7.	Виконання завдання до підрозділу «Безпека життєдіяльності»	04.04.2022-17.04.2022	*Виконано*
8.	Виконання завдання до підрозділу «Основи охорони	18.04.2022-01.05.2022	*Виконано*
	праці»		
9.	Оформлення кваліфікаційної роботи	02.05.2022-15.05.2022	*Виконано*
10.	Нормоконтроль	16.05.2022-22.05.2022	*Виконано*
11.	Перевірка на плагіат	27.05.2022	*Виконано*
12.	Попередній захист кваліфікаційної роботи	30.05.2022	*Виконано*
13.	Захист кваліфікаційної роботи	13.06.2022	

Студент _____ Осипчук Н.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Марценко С.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка локальної комп’ютерної мережі для м’ясопереробного цеху с.Мшанець Зборівського району Тернопільської області // Кваліфікаційна робота освітнього рівня «Бакалавр» // Осипчук Наталія Вікторівна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно–інформаційних систем і програмної інженерії, кафедра комп’ютерних наук, група СНзс–42 // Тернопіль, 2022 // С. 42, рис. – 5, табл. – 5, кресл. – , додат. – , бібліогр. – 30.

Ключові слова: локальна мережа, IP адреса, комутатор, маршрутизатор, бездротова точка доступу, топологія.

У роботі зійснено розробку проекту локальної комп’ютерної мережі для м’ясопереробного цеху с.Мшанець.

Метою роботи є здійснити аналіз вимог до розробки локальної комп’ютерної мережі у м’ясопереробному цеху та розробити проектні рішення для її побудови.

Перший розділ кваліфікаційної роботи розглядає питання аналізу технічного завдання на створення локальної комп’ютерної мережі для м’ясопереробного цеху с.Мшанець. При цьому виділено важливі для діяльності організації функції роботи мережі через впровадження надійного та захищеного цифрового документообігу, системи відеоспостереження, безпечного віддаленого доступу до ресурсів мережі.

В другому розділі проведено розробку фізичної топології локальної комп’ютерної мережі для м’ясопереробного цеху с. Мшанець. Розроблено логічну топологію, що враховує особливості організації праці цеху. Проведено моделювання проектованих рішень з подальшим тестуванням, що дасть змогу перевести модель у реальну мережу з найменшими помилками.

ANNOTATION

A local computer network development for the meat processing plant in the borough of Mshanets, Zboriv district, Ternopil region // Diploma thesis Bachelor degree // Osypchuk Nataliia V. // Ternopil' Ivan Pul'uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science // Ternopil', 2022 // P. 42, Tables – 5, Fig. – 5, Diagrams – , Annexes. – , References – 30.

Keywords: local area network, IP address, switch, router, wireless access point, topology.

The project of the local computer network for the meat processing plant in the village of Mshanets was developed.

The aim of the work is to analyze the requirements for the development of a local computer network in a meat processing plant and to develop design solutions for its construction.

The first section of the qualification work considers the analysis of the technical task for the creation of a local computer network for the meat processing plant in the village of Mshanets. At the same time, the important functions of the network operation for the organization through the introduction of reliable and secure digital document management, video surveillance system, secure remote access to network resources are highlighted.

In the second section, the development of the physical topology of the local computer network for the meat processing plant with. Mshanets. A logical topology has been developed that takes into account the peculiarities of the shop's labor organization. The simulation of the designed solutions was carried out with further testing, which will allow to translate the model into a real network with the least errors.

ЗМІСТ

ВСТУП

Цифровізація суспільства відбувається на всіх етапах сучасного життя. Сучасне виробництво неможливо уявити без новітніх технологій. Для організації роботи багатьох систем на виробництві потрібно забезпечити їх зв'язок через комп'ютерну мережу. Електронний документообіг, системи відеоспостереження, моніторинг роботи виробничих процесів – це лиш невеликий перелік сучасних методів ведення господраської діяльності.

Актуальність теми. Створення проекту локальної мережі для м'ясопереробного цеху с.Мшанець є актуальним завданням, що дасть змогу впровадити нові методи роботи, управління та організації сучасного ведення господарської діяльності.

Мета і завдання кваліфікаційної роботи. Метою роботи є провести:

– проаналізувати плани будівель цеху для визначення можливості впровадження планованих рішень;

– здійснити огляд технологій та методів покращення ведення діяльності через впровадження інформаційних технологій мережевого спрямування;

– виконати розроблювання фізичної та логічної топологій з врахуванням специфіки роботи організації;

– запропонувати активне мережеве обладнання;

– здійснити моделювання проектованих рішень для перевірки їх достовірності.

Практичне значення одержаних результатів. Розглянуто питання аналізу технічного завдання на створення локальної комп'ютерної мережі для м'ясопереробного цеху с.Мшанець. При цьому виділено важливі для діяльності організації функції роботи мережі через впровадження надійного та захищеного цифрового документообігу. Проведено огляд можливості впровадження системи відеоспостереження для убезпечення території та

приміщень, подано організацію комплексної безпеки з відео та аудіо записом. Розглянуто методи безпечного віддаленого доступу до ресурсів мережі через використання технології VPN. Як оптимальні показано методи організації VPN через використання протоколів SSL та TLS, що є вбудованими функціями сучасних браузерів. Проаналізовано використання брандмауерів для захисту критичних вузлів та програм, що дасть змогу попередити вплив шкідливих програм та зловмисників на мережу. Проведено розробку фізичної топології локальної комп'ютерної мережі для м'ясопереробного цеху с. Мшанець. Здійснено розведення кабелів для підключення активного мережевого обладнання та визначено точки розміщення камер відеоспостереження. Розроблено логічну топологію, що враховує особливості організації праці цеху. Виконано поділ на віртуальні мережі для підвищення захищеності з'єднань між відділами. Розраховано IP схему для кожного відділу та з'єднання до мережі Інтернет. Проведено моделювання проектованих рішень з подальшим тестуванням, що дасть змогу перевести модель у реальну мережу з найменшими помилками.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз технічного завдання на розробку локальної комп’ютерної мережі для м’ясопереробного цеху с.Мшанець

Технічне завдання на створення локальної мережі м’ясопереробного цеху повинно включати огляд цілей та мети роботи для забезпечення безперебійного обміну данними [1-5].

Основними областями застосування будуть:

– забезпечення обміну цифровими даними та документообігу;
– система відеоспостереження;
– доступ до глобальної мережі Інтернет;
– організація захищеного доступу;
– облік готової продукції через моніторинг автоматизованих ліній.

Основним видом діяльності м’ясопереробного цеху є виготовлення напівфабрикатів та готової продукції. При цьому цифрові технології задіяні у багатьох технологічних процесах та надають можливість віддалено контролювати основну діяльність організації.

Аналіз технічного завдання на виконання розробки комп’ютерної мережі повинен включати визначення кількості та місця під’єднання мережевих пристроїв та користувацького обладнання. На цьому етапі будуть проведені дослідження планів будівель для оптимального вибору розташування серверних кімнат та комутаційних шаф. Дизайн мережі повинен враховувати існуючі потреби та за можливості забезпечувати майбутній ріст мережі у випадку розширення виробництва чи необхідності впровадження нових технологій.

Ведення цифрового документообігу стало актуальним та важливим питанням з розвитком пандемії. Подача звітів в конролюючі органи без

небезпеки відвідування громадських місць стало можливим за допомогою сучасних технологій комп’ютерних мереж.

Разом з створенням та передаванням зовнішніх документів у вигляді звітів існує ряд завдань, що вирішуються внутрішнім документообігом. Наприклад, отримання вартості сировини в електронному вигляді, моніторинг цін на готову продукцію для створення конкурентоспроможної цінової політики, ведення систем роботи з постачальниками та клієнтами з актуалізацією прайсів.

Ведення електронного документообігу може бути підсилене використанням хмарного зберігання документів. При цьому забезпечується використання усіх функцій та переваг, що надаються такими сервісами.

Хмарне сховище дає користувачам можливість отримати доступ до завантажених файлів з будь-якого місця, надаючи професіоналам гнучкість, що необхідна для виконання роботи. Якщо організація вибрала правильне рішення хмарного сховища для своїх потреб, вона не тільки має можливість завантажувати документи з різних пристроїв і місць, але й бути впевненою в захищеності своїх даних.

Наведемо лише деякі переваги впровадження рішення хмарного сховища у організації:

– доступ у будь-який час. Немає нічого гіршого, ніж працювати над проектом вдома і зрозуміти, що ви залишили потрібні документи на своєму столі або зберегли їх лише на офісному настільному комп’ютері. Хмарні зберігання даних дозволяють отримувати доступ до документів з будь-якого місця.

– простий у використанні. Часто існуючі рішення пропонують однаковий функціонал, проте мають незрозумілий та недружній інтерфейс. На ринку існує багато популярних хмарних продуктів, що мають простий дизайн, який забезпечує навіть початківцям легкий доступ до хмарного документообігу.

– швидке налаштування. Хмарні зберігання даних легко налаштувати – у багатьох випадках просто потрібно створити обліковий запис.

Аналіз технічного завдання на розробку локальної мережі для м’ясопереробного цеху с. Мшанець показав, що впровадження нових технологій та можливостей цифрового світу покращать роботу даної організації та підвищать надійність та захищеність її ресурсів.

1.2 Огляд хмарних рішень для цифрового документообігу

Найкраще хмарне сховище документів спрощує керування та організацію спільних файлів і папок у роботі організації [6-9].

Функціонуваня організації в сучасному світі суттєво спрощене через зберігання документів у хмарах які пропонують доступний спосіб збереження файлів, архівів папок, різноманітних документів та зображеннь. Такий підхід забезпечує захист від збою фізичних носіїв даних чи інших подібних проблем і дає змогу працівникам організації отримувати доступ до цих самих файлів з робочих та персональних пристроїв.

Існує ряд інструментів для спільної роботи, що дає змогу документам, які зберігаються в хмарі, отримувати дозволи на доступ для обміну файлами з членами команди, допомагаючи підвищити ефективність роботи в офісі. Найбільш ефективно це працює для створення та редагування документів, використання спеціалізованрго програмного забезпечення, керування додатками організації роботи з клієнтами.

Деякі програми зберігатимуть дані в хмарі за вибором організації, проте також надають можливість використовувати служби розробників програмного забезпечення або інтегрувати існуючого постачальника хмарного сховища.

Важливість хмарного зберігання документів для сучасного бізнесу підсилена реаліями, що зараз так багато людей працює вдома і для них це є можливість нового способу роботи.

Проведемо аналіз найбільш популярних хмарних рішень для роботи та збереження документів та файлів.

Microsoft OneDrive розгорнутий у 2007 році у вигляді власного рішення хмарного сховища Microsoft. Він входить до частини офісного пакету Microsoft 365. Користувачам надається 5 ГБ хмарного місця для зберігання. Для студентів та навчальних організації існує можливість отримати 1 ТБ місця для безкоштовного сховища.

Для використання OneDrive необхідно мати або створити обліковий запис, після налаштування якого існує можливість спільної робои над документами, їх розповсюдженням та підтримки версійності збереження. Великою перевагою даного рішення є його універсальність для багатьох платформ.

За допомогою OneDrive можна використовувати документи офлайн, що уможливлює роботу з ними у випадку відстутності мережевого з'єднання. Даний продукт попередньо встановлений на всіх машинах з Windows 10. За потреби можна завантажити його на інші платформи для збереження спільного доступу до контенту.

Google Drive є іншим популярним рішенням хмарного збереження та роботи з документами. На початку використання даний продукт забезпечує 15 ГБ вільного місця. Сюди входить не лише документи у обліковому профілі Google Drive, а й, наприклад, Gmail та завантажені в Google Photos високоякісні зображення.

Google One пропонує не лише додатковий простір для зберігання, але й додаткові функції. Тарифні плани для окремих осіб включають можливість отримати 100 ГБ або 200 ГБ. Для найбільш вибагливих існує

місце розміром у 2 ТБ. При індивідуальних потребах можна використати додаткові плани, що забезпечують ще більше місця.

Додатковою перевагою цих індивідуальних планів є можливість налаштування спільного сімейного облікового запису, що дає можливість використовувати контексну рекламу та інші акції від служб компанії провайдера.

Для ведення ділового документообігу більше прийнятним буде Google Workspace після ребрендингу G Suite.

Компанія Dropbox є одним із найдовше присутніх давачів послуг хмарного збереження, що існує сьогодні на ринку. За сьогоднішніми мірками базовий тарифний план забезпечує досить мізерні 2 ГБ. Особливістю роботи даного давача послуг є можливість збільшити до 16 ГБ вільного місця використовуючи рекомендації цього сервісу своїм знайомим чи співробітникам. Інший спосіб зміни розміру місця є прив'язка Dropbox до профілів соціальних мереж.

На даний момент це один із найпростіших у використанні постачальників даних послуг. Dropbox можна встановити на більшість комп'ютерів або пристроїв і легко синхронізуватися між додатками. Висока сумісність різноманітних типів даних при використанні цієї програми робить її хорошим вибором для впровадження.

Для спільної роботи з файлами можна використовувати посилання і користувачі, які не мають реєстрації на цьому сервісі зможуть з ними працювати.

До основних недоліків цього провайдера послуг є його цінова політика і якщо потрібно збільшити хмарне місце – це може коштувати значних коштів.

Компанію Egnyte засновано в 2007 році. Вона надає програмне забезпечення для синхронізації корпоративних файлів і обміну ними.

Для підвищення безпеки Egnyte дає змогу компаніям зберігати свої дані локально та в хмарі. Такий поділ збереження уможливлює вибирати ступінь захищеності даних і для важливих файлів обирати локальне збереження, а не хмарне рішення.

За допомогою даного рішення організовано роботу команд через власну платформу сервісів та моливість інтегрування з відомими додатками.

Тарифікація проводиться на основі кількості працівників, що будуть спільно використовувати дану платформу.

Adobe Document Cloud є іншим популярним продуктом, що більшість компаній активно використовує при необхідності обробляти PDF-документи. Використання ціє платформи дає можливість заберігати файли PDF в хмарі, редагувати її та за потреби виконувати інші дії притаманні для даних такого характеру.

Основна робота Adobe Document Cloud базується на використанні Adobe Acrobat CC і Adobe Sign. Це дає можливість проводити операції з документами PDF виконуючи всі необхідні дії. Дана платформа не є пасивним сховищем даних, а забезпечує активну роботу з даними пропонуючи редагування, імпорт чи експорт даних, а також сканування.

Ще одна перевага Adobe Document Cloud полягає в тому, що він має ряд інтеграцій, наприклад, для програмного забезпечення CRM, ERP та HR, Microsoft 365, Salesforce, Zoho, IBM та Oracle.

Основним стримуючим фактором використання даного рішення для невеликих організації може бути вартість тарифного плану, оскільки в більшій мірі це орієнтовано на корпоративних колієнтів.

Проведений анаіз хмарних рішень для документообігу може бути використаний для вибору найбільш прийнятного по тарифному плані та функціоналу.

1.3 Системи відеоспостереження та моніторингу фізичної активності

На відміну від інших заходів фізичної безпеки, які рідко порушують конфіденційність інших людей, відеоспостереження є досить чутливим питанням. Разом з іншими питаннями це також величезні інвестиції. Разом з іншими завданнями розробки локальної мережі м’ясопереробного цеху необхідно провести аналіз можливості встановлення систем відеоспостереження з реєстрацією, що буде враховувати потреби бізнесу та співробітників з різних сторін [10-15].

Вкладення грошей у систему безпеки буде марним, якщо ці заходи не відповідають потребам безпеки організації. Наприклад, якщо будуть витрачені великі кошти на фізичну безпеку, подекуди буде важко отримати доказову базу для підтвердження факту крадіжки або виявлення осіб причетних до цього.

Потрібно проаналізувати точні потреби організації, перш ніж впроваджувати систему відеоспостереження. Необхідно врахувати розмір території та приміщень, оскільки це визначить кількість камер відеоспостереження, які потрібно буде придбати. Також потрібно розуміти, який тип камери підійде краще і буде відповідати запланованому бюджету. Необхідно визначити чи потрібна бездротова камера або буде достатньо звичайної IP камери. Для якісного покриття буде використана куляста камера, чи знадобиться купольна камера.

Визначаючи кількість і тип камер, слід пам’ятати про найбільш чутливі зони та ті, які потребують найменшого спостереження. Наприклад, можна встановити дорогі камери з багатьма цінними функціями у важливих зонах і використовувати камери з кулею для областей з найменшою загрозою.

Закон зобов’язує повідомляти людям, що за ними спостерігають. Тому потрібно формально донести до своїх співробітників впровадження системи відеоспостереження перед її впровадженням. Інакше вони можуть заявити, що їх конфіденційність порушується.

Аналогічно, якщо положення камер може вплинути на інші підприємства або житлові будинки, потрібно отримати офіційний дозвіл у відповідних органів влади. Виникає необхідність ефективно повідомити про це відповідним людям і попросити їх надати письмовий дозвіл на встановлення камер. Останнє дозволить уникнути суперечок щодо конфіденційності в майбутньому.

Необхідно переконатися, що постачальник послуг безпеки, який виконує завдання, має репутацію та надійність. У той час як деякі постачальники безпеки виявлятимуть легковажність під час роботи з конфіденційною інформацією організації, інші можуть навіть виявитися шахраями та зловмисниками. Тому не останнім завданням є захист доступу до камер та збережених даних.

Повністю інтегрована система безпеки будівельного майданчика – це повна система безпеки, яка захистить майно від усіх потенційних загроз безпеці. Інтегрована система безпеки – це не просто невелика система безпеки, вона поєднує в собі комплекс функцій безпеки, необхідні для захисту об’єктів відеоспостереження.

Інтегрована система безпеки має кілька рівнів безпеки, таких як спостереження, сигналізація, детектори диму, теплові датчики, детектори розбиття скла, датчики дверей і вікон, а також моніторинг периметра.

Інтегрована система безпеки – це поєднання систем відео, сигналізації та аудіоспостереження. Усі ці системи працюють разом як одне ціле, щоб забезпечити повноцінну безпеку майданчика.

Оскільки ці системи краще реагують на незвичайні дії в порівнянні зі стандартною системою безпеки, вони ідеально підходять для виробничих приміщень та території.

Якщо існує потреба захистити територію цеху, важливо знати, коли хтось входить і виходить з приміщень та території.

Повністю інтегрована система безпеки веде облік кожного, хто входить і виходить з області спостереженян і дозволяє віддалено контролювати периметр.

Відеоспостереження виступає як вирішальний інструмент допомоги у разі злому, оскільки поліція матиме відеозйомку грабіжника, щоб їм було легше зловити зловмисника.

Таким чином, за допомогою інтегрованої системи безпеки можна реєструвати всі точки входу та виходу з організації, а також вести облік усіх відвідувачів.

Без звуку відеозапису може бути не завжди достатньо і іноді корисно мати зображення та розмови, щоб зловити злочинця.

Відеоспостереження покаже лише про те, хто заходив і виходив із власності, але якщо існує потреба знати, що вони робили на території і можливо скомпроментували себе, тоді знадобиться аудіозапис.

Завдяки повністю інтегрованій системі безпеки існує можливість записувати аудіо на території, що охороняється, а також записувати всі розмови.

1.4 Організація віддаленого захищеного доступу до ресурсів мережі

Віртуальна приватна мережа (VPN) набула популярності і стала стандартом для компаній, які мають дистанційних співробітників, керівників і продавців, яким потрібен доступ до мережі, коли вони в дорозі або партнерів і клієнтів, яким потрібен доступ до ресурсів у корпоративній

мережі. Метою мережі VPN є надання віддаленого доступу до ресурсів у корпоративній мережі, які в іншому випадку були б доступні лише за умови безпосереднього підключення користувача до корпоративної локальної мережі. При підключенні VPN користувач має “віртуальний” зв’язок “точка-точка” між віддаленим користувачем VPN і корпоративною мережею. Користувач може працювати як на місці; програми та служби, що працюють на комп'ютерах користувачів, розглядають VPN-з’єднання як звичайне з’єднання Ethernet. Інтернет, через який клієнт підключений до корпоративної мережі, повністю прозорий для користувачів і додатків.

Однією з основних переваг використання VPN з’єднання у порівнянні з веб-програмами клієнт/сервер є те, що користувачі VPN у віддалених місцях можуть потенційно отримати доступ до всіх протоколів і серверів у корпоративній мережі. Це означає, що користувачі можуть отримати доступ до повного спектру послуг на серверах Microsoft Exchange, Microsoft SharePoint Server, Microsoft SQL Server і Microsoft Live Communication Server так само, як вони мають пряме підключення до мережі в корпоративному місці. Клієнтське програмне забезпечення VPN вбудовано у всі сучасні операційні системи Windows. Користувачеві VPN не потрібне спеціальне програмне забезпечення для підключення до кожної з цих служб, і не потрібно створювати спеціальні проксі-додатки, щоб дозволити користувачам підключатися до цих ресурсів [16-22].

VPN “віддаленого доступу” безпечно підключає пристрій за межами офісу. Кінцеві пристрої можуть бути ноутбуками, планшетами або смартфонами. Розвиток технології VPN дозволив проводити перевірки безпеки на кінцевих пристроях, щоб переконатися, що вони відповідають певним вимогам перед підключенням.

VPN типу “сайт-сайт” з’єднує офіс з філіями через Інтернет. VPN типу “сайт-сайт” використовуються, коли відстань робить непрактичним

пряме мережеве з’єднання між цими офісами. Для встановлення та підтримки з’єднання використовується спеціальне обладнання.

VPN з віддаленим доступом дає змогу використовувати майже будь-яку програму для передачі даних, голосу або відео на віддалений пристрій.

Secure Sockets Layer (SSL) VPN і IP-безпека (IPsec) – це технології тунелів і аутентифікації. Фірми можуть використовувати SSL VPN, IPsec або обидва для розгортання VPN з віддаленим доступом, залежно від вимог до розгортання. SSL VPN і IPsec захищають дані, що проходять через VPN від несанкціонованого доступу.

Функція SSL VPN вже вбудована в сучасні веб-браузери, що дозволяє користувачам з будь-якого місця з підтримкою Інтернету запускати веб-браузер для встановлення VPN-з’єднань з віддаленим доступом. Технологія SSL VPN не тільки може допомогти підвищити продуктивність робочої сили, але також може знизити витрати на програмне забезпечення та підтримку клієнта VPN.

Більшості користувачів не потрібно встановлювати клієнтське програмне забезпечення. SSL VPN використовує протокол SSL та його наступника, Transport Layer Security (TLS), щоб забезпечити безпечне з’єднання між віддаленими користувачами та внутрішніми мережевими ресурсами. Оскільки більшість веб-браузерів тепер мають SSL/TLS, користувачам, як правило, не потрібно встановлювати клієнтське програмне забезпечення для використання SSL VPN. Ось чому SSL VPN також відомий як “безклієнтська VPN” або “веб-VPN”.

SSL VPN також простий у використанні. Різні постачальники IPsec VPN можуть мати різні вимоги до реалізації та конфігурації. Але SSL VPN вимагає від користувачів лише сучасного веб-браузера. Користувачі можуть навіть вибрати свої улюблені веб-браузери без обмежень операційною системою.

Безпека VPN настільки сильна, наскільки сучасні методи, які використовуються для автентифікації користувачів і пристроїв на віддаленому кінці VPN-з’єднання. Прості методи аутентифікації піддаються атакам “злому” пароля, підслуховування або навіть атак соціальної інженерії. Двофакторна аутентифікація є мінімальною вимогою для забезпечення безпечного віддаленого доступу до корпоративної мережі.

Віддалений доступ є основною загрозою безпеці мережі. Віддалений комп’ютер, який не відповідає вимогам корпоративної безпеки, потенційно може пересилати інфекцію, таку як хробак або вірус, із середовища локальної мережі до внутрішньої мережі. Найновіша антивірусна програма на віддаленому комп’ютері необхідна для зменшення цього ризику.

Розділене тунелювання відбувається, коли пристрій на віддаленому кінці VPN-тунелю одночасно обмінюється мережевим трафіком як з загальнодоступною, так і з приватною мережами, не розміщуючи спочатку весь мережевий трафік всередині тунелю VPN. Це може дозволити зловмисникам у спільній мережі зламати віддалений комп’ютер і отримати доступ до приватної мережі.

1.5 Використання firewall для захисту локальної мережі

Брандмауер нового покоління входить до третього покоління технології брандмауера, розробленого для боротьби з розширеними загрозами безпеки на рівні програми за допомогою інтелектуальних функцій безпеки, що залежать від контексту. Next generation firewall (NGFW) поєднує традиційні можливості брандмауера, такі як фільтрація пакетів і перевірку стану, з іншими, щоб приймати кращі рішення щодо того, який трафік дозволити [23-26].

Брандмауер нового покоління має можливість фільтрувати пакети на основі програм і перевіряти дані, що містяться в пакетах (а не лише їх IP-

заголовки). Іншими словами, він працює на рівні до 7 (рівень прикладних програм) у моделі OSI, тоді як попередня технологія брандмауера працювала лише до рівня 4 (транспортний рівень). Атаки, які відбуваються на рівнях 4–7 моделі OSI, збільшуються, що робить це важливою можливістю.

Специфікації брандмауера наступного покоління залежать від постачальника, але зазвичай вони включають певну комбінацію наступних функцій:

– обізнаність із програмою або здатність фільтрувати трафік та застосовувати складні правила на основі програми (а не лише на основі порту). Це ключова особливість брандмауерів наступного покоління: вони можуть блокувати трафік від певних програм, а також підтримувати більший контроль над окремими програмами;

– глибока перевірка пакетів, яка перевіряє дані, що містяться в пакетах. Глибока перевірка пакетів є вдосконаленням порівняно з традиційною технологією брандмауера, яка перевіряє лише IP-заголовок пакета, щоб визначити його джерело та призначення;

– система запобігання вторгненням (IPS), яка відстежує мережу на наявність шкідливої активності та блокує її там, де вона виникає. Цей моніторинг може бути на основі сигнатур (узгодження активності з сигнатурами добре відомих загроз), на основі політики (блокова діяльність, яка порушує політику безпеки) або на основі аномалій (моніторинг ненормальної поведінки);

– висока продуктивність, що дозволяє брандмауеру відстежувати великі обсяги мережевого трафіку без уповільнення. Брандмауери нового покоління включають ряд функцій безпеки, які вимагають часу на обробку, тому висока продуктивність важлива, щоб уникнути порушення бізнес-операцій;

– зовнішня розвідка загроз або зв’язок із мережею розвідки загроз, щоб переконатися, що інформація про загрози є актуальною та допоможе виявити поганих дійових осіб.

На додаток до цих основних функцій, брандмауери нового покоління можуть включати додаткові функції, такі як захист від вірусів і шкідливих програм. Вони також можуть бути реалізовані як брандмауер Firewall as a Service (FWaaS), хмарна служба, яка забезпечує масштабованість і спрощене обслуговування. За допомогою FWaaS програмне забезпечення брандмауера підтримується постачальником послуг, а ресурси автоматично масштабуються, щоб задовольнити попит на обробку. Це звільняє корпоративні IT-команди від тягаря обробки виправлень, оновлень і розмірів.

Брандмауери нового покоління забезпечують набагато кращий і надійніший захист, ніж традиційний брандмауер. Традиційні брандмауери обмежені у своїх можливостях: вони можуть блокувати трафік через певний порт, але вони не можуть застосовувати правила, що стосуються програми, захищати від шкідливого програмного забезпечення або виявляти та блокувати аномальну поведінку. В результаті зловмисники можуть уникнути виявлення, ввійшовши через нестандартний порт, чому брандмауер наступного покоління завадить. Завдяки своїй природі з урахуванням контексту та здатності отримувати оновлення від зовнішніх мереж аналізу загроз, брандмауери нового покоління здатні захищати від широкого й постійно мінливого набору передових загроз і навіть можуть використовувати інтелектуальну автоматизацію для підтримки політики безпеки. на сьогодні, не вимагаючи втручання з боку зайнятого IT-персоналу.

Крім того, брандмауери нового покоління пропонують вдосконалену інфраструктуру безпеки, яку легше й дешевше обслуговувати, оновлювати й контролювати. Вони об’єднують кілька функцій безпеки в одне рішення

та повідомляють про інциденти через єдину систему звітності. Альтернатива підтримці багатьох різних продуктів безпеки створює додатковий тягар для IT-персоналу та збільшує ймовірність порушень безпеки.

Традиційні брандмауери покладаються на перевірку портів/протоколів і блокування для захисту корпоративних мереж на рівнях каналу передачі даних і транспортних рівнях (рівні 2 і 4 моделі OSI). Цей статичний підхід був ефективним у минулому, коли IT-середовище було менш динамічним, ніж зараз, і програми можна було ідентифікувати за портом. Але зі зростаючою складністю віртуалізованих мереж і розширеними загрозами безпеки цього вже недостатньо. Брандмауери нового покоління розумніші: вони можуть фільтрувати пакети на основі додатків (рівень 7 моделі OSI) і навіть на основі поведінки, роблячи чіткі відмінності, які набагато ефективніші, ніж загальні методи, які використовуються традиційними брандмауерами. Вони також посилаються на зовнішні дані для виявлення загроз. Цей динамічний, гнучкий підхід дозволяє їм виявляти та захищатися від нападників, які набагато досконаліші, ніж у минулому.

На сьогоднішній день існує п’ять типів брандмауерів:

– брандмауер фільтрації пакетів: переглядає IP-заголовок пакетів і відкидає ті, які позначені;

– шлюз на рівні ланцюга: позначає шкідливий вміст на основі рукостискань TCP та інших повідомлень про початок сеансу мережевого протоколу, а не переглядає самі пакети;

– брандмауер перевірки стану: поєднує фільтрацію пакетів із моніторингом сеансу для додаткового рівня безпеки;

– шлюз на рівні програми: фільтрує пакети за портом призначення та рядком запиту HTTP. Також відомий як брандмауер проксі.

– брандмауер нового покоління: використовує інтелектуальну технологію на рівні додатків з урахуванням контексту для захисту від передових загроз.

Цілеспрямовані та складні загрози безпеці завдають шкоди внутрішнім мережам більше, ніж будь-коли раніше. Традиційні технології брандмауера в значній мірі залежать від перевірки портів/протоколів, що неефективно у віртуалізованому середовищі, де адреси та порти призначаються динамічно. Для порівняння, брандмауер нового покоління використовує глибоку фільтрацію пакетів для перевірки вмісту пакетів, забезпечує фільтрацію додатків рівня 7 і навіть може відстежувати й блокувати підозрілу активність. Ці можливості необхідні для забезпечення безпеки в складному, динамічному середовищі.

1.6 Висновки до першого розділу

Перший розділ кваліфікаційної роботи розглядає питання аналізу технічного завдання на створення локальної комп’ютерної мережі для м’ясопереробного цеху с.Мшанець. При цьому виділено важливі для діяльності організації функції роботи мережі через впровадження надійного та захищеного цифрового документообігу. Проведено огляд можливості впровадження системи відеоспостереження для убезпечення території та приміщень, подано організацію комплексної безпеки з відео та аудіо записом. Розглянуто методи безпечного віддаленого доступу до ресурсів мережі через використання технології VPN. Як оптимальні показано методи організації VPN через використання протоколів SSL та TLS, що є вбудованими функціями сучасних браузерів. Проаналізовано використання брандмауерів для захисту критичних вузлів та програм, що дасть змогу попередити вплив шкідливих програм та зловмисників на мережу.

2 РОЗРОБКА ПРОЕКТУ ЛОКАЛЬНОЇ МЕРЕЖІ ДЛЯ М’ЯСОПЕРЕРОБНОГО ЦЕХУ С.МШАНЕЦЬ

2.1 Розробка фізичної топології для мережі м’ясопереробного цеху

Проектування мережі починається з визначення ділових і технічних вимог і триває до початку етапу впровадження мережі (коли фактично виконується робота з розгортання та налаштування того, що було розроблено). Проектування мережі включає такі речі, як аналіз мережі, IP-адресацію, вибір обладнання та планування впровадження.

Однією з найпопулярніших моделей життєвого циклу мережі є модель Cisco PPDIOO (Prepare, Plan, Design, Implement, Operate and Optimize) [27-30]:

– приготування. На цьому етапі визначаються вимоги та стратегія очікуваних результатів від впровадження мережі в м’ясопереробному цеху. Наприклад, наслідком виконання дій на цьому етапі може бути оформлення документації на проектування чи дослідження особливостей роботи мережевих елементів;

– планування. Послідовно процес переходить на даний етап використовуючи інформацію про конкретні вимоги, які зібрані на етапі планування;.

– дизайн. Використовуючи результати попередніх двох етапів проводиться розробка дизайну мережі та проектування необхідних технічних рішень.

– реалізація. Виконується впровадження проектних рішень, проводиться налаштування обладнання та розгортання мережевих служб. Для перевірки правильності роботи здійснюється тестування працездатності;

– оперування. Це частина життєвого циклу, де мережа використовується у роботі в цеху. Впровадження моніторингу є необхідною

умовою на даному етапі. За допомогою постійного спостереження відбувається перевірка правильності роботи згідно планованих результатів, а також приймаються міри у випадку невідповідності очікуваних величин;

– оптимізація. У певний момент життєвого циклу більшості мереж потрібні налаштування та оптимізація. Це етап, на якому визначаються зміни, що покликані покращити роботу мережі. Для серйозних змін цикл починається знову з їх планування та реалізації.

На рисунку 2.1 показано цикл моделі Cisco PPDIOO

Рисунок 2.1 – Цикл проектування мережі

Використовуючи запропоновану архітектуру проведемо виконання необхідних кроків для приготування до планування розробки проекту локальної комп’ютерної мережі м’ясопереробного цеху с.Мшанець.

Для розробки фізичної топології комп’ютерної мережі на рисунку 2.2 показано план першого поверху будівлі цеху. Аналіз приміщень дає змогу визначити точки встановлення камер відеоспостереження, коробів для прокладання кабелів, точок підключення користувачів, розміщення бездротових точок доступу. При плануванні також необхідно врахувати наявність підключення живлення або необхідність використання подачі живлення через мережеві кабелі і потребу відповідного обладнання.

Розумне технологічне обладнання також повинне бути врахованим на цьому етапі для збирання статистики про виробничі процеси.

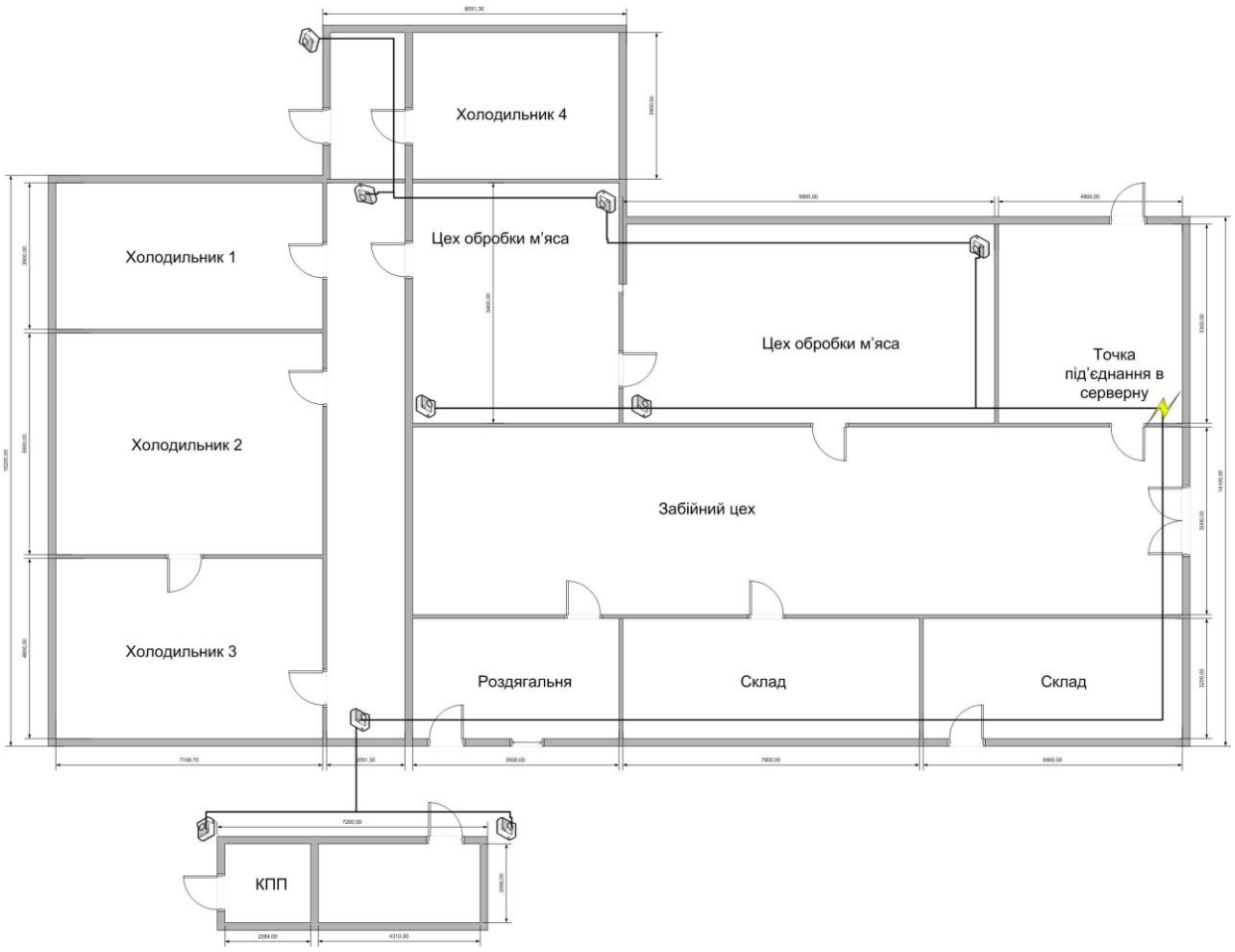


Рисунок 2.2 – План першого поверху м’ясопереробного цеху

Планування будемо проводити починаючи з контрольно пропускного пункту та рухаючись за годинниковою стрілкою. В’їзд на територію котролюється автоматичиними воротами та камерами відеоспостереження. Результати зберігаються на локальному сервері і два рази на добу синхронізуються з хмарним сховищем для підвищення надійності у випадку фізичної поломки. Холодильники 1, 2, 3 є послідовно розміщеними холодильними кімнатами і моніторяться через спільний коридор двома камерами відеоспостереження. Оскільки в них тільки один вхід та вихід цього є достатньо для контролю периметра. Обладнання холодильних

кімнат має мікропроцесори моніторингу виробничих параметрів. Покази температури, вологості та змін інших параметрів в режимі реального часу фіксуються та передаються на сервер збереження, що також синхронізованих з хмарними сховищами. Такий підхід забезпечує можливість цілодобового контролю вихідних параметрів та оперативного реагування у випадку виходу з ладу якогось обладнання. Холодильник 4 розміщений окремостоячим і моніториться окремою камерою, що також захоплює периметр огородженої території цеху. Цехи обробки м’яса знаходяться під постійним відеоспостереженням з двох причин. Перша – це контроль за виконанням виробничих процесів, а друга – можливість убезпечити себе від наслідків нещасних випадків на виробництві.

Вхід в роздягальню та в приміщення складських приміщень моніториться зовнішьою камерою на будинку КПП, що дає змогу проводити ретельний моніторинг входу та виходу персоналу з детальною фіксацію часу.

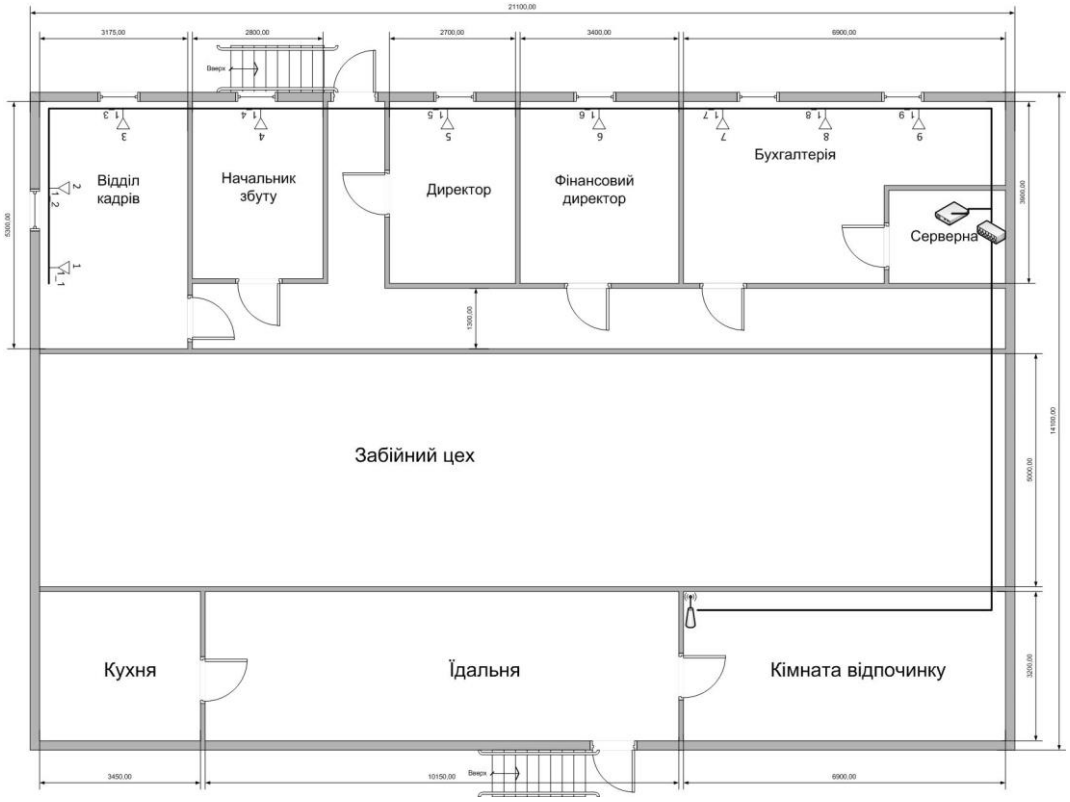


Рисунок 2.3 – План другого поверху цеху

На рисунку 2.3 показано планування другого поверху цеху. Як видно з поданого матеріалу, цей поверх є також адміністративним. Огляд будемо проводити за годиниковою стрілкою згідно попередього етапу.

Оскільки на виробництві позмінна робота, то в цеху організовано приготування їжі для працівників. Кухня знаходиться в зоні дії бездротового зв'язку. Відділ кадрів має три робочих місця для операторів ПК, два з яких задіяні і одне резервне.

Одразу біля відділу кадрів розміщено кабінет начальника відділу збуту, який може користуватись проводовим під'єднанням для настільного комп'ютера, а також використовувати ноутбук з бездротовим підключенням. Директора та фінансовий директор мають аналогічні з начальником відділу збуту опції для роботи з комп'ютерною мережею. Бухгалтерія використовує тільки проводове підключення із забороною використання переносних комп'ютерів.

В приміщенні бухгалтерії розміщено окрему кімнату, що використовується як серверна. Дана кімната замикається на ключ і доступ до неї є тільки в обслуговуючого персоналу мережі цеху.

2.2 Створення логічної топології для локальної комп'ютерної мережі м'ясопереробного цеху.

Аналіз планів приміщень та організаційної структури мережі показав необхідність розділення мережі цеху на складові елементи, що не будуть мати прямого доступу один до одного. Найпростішим способом організувати поділ мережі не сегменти є використання технології VLAN (Virtual Local Area Network), що спростить управління функціями мережі.

Результати організації розподіленої на відділи мережі показано в таблиці 2.1.

Таблиця 2.1 – Організаційний поділ мережі

Назва відділу	Планове значення VLAN	Наявні та потенційні точки під’єднання користувачів
Камери відеоспостереження	VLAN 10	10
Відділ кадрів	VLAN 11	4
Начальник збуту	VLAN 12	2
Директор	VLAN 13	2
Фінансовий директор	VLAN 14	2
Бухгалтерія	VLAN 15	4
Бездротові користувачі	VLAN 16	10

Для контролю прокладання та використання кабелів в мережі створено схему з позначеннями номерів та відповідності прокладки. Таблиця 2.2 показує результати такого проектування.

Таблиця 2.2 – Створення схеми кабелів цеху

Номер кабелю	Порти на комутаторі	Відділ	Статус кабелю
К1_1, К1_2, К1_3	Gi 0/1, 0/2, 0/3	Кадри	Викор.
Кадр_1	Gi 0/4	Кадри	Резерв
З1_4	Gi 0/5	Збут	Викор.
Збут_1	Gi 0/6	Збут	Резерв
Д1_5	Gi 0/7	Директор	Викор.
Дир_1	Gi 0/8	Директор	Резерв

Продовження таблиці 2.2

Ф1_6	Gi 0/9	Фін. директор	Викор.
ФінД_1	Gi 0/10	Фін. директор	Резерв
Б1_7, Б1_8, Б1_9	Gi 0/11, 0/12, 0/13	Бухгалтерія	Викор.
Бухг_1	Gi 0/14	Бухгалтерія	Резерв
Т1_10	Gi 0/15	Бездротовий зв’язок	Викор.
Точка_1	Gi 0/16	Бездротовий зв’язок	Резерв
І1_11	Gi 0/17	Інтернет	Викор.
Інтернет_1	Gi 0/18	Інтернет	Резерв

Документування кабелів є необхідною умовою при монтажі. Кожен кабель згодом маркується згідно визначеної схеми і це допоможе в подальшому швидко виправляти поломки.

Таблиця 2.3 – Логічна схема мережі цеху

Призначення	VLAN	Ім’я VLAN	Підмережа	Шлюз
Спостереження	10	VideoLAN	192.168.10.48/28	192.168.10.62
Кадри	11	HR	192.168.10.24/29	192.168.10.30
Збут	12	Marketing	192.168.10.32/30	192.168.10.34
Директор	13	Director	192.168.10.36/30	192.168.10.38
Фінансовий директор	14	Fdirector	192.168.10.40/30	192.168.10.42
Бухгалтерія	15	Finance	192.168.10.16/29	192.168.10.22

Продовження таблиці 2.3

Бездротові користувачі	16	WiFi	192.168.10.0/28	192.168.10.14
Інтернет	–	–	192.168.10.44/30	192.168.10.46

В таблиці 2.3 наведено логічні адреси та їх розподіл у мережі м’ясопереробного цеху с. Мшанець.

2.3 Пропонований набір активного обладнання для цеху

Для побудови мережі цеху зарпопоновано використання комутатора третього рівня, що буде задовольняти проектовані рішення, описані в попередніх розділах.

В таблиці 2.4 подано основні характеристики вибраного комутатора.

Таблиця 2.4 – Основні характеристики комутатора

Версія ПЗ	Назва пристрою	Набори портів	Можливість забезпечення живлення
Базовий IOS	PC-C3560X-48T-L	48 портів	потужність 350W
Базовий IOS	PC C3560X-48P-L	48 портів з PoE+	потужність 715W
Базовий + IP	PC C3560X-48T-S	48 портів	потужність 350W
Базовий + IP	PC C3560X-48P-S	48 портів з PoE+	потужність 715W
Базовий + IP + розширення	PC C3560X-48P-E	48 портів з PoE+	потужність 715W

Для забезпечення потреб цеху згідно проектних рішень та майбутнього розширення мережі доцільно взяти робочий свіч C3560X-48P-E.

Забезпечення бездротового доступу користувачів повинно бути надійним та захищеним. Для вибору точки доступу порівняємо наступні екземпляри.

Таблиця 2.5 – Вибір точки доступу

	D-Link DAP-1525	Linksys WRT 300N
Підтримка стандартів	802.11n, 802.11g, 802.11b, 802.11a	802.11n, 802.11g, 802.11b, 802.11a
Максимальна швидкість	до 300 Мбіт/с	до 300 Мбіт/с
Підтримка шифрування AES	+	+
Частоти роботи	2,4 ГГц та 5ГГц	2,4 ГГц та 5ГГц

Оскільки обидві точки доступу мають практично однакові характеристики, то основним при їх виборі буде інтеграційна складова. Обладнання однієї фірми краще працює одне з одним і тому для проекту мережі цеху буде взято точку Cisco.

2.4 Тестування модельованих рішень мережі м’ясопереробного цеху с. Мшанець

Моделювання є зручним інструментом для перевірки пропонованих рішень, що дає змогу на етапі розробки та проектування провести перевірку вірності запропонованих технологій та конфігурувань.

На рисунку 2.4 показано спрощену модель роботи локальної комп’ютерної мережі для м’ясопереробного цеху.

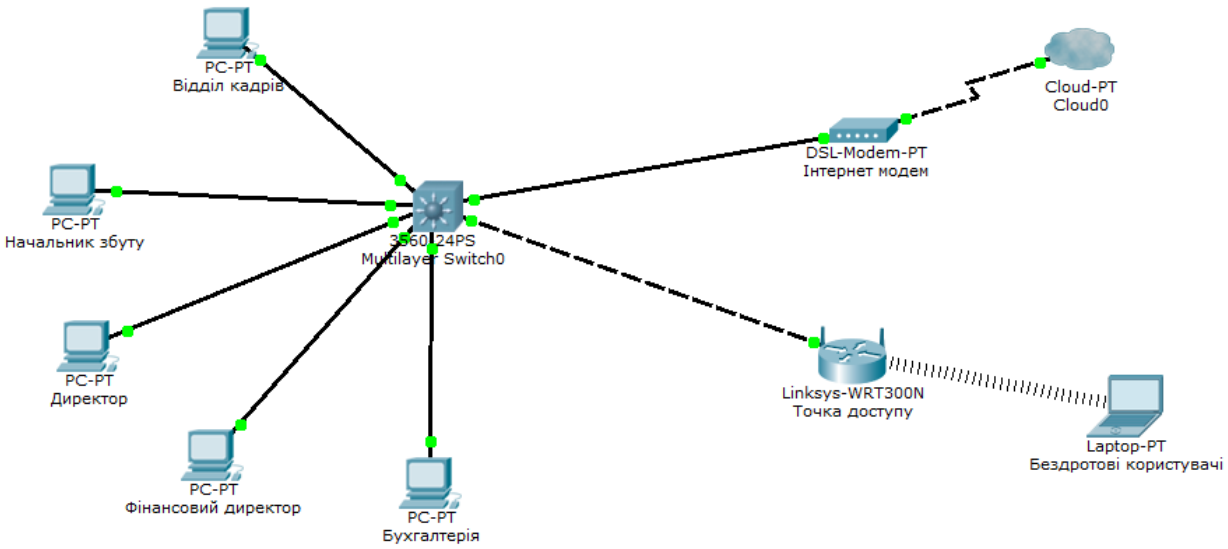
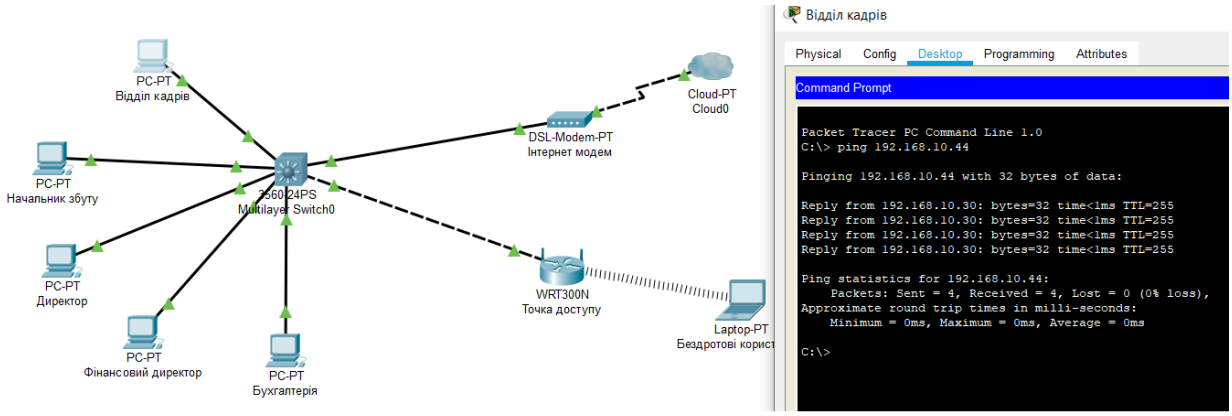


Рисунок 2.4 – Модель роботи мережі цеху

Спрощення моделі відбулось без втрати основних компонентів, що потребують перевірки на даному етапі.

Для перевірки з'єднання проведемо тестування доступу Відділу кадрів до Інтернету, результати яких показано на рисунку 2.5



Результати тестування показують, що налаштування пристроїв виконано вірно та згідно розроблених схем. З'єднання функціонує без втрат пакетів. Модельовані рішення можуть бути перенесені в реальну мережу, що буде гарантувати ефективність роботи.

2.5 Висновки до другого розділу

В другому розділі проведено розробку фізичної топології локальної комп’ютерної мережі для м’ясопереробного цеху с. Мшанець. Здійснено розведення кабелів для підключення активного мережевого обладнання та визначено точки розміщення камер відеоспостереження. Розроблено логічну топологію, що враховує особливості організації праці цеху. Виконано поділ на віртуальні мережі для підвищення захищеності з’єднань між відділами. Розраховано IP схему для кожного відділу та з’єднання до мережі Інтернет. Проведено моделювання проектованих рішень з подальшим тестуванням, що дасть змогу перевести модель у реальну мережу з найменшими помилками.

3 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

3.1 Конституційні засади охорони праці у м’ясопереробному цеху с.Мшанець

Законодавчими актами, що визначають основні положення про охорону праці є загальні закони України, а також спеціальні законодавчі акти. До загальних законів належать: Конституція України, Закони України: “Про охорону праці”, “Про охорону здоров’я”, “Про пожежну безпеку”.

Спеціальними законодавчими актами є Державні нормативні акти про охорону праці, будівельні норми та правила.

В основному законі України – Конституції питанням охорони праці присвячені статті 43, 45 та 46.

Стаття 43: “Кожен має право на працю, що включає можливість заробляти собі на життя працею яку він вільно обирає, або на яку вільно погоджується”, “Кожен має право на належні, безпечні і здорові умови праці, на заробітну плату, не нижчу від визначеної законом”, “Використання праці жінок і неповнолітніх на небезпечних для їхнього здоров’я забороняється”.

Стаття 45: “Кожен хто працює має право на відпочинок. Це право забезпечує наданням днів щотижневого відпочинку, а також оплачуваної щорічної відпустки, встановленням скороченого робочого дня щодо окремих професій, скороченої тривалості роботи у нічний час”.

Стаття 46: “Громадяни мають право на соціальний захист, що включає право на забезпечення їх у разі повної, часткової або тимчасової втрати працездатності, втрати годувальника, безробіття з незалежних від них обставин, а також у старості та інших випадках, передбачених законом”.

Основоположним законодавчим документом у галузі охорони праці є Закон України “Про охорону праці”. З набуттям незалежності України перша серед республік прийняла цей закон 14 жовтня 1992 року. Цей закон визначає основні положення щодо реалізації конституційного права громадян про охорону їх життя і здоров’я в процесі трудової діяльності, регулює за участю відповідних державних органів відносини між власником підприємства, установи і працівником з питань безпеки праці.

Специфічною особливістю, цього Закону є високий рівень прав і гарантій працівника. Вперше в історії держави працівникам було надано право відмовитися від дорученої роботи, якщо створилася виробнича ситуація, небезпечна для його життя чи здоров’я або для людей які його оточують, і навколишнього природного середовища. Розширено права працівників у соціальних гарантіях відшкодування збитків у випадку їх ушкодження їх здоров’я на виробництві. Передбачається нова система фінансування охорони праці планування системи страхування від нещасних випадків і профзахворювань. До позитивних моментів закону також належить закріплення за державою функції нагляду за охороною праці.

Конституція України (ст.24) на вищому законодавчому рівні закріпила рівність прав жінки і чоловіка. Разом з тим, трудове законодавство, враховуючи фізіологічні особливості організму жінки, інтереси охорони материнства і дитинства, встановлює спеціальні норми що стосуються охорони праці та здоров’я жінки.

Відповідно до ст. 174 КЗпП забороняється застосування праці жінок на важких роботах і на роботах зі шкідливими або небезпечними умовами праці, а також на підземних роботах, крім деяких підземних робіт (нефізичних робіт або робіт по санітарному та побутовому обслуговуванню).

У законодавчих актах про охорону праці приділяється значна увага наданню пільг вагітним жінкам і жінкам які мають дітей віком до трьох

років. Таких жінок забороняється залучати до роботи у нічний час, робіт у вихідні дні, а також направляти у відрядження.

Відповідно до Закону України “Про відпустки” (ст. 17) на підставі медичного висновку жінкам надається оплачувана відпустка у зв’язку з вагітністю та пологами тривалістю 1265 календарних днів (70 днів до пологів і 56 після). Відповідно до ст.19 Закону України “Про відпустки” жінці, яка працює і має двох і більше дітей віком до 15 років або дитину-інваліда, за її бажанням щорічно надається додаткова оплачувана відпустка тривалістю 5 календарних днів без урахування вихідних.

Забороняється відмовляти жінкам у прийнятті на роботу і знижувати їм заробітну плату за мотивів пов’язаних з вагітністю або наявністю дітей віком до трьох років. Звільняти жінок, які мають дітей до трьох років, з ініціативи власника або уповноваженого ним органу не допускається, крім випадків повної ліквідації підприємства, установи, організації, але з обов’язком працевлаштування (ст. 184 КЗпП.).

Держава враховує певні фізичні, фізіологічні та інші особливості неповнолітніх і виявляє турботу про здоров’я молодого покоління. Законодавчо це закріплено, зокрема, в ст. 43 Конституції України. Законом України “Про охорону праці” забороняється застосування праці неповнолітніх, тобто осіб віком до вісімнадцяти років, на важких роботах і на роботах із шкідливими або небезпечними умовами праці, а також на підземних роботах. Забороняється також залучати неповнолітніх до піднімання і переміщення речей, маси яких перевищує встановлені для них граничні норми. Не допускається прийняття на роботу осіб молодше від шістнадцяти років. Однак, як виняток, можуть прийматися на роботу особи, які досягнули п’ятнадцяти років за згодою одного з батьків або особи, що його замінює. Для підготовки молоді до продуктивної праці допускається прийняття на роботу, учнів загальноосвітніх шкіл, професійно – технічних і середніх спеціальних навчальних закладів для виконання легкої роботи, яка

не завдає шкоди здоров’ю і не порушує процесу навчання, у вільний від навчання час по досягненні ними чотирнадцятого річного віку за згодою одного з батьків або особи, що його замінює (ст. 188 КЗпП). Забороняється залучати неповнолітніх до нічних, надурочних робіт та робіт у вихідні дні. Усі особи молодше вісімнадцяти років приймаються на роботу лише після попереднього медичного огляду.

Для неповнолітніх у віці від 16 до 18 років встановлений скорочений 36 – годинний робочий тиждень, а для п’ятнадцятирічних – 24-годинний. Заробітна плата працівникам молодше від вісімнадцяти років при скороченій тривалості щоденної роботи виплачується в такому ж розмірі, як працівникам відповідних категорій при повній тривалості щоденної роботи (ст. 194 КЗпП). Щорічні відпустки неповнолітнім надаються в літній час або, на їх бажання в будь-яку іншу пору року (ст. 195 КЗпП). Тривалість такої відпустки один календарний місяць.

3.2 Технічні засоби безпеки у м’ясопереробному цеху с. Мшанець

Системи пожежної сигналізації у м’ясопереробному цеху с. Мшанець представляють собою комплекс технічних засобів, службовців для своєчасного виявлення спалаху в приміщеннях.

В ідеалі будь-яке приміщення має бути обладнане пожежною сигналізацією, яка працює цілодобово. Вона допоможе вчасно виявити загоряння, знищити його вогнище, подасть сигнал до евакуації людей, що є особливо важливим в освітніх установах.

Особливістю системи пожежної сигналізації є можливість її автоматичного перемикання на живлення від акумулятора при відключенні в будинку електрики. Автоматично ж відбувається і заряджання акумулятора.

Важливою частиною пожежної сигналізації є спеціальні датчики. Звичайно застосовуються детектори температури і наявності диму і газів.

Існують прості моделі датчиків, наприклад порогові неадресні, за допомогою яких важко точно визначити місце загоряння, а також складніші. Так аналогові адресні сповіщувачі забезпечені індивідуальними адресами, за якими система швидко знаходить джерело пожежі. Зазвичай аналогові сповіщувачі використовуються для уловлювання диму і контролю за температурою в приміщенні.

Димовловлювачі діляться на іонізуючі і оптичні. Обидва типи датчиків реагують на появу в приміщенні, що охороняється диму і визначають його концентрацію. Оптичний прилад діє за допомогою розсіяного інфрачервоного випромінювання, а іонізуючий використовує іонізаційну камеру.

Для забезпечення контролю за всіма вікнами та дверима в будівлі на них необхідно встановити спеціальні датчики. Зазвичай в таких випадках застосовуються датчики розбитого скла, інфрачервоні датчики руху і присутності, магнітоконтактні і вібродатчики. Інформація з датчиків передається на контрольний пульт за допомогою комп'ютера або телефонної лінії.

Для контролю за територією, що безпосередньо примикає до входу в будівлю, зазвичай використовуються датчики руху. При виникненні в контрольованій зоні переміщається об'єкта датчик передає сигнал на пульт управління. Сучасні пристрої дозволяють так запрограмувати детектори даного виду, щоб вони не реагували на рухи домашніх тварин.

3.3 Висновки до третього розділу

В цьому розділі кваліфікаційної роботи розглянути питання, що стосуються безпеки життєдіяльності та охорони праці в школі.

ВИСНОВКИ

В кваліфікаційній роботі здійснено розробку проекту локальної комп’ютерної мережі для м’ясопереробного цеху с. Мшанець:

– здійснено аналіз технічного завдання на розробку мережі для м’ясопереробного цеху, що дало змогу визначити основні аспекти проектування майбутньої мережі;

– проведено огляд хмарних рішень для організації цифрового документообігу, що покращить умови праці в офісі та зробить збереження даних більш стійким до неочікуваних втрат;

– проаналізовано системи відеоспостереження та моніторингу фізичної активності, що допоможе контролювати працівників та відвідувачі, а також буде доказовою інформацією у випадку надзвичайних подій;

– проведено огляд можливих рішень для забезпечення віддаленого захищеного доступу до ресурсів мережі;

– запропоновано використання брандмауерів для підвищення захищеності мережевих елементів та програм;

– здійснено розроблювання фізичної та логічної топологій для м’ясопереробного цеху з вибором активного мережевого обладнання;

– проведено тестування проектованих рішень.

В розділі «Безпека життєдіяльності, основи охорони праці» розглянуто питання конституційних засад охорони праці у цеху та технічних засобів безпеки при роботі.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. S. Wilkins and T. Smith, CCNP Security. SECURE 642-637 Official Cert Guide. Cisco Press, 2011, ISBN: 978-1-58714-2802.

2. A. D wankhade and P. N. Dr Chatur, “Comparison of Firewall and Intrusion Detection System,” Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 1, pp. 674–678, 2014, URL: http://ijcsit.com/docs/Volume 5/vol5issue01/ijcsit20140501145.pdf/.

3. T. King et al., “BLACKHOLE Community,” Internet Engineering Task Force (IETF), 2016. [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc7999. – Назва з екрану. – Дата звернення: 4.04.2022.

4. D. S. Ms. Charjan, P. S. Ms. Bochare, and Y. R. Bhuyar, “An Overview of Secure Sockets Layer,” Int. J. Comput. Sci. Appl., vol. 6, no. 2, pp. 388–393, 2013

5. “Cisco Network Admission Control (NAC) Solution Data Sheet - Cisco.” [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/nacappliance-cleanaccess/product_data_sheet0900aecd802da1b5.html. – Назва з екрану. – Дата звернення: 14.04.2022

6. M. Kozlova (AKA M. Kozlova, “7 luchshikh servisov zashchity ot DDoS-atak dlya povysheniya bezopasnosti [The 7 best services of protecting from DDoS- attacks for the increase of safety],” HOSTING.cafe, 2017. [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/company/hosting-cafe/blog/324848/. – Назва з екрану. – Дата звернення: 15.04.2022

7. Приїхав до Польщі – користуйся Інтернетом! [Електронний ресурс] – Режим доступу: http://naszwybir.pl/internet/. – Назва з екрану. – Дата звернення: 15.04.2022

8. V. F. Shangin, Informatsionnaya bezopasnost [Information Security]. Moscow, Russia: DMK Press, 2014.

9. Беркман Л. Н. Архітектурна концепція побудови, принцип реалізації, ефективність застосування інтелектуальної телекомунікаційної мережі / Л. Н. Беркман, С. В. Толюпа // Зб. наук. праць ВІТІ НТУУ ―КПІ‖. – 2007. – №3. – С. 9-17.

10. Колченко В. О. Впровадження інтелекту в мережі наступного покоління (NGN) – перехід до мереж майбутнього покоління (FGN) / В. О. Колченко / Наукові записки УНДІЗ. – 2010. – №2(14). – С.80-85.

11. Беркман Л. Н. Проблеми створення сучасної конвергентної мережі на базі концепції FMC (Fixed-Mobile Convergence) / Л. Н. Беркман, О. І. Чумак, В. В. Григорович, П. Ю. Дещинський // Вісник УНДІЗ. – 2008. – №2. – С. 61-63.

12. Мурай А. В. Оценка качества телекоммуникационных услуг с учетом степени удовлетворения ожиданий и требований пользователей / А. В. Мурай // Наукові записки УНДІЗ. – 2013. – № 2(26). – С. 68-75.

13. Гребенніков В. О. Проблема загальнодоступності основних телекомунікаційних і інформаційних послуг в Україні та загальні підходи до її розв’язання / В. О. Гребенніков, Г. Ф. Колченко // Наукові записки УНДІЗ. – 2013. № 1(25). – С. 5-13.

14. Колченко Г. Ф. Розроблення нормативних документів для забезпечення функціонування системи оперативно-технічного управління телекомунікаційними мережами / Г. Ф. Колченко, І. В. Шестак // Наукові записки УНДІЗ. – 2012. – № 2(24). – С. 5-8.

15. Система управління сучасними телекомунікаційними мережами : монографія : у 2 ч. / [Кривуца В. Г., Беркман Л. Н., Климаш М. М. та ін.]. – Київ : ДУІКТ, 2009. – 268 с.

16. Шерстнева О. Г. Подходы к оценке качества управления связью / О. Г. Шестернева // Сети и системи связи. – 2008. – №11. – С. 35-41.

17. What is SD-WAN (Software-Defined Wide Area Network)? [Електронний ресурс]. – Режим доступу: https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/ – Назва з екрану. – Дата звернення: 12.04.2022.

18. SD-WAN vs MPLS: The Pros and Cons of Both Technologies)? [Електронний ресурс]. – Режим доступу: https://www.sdxcentral.com/networking/sd-wan/definitions/sd-wan-vs-mpls-pros-cons-technologies/ – Назва з екрану. – Дата звернення: 18.04.2022.

19. Cisco Software-Defined WAN (SD-WAN) FAQ [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sw-defined-wan-faq-cte-en.html?dtid=osscdc000283 – Назва з екрану. – Дата звернення: 18.04.2022.

20. Cisco Software-Defined WAN (SD-WAN) Cloud onRamp for Colocation At-a-Glance [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-on-ramp-aag-cte-en.html – Назва з екрану. – Дата звернення: 20.04.2022.

21. Draft-ietf-nvo3-geneve-08 [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/draft-ietf-nvo3-geneve-08 – Назва з екрану. – Дата звернення: 22.04.2022.

22. What Is Network Virtualization? [Електронний ресурс]. – Режим доступу: https://blog.gigamon.com/2018/01/04/network-virtualization-optimize/ – Назва з екрану. – Дата звернення: 22.04.2022.

23. Solving the Network Virtualization Conundrum [Електронний ресурс]. – Режим доступу: https://www.arista.com/en/solutions/network-virtualization – Назва з екрану. – Дата звернення: 23.04.2022.

24. F. Dad et al., “Optimal Path Selection Using Dijkstra’s Algorithm in Cluster-based LEACH Protocol,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 2, pp. 194–198, Feb. 2017.

25. Z. U. Rahman et al., “Investıgatıng the Pakıstan's Offshore Software Industry Infrastructure,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 3, pp. 237–243, Mar. 2017

26. Z. U. Rahman et al., “Magnetic Resonance Images Classification through Relevance Vector Machine,” Journal of Applied Environmental and Biological Sciences, vol. 7, no. 1, pp. 213–217, Jan. 2017

27. Membrey, Peter, Eelco Plugge, and David Hows. Practical Load Balancing: Ride the Performance Tiger. Apress, 2012.

28. Popovic, Miroslav. Communication protocol engineering. CRC press, 2016. 277

29. S. Tim, Cisco Telepresence Fundamentals. Pearson Education India, 2010.

30. Tate, Jon, et al. IBM Flex System and PureFlex System Network Implementation. IBM, International Technical Support Organization, 2013.