

Хмельницький національний університет
Факультет програмування
та комп'ютерних і телекомунікаційних систем
Кафедра комп'ютерної інженерії та системного програмування

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Локальна комп'ютерна мережа для дитячої амбулаторії
Назва теми

КВРКІ.170374.17.03.04 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»

Шифр, назва

Спеціальність 123 «Комп'ютерна інженерія»

Шифр, назва

Освітня програма «Комп'ютерна інженерія»

Назва

Виконав: студент IV курсу, група КІ-17-3


Підпис

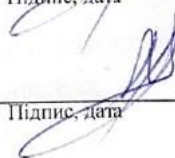
Ю.І. Космина
Ініціали, прізвище

Керівник


Підпис, дата

С.М. Лисенко
Ініціали, прізвище

Нормоконтролер


Підпис, дата

С.М. Лисенко
Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної
Інженерії та системного
Програмування


Підпис

Т.О. Говорущенко

Ініціали, прізвище

« 7 » червня 2021 р.

Хмельницький 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ПРОГРАМУВАННЯ ТА КОМП'ЮТЕРНИХ І ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА СИСТЕМНОГО ПРОГРАМУВАННЯ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЯ ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ

Завідувач кафедри Т.О. Говорушенко

“ 05 ” 02 2021 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Космині Юрію Івановичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Локальна комп'ютерна мережа для дитячої амбулаторії

Керівник проекту (роботи) Лисенко Сергій Миколайович

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

кандидат технічних наук, доцент

Затверджена наказом ректора університету від 05.02.2021 № 11 додаток №7

2. Строк подання студентом проекту (роботи) на кафедру 28.05.2021

3. Вихідні дані до проекту (роботи) локальна мережа для дитячої амбулаторії

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) _____

Дослідження предметної області та постановка задачі: обґрунтування базових положень щодо проектування локальної мережі, проектування логічної і фізичної структури, адресація і розбиття VLAN.





5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Логічна топологія мережі (E8)

Фізична топологія мережі (E8)

Адресація і розподіл VLAN (E8)

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання при
Нормоконтроль	Лисенко С.М., професор кафедри КІСПр		
Антиплагиат	Нічепорук А.О., доцент кафедри КІСПр		



7. Дата видачі завдання « 08 » 02 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Пр
1.	Підготовка вступного розділу	Березень - 1 декада	
2.	Огляд існуючих методів, засобів	Березень - 2 декада	
3.	Обґрунтування обраних рішень	Березень - 3 декада	
4.	Підготовка опису електричних схем	Квітень - 1 декада	
5.	Виконання розрахункової частини	Квітень - 1 декада	
6.	Підготовка ескізів креслень	Квітень - 2 декада	
7.	Формулювання висновків	Квітень - 3 декада	
8.	Розробка додатків	Травень - 1 декада	
9.	Погодження розділів з консультантом з нормоконтролю	Травень - 1 декада	
10.	Оформлення графічного матеріалу	Травень - 2 декада	
11.	Оформлення пояснювальної записки	Травень - 2 декада	
12.	Попередній захист кваліфікаційної роботи	Травень - 3 декада	
13.	Доопрацювання кваліфікаційної роботи	Травень - 3 декада	
14.	Подання роботи для перевірки на плагіат	Травень - 3 декада	
15.	Захист кваліфікаційної роботи	Червень - 1 декада	

Студент

Керівник проекту (роботи)


Підпис

Підпис

Ю.І.Косми
Ініціали, прізвище
С. М. Лисенко
Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Локальна комп'ютерна мережа для дитячої амбулаторії».

Автор роботи: Космина Юрій Іванович.

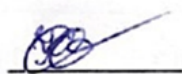
Керівник роботи: Лисенко Сергій Миколайович.

Пояснювальна записка: 67 с., 20 рис., 9 табл., 4 дод., 40 джерел.

Графічна частина: 9 презентаційних слайдів.

ЛОКАЛЬНА МЕРЕЖА, КОМУТАТОР, МАРШУТИЗАТОР, ДИТЯЧА АМБУЛАТОРІЯ, CISCO PACKET TRACER, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ.

Метою роботи є розробка локальної мережі для дитячої амбулаторії. В роботі реалізовано мережу з основним активним мережевим обладнанням, налаштовано адресацію та VLAN. Моделювання мережі реалізовано в середовищі Cisco Packet Tracer



Підпис студента

07.06.2021

Дата

ЗМІСТ

СКРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ	4
ВСТУП.....	5
1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ ..	6
1.1 Локальна мережа і її задачі.....	6
1.2 Типи мереж	7
1.3 Мережева топологія	9
1.4 Основні групи кабелів, які використовуються в локальних мережах	12
1.5 Основні складові кожної локальної мережі.....	14
1.6 Програмне забезпечення локальних мереж.....	16
1.7 Протоколи мережі	17
1.8 Детальніший розбір окремих протоколів	19
1.9 Технологія Wi-Fi.....	20
1.10 Висновки.....	22
2 ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ.....	23
2.1 Дослідження основних користувацьких вимог.....	23
2.2 Використання Wi-Fi в дитячій амбулаторії.....	23
2.3 Види можливих для використання мереж	25
2.4 Способи несанкціонованого доступу до мережі	27
2.5 Методи конструювання безпеки в мережі.....	29
2.6 Способи захисту медичної інформації.....	30
2.7 Етапи захисту інформації	31
2.8 Приклади застосування локальних мереж у інших медичних закладах....	32
2.9 Висновки.....	36
3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПРОГРАМНО-ТЕХ	
3.1 Середовище програмно-апаратної реалізації	37
3.2 Розробка логічної структури локальної мережі	39
3.3 Розробка фізичної структури локальної мережі	41

КВРКІ.170374.17.03.04 ПЗ				
Зм.	Арк.	Медокум.	Підпис	Дата
Виконав		Космина Ю.І.		07.06.21
Перевір.		Лисенко С.М.		07.06.21
Н.контр.		Лисенко С.М.		07.06.21
Затвер.		Говорущенко Т.О.		07.06.21
Локальна мережа в дитячій амбулаторії				
		Літера	Арквш	Арквшів
			2	66
ХНУ, КІ-17-3				

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ЛМ – локальна мережа

КПК – кишеньковий персональний комп'ютер

БД – база даних

ОС – операційна система

DHCP - Dynamic Host Configuration Protocol

ACL - Access Control List

VLAN – Virtual Local Area Network

SSH - Secure Shell

ПЗ – програмне забезпечення

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						3
Зм..	Арк.	№докум.	Підпис	Дата		

ВСТУП

Останнім часом все що зв'язане з комп'ютерними технологіями стає до нас все ближче і ближче. І для комунікації між пристроями використовують локальні мережі. Вони широко використовуються в майже усіх сферах діяльності людини. Однією з таких і є медицина, а у моєму випадку дитяча амбулаторія.

Не виникає сумнівів, що локальна мережа у цій сфері є незамінним помічником в спрощенні і пришвидшенні робочого процесу.

В таких мережах без перешкод можливо вийти у мережу Інтернет, є доступ до усіх баз даних лікарні і інших керуючих документацій. Крім того мережа повинна мати повну підтримку усіх прикладних програм які в свою чергу допомагають у цій сфері.

Мета цієї дипломної роботи розробка локальної мережі в дитячій амбулаторії, яка хоча б мінімально, але допомогла підвищити продуктивність в медицині.

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						4
Зм..	Арк.	№докум.	Підпис	Дата		

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Локальна мережа і її задачі

Локальною мережею називають групу пристроїв, які з'єднані між собою за допомогою, спеціально призначених для цього, дротів які в свою чергу можуть обмінюватись інформацією між собою.

Найперші локальні мережі використовувались для вираховування числових даних. З часом почала широко використовуватись у різноманітних сферах. Користувачі не могли швидко обмінюватися даними. І для цього було використано кабель, яким з'єднали декілька комп'ютерів, щоб вони мали змогу передавати інформацію з однієї машини в іншу. Таким чином були і створені одні з перших локальних мереж.

Залежно від призначення пристрої поділяються на два основні типи:

1. Сервер – це логічний центр локальної мережі, що обробляє різноманітні запити на себе.
2. Користувач – це пристрій від якого іде запит на сервер.

Основні задачі локальної мережі:

- 1) об'єднання груп пристроїв для збільшення швидкості і продуктивності робочого процесу і доступу до важливих файлів;
- 2) копіювання даних для підвищення надійності їх в інформаційних сховищах. Таким чином, всі важливі компоненти файлів розташовані на декількох машинах одночасно, і якщо якийсь комп'ютер вийде з ладу, то будуть використані копії з іншого. Це і є працездатність з апаратною поломкою;
- 3) розгалуження різних типів даних, для досягнення вищого рівня безпеки;
- 4) забезпечення роботи у групах, що дозволяє водночас займатися однією задачею декільком співробітникам;
- 5) зручність у розширенні мережі по мірі потреби в цьому;

					КвРКІ.170374.17.03.04 ПЗ	Арк. 5
Зм..	Арк.	№докум.	Підпис	Дата		

1.2 Типи мереж

За видом розповсюдженості:

1. LAN – Local Area Network – звичайна локальна мережа, всі пристрої в якій розташовані недалеко один від одного.
2. MAN – Metropolitan Area Network – мережа в якій усі пристрої знаходяться в зоні міського району невеликого міста.
3. WAN – Wide Area Network – мережа яка включає в себе комп'ютери на цілій країні або континенті.
4. HAN – Home Area Network – мережа в домівці.

За пропускною здатністю:

- 1) низько швидкісні мережі – до 10 Мбіт/с;
- 2) середньо швидкісні мережі – до 100 Мбіт/с;
- 3) високо швидкісні мережі – більш ніж 100 Мбіт/с.

За типом з'єднання:

- 1) дротові – зв'язаними між собою різноманітними кабелями;
- 2) бездротові – передача здійснюється за допомогою радіоканалу.

За взаємодією пристроїв між собою:

- 1) однорангове;
- 2) ієрархічні мережі.

Всі пристрої в однорангових мережах рівні у своїх правах. Будь який користувач мережі має змогу зчитувати, копіювати, видаляти інформацію яка зберігається в межах цієї мережі. Основною перевагою таких мереж є те що вони прості в встановленні і експлуатації. Але в цьому випадку в мережі будуть проблеми з безпекою даних. Через це такий тип використовується для не великих мереж, в якому захист не є на першому місці.

Що стосується ієрархічних мереж, то ще при плануванні мережі враховуються сервери які будуть керувати доступом до даних. Будь який пристрій який включений в мережу є її клієнтом.

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						6
Зм..	Арк.	№докум.	Підпис	Дата		

Сервер в цій мережі слугує таким званим «регулювальником», який керує усім доступом користувачів до чітко визначених даних. Будь який пристрій який взаємодіє з сервером вже є клієнтом цієї мережі, або робочим простором.

І сам сервер слугує сховищем різноманітних ресурсів. Він може підпорядковуватися іншому серверу, який в ієрархічному ланцюгу стоїть вище. Основними компонентами хорошого серверу є: великий за обсягом жорсткий диск, з потужним процесором(або декількома) і з мережевою картою яка має високу пропускну здатність.

На сьогодні цей тип мережі є більш популярніший ніж одноранговий. Так як від дозволяє створити узгоджену і безпечну мережу у якій всі основні ресурси будуть розподілені рівномірно.

Основними ж недоліками є:

1. Встановлення спеціально призначеного програмного забезпечення.
2. Складність у розширенні мережі.
3. Обов'язково потрібен сервер.

Сервер в свою чергу поділений на два типи:

1. Файл-сервер.
2. Користувач-сервер.

Файл-сервер використовується для зберігання на ньому великої кількості даних. І коли користувачу потрібна та чи інша інформація, сервер її надсилає. Сам процес обробки і відправлення відбувається на відведеному для цього пристрої.

Користувач-сервер представляє собою зв'язок між додатком-користувача і додатком-сервера. Процес обробки інформації в даному випадку виконує сервер, який в свою чергу слідкує за безпекою доступу до даних. Середовище яке надсилало запит, отримує тільки результат.

Мережі з вбудованим сервером, мають можливість з'єднувати понад тисячу пристроїв. Через це можливо використовувати не такі потужні пристрої, як це би було з одноранговими мережами. Користувачам також простіше користуватися такими мережами тому, що все що зв'язане з безпекою виконує сервер.

Є три основних складові ієрархічної мережі:

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						7
Зм..	Арк.	№докум.	Підпис	Дата		

Вузол - це пристрій який був включений в локальну мережу і функціонує в ній. Найчастіше в ролі вузла виступає комп'ютер, але це не завжди так тому, що принтери, камери, ноутбуки також використовуються як вузли.

Сервер – також є вузлом, який обробляє і передає дані усім користувачам. В свою чергу підтримуючи цим самим усю мережу. В мережі необов'язково розташований тільки один сервер, за потребою їх може бути декілька.

Клієнт – це користувач який тільки користується мережевими ресурсами, але сам свої в мережу не додає. Простими словами він тільки користується нею.

Комп'ютер є універсальним вузлом, так як він може бути як і сервером так і клієнтом.

1.3 Мережева топологія

Ця топологія має вигляд геометричний вигляд мережи, зазвичай вона має вигляд графа. Існує декілька типів мереж, а саме: шинна, зоряна, ієрархічна кільцева і довільна.

Шинна (Bus) – ця топологія являє собою суцільний загальний кабель (магістраль або шина) до якого підключенні різноманітні машини. Для забезпечення відбиття сигналу на кінцевій частині кабелю встановлюється термінатор(резистор). Графічне зображення показано на рисунку 1.1..

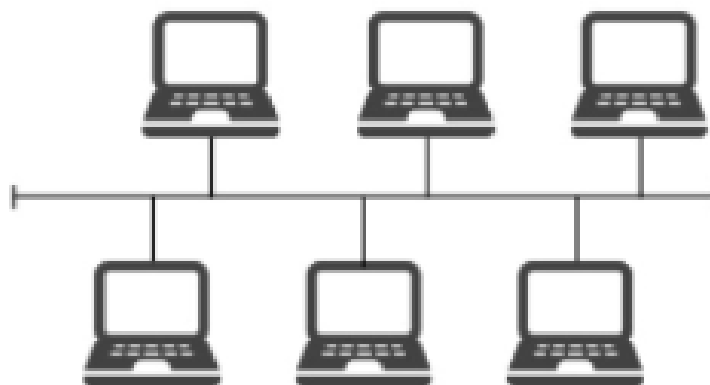


Рисунок 1.1 – Шинна топологія

Зм..	Арк.	№докум.	Підпис	Дата

Зоряна (Star) – це топологія в якій є центральний керуючий вузол, до якого підключені усі інші машини. Перевагами його є що усі пакети ізольовані один від одного, просте додавання нового апарату та несправні деталі легко полагодити або замінити. На рисунку 1.2 показано його графічне зображення.

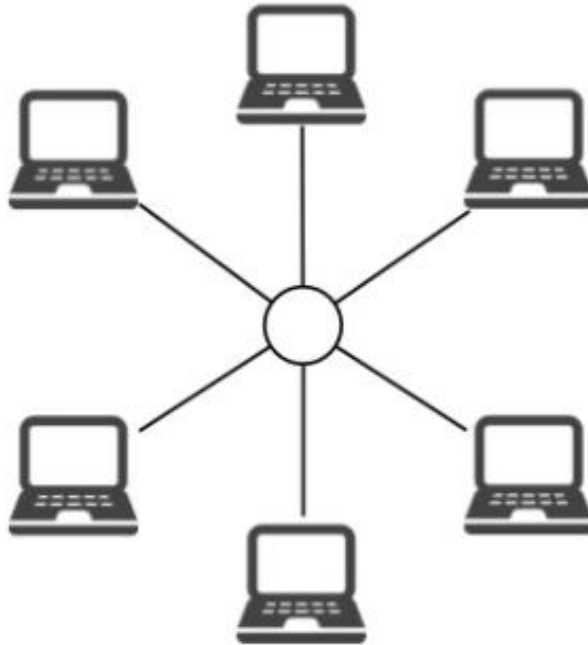


Рисунок 1.2 – Зоряна топологія

Кільцева топологія (ring) – це топологія в якій кожен комп'ютер зв'язаний тільки з двома іншими, а саме від одного джерела він отримує інформацію, а іншому надсилає.

Перевагами є те що на відміну від шинної топології, кільцевій не потрібний термінатор.

Недоліками є те що підключення нових пристроїв є не так вже і просто і всі комп'ютери у мережі не є повністю рівноправними, так як один з них обов'язково отримує інформацію від комп'ютера, який веде передачу в той момент, раніше, а інший пізніше.

Зм..	Арк.	№докум.	Підпис	Дата

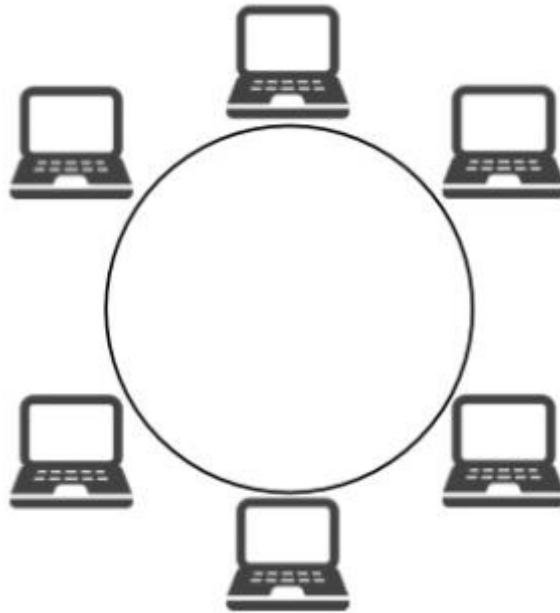


Рисунок 1.3 – Кільцева топологія

Ієрархічна (hierarchical) – вона схожа на зірку(star) але це більш розширений варіант, а саме вона має: додаткові мережеві пристрої, зазвичай мережевий кабель підключений до комутатора до якого підключенні кілька інших комутаторів. В даний час є однією з найпоширеніших топологію.

Більшість сфер діяльності які використовують цю топологію реалізують розподільний підхід до ієрархії в якій кожна станція яка знаходиться вище в ієрархії забезпечує керування нижньої і так по спадаючій.

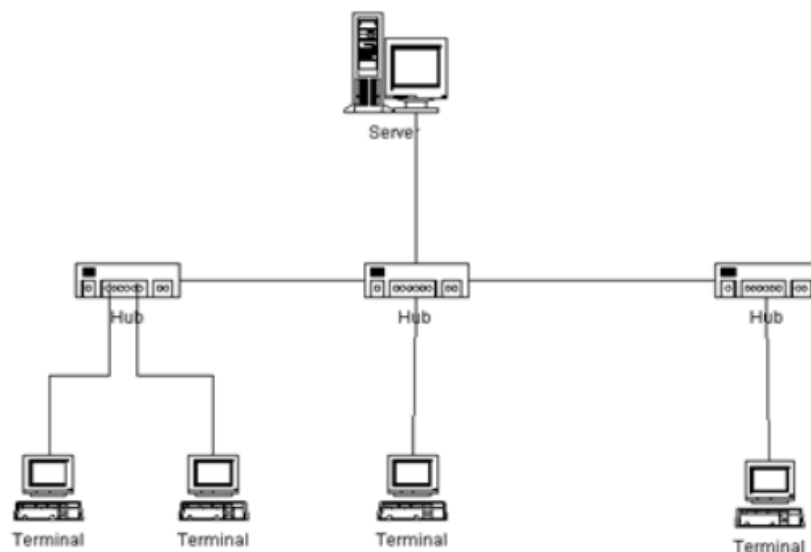


Рисунок 1.4 – Вигляд довільної топології

Зм..	Арк.	№докум.	Підпис	Дата

Довільна топологія – являє собою збір усіх складових інших топологій, а саме: видалення або додавання зав'язків між компонентами мережі.

1.4 Основні групи кабелів, які використовуються в локальних мережах

Сьогодні більшість комп'ютерів використовують для з'єднань між собою проводи кабелі. Вони виконують роль передачі даних та сигналів між пристроями. Через це є декілька видів кабелів для виконання різних задач. Основними з них є:

- 1) вита пара (twisted);
- 2) коаксіальний кабель (coaxial);
- 3) неекранований (unshielded);
- 4) екранований (shielded);
- 5) оптоволоконний (fiber optic).

Вита пара – кабель який має одну або декілька звитих разом провідників які використовуються для зменшення, при передачі сигналу, взаємних наведень. Широко використовується в різних мережах за рахунок своєї дешевизни.

До мережі провідник приєднується за допомогою конектора 8P8C.

Передає інформацію на відстань близько 100 метрів. Для більш довгих шляхів можливе використання повторювача, або ж замінити виту пару на коаксіальний кабель.

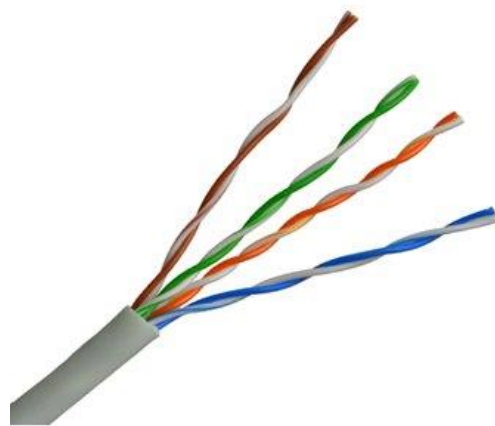


Рисунок 1.5 – Вита пара

Вита пара залежно від своєї захисної оболонки поділяється на:

					КвРКІ.170374.17.03.04 ПЗ	Арк.
Зм..	Арк.	№докум.	Підпис	Дата		11

- 1) екранована вита пара (STP – Shielded twisted pair);
- 2) неекранована вита пара (UTP – Unshielded twisted pair);
- 3) фольгована вита пара (FTP – Foiled twisted pair);
- 4) фольгована екранована вита пара (SFTP – Shielded Foiled twisted pair).

В деяких випадках захист кабелю використовується навкруги кожної окремої пари. Що забезпечує найкращий захист від електромагнітних наведень.

Коаксіальний кабель – електричний кабель який складається з центрального провідника і екрана навкруги. Вони між собою розділені ізоляційним матеріалом в деяких випадках повітряним проміжком, що запобігає випроміненню.

Має однорідну січку і виконаний з більш якісних матеріалів. Через це широко використовувався у побудові локальних мереж і передачі даних на велику відстань аж поки не був витіснений витюю парою.

Ще одною сферою це був використаний це кабель є телебачення. Основною перевагою його було це хвильовий опір. Усі мережі або інші сфери де він використовувався зазвичай вимушені використовувати термінатори.



Рисунок 1.6 – Коаксіальний кабель

Найбільш поширені категорії кабелю:

- 1) RG-8 і RG-11 - «Товстий Ethernet» (Thicknet), 50 Ом. Стандарт 10BASE5;
- 2) RG-58 - «Тонкий Ethernet» (Thinnet), 50 Ом. Стандарт 10BASE2;
- 3) RG-58 / U - суцільний центральний провідник;
- 4) RG-58A / U - багатожильний центральний провідник;
- 5) RG-58C / U - військовий кабель;

					КвРКІ.170374.17.03.04 ПЗ	Арк. 12
Зм.	Арк.	№докум.	Підпис	Дата		

6) RG-59 - телевізійний кабель (Broadband / Cable Television), 50 Ом. аналог РК-50 (Радіо-кабель);

7) RG-59 / U - телевізійний кабель (Broadband / Cable Television), 75 Ом. аналог РК-75; × RG-62 - ARCNet, 93 Ом.

Екранований кабель використовується для передачі цифрових даних і має спеціальне захисне екранування. Всередині кабелю знаходяться тонкі дроти які в свою чергу передають дані.

Відрізняються вони від усіх інших наявністю надійного захисту від електромагнітних випромінювань і забезпечують надійну роботу усіх систем де вони використовуються. Цю функцію виконують вбудовані екрани які виготовлені з різноманітних матеріалів яких як: фольга, дроти, немагнітних стрічок та інших.

На сьогоднішній день найбільш широко використовуваними є мідні екрановані кабелі, так як мідь має низький опір і високу провідність струму. Для різних задач використовується різна кількість дротів.

Основними перевагами є: захист від навколишніх електромагнітних завад і захист навколишнього середовища від випромінювання самого кабелю. Особливості того чи іншого кабелю можна дізнатися по його маркуванню:

1. В – Оболонка з полівінілхлоридного пластику.
2. К – Контролюючий кабель.
3. Е – Наясність екрану.
4. Нг – Захищений від горіння.
5. ВВГ – Ізольований дріт який має оболонку з ПВХ пластику.

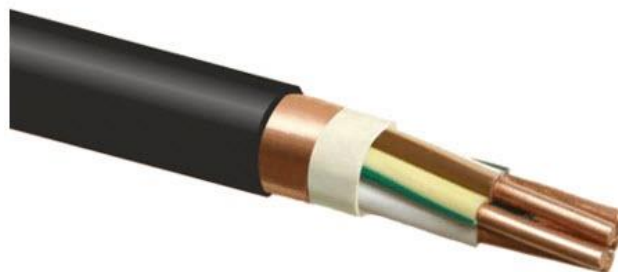


Рисунок 1.7 – Екранований кабель

1.5 Основні складові кожної локальної мережі

Різні сполучні компоненти з'єднують пристрої в середині мережі і забезпечують обмін інформацією набагато простіше, аніж без неї. Грамотний вибір комплектуючих відіграє важливу роль у плануванні мережі, тому що є найзатратною частиною проекту. Ще однією причиною чому важлива кожна складова є те що, при поломці в будь якій частині мережі, це буде досить таки дорого в обслуговуванні, через незручність у відновленні.

Є декілька основних видів мережевих компонентів:

Мережеві карти – це невід'ємний компонент будь якої комп'ютерної мережі, який вбудовується в материнську плату на пристрої. За допомогою цієї карти відбувається передача і прийом сигналів в мережі. Останнім часом вона є вже вбудована в материнську плату пристрою.

Маршрутизатори – компонент мережі який направляє дані з однієї мережі в іншу. На сьогодні більшість маршрутизаторів мають декілька портів для кабелів які підключають пристрої в мережу. Зазвичай він під'єднаний до мережі Internet через мережевий дріт і до інших вузлів вже у вашій мережі. Маршрутизатор зазвичай має набагато більше функцій аніж інші з'єднувальні компоненти мережі. Він може аналізувати дані і міняти адрес доставки мережевих пакетів. Виконує він також функції простого комутатора, який з'єднує декілька пристроїв для спільного використання. Він часто виступає в ролі DHCP – сервера і надає пристрою свою унікальну адресу.

Маршрутизатор це як мініатюрні комп'ютери які мають у своєму арсеналі процесор і якийсь запас пам'яті, який допомагає йому обробляти дані які надійшли до нього. Він має свою унікальну операційну систему яка допомагає налаштувати його під себе.

Термінатор – іншими словами це резистори які вбирають в себе надлишковий сигнал. Зазвичай розташовані в кінці дротів в мережі.

Комутатор – одне із центральних управляючих компонентів мережі, який аналізує пакети, які надходять до нього, і відправляє на відповідний адрес. Мережі

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						14
Зм..	Арк.	№докум.	Підпис	Дата		

які сконструйовані на базі комутаторів можуть вміщати понад тисячу пристроїв і мати довжину декількох кілометрів.

Повторювач – компонент мережі який підсилює сигнал, який не можливо передавати на велику відстань. Він слугує для зв'язування сигналу двох або більше пристроїв які знаходяться в мережі.

Міст – це з'єднувач, що сполучає декілька частин мережі, які через ту чи іншу причину коротші ніж потрібно. Також з функцією мостів є те, що вони підсилюють і перетворюють сигнал для інших кабелів.

Мультиплексор – це компонент, який підтримує понад сотню користувацьких мережевих сполучень. Вони передають свої дані через телефоні сполучення, в подальшому які передаються через один спільний канал в мережу.

Брандмауер – за границя між декількома мережами, яка не допускає підозрілі з'єднання до мережі. Зазвичай цю технологію використовують для захисту доступу до своєї мережі з мережі інтернет.

1.6 Програмне забезпечення локальних мереж

Існує три базові складові, які забезпечують працездатність локальної мережі:

Автономні операційні системи – програмне забезпечення, яке встановлене безпосередньо на пристроях користувачів.

В сучасному світі зазвичай використовують 64-бітні операційні системи на базі Linux і Windows 10

Мережеві операційні системи – програмне забезпечення, яке встановлюється на спеціально призначених серверах. Воно забезпечує основу для будь якої локальної мережі.

Найпопулярнішими з них є:

1. Операційна система Unix досить таки гнучка і зможе підстроюватись під будь які завдання користувача. Включає в себе велику базу вбудованих компонентів, які допоможуть вирішити проблеми що зв'язані з роботою в локальній мережі. Основними перевагами цієї операційної системи є її надійність і легка автоматизація. Легкість у керуванні забезпечується тим, що вона

створювалась для обробки величезних за обсягом файлів, тому вона на голову перевищує своїх «однокурсників».

2. Операційна система NetWare популярність вона здобула через те, що була однією із перших операційних систем. Вона може керувати сервер який буде звичайним комп'ютером. Основними функціями операційної системи є керування інформацією і переправлення сигналів у відповідні для неї пристрої. Системні дані зберігаються на звичайних жорстких дисках сервера, а не на носіях робочих пристроїв.

3. І безліч операційних системних компонентів від компанії Microsoft (Microsoft Windows Server, Windows NT).

Мережеві додатки і служби – різноманітні софт-програми які допомагають користуватися і керувати мережею.

Основною задачею додатків і служб є забезпечення спільної роботи користувачів на різних частинах локальної мережі.

Програмним забезпеченням можливо узгодити усі дані на усіх пристроях. Забезпечити доступ до файлів визначеному колу людей. Швидко передавати інформацію на великі відстані. Розподіляти ресурси за потребою.

1.7 Протоколи мережі

Для того щоб отримувач даних або сигналів правильно зрозумів наказ, усю інформацію ділять на визначеними правилами передачі інформації. Обов'язково для локальної мережі використовується свій протокол передачі інформації.

Так що це таке протокол? Протокол це певний узгоджений системою набір правил передачі інформації між пристроями у вашій мережі. В локальних мережах вони не тільки поєднують пристрої працівників закладу, але різноманітні додатки, за допомогою яких можливо підтримувати спілкування між персоналом.

На сьогоднішній день найбільш популярною є протоколи на основі OSI. У цій технології протоколи діляться на сім рівнів взаємо пов'язаних частин, від фізичного до програмного рівня.

Найпершим є прикладний рівень він забезпечує безпосередній зв'язок користувача з мережею. Цей протокол надає доступ до головного сервера, баз даних і доступ до основних файлів. Також відсилає різноманітні команди в системі і формує відгуки про помилки.

Наступним рівнем є представлення. Він конвертує протоколи в відповідні формати мережі. Простими словами, сигнали отримані від мережі перетворюються в сигнали зрозумілі для додатків і навпаки. Також на цьому рівні виконується архівування даних і переправлення сигналів іншому абоненту мережі.

П'ятим у списку є сеансовий рівень, він підтримує мережу в активному стані і не дає їх вимкнутись при тривалому використанню. Виконує синхронізацію передачі даних між пристроями.

Наступним йде транспортний рівень – слугує для забезпечення цілісності даних в тому вигляді в якому вони були відправленні. Позбавляється від пошкоджених і повторюваних файлів. І не залежить які дані були передані, на цьому рівні виконується сама функція передачі інформації. Різноманітні скупчення файлів розділяються на менші для зручності передачі. Одними із широко використовуваними є протоколи: TCP і UDP.

Мережевий рівень представляє собою визначення адресу доставки інформації. Він обирає найкоротший шлях для передачі даних, визначає помилки в мережі, перевіряє наявність пошкоджень безпеки і в цілому адресацію даних. В цьому рівні використовуються відомі для звичайного користувача маршрутизатори.

Наступним йде каналний рівень він контролює дані на фізичному рівні, перевіряє мережу на помилки, які виникають при транспортуванні даних. Усі сигнали які надійшли до нього він поміщає в спеціальні «комірки» і перевіряє їх працездатність. На цьому рівні використовуються комутатори мережі.

Останнім є фізичний рівень який безпосередньо забезпечує передачу сигналів. На цьому рівні здійснюються передача і конвертація даних в залежності від їх отримувача. Потік даних забезпечують оптичні кабелі, радіосигнали або супутникова передача. В цьому рівні використовуються хаби і повторювачі.

Фізичний рівень підключений до усіх пристроїв, які підключені до мережі, мережевим з'єднувачем.

1.8 Детальніший розбір окремих протоколів

Найпопулярнішим на сьогодні є протокол HTTP – це протокол забезпечує передачу гіпертексту. Вважається протоколом найвищого рівня, був спеціально винайдений для передачі інтернет інформації. Через цей всебічний протокол ми спостерігаємо в мережі Інтернет такі красиві і функціональні сайти. Він є ядром мережі «W.W.W.». Функціонування його забезпечується таким чином: користувач надає HTTP запит в своєму браузері, який в свою чергу і є HTTP сервером. Під час переходу на іншу веб сторінку браузер здійснює запит на сервер відповідної сторінки. Щоб весь контент на сторінці відображався так як це задумав сам автор, використовується така мова розмітки як HTML.

Сама адреса сайту протоколу HTTP має наступний вигляд:
`http://www.hello.ua .`

Наступним по використанню йде протокол FTP – призначений для передачі даних в мережі інтернет. Має наступний вигляд: `ftp://....com .`

IP протоколи – цей протокол використовується на мережевому рівні. Основною функцією є передача пакетів від відправника до отримувача. Усі пакети цього протоколу мають свою унікальну IP адресу і адресу відправника і отримувача. Але відповідний порядковий номер порту не використовується. Простими словами він виконує функцію передачі інформації, і не знає якому додатку був надісланий запит і чи дійшов він до кінцевої точки. Отримання інформації про виконання запиту виконується на транспортному рівні.

Одним із таких є UDP протокол – він ініціалізує порт відправника сигналу і порт отримувача відповідно.

Порт TCP – це протокол виявляє чи був доставлений той чи інший пакет до отримувача. Перед передачею даних йде ехо запит який перевіряє чи дві транспортні точки зв'язані між собою. І тільки після цього файли будуть передаватися до тих пір, поки не дійдуть усі. В деяких випадках пакети

					КвРКІ.170374.17.03.04 ПЗ	Арк. 18
Зм.	Арк.	№докум.	Підпис	Дата		

надсилаються повторно, через перепої в транспортній системі. Якщо якийсь окремий пакет не дійшов до отримувача, він буде відправлений ще раз.

UDP – цей протокол також виконує функцію передачі інформації, але не гарантує успішну передачу даних. Основною перевагою цього протоколу є простота у реалізації передачі.

1.9 Технологія Wi-Fi

Сьогодні наше життя не можна уявити без цієї технології, так як вони сильно закріпилися. Wi-Fi можна зустріти майже всюди, починаючи від нашої домівки і до різноманітного транспорту і навіть літаків. Ще в дев'яностих роках минулого століття велися роботи над різними стандартами цієї технології. І в підсумку ми маємо єдиний бездротовий клас мереж: IEEE 802.11 wireless LAN або іншими словами Wi-Fi.

Сьогодні існує декілька базових стандартів а саме: 802.11, 802.11b, 802.11a, 802.11g. Але основним став стандарт 802.11g, який по використанню сильно переганяє своїх «однокласників». Проте є маршрутизатори які працюють на декількох стандартах водночас.

Наприклад:

- 1) на подвійному це: 802.11.a/g;
- 2) на потрійному це: 802.11.a/b/g.

Спільного в них також багато чого. Вони всі використовують однаковий протокол доступу це – CSMA/CA. І всі стандарти що зв'язані з канальним рівнем, у них також ідентичні. Вони мають змогу зменшувати швидкість передачі даних для того щоб збільшити дальність маршруту. Порівняння основних стандартів знаходиться в таблиці 1.1.

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						19
Зм..	Арк.	№докум.	Підпис	Дата		

Таблиця 1.1 – Порівняльна характеристика стандартів Wi-Fi

Стандарт	Діапазон частот (МГц)	Швидкість передачі інформації (Мбіт/с)
802.11.b	2400-2483,5	До 11
802.11.a	5150-5350	До 54
802.11.g	2400-2483,5	До 54

Стандарт 802.11.b має швидкість передачі даних близько 11 Мбіт/с і працює в одному діапазоні з мобільними телефонами і мікрохвильовками. Різноманітні перешкоди такі як: стіни, двері, металеві пластини знижують якість зв'язку. Цей стандарт має декілька алгоритмів які допомагають йому уникати перешкод і прояву проблем через використання великого числа пристроїв. Можливість збільшити дальність сигналу за допомогою встановлення додаткових антен. Смуга сигналу поділена на 14 каналів з шириною в 22 МГц.

Якщо говорити про стандарт 802.11.a, то передача даних відбувається в більш високому діапазоні, але цей стандарт страждає від великої кількості пристроїв навкруки, через це втрачає свою пропускну здатність.

Мережі з типом 802.11.g працюють в однаковому діапазоні що і 802.11.b і мають взаємний зв'язок між собою. Через це користувачам досить просто перейти на новий стандарт 802.11.g. Основною перевагою якого є висока швидкість передачі даних.

Найновішим стандартом який стрімко набирає свою популярність є 802.11.n відрізняється він тим, що використовує технологію multipleinput & multiple-output – МІМО. Таким чином відправник і одержувач мережевих пакетів може вбудувати в свою систему дві і більше антени, які будуть передавати або приймати сигнали відповідно. Швидкість може досягати навіть декількох сотень мегабайт в секунду.

В першому розділі бакалаврської роботи, було проаналізовано предметну область мережі. Розібрано усі види кабелів та активного мережевого обладнання. Проводився вибір виду мережевої адаптації.

Також обговорювалося доцільність використання і актуальності даної технології в наші часи, та подальшого модернізування.

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						21
Зм..	Арк.	№докум.	Підпис	Дата		

2 ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ

2.1 Дослідження основних користувацьких вимог

На даний момент людство переживає етап стрімкого розвитку цифрового обладнання, і автоматизації всього що нас оточує. Вже для нас не в новинку, що ми можемо віддалено керувати своїми пристроями та автоматизувати будь яке виробництво. І це допомагає у оптимізації нашого часу і реалізації комфортних умов для робочого процесу. Це зумовлено тим, що людина завжди хоче якось спростити свої завдання. Так і у медицині є вже дуже багато різноманітних датчиків, портативних лабораторій і навіть роботів.

Сама суть усіх цих технологій у покращенні і оптимізації робочого процесу в медицині. Фактично зараз ми живемо у час комп'ютерних технологій, тому використання локальних мереж і різноманітних пристроїв зв'язку допоможе б ефективніше відслідковувати робочий процес в медицині, а саме в амбулаторіях. Через це створення мережі з вбудованою системою керування і спостереження є досить таки актуальним завданням на сьогоднішній день. Об'єктом дослідження є моніторинг палат пацієнтів за допомогою відеоспостереження, спілкування через їх пристрої (телефони, планшети, ноутбуки та ін.).

Основними вимогами до проекту є:

- 1) зв'язок усіх пристроїв які знаходяться у мережі;
- 2) моніторинг зображення з камер на окремому комп'ютері;
- 3) розподіл пристроїв на окремі VLANи;
- 4) забезпечити захист комутаторів за допомогою паролю;
- 5) забезпечити бездротовий доступ до локальної мережі.

2.2 Використання Wi-Fi в дитячій амбулаторії

На даний момент більшість країн світу інвестують в розвиток медицини, тому що дбають про фізичний стан своїх жителів. І ця сфера є одна із найкращих для досліджень нових технологій тому, що там можна поєднати теорію і практику. Наприклад сьогодні можливо провести дистанційний огляд і консультацію людини

					КвРКІ.170374.17.03.04 ПЗ	Арк. 22
Зм..	Арк.	№докум.	Підпис	Дата		

за декілька сотен кілометрів до неї. Передавати різну інформацію, а саме: результати аналізів, діаграми високої якості які потребують швидкого транспортування. Керування медичними роботами дистанційно в тих випадках коли не має можливості очно зустрітися з пацієнтом. І для розвитку нових технологій для цієї структури потрібні дослідження і кошти.

Коли з'явилися бездротові мережі, до них в ту саму мить піднявся інтерес з сторони різних сфер, які зв'язані з комунікацією з людьми. Однією з таких є медицина і сьогодні майже усі клініки намагаються включити цю технологію в свій робочий процес.

Зарубіжна компанія Frost and Sullivan провела аналіз ринку в області охорони здоров'я, і вони дійшли до висновку що технологія локальних мереж буде зростати більш на п'ятдесят відсотків в рік. Найпершим впровадженням в медицину є встановлення мережевого з'єднання в службах швидкої допомоги і в палатах.

Ще одна досить таки відома компанія використала цю технологію в своєму закладі, який розрахований вміщує в собі понад тисячу пацієнтів. Зазвичай медсестра записувала інформацію про пацієнта на папері, і вже пізніше записувала ці дані в комп'ютер. Після встановлення локальної мережі в заклад, вони можуть на території усієї лікарні вводити і змінювати дані. Таким чином економити час якого зазвичай так не вистачає.

Мережі сьогодні прогресивно розвиваються і вже в найближчому майбутньому в усіх сферах їх будуть використовувати. І практично всі лікарні будуть мати вбудовану Wi-Fi мережу.

На мою думку використання мережі в дитячій амбулаторії дозволить робітникам закладу:

1. Переміщатися по території закладу і бути завжди у мережі.
2. Мати дистанційний доступ до мережі з будь якої точки.
3. Wi-Fi допоможе мати доступ там же прокладення провідного з'єднання неможливе.
4. Зв'язувати офіси між собою.
5. Підвищити ефективність робочого процесу тому, що можливо вносити дані про пацієнта на момент його огляду.

					КвРКІ.170374.17.03.04 ПЗ	Арк. 23
Зм..	Арк.	№докум.	Підпис	Дата		

6. Зменшення втрачених даних за рахунок запису інформацію в туж мить як тільки її отримав.

7. Доступ мережі для пацієнтів лікарні також буде позитивно впливати на їх дозвілля.

2.3 Види можливих для використання мереж

Мережі в медицині поділяють за рівним використання на:

1. Обслуговування медичних закладів на територіальному рівні.
2. Керування різноманітними медичними службами.
3. Керування службами які займаються профілактикою захворювань.
4. Керування закладами освіти.
5. Довідка мед персоналу.
6. Керування службами які надають послуги екстреної допомоги.
7. Онлайн перевірка стану здоров'я населення.
8. Забезпечення інформації для наукових робіт.
9. Керування інформацією в локальних мережах.

Ще мережі поділяють за функціональним призначенням:

1. Система стаціонарного обслуговування – використовується для автоматизації закладу. Вона надає послуги онлайн обміну даними і віддаленого онлайн сховища інформації.

2. Інформаційна система для амбулаторій – призначення для обслуговування амбулаторій. Виконує функції статистичного збору інформації, веде автоматичний запис виписаних з лікарні пацієнтів з вбудованою базою даних.

3. Фінансова інформаційна система – її основною задачею є збір усієї інформації між страховими, санітарними, профілактичними закладами і різноманітними благодійними фондами з допомоги населення.

4. Інформаційна система «Сховище» - використовується для зберігання і конвертування інформації в усі популярні формати баз даних.

5. Автоматизована система зберігання важливих зображень (флюорографія, магнітно резонансні томографії, електро-кардіограма, енцефалограма та інші.)

					КвРКІ.170374.17.03.04 ПЗ	Арк. 24
Зм..	Арк.	№докум.	Підпис	Дата		

6. Автоматизація робочих місць персоналу в медичних закладах.

7. Автоматизовані системи управління базами даних – слугує для узгодження даних в мережі.

Стандартна система управління інформацією має наступний вигляд:



Рисунок 2.1 – Схема потоку інформації в амбулаторії

Кругообіг інформації в мережі медичного закладу забезпечується тільки тоді, коли усі стандарти і формати є узгодженими. З постійним розвитком цієї сфери гостро встає питання про створення єдиного універсального стандарту для усіх закладів.

2.4 Способи несанкціонованого доступу до мережі

Забезпечення захисту даних – це запобігання спроб втручання в сталий робочий процес мережі, захист від крадіжки інформації або її змін.

Головною загрозою безпеці є неавторизоване керування, пошкодження, або навіть знищення важливої інформації.

На сьогоднішній день з'являється зовсім нова технологія безпеки в інформаційних технологіях. Для забезпечення цієї технології потрібно значне використання коштів і людської праці. Але це покращення допоможе запобігти ураженню інформації і втрати її від сторонніх лиць.

Активні загрози – це загрози які мають чітку ціль, вони поражають систему інформації заплановано. Основні види активної загрози:

1. Ураження пристроїв для повного виводу зі строю.
2. Пошкодження бази даних.
3. Знищення програмних компонентів пристрою.
4. Зрушення зв'язувальних мереж між пристроями.

Головним джерелом небезпеки зазвичай є шахраї або спеціально розроблені для цього програмне забезпечення.

Ненавмисне розповсюдження інформації її власником, або людьми які знали це за своєю посадою. Вихід неконтрольованої важливої інформації по різноманітним оптичним або радіо каналам.

Несанкціонований доступ – це незаконне заволодіння чужою інформацією людиною, яка не має право на це.

Види несанкціонованих загроз:

1) логічна вибухівка – слугує для пошкодження або знищення важливої інформації, інколи її ще використовують для викрадення даних. Зазвичай цей метод

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						26
Зм..	Арк.	№докум.	Підпис	Дата		

використовують не зовсім компетентні співробітники, яким чимось не сподобалось їх становище в робочому процесі;

2) троян – програмне забезпечення, яке виконує додаткові шахрайські дії для заволодіння важливою інформацією. Зазвичай маскується під іншу, довірену для мережі, програму;

3) вірус – програмне забезпечення яке пошкоджує якийсь компонент системи і робить його копію. Використовується для пошкодження або знищення даних. Інколи віруси мають можливість розмноження в системі;

4) черв'як – шкідливе програмне забезпечення яке проникає в пристрій через мережу інтернет і не залишає після себе ніяких слідів. Він використовує механізм для модифікування вхідного вузла і очікує подальших наказів від свого основного тіла;

5) зчитувач паролів – слугує для викрадення різноманітних важливих значень або кодів доступу в системі;

б) компрометація інформації – це неавторизоване змінення значень в базі даних, після цього користувачеві потрібно шукати усі зміни і виправляти їх, або створювати нову базу даних.

Різновиди несанкціонованого доступу до даних:

Несанкціоноване використання інформації являє собою витік даних за допомогою різних видів загроз, який можливо допоможе шахраям втрутитися в робочий процес вашої локальної мережі.

Також ця проблема виникає при використанні даних авторизованим користувачем але який не зовсім компетентний у своїй сфері, через це і відбувається витік інформації у вільні джерела.

Цей витік інформації можливо попаде в руки шахраєві, який зможе отримати доступ в місце, в яке йому заборонено втручатись.

Не підтверджена передача інформації між користувачами, також може спричинити отримання важливої інформації стороною, яка не має права володіння цією інформацією. І це може призвести до зламу безпеки мережі.

Порушення обслуговування даних – загроза, якою зазвичай стає сама мережа. Одним із випадків є затримка запиту у системі, що призведе до незапланованим

					КвРКІ.170374.17.03.04 ПЗ	Арк. 27
Зм..	Арк.	№докум.	Підпис	Дата		

наслідкам. Невчасна доставка інформації до користувача може призвести до невірному вирішенню того чи іншого робочого питання.

Несанкціоноване користування привілеями мережі – проникання в мережу користувача який не має на це права, і тоді система виконує спеціальні дії для виявлення, шкідливо для системи, об'єкта.

2.5 Методи конструювання безпеки в мережі

Є декілька основних принципів за якими будується система безпеки у будь якій мережі. Ось основні з них:

Системний підхід створення елементів захисту, передбачає оптимальну сукупність усіх властивостей які були використані в минулих проектах, які зарекомендували себе з кращої сторони і не викликають зайвих труднощів в побудові.

Система повинна мати безперервний розвиток. Тому, що усі загрози удосконалюються, і якщо система безпеки не бути йти з ними нога в ногу, то шахраям буде досить легко проникати у мережі.

Раціональний розподіл доступу до інформації, іншими словами: надання користувачам конкретних можливостей, для запобігання використування ресурсів не призначених для них.

Повний контроль над усіма користувачами в мережі, чіткий запис всіх дій що вони виконують для подальшого дослідження виниклої помилки мережі. А також для неможливість виконати будь якої дії, без авторизації користувача.

Забезпечення сталого рівня захисту системи, який би забезпечив сталий захист мережі в моменти її пошкодження. Іншими словами працездатність мережі потрібно буде підтримувати в будь який момент, навіть в момент злому або її вимкнення.

Забезпечення мережі системою пошуку і знешкодження шкідливих програмних компонентів, за рахунок програмного забезпечення і працівників мережі.

					КвРКІ.170374.17.03.04 ПЗ	Арк. 28
Зм..	Арк.	№докум.	Підпис	Дата		

Система безпеки повинна бути економічно співставною з цінністю інформації захищеної нею. І не виникати зайвих проблем з встановленням її в мережу.

2.6 Способи захисту медичної інформації

Правовий захист – збір нормативно правових актів, законів, які контролюють безпеку мереж в медицині на законному рівні. Користувачі які порушують безпеку мережі можуть підпорядковуватись навіть кримінальним кодексом.

Інформаційне забезпечення – це усі записи, дані і правила які зберігаються на пристроях в мережі, і забезпечують її безперебійне функціонування.

Апаратне забезпечення – сукупність спеціалізованих технічних рішень, що підтримують і захищають мережу від шкідливого впливу.

Програмне забезпечення – простими словами це сукупність програм які ведуть статистику, перевіряють різноманітні датчики і сканують стан мережі. Запобігають сторонньому втручанням до інформації закладу.

Математичний захист – метод математичного розрахунку ризиків які можуть статися в мережі. Оцінка методів шахраїв, якими вони руйнують або викрадають інформацію.

Лінгвістика – це сукупність термінів і позначень для забезпечення спеціалістами грамотної комунікації між собою.

Нормативний захист – він включає в себе діяльність різноманітних органів захисту в мережі, інструкції, методи, поради які забезпечують захист інформації в умовах жорсткого контролю даних.

Ще одним із актуальних способів захистити свою інформацію є криптографія. Це вид шифрування який забезпечує безпеку даних шляхом перетворення їх в незрозумілий для звичайного користувача код. Щоб розшифрувати це повідомлення потрібно використовувати унікальний дешифратор. На даний час цей метод широко використовується за рахунок своєї надійності.

					КвРКІ.170374.17.03.04 ПЗ	Арк. 29
Зм..	Арк.	№докум.	Підпис	Дата		

2.7 Етапи захисту інформації

Перший етап розпочинається з оцінки і розподілу самих даних:

- 1) власники інформації оцінюють які дані потрібно захищати;
- 2) для особливо важливих даних виділяється окрема категорія;
- 3) розраховується термін придатності для особливо важливої інформації, це робиться для того, щоб шахраї не встигали реалізувати викрадену інформацію;
- 4) виділяють основні аспекти в групах інформації, щоб простіше було ділити дані;
- 5) розбиття інформації за типом призначення.

Другий етап представлений способів для виявлення різноманітних шляхів викрадення інформації.

- 1) обговорюється кому будуть вигідні конфіденційні дані;
- 2) визначаються якими методами викрадають інформацію шахраї;
- 3) знаходження «дірок» в мережі;
- 4) конструюються методи по ліквідації шахраїв.

Третій етап передбачає в собі перевірку вже активних методів боротьби проти втрати інформації (надійність персоналу, програмне забезпечення, безпека паперових варіантів).

Четвертим етапом є вибір індивідуальних методів захисту, на основі вже проведених досліджень в минулих етапах. Ще на цьому етапі розробляються нові засоби захисту інформації.

На п'ятому етапі керівництво закладу, вислухавши усі методи, приймає рішення в подальшому їх використанню.

Шостим етапом є реалізація вже узгоджених систем захисту інформації, з урахуванням усіх порад від керівництва.

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						30
Зм..	Арк.	№докум.	Підпис	Дата		

2.8 Приклади застосування локальних мереж у інших медичних закладах

Одним із прикладів буде лікарня в Великобританії, а саме: «Gastrointestinal Unit, Western General Hospital» який знаходиться в Единбурзі. В цій локальній мережі використовуються різноманітні методи, як вже відомі так і є декілька нестандартних. Але поки багато з них ще не інтегровані, і знаходяться в статусі розробки. Основним є використання кишенькового комп'ютера. Зрозуміло що лікарі затурбовані безпекою інформації у своєму закладі. І тому по всякому захищають свою мережу від атак шахраїв.

Головними складовими мережи є:

1) миттєво доставляти інформацію в будь яку точку закладу, коли цього хтось вимагає. Ця інформація включає в себе всі основну інформацію про пацієнта, а саме: записи, демографічні дані, направлення та анамнез;

2) мати можливість замовити додаткове обстеження та онлайн консультацію.

Ці два головних правила і є основою їх мережі.

Розвиток локальних мереж у медицині різко піднявся за останні роки. У цьому закладі бездротові мережі використовуються для забезпечення доступу до клінічної інформації, запису пацієнтів. Також використовується для обміну інформації між колегами протягом обстеження пацієнтів, а також до доступу результатів аналізів пацієнтів.

За основу вони вибрали HP iPaQ для кишенькового комп'ютера, через те що вони працюють на операційній системі MS Windows та мають вбудований модуль бездротової мережі. За допомогою цього пристрою вони мали доступ до баз даних реалізованих за допомогою MySQL і працює на основі інтрамережі. Під'єднання комп'ютерів відбувається за допомогою стандартних компонентів від компанії CISCO. Також наявний аудіо вихід з мікрофоном, що дозволяє вести запис розмови та швидкого голосового спілкування. Далі трішки докладніше про вибране обладнання:

В їх проекті було використано бюджетне обладнання. Сервер містив базу даних GIPSY (GI Patient System), яка була написана індивідуально на веб сервері

					КвРКІ.170374.17.03.04 ПЗ	Арк. 31
Зм..	Арк.	№докум.	Підпис	Дата		

Apache та сервері баз даних SQL. Для точок доступу мережі використовувалися пристрої від компанії CISCO AIRONET 1200. В цю точку доступу було ініційовано захист типу CISCO PIX 506E, що забезпечує надійне VPN з'єднання з мережею закладу. Усі пакети які проходять через цей захист надійно шифруються для забезпечення найвищого рівня захисту інформації. На кишеньковому комп'ютері використовується операційна система Pocket PC, яка забезпечує підключення до таких точок доступу.

Бази даних на основі MySQL здатні впоратись навіть з дуже великими обсягами файлів які знаходяться у системі GIPSY. Дані передаються досить таки швидко і надійно. Це база типу клієнт – сервер і тому записує будь які дії і відновлення системи після помилок в системі.

Під час розробки мережі було декілька структур бази даних, а саме: ORACLE і MySQL. MySQL – це системне програмне забезпечення в відкритим кодом яке має юридичну ліцензію GNU. Основною перевагою MySQL є низька вартість обслуговування і сумісність з усіма іншими компонентами мережі. Мовою для функціонування запитів було обрано PHP. І в кінцевому результаті вони мали сервер Apache, бази даних MySQL, і мову PHP. Тому що це три безкоштовні компоненти які між собою співставні.

Оскільки для використання кишенькового комп'ютера потрібно то бездротове рішення також використовувалася у цьому проекті. І тому потрібно вдало проробити систему безпеки у такій мережі. Забезпечується це тим що відключаються порти які ніде не задіяні с системі. Також усі пристрої закладу мають свою унікальний код який внесений у їх мережеву карту, по якій і відбувається авторизація в системі. Ця технологія називається WEP (Wired Equivalent Privacy), Також вона забезпечує захист до дротових мереж. Основною перевагою цієї технології є, що вона впливає тільки на два зв'язки між пристроями, які обмінюються даними. Також часто будь яке дротове підключення також буде захищене системою WEP.

Але ця технологія має свою слабкість, вона передає не велику кількість пакетів і через криптографічну будову ключів захист можна відновити ключ до безпеки мережі. Але щоб уникнути усіх цих недоліків було обрано іншу технологію

					КвРКІ.170374.17.03.04 ПЗ	Арк. 32
Зм..	Арк.	№докум.	Підпис	Дата		

а саме: IPSec – це новий захист інформації в бездротових мережах. Ця технологія має вбудований VPN в усіх її частинах. За допомогою неї створюється надійно захищений зв'язок в середині незахищеного. У їх випадку це кишеньковий комп'ютер і сервер. Ще однією причиною вибору є те, що захист відбувається в одному тунелі. Між IPSec з'єднанням і кишеньковим комп'ютером знаходиться брандмауер, який в свою чергу також захищає важливу для медицини інформацію. Дротові пристрої не підключаються на пряму в мережу, вони підключаються через спеціальний ізольований канал який вже потім з'єднується з IPSec, гарантуючи ще вищий рівень безпеки.

Після багаторазових тестувань системи, не було виявлено ніяких перешкод у подальшій експлуатації цієї мережі. Бездротове підключення відбувається за стандартом 802.11b і на частоті 2.4 ГГц.

Також проводилися різноманітні випробування дальності прийому сигналу на відстані від 5 до 50 метрів до обладнання клініки. Проводилось обережне прокладання дротового каналу, щоб усі елементи не перетинали вже існуючі. Кардіологічний блок використовується від компанії Symbol Technologies. Виробник завіряє що система має високу стійкість до електронних перешкод. Вибрана технологія широко використовується в багатьох медичних закладах. В управлінні живленням використовується система DSSS (Direct Sequence Spread Spectrum) в якій можливо налаштувати потужність живлення. На сьогоднішній день не зафіксовано ні одного випадку з втручання в електромагнітну мережу з обладнанням від компанії Cisco.

В цьому закладі ця система використовується близько одного року. Інші міські лікарні Единбургу боялися використовувати цю технологію в робочому процесі тому, що думали що вона є ще «сирою». Але страх був невиправданий тому, що лікарня Gastrointestinal Unit, Western General Hospital цілком добре функціонувала з цією мережею з кишеньковими комп'ютерами.

З самого початку впровадження цієї технології в робочий процес, працівники захоплювалися різноманітністю в їх рутину працю. Хоча і перед тим було багато випробувань, налаштувань і покращень доступності до мережі.

Переваги кишенькового комп'ютера:

					КвРКІ.170374.17.03.04 ПЗ	Арк. 33
Зм..	Арк.	№докум.	Підпис	Дата		

Надає доступ до важливих паперів, зображень та записам про пацієнтів а саме:

Доступ до даних про пацієнта, що зберігаються в базі даних GIPSY. Воно включає в себе демографічні деталі та можливість відображення всебічної клінічної історії, та всі попередні листування щодо пацієнта. Це надзвичайно корисно, особливо там де паперові примітки до справи відсутні. Такі зображення, як рентгенівські та ендоскопічні зображення, які можна зберігати, переглядати на пристроях.

The Lothian Drug Formulary , який містить дані про всі лікарські препарати, затверджені в лікарні доступний на КПК для негайної консультації. Це по суті позбавляє потреб носити з собою громіздкі записи. Оновлення ліків здійснюється по бездротовій мережі з мережевого сервера.

Доступ до керуючих систем. Вони становлять неоціненний довідковий посібник. У своєму новому форматі кишеньковий комп'ютер зараз постійно доступний в будь-якому місці, і оновлення на нього легко застосовуються з сервера.

Нарешті, Pocket Acrobat Reader дозволяє переглядати та обмінюватися роботами та журналами на кишеньковому комп'ютері. Кишеньковий доступ до цих документів приносить значні ергономічні переваги. Молодшим лікарям особливо подобається зручний розмір пристрою. Очікується, що він завжди замінить собою BNF (British National Formulary) - стандартне посилання на ліки), керівництво з експлуатації та диктофон, які могли б зараз всі вони носити з собою замінені одним кишенькового комп'ютера. Однак у деяких аспектах малий розмір може бути небезпечним - було висловлено занепокоєння тим, що він підстрибує у машині швидкої, і може випасти у важливий момент.

Основні недоліки мережі з кишеньковими комп'ютерами:

Основним недоліком є автономність роботи. Тому, що звичайний робочий день перевищує автономність роботи на вісім годин, і тому слід використовувати його тільки по потребі. На це впливає також зв'язок по бездротовій мережі, на який також витрачається частина автономності акумулятора. Було виявлено що середній час автономної роботи кишенькового комп'ютера становить три або чотири години. І лікарі почали використовувати його тільки тоді, коли це дійсно потрібно.

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						34
Зм..	Арк.	№докум.	Підпис	Дата		

Видача нових повністю заряджених акумуляторів, не стало вирішенням проблеми, через те, що акумулятори є досить такі дорогі і вони часто губилися. Рішенням стало розташування зарядних станцій по всій території закладу.

Також були випадки після повного розрядження пристрою, зникала уся інформація яка була на ньому. Але це не принесло великих проблем. Тому, що інформацію можливо було відновити з резервних копій.

2.9 Висновки

В даному розділі проводилася робота по пошуку шляхів покращення моєї мережі. Було проаналізовано усі джерела небезпеки та «дірок» які можуть перешкодити продуктивній роботі в мережі.

Також була визначена доцільність використання технології Wi-Fi в дитячій амбулаторії.

Розглядалося вже відомі рішення, з унікальними функціями, будови мережі в іноземних компаніях. Що допомогло мені в подальшому плануванні своєї мережі для дитячої амбулаторії.

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						35
Зм..	Арк.	№докум.	Підпис	Дата		

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ПРОГРАМНО-ТЕХНІЧНОГО ЗАСОБУ

3.1 Середовище програмно-апаратної реалізації

Кожний проект починає свій розвиток з точного моделювання. І перш ніж розпочинати планування, потрібно визначитись з середовищем. Порівнявши усі плюси і мінуси, я залишив свій вибір на Cisco Packet Tracer. Тому що, це одна із найкращих програм для моделювання своєї мережі. Її можливо використовувати на усіх передових операційних системах (Windows, Linux, Mac OS та інших). Також доступна і мобільна версія, для портативного редагування проекту.

Це середовище дозволяє додавати і керувати різноманітними маршрутизаторами, комутаторами та іншими компонентами мережі. Для фізичного зв'язку використовуються велика кількість кабелів, що дає змогу налаштовувати мережу більш детально. Усі види кабелів зображені на рисунку 3.1.

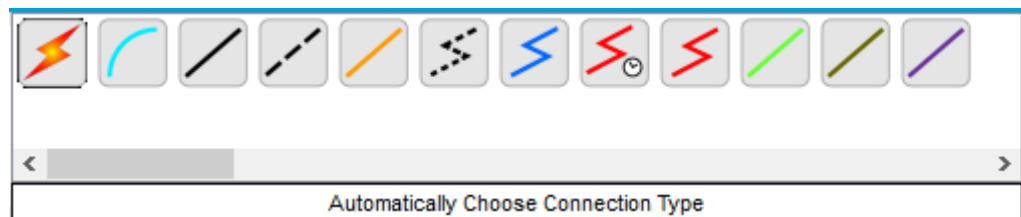


Рисунок 3.1 – Види кабелів в Cisco Packet Tracer

За допомогою функціоналу Cisco Packet Tracer можливо з легкістю будувати моделі будинків та навіть цілих населених пунктів.

Чому ж я обрав саме це середовище? Через його високу функціональність і гнучкість. На рисунку 3.2 зображено усі види компонентів які використовуються в цьому середовищі.



Рисунок 3.2 – Компоненти мережі Cisco Packet Tracer

Можливо зручно взаємодіяти з ними, а саме просто перетягнути потрібний елемент на робочий простір, і він опиниться там, для подальшого його використання.

Саме налаштування пристроїв відбувається у зрозумілому для користувача інтерфейсі, який не вимагає від нього якихось глибоких знань в області моделювання мереж. Я детальніших налаштувань використовується консольна симуляція CLI.

Ще однією причиною, чому я обрав саме це середовище, є те що є зручний поділ мережі на логічний і фізичний рівень. Що допомагає більш детальніше формувати план мого проекту. За замовчуванням усі пристрої знаходяться на одному фізичному рівні, але мені потрібно було розмістити їх в різних приміщеннях. Для поверхневого планування мережі це не грає значну роль, але для мене це була невід’ємна складова середовища розробки.

Cisco Packet Tracer також може імітувати погодні умови, поведіку датчиків та багато іншого. Це можливо реалізувати за допомогою різноманітних мов програмування.

Роблячи висновок, порівнявши усі інші середовища з Cisco Packet Tracer, я обрав саме його, через його обширний функціонал і розподіл на фізичний і логічний рівень.

3.2 Розробка логічної структури локальної мережі

Під час розробки будь якої локальної мережі першим кроком є планування логічної структури. Основною задачею для чого призначене логічне проектування це розмежовування трафіку між фізичними компонентами. Після її реалізації продуктивність стрімко підіймається, за рахунок того, що пристрої не простоюють просто так, коли відбувається передача даних на іншій частині мережі. Ще логічна структура дозволяє покращити пропускну здатність та дозволяє адміністраторам мережі краще і швидше контролювати її.

Для зменшення навантаження на мережу, потрібно розбити весь трафік на деякі підрозділи. В моєму випадку я розбив на 3, а саме: медики та персонал, камери відеоспостереження і охоронець, пацієнтів та відділ безпеки. Для всіх хто входить в ці групи права і доступ є однаковим. Вимоги і пропускну здатність також.

Для підвищення продуктивності я розбив це все на відповідні віртуальні підмережі. Цей розподіл я реалізував за допомогою технології VLAN, яка дозволяє ділити мережу, на менш дрібніші віртуальні мережі. VLAN, простими словами, це сукупність вузлів які мають спільне налаштування доступу і з основною мережею взаємодіють ніби знаходяться в іншій. Єдиним мінусом цієї технології є те, що вона ділить пропускну здатність в мережі.

Таблиця 3.1 - Поділ вузлів мережі на VLAN

Назва відділу	Кількість вузлів	Назва VLAN	Номер VLAN
Медики і персонал	7	Medic	10
Камери відеоспостереження та охорона	12	Cameras	20
Пацієнти і гості	4	Patient	30

Зм..	Арк.	№докум.	Підпис	Дата

Залежно від потреб мережі, вона поділена на три VLANa, до медиків і персоналу під'єднано 7 вузлів, до камер відеоспостереження та охорони 12 та до пацієнтів та гостей під'єднано 4.

Діапазон приватних адрес в мережі я використав починаючи з 192.168.1.1 і так далі.

Розподіл адрес в мережі Wi-Fi, здійснюється за допомогою DHCP модуля, який вбудований в маршрутизатор.

Таблиця 3.2 – Адреси усіх вузлів в дитячій амбулаторії

Назва вузла	IP-адреса	Маска підмережі	Шлюз за замовчуванням
PC-0	192.168.3.2	255.255.255.0	192.168.3.1
PC-1	192.168.3.3	255.255.255.0	192.168.3.1
PC-2	192.168.3.5	255.255.255.0	192.168.3.1
PC-3	192.168.3.6	255.255.255.0	192.168.3.1
PC-4	192.168.3.7	255.255.255.0	192.168.3.1
Security_PC	192.168.3.4	255.255.255.0	192.168.3.1
Cam_1	192.168.3.20	255.255.255.0	192.168.3.1
Cam_2	192.168.3.21	255.255.255.0	192.168.3.1
Cam_3	192.168.3.22	255.255.255.0	192.168.3.1
Cam_4	192.168.3.23	255.255.255.0	192.168.3.1
Cam_5	192.168.3.24	255.255.255.0	192.168.3.1
Cam_6	192.168.3.25	255.255.255.0	192.168.3.1
Cam_7	192.168.1.20	255.255.255.0	192.168.1.1
Cam_8	192.168.1.21	255.255.255.0	192.168.1.1
Cam_9	192.168.1.22	255.255.255.0	192.168.1.1
Cam_10	192.168.1.23	255.255.255.0	192.168.1.1
Cam_11	192.168.1.24	255.255.255.0	192.168.1.1
Cam_12	192.168.1.25	255.255.255.0	192.168.1.1

Пристрої які підключені через бездротове з'єднання отримують свою IP-адресу через DHCP.

3.3 Розробка фізичної структури локальної мережі

Фізична структура мережі представляє собою розподіл мережі безпосередньо в будівлі дитячої амбулаторії. Головна структура амбулаторії складається з трьох поверхової будівлі. Стіни кімнат зроблені з цегли і покриті шаром штукатурки.

Це моделювання повинно буде забезпечувати все фізичне функціонування мережі. Сукупність кабелів розроблена для забезпечення зв'язку між компонентами мережі.

Для передачі інформації в структурі дитячої амбулаторії і подальшого функціонування усіх компонентів потрібно використовувати пропускну здатність не менше 100 Мбіт/с.

На кожному поверсі є декілька кімнат, а саме: на першому дві кімнати, на другому також дві кімнати, а на третьому розміщені п'ять палат для пацієнтів. Також на першому та другому поверсі є багато вільного місця для подальшого розширення мережної частини. Головний сервер розміщений у кімнаті на другому поверсі.

Для поєднання мережі було використано наступні дроти:

- 1) кабелі типу вита пара, для з'єднання пристроїв;
- 2) та кабель типу Serial, для з'єднання двох маршрутизаторів.

Детальніше про те, де саме використовувався той чи інший дріт можливо побачити у додатку А копія креслення логічної топології мережі.

На першому поверсі також розміщено приміщення для охорони, в якому стоїть комп'ютер, який в свою чергу зв'язаний зі всіма камерами в амбулаторії.

Для забезпечення зв'язку між вузлами в мережі, використовується стандарт Ethernet, і також через високу пропускну здатність маршрутизатора я використав більш вдосконалений варіант цього стандарту Gigabit Ethernet. Що забезпечить підвищення пропускну здатності всієї мережі, і дасть доступ до удосконалення її в

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						40
Зм..	Арк.	№докум.	Підпис	Дата		

майбутньому. Для кожного працівника виділено по одній розетці. З розеткою Cablexpert (NCAC-1U5E-01) RJ-45, він зображений на рисунку 3.3.



Рисунок 3.3 – Розеточний модуль Cablexpert (NCAC-1U5E-01) RJ-45

Прикріпленні вони будуть на столах користувачів на висоті одного метра. Всього потрібно розташувати сім таких розеток по всій амбулаторії.

Для прокладання кабелів в коридорах, кабінетах та палатах доцільніше було використати пластикові коробки. Головною перевагою яких є їх дешева ціна і легкість в експлуатації. Використовуваний пластиковий короб зображений на рисунку 3.4.



Рисунок 3.4 – Пластиковий короб 220 TM Professional

Зм..	Арк.	№докум.	Підпис	Дата

Пластикові коробки закріплюється за допомогою дюбелів з шурупами. Перед встановленням їм потрібно зрізати гострі кінці, для того щоб при доторканні до них не пошкоджувались меблі.

Для забезпечення системі безпечного відключення через перебої в електричній мережі було використано блок безперебійного живлення Powerwalker VI 3000 RLE. Зовнішній вигляд якого зображений на рисунку 3.5.



Рисунок 3.5 – Блок безперебійного живлення Powerwalker VI 3000 RLE

3.4 Вибір активного обладнання

Для управління всією мережею використовують активне обладнання, ним є: маршрутизатори, комутатори, сервери та багато іншого. Від вибору компонентів мережі залежить весь її функціонал і продуктивність. Саме ці складові виконують всі узгодження і об'єднують все разом до однієї локальної мережі. Воно повинно забезпечувати високу продуктивність і не протидіяти робочому процесу, а навпаки його оптимізувати.

В своїй мережі я використав:

Таблиця 3.3 – Типи та кількість активного обладнання яке я використав.

Номер	Тип	Кількість
1	Маршрутизатори	2
2	Комутатори	3
3	Камери відеоспостереження	12
4	Сервер	1
5	Робочі комп'ютери	6

Детальніший розбір обладнання я розпочну з маршрутизаторів. Він призначений на сам перед поєднувати різні частини мережі разом, також регулює пересилання пакетів в відповідні адреси. Але ж основною задачею для чого я його використав це об'єднання різноманітних вузлів в одне ціле, які між собою не можуть функціонувати при відсутності маршрутизатора. Також маршрутизатор я використовував для видачі приватних локальних IP-адрес для всіх вузлів мережі. Він є невід'ємним компонентом усіх мереж, починаючи від маленьких домашніх, закінчуючи величезними мережами для цілих фірм. Зо допомогою його виконується захист від втручання не бажаних користувачів мережі, фільтрація пакетів та якщо потрібно то автоматична видача IP-адрес за допомогою DHCP серверу.

Для збільшення пропускної швидкості мережі маршрутизатори поділяють на ширококомвні домени та домени колізій, які в свою чергу забезпечують фільтрування даних. Саме маршрутизатор забезпечує доступ в Інтернет.

Основними функціями маршрутизатора в моїй мережі є:

- 1) керування трафіком для його розподілення по вузлам;
- 2) використання DHCP видачі IP-адрес для бездротових маршрутизаторів.

Для вирішення цих питань, мені підійшли два маршрутизатора, а саме дротовий CISCO 1941 і бездротовий WRT300N. Зовнішній вигляд маршрутизаторів зображений на рисунках 3.6 та 3.7 відповідно.



Рисунок 3.6 – Маршрутизатор CISCO 1941



Рисунок 3.7 – Бездротовий маршрутизатор WRT300N

Маршрутизатори фірми CISCO славляться своєю продуктивністю та надійністю, вони досить таки легкі в експлуатації, та мають надійний захист від стороннього втручання.

Він забезпечує оптимальну передачу пакетів, простими словами, він сортує усі дані, та передає їх користувачам. Пропускна здатність його і кількість портів цілком забезпечить всі примхи нашої невеликої дитячої амбулаторії. Основні характеристики маршрутизатора Cisco 1941 знаходяться в таблиці 3.4.

Таблиця 3.4 – Основні характеристики маршрутизатора Cisco 1941.

Основні характеристики	Значення
Виробник	Cisco
Опис продукту	Комплект безпеки Cisco 1941 з ліцензією SEC PAK
Загальна кількість портів	2
USB	Так
Порт управління	Так
Пам'ять	512 мб.
Кількість широкосмугових портів	2
Технологія Ethernet	Gigabit Ethernet
Безпека	IPSec, SSL, Фільтрування вмісту IOS, Гнучка відповідність пакетів, AAA, L2TPv3, MARS безпеки Cisco.

Зм..	Арк.	№докум.	Підпис	Дата

До маршрутизаторів також підключені комутатори. Вони слугують для поєднання великої кількості вузлів в мережі в одне ціле і забезпечення поліду їх на віртуальні локальні мережі Основними вимогами до якого є:

- 1) велика пропускна здатність, для швидкої передачі медичної інформації в мережі;
- 2) захист від мережевих штормів;
- 3) адаптивна функція вибору більш пріоритетних пакетів.

Для цього мені підходять комутатори Cisco 2960-24TT. Детальний вигляд такого комутатора зображений на рисунку 3.8.



Рисунок 3.8 – Комутатор Cisco 2960-24TT

Цей комутатор також має вбудовану систему по сортуванню пакетів за пріоритетом. Його можливо налаштовувати не тільки через інтерфейс консолі, але і він ще має зручний Web інтерфейс для зручного налаштування. Основні характеристики комутатора знаходяться в таблиці 3.5.

В своїй мережі я використав таких три, по одному на поверх. В комутаторах є багато вільних портів для забезпечення розширення мережі в майбутньому.

Таблиця 3.5 – Основні характеристики маршрутизатора Cisco 1941.

Основні характеристики	Значення
Виробник	Cisco
Опис продукту	Catalyst 2960 24 10/100 + 2 1000BT LAN
Загальна кількість портів	24
Комутатор Ethernet	Інтерфейси / порти
Подробиці про порт	2 x Gigabit Ethernet Uplink
Підтримуваний тип носія	Вита пара
Мережеві технології	10Base-T, 10/100 / 1000Base-T
Вхідна напруга	110 В
Пропускна здатність	16 Гбіт/с

Якщо говорити про сервер, то це один із найважливіших компонентів в мережі. Він забезпечує зберігання і обробку файлів. Зазвичай сервери використовуються для підтримки функціонування мережі. Дуже часто у якості серверу використовується потужний персональний комп'ютер. Основною задачею сервера є здатність безперебійно працювати протягом довгого проміжку часу.

Вибирати сервер потрібно з головою, так як він забезпечує роботу усієї локальної мережі. Також він слугує для збереження та синхронізації усіх даних. Забезпечує резервне копіювання записів працівників.

Для своєї мережі, я вибрав вже не готовий варіант серверу, а підібрав усі комплектуючі сам. Так, як це значно зменшить витрату коштів на нього. Тому що, зазвичай виробники вже готових збірок серверів беруть кошти ще за підбір і збірку. І для моїх потреб в мережі, я підібрав сервер з наступними характеристиками:

Таблиця 3.6 – Характеристики серверу

Частина сервера	Комплектуючі
Чипсет	Intel C242
Процесор	Intel Xeon E-2100 3.3/4.5ГГц 4С
Пам'ять	1x 8Гб DDR4 2600МГц ECC
Жорсткий диск	2 TB WD Blue
Блок живлення	400Вт



Рисунок 3.9 – Зовнішній вигляд обраного серверу

На вибраному сервері була інстальована операційна система Windows Server 2016 та інший набір програм який використовується в медичних закладах. Також ще потрібно налаштувати файлову систему, але це вже можливо зробити в самій операційній системі Windows. Ще однією складовою сервера є узгодження його з іншими вузлами в мережі, щоб вони могли обмінюватись інформацією і керувати ним.

3.5 Моделювання мережі

Для моделювання мережі, як я вже визначив, я використовував Cisco Packet Tracer. Воно дозволяє розробити мережу і налаштувати її основні можливості. Використовувані пристрої я обрав продукцію компанії Cisco, так як і в фізичній розробці, щоб повністю імітувати модель мережі віртуально.

Всі моделювання мережі відбувалися згідно вимог.

Проектована схема знаходяться у додатку А копія креслення логічної топології мережі.

3.6 Налаштування обладнання

У цьому розділі буде все основне налаштування мережевого обладнання, а саме: це два маршрутизатори та три комутатори. Основною функцією маршрутизатора в мережі є передавання пакетів. Комутатор же в свою чергу зв'язує вузли в віртуальні мережі (VLAN).

3.6.1 Налаштування доступу до мережі

Щоб забезпечити віддалене керування на таких пристроях як маршрутизатори і комутатори, для них потрібно налаштувати доступ з вузлів мережі. Є декілька основних протоколів які це забезпечують, а саме: SSL, Telnet та SSH. Спільним в них є те що вони всі захищають мережу, але відмінне те що ступінь захисту в них різний.

В своєму випадку я обрав протокол SSH, так як він забезпечує кращий рівень захисту даних ніж стандартний Telnet, а також має пароль доступу.

План налаштування віддаленого керування SSH:

- 1) відкрити CLI консоль комутатора або маршрутизатора;
- 2) задати найменування для домену відповідного пристрою;
- 3) згенерувати захисний ключ доступу;
- 4) генерування віртуальних сесій;
- 5) обмежуємо доступ, і робимо його тільки за допомогою SSH;
- 6) придумуємо і налаштуємо пароль доступу.

Для виконання усіх цих дій знадобляться наступні команди:

```
R1>enable
```

```
R1#config terminal
```

```
R1(config)#hostname R1
```

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						48
Зм..	Арк.	№докум.	Підпис	Дата		

```
R1(config)#ip domain-name kidamb.com
```

```
R1(config)#crypto key generate rsa
```

```
R1(config)#line vty 0 4
```

```
R1(config-line)#transport input ssh
```

```
R1(config-line)#password secret zxc
```

Також не лишнім буде встановити доступ по паролю для комутатора. Для встановлення його для режиму EXEC, потрібно перейти в режим конфігурації, та вписати туди відповідні для цього команди:

```
S1# configure
```

```
S1(config)# line console
```

```
S1(config-line)# password zxc
```

```
S1(config-line)# login
```

```
S1(config-line)# end
```

Після цих дій для того щоб отримати доступ до консолі комутатора потрібно буде ввести пароль – «zxc».

Для ще більшої надійності я також встановив кодовий доступ для привілейованого режиму конфігурації, який слугує для основних змін в налаштуванні пристрою.

Щоб це забезпечити потрібно ввести два рядочки команд:

```
S1# configure
```

```
S1(config)# enable secret zxczxc
```

3.6.2 Налаштування віртуальних мереж

Для об'єднання вузлів в віртуальні локальні мережі застосовується технологія VLAN. Налаштовування якої відбувається тільки на комутаторах в мережі.

Для створення і конфігурації VLAN потрібно слідувати плану:

- 1) для початку потрібно зайти в CLI консоль на комутаторі;
- 2) створити віртуальну мережу VLAN;
- 3) надати унікальний номер та ім'я;

- 4) надати доступ «access» для VLAN;
- 5) включити набір вузлів мережі в VLAN.

Щоб це застосувати на комутаторі я виконав наступні команди:

```
Switch>enable
```

```
Switch#configure
```

```
S3(config-vlan)#vlan 20
```

```
S3(config-vlan)#name Cameras
```

```
S3(config)#interface range f0/11-16
```

```
S3(config-if-range)#switchport mode access
```

```
S3(config-if-range)#switchport access vlan 20
```

```
S3(config-if-range)#exit
```

За допомогою цих команд виконується налаштування усіх віртуальних мереж в нашій локальній мережі.

Для перевірки створених VLAN і їх налаштувань прописується команда в режимі «enable» яка виглядає наступним чином: show vlan brief.

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig0/1, Gig0/2
10	Medic	active	Fa0/3, Fa0/4
20	Cameras	active	Fa0/2, Fa0/11, Fa0/12, Fa0/13
30	Patient	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Рисунок 3.10 – Таблиця VLAN в комутаторі

Також не потрібно забувати про інтерфейс який буде зв'язаний з маршрутизатором та іншими комутаторами. Він слугує для синхронізації інформації між пристрої.

Щоб налаштувати цей інтерфейс потрібно:

- 1) потрібно зайти в CLI консоль на комутаторі;
- 2) вибрати відповідний інтерфейс;
- 3) ввімкнути trunk канал;
- 4) виділити віртуальні мережі які будуть синхронізовані.

Команди які для цього використовуються:

```
S1>enable
```

```
S1#conf
```

```
S1(config)#int f0/10
```

```
S1(config-if)#switchport mode trunk
```

```
S1(config-if)#switchport trunk allowed vlan 10, 20, 30
```

3.6.3 Налаштування DHCP

Щоб пацієнти в амбулаторії змогли користуватися мережею я реалізував DHCP сервер, який знаходиться в бездротовому маршрутизаторі.

Але щоб використовувати DHCP потрібно налаштувати інтерфейси які виконують функцію узгодження IP-адрес в віртуальних мережах.

Для створення таких інтерфейсів потрібно виконати наступні пункти:

- 1) відкрити на маршрутизаторі його консоль управління;
- 2) обмежити додавання IP-адрес на вибраний інтерфейс;
- 3) виділити інтерфейс для узгодження;
- 4) надати інтерфейсу власну IP-адресу.

Для реалізації в консолі потрібно виконати наступні команди:

```
WirelessRouter>enable
```

```
WirelessRouter #configure terminal
```

```
WirelessRouter (config)#int FastEthernet0/0
```

```
WirelessRouter (config)#no shutdown
```

```
WirelessRouter (config-if)#int fa0/0.10
```

```
WirelessRouter (config-subif)#encapsulation dot1q 10
```

```
WirelessRouter (config-if)#ip address 192.168.1.1 255.255.255.0
```

IP-адреса видається пристрою залежно від маски і вузла по замовчуванню маршрутизатора.

3.6.4 ACL та їх налаштування

Для підвищення продуктивності мережі, за рахунок обмеження пропускної здатності для окремих елементів мережі. Також Access Lists забезпечують керування доступом до конфіденційних даних. Це реалізовано на спеціальних унікальних списках доступу.

Звичайний формат вводу списків доступу май наступний вигляд:

```
Router(config)#access-list «Номер» {permit | deny | remark} «IP-адреса отримувача» «Обернена маска адреси».
```

Спочатку обирається порядковий номер списку, він може бути в межах від одного до дев'яносто дев'яти. Потім вказується правило за яким визначається що відбувається з отриманими пакетами інформації. І завершальним ступенем налаштування є запис IP-адреси і її оберненої маски.

Також ще є і розширений список доступу. Він відрізняється від звичайного тим, що вони детальніше визначають адресу вузла який відправив пакети, і можливістю точно визначати тип даних який передається.

В консолі налаштувань маршрутизатора конфігурація списків доступу виглядає:

```
WirelessRouter (config)#access-list 101 deny ip 192.168.1.1 0.0.0.255 0.0.0.0 0.0.0.0
```

```
WirelessRouter (config)#access-list 101 deny ip 192.168.1.50 0.0.0.255 0.0.0.0 0.0.0.0
```

3.7 Налаштування комп'ютерів та перевірка з'єднання

Для забезпечення виділення IP-адрес в вузлах, потрібно правильно конфігурувати. Для цього перейти в налаштування протоколу IPv4 на комп'ютері

					КвРКІ.170374.17.03.04 ПЗ	Арк. 52
Зм..	Арк.	№докум.	Підпис	Дата		

перейти у пункт «Сеть», далі в пункт «IP версії 4 (TCP/IPv4)», і там поставити галочку на пункті «Получить IP-адрес автоматически». Вікна з налаштуваннями зображені на рисунку 3.11.

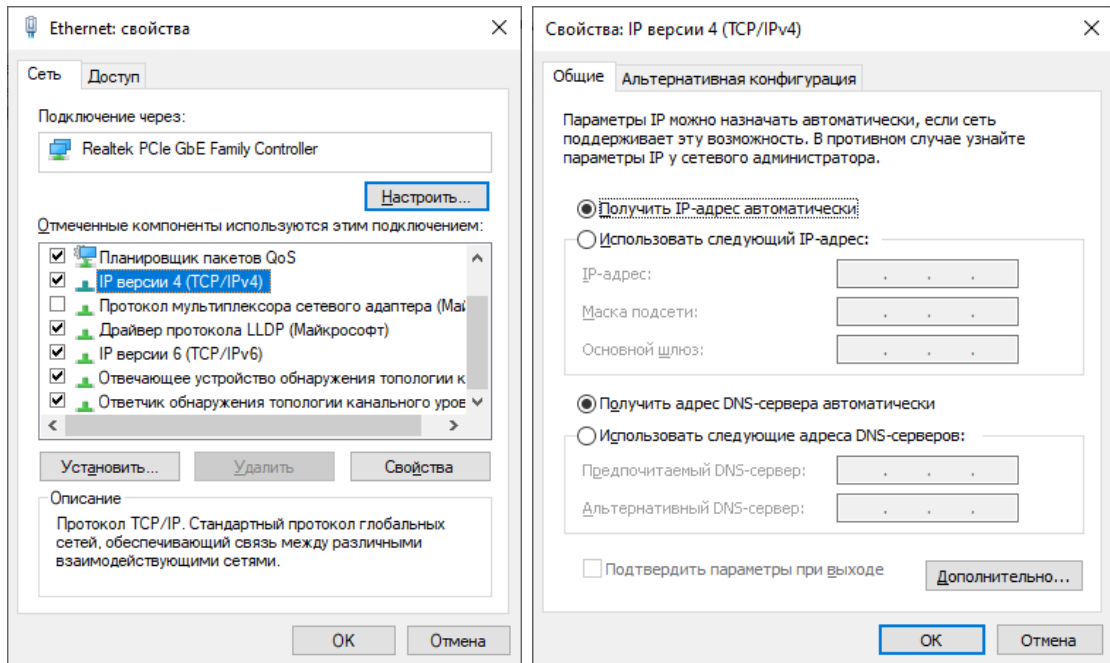


Рисунок 3.11 – Налаштування комп'ютерів

Протестувати зв'язок між пристроями можливо за допомогою командного рядка. Там прописати команду ping і IP-адрес вибраного вузла.

Вигляд командного рядка з перевіркою з'єднання зображено на рисунку 3.11.

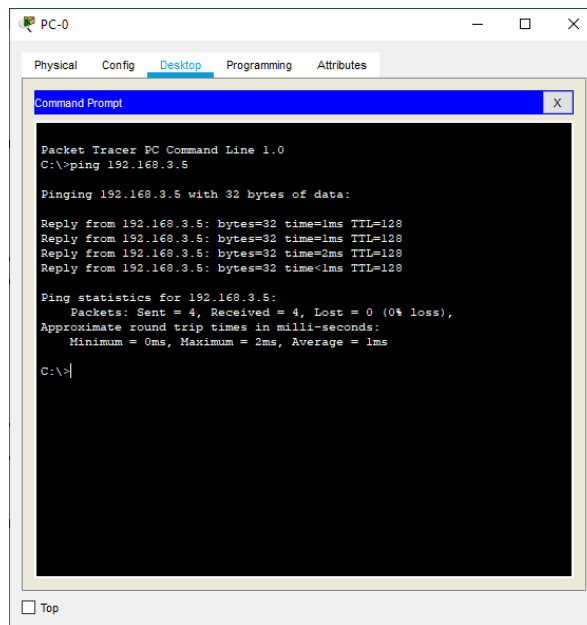


Рисунок 3.11 – Превірка з'єднання комп'ютера з іншим комп'ютером

Зм..	Арк.	№докум.	Підпис	Дата

3.8 Розрахунок вартості обладнання

Підрахунок вартості основних мережевих компонентів відбувався за цінами, взятими з інтернет магазину «Rozetka» станом на 07.05.2021р.

Збірка комп'ютера виконувалася мною. Тому що, не хотів переплачувати за готові варіанти. Я врахував усі вимоги для дитячої амбулаторії, і в мене вийшли комп'ютери з наступними характеристиками:

Таблиця 3.7 – Характеристики серверу

Тип комплектуючого	Марка і модель	Ціна грн.
Процесор	I3-10100F(3,6-4,3 ГГц)	3 400
Материнська плата	Intel H410 (ASUS PRIME H410M-R-SI)	1 500
Оперативна пам'ять	Оперативная память 8GB (2x4GB) DDR3 ECC Registered	1 200
Вінчестер	wd blue 1tb	1200
Монітор	Samsung F24T350FHI Dark Gray	3599
Клавіатура	Logitech K120 USB RUS OEM	250
Мишка	Genius NetScroll 120	300
Корпус	Aerocool PGS CS-102 Black	599
Відео карта	GeForce GTX 1050 Ti	7 618
Всього: 19 666 грн		

Для мінімального функціоналу мережі потрібно буде щонайменше шість таких комп'ютерів. З цього виходить що $19\ 666 * 7 = 137\ 662$ грн. знадобиться тільки на комп'ютери.

Далі йдуть інші мережеві обладнання, про які я вже розповідав вище.

Таблиця 3.8 – Вартість основного мережевого обладнання

Пристрій	Марка і модель	Ціна грн.
Маршрутизатори	CISCO 1941	38 330
	WRT300N	1 957
Комутатори	2960-24TT	20 205
Камери відеоспостереження	Hikvision DS-2CE16D0T-IRF	1010
Сервер	Власна збірка	24 300

Підрахунок всієї вартості:

Ціна за два маршрутизатори Cisco 1941 становить 76 660 грн. Також три комутатори 2960-24TT коштують 60 615 грн. Дванадцять камер відеоспостереження обійдуться в 12 120 грн. І того, все основне мережеве обладнання обійдеться в: $76\ 660 + 1\ 957 + 60\ 615 + 12\ 120 + 24\ 300 = 175\ 652$ грн.

3.9 Висновки

В даному розділі було розроблено логічну і фізичну структуру мережі. Також обрано середовище для моделювання локальної мережі. Налаштування проводилося для забезпечення продуктивного функціонування закладу. Вдалося трішки заощадити коштів на збірці обладнання власноруч, а не купівлі вже готових варіантів.

Також не менш важливим було і забезпечення захищеного доступу до мережі. І це було реалізовано за допомогою Access Control List та звичайних доступі по паролю на комутаторах.

ВИСНОВКИ

В даній дипломній роботі я проектував локальну мережу для дитячої амбулаторії. В процесі розробки використав мережу з пропускнуою здатністю 100 Мбіт/с, та проаналізував вже відомі мережі в медицині.

Перелік виконаних досліджень:

1. Проаналізовано вже відомі рішення що до використання локальних мереж в медичних закладах. Після цього вибрано найбільш підходящу реалізацію під мою закладу.

2. При розробці мережі використано наступні технології: Virtual Local Area Network, DHCP сервер, технологія списків доступу Access Control List, та SSH.

3. Складено фізичну і логічну структуру мережі, а саме обрано невелику будівлю з трьома поверхами, для забезпечення усіх вимог амбулаторії.

4. Вибрано основне мережеве обладнання, яке забезпечує базове функціонування усієї мережі. Основними компонентами якої в більшості стали пристрої компанії Cisco, а саме: маршрутизатор Cisco 1941 та бездротовий WRT300N, комутатори 2960-24TT. Базовий набір комп'ютерів та сервер використовують власно зібрану «начинку» задля заощадження коштів.

5. Моделювання проводилося в середовищі Cisco Packet Tracer, в якому використовувалися відповідні пристрої в мережі.

					КвРКІ.170374.17.03.04 ПЗ	Арк.
						56
Зм..	Арк.	№докум.	Підпис	Дата		

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Павленко, О. М. Основні принципи та стандарти побудови локальних обчислювальних мереж. *Кооперація в системі общественного воспроизводства*. 2013. № 2. С. 267-270.
2. М. Феоктістов. Сайт Small HTTP Server. Наука та інновації. URL: <http://home.lanck.net/mf/srv/index.html> (дата звернення: 15.05.2021).
3. Верещага В. М., Конопацький Є. В., Павленко О. М. Визначення площі, обмеженої топографічною замкненою плоскою кривою. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*. 2015. № 20. С. 119-123.
4. Стасюк О.І., Гончарова Л.Л., Максимчук В.Ф. Методи організації інтелектуальних електричних мереж залізниць на основі концепції SMART Grid. *Інформаційно-керуючі системи на залізничному транспорті, науково-технічний журнал*, 2014. № 2. С.29 –37.
5. В. І. Романчук, С. В. Алексєєв, В. В. Червенець, Р. С. Колодій Аналіз структури мережевого трафіку та мережевих аномалій на прикладі сегмента локальної мережі кампусу Національного університету “Львівська політехніка” *Вісник Національного університету "Львівська політехніка"*. Львів, 2014. № 796 С. 157-163.
6. В. Олифер, Н. Олифер Компьютерные сети. *Принципы, технологии, протоколы*. 2016 СПб. С. 992.
7. Захист інформації в глобальній мережі. URL: <https://mirznanii.com/a/122769/zashchita-informatsii-v-globalnoy-seti/> (дата звернення: 22.05.2021).
8. Росляков, А.В. Виртуальные частные сети. *Основы построения и применения*. 2015. №54. С. 626.
9. Катаев, А. В. Информационные системы и модели оптимизации распределения заказов в партнерской сети виртуального предприятия. *Локальная сеть*. 2019. С. 599.

					КвРКІ.170374.17.03.04 ПЗ	Арк. 57
Зм..	Арк.	№докум.	Підпис	Дата		

10. Визавитин О. И. Практика защиты информации в Wi-Fi сетях на основе современных программно-аппаратных средств. *Молодой ученый*. 2016. № 5. С. 182–184.

11. Кононова В. О., Грибков С. В., Харкянен О. В. Оцінка засобів захисту інформаційних ресурсів. *Вісник Нац. ун-ту “Львівська політехніка”*. 2014. № 806. С. 99–105.

12. Network Mapper. URL: <https://nmap.org/> (дата звернення: 22.05.2021).

13. Пасічник В.В., Іванущак Н.М. Дослідження та моделювання складних мереж. *Східно-Європейський журнал передових технологій*. 2016. №44, С. 43-48.

14. Пасічник В.В., Іванущак Н.М. Структуризація та динамічні властивості складних комп'ютерних мереж. *Східно-Європейський журнал передових технологій*. 2017. №46, С. 16-21.

15. Опришко В.П. Регулювання режимів електропостачання в локальних системах microgrid. *Технічна електродинаміка*. 2016. № 4. С. 77-79.

16. Мельник А. О., Лихотоп Д. В., Гребеняк А. В. Вбудована локальна комп'ютерна Wi-Fi мережа з конфігуруванням за допомогою технології Bluetooth. *Вісник Національного університету «Львівська політехніка». Серія: Комп'ютерні системи та мережі*. — Львів : Видавництво Львівської політехніки, 2017. № 881. С. 66–86.

17. Яремчук Ю. Є. Алгебраїчні моделі асиметричних криптографічних систем. *Захист інформації*. 2014. №16. С. 68–80.

18. Марченко, В.Л. Продуктивність локальних мереж та апаратних засобів. *Вісник Хмельницького національного університету*. 2016. №4. С. 124-127.

19. Семенов Ю.А. Протоколы Internet. Энциклопедия. *Горячая линия – Телеком*. 2013. С. 110.

20. Курносое В.И., Буренин А.Н., Теоретические основы управления современными телекоммуникационными сетями. *Активное сетевое оборудование*. 2014. С. 18 – 20.

21. Романюк В.А., Лисенко О.І., Алексеева І.В., Романюк А.В., Новіков В.І. Підходи до розробки нової архітектури системи управління неоднорідними

					КвРКІ.170374.17.03.04 ПЗ	Арк. 58
Зм..	Арк.	№докум.	Підпис	Дата		

безпроводовими сенсорними мережами. *Математичні машини і системи*. 2017. № 2. С. 15–23.

22. Высочина О.С. Анализ систем мониторинга телекоммуникационных сетей. *ЗНТУ. Науковий журнал. Радіоелектроніка, інформатика, управління*. 2010. № 2. С. 139–142.

23. Чусавитин М.О., Чусавитина Г.Н., Чернова Е.В., Повитухин С.А. Обеспечение непрерывности итсервисов с использованием программно-определяемых систем хранения данных. *Фундаментальные исследования*. 2015. №11-3. С. 524-528.

24. Копейка О. В. Архитектура системы управления ИТ-инфраструктурой в современных Дата-центрах. *Наукові записки Українського науково-дослідного інституту зв'язку*. 2014. № 29. С.29- 37.

25. Сабанов А.А. Некоторые аспекты защиты электронного документооборота. *Connect! Мир связи*. 2012. № 7. С. 62–64.

26. Шрамко В.Н. Комбинированные системы идентификации и аутентификации. *PCWeek/RE*. 2004. №45. С. 75.

27. Петренко І.І., Убайдуллаев Р.Р. Пассивные оптические сети PON. *Архитектура и стандарты*. 2016, № 1.

28. Петренко І.І., Убайдуллаев Р.Р. Пассивные оптические сети PON. *Проектирование оптимальных сетей*. 2016. № 3.

29. Інформаційно-новинний сайт «Хабрахабр». /<https://habrahabr.ru> (дата звернення: 02.05.2021).

30. Інформаційний ресурс «Icline». URL: www.ic-line.ua/ (дата звернення: 08.05.2021).

31. Филиппов Е. В. Настольная книга 1С. *Эксперта по технологическим вопросам*. 2012. С. 247.

32. Канер Кем, Фолк Джек, Нгуен Енг Кек. Тестирование программного обеспечения. *Фундаментальные концепции менеджмента бизнес-приложений*. Київ. 2018. С. 544.

33. О. Ибе Сети и удаленный доступ. *Протоколы, проблемы, решения*. 2013. С. 336.

					КВРКІ.170374.17.03.04 ПЗ	Арк. 59
Зм..	Арк.	№докум.	Підпис	Дата		

34. Габец А.П., Козырев Д. В., Кухлевский Д. С., Хрусталева Е. Ю. Реализация прикладных задач в системе “1С:Предприятие 8.2”. *Основы Windows Communication*. 2013. С. 714.

35. Бойко В. Проектирование баз данных информационных систем. *Финансы и статистика*. 2012. С. 838.

36. Configuring SNMP and using the NetFlow. URL: <https://www.cisco.com/c/en/us/td/docs/iosxml/ios/netflow/configuration/12-4t/nf-12-4t-book/cfg-snmp-mib-mon-nf.html> (дата звернення: 14.05.2021).

37. Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки URL: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742 (дата звернення: 16.05.2021).

38. SIEM – Security Information and Event Management. URL: <https://amica.ua/siem-security-information-and-eventmanagement/> (дата звернення: 18.05.2021).

39. Янчук, В. О. Методика оцінювання стану захисту інформації локальних об’єктів системи електронного врядування. URL: <http://academy.gov.ua/ej/ej11/txts/10ivoseu.pdf> (дата звернення: 06.05.2021).

40. Толюпа С. В., Самохвалов Ю. Я., Цьопа Н. В. Комплексні системи захисту інформації спеціальних об’єктів та методика їх оцінки. *Сучасний захист інформації*. 2014. № 2. С. 25-27.

					КвРКІ.170374.17.03.04 ПЗ	Арк. 60
Зм.	Арк.	№докум.	Підпис	Дата		

Додаток Г

(Обов'язковий)

Основні налаштування активного мережевого обладнання

R1

```
Router>enable
```

```
Router#configure
```

```
Router(config)#hostname
```

```
Router(config)#hostname R1
```

```
R1(config)#int gigabitEthernet 0/1
```

```
R1(config-if)#ip add 192.168.1.1 255.255.255.0
```

```
R1(config-if)#no shut
```

```
R1#configure
```

```
R1(config)#int serial 0/0/0
```

```
R1(config-if)#ip add 192.168.2.1 255.255.255.252
```

```
R1(config-if)#no shutdown
```

```
R1(config)#router ospf 1
```

```
R1(config-router)#network 192.168.2.0 0.0.0.3 area 0
```

```
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

R2

```
Router>enable
```

```
Router#configure
```

```
Router(config)#hostname R2
```

```
R2(config)#int serial 0/0/0
```

```
R2(config-if)#ip add 192.168.2.2 255.255.255.252
```

```
R2(config-if)#no shutdown
```

```
R2(config)#int gigabitEthernet 0/1
```

```
R2(config-if)#ip add 192.168.3.1 255.255.255.0
```

```
R2(config-if)#no shutdown
```

```
R2(config)#router ospf 2
```

```
R2(config-router)#network 192.168.2.0 0.0.0.3 area 0
```

```
R2(config-router)#network 192.168.3.0 0.0.0.255 area 0
```

```
02:17:58: %OSPF-5-ADJCHG: Process 2, Nbr 192.168.2.1 on Serial0/0/0 from  
LOADING to FULL, Loading Done
```

S1

```
Switch>enable
```

```
Switch#conf
```

```
Switch(config)#hostname S1
```

```
S1(config)#vlan 10
```

```
S1(config-vlan)#name Medic
```

```
S1(config-vlan)#vlan 20
```

```
S1(config-vlan)#name Cameras
```

```
S1(config-vlan)#vlan 30
```

```
S1(config-vlan)#name Patient
S1(config)#interface range f0/3-4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#exit
S1(config)#interface range f0/11-13
S1(config)#interface range f0/11-13
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 20
S1(config-if-range)#exit
S1(config)#int fa0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
S1(config-if)#exit
S1(config)#exit
S1(config)#interface f0/10
S1(config-if)#switchport mode dynamic desirable
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed
state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed
state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed
state to up
```

```
S2
Switch>enable
Switch#conf
Switch(config)#hostname S2
S2(config)#vlan 10
S2(config-vlan)#name Medic
S2(config-vlan)#vlan 20
S2(config-vlan)#name Cameras
S2(config-vlan)#vlan 30
S2(config-vlan)#name Patient
S2(config-vlan)#exit
S2(config)#int
S2(config)#interface range f0/2-4
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#exit
S2(config)#interface range f0/11-13
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 20
```

```
S2(config-if-range)#exit
S2(config)#interface f0/24
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
```

```
S3
Switch>enable
Switch#configure
Switch(config)#hostname S3
S3(config)#vlan 10
S3(config-vlan)#name Medic
S3(config-vlan)#vlan 20
S3(config-vlan)#name Cameras
S3(config-vlan)#vlan 30
S3(config-vlan)#name Patient
S3(config-vlan)#exit
S3(config)#interface range f0/11-16
S3(config-if-range)#switchport mode access
S3(config-if-range)#switchport access vlan 20
S3(config-if-range)#exit
S3(config)#interface f0/2
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 30
S3(config-if)#exit
```

Назва документа: Космина_Локальна комп'ютерна мережа для дитячої амбулаторії

Кількість сторінок: 59

Кількість слів: 11635 Кількість символів: 87696 Розмір файлу: 1.20 MB

ID файлу: 1008275340

8.82%**Схожість**

6.15% Джерелаз Інтернету 25

Найбільша схожість: 7.02% з джерелом з Бібліотеки (ID файлу: 1008248421)

7.96% Джерелаз Бібліотеки 66

..... Сторінка 61

..... 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 5

Anti-Plagiarism v-15.257**Максимальное совпадение с одним документом 1.0%****Словари проверки: en_US, ru_RU, ua_UA. Ошибок в документах: 8%**

ID: 92380 Название: Локальна комп'ютерна мережа для дитячої амбулаторії Добавлено в БД: 2021-06-06 Авторы: Космина Ю.І. Руководители: Лисенко С.М. Консультанты: Опоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	65325	725	1285 (2%)	19 (3%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Космина Юрій Іванович

Тема: Локальна комп'ютерна мережа для дитячої амбулаторії

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень 3 Кількість сторінок записки 97

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є проектування локальної комп'ютерної мережі для дитячої амбулаторії.

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: В першому розділі кваліфікаційної роботи проведено дослідження предметної області (проаналізовано теорію проектування комп'ютерних мереж) та виконано постановку задачі дослідження. В другому розділі кваліфікаційної роботи проведено аналіз засобів проектування комп'ютерних мереж. В третьому розділі кваліфікаційної роботи виконано реалізацію локальної комп'ютерної мережі для дитячої амбулаторії, зокрема спроектовано карту локальної мережі для дитячої амбулаторії, топологічну схему корпоративної локальної мережі.

4. Позитивні сторони роботи: висока практична цінність проведеної роботи.

5. Негативні сторони роботи: не достатньо описане програмне забезпечення, яке необхідне для функціонування інфраструктури для дитячої амбулаторії.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: -

9. Оцінка дипломної роботи: добре

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) доцент кафедри інженерії програмного забезпечення Хмельницького національного університету, к.т.н., доцент, Гурман І.В.

"19" травня 2021 р.

 (підпис)

Завідувачу кафедри КІСП
д-ру техн.наук, проф. Говорущенко Т. О.

Космини Ю.І.

ІІБ здобувача вищої освіти

ФПКТС, 4 курсу, групи КІ-17-3

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 наявність плагіату ознайомлений(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.

04.06.2021

дата

підпис

РІШЕННЯ ЕКСПЕРТНОЇ КОМПІСІЇ
КАФЕДРИ 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: Локальна комп'ютерна мережа для дитячої амбулаторії

Автор: Космина Юрій Іванович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Лисенко Сергій Миколайович доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. 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. 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 письмової роботи та ідентичності друкованої та електронної 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 (наступного року) після 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.	

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) окремі виявлені збіги є загальноживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-20 джерелами на один фрагмент речення;
- 3) в якості запозичень в окремих місцях системою зафіксовано частини коду, які є загальноживаними для великої кількості задач і не можуть розглядатися як об'єкт авторських прав і, відповідно, їх порушення;
- 4) найбільша частина збігів, а саме 7.02%, припадає на титульну сторінку і рамки документу, які використовуються для оформлення пояснювальної записки.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ідентичності/схожості, складає 8.82% і адресується до 25 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи

Гарант ОП

Завідувач кафедри КІСП

С. М. Лисенко

С. М. Лисенко

Т. О. Говорущенко