Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Програмно-технічні засоби забезпечення функціонування мережі із захищеними каналами передачі даних
Назва теми

Галузь знань 12 «*Інформаційні технології*»
Спеціальність *123 «Комп'ютерна інженерія»*
Освітня програма «*Комп'ютерна інженерія*»
Шифр *КРКІ.190169.19.01.14 ПЗ*

Виконав: студент IV курсу, група КІ1с–19-1 _____ О.В. Сукач
Підпис Ініціали, прізвище

Керівник _____ Ю.В.Хмельницький
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ 09.06.22 С.В. Мостовий
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки _____ Ю.П. Кльоц
Підпис,дата Ініціали, прізвище

«9» червня 2022 р.

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЯ ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П.Кльоц

"11" 01 2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Сукач Олександр Володимирович
Прізвище, ім'я, по батьков студента

1. Тема проекту (роботи): Програмно-технічні засоби забезпечення функціонування мережі із захищеними каналами передачі даних
Керівник роботи Хмельницький Юрій Владиславович к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджено наказом ректора університету від 06. 01. 2022 року №1, додаток №
2. Строк подання студентом проекту на кафедру: 07.06. 2022 р.
3. Вихідні дані до проекту Завдання на дипломне проектування
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Здійснити огляд, провести аналіз та дослідження існуючих рішень по реалізації програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних. Описати етапи дослідження та здійснити проектування системи захисту мережі, схеми мережі та необхідні розрахунки. Виконати обґрунтування кваліфікаційної роботи та побудову програмно-технічного засобу підвищення ефективності роботи системи захисту для доступу користувачів на базі відомих моделей захисту каналів передачі та на основі алгоритмів захищеного доступу до потоків інформації.
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Настройка роботи комп'ютерної мережі, Загальна структура мережі, Схеми захищеного доступу, Роботи по настроюванню системи, Реалізація забезпечення системи функціонування мережі із захищеними каналами передачі даних.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання Видав	Завдання Прийняв
Нормо контроль	Мостовий С.В., викладач кафедри КБ		
Плагіат	Мостовий С.В., викладач кафедри КБ		

7. Дата видачі завдання 06.01. 2022 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапу (розділу) кваліфікаційної роботи	Строк виконання етапу роботи	Примітка
1.	Вступ. Огляд існуючих методів, засобів.	1 декада Лютий	Виконано
2.	Обгрунтування вибраного варіанту.	2 декада. Лютий	Виконано
3.	Опис характеристики та роботи .	3 декада. Лютий	Виконано
4.	Розробка організаційної структури	1 декада. Березень	Виконано
5.	Розробка схеми розташування станцій	2 декада. Березень.	Виконано
6.	Підготовка ескізів креслень.	3 декада. Березень	Виконано
7.	Розробка частини по захисту	1 декада . Квітень	Виконано
8.	Розрахункова частина.	2 декада . Квітень	Виконано
9.	Висновки.	3 декада. Квітень.	Виконано
10.	Погодження з консультантами.	1 декада. Травень	Виконано
11.	Оформлення графічного матеріалу.	1 декада. Травень	Виконано
12.	Оформлення пояснювальної записки.	2 декада. Травень	Виконано
13.	Попередній захист кваліфікац. роботи.	3 декада. Травень	Виконано
14.	Подання роботи на плагіат	3 декада. Травень	Виконано
15.	Захист кваліфікаційної роботи	1 декада . Червень	Виконано

Студент _____ О.В. Сукач
(підпис) (Ініціали, прізвище)

Керівник роботи _____ Ю. В.Хмельницький
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Програмно-технічні засоби забезпечення функціонування мережі із захищеними каналами передачі даних»

Автор роботи: Сукач Олександр Володимирович

Керівник роботи: Хмельницький Юрій Владиславович

Пояснювальна записка: 6 с., табл. 3, форм.37, 26 джерел.

Графічна частина: 7 презентаційних слайдів.

МЕРЕЖА ПЕРЕДАЧІ ДАНИХ, ІНФОРМАЦІЙНІ ПОТОКИ, ЗАХИЩЕНА ЛІНІЯ, ДОСТУП, ЕФЕКТИВНІСТЬ РОБОТИ, ЗАХИЩЕНІ КАНАЛИ ПЕРЕДАЧІ.

Метою кваліфікаційної роботи є підвищення ефективності та якості функціонування мережі, захищеності та пропускної здатності систем передачі даних по захищених каналах на основі використання сучасних методів та засобів захисту каналів передачі та покращенню пропускної здатності цих ліній шляхом вдосконалення та розширення функціональності мережі, покращенню алгоритмів її роботи, впровадженню та удосконаленню засобів для підвищенням захищеності при передаванні потоків інформації. Поставлена у кваліфікаційній роботі ця мета досягається розв'язанням задач:

1) виконати аналіз вже існуючих методів та засобів захисту каналів передачі даних по лініях зв'язку у мережах;

2) уточнити та визначити адаптивні шляхи підвищення функціональності роботи мережі та її програмно-технічної системи для передачі захищеної інформації;

3) виконати якісну інфраструктурну реалізацію побудови мережі та спроектувати програмно-технічної засоби для захисту каналів передачі інформації .

Отримані результати і їх новизна – удосконалена мережа, що якісно функціонує та має захищені канали для передачі даних, що дозволяє підвищити ефективність роботи цієї мережі та функціонування системи захисту інформації. Область її застосування – забезпечення працездатності програмно-технічної системи для передачі інформації мережею із захищеними каналами передачі.

09.06.2022

Формат	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
				Текстові документи		
А4		1	КРКІ.190169.19.01.14 ПЗ	Пояснювальна записка	1	
				Графічні матеріали		
А4		2	КРКІ. 190169.19.01.14 Е8	Захист мереж в різних	1	
				технологіях		
А4		3	КРКІ. 190169.19.01.14 Е8	Схема мережі	1	
				загальна		
А4		4	КРКІ. 190169.19.01.14 Е8	Схема розташування	1	
				комп'ютерів мережі		
А4		5	КРКІ. 190169.19.01.14 Е8	Настройка роботи	1	
				мережі		
А4		6	КРКІ. 190169.19.01.14 Е8	Статистика роботи	1	
				мережі		
А4		7	КРКІ. 190169.19.01.14 Е8	Схема резервування	1	
				роботи мережі		
А4		8	КРКІ. 190169.19.01.14 Е8	Організаційна	1	
				структура мережі		

КРКІ. 190169.19.01.14 ВП

Зм.	Арк.	№ Докум.	Підпис	Дата
Розробив		Сукач О.В.		09.06
Перев.		Хмельницький Ю.		
Н. контр.		Мостовий С.В.		09.06
Затверд.		Кльоц Ю.П.		9.06.22

Програмно-технічні засоби забезпечення функціонування мережі із захищеними каналами передачі даних
Відомість проекту

Літера	Аркуш	Аркушів
У	1	1

ХНУ, КПс-19-1

ЗМІСТ

ВСТУП

Метою кваліфікаційної роботи є розробка програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних, підготовка проекту однієї із ліній передачі між центрами зв'язку, що буде слугувати для покращення її роботи та функціонування. Ще декілька років тому не було уявлення про Інтернет, то на сьогоднішній день вже практично більшість усіх комп'ютерів підключено до мереж Інтернет. На сьогодні кількість користувачів мережі Інтернет росте та зростає їх розширені потреби, у якісному та доступному їх сервісі, який їм вже надають різні провайдери для доступу до такої мережі. Широке використання таких сучасних інформаційно-телекомунікаційних систем, а також пов'язане із цим збільшення об'ємів потоків інформації, що обробляється, вимагають на сьогодні розширення кола для нових користувачів, яким потрібен широкий доступ до ресурсів та даних інформаційних систем. Найдоступнішим на сьогодні методом організації такого доступу є створення комп'ютерних мереж. Проте використання таких мереж у регіональному їх масштабі із можливістю для доступу до глобальної мережі Інтернет вже породжує нові питання щодо безпеки зберігання та передачі такої інформації. При експлуатації таких систем має значна увага приділятися для захисту інформаційних ресурсів від несанкціонованих користувачів які бажають їх використати та модифікувати чи просто її знищити. Під захистом такої інформації мається на увазі підтримання повної цілісності, доступності та конфіденційності цих даних які використовуються для уведення та зберігання, обробки та передачі цих потоків. Також важливою складовою для захисту інформації є забезпечення її повної безпеки при передачі каналами ліній зв'язку, по скільки саме на цьому на шляху для передачі інформаційного контенту тут можливе її перехоплення, що ставить під загрозу для конфіденційності цих даних. По скільки для зберігання, її обробки та передачі інформаційних даних використовується сучасне комп'ютерне та мережне обладнання, тому для вирішення цієї проблеми для захисту інформації необхідне вже поєднання роботи програмних та різних апаратних засобів. На сьогодні в Україні чимало підприємств та фірм, які б могли похвастатися безпекою та якістю

роботи на основі технологічних баз, які можуть значно спростити весь процес їх роботи у цілому.

На сьогоднішній день сама мережа Інтернет стає невід'ємною її частиною для ведення різного бізнесу, що дозволяє працювати із великими потоками масивів інформації та здійснювати миттєву комунікацію із географічно розрізненими регіонами держави. Мережа Інтернет стала універсальним засобом для зв'язку та спілкування практично всіх людей. Разом із тим, мережа Інтернет є важко контрольованим каналом для поширення потоків інформації, що іноді призводить до того, що різні мережеві засоби нерідко використовуються і для отримання різного несанкціонованого доступу до конфіденційної та закритої інформації із боку зловмисників та різного роду мережевих шахраїв. Сама мережа Інтернет [1] відіграє тут істотну роль і у конкурентній розвідці, а це збір відомостей про дії та плани їх конкуруючих організацій із метою для подальшого ослаблення їх ринкових позицій. У мережі різного роду інформаційні загрози для діяльності організацій та підприємств можуть створюватися як ще одиничними шахраями чи непрофесійними суб'єктами і також потужними та високопрофесійними спеціальними організаціями, що задіяні у багаторівневих стратегіях їх конкурентної боротьби.

На сьогодні вимоги організацій та користувачів до мережі Інтернет задовольняються покращенням якості інформаційних каналів для передачі даних, де на заміну звичайним телефонним дротам та кабелям прийшлі оптично-волоконні лінії, нові канали передачі даних за допомогою сучасного супутникового зв’язку тощо. Проте все ж значну роль при такій кількості різних з’єднаних у мережу комп’ютерів вже відіграє якість протоколів при допомозі яких і здійснюється передача потоків даних між серверами та протоколів для маршрутизації і алгоритмів, на яких вони побудовані. Усі сучасні інформаційні системи побудовані вже по багаторівневому принципу і тому для організації зв'язку хоча б двох комп'ютерів, потрібно спочатку створити правила для їхньої взаємодії та визначити мову для їхнього спілкування. Тобто треба визначити, що означають ті сигнали, що посилаються ними. Ці правила та основні визначення загалом називаються протоколами. Для роботи різних інформаційних систем необхідно запастись багатьма вже різноманітними протоколами: управляти фізичним зв'язком,

установлення необхідного зв'язку по мережі, доступом до різноманітних інформаційних ресурсів тощо. Багаторівнева структура інформаційної мережі має бути розроблена із метою спростити та впорядкувати цю безліч протоколів та відношень і розробити засоби для забезпечення функціонування мережі із захищеними каналами передачі даних. Взаємодія різних рівнів у цій моделі такої системи - ординарна. Тут кожний рівень може реально взаємодіяти тільки із сусідніми йому рівнями, а віртуально тільки із аналогічним рівнем на іншому кінці лінії такої ж інформаційної мережі.

У кваліфікаційній роботі для вирішення поставленої задачі буде проведено аналіз сучасних методів та засобів захисту інформації у мережах передачі даних, як програмних, так апаратних. До програмних засобів захисту інформації тут можна віднести різні програмні шифратори інформації та мережні брандмауери. Надійність таких методів захисту на сьогодні є сумнівною, по скільки всі ці програмні засоби працюють під керуванням різних операційних систем які легко піддаються зовнішнім атакам. Це може вже призвести до втрати цінної та конфіденційної їх інформації. Сучасні апаратні засоби не мають таких тут суттєвих недоліків, по скільки їх головна ідея, це реалізація їх у вигляді автономних пристроїв, в яких вже будуть алгоритми шифрування які виконуються чи вбудовані у модулях ПЛІС [2] або у захищених електронних модулях які побудовані на базі процесорів чи контролерів із використанням оригінальних нових операційних систем. Сучасні брандмауери можна віднести до програмних і до апаратних засобів у залежності від їх реалізації.

Проблемою для цих обох видів засобів захисту інформації є те, що доступ до потоків інформації може відбуватися не шляхом атаки на їх робочі станції, а вже шляхом перехопленням інформації у самих каналах зв’язку. Такий тип атаки проконтролювати досить важко тому, що ставить під загрозу збереження усієї конфіденційності інформації. Під реальною взаємодією для таких інформаційних систем розуміємо безпосередню їх взаємодію, безпосередню передачу всієї інформації. При безпосередній передачі усі потоки даних залишаються незмінними увесь цей час. Під віртуальною ж взаємодією тут розуміємо опосередковану їх взаємодію та передачу даних. Ці дані у процесі передачі можуть бути вже

визначеними та заздалегідь обговореним способом видозмінитися. У зв'язку із вищевказаними причинами забезпечення функціонування інформаційної мережі постійно треба оптимізувати, тобто проводити певні зміни для покращення роботи та захистити канали передачі. У даній кваліфікаційній роботі буде проведено удосконалення існуючих програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних для покращення пропускної здатності каналів зв'язку.

Актуальність кваліфікаційної роботи полягає у вдосконалені топології та архітектури програмно-технічних засобів для забезпечення функціонування мережі із захищеними каналами передачі даних на основі використання сучасних засобів та покращення пропускної здатності ліній передачі шляхом використання захищених каналів для передачі інформації , що зумовлює актуальність теми для цієї кваліфікаційної роботи. Прикладною задачею, що вирішується у даній кваліфікаційній роботі є забезпечення підвищення якості функціонування, захищеності та пропускної здатності систем передачі інформації у мережі.

Метою роботи є підвищення ефективності та якості функціонування мережі, захищеності та пропускної здатності систем передачі даних по захищених каналах на основі використання сучасних методів та засобів захисту каналів передачі та покращенню пропускної здатності цих ліній шляхом вдосконалення та розширення функціональності мережі, покращенню алгоритмів її роботи, впровадженню та удосконаленню засобів для підвищенням захищеності при передаванні потоків інформації. Поставлена у кваліфікаційній роботі ця мета досягається розв'язанням задач:

1) виконати аналіз вже існуючих методів та засобів захисту каналів передачі даних по лініях зв'язку у мережах;

2) уточнити та визначити адаптивні шляхи підвищення функціональності роботи мережі та її програмно-технічної системи для передачі захищеної інформації;

3) виконати якісну інфраструктурну реалізацію побудови мережі та спроектувати програмно-технічної засоби для захисту каналів передачі інформації .

Отримані результати і їх новизна – удосконалена мережа, що якісно функціонує та має захищені канали для передачі даних, що дозволяє підвищити

ефективність роботи цієї мережі та функціонування системи захисту інформації. Область її застосування – забезпечення працездатності програмно-технічної системи для передачі інформації мережею із захищеними каналами передачі.

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ЗАХИСТУ ДАНИХ ТА ОГЛЯД ІСНУЮЧИХ ЗАСОБІВ, МЕТОДІВ ТА ТЕХНОЛОГІЙ

1.1 Аналіз основ функціонування та побудови систем захисту мереж при передачі захищеної інформації у каналах комунікації

На сучасному етапі розвитку цивілізації який характеризується швидким переходом від його індустріального до інформаційного суспільства, у якому передбачається вже наявність нових форм для соціальної та економічної їх діяльності. Це все базується на масовому використанні сучасних інформаційних та телекомунікаційних технологій. Усі існуючі мережі для зв'язку загального користування використовують технологію із комутацією каналів та комутацією пакетів, що у даний час вони не зовсім відповідають перерахованим вище вимогам до них. Обмежені їх можливості для традиційних мереж є досить стримуючим чинником на шляху до впровадження нових інформаційних послуг та їх мереж. Сучасні мережі являють собою досить самостійний клас таких мереж, що будуються на основі нових концепцій, на базі яких може бути вже здійснено надання більш широкого набору як для традиційних, так і для сучасних нових інформаційних послуг. Визначення сучасних захищених мереж як самостійного класу вже означає, що їх регламентація має уже здійснюватися на основі нової нормативно-технічної бази, що уже враховує особливості для інтеграції усіх послуг та системно-технічних рішень у рамках однієї інформаційної захищеної мережі.

Інформаційна захищена мережа - це багато сервісна мережа зв'язку, що підтримує інтеграцію різних послуг для передавання мови, даних та медіа, що базується на основі IP-мережі. Основна ж відмінність таких мереж сучасного покоління від традиційних мереж є у тому, що уся медійна інформація яка циркулює

у комп'ютерній мережі може бути розбита на дві її складові. Це є сигнальна інформація, що забезпечує комутацію різних користувачів та надання інформаційних послуг. Безпосередньо захищені дані користувача, що містять необхідну корисну інформацію, призначену для абонентів, а це голос, відео, дані та захищені шляхи для її проходження усіх сигнальних повідомлень та даних користувача тут можуть не збігатися. Окрім того, при формуванні основних вимог до перспективних багато сервісних мереж необхідно враховувати особливості їх діяльності для постачальників послуг у цій мережі. Тут сучасні підходи до регламентації різних послуг для приєднання передбачають доступ постачальників інформаційних послуг, у тому числі, що не володіють власною своєю інфраструктурою, до ресурсів такої мережі для загального користування без їх дискримінації.

Для забезпечення функціонування мережі із захищеними каналами передачі даних в положеннях із побудови багато сервісних мереж [3] використовуються такі основні терміни та їх визначення:

- Мережі для зв'язку наступного покоління – це концепція побудови для мереж передачі, що забезпечують надання для необмеженого набору інформаційних послуг із гнучкими можливостями для їх управління і персоналізації та створенню різних нових послуг за рахунок мережевих рішень. Це передбачає вже тут реалізацію транспортної мережі із розподіленою комутацією, винесення функцій для надання послуг у кінцеві мережеві вузли та інтеграцію із традиційними мережами.
- Багато сервісна мережа - це мережа передачі, побудована відповідно до концепції нового покоління та забезпечує тут надання необмеженого набору їх послуг.
- Багато протокольна мережа – це транспортна мережа передачі, що входить до складу багато сервісної мережі та забезпечує вже перенос різних видів потоків інформації із використанням різних для протоколів передачі.
- Інформаційна комунікаційна мережа - це є технологічна система, що включає у себе окрім засобів для доставки і засоби зберігання, обробки та пошуку інформації яка призначена для забезпечення користувачів зв'язком та доступом до необхідної їм різної інформації.

Мережа для зв'язку загального користування загалом призначена для надання

послуг сучасного електрозв'язку користувачам на прилежній території. Мережа для зв'язку включає також мережі із географічної та не географічної системою їх нумерації. Не географічна система для нумерації використовується у технологічних та спеціальних комунікаційних мережах. Мережа для зв'язку являє собою повний комплекс взаємодіючих між собою мереж передачі, включаючи і мережі для розповсюдження програм різного телевізійного та радіо мовлення. Мережі ж загального користування мають приєднання до комунікаційних мереж загального користування різних держав. Технологічні та мережі спеціального призначення вже утворюють групу для мереж обмеженого користування тому що контингент їх користувачів обмежений їх корпоративними клієнтами. Такі мережі передачі можуть взаємодіяти між собою, проте не мають приєднання до основних мереж для загального користування, а також до комунікаційних мереж загального користування. Виділена інформаційна мережа може бути приєднана до мереж для загального користування із переведенням їх у категорію мереж для загального користування, якщо вона ще відповідає її вимогам.

Сучасні технологічні мережі призначені для забезпечення різної виробничої діяльності для організацій та управління їх технологічними процесами. При наявності великої вільних ресурсів для цих мереже ресурси можуть бути приєднані до комунікаційних мережі для загального користування із переведенням їх у категорію для мереж загального користування та для використання для них надання платних послуг для будь-якого користувача. Мережі для спеціального призначення використовуються для забезпечення потреб управління, безпеки та охорони правопорядку. Такі спеціальні мережі не можуть використовуватися для платного надання інформаційних послуг, якщо це не передбачено законодавством. За основною функціональною ознакою самі мережі розділяються на комунікаційні мережі доступу та транспортні мережі передачі. Транспортною є та частина мережі, що виконує свої функції для переносу чи транспортування інформаційних потоків повідомлень від їхніх джерел із однієї комунікаційної мережі доступу до різних одержувачів таких повідомлень для іншої мережі доступу вже шляхом розподілу цих інформаційних потоків між цими мережами доступу. Мережею доступу для комунікаційної мережі є та її частина, що пов'язує це джерело

повідомлень із вузлом для доступу, що є граничним між комунікаційною мережею доступу та транспортною мережею. При проектуванні програмно-технічних засобів для забезпечення функціонування мережі із захищеними каналами передачі даних у мережі за типом приєднування абонентів загалом комунікаційні мережі поділяються на [4]:

- це мережі для фіксованого зв'язку, що забезпечуються по приєднанню стаціонарних абонентів;

- це мережі для рухомого мобільного зв'язку, що забезпечують приєднання різних рухомих абонентів.

Загальні ж підходи до побудови багато сервісних мереж знайшли відображення у концепції перспективних мереж наступного покоління [5]. Базовим же принципом для нової концепції є відділення один від одного різних функцій для переносу та комутації, функцій для управління викликом та управління послугами. Функціональна модель для такої мережі у загальному випадку може бути представлена її трьома рівнями – це транспортний, управління комутацією та передачею потоків інформації, управління їх послугами. Завданням основного транспортного рівню є комутація та прозора передача потоків інформації для користувачів. Завданням ж рівня його управління комутацією та передачею інформації є обробка потоків інформації для сигналізації, маршрутизація її викликів та керування потоками передачі.

Рівень для управління інформаційними послугами містить різні функції для управління логікою послуг та додатків та являє собою розподілену середовище, що забезпечує надання інформаційних комунікаційних послуг, управління цими послугами, створення та впровадження нових інформаційних послуг, можлива взаємодія різних послуг [6]. Рівень управління послугами вже дозволяє реалізувати специфіку для цих послуг та застосовувати одну програму для логіки послуги, незалежно від типу її транспортної мережі та способу її доступу. Наявність для цього рівня дозволяє вводити на такій мережі будь-які нові інформаційні послуги без втручання у режим функціонування інших рівнів. Рівень для управління послугами може також включати безліч підсистем, що базуються на різних

технологіях роботи, мають своїх користувачів та використовують внутрішні системи для адресації.

Архітектура для таких мережі, яка побудована у відповідності із новою концепцією, складає універсальна транспортна мережа, яка реалізує функції транспортного рівню та рівня для управління комутацією і її передачею. До складу такої транспортної мережі можуть входити – різні транзитні вузли, що тут виконують функції по переносу та комутації, кінцеві вузли, що вже забезпечують доступ користувачів до ресурсів багато сервісної мережі, різні контролери сигналізації, що тут виконують функції для обробки інформації та сигналізації, управління викликами і їх з'єднаннями, різні шлюзи які забезпечують підключення традиційних мереж. Контролери для сигналізації можуть бути вже винесені у окремі пристрої, які призначені для обслуговування їх декількох вузлів для комутації. Використання ж загальних контролерів дозволяє тут розглядати їх як єдину інформаційну систему, розподілену по цій мережі. Таке комунікаційне рішення не тільки значно спрощує алгоритми для встановлення з'єднань та є більш економічним для операторів, постачальників цих послуг. Це дозволяє замінити дорогі системи для комутації великої ємності досить невеликими, гнучкими та доступними за вартістю різним дрібним постачальникам інформаційних послуг. Призначення транспортної мережі є швидке надання послуг для перенесення потоків інформації. Реалізація інформаційних комунікаційних послуг здійснюється на базі вузлів служб та вузлів для управління послугами . Кожен вузол служб є обладнанням для постачальників послуг та може розглядатися у якості серверу для додатків цих інформаційних комунікаційних послуг, клієнтська частина для яких реалізується самим кінцевим обладнанням його користувача.

Всі вузли управління послугами є деякими елементами розподіленої платформи для інтелектуальної мережі та виконує функції по управлінню логікою та атрибутами їх послуг. Сукупність цих кількох вузлів служб чи вузлів для управління їх послугами, які задіяні для надання одних послуг, утворюють вже платформу для управління такими послугами. До складу цієї платформи також можуть вже входити вузли для адміністративного їх управління цими послугами та сервери їх різних додатків. Кінцеві ж вузли для транспортної мережі можуть тут

виконувати різні функції вузлів цих служб. Склад цих функцій для граничних вузлів може бути розширений за рахунок додавання нових функцій по наданню послуг. Для проектування та побудови таких вузлів може вже використовуватися технологія їх гнучкої комутації. Інформаційні комунікаційні послуги припускають вже взаємодію для постачальників таких послуг та операторів передачі, що може забезпечуватися на основі функціональної моделі для розподілених баз даних, що виконуються згідно із рекомендаціями. Доступ до таких баз даних зорганізується із використанням протоколу такого як LDAP. Згадані ці бази даних дозволяють все вирішувати для наступних завдань – це створення довідників, автоматизація для взаєморозрахунків між операторами та їх постачальниками для цих послуг, забезпечення їх взаємодії між операторами у процесі надання інформаційних послуг, забезпечення їх взаємодії , що мають тут різні функціональні можливості, на двох різних кінцях для з'єднання.

У мережі із захищеними каналами бази даних можуть вже використовуватися постачальниками послуг для організації їх платних інформаційних довідкових послуг. Концепція такої мережі де в чому спирається на нові технічні рішення, що розроблені міжнародними організаціями для стандартизації. Для управління інформаційними послугами будуть використані такі протоколи та підходи, що застосовуються у сучасних інтелектуальних мережах. У якості технологічної основи для побудови транспортного рівня багато сервісних мереж розглядаються протокол IP із можливим застосуванням у оптичної їх комутації. У рекомендаціях усі інформаційні послуги пропонується ділити на інтерактивні та мовні послуги. Приклад діалогових інформаційних послуг наведені у таблиці 1.1.

Таблиця 1.1 - Приклад діалогових інформаційних послуг служб

Тип інформації	Широкосмугова послуга	Область їх застосування
Рухомі зображення та звук	Відео та телефонія	Системи зв'язку для передачі мови, їх нерухомих та рухомих зображень між двома їх користувачами
	Відео конференції	Системи зв'язку для їх передачі мовою, документів, нерухомих та рухомих зображень
	Відео спостереження	Системи охорони та моніторингу технологіч-

		них процесів, дорожнього їх руху
	Передача відео та аудіо інформації	Передачі ТБ, робота із БД медіа
Звук	Передача безлічі звукових каналів	Передача кількох радіо програм, інформація про канали на декількох мовах одночасно
Дані	Високошвидкісна передача для інформації у цифровій формі	Передача даних при їх взаємодії: мережі, розподілені мережі, комп'ютери, передача відеоінформації та нерухомих зображень.
	Високошвидкісне телеуправління	Системи сигналізації, Телеметрія, Системи контролю у реальному часі.
Документи	Високошвидкісний факс	Передача зображень, текстів та малюнків
	Передача відео високої роздільної здатності	Передача відео із проф. якістю. Комп'ютерні різні ігри із віддаленими користувачами
	Обмін документами	Передача різних змішаних документів

Багато сервісна мережа може бути побудована із використанням обладнання різних фірм і така схема мережі може бути побудована за допомогою нового обладнання. Багато сервісний комутатор доступу у такій мережі являє собою програмно-апаратний комплекс, що призначений для надання послуг передачі у місцевих телекомунікаційних мережах. На його базі вже можливо створення корпоративних мереж та організація системи передачі у офісах. Багато сервісний комутатор доступу виконує функції SOFTSWITCH у такій мережі, тобто він підтримує обмін як мовною так і медійною інформацією у передачі по мережі. В багато сервісних мережах взаємодія із транспортною IP-мережею відбувається по інтерфейсу GIGABIT ETHERNET та використовує нові протоколи для сигналізації для взаємодії із вузлами мережі. На базі всього однієї такої системи можливо організувати мережі для зв’язку. Розширення такої мережі можливо за допомогою встановлення додаткових модулів для обробки викликів.

Загалом така технологія – це нова концепція для гетерогенної багато сервісної мережі, що забезпечує передачу інформаційних потоків усіх видів медіа та розподілене надання різного необмеженого спектру телекомунікаційних послуг. Тут є можливість для їхнього додавання та редагування такої їх розподіленої тарифікації. Виділення кожному такому сервісу потрібної смуги для пропускання дозволяє оператору передачі впроваджувати різні сервіси, які враховують вимоги

їх клієнтів. У основі мережі лежить пакетна мережа передачі медіа даних. Інноваційна сутність такої технології полягає навіть не в тому, що вона забезпечує більш гнучке, швидкісне та ефективне середовище для передачі, а у тому, що вона не прив'язана до самої концепції каналу передачі та забезпечує повно зв’язність такої мережі. Це все досягається за рахунок фізичного та логічного ділення передачі та маршрутизації їх пакетів, а також його встаткування для передачі пристроїв та логіки для керування викликами і послугами [7]. Впровадження такої технології дозволяє оператору передачі замість двох мереж: звичайної комунікаційної мережі та мережі Інтернет - отримати одну інформаційну мережу, що поєднує у собі всі їх кращі риси, а це адаптованість для передачі потоків будь-якого типу, низьку їх вартість для передачі у розрахунку на одиницю її об'єму інформації, які властиві для комп’ютерної мережі та Інтернет, та також якість голосового зв'язку і критично важливих їх додатків для передачі даних, які властиві мобільній мережі.

Використання такої багато сервісної мережі забезпечує мінімізацію для капітальних та експлуатаційних витрат для оператору передачі. Така мережа об’єднує під одною назвою всі новітні досягнення науки та техніки, технологію, що не накладає обмежень на пропускну здатність каналів передачі завдяки ущільненню у одному чи декількох їх оптичних сигналів із різними довжинами хвиль. Використання такої технології дозволяє оператору передачі краще, простіше та дешевше вже надавати усі най різноманітні послуги, незалежно від типу передачі даних та доступу. Винаходити нові види сервісів, що у свою чергу гратиме тут вирішальну роль у забезпеченні їх конкурентоспроможності.

1.2 Особливості застосування систем захисту при побудові системи передачі даних

У кваліфікаційній роботі для аналізу особливостей систем захисту для програмно-технічних засобів забезпечення функціонування мереж із захищеними каналами передачі даних необхідно розглянути засоби для здійснення авторизації доступу до таких каналів передачі потоків даних. Система безпеки мережі повинна забезпечити обмеження для фізичного доступу персоналу організації чи

підприємства та можливе повне виключення доступу сторонніх при монтажу приймального та різного роду випромінюючого устаткування радіо мереж для передачі даних. Доступ вже повинен контролюватися службою безпеки. Прокладка каналів для високочастотного кабелю має бути вже виконана прихованим способом чи у коробах із подальшим опломбуванням цих коробів. Сама довжина для високочастотного кабель сегменту має бути досить мінімальною. Сам доступ у приміщення із модемами, мостами та станціями передачі, які оснащені радіо адаптерами повинен вже контролюватися службою безпеки. Адміністратор такої мережі повинен все детально документувати та всі процедури для налаштування модемів, мостів та станцій передачі, що оснащені радіо адаптерами.

Для організації захищених каналів передачі у особливості роботи адміністратора мережі має входити процедури, щоб регулярно міняти реквізити для авторизації видаленого управління усіма цими пристроями. Також адміністратор мережі має мати виділений окремий адресний пул для його адміністрування по цих пристроях. Сам же адміністратор такої мережі із захищеними каналами передачі має відключити усі невживані функції для модемів, мостів та станцій передачі, що оснащені радіо адаптерами. При функціонуванні мережі адміністратор повинен буде активувати функції модему чи мосту тим самим забезпечуючи тунель та криптографічний захист усіх повідомлень, що вже приймаються. Сам адміністратор має повно контролювати доступ до таких модемів, мостів та різних станцій, які оснащені радіо адаптерами із боку вузлів такої комп'ютерної мережі. Один із можливих способів для такого контролю, це використання між мережевого екрану у цій системі захисту.

При авторизації доступу на канальному рівні для організації роботи комп’ютерних мереж до особливостей забезпечення безпеки використовують для захисту розділення середовища для його передачі різними комунікаційними засобами їх канального рівня. Усі протоколи та стандарти для цього рівня описують вже усі процедури для перевірки доступності такого середовища передачі та коректності передачі цих даних. Для здійснення контролю по доступності всі середовища необхідно використовувати, по скільки специфікації для фізичного рівня уже не враховують те, що у деяких інформаційних комунікаційних системах

лінії передачі можуть розділятися між декількома уже взаємодіючими їх вузлами і тому фізичне їх середовище передачі може бути зайнято. Переважна ж більшість комп'ютерних інформаційних комунікаційних систем вже побудована на основі відомої технології ETHERNET. До особливостей її функціонування можливо віднести, що алгоритм її роботи для визначення доступності такого середовища для усіх її технологій однаковий та заснований на постійному прослуховуванні цього середовища передачі усіма підключеними до неї вузлами такої інформаційної системи.

Ця особливість її роботи може використовуватись зловмисниками для організації потоків різних видів атак на ці комп'ютерні інформаційні мережі. Навіть за умови уже дотримання усіх рекомендацій щодо виключення розділення для середовища передачі сам же зловмисник може здійснити просте прослуховування потоку між довільно вибраною ним парою вузлів такої мережі. Тут використання простих мережевих комутаторів не є дуже серйозною перешкодою для таких зловмисників. Загалом же твердження про повну захищеність інформаційних мереж, що побудовані на основі топології їх фізичних зв'язків типу «зірка» та оснащених простими комутаторами є досить серйозною їх помилкою. Розглянемо також недоліки по застосування простих мережевих комутаторів як засобів забезпечення інформаційного обміну у комп'ютерних інформаційних мережах на канальному рівні.

У процесі проектування програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних було визначено, що процес передачі потоків інформації від одного вузла до іншого через простий мережевий комутатор відбувається поетапно та у подальшому потік передаються блоками. Сам же розмір блоків визначений відомими стандартами канального рівня. Основний блок даних, яким вже оперує протокол його канального рівню, називається загалом його кадром. Допустимо, що передавальний вузол визначив доступність свого середовища та початки для передачі. У його першому кадрі буде завжди широкомовний запит до усіх вузлів мережі про пошук вузлу із необхідною мережевою адресою. Такий запит містить його апаратну адресу як вузла

відправника та його мережеву адресу, де у даному випадку мова йде про його IP як протоколі для мережевого рівня.

Тут відмітимо, що цей комутатор відповідно до вимог специфікацій його канального рівню зобов'язаний передати свій широкомовний запит усім підключеним до його мережевих портів вузлам. У комп'ютерній мережі має бути також виконана вимога щодо виключення розділення середовища для передачі між двома вузлами, і тому кожен вузол буде підключений безпосередньо до свого порту цього комутатору. Тому незважаючи на виконання даної рекомендації, різні зловмисники отримують широкомовний запит вузла , по скільки вузол зловмисника може опинитися ошуканим. Тому зловмисник отримуватиме нарівні зі усіма останні широкомовні запити на дозвіл цих мережевих адрес. А далі накопичуючи відомості із широкомовних запитів, сам зловмисник матиме повне уявлення про мережеву активність усіх цих вузлів тобто хто і у який час із ким намагався почати свій інформаційний обмін. За такою простою допомогою цієї нескладної техніки сам зловмисник може визначити усі апаратні та мережеві адреси для вузлів, що є серверами та маршрутизаторами мережі. Основна ж кількість запитів на дозвіл до мережевої адреси серверу та маршрутизатору буде на декілька порядків вже вище, ніж до звичайної робочої станції. Таким чином сформувавши відомість для мережевої активності та карту її мережі із адресами передбачуваних у мережі серверів та маршрутизаторів, сам зловмисник відразу зможе також приступити до реалізації своєї атаки та відмови у доступі до цих вузлів. Тому до особливостей роботи такої мережі слід віднести , що у процесі збору широкомовних пакетів сам зловмисник не проявляв ніякої його мережевої активності, тобто він залишався невидимим для усіх вузлів такої мережі окрім самого простого комутатору, до порту якого він був підключений.

1.3 Обґрунтування і аналіз роботи програмних засобів та вирішення проблеми захисту системи передачі

При виконання кваліфікаційної роботи програмно-технічні засоби забезпечення функціонування мережі із захищеними каналами передачі даних

розглянемо, що відбувається після того, як вузол для призначення, що отримав кадр із запитом на дозвіл до своєї мережевої адреси діє далі та проаналізуємо це. Згідно вимог специфікацій для канального рівню вузол любої мережі, отримавши такий широкомовний кадр, що містить вже запит на дозвіл до своєї мережевої адреси, зобов'язаний тут же передати відправникові цього кадру свою відповідь, що містить власні мережеві та апаратні його адреси. Відповідь такого вузла буде уже не широкомовною, а просто адресованою конкретному вузлу. Мережевий комутатор зобов'язаний далі транслювати цю відповідь вузла тільки на той порт, до якого до якого був підключений цей вузол. Сам же кадр його канального рівню, що містить відповідь такого вузла вже ніяк не потрапить до самих зловмисників. Все це пояснюється тим, що у середовищі передачі, яке використовується для підключення самого зловмисника до такого комутатору, буде вільне у момент для передачі йому відповіді. Далі після отримання такого кадру із відповіддю, вузол дізнається його апаратну MAC адресу тобто вузла прийому та зможе почати передачу різних пакетів для мережевого рівня на адресу такого вузла. Подальші ж взаємодії таких вузлів знаходяться поза компетенцією для протоколів канального рівню.

Основне завдання для протоколу канального рівня вважається уже за виконане, якщо тут обмінюються інформаційними даними усі вузли, що знають апаратні адреси як один одного та можуть вже вставити мережеві пакети у кадри для канального рівню, що ідентифікується як комутатор по MAC-адресам цих вузлів. Вразливість такої системи для дозволу мережевих її адрес, що описана вище та називається ARP полягає у тому, що вузол довіряє свій вмісту кадру із відповіддю. Всі дані, що передані у відповідь на цей запит про дозвіл її мережевої адреси, ніяк не перевіряються та ніким і нічим не підтверджуються. Особливістю такої уразливістю вже може скористатись сам зловмисник, який хоче підмінити собою вузол чи прослуховувати весь потік мережевих кадрів, що передаються між будь-якими двома вузлами такої мережі.

Все це відбувається наступним чином. Сам зловмисник, вузол якого завчасно визначає апаратну та мережеву необхідну адреси тих вузлів, що будуть атакуватись. Далі починається процес по безперервно відправці на адресу вузла помилкових відповідей із вказівкою мережевої адреси необхідного вузла та апаратної MAC

адреси свого вузла. Система отримуючи помилкові відповіді від вузол перебудовує свою таблицю для дозволу своїх мережевих адрес та тому із цієї миті усі мережеві кадри, що відправляються їм на адресу вузла матимуть у заголовку апаратну адресу для вузла зловмисників. По стільки сам комутатор ухвалює рішення про трансляцію такого кадру на той чи інший його порт тільки на підставі його апаратної адреси, яка вказана у заголовку для цього кадру, тепер зловмисник вже отримуватиме усі повідомлення, що адресовані такому вузлу. Якщо ж зловмисникові вже необхідно організувати прослуховування усього потоку інформації між різними вузлами він здійснює навмисно помилкову розсилку для відповідей на адресу обох цих вузлів та отримані у свою чергу адресу кадри після перегляду та аналізу транслює його вузлу, якому вони вже призначалися.

У кваліфікаційній роботі вище описана техніка для підміни апаратних адрес не є якоюсь новою, бо різні варіанти для її реалізації давно доступні користувачам мережі Інтернет у вигляді вже готових програм із докладним керівництвом для користувачів. Практика проектування мереж показує, що у комп'ютерних інформаційних мережах продовжується використання досить дешевих простих комутаторів на досить відповідальних ділянках роботи мережі при підключенні критично важливих для них різних вузлів, серверів, маршрутизаторів тощо. Сучасні комп'ютерні інформаційні мережі, оснащені вже багатофункціональними керованими мережними комутаторами, часто ще також залишаються уразливими до таких та подібного роду атак. У досить багатьох випадках усі функції для захисту та розмежування доступу до середовища по передачі, які реалізовані у цих пристроях, залишаються практично незатребуваними у зв'язку із недостатнім кваліфікації адміністраторів мережі чи недбалістю самих системних адміністраторів вищого рівню. Ефективне ж розмежування по доступу засобами такого канального рівня можливо тільки вже за умови їх повної інвентаризації для цих вузлів мережі та формалізації основних правил взаємодії між ними. На практиці ж керівники неохоче виділяють кошти на проведення подібних захисних робіт, не розуміючи їх високої важливості для забезпечення захисту їх комп'ютерної мережі.

У ході проектування мережі для вирішення проблеми захисту системи передачі розглянемо відомі та вже приведені рекомендації, щодо використання та

проходження яких дозволяє додатково захистити комп'ютерну інформаційну мережу засобами для канального рівня. При проектуванні мережі адміністратор служби безпеки повинен вести свою інвентаризаційну відомість по відповідності апаратних та мережевих адрес для усіх вузлів мережі. Самою службою для безпеки і вже спільно із відділом цих інформаційних технологій, має вже бути розроблена нова політика для захисту комп'ютерної мережі різними засобами їх канального рівня, що визначає лише допустимі маршрути для передачі кадрів їх канального рівня. Розроблена ж політика повинна забороняти всі типи зв'язків типу один до - багатьох, та необґрунтовані вимогами для інформаційної підтримки діяльності мережі. Такою політикою також мають бути визначені усі робочі місця, із яких дозволена конфігурація цих засобів для комутації їх канального рівня. Основні ж засоби комутації для канального рівня, використовувані у комп'ютерній мережі, мають вже бути такими, щоб настроюються та мають забезпечувати розмежування доступу між усі ми вузлами мережі вже відповідно до розробленої їх політики. Тому як правило, ці засоби підтримують віртуальну технологію VLAN, що дозволяє у рамках комутатору, щоб виділити групи для адрес та сформувати для них правила для трансляції кадрів.

При роботі мережі адміністратор такої мережі повинен виконати усі налаштування для підсистеми управління VLAN комутатору, та інших їх підсистем, які необхідні для реалізації розробленої вже ними політики для захисту системи передачі. У основний обов'язку адміністратору мережі входить відключення усіх невживаних підсистем для комутатора. Сам же адміністратор мережі має регулярно все контролювати на відповідність конфігурацій цих комутаторів усій розробленій політиці по захисту. Також він у мережі має вести весь моніторинг для мережевої активності всіх користувачів із метою виявлення усіх джерел їх аномально високої кількості для широкомовних запитів. Сама служба безпеки тут має контролювати регулярність для зміни реквізитів їх авторизації їх адміністратора у підсистемах для управління комутаторами. Також служба безпеки має вже контролювати регулярність по виконанню адміністратором усіх заходів, які пов'язані із моніторингом такої мережі, здійсненням також профілактичних робіт по на-лаштуванню всіх комутаторів, а також по створенню резервних копій для

конфігурацій комутаторів. Ще служба безпеки має також забезпечити контроль доступу у приміщення, у яких розташовані комутатори та робочі станції із яких дозволено управління комутаторами.

При розробці програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних враховується, що авторизація доступу на мережевому рівні для організації роботи комп'ютерних мереж буде використання у цій інформаційній системі протоколів для мережевого рівня є вже необхідною умовою для забезпечення їх взаємодії між різними вузлами мереж із різними канальними їх протоколами. Мережеві сучасні протоколи вже дозволяють подолати усі обмеження, що накладаються основними специфікаціями для канального рівня. Вони дозволяють вже об'єднати комп'ютерну мережу із мережею Інтернет – основного провайдеру із використанням мереж для загального користування. Зробити це можливо тільки засобами для канальних протоколів на сьогодні досить складно. Окрім того, що об'єднання двох різних за призначенням комп'ютерних мереж із використанням різних мостів вкрай негативно позначається на рівні його захищеності для об'єднуваних мереж. У більшості ж випадків сам адміністратор та служба її безпеки не можуть повністю визначити вузли для цієї мережі, що підключається та формалізувати усі правила для обміну кадрами їх канального рівня.

Ще один аспект для використання протоколів мережевого їх рівня - це розмежування для доступу до ресурсів всередині мережі, що використовує тільки один стандарт для канального рівню. Використання ж для цієї мети усіх протоколів мережевого рівня дуже ефективно навіть для тих мереж, які побудовані із використанням тільки стандартів для канального рівня. Проблема ж сумісності у таких комп'ютерних мережах не актуальна тому, що корисні властивості мережевих протоколів вже можна використовувати для захисту системи передачі від дії на мережу зловмисників. Однією із таких основних властивостей є використання цими протоколами мережевого рівня для роздільної схеми адресації такої мережі та окремо взятого вузла для цієї групи користувачів. Тут зокрема адреса для протоколу мережевого рівня IP вже складається із двох частин, це номер мережі та номеру її вузла. Вже при цьому максимальна можлива тут кількість вузлів у такій мережі чи її

адресний простір вже визначається значенням їх мережевої маски чи класом такої мережі.

Таку її особливість для адресації можуть тут використовувати адміністратори мережі та різні зловмисники. Основним із завдань для адміністратора комп'ютерної мережі та для її співробітників служби безпеки буде захист їх адресного простору такої мережі від можливості для його використання різними зловмисниками. Частково вже таку функцію виконують різні механізми для маршрутизації, які реалізовані модулями для протоколу мережевого рівня. Здійснення ж для обміну потоками між вузлами таких мереж із різними номерами вже неможливе без попереднього їх налаштування для локальних таблиць по маршрутизації вузлів для цих мереж чи без внесення нових змін до конфігурації їх маршрутизатору, що здійснює обмін інформаційними пакетами. Майже завжди у їх адресному просторі комп'ютерної мережі залишається ще частина адрес, що не зайняті зараз та тому доступні для експлуатації різним зловмисникам. Це все і пояснюється форматом для представлення номеру мережі та номера вузла для IP-протоколу. Кількість різних вузлів у такій мережі, це завжди є 2n, тобто 4,8,16,32,64 тощо. Реальна ж кількість вузлів не завжди буває такою. Окрім того, сам адміністратор завжди має вже зарезервувати адресний її простір для нових вузлів у мережі. Тому саме цей резерв і може також бути використаний різними зловмисними для здійснення інформаційних атак на функціонуючі вузли такої комп'ютерної мережі.

Для вирішення проблеми захисту системи передачі у мережі потрібно використовувати уже весь адресний простір та не дати якусь можливість різним зловмисникам захопити адреси для невживаних вузлів. Ще одним із способів захисту є застосування у службі моніторингу комп'ютерної мережі та підтримки її віртуальних вузлів у резервному діапазоні її адрес. Така служба постійно використовує уже вільний адресний для простору мережі, та також створює власні віртуальні вузли мережі де нові віртуальні вузли мережі створюються відразу вже після відключення від комп'ютерної мережі реально функціонуючих та довірених вузлів. Тут таким чином, ця служба підміняє собою відсутні зараз любі робочі станції, сервери та маршрутизатори тощо. Для авторизації доступу на транспортному рівні для організації комп'ютерних мереж можуть використовувати властивості

транспортних протоколів, що створює найбільш ефективну перешкоду для діяльності різних зловмисників.

Для захисту системи передачі використовуються ті ознаки, що містяться у заголовках їх сегментів тобто блоків даних із якими працює її транспортний протокол. Основними ознаками тут є тип транспортного його протоколу, номер його порту та прапор синхронізації для з'єднання. Якщо ж засобами для канального рівню можна захистити любу апаратуру комп'ютерної мережі, а самі протоколи мережевого рівня тут дозволяють розмежувати доступ до її окремих вузли мережі та під мереж, то вже транспортний протокол тут використовується як основний засіб для комунікації мережевих застосувань, що вже функціонують на платформі для окремих вузлів такої мережі. У системі будь-яке мережеве застосування вже використовує її транспортний протокол для доставки різних оброблюваних її інформаційних даних. У мережі в кожного класу їх додатків є свій специфічний номер для свого транспортного порту. Така властивість може бути вже використано зловмисниками для атаки на конкретний її мережевий сервіс, її службу чи адміністратору комп’ютерної мережі для захисту їх мережевих сервісів та служб.

При проектуванні програмно-технічних засобів для забезпечення функціонування мережі із захищеними каналами передачі даних для роботи адміністратор такої інформаційної системи формує свою політику для захисту засобами транспортного рівня вже у вигляді відомості відповідності вузлам мережі, які використовуються ними для мережевих адрес та їх довірених застосувань, що вже функціонують на платформах цих вузлів мережі. Для формалізованого запису цієї відомості є загальна таблична структура, що містить у собі перелік своїх вузлів, їх символьні імена, відповідні цим вузлам їх мережеві адреси, перелік усіх використовуваних кожним його вузлом транспортних протоколів, перелік його мережевих застосувань, що вже функціонують у кожному його вузлі та і відповідні цим застосуванням їх порти його транспортного протоколу, а також по кожному мережевому їх застосуванню необхідно вже встановити чи воно установлено його споживачем чи постачальником такого ресурсу, тобто знати чи дозволено йому ініціювати нові з'єднання чи також приймати ті що уже входять. Загалом же реалізація політики для захисту засобами його транспортного рівня здійснюється за

допомогою між мережевих екранів. Між мережевий екран, це є спеціалізоване програмне забезпечення, що реалізовує фільтрацію потоку інформаційної системи відповідно до їх правил політики захисту мережі. Таке програмне забезпечення функціонує на платформі маршрути заторів та керує інформаційними потоками для вузлів різних мереж.

1.4 Висновки. Постановка задачі

У розділі проведено дослідження її предметної області для захисту даних та огляд існуючих засобів, методів та технологій щодо забезпечення функціонування мережі із захищеними каналами передачі даних. Також проведено аналіз основ функціонування та побудови систем для захисту мереж при передачі різної захищеної інформації у її каналах комунікації. В розділі проведено огляд особливості застосування систем захисту при побудові таких системи передачі даних. В процесі роботи проведено обґрунтування та аналіз роботи програмних засобів і вирішення проблеми захисту системи передачі. Поставлена у даній кваліфікаційній роботі мета досягається розв’язанням наступних задач, а це виконати аналіз уже існуючих методів та засобів захисту каналів передачі даних по лініях зв’язку у мережах, уточнити та визначити адаптивні шляхи для підвищення функціональності роботи мережі та її програмно-технічної системи для передачі захищеної інформації та виконати якісну інфраструктурну реалізацію для побудови мережі та спроектувати програмно-технічної засоби для захисту каналів передачі потоків інформації .

2 ПРОЕКТУВАННЯ ПРОГРАМНО-ТЕХНІЧНИХ ЗАСОБІВ МЕРЕЖІ ІЗ ЗАХИЩЕНИМИ КАНАЛАМИ ПЕРЕДАЧІ ДАНИХ

2.1 Засоби та вимоги до пристроїв у мережі із захищеними каналами передачі даних

На етапі планування багато сервісної комп’ютерної мережі з захищеними каналами передачі даних спочатку досліджується існуюча обстановка, визначаються основні способи роботи її організації, вузькі для неї місця та потреби

системи. Повертаючись же до конкретного її завдання, а саме до розробки багато сервісної мережі, першою її стадією для планування мережі буде дослідження усіх принципів для роботи та її структури. Організація такої мережі з захищеними каналами передачі даних має центральний та віддалені корпуси, що знаходяться на деяких відстанях до її центрального корпусу. Структура для центрального корпусу наступна та включає у себе таких користувачів, а це директор та його секретар, головний бухгалтер, заступник директора, зав. відділом та інспектори.

Тому сучасні комп’ютерні мережі дозволяють організувати спільне для них використання пристроїв та розподілену обробку даних на декількох її мережних комп’ютерах, що дає економію матеріальних засобів та прискорення процесу для обміну інформацією у такій мережі. Мережа дозволяє для групи її користувачів виконувати спільні проекти де використовуються особливі мережні версії для прикладних програм, що спеціально призначені для роботи у таких мережах і мають спеціалізовану ліцензію, що надає їм право для групового використання цих програм. При створені мережі із захищеними каналами передачі даних необхідно передбачити різні варіанти роботи для її ефективного використання, а це обмін даними у мережі передачі даних, повний доступ до усіх ресурсів мережі Інтернет, забезпечення надійних захищених каналів для передачі у мережі передачі даних, підготовка основи для створення спільного інформаційного простору та використання пристроїв, забезпечення їх систем безпеки при розгортанні такої мережі.

У залежності від того, як розподілені функції між комп'ютерами багато сервісної мережі із захищеними каналами передачі даних, вони можуть тут виступати у трьох різних його ролях - це просто комп'ютер, що займається винятково обслуговуванням запитів усіх інших комп'ютерів та тут відіграє роль як виділений сервер мережі. Як комп'ютер, що звертається із різними запитами до ресурсів інших машини та відіграє тут роль вузла його клієнта. Це комп’ютер, що сполучає у собі функції клієнту і серверу одночасно та тут є одноранговим вузлом. При плануванні структури та архітектури захищеної мережі також врахуємо, що ця комп'ютерна мережа - це система яка в основному має кілька комп'ютерів у межах досить обмеженої території та перебувають у одному із приміщень і підключені до

одних ліній передачі інформації. На сьогодні ж більшість захищених комп'ютерних мереж загалом розміщаються усередині одного із будинків та засновані у основному на їх комп'ютерній моделі типу клієнт - сервер. Основне мережне їх з'єднання може складатися мінімум із двох комп'ютерів для такої мережі, що зв'язані між собою. Також тут можливо створити цю мережу використовуючи нові бездротові технології. У такій новій моделі клієнт - сервер зв'язок по усіх каналах передачі по цій мережі ділиться на вже дві такі основні області. Це сторона клієнту та сторону його серверу. По самому визначенню вже сам її клієнт запитує інформацію чи послуги із серверу такої мережі. Сервер же у свою ж чергу обслуговує запити для своїх клієнтів. Кожна сторона у цій моделі типу клієнт - сервер може виконувати функції як серверу так і клієнту.

При створенні комп'ютерної мережі із захищеними каналами передачі даних необхідно вибрати різні засоби та компоненти, що визначають яке його програмне забезпечення і устаткування можливо використовувати, проектуючи цю мережу. Так як комп'ютерна мережа - це невід'ємна частина для сучасної ділової інфраструктури, а сама мережа це лише одне із можливих використовуваних у ній прикладних додатків і тому не повинна бути тим єдиним фактором, що визначає вибір для компонентів мережі. Всі необхідні компоненти для мережі повинні стати доповненням до вже наявної комп'ютерної мережі та не приводить до зміни її існуючої архітектури. У даній мережі буде реалізуватись фізична топологія шина, що включає всі комп'ютери уже існуючої мережі із захищеними каналами передачі даних. Також тут у даній топології можуть використовуватися існуючі комутатори які вже з'єднані між собою та утворюють магістральну опорну її шину. До кожного такого із комутаторів при цьому підключаються також окремі комп'ютери та його шинні сегменти. Кожний користувач такої комп'ютерної мережі отримує можливість досить гнучко комбінувати переваги як шинної так і зоряної топології, а також досить легко змінювати необхідну кількість комп'ютерів, що підключені до такої мережі. У нашому проекті мережі із захищеними каналами буде використовуватися топологія «зірка», що має наступні свої переваги:

- це вихід із ладу однієї робочої станції не відбивається на роботі усієї мережі;
- це хороша масштабованість такої мережі;

- це легкий пошук несправностей та обривів у мережі;
- це висока продуктивність роботи та захищеність мережі клубу;
- це досить гнучкі можливості для адміністрування мережі.

На практиці фактично кожна організація чи фірма формулює свої власні вимоги до конфігурації їх мережі, що обумовлені характером їх розв'язуваних завдань. Тут у першу чергу необхідно визначити, скільки їх людей будуть працювати у цій мережі. Від цього їх рішення будуть залежати усі наступні етапи для створення мережі. Кількість же робочих станцій буде прямо залежати від передбачуваного числа їх співробітників. Комп'ютерна мережа із горизонтальною структурою, де усі співробітники повинні мати добрий доступ їх даних один до одного, оптимальним же рішенням є тут однорангова структура такої мережі. Організації, що побудовані за принципом вертикальної їх структури де точно відомо, який співробітник та до якої її інформації він повинен мати доступ, слід вже орієнтуватися на більш дорогий варіант такої мережі, а це система із виділеним сервером для мережі. Тільки у багато сервісній мережі існує можливість для адміністрування прав їх доступу. Загалом така мережева архітектура - це є комбінація топології, методів доступу, їх стандартів, які необхідні для створення працездатної комп'ютерної мережі.

Вибір самої топології визначається вже плануванням приміщення, у якому буде розвертатися наша комп'ютерна мережа. Велике також значення при планування мають витрати на придбання та установку всього мережевого устаткування, що є досить важливим питанням для побудови мережі. Топологія мережі типу «зірка» являє собою продуктивну її структури де їх кожен комп'ютер, у тому числі і сервери, з'єднується вже окремим сегментом кабелю із його центральним пристроєм, та все ж основною перевагою такої мережі є її значна стійкість до збоїв та загроз, що виникають внаслідок неполадок на окремих комп'ютерах чи через ушкодження його мережевого кабелю. Найважливішою ж характеристикою для обміну інформацією у таких мережах є методи доступу, що регламентують тут порядок коли їх робоча станція одержує свій доступ до усіх мережних ресурсів та може обмінюватися своїми даними. Загалом абревіатура терміну CSMA/CD - це є колективний доступ із контролем несучої та виявленням їх

колізій де за допомогою цього методу усі комп'ютери мережі одержують тут рівноправний доступ. Кожна робоча станція у такій мережі перед початком його передачі даних перевіряє, чи вільний канал передачі мережі. По закінчені передачі робоча станція перевіряє вже чи досяг адресату відправлений пакет її даних та якщо її відповідь негативна, то цей вузол робить повторний цикл для передачі контролю приймання її даних, поки не одержить повідомлення про успішне його приймання по інформації цим адресатом мережі. Тому цей метод добре зарекомендував себе у малих та середніх комп'ютерних мережах, для нас даний метод також підійде. Мережна архітектура типу ETHERNET, що буде використовуватися у даній мережі, використовує саме цей метод для доступу. У такій технології застосовується стандартний кабель на основі скрученої пари та є найбільш популярною схемою побудови мереж. Такий вид кабелю не викликає труднощів при його прокладці, тому мережа на основі такої скрученої пари, на відміну від подібних тонкого чи товстого коаксіального кабелю, будується вже по топології зірка.

Для того щоб побудувати мережу по зіркоподібній топології, то вже потрібно використати більшу кількість такого кабелю. Подібна схема має і свою перевагу, а це висока стійкість до відмови у мережі. Вихід із ладу однієї чи декількох робочих її станцій не призводить до відмови також усієї системи передачі. Якщо ж із ладу вийде центральний її вузол то його відмова вже торкнеться усього підключеного через пристрій обладнання такої мережі. Однією із основних переваг даного варіанту побудови є простота схема розширення мережі, по скільки при її використанні для додаткових пристроїв з'являється проста можливість для підключення великої кількості нових робочих станцій. При застосуванні ж неекранованої скрученої пари довжина його сегменту між комутатором та робочою станцією не повинна перевищувати 100 метрів, що не спостерігається у даній мережі.

При проектуванні програмно-технічні засобів забезпечення функціонування мережі із захищеними каналами передачі даних треба враховувати, що існують два основні підходи до побудови комп'ютерних мереж – це мережі типу «клієнт та сервер» та різні однорангові мережі. Мережа, у якій комп'ютер одночасно може бути і клієнтом та і одночасно виконувати функції серверу для інших тут на-

зивається одноранговими мережами. У таких мережах усі виділені сервери не використовуються. Хоча є багато способів зв'язати усі персональні комп'ютери у єдиний комплекс. У цьому випадку вже є можливість копіювати різні файли із диску одного комп'ютеру на інший, використовуючи всього лиш тільки файлові менеджери чи інші стандартні засоби її операційної системи. Технологія ж клієнт - сервер, що широко застосовується при роботі із базами даних у мережі, відома вже давно та найчастіше застосовувалась у великих підприємствах. На сьогодні така технологія усе частіше приваблює погляди для розробників програмного забезпечення комп'ютерних мереж, по скільки у всьому світі нагромаджено велику кількість медійної інформації по різноманітних питаннях та найчастіше уся ця інформація зберігається у різних базах даних.

У нашому проекті для побудови програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних буде використовуватися архітектура клієнт - сервер, тому, що у такій мережі постійно знаходиться адміністратор мережі який слідкує за цією комп'ютерною мережею. Сам же комп'ютер для адміністратора мережі може виступати також і у ролі серверу. Важливим аспектом для планування мережі є її спільне використання їх мережних ресурсів. Усі ресурси можуть уже використовуватися у однорангових мережах і у мережах із виділеним для них сервером. У випадку одноранговой мережі відразу ж виявляються її основні структурні недоліки, так як щоб працювати із вище перерахованих компонентів їх потрібно також встановити на їх робочу станцію чи підключити до неї його периферійне обладнання. При роботі мережі усі підключенні до цієї станції пристрої та компоненти, а також відповідні їх служби стають недоступними для колективного користування цими мережі. В усіх мережах з сервером його комп'ютер тут існує по визначенню самої системи, де його мережний сервер ніколи не вимикається окрім коротких зупинок для технічного їх обслуговування цієї мережі. Тут забезпечується цілодобовий доступ до усіх його робочих станцій до необхідної мережної периферії . У мережі є принтери, що знаходяться у кожному відособленому приміщенні. Існує декілька способів для роботи багато сервісної мережі:

- Це підключення до самої робочої станції. Тут принтер підключається до тієї необхідної робочої станції, що перебуває до нього найближче. У результаті робоча станція вже стає сервером друку. До недоліків такого підключення можливо віднести то, що при виконанні завдань на різний друк продуктивність такої робочої станції на якийсь час знижується, що досить негативно позначається на роботі інших прикладних програм при використанні цього принтеру. Окрім того, що машина буде виключена то сервер друку стане недоступним для інших вузлів такої мережі.

- Це підключення до самого серверу. Тут принтер підключається до паралельного порту такого серверу за допомогою спеціального кабелю. В цьому випадку він постійно доступний для усіх робочих станцій такої мережі. Як недолік подібного рішення тут буде обумовлений обмеженням у довжині самого принтерного кабелю, що він забезпечує для коректної передачі даних. Хоча сам кабель тут можна простягнути десь до десятків метрів, його слід прокладати вже у коробах чи у перекриттях, що значно підвищить витрати на організацію мережі.

- Це підключення до мережі через спеціальний мережний його інтерфейс. Тут принтер обладнується мережним його інтерфейсом та вже підключається до мережі як проста робоча її станція. Плата інтерфейсу тут працює як її мережний адаптер, а сам принтер реєструється на сервері як простий вузол мережі. Програмне ж забезпечення серверу у мережі здійснює передачу завдань на сам друк по багато сервісній мережі уже безпосередньо на підключений його мережний принтер. У багато сервісних мережах із шинною їх топологією цей мережний принтер та робочі станції з'єднується із мережним кабелем за допомогою їх з’єднувача, а при використанні схеми зірка - через їх комутатор.

- Це підключення пристроїв до виділеного серверу для друку, що є альтернативою третьому варіанту. Він передбачає використання спеціалізованих серверів для друку. Такий сервер вже являє собою мережний його інтерфейс який скомпонований у окремому корпусі, із одним чи декількома розніманнями для підключення цих його принтерів. Хоча у такій мережі використання серверу для друку є непрактичним.

2.2 Розрахунок параметрів підключення пристроїв до каналів системи передачі та вибір забезпечення

При проектуванні програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних самим підходящим способом для підключення різних мережевого пристроїв є підключення до мережі через спеціальний мережний інтерфейс. Для кожної із таких задач підключення визначається ефективний потік передачі даних за формулою:

$$П_{Эі} = \frac{T_{CPi}}{T_{РАБ}} * П_{НОМ} \qquad (2.1)$$

де T_{CPi} - це є середній час заняття пристрою завданням мережі,

$T_{РАВ}$ - це загальний часу роботи усієї мережі,

П н - номінальна пропускна здатність мережі, у разі фіксованого потоку передачі.

Загальний мережевий потік передачі по захищених каналах мережі визначається за наступною формулою:

$$П_{\Sigma} = \sum П_{Эі} * K_{СТ} * K_З * N_К * T_{СРС} * N_С * K_{СТ} * K_З, \qquad (2.2)$$

де Σ Пэі – це усіх сума мережних задач,

КСТ - коефіцієнт службового потоку передачі (0.05 - 0.07),

К з - коефіцієнт запасу каналу(1,2 - 2.0),

N к – це кількість комп'ютерів у мережі,

N с – це кількість серверів у мережі,

Т срс – це середній час на виконання одного завдання для серверу.

Також розраховується коефіцієнт використання комп’ютерної мережі К вик = П заг / П ном, який повинен знаходитися у межах (0,3 - 0, 6) [8]. Для розрахунку потоку передачі по захищених каналах багато сервісної мережі вона розбивається на її логічні сегменти за допомогою мережевих комутаторів. Сумарний

же потік передачі перераховується для кожного її логічного сегменту. Для такого логічного сегменту уточнюється коефіцієнт використання самої мережі, як зазначено вже вище. Загальний мережний потік для усієї мережі багато сервісної мережі:

$$53,85 + 55,75 / 2 = 54.80\text{Мбіт/с.} \quad (2.3)$$

Коефіцієнт для використання усієї багато сервісної мережі:

$$(0,5572 + 0,5575) / 2 = 0,5573 \quad (2.4)$$

У кваліфікаційній роботі по програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних_ із отриманого результату можливо сказати, що загальний коефіцієнт для використання багато сервісної захищеної мережі знаходиться у нормі. Вибір та обґрунтування основних апаратних та програмних засобів комп'ютерної багато сервісної мережі, що включає необхідне спеціальне мережеве обладнання та програмне забезпечення для самої мережі. Із основного обладнання для компонентів та пристроїв комп'ютерної мережі окрім комп'ютерів, а це робочі станції та сервери, відносяться також кабелі із конструкціями для їх прокладання у приміщені і відповідних кабельних з'єднувачів, мережевих комутаторів, маршрутизатори тощо. Щоб комп'ютер як робочу станцію можливо було увімкнути у систему багато сервісної мережі, він вже повинен бути обладнаний мережевим адаптером. Сам же тип мережевого адаптеру визначається його мережевим програмним забезпеченням та типом його кабелів, що використовуються для об'єднання усіх комп'ютерів у багато сервісну мережу.

При проектуванні програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних розглянемо також і системне програмне забезпечення для такої мережі. Будемо у мережі використовувати WINDOWS – це операційна система сімейства від компанії MICROSOFT і така її назва походить від англ. досвід. Ця назва увійшла у практику для використання, як професійна версія її системи. На відміну від попередньої версії системи WINDOWS , що поставлялася як серверна система у клієнтському варіантах, сама вона є виключно клієнтською її системою. Її серверним варіантом є випущена нова система, що побудовані на основі одного ядра її операційної системи де в результаті отримав її розвиток та оновлення яке йшло паралельно.

Надійність такої програмної системи дозволяє використовувати її у якості основи для тих задач, що вимагають саме цієї властивості. Вона також пристосована для роботи у мережі у якості також робочої станції, де потрібна підвищена її стійкість та висока продуктивність.

У комп'ютерній мережі вона є багато розрядної системою тому вона працює із лінійної моделлю пам'яті, що дозволяє адресувати до великої кількості байт пам'яті. Програма використовує метод для багато заданості, що тут гарантує адекватний розподіл її ресурсів для процесора протягом усієї її роботи. Це запобігає її монопольному захопленню самого процесору додатком та зупинку усієї системи в тих її випадках, коли сама програма працює досить нестабільно чи можливо раптово припинила свою роботу. Це також дозволяє цій програмній системі працювати навіть тоді, коли інша операційна система вже остаточно зависла. Сама ж файлова система NTFS уже удосконалена та досить надійна у своєї роботі. Використовуючи тут різні транзакції, вона має можливість щоб скасувати незавершену чи неправильну операцію для запису, що виникає у разі збою апаратного чи програмного її забезпечення.

При проектуванні завдяки такому підходу ця файлова система уже набагато менш схильна до її руйнування при різних їх нештатних ситуаціях в такій комп'ютерній мережі. Програмна система ж SERVER в основному розвиває свої функції, що закладені у попередній версії її системи. На це також вже вказувала і її версія де є нові ядра системи. Сама ж програмна система – це перша із операційних систем фірми, яка поставляється із перед установленою оболонкою NET. Це також дозволяє даній програмній системі виступати у ролі її серверу додатків для платформи NET без встановлення будь-якого вже додаткового програмного забезпечення. Поліпшений її користувальницький інтерфейс для системи по управлінню каталогом і тому стало можливим переміщати різні об'єкти шляхом їх простого перетягування та одночасного уже змінювати властивості для декількох її об'єктів. Поліпшені засоби для управління груповою її політикою для системи, включаючи нові програмні засоби. За заявами фірми, у цій системі велика увага була уже приділена для безпеки системи. Система сама тепер встановлюється у її максимально обмеженому вигляді вже без будь-яких додаткових служб, що значно

зменшує поверхню для атаки із за зовні комп'ютерної мережі. У цій програмній системі уже включений програмний між мережевий її екран FIREWALL. Також уже згодом до цієї системи був випущений ще новий пакет для оновлення, що повністю зосереджений на підвищенні самої безпеки програмної системи та включає ще декілька додаткових її функцій для захисту від атак на багато сервісну комп'ютерну мережу.

2.3 Проектування етапів планування комп'ютерної мережі з захищеними каналами передачі потоків даних

Саме проектування комп'ютерної мережі з захищеними каналами передачі даних відбувається у декілька її етапів, першим із яких є планування засобів забезпечення функціонування мережі, який у свою чергу вже може складатись із декількох її стадій. У загальному випадку для планування мережі необхідно провести аналіз економічних та технічних її показників, провести вибір найбільш прийнятних рішень для планування та провести планування проекту із врахуванням конкретних вимог до ресурсів та до самої мережі. Для забезпечення швидкісного доступу багато сервісної мережі з захищеними каналами передачі даних до мережі Інтернет будемо використовувати її доступ за допомогою ADSL. При розробці багато сервісної мережі будемо виходити із цих її характеристик. При подальшому проектуванні мережі далі розглянемо самі принципи роботи мережі. У першій будівлі для проектування знаходиться комп'ютерний центр із сервером S1. На нього будуть надходити усі запити від усіх робочих станцій, що знаходяться у приміщені підприємства, а також по необхідності і усі запити від різних інших станцій у цій будівлі та від її віддаленого серверу (S2), що знаходиться у віддаленому корпусі. Сервер же S2 з'єднаний із центральним її сервером S1 мережевим кабелем.

Усі завдання які тут будуть вирішуватись у першому приміщені – це різні мультимедійні програми, також робота у мережі Інтернет, а також створення її WEB - сторінок та графічних їх ресурсів. На сервері будуть надходити також запити від різних робочих станцій, а це від PC1до- PC25 та його сервер S2 при роботі у мережі Інтернет та для різного копіювання потрібної інформації із серверів на робочі

станції чи для збереження усієї потрібної інформації по мережі. Якщо ж виникне потреба у розмножені різних документів, тоді можна буде уже використати пристрої, що є у цій мережі. Для доступу ж до мережі Інтернет буде використовуватись пристрої ADSL вже який буде підтримувати його достатню швидкість для передачі даних, що повністю задовольняє потребу мережі. Відповідні робочі станції PC19 - PC23 будуть надсилати свої запити на сервери для поточного зберігання чи зчитування із їх бази даних необхідної інформації про свої завдання та будуть виконувати свої індивідуальні завдання на конкретному робочому місці. Для виконання цього у кабінеті вже встановлений лазерний пристрій, так як цей пристрій має дуже швидкі характеристики які достатні для одного такого пристрою. Тут також усі робочі станції будуть вже мати доступ до мережі Інтернет та можливість для перегляду електронної пошти у мережі. Робочі місця для директора, а це PC1 та його заступнику PC2 будуть виконувати уже схожі свої функції, а це перегляд у базі даних, набір та друк необхідних їх документів, робота у мережі Інтернет та перегляд пошти. Усі робочі місця у бухгалтерії будуть виконувати свої функції та виконувати роботу у спеціальній програмі для її бухгалтерії.

Тут також усі робочі станції мають доступ до глобальної мережі Інтернет та можливість для перегляду пошти. У віддаленому корпусі та у комп'ютерному приміщені вже плануються роботи із офісних та прикладних програмах. Усі комп'ютери головної будівлі, робочі станції PC3 – PC15 будуть мати також доступ до мережі Інтернет та можливість для перегляду почти. Сервер для мережі S2 – це фактично зв'язуючи ланка між головною будівлею та її віддаленим корпусом. А ось сервер S2 буде виконувати вже приблизно такі ж функції, що виконує і сервер S1..У корпусі є два приміщення для роботи інспекторів по захисту. У першому приміщені встановлено дві робочі станції PC16 та PC17, а у іншому її приміщенні встановлено ще дві робочі станції PC18 та PC19. У цих приміщеннях головні інспектори будуть розробляти свої плани, вказівки, заповнювати та редагувати данні із бази даних, а також і редагувати усі необхідні документи.

При проектування мережі з захищеними каналами передачі даних необхідно врахувати, що директора підприємства також потрібно з'єднати із мережею Інтернет. Для доступу до бази даних бухгалтерії підприємства доцільно

використовувати додаткову систему її захисту, у основі якої є свої паролі. Доступ до цих бази даних є у самого директора, його головного бухгалтера та також людини, що супроводжує роботу програми та виконує її резервне копіювання у мережі. У мережі неповний доступ, а це дозволити окремі операції слід також надати заступникам. Усім іншим працівникам підприємства, у рамках для забезпечення безпеки, у доступі до цих бази даних її бухгалтерії слід відмовити. Ще одним із джерел важливих потоків даних є робочий комп'ютер для секретаря, де усі захищені дані, а саме це їх угоди, договори та листи, акти, таблиці та діаграми, які зберігаються на комп'ютері у секретаря. У мережі іноді виникає потреба щоб переглянути якийсь документ, внести до нього зміни чи роздрукувати його, а виявляється, що потрібний документ було загублено та його потрібно досить швидко відновити. Тому директор та головний бухгалтер завжди повинні мати тут доступ до усіх цих даних. Також є ще один аспект їх роботи, а це коли ці дані є важливі та є на робочому комп'ютері секретаря і тут може також зберігатись повний архів усіх документів які треба періодично зберігати, хоча іноді їх об'єм вимагає багато часу для їх резервного копіювання. Тому сам комп'ютер секретаря також обов'язково потрібно з'єднати до цієї мережі, а задачу для резервного копіювання цих документів слід доручити окремій компетентній людині у мережі. На цю таку роль підійде та ж сама людина, що вже відповідає за резервне копіювання усіх бази даних для роботи бухгалтерії. Логічно усі ці функції забезпечення безпеки усіх комерційних даних підприємства покласти на одну людину, а це є адміністратор мережі. Це значно зменшить розповсюдження захищеної інформації, до того ж розміри мережі дозволяють зробити це.

Для підвищення ефективності функціонування роботи багато сервісної мережі із економічної точки зору варто також запровадити її централізоване керування. Керівникам підприємства для управління не потрібно чекати, поки різні керівники проведуть ряд їх грошових операцій, а потім вишлють ці гроші, замість того щоб гроші відразу надходять на рахунок. Звичайно тут можуть виникати певні незручності із приводу цієї системи бо можуть виникати певні затримки із приводу поставки засобів, так як вони спочатку повинні з'явитись для системи управління, а потім вже на підприємство. Це було б критично, якщо б система знаходилась на

великій відстані. Проте на практиці нічого не заважає у випадку її відсутності доставити його на підприємство і навпаки. Для того щоб реалізувати їх централізоване керування слід врахувати, що управління це окремі об'єкти, але бухгалтерський облік тут ведеться по одному рахунку, із нього ж робляться всі різні грошові перерахування.. Фактично тут потрібно об'єднати роботу всіх цих мереж у рамках однієї інформаційної захищеної системи із єдиною системою для обліку та звітності у такій мережі. Щоб тут реалізувати щось подібне на практиці всього достатньо перенести інформаційну її структуру для управління.

Таким чином одержуємо у мережі до якої з'єднано також заступника директора, бухгалтера та людину, яка відповідає за безпеку даних у цій мережі. На їх робочі станції у системі встановлюється таке ж саме прикладне програмне забезпечення, що необхідно для управління. Важливою також умовою є, щоб сам формат інформаційної бази даних тут співпадав. Для забезпечення їх синхронізації для цих даних на усе серверне програмне забезпечення, що зберігає всі захищені дані для бухгалтерії буде покладено також і функцію її реплікації. Ця реплікація тут виконує вже дублювання інформації між декількома її серверами. Вона також дозволяє синхронізувати і розташовані у різних доменах різні джерела інформації, навіть тоді коли всі ці домени уже розташовані в різних її місцях та з'єднані суміжно між собою лише не дуже швидкісними каналами для зв'язку та передачі даних. Головна ж ідея для реплікації полягає у здійсненні контролю за основними процесами по зміні інформації у всіх базі даних та відслідковувати перекази повідомлень про ці зміни на самій віддаленій системі, що повинна їх враховувати.

У такій моделі побудови мережі з захищеними каналами передачі даних система для транзакцій використовується як метод для вільного їх об'єднання – тобто це об'єднання їх серверів є наслідком для використання моделі уже майже реального часу. Все це означає, що уся ця інформація розповсюджується по серверах такої системи не у реальному часі та не обов'язково у їх пакетному режимі, однак із максимально тут можливою швидкістю передачі даних. Для формулювання майже реального часу було вперше вжито ще стосовно методів, що передбачають використання пошти для розсилання різної інформації на віддалені вузли такої багато сервісної мережі. Вже у цьому випадку сама система працює не в реальному

часі, по скільки між їх серверами не встановлюється прямого її мережного з'єднання. Для повного та своєчасного отримання нової інформації чи їх змін, що вносяться до системи для підприємства стає уже важливим питання для забезпечення її надійного та безпечного сполучення із мережею Інтернет. Неможливість же у потрібний час установити зв'язок із Інтернет та його сполучення може тут призвести, що інформаційні потоки їх даних, якими вони володіють просто можуть не відповідати тому, що вже є насправді.

Тут основним виходом є оренда їх виділеної лінії та підписання контракту із провайдером на надання Інтернет послуг у денний час для роботи. Окрім бухгалтерського програмного забезпечення також мережею Інтернет для захищеного сполученням може користуватись ще робота адміністратора. Так як у основі діяльності багато сервісної мережі лежать сучасні інформаційні технології, то адміністратор просто зобов'язаний мати повний доступ до усієї мережі для того, щоб відвідувати різноманітні загрозливі WEB-сторінки та користуватись захищеними засобами пошти для зв'язку із різними колегами. Усе це вказує на те, що необхідно буде створити високошвидкісну захищену мережу.

2.4 Висновок

У даному розділі кваліфікаційної роботи при розробці та проектуванні програмно-технічних засобів мережі із захищеними каналами передачі даних було розглянуто засоби та вимоги до їх пристроїв у мережі із такими каналами передачі. Також при проектуванні мережі проведено розрахунок параметрів для підключення пристроїв до її каналів системи передачі та проведено вибір забезпечення системи керування у мережі. Ще у рамках цього розділу було проведено і проектування загальних етапів планування усієї комп'ютерної мережі із каналами передачі потоків даних. Аналіз показав, що крім бухгалтерського програмного забезпечення у даній мережі та Інтернет для захищеного сполученням може також використовуватись інтенсивна робота адміністратору. Так як у основі функціонування та діяльності багато сервісної мережі лежать різні сучасні інформаційні технології, то адміністратор такої просто зобов'язаний мати увесь

повний доступ до параметрів всієї комп'ютерної мережі для того, щоб він міг відвідувати різноманітні потенційні загрозливі WEB-сторінки та користуватись різноманітними захищеними засобами їх пошти для зв'язку із різними колегами для виявлення та попередження усіх потенційних загроз для цієї мережі.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ ФУНКЦІОНУВАННЯ КАНАЛІВ ПЕРЕДАЧІ ДАНИХ

3.1 Реалізація системи захисту для сегментів комп'ютерної мережі

Для реалізації програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних у багато сервісної системі можна виділити наступні сегменти такої мережі:

- Перший сегмент мережі охоплює усі робочі станції керівників тобто директора та головного бухгалтера, секретаря та заступників та людини, на яку тут покладено обов'язки для адміністрування цієї системи. Для сполучення із мережею Інтернет через виділену лінію на комп'ютері його адміністратора встановлюється пристрій ADSL. До додаткового обладнання належать пристрої у секретаря, у головного бухгалтера та у кабінеті заступників який здатний працювати у мережі. Щодо швидкості передачі для даного сегменту мережі, то вона не є критичним фактором, по скільки потік передачі у мережі буде дуже невеликий.
- Другий сегмент мережі охоплює робочі станції у різних комп'ютерних приміщеннях. Одне робоче місце тут слід виділити під файловий сервер нашої мережі. Швидкість роботи для даного сегменту мережі має бути досить високою.
- Третій сегмент мережі охоплює усі не комп'ютерні приміщення, та який має вихід у мережу Інтернет через з'єднання із провайдером та використовуючи його захищений доступ. Слід також виділити ще один файловий сервер, який би міг зберігати вихідні тексти для захищених програм. До складу додаткових пристроїв відносяться засоби захисту каналів передачі. Швидкість у цій мережі для цього випадку відіграє досить важливу роль через потужний потік передачі у цій мережі та через досить велику кількість її робочих станцій. Щодо самої мережі у їх віддалених корпусах для багато сервісної мережі, то тут немає необхідності розбивати цю

мережу на декілька її під мереж через невелику кількість її робочих станцій. Прийнятним же рішенням у даній ситуації буде процедура об'єднати увесь персонал приміщення у рамках одного каналу швидкісної мережі, а це звичайно виходить із додержанням усіх правил безпеки роботи у мережі.

В ході планування та реалізації роботи сегментів багато сервісної мережі прийшли до висновку, що цю мережу потрібно розбити на декілька її сегментів. Таке практичне розбиття забезпечує стабільну роботу усієї мережі, по скільки у кожного сегменту є свої вимоги щодо швидкості роботи та параметрів безпеки у мережі, організації такої безпеки, доступу до потоків передачі інформації тощо. Працюючи у рамках своїх мережевих сегментів, різні користувачі одного сегменту не заважають різним користувачам із інших приміщень. Такий підхід по плануванню зменшує потік передачі даних у мережі, а отже значно збільшує стабільність, захищеність та надійність такої мережі. Для сегменту багато сервісної мережі до складу якого входять керівники, а це директор, бухгалтери та його секретар також потрібно створити надійну її під мережу, яка б гарантувала захищену та стабільну роботу, при цьому її швидкість у мережі не є вже критичним фактором.

При такій реалізації програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних уже можна сказати, що така мережна технологія задовольняє усім цим вимогам побудови. При цьому уже немає необхідності проводити додаткову її конфігурацію для цієї мережі. На робочих станціях даного сегменту мережі зберігаються досить важливі дані, втрата яких є досить критичною для організації, тому виділено одне робоче місце для посади адміністратора мережі. Тут у його обов'язки буде входити повне забезпечення стабільної роботи, її резервне копіювання та дублювання даних, захист цих даних. По скільки усі дані, що представляють інтерес для сторонніх – це є бази даних у бухгалтерії, текстові службові документи та діаграми, для їх резервного копіювання вистачить додаткового накопичувача. Об'єм та швидкість для роботи цього накопичувачів цілком вистачить при резервному копіюванні у цій мережі. Ще одним із аспектів є здатність цих баз даних втрачати свою інформацію при поломках та невчасному виході із ладу пристроїв, апаратури чи різких перебоях у

енергопостачанні всієї мережі. При виході із ладу пристроїв, апаратури тут важко чим зарадити хоча б тому, що усі комп'ютерні комплектуючи слід підбирати від таких фірм та виробників, що їх вироби мають добру репутацію як надійних, безпечних та гарантія на ці пристрої дається на строк більше, ніж на вироби та пристрої інших аналогічних фірм. Із перебоями у системі енергопостачанні набагато легше вже справлятись бо тут достатньо на усі робочі станції, де бувають перебої електроенергії, що можуть спричинити втрату важливих даних просто установити джерела безперебійного їх живлення.

Для забезпечення функціонування мережі із захищеними каналами передачі даних усе програмне забезпечення, що буде встановлено у даному сегменті цієї багато сервісної мережі включає у себе наступне забезпечення. Це операційна система WINDOWS на кожному із комп'ютерів, MICROSOFT OFFICE на кожному із комп'ютерів мережі, програмне забезпечення для виготовлення та перегляду презентацій, мережева версія системи для бухгалтерського обліку тощо. Для ідентифікації користувачів у багато сервісній мережі використовується та відбувається на рівні їх паролів. Права для доступу до тієї чи іншої важливої інформації надаються у залежності від профілю користувача. Весь повний доступ до важливих даних мають лише головний бухгалтер та директор. У мережі в якості пристроїв для множення оберемо для бухгалтера та секретаря звичайні пристрої із мінімальним об'ємом пам'яті. Цього вже буде досить для того, щоб розмножити звичайні текстові їх документи та невеликі графіки.

Далі розглянемо та переходимо до іншого сегменту нашої багато сервісної мережі , що охоплює різні комп'ютерні приміщення. Тут кількість користувачів мережі становить десь 11-12 чоловік на це приміщення. Основне призначення для даного сегменту комп'ютерної мережі - це швидкісна передача та доставка даних, де важливим фактором є швидкість їх передачі для цих даних. По скільки у даних приміщеннях практично немає інформації де втрата б була критичною, вимоги до захищеності, стабільності та надійності багато сервісної мережі значно менші ніж у попередньому сегменті. Швидкість доступу у повній мірі є вже задовільною у даному випадку та становить близько 100Mbit. Тут найбільш простим та недорогим рішенням для безпеки є встановлення більш швидкісної мережі. Така мережа

використовує доступ CSMA/CD, а це множинний доступ до середовища із контролем несучої та виявленням колізій. Коли їх інтерфейс повинен відіслати нове повідомлення, мережна станція чекає поки у каналах передачі не настане повна тиша. Лише потім вона відсилає необхідний пакет та одночасно прослуховує цей канал на випадок чи не послав ще хто-небудь своє повідомлення одночасно із нею. Якщо ж це трапилось, то обидва ці пакети не доходять до адресатів. Якщо колізій не має то система повинна передавати потік даних далі. При цьому вона все рівно чекає ще декілька мікросекунд перед тим, як знову зробить спробу передати та послати нову порцію даних. Це все зроблено для того, щоб станції також могли просто працювати та ніхто не зміг би монопольно заволодіти усім каналом передачі. У випадку ж появи колізії обидва ці пристрої будуть мовчати невеликий проміжок часу який з генерований випадковим чином, а потім будуть роблять нові спроби для передачі даних багато сервісної мережею . Формально цю технологію іменують як IEE802.3 u, 100Base T, а це є розширенням попереднього стандарту із малою пропускною здатністю.

Загалом є три різновидності цієї технології – це 100BaseTX, що використовує звиту пару у якості її передаючого середовища 5,6,7-ої категорії та використовуються в основному 2-і із 4-ох пар. Друга технологія 100BaseT4 – використовує звиту пару 5,6,7-ої категорій всі 4-и із 4-ох пар дротів. А технологія 100BaseFX у якості передаючого свого середовища використовує оптичне волокно. Найбільш прийнятним рішенням при побудові програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних є технологія 100BaseTX, по скільки він забезпечує повно дуплексний режим для прийому при роботі із її мережевими серверами, а також тут використовує всього 2-і із 4-ох пар восьмижильного її кабелю. Для встановлення багато сервісної мережі необхідно придбати нових 11-12-ть адаптерів, що підтримують цей стандарт, бажано із здатністю вже автоматично без додаткової конфігурації переходити на різні при необхідності. Тут вже за допомогою кабелів звитої пари усі станції мережі необхідно з’єднати до їх центрального пристрою, а це комутатор. При вмиканні ж серверу чи робочої станції із цими адаптерами, останній видасть сигнал, що буде сповіщати про те, що він вже може забезпечити пропускну його здатність. Якщо ж

станція яка приймає сигнал уже також розрахована на роботу, вона у відповідь видасть сигнал, по якому цей комутатор та ця робоча станція чи сервер автоматично переходять у необхідний режим. В рамках даного сегменту мережі слід виділити один файловий сервер для збереження усіх діагностичних програм та драйвери для пристроїв мережі. Щоб запобігти втраті важливої інформації у мережі під час збоїв у її енергопостачанні, встановимо ще на сервер пристрій для безперебійного живлення, а на усі робочі станції поставимо мережеві фільтри-продовжувачі.

Для забезпечення функціонування мережі із захищеними каналами передачі даних у наступний сегмент багато сервісної мережі входять відділ супроводження та захисту. Цей сегмент є найбільшим у даній мережі – тут кількість робочих станцій досить велика. У якості їх мережевої технології оберемо як і у попередньому випадку, по скільки тут головною вимогою до такої мережі є швидкість її передачі та безпечного доступу. Для реалізації багато сервісної мережі знадобляться такі ж мережеві адаптерів та комутатори хоча б на 16 портів у кожному. Усі робочі станції мережі з'єднаємо до їх комутаторів, а самі комутатори об'єднаємо між собою через порти їх розширення. Є також необхідність у створенні файлового серверу самої мережі. У якості операційних систем на усі робочі станції встановимо систему WINDOWS, а на його сервер – WINDOWS SERVER. У даному сегменті для багато сервісної мережі для захисту даних необхідно обмежити певним її групам користувачів доступ до даних на догму файл сервері. Тому тут створимо 3 групи для користувачів на сервері – це є розробники, групи супроводження та прості користувачі. Перебої у їх енергопостачанні під час розробки та передачі програм можуть нанести значної їм шкоди та сповільнити самі темпи розробки, по скільки при активних збоях сам комп'ютер просто перезавантажується, а якщо користувач чи програміст не зберіг дані на диску то потрібно усе робити заново. Тому на цей сервер багато сервісної мережі та на кожну робочу станцію у даному її сегменті встановимо пристрої для безперебійного живлення.

Таким чином у нашій багато сервісній мережі маємо три незалежних сегмента її мережі. Проте тут буде виникати потреба у передачі захищених даних із одного сегменту у інший сегмент. Для сполучення використаємо відому технологію на звитій парі. Вона заснована на стандарті IEEE802.3u та передає захищені дані із

швидкістю більше 100Мбіт/с. У нашій мережі усі пристрої перевіряють на наявність сигналу у їх мережному каналі. Для того, щоб забезпечити певні захищені права для доступу різним групам їх користувачів, встановимо на робочих станціях ОС WINDOWS та створимо різні групи для користувачів. Керівники, а це директор, бухгалтер мають повний доступ до мережевої версії усієї системи бухгалтерського її обліку. Вимоги до повного захисту даних багато сервісної мережі визначають тип та комплекс різних засобів для їх адміністративного керування такою мережею.

При побудові мережі основними напрямками її адміністративної політики для мережі є питання своєчасного резервного копіювання потоків даних та їх технічного обслуговування, контроль за їх програмним забезпеченням, перевірка їх ліцензій, модернізація існуючих програмних засобів, правила для поведінки у непередбачуваних ситуаціях, основні міри для забезпечення безпеки, створення та видалення різних користувачів, надання користувачам прав для доступу до важливої інформації тощо. Виконання всіх цих вищезгаданих заходів тут покладемо на окрему людину, а це системний адміністратора цієї мережі. У системі маємо три сегмента нашої мережі, то також виділяємо робоче місце для його системного адміністратору. В першому сегменті мережі системний адміністратор керує нею і у яку входять лише ті робочі станції де окрім нього є важливі користувачі. Проте на нього покладається велика відповідальність за збереження усієї інформації, по скільки її втрата є критичною. У якості ж операційної системи на усіх робочих станціях багато сервісної мережі обрали класичну. При завантаженні самим комп'ютером операційної системи, останній автоматично вже з'єднується до нашої мережі.

При проектування програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних першим рівнем для захисту від несанкціонованого втручання у дану мережу буде встановлення паролів на рівні їх системи BIOS. На кожну їх робочу станцію сам системний адміністратор мережі також встановлює пароль та повідомляє його працівнику за даним робочим місцем. Також один раз у місяць цей системний адміністратор змінює усі паролі в мережі. Формат таких паролів визначає сам адміністратор мережі, проте вони повинні складатися як з символів так і із цифр та мати не менше 6-и символів. На

усіх робочих станціях, окрім станції головного бухгалтеру встановлено програми-клієнти для бухгалтерського та складського обліку. Вони на своїх комп'ютерах не зберігають нічого як і на своїх дисках, а отримують її через мережу із робочої станції головного бухгалтеру. Програми - клієнти на усіх робочих станціях мережі однакові, а тому права які слід надати тому чи іншому користувачеві визначає сам програмний сервер, що ідентифікує користувачів за допомогою їх паролю у мережі. Кожний такий користувач має свій власний персональний пароль. Адміністрування ж у програмному -сервері проводить сам адміністратор мережі. Програмний сервер дозволяє створювати різні файли для користувачів та надавати їм їх права. Директор та головний бухгалтер мають усі повні права, всі інші користувачі – лише до тієї частини потоків інформації, із якою вони працюють. По скільки важливі дані становлять комерційну їх таємницю, то вимоги до формату паролів тут значно вищі – він має бути не менше ніж на 10 символів та змінюватись хоча б один раз у місяць. Самі ж бази потоків даних зберігаються у мережі в зашифрованому вигляді.

Для забезпечення функціонування мережі із захищеними каналами передачі даних у обов'язки адміністратора мережі входить необхідність кожен день у кінці робочого дня робити всю резервну копію даних за допомогою накопичувачів у трьох екземплярах. Одну копію інформації записується раз в місяць, а інші через день почергово. У кінці робочого дня адміністратор мережі перевіряє їх журнал роботи для програми, який ведеться у автономному режимі. Для виявлення та знешкодження нападів та вірусів у мережі на кожний комп'ютер встановлюється різне антивірусне забезпечення, що сканує усі ресурси цих комп'ютерів на предмет наявності у них вірусів, та при можливості їх знешкоджує. Проте це ще не гарантує повної безпеки для мережі та її каналів передачі, так як кожен день з'являються усе нові та нові різновиди вірусів. Тому адміністратор нашої мережі повинен регулярно оновлювати бази даних їх антивірусних програм багато сервісної мережі.

Для реалізації системи захисту у другому сегменті багато сервісної мережі основним робочим місцем для адміністратора мережі є його файл-сервер. Операційною системою обрали класичну. Доступом до потоків інформації на кожній такій робочій станції керує власне її користувач. Вже у цьому сегменті не має дуже важливих даних, втрата яких була б критичною для системи і комерційних

важливих програмних продуктів тут також досить мало. Тут в основному це є комерційні програми для діагностики роботи, тому усі ліцензії на ці програми зберігаються уже в системного адміністратора. Для дублювання ж потоків інформації на файл-сервері встановлено два паралельних диски і тому при виході із ладу одного із них, інформація буде доступна із іншого диску. Для протидії нападам та вірусам, на усі робочі станції буде встановлено антивірусне програмне забезпечення, де за оновленням якого уже буде слідкувати також адміністратор багато сервісної мережі.

Для реалізації захисту у третьому сегменті багато сервісної мережі на системного її адміністратора покладено широкий ряд задач. Тут постає основна задача для захисту каналів передачі для вихідних текстів програм та надання їм доступу до тієї інформації, що потрібна. Для вирішення цієї проблеми захисту встановимо на файл-сервері операційну систему WINDOWS та об'єднаємо усі робочі станції мережі в рамках одного його домену для мережі. Першим рівнем для захисту від несанкціонованого втручання у багато сервісну мережу є паролі на рівні їх BIOS. Користувачі тут вже самі обирають собі їх паролі та повідомляють про це свого адміністратора. Адміністратор оголошує один раз в місяць про зміну їх паролів та перевіряє чи дотримуються вони для цього користувача. Для доступу до важливої інформації сам адміністратор створює три групи, а це розробники, група супроводження та користувачі . Кожна із цих різних груп має свій власний персональний пароль та певний обсяг доступу до даних на файл сервері. Формат самого паролю мережевий адміністратор надає можливість встановити самому користувачеві. Дані на файл-сервері тут також дублюються на додатковий диск мережі.

Адміністратор мережі проводить повний аналіз роботи багато сервісної мережі через свій аналізатор протоколів та монітор для завантаження мережі. По скільки у цьому даному сегменті мережі є прямий вихід в Інтернет то він встановлює програми типу FIREWALL, для заборони передачі по каналах та пересилки пакетів за рамки мережі, а також для блокування потоків інформації із зовні, що може представляти велику небезпеку для системи. У віддаленому ж корпусі встановлена класична операційна система на усіх робочих станціях і на

файл сервері також. По скільки основна кількість працюючих на філіях є невеликою то це дозволяє створити на сервері даної мережі обліковий запис кожного його користувача.

Для системи захисту сегментів комп'ютерної мережі у процесі її реалізації для інформаційної мережі усі електронні пристрої, що виконують різні свої задачі у системі захисту зможуть принести значно більше користі, якщо вони тут будуть частиною однієї системи безпеки у якій, на основі даних від їх одних пристроїв усі інші виконують ті чи інші безпечні дії. Для повного забезпечення подібного рівня інтеграції усі ці пристрої повинні бути підключені до єдиної їх інформаційної мережі, в основу якої складає її кабельна інфраструктура, що ще називають структурованою кабельною системою. Ця кабельна система багато сервісної мережі можна охарактеризувати як вже стандартизовану технологію для побудови єдиної кабельної інфраструктури усієї будівлі для мережі, що забезпечує функціонування каналів передачі та різних систем і додатків, що вони використовують для компонентів, які відповідають певним її стандартам. Фактично кабельна система багато сервісної мережі складається із декількох основних її компонентів. У першу чергу це є магістральна проводка, що зв'язує усі структурні підрозділи нашої мережі і є основною їх інформаційною трасою. Тут відповідно до стандарту довжина цього магістрального сегменту між окремими будівлями не може перевищувати більше 1500м. У ідеальному ж випадку магістраль з'єднує між собою усі різні будівлі у яких існує вертикальна проводка між його поверхами де максимальна довжина не повинна перевищувати 500м. Мережні системи, що мають зв'язок вже більшої довжини, відносяться уже до не стандартних її рішень.

У мережі для з'єднання окремих його пристроїв із магістраллю уже використовується горизонтальна її проводка довжиною не більше ніж 90м. Для самого ж об'єднання усіх цих мережних провідників у єдину багато сервісну мережу на стиках між ними також використовується їх комутаційне та кросове обладнання. При цьому тут кожен елемент кабельної системи мережі повинен мати такі характеристики, що відповідають характеристикам усіх інших його елементів. Вони повинні бути встановленими по усім правилах та стандартах і протестованими у складі для всієї лінії каналів передачі. Розташованими вони мають таким чином,

щоб усі наступні кабельні зміни та доповнення можна було б провести шляхом простої їх пере комутації для провідників на розподільчому чи їх комутаційному шафах. Як і любий проект для мережі, побудова кабельної системи не можлива без її планування. При цьому при побудові варто враховувати, що кабельна система будується не на один рік, а середній строк її служби складає більше 20 років, що співпадає із проміжками для часу між капітальними їх ремонтами для будівлі. Початкові затрати на створення кабельної системи зазвичай складають приблизно 30% від вартості усієї інформаційної багато сервісної мережі, проте ця цифра значно зменшиться, якщо тут врахувати вартість для підтримки на експлуатацію її та можливі втрати, якщо при її основній побудові не врахувати також можливість для модернізації та резервування.

Для реалізації захисту каналів передачі швидкість доступу у першому сегменті багато сервісної мережі не буде дуже перевищувати 100Мбіт будемо використовувати кабель 6-7-ої категорії, так як він тут надає можливість для переходу на більш високошвидкісні його рішення. Для того, щоб ще полегшити доступ до комунікаційного його обладнання, розташуємо ці комунікаційні шафи у коридорах біля виходу зі його сходів. Звичайно най кращим рішенням було б розташувати ці комунікаційні шафи у спеціальних приміщеннях тобто апаратних кімнатах, але для планування приміщень не дозволяє це зробити. Прокладка ж кабелю здійснюється у відповідності із вимогами до прокладки кабелю 6-7-ої категорії тут не дозволяється перевищення певного рівня для натяжки кабелю, а також неправильні радіуси перегинання, наявність їх механічного напруження у прокладеному кабелі, кріпленню та наявність різних механічних пошкоджень. Тому небезпека такого роду для різних помилок полягає у тому, що всі вони не проявляються під час їх тестування багато сервісної мережі, а лише через деякий час її роботи.

Усі загрози та пошкодження можуть усуватись для таких помилок тільки можливе шляхом прокладки уже нового кабелю в мережі. З’єднання ж між поверхами тут відбуваються через отвори у стінах. Для вертикальної ж прокладки використовуються різні труби із різноманітними рівнями їх захищеності від зовнішніх їх впливів. Для самої ж горизонтальної прокладки використовують

спеціальні пластикові короба. У випадку прокладки необхідно заповнювати до 40% їх об'єму для проводу, щоб була можливість передбачити місця для їх подальшого нарощування для мережі чи вже модифікувати існуючу кабельну систему. Тому тут діаметр труби становить вже десь 12-15 см, а висота до 3м, це висота стелі. Для самої ж горизонтальної прокладки уже вистачить коробу шириною та висотою до 5-6 см. При прокладці кабелю у деяких місцях проводка може здійснюватись безпосередньо через саму стіну, а це дає можливість щоб зменшити кабельну довжину мережі. Для такого випадку у стіні висвердлюється отвір десь діаметром до 5 см та у нього вставляється фрагмент труби потрібної їх довжини.

Щоб забезпечити захист передачі даних тут важливо правильно розташувати так усі робочі станції, щоб відстані між ними вже не були меншими за допустимі, а сама довжина усієї багато сервісної мережі не повинна були більшою за 250м. Проводка ж кабелів та розташування їх комутаційних пристроїв та обчислювальних засобів зображено на схемі розміщення пристроїв мережі. Довжина першого сегменту у мережі становить десь 60м, довжина другого сегменту десь 70м, довжина третього сегменту до 150м. Саме ж з'єднання сегментів у цій мережі відбувається по технології 802.3 із шинною топологією. Загальна довжина кабелю до робочих станцій 30м. Довжина самої мережі у віддаленому її корпусі для мережі становить 120м. Мінімальна ж відстань між робочими станціями десь 1,2м, що задовольняє вимогам. На кабельну систему дається гарантія не менш ніж 20 років, що означає для усі елементи системи передачі не мають різних виробничих дефектів та виконані у відповідності до стандартів і уже можуть відслужити строк без погіршення їх експлуатаційних характеристик для багато сервісної мережі.

Для побудови захищеної багато сервісної мережі використаємо 5-ть комутаторів для з'єднання між комп'ютерів. Два із них будуть розбиті на декілька її під мереж та для них будуть створенні віртуальні мережі, що будуть прив'язані до портів цього комутатору, а далі уже будуть створені також інтерфейси яким будуть присвоєнні їх IP адреси. До одного із цих комутаторів з'єднаний також маршрутизатор, що організує зв'язок по комп'ютерній мережі із п'ятим його комутатором. Тут зв'язок буде відбуватись через його проміжну мережу за допомогою тунелю для мережі. Для цього уже потрібно два маршрутизатори, де

один із яких буде виконувати тут роль серверу та клієнту. У ролі такого маршрутизатору використовуються два комп'ютери, на яких встановлена операційна система Free-BSD. Для усіх інших налаштувань тут використовують програму VTUN, яка дозволяє вже зручно зробити усе необхідне для коректної роботи цих віртуальних мереж. При запуску програми на комп'ютері клієнті буде використаний також ключ для пере підключення при розриві, що забезпечить тут стабільний зв'язок у мережі. На маршрутизаторах будуть встановлені по уже по дві мережеві плати, одна із яких буде мати вихід на її зовнішню, а друга на внутрішню її мережу.

3.2 Програмне налаштування для реалізації забезпечення функціонування мережі

Для проектування та програмного налаштування програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних створимо віртуальні мережі на базі комутаторів багато сервісної мережі. На двох цих комутаторах має бути по дві мережі, тому тут створюємо віртуальні мережі та їх інтерфейсах для цих комутаторах та прив'язуємо їх до портів самого комутатору.

Комутатор 195.120.010.002

create VLAN vlIp2 tag2

config VLAN default delete 1- 12

config VLAN vlIp2 add untagged 1-12

create IP if Sys Ip2 172.20.0.1/16 vlIp2 state enable

show VLAN

show IPif

Комутатор 195.120.010.004

create VLAN vlIp4 tag 2

config VLAN default delete 1-12

config VLAN vlIp4 add untagged 1-12

create ip if Sys Ip4 145.089.0.001/16 vlIp4 state enable

show VLAN

show IPif

Для самої багато сервісної мережі проведемо резервування їх зв’язку за допомогою протоколу його покриваючого дерева. Найбільш тут небезпечною проблемою є генерація для декількох зациклених її шляхів у об'єднаній мережі. Зациклення для одного шляху породжує також зациклення по інших шляхах у мережі, а уже шторм широкомовних його повідомлень посилюватиметься уже до такої міри, що станеться повна зупинка у роботі багато сервісної мережі. Уникнути цих проблем із зацикленням тут допомагає протокол чи алгоритм для покриваючого дерева. Сам цей протокол для покриваючого дерева STP був розроблений компанією, яка пізніше була придбана та увійшла до складу іншої компанії. Інститут IEEE створив свою власну версію для протоколу STP яку він назвав IEEE802.1d. Усі комутатори зараз працюють по протоколу IEEE802.1d для алгоритму STP, який вже не сумісний із вихідною версією компанії. Основне ж завдання для протоколу STP полягає у виключенні проблеми зациклення у мережах на 2-гому рівні. Протокол же STP передбачає постійний моніторинг для багато сервісної мережі для знаходження усіх зв'язків та усунення зациклення за рахунок швидкого відключення її надлишкових зв'язків.

Сам же протокол STP дозволяє знайти усі зв'язки у мережі та виділити серед них усі надлишкові, щоб відключити всі ці надлишкові зв'язки та тим самим усунути будь-які зациклення у цій мережі. Для цього уже робиться вибір для кореневого мосту, який стежитиме за усією мережною топологією. У сучасній будь-якій мережі може бути лише один кореневий міст і тому порти такого мосту називаються призначеними, по скільки вони працюють в режимі стану їх пересилки. Порти пересилки стану приймають та відправляють потік даних багато сервісної мережі. Інші ж перемикачі у такій мережі називаються некореневими її мостами. Призначеними також називаються її порти, що ведуть до самого кореневого мосту та мають уже най меншу її вартість. Усі інші порти цього мосту є не призначеними та вже не здатні приймати та відправляти потік даних мережі і тому цей режим називається блокуванням.

При проектування програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних усі виконуючі протокол STP перемикачі та мости уже обмінюються інформацією про самі елементи даних протоколу для моста та передають повідомлення про їх конфігурацію у кадрах широкомовних їх розсилок. За їх допомогою останнім пристроям пересилається уже ідентифікатор для кожного мосту. Цей ідентифікатор мосту служить для виявлення у багато сервісній мережі кореневого мосту та призначених її кореневих портів. Сам ідентифікатор має довжину у 8 байтів та містить відомості про його пріоритет та MAC - адресу цього пристрою. Якщо ж уже два перемикачі чи мости мають однакове їх значення по пріоритету, то MAC - адреса служить для виявлення уже пристрою із найменшим її ідентифікатором. Для багато сервісної мережі було обрано варіант, де її кореневим буде комутатор 195.120.10. 002 і таким чином усі його порти будуть назначеними. У комутатору буде ID = 4096. Блокована ж резервна лінія буде між комутаторами у яких їх ID = 128 та ID = 164. Тут блокується порт, який знаходиться на комутаторі із його ID = 128, адже вартість доступу на його порту буде набагато більша за вартість на порту комутатора із ID = 164. Приведемо далі команди якими будуть настроюватися ці комутатори багато сервісної мережі.

Для виконання настройки підключаємося до комутаторів багато сервісної мережі через TELNET. Додаток Б.

Таблиці для маршрутизації багато сервісної мережі будуються для можливості коректного звертання робочих станцій до різних під мереж. Вказується правила, які указують куди пересилати пакет, якщо ж він направлений до конкретної під мережі. У даній багато сервісної мережі таблиці маршрутизації створюються автоматично за допомогою протоколу покриваючого дерева STP.

При проектуванні програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних було створено мережі VPN. Безпека для передавання пакетів через таку загальнодоступну мережу може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал для обміну інформацією. VPN також дозволяє об'єднати декілька географічно віддалених мереж для багато сервісної мережі у

єдину мережу із використанням для каналів зв'язку та передачі між ними непідконтрольних їм каналів.

У програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних використовуються для випадків, коли передавальне середовище можна уже вважати надійним та необхідно вирішити лише завдання для створення віртуальної її під мережі у рамках більшої їх мережі. У нашому ж випадку віртуальна приватна мережа буде проходити через проміжну мережу класу А із її адресою 67.0.0.0., табл..3.1.

Таблиця 3.1 – Внутрішні інтерфейси мережі

Ім'я машини	Внутрішня під мережа	Внутрішній інтерфейс		Зовнішній інтерфейс		Віртуальний інтерфейс
Router1	172.200.0.0	172.200.0.036	Re0	67.010.0.244	Rl0	10.0.0.001
Router2	196.50.200.0	196.50.200.013	Re0	67.98.01.015	Rl0	10.0.0.002

Сам конфігураційний файл мережі /usr/local/etc/vtund.conf серверу у мережі, Додаток В. У системі настроювання роботи –s тут означає запуск серверу багато сервісної мережі, а параметр -p можливість виконати пере підключення до серверу після його розриву каналу передачі та зв'язку, параметр var4 – ім'я мітки у конфігураційному файлі серверу, 067.010.0.244 – це адреса його серверу до якого підключається сам клієнт. Обмеження для проходження потоку даних по портах у комп'ютерній багато сервісній мережі. Комутатори ж для обмеження проходження потоку даних дозволяють уже створювати профілі для доступу, що вказують йому якого йому вигляду пакети набирати, а які уже відкидати. За допомогою уже сформованих списків для управління доступом профіль для управління доступом дає уже тут можливість переглядати певні пакети даних, які вказані у списках його ACL. Процес настроювання ділитися на дві такі частини:

1. Це створення маски для профілю доступу де вказується, яку частину чи частини кадру буде перевіряти комутатор, наприклад IP – адресу його призначення чи IP - адресу призначення та IP адресу джерел.

2. Це створення правил для профілю доступу. Тут уводиться умова, яку сам комутатор використовуватиме для визначення цієї дії над цим кадром.

Ці правила прописуються на самому комутаторі, до якого приєднаний заданий комп'ютер багато сервісної мережі. У нашому випадку адрес робочої станції – 172.020.0.050, тому адреса комутатора 172.020.0.001. Створюємо одну маску для профілю, а далі задаємо уже два правила для його доступу.

create access_pro file ip destination_IP_mask 255.255.255.255 source_IP_mask 0.0.0.0 TCP dst port_mask 0xFFFF src_port_mask 0 x 0 deny profile_id1

config access_profile pro file_id1 add access_id1 IP destination_ip 172.020.0.031 source_ip 172.20.0.1 tcp dst_port 23 та 27

3.3 Програмні засоби для вимірювання передачі даних з часом для захищених каналів комп'ютерної мережі

Як інструмент для організації сервісу для моніторингу та вимірювання даних з часом для програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних використаємо програму MRTG. Дані від різних джерел системи передачі збираються, а потім уже відображаються у вигляді різних графіків. Налаштування та установка пакету програм MRTG для багато сервісної мережі проводиться у наступній її послідовності.

Створюємо наступну її директорію для компіляції

mkdir/ usr/ local/ src

cd /usr/ local/ src

Установлюємо бібліотеку ZLIB, що знаходиться за адресою ftp:// sunsite.cnlab - switch.ch/ mirror/info zip/ zlib/zlib.tar.gz

Gun ZIP - d zlib.tar.gz

tar xf z lib.tar

mv zlib -?.?.?./ z lib

cd zlib

/configure

make

cd …

У подальшому встановимо бібліотеку LIB PNG, що знаходиться за адресою http:// www. libpng.org/pub/ png/src/libpng-001.0.011.tar.gz

```
Gun zip -d lib png-*.tar.gz
tar xf  lib png -*.tar
rm lib png -*.tar.gz
mv lib png -* lib png
cd lib png
make - f scripts/makefile.std C C=gcc Z LIB LIB=../zlib Z LIBINC=../ zlib
rm *.so.*. *.so
cd …
```

Також далі уже встановимо бібліотеку gd (http // www .boutell.com/gd/http/gd-1.8.3.tar.gz)

```
gun zip - d gd- 1.8.3.tar.gz
tar xf  gd - 1.8.3.tar
mv gd-  1.8.3 gd
cd …
```

Далі для моніторингу та вимірювання даних усі ці бібліотеки нам потрібні для роботи із графіками у форматі png. У подальшому компілюємо пакет MRTG для багато сервісної мережі.

```
cd /usr /local/src
gun zip - d mrtg - 2.9.17.tar.gz
tar xv f mrtg - 2.9. 17.tar
cd mr tg - 2.9.17
/configure –prefix = /usr/local/mrtg - 2 \
        make
make install
```

Далі для моніторингу та вимірювання даних створюємо також конфігураційний файл для отримання потоку даних у захищених каналах передачі маршрутизатору багато сервісної мережі, який входить та виходить по адресі 192.168.10.010 із використанням протоколу SNMP.

Файл по моніторингу та вимірювання даних для багато сервісної мережі записуємо у каталог /usr/ home/ denys/ public_html/ mrtg/cfg під ім'ям mrtg.cfg

3.4 Висновок

У цьому розділі при виконанні кваліфікаційної роботи по проектуванню програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних було проведено програмно-апаратна реалізація для технічних засобів по функціонуванню каналів передачі даних. Також була проведена реалізація системи захисту для сегментів комп'ютерної мережі яка дала можливість сформувати сегменти мережі. Для забезпеченні функціонування захищених каналів передачі було проведено програмне налаштування для цієї реалізації по забезпеченню функціонування такої мережі . Для вимірювання передачі потоку даних з часом для захищених каналів комп'ютерної мережі були використані відповідні програмні засоби.

ВИСНОВКИ

При виконанні кваліфікаційної роботи програмно-технічні засоби забезпечення функціонування мережі із захищеними каналами передачі даних, була розроблена комп'ютерна багато сервісна мережа. У процесі виконання роботи було проведено дослідження предметної області по захисту передачі даних та огляд існуючих засобів, методів і технологій по даному напряму. Також у процесі дослідження проведено аналіз основ функціонування каналів передачі та побудови доступних систем захисту таких мереж. Проектування комп'ютерної мережі передбачало особливості побудови транспортної системи для передачі захищеної інформації у каналах її комунікації. У процесі проектування розглянуто Особливості застосування систем захисту при побудові системи передачі даних обґрунтування та аналіз роботи їх програмних засобів та можливості для вирішення проблеми для захисту її системи передачі потоків даних. Сам процес побудови

програмно-технічних засобів забезпечення функціонування комп'ютерної мережі із захищеними каналами передачі даних передбачає планування , проектування та розробку системи захисту каналів передачі потоків даних та інформації і для його реалізації було вибрано транспортні траси із врахуванням із процесом мінімізації обсягу робіт для планування та із врахуванням можливості застосування різних доступних механізмів при його проектуванні, а також із врахуванням існуючих джерел по побудові комп'ютерних мереж. У процесі проектування розглянуто засоби та вимоги до пристроїв у комп'ютерній мережі із захищеними каналами передачі даних і на основі цих досліджень вибрані необхідні засоби для побудови мережі. Проведено розрахунок для параметрів підключення пристроїв до самих каналів системи передачі та проведено вибір програмного забезпечення. Було проведено також проектування етапів планування самої комп'ютерної мережі із каналами передачі потоків даних для програмно-апаратної реалізація технічних засобів при функціонуванні каналів передачі даних. Для мережі проведена реалізація системи захисту для сегментів комп'ютерної мережі та вибрано програмне налаштування для реалізації забезпечення функціонування мережі. При реалізації системи були вибрані програмні засоби для вимірювання передачі даних з часом для захищених каналів нашої комп'ютерної мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Стеклов В. К. Інформаційна система: підручник студентам вищих навчальних закладів по напрямку «Телекомунікації» / В.К. Стєклов, Л.Б. Беркман // – К.: Техніка, 2014. 792 с.
2. Романец, Ю.В. Защита информации в компьютерных системах и сетях /Ю.В.Романец, П.А.Тимофеев, В.Ф.Шаньгин // - К. : Зв'язок, 2019. 328 с.
3. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко // – К. : Телеком, 2019. 452 с.
4. Воргуль О. В. Проблеми безпеки при використанні віртуальних приватних мереж / О. В. Воргуль, О. Г. Білоцерківець, А. О. Серіков // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Все- української науково-практичної

конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. ЛДУ БЖ, 2020. С. 29–30.

5. Ерохин, В.В. Безопасность информационных систем /В.В.Ерохин, Д.А.Погонышева, И.Г.Степченко // – К. : Флинт - Наука, 2015. 182 с.

6. Завгородний, В.И. Комплексная защита информации в компьютерных системах: учебное пособие для вузов/ В.И. Завгородний. – К. : Логос, 2011. 264 с.

7. Бузов Г. А. Защита от утечки информации по техническим каналам: Учебное пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев // – К.: Телеком, 2015. 416 с.

8. Галицкий А.В. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д . Рябко, В.Ф. Шаньгин // - К.: Пресс, 2014. 616 с.

9. Безрук В. М. Інформаційні мережі зв'язку. Ч. 2. Телекомунікаційні технології стаціонарних мереж зв'язку : навч. посібник / Безрук В. М., Бідний Ю. М., Колтун Ю. М., Астраханцев А. А., Свид І. В., Ширяєв А. В., Харченко Н.А// – Харків: ХНУРЕ, 2011. 492 с.

10. Стасєв Ю.Б. Комп'ютерні мережі. Технології та протоколи для моделювання: навчал. посіб. / І.В. Рубан, С.В. Дуденко, О.І. Тимочко // – Х.: ХУПС, 2014. 359 с.

11. Казимир В. В. Інформаційні основи побудови їх телекомунікаційних мереж / В. В. Казимир, В.А. Литвинов, С.М. Шкарлет, С.В. Зайцев // Вісник Чернігівського держав. техн. універ. - Чернігів : ЧДТУ, 2013. 340 с.

12. Исаченко О. В. Введение в информационные технологи / О. В. Исаченко // - К.: Фенікс, 2019. 240 с.

13. Карабутов Н. К. Адаптивная идентификация систем. Информационный синтез / Н. К. Карабутов // -К.: КомерКнига, 2016. 384 с.

14. Бабич В.Д. Завадостійкість для каналів зв'язку : навч. посіб. / В.Д. Бабич, О.Д. Кувшинов, О.П. Лежнюк, С. Лівенцев // - К.: КВІУЗ, 2021. 150 с.

15. Кривуца В.Г. Управління телекомунікаціями з застосуванням новітніх технологій / В.Кривуца, В.К.Стеклов, Л.Н.Беркман, Б.Костік, В.Олійник, С.Скляренко // Підручник для ВНЗ. – К.: Техніка, 2007. 384 с.

16. Горбатий, І. В. Телекомунікаційні системи і мережі. Принципи функціонування, технології і протоколи : навч. посібник / І.В. Горбатий, А.В. Бондарєв // – Львів : Видав. Львівської політехніки, 2016. 336 с.

17. Стасєв Ю.В. Комп'ютерні мережі: Технології, протоколи та їх моделювання: навчал. посібн. / І.В. Рубан, С.В. Дуденко, Д.В. Сумцов, О.І. Тимочко // – Х.: ХУПС, 2014. 35 9 с.

18. Климаш М.М. Сучасні перетворення в архітектурах розподілених їх систем: монографія / М.М. Климаш, А. Лунтовський, В. Романчук // – Львів-Дрогобич: Коло, 2015. 328 с.

19. Горбатий, І. В. Телекомунікаційні системи і мережі. Принципи функціонування, технології і протоколи : навч. посібник / І.В. Горбатий, А.В. Бондарєв // – Львів : Видав. Львівської політехніки, 2016. 336 с.

20. Советов, Б. Я. Моделирование систем: учебник для бакалавров / Б. Я. Советов, С. А Яковлев // — 7-е издан. — К. : Издат. Юрайтс, 2015. 343 с.

21. Лунтовський А. О. Етапи розвитку сучасних інфо-телекомунікаційних сервісів та енергетична ефективність мережевих технологій / А.О. Лунтовський, П. Гуськов, А. Масюк // *Вісник Націон. Універ. «Львівська політехніка». Серія: Радіоелектроніка та телекомунікації*. — Львів: Вид. Львів. політ., 20 14. - № 796. С. 131-139.

22. Кирик М.І. Багаторівнева модель для буферу даних в вузлах обслуговування мультисервісного потоку навантаження / М.І. Кирик, Н. К.Плесканка, Ю.В. Климаш *// Фізико – техноогла. проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано - та мікроелектроніки*: матеріал. I V Міжнародн. науково-практичних конференцій (23-25 жовтня 2014 р. м. Чернівці), 2014. С. 110-111.

23. Романчук В.І. Дослідження методів для оцінювання якості сприйняття їх послуг для різних типів телекомунікаційних мереж / В.І. Романчук, М. Климаш, Б. Янишин *// Радіоелектроніка і телекомунікації [зб. пр.] / ред. Б.А. Мандзій*. – Л. : Вид-тво Нац. ун-т "Львів. Політех.", 2012. - № 73. С. 165-172.

24. Арсенюк І.Р. Комп'ютерні мережі: навчальний посібник / І. Арсенюк, А.А. Яровий // – Вінниця: ВНТУ, 2020 . 145 с.

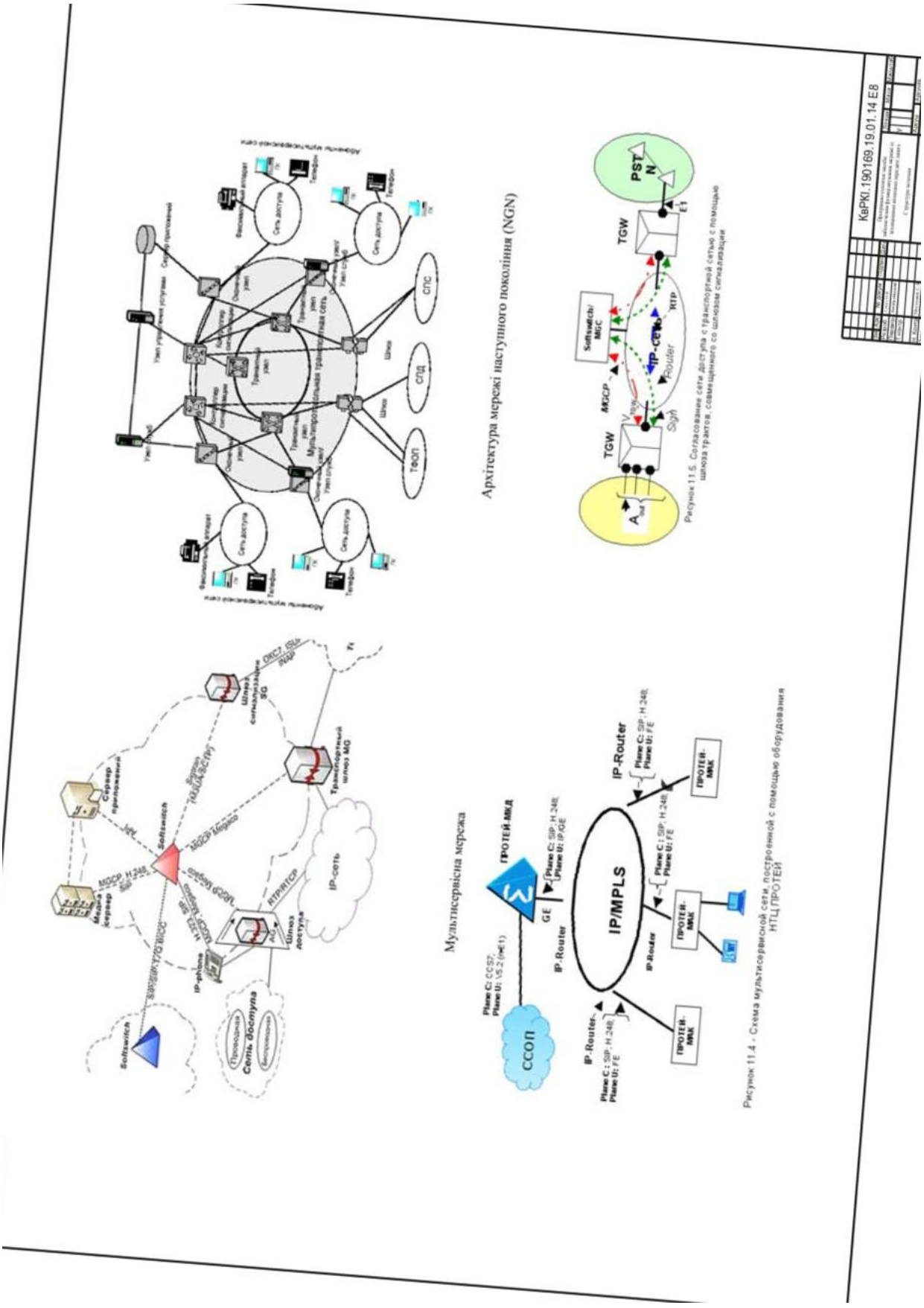
25. Лунтовський А. О. Етапи розвитку сучасних інфо-телекомунікаційних сервісів та енергетична ефективність мережевих технологій / А.О. Лунтовський, П. Гуськов, А. Масюк // *Вісник Націон. Універ. «Львівська політехніка». Серія:*

Радіоелектроніка та телекомунікації. — Львів: Вид. Львів. політ., 20 14. - № 796. С. 131-139.

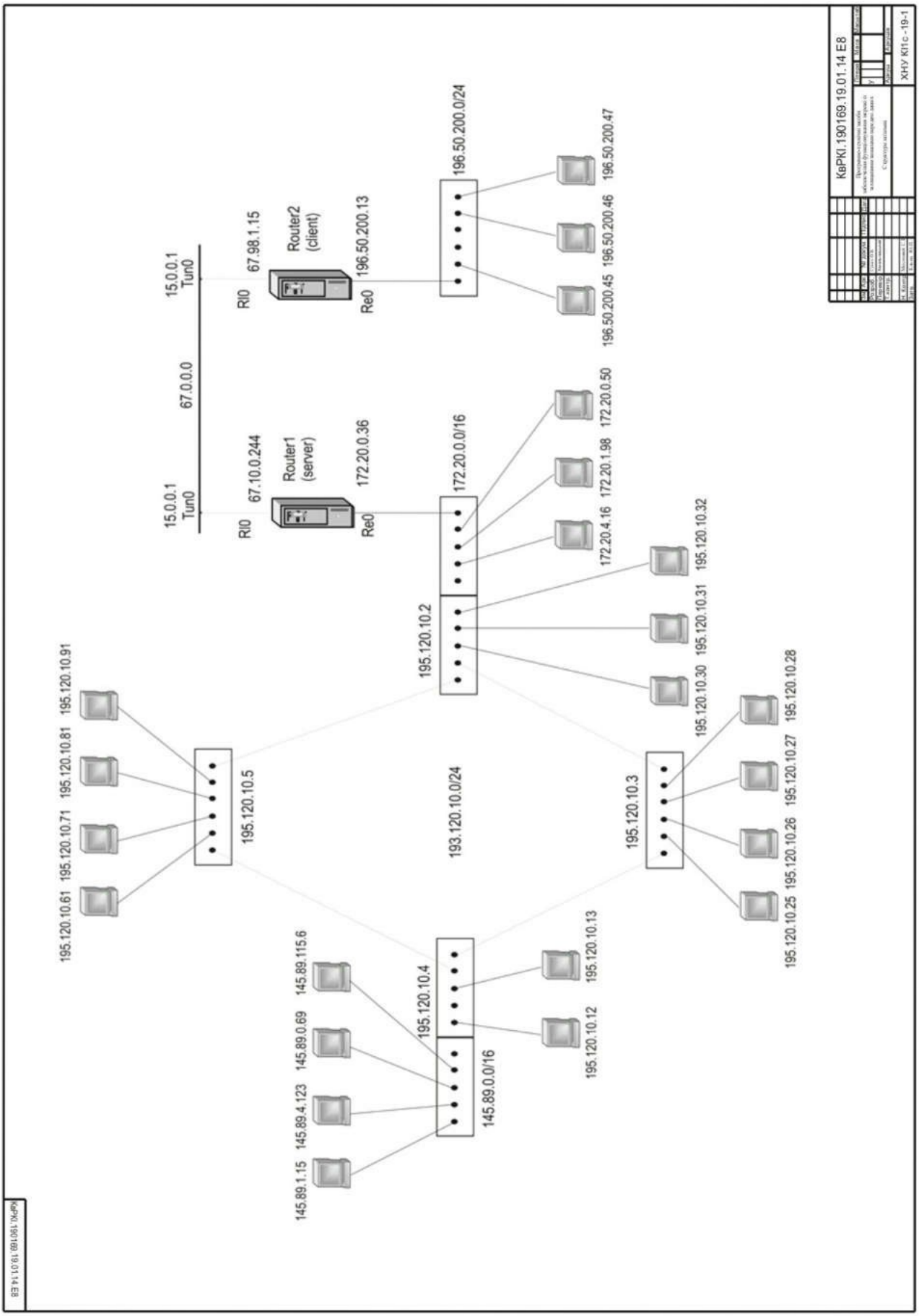
ДОДАТОК А

(Обов’язковий)

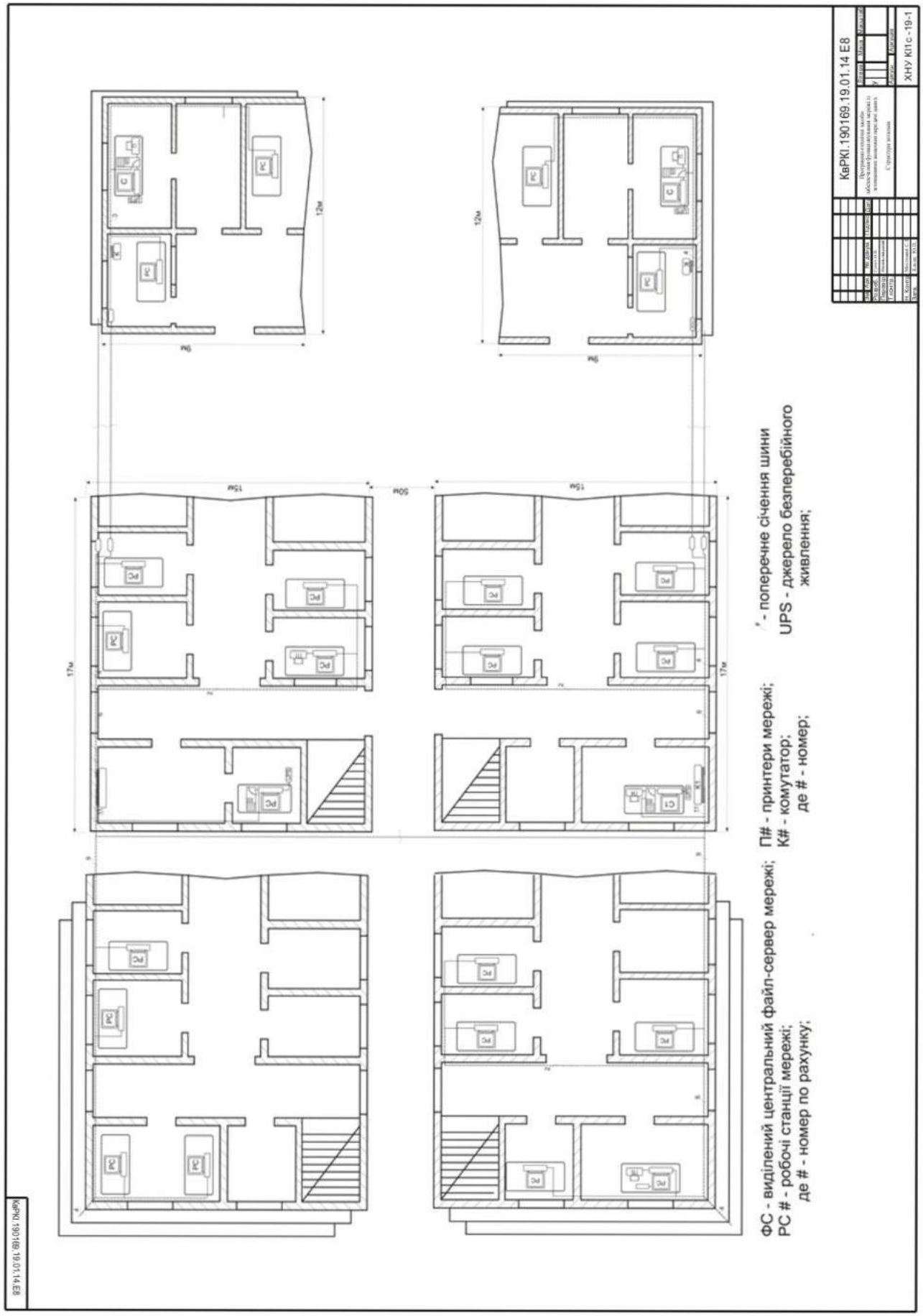
Копія креслення “ Захист мереж у різних технологіях “



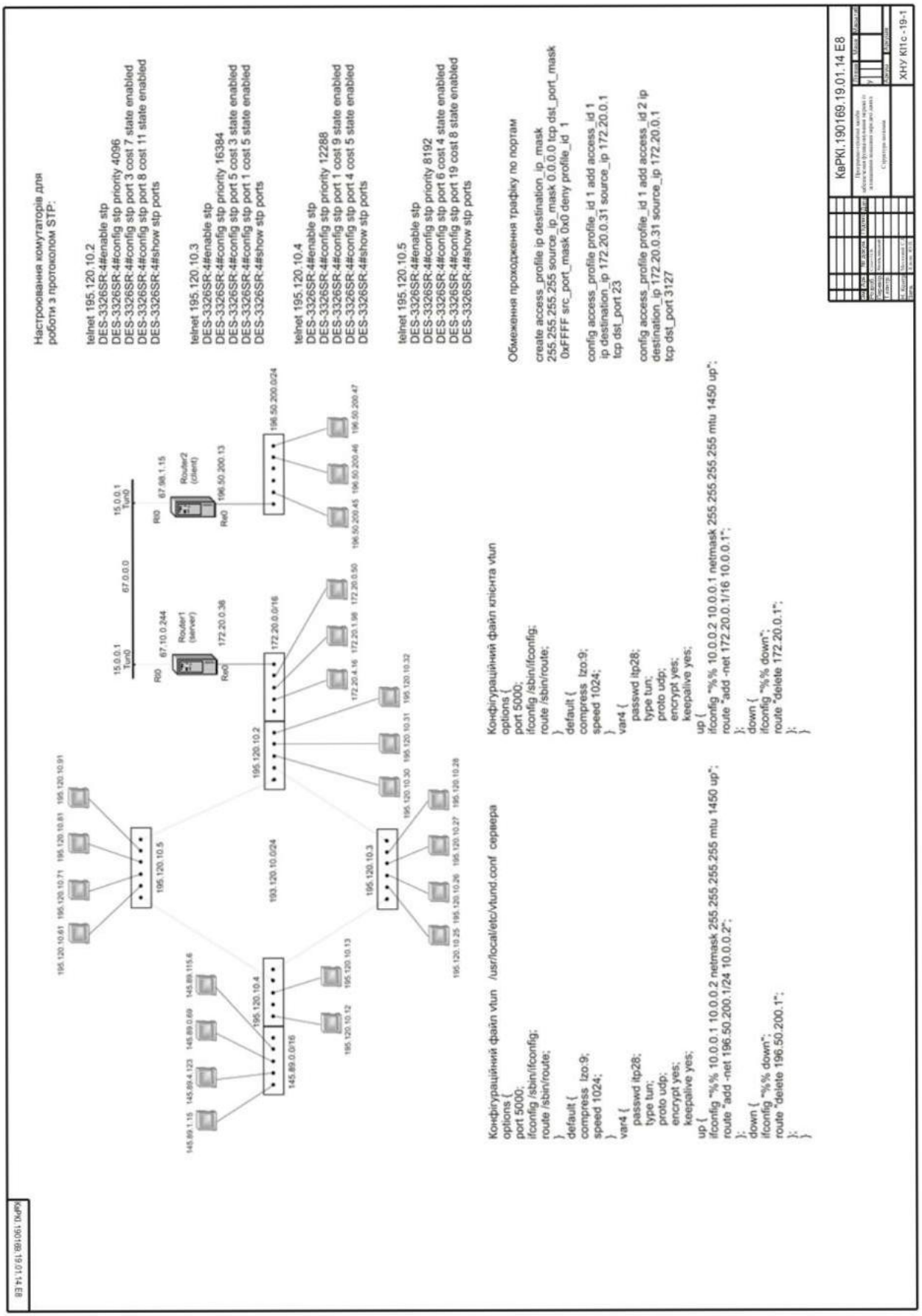
Копія креслення “ Схема мережі загальна“



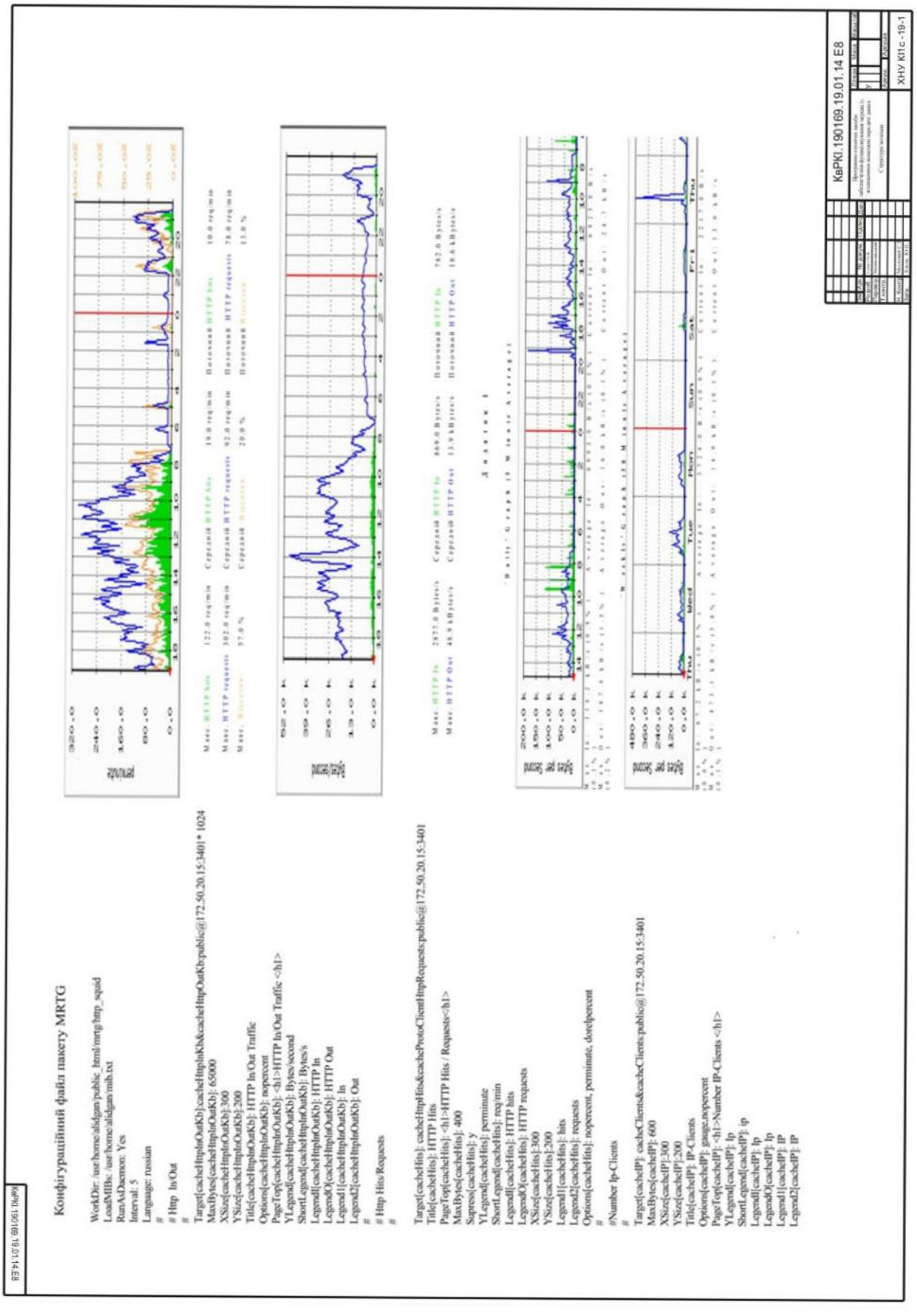
Копія креслення “ Схема розташування комп'ютерів мережі “



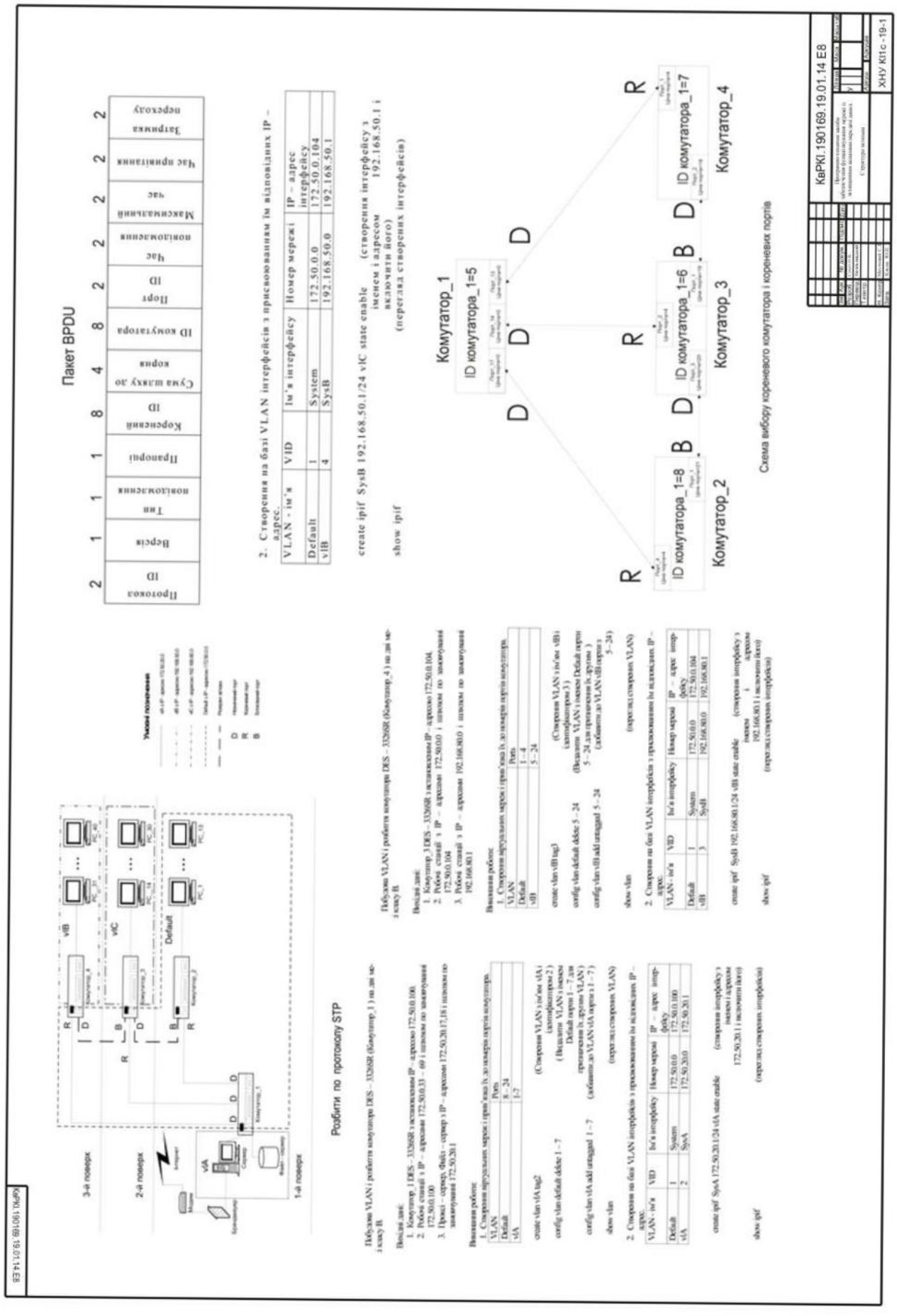
Копія креслення “ Настройка роботи мережі “



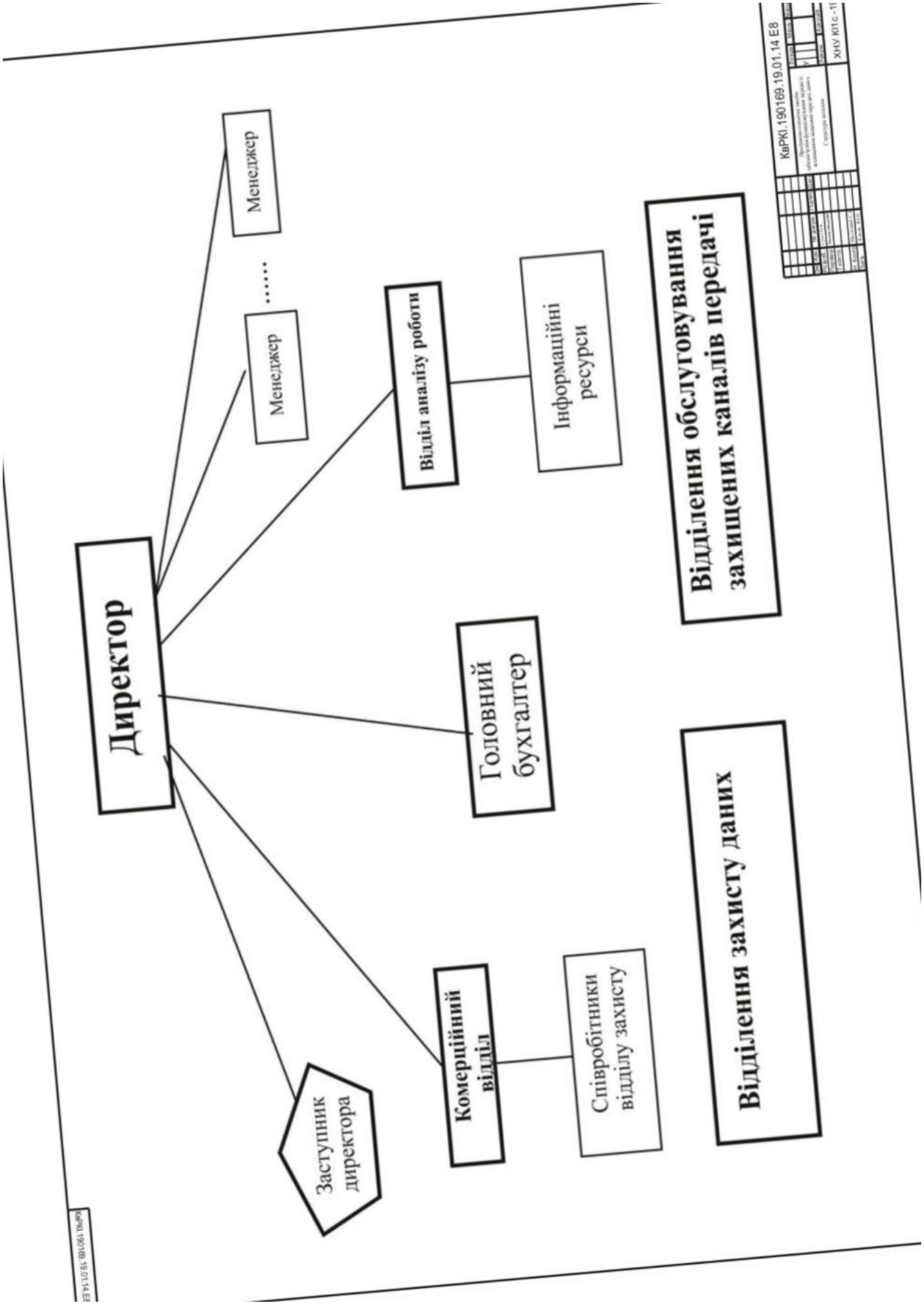
Копія креслення “ Статистика роботи мережі “



Копія креслення “ Схема резервування роботи мережі “



Копія креслення “ Організаційна структура мережі“



ДОДАТОК Б

НАСТРОЙКА РОБОТИ КОМУТАТОРІВ

Комутатор мережі 195.120.010.002

TELNET 195.120.010.002

DES -3326 SR: 4 # enable STP (дозволяємо STP на комутатор)

DES -3326 SR: 4 # config STP priority 4096 (пріоритет комутатор)

DES -3326 SR: 4 # config STP port 3 cost 7 state enabled

(конфігуруємо порт 3 із значенням 7)

DES-3326 SR: 4 # config STP port 8 cost 11 state enabled

(конфігуруємо пот 8 із значенням 11)

DES -3326 SR: 4 # show STP ports (перевіряємо правильність установок для портів)

Комутатор мережі 195.120.010.003

TELNET 195.120.010.003

DES -3326 SR: 4 # enable STP (дозволяємо STP на цьому комутаторі)

DES -3326 SR:4 #config STP priority 16384 (встановлюємо пріоритет для комутатору)

DES -3326 SR:4 # config STP port 5 cost 3 state enabled

(конфігуруємо порт 5 із значенням його 3)

DES -3326 SR: 4 #config STP port 1 cost 5 state enabled

(конфігуруємо порт 1 із значенням 5)

DES -3326 SR: 4 #show STP ports (перевіряємо правильність установок для портів)

Комутатор мережі 195.120.010.004

TELNET 195.120.010.004

DES -3326 SR: 4#enable STP (дозволяємо STP на комутатор)

DES -3326 SR: 4# config STP priority 12288 (пріоритет для комутатору)

DES -3326 SR: 4 #config STP port 1 cost 9 state enabled

(конфігуруємо порт 1 із значенням його 9)

DES – 3326 SR: 4 #config STP port 4 cost 5 state enabled

(конфігуруємо порт 4 із значенням його 5)

DES- 3326 SR: 4 #show STP ports (перевіряємо правильність установок для портів)

Комутатор мережі 195.120.010.005

TELNET 195.120.010.005

DES – 3326 SR: 4#enable STP (дозволяємо STP на комутатор)

DES – 3326 SR: 4#config STP priority 8192 (пріоритет для комутатору)

DES – 3326 SR: 4 #config STP port 6 cost 4 state enabled

(конфігуруємо порт 6 із значенням його 4)

DES -3326 SR: 4 #config STP port 19 cost 8 state enabled

(конфігуруємо порт 19 із значенням його 8)

DES – 3326 SR: 4 #show STP ports (перевіряємо правильність установок для портів)

ДОДАТОК В

НАСТРОЙКА КОНФІГУРАЦІЙНОГО ФАЙЛУ

Конфігураційний файл /usr/local/etc/vtund.conf серверу комп’ютерної мережі

```
options {
port 5000;
if  config /sbin/ ifconfig;
route / sbin/ route;
default
compress  lzo: 9;
speed 1024;
}
var4 {
   passwd ITP 28;
   type tun;
   proto UDP;
   encrypt yes;
   keepalive yes;
up
IF config "%% 10.0.0.01 10.0.0.02 netmask 255.255.255.255 MTU 1450 up";
route "add -net 196.50.200.1/24 10.0.0.02";
down
IF config "%% down";
route "delete 196.50.200.001";
};
```

Конфігураційний файл для клієнта комп’ютерної мережі

```
options {
port 5000;
IF Config /sbin/if config;
route /sbin/ route;
```

```
default
compress  LZO: 9;
speed 1024;
}
Var 4 {
   passwd ITP 28;
   type tun;
   proto UDP;
   encrypt yes;
   keepalive yes;
UP
IF config "%% 10.0.0.2 10.0.0.001 netmask 255.255.255.255 mtu 1450 up";
route "add -net 172.20.0.1/16 10.0.0.01";
down
IF config "%% down";
route "delete 172.20.0.01";
}
```

Запуск демону на сервері для комп'ютерної мережі vtund –s.

На клієнті VTUN d -p var4 067.10.0.244

Такі правила прописуються вже на комутаторі, до якого вже приєднаний заданий комп'ютер нашої комп'ютерної мережі. У випадку адреси робочої станції – 172.020.0.50, тоді тут адреса комутатору буде 172.020.0.01. Створюємо ще одну маску для профілю, а далі вже задаємо два основних правила доступу до мережі.

create access_pro file IP destination_IP_mask 255.255.255.255 source_ip_mask 0.0.0.0 tcp dst_port_mask 0 x FFFF src_port_mask 0 x 0 deny profile_id 1

config access_profile pro file_id 1 add access_id 1 ip destination_ip 172.20.0.31 source_ip 172.20.0.01 TCP dst_port 23

config access_pro file pro file_id 1 add access_id 2 ip destination_ip 172.20.0.31 source_IP 172.20.0.01 TCP dst_port 3127

Також проведемо налаштування та установка пакету програм настройки MRTG для комп'ютерної мережі яке проводиться у наступній послідовності. Спочатку створюємо директорію для компіляції програми

Mk dir/ usr/ local/src

cd /usr/ local/src

Далі встановлюємо бібліотеку ZLIB, що вже знаходиться за адресою ftp:// sunsite.cnlab - switch.ch / mirror/infozip/ zlib/zlib.tar.gz

Gun zip - d zlib.tar.gz

tar xf z lib.tar

mv zlib - ?.?.?./ z lib

cd zlib

/configure

make

cd … .

Також далі встановимо бібліотеку lib PNG, що знаходиться за наступною її адресою http:// www. libpng.org/pub/ png/src/libpng -1.0.011.tar.gz

gun zip -d lib png- *.tar.gz

tar xf lib png- *.tar

rm lib png- *.tar.gz

mv lib png- * lib png

cd lib png.

make -f scripts/makefile.std C C = gcc Z LIB LIB=../zlib ZLIBINC=../ zlib

rm *.so.* *.so

cd … .

А далі ми встановимо бібліотеку gd (http//www.boutell.com/gd/http/gd-1.8.3.tar.gz)

gun zip - d gd- 1.8.3.tar.gz

tar xf gd - 1.8.3.tar

mv gd - 1.8.3 gd

cd gd

```
make IN CLUDE DIR S="-I. -I../zlib -I../lib png" \
    LIB DIR S="-L../z lib -L. -L../lib png" \
    LIB S="-lgd -lpng -lz -lm"
cd … .
```

Також всі ці бібліотеки у програмі потрібні для роботи із графіками у форматі PNG. У подальшому компілюємо пакет MRTG для комп'ютерної мережі.

```
cd /usr /local/src
gun zip - d mrtg- 2.9.17.tar.gz
tar xv f mrtg-2.9. 17.tar
cd mr tg-2.9.17
/configure –prefix = /usr/local /mrtg -2 \
        -with-gd = /usr/local/src/gd \
         -with-z = /usr/local/src/zlib  \
         -with-png = /usr/local/src/lib png
make
make INSTALL
```

Файл для комп'ютерної мережі підприємства записуємо у новий каталог /usr/ home/ denys/ public_html/ mrtg/cfg під ім'ям mrtg.cfg

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент _____Сукач Олександр Володимирович_____
Тема: «Програмно-технічні засоби забезпечення функціонування мережі із захищеними каналами передачі даних»_____
Галузь знань 12 «*Інформаційні технології*» Спеціальність 123_____
«*Комп'ютерна інженерія*» Освітня програма « Комп'ютерна інженерія»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 9 ; кількість сторінок записки 60;

1. Короткий зміст КвР та прийнятих рішень В рамках кваліфікаційної роботи проведено проектування та розробку програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних на основі відомих рішень. Захищена мережа передачі даних має бути побудована із врахуванням досвіду побудови аналогічних мереж передач у різних країнах та задовольняти усім вимогам, враховувала можливість їх вдосконалення та розширення. Поставлена у кваліфікаційній роботі мета досягається розв'язанням наступних задач: 1) виконати аналіз вже існуючих методів та засобів захисту каналів передачі даних по лініях зв'язку у мережах; 2) уточнити та визначити адаптивні шляхи підвищення функціональності роботи мережі та її програмно-технічної системи для передачі захищеної інформації; 3) виконати якісну інфраструктурну реалізацію побудови мережі та спроектувати програмно-технічної засоби для захисту каналів передачі інформації, 4) уточнити та визначити шляхи для підвищення параметрів роботи системи._____

У роботі було спроектовано програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних шляхом вдосконалення та розширення відомих захищених мереж передачі які функціонують за рахунок досвіду уже розроблених мереж та покращено її роботу по надання послуг захищеної передачі. Отримані результати і їх новизна – удосконалена мережа, що якісно функціонує та має захищені канали для передачі даних, що дозволяє підвищити ефективність роботи цієї мережі та функціонування системи захисту інформації. Викладене вище зумовлює актуальність теми кваліфікаційної роботи._____

2. Висновок про відповідність КвР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.___

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок у галузі знань «Інформаційні технології» та спеціальністю «Комп'ютерна інженерія», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було проведено огляд існуючих методів, засобів та технологій у галузі, сучасні засоби та технології, досліджено комп'ютерні технології по захисту даних. У другому розділі проведено проектування програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних. У третьому розділі виконано реалізацію програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних у рамках якої було розроблено мережу та програми для настройки мережі який показує, що основна робота для такої захищеної мережі це організація його основного завдання

по передачі потоків захищеної інформації та підвищення ефективності її роботи, що характеризують стан та напрями для подальшого її розвитку та розроблені основні засоби для комп'ютерної мережі по впливу на процеси захисту даних із метою досягнення зазначених параметрів для їх подальшого розвитку.

4. Позитивні сторони кваліфікаційної роботи полягають у тому що, для вирішення задачі проектування було грунтовно проаналізовано та проведено обгрунтування варіанту побудови засобів для підвищення ефективності роботи програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних, зроблений якісний вибір її основних компонентів та елементів для комп'ютерної мережі по побудові захищеної системи передачі даних.

5. Негативні сторони проекту : У роботі при оцінці параметрів для реалізація використання та забезпечення роботи програмно-технічних засобів забезпечення функціонування мережі із захищеними каналами передачі даних не достатньо приділено уваги практичній стороні втілення сучасних підходів для організації таких систем захисту передачі потоків інформації.

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі проектування.

8. Інші зауваження

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки « добре ».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)

Огнєвий Олександр Вікторович,
доцент каф. ТМТТ

« ____ » _____ 2022 . _____ (підпис)

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Сукача Олександра Володимировича
ПІБ здобувача вищої освіти

студента ФІТ, 4 курсу, групи КІ1с-19-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

06.06.2022
дата

підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА СИСТЕМНОГО ПРОГРАМУВАННЯ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Програмно-технічні засоби забезпечення функціонування мережі із захищеними каналами передачі даних

Автор: Сукач Олександр Володимирович

Галузь знань *12 «Інформаційні технології»*

Спеціальність: 123 – *«Комп'ютерна інженерія»*

Освітня програма: *«Комп`ютерна інженерія»*

Науковий керівник: Хмельницький Юрій Владиславович, к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання роботи та ідентичності версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-30 джерелами на один фрагмент речення;
4) в якості запозичень в окремих місцях системою зафіксовано послідовності кодів, які є вхідними даними до великої кількості задач і не можуть розглядатися як об'єкт авторських прав і, відповідно, їх порушення;
5) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає % і адресується до першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру роботи і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Ю.В.Хмельницький

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц

Дата: 01..06.2022

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ

Направляється студент Сукач Олександр Володимирович на захист дипломного проєкту (роботи)
(прізвище, ім'я, по батькові)

за спеціальністю 123 - Комп'ютерна інженерія

На тему: Програмно-технічні засоби забезпечення функціонування мережі із захищеними каналами передачі даних

Дипломний проєкт (робота), рецензія і довідка про перевірку на плагіат додаються.

Декан факультету _____ Олег САВЕНКО
(підпис) (ім'я, прізвище)

ДОВІДКА УСПІШНОСТІ

Сукач О. В. за період навчання на факультеті інформаційних технологій з 2019 по 2022 роки повністю виконав навчальний план спеціальності з таким розподілом оцінок за:
національною шкалою: відмінно 0,00 %, добре 30,00 %, задовільно 70,00 %.
шкалою ЄКТС: A 0,00 %, B 2,86 %, C 28,57 %, D 34,29 %, E 34,29 %.

Методист факультету _____ _____
(підпис) (ім'я, прізвище)

ВИСНОВОК КЕРІВНИКА ДИПЛОМНОГО ПРОЄКТУ (РОБОТИ) ТА ОБГРУНТУВАННЯ ОЦІНКИ

Студент Сукач О.В. повністю виконав завдання на дипломне проектування, оформив пояснювальну записку та необхідні графічні матеріали.

Оцінка дипломного проєкту (роботи) добре

Керівник дипломного проєкту _____ Хмельницький
(підпис) (ім'я, прізвище)

"8" 06 2022 р.

ВИСНОВОК КАФЕДРИ ПРО ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ)

Дипломний проєкт (роботу) розглянуто. Студент Сукач О. В. допускається до захисту цього проєкту (роботи) в екзаменаційній комісії.

Завідувач кафедри кібербезпеки
(назва)

Клюх В.Н.
(підпис, ім'я, прізвище)

"9" 06 2022 р.

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 2.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 7%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 104638 Название: Програмно-технічні засоби забезпечення функціонування мережі із захищеними каналами передачі даних Добавлено в БД: 2022-06-07 Авторы: Сукач Олександр Володимирович Руководители: Хмельницький Ю.В. Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	119426	780	3598 (3%)	48 (6%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1011481297

Дата перевірки:
07.06.2022 09:21:45 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
07.06.2022 09:23:45 EEST

ID користувача:
100008300

Назва документа: **Плагіат Кваліфакаційна робота Сукач О В. КІ1с-19-1**

Кількість сторінок: **59** Кількість слів: **17870** Кількість символів: **128891** Розмір файлу: **440.50 KB** ID файлу: **1011358683**

8.28%
Схожість

Найбільша схожість: **4.24%** з джерелом з Бібліотеки (ID файлу: **1008399477**)

0.56% Джерела з Інтернету	38	Сторінка 61
8.13% Джерела з Бібліотеки	75	Сторінка 61

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	20