Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет прикладних інформаційних технологій та електроінженерії
(назва факультету)
Автоматизації технологічних процесів і виробництв
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

На здобуття освітнього ступеня

магістр
(освітній ступінь)

на тему: **«Розробка та дослідження інформаційно-управляючої системи Костільницької ЗОШ І-ІІ ступенів»**

Виконав: студент (ка) 6 курсу, групи КАм-61
спеціальності 151
“Автоматизація та комп’ютерно-інтегровані технології”
(шифр і назва спеціальності (напряму підготовки))

(підпис) Литвиненко І.М (прізвище та ініціали)

Керівник (підпис) Коноваленко І.В (прізвище та ініціали)

Нормоконтроль (підпис) Козбур І.Р (прізвище та ініціали)

Рецензент (підпис) Дідич І.С (прізвище та ініціали)

м. Тернопіль – 2020

АНОТАЦІЯ

Кваліфікаційна робота складається з пояснювальної записки та графічної частини . Об’єм пояснювальної записки складає 72 друкованих сторінок формату А4 , об’єм додатків – 21 друкованих сторінок формату А4. Кваліфікаційна робота складається з шести розділів, в яких нараховується 18 рисунків та 16 таблиць з даними. В роботі використано 29 літературних джерел.

Мета роботи - це розробка локальної мережі школи на основі існуючого апаратного і програмного забезпечення, забезпечення потрібної швидкості передачі інформації та спільного використання ресурсів, а також як повпливали інформаційні системи в управлінні школами.

Пояснювальна записка складається з шисти розділів.

В першому розділі описано спосіб побудови локальної мережі, який було обрано і чому саме він був обраний, вказано майбутні стадії та етапи розробки. Описано призначення даної мережі, вимоги до програмного, апаратного забезпечення та ведення документації та технічне завдання.

В другому розділі дається загальний опис задачі та її специфічні особливості. Здійснюється розробка схеми фізичного розташування кабелів та вузлів. Також тут здійснено обґрунтування вибору операційних систем, програмного забезпечення та обладнання для мережі.

В третьому та четвортому розділі описано процедуру тестування мережі при вводі її в експлуатацію. Також описано використання тестових програм та інструкцію з інсталяції та конфігурації програмного забезпечення. Розглянуто і створено модель мережі.

В пятому розділі було проведено науковий дослід інформаційних технологій у школах, та було розглянуто що внесли інформаційні системи в управління школами, та з якими проблемами вони зіткнулись.

В шостому розділі було описано охорону праці та безпуке в надзвичайних ситуаціях.

Ключові слова: ЛОКАЛЬНА КОМП’ЮТЕРНА МЕРЕЖА, КОМУТАТОР, ДОСТУП ДО ІНТЕРНЕТ, D-LINK, UBUNTU, ШКОЛА.

SUMMARY

The qualifying work consists of an explanatory note and a graphic part. The volume of the explanatory note is 72 printed pages of A4 format, the volume of appendices is 21 printed pages of A4 format. The qualification work consists of six sections, in which there are 18 figures and 16 tables with data. 29 literary sources were used in the work. The purpose of the work is to develop the local network of the school on the basis of existing hardware and software, to ensure the required speed of information transfer and resource sharing, as well as how information systems have affected the management of schools. The explanatory note consists of six sections. The first section describes the method of building a local area network, which was chosen and why it was chosen, indicates the future stages and stages of development. The purpose of this network, requirements for software, hardware and documentation and terms of reference are described. The second section gives a general description of the problem and its specific features. The scheme of physical arrangement of cables and knots is developed. The selection of operating systems, software and equipment for the network is also substantiated here. The third and fourth sections describe the procedure for testing the network during its commissioning. The use of test programs and instructions for installing and configuring software are also described. The network model is considered and created. In the fifth section, research on information technology in schools was conducted, and it was considered what information systems have contributed to school management, and what problems they have faced. Chapter 6 described occupational safety and health in emergencies.

Keywords: LOCAL COMPUTER NETWORK, SWITCH, INTERNET ACCESS, D-LINK, UBUNTU, SCHOOL.

ЗМІСТ

ВСТУП

Сьогодні, який ми називаємо інформаційним століттям, оскільки багато технологічних розробок було пережито; найбільший ризик, на який може піти організація, - це залишатися нечутливим до змін. Багато значущих факторів, такі як постійний розвиток інформаційних технологій, обмін інформацією, зростаючі очікування суспільства, сучасне управління сприйняттям та застосуванням змушують організації у всьому світі розробляти нові програми, щоб вижити. Через свою пріоритетність у сучасному суспільстві Інформаційні технології також досягли першочергового рівня в освіті.

В сфері освіти засобам комунікації приділяється велика увага, як і системам передачі даних на великі відстані. Індустрія глобальних мереж розвивається дуже швидко і займає домінуюче положення в роботі організацій. Локальні мережі є важливою складовою роботи сучасних підприємств, забезпечуючи засоби передачі даних між працівниками та їх оперативний зв’язок.

Впровадження локальних мереж мотивується в основному підвищенням ефективності праці і продуктивності персоналу.

У процесі виконання кваліфікаційної роботи було проведено загальний аналіз інформаційних технологій у школах, розробка комп'ютерної мережі, на базі що вже існує (апаратного і програмного забезпечення) для, Костільницької ЗОШ І-ІІ ст. Бучацького р-ну а також підключення, що відповідає сьогоднішнім технічно-науковим вимогам.

1 АНАЛІТИЧНА ЧАСТИНА

1.1 Аналітичний огляд існуючих рішень

В наш час стрімко розвиваються різні види технологій, а саме перше місце по розвитку займають інформаційні технології. Появляються нові прилади, програмні засоби та багато іншого, що полегшує роботу людини, та збільшує обсяг виконаних тих чи інших завдань. [8]

Аналогічно, з збільшенням продуктивності різних програм та приладів, випливає потреба в збільшенні пропускної здатності, та швидкодії між структурних з'єднань. Тобто виникає нагальна потреба в модернізації мережного обладнання, так як об'єм передавання інформації стрімко зростає з кожним днем.

Для передачі даних використовуються різні середовища передачі, зокрема різні кабельні системи.

Застарілими системами є системи з використанням кабельних мереж на коаксіальному кабелі, які на даний час практично не використовуються за виключенням мереж кабельного телебачення.

Скручена (вита) пара.[3]

Кабель "вита пара" - це провід з 4-х чи 8-и проводів, що скручені між собою попарно. Цей кабель буває одножильний і багатожильний (залежно від типу провода), екранований і звичайна (екранований зменшує вплив зовнішніх факторів). Кабель "вита пара" - Twisted Pair (TP): UTP - назва для неекранованого (unshielded), а STP - для екранованого (shielded). UTP - підрозділяється на рівні (напр. Рівень 1, 2,...) і класи (A,B,C...) в залежності від можливості передавати дані.

Категорії кабелів представлено в таблиці 1.1

Таблиця 1.1 - Категорії, частоти та застосування витої пари

Частота, МГц	Застосування	Категорії
0,1	аналогові телефони	1
1	цифрові телефони, ISDN	2
16	10baset (Ethernet)	3
20	TokenRing	4
100	100BaseTX	5
125	1000BaseTX	5e
200 (250)	1000BaseTX	6
600	1000BaseTX	7

Екранований кабель відмінний від неекранованого не лише більшою вартістю. При правильному заземленні екрана він забезпечує кращу електромагнітну захищеність кабельної системи від джерел пошкоджень. Однак некоректне заземлення екрана може призвести до зворотнього результату.

Крім цього, існує відмінність в оболонці кабеля - вона може бути полівінілхлоридною чи тефлоновою.

Температура при роботі і зберіганні:[8]

35... +60 - для кабеля в полівінілхлоридній оболонці;

55... + 200 - для кабеля в тефлоновій оболонці.

Температура при монтажі:

20... +60 - для кабеля в полівінілхлоридній оболонці;

36... +200 - для кабеля в тефлоновій оболонці.

Відносна вологість:

0... 100% для кабеля в полівінілхлоридній оболонці допускається випадкова конденсація.

Можливість застосування на відкритому повітрі:

– заборонено - для кабеля в полівінілхлоридній оболонці;

– дозволено - для кабеля в тефлоновій оболонці.

Для підключення витої пари використовується затискачі RG-45 або RG-21 "telco"

Волоконно-оптичний кабель [5]

Найперспективнішим середовищем передачі є забезпечення швидкісної передачі інформації на великі відстані є оптичний кабель.

Оскільки оптичний кабель використовується як середовище передачі в оптичному кабелі, це тонкий скляний або пластиковий дріт товщиною 8,3-100 мкм, який може надати скорість передачі даних більше 40 Гбіт/с. Оптичне волокно покрите скляною оболонкою, яка має коефіцієнт відбиття, відмінний від оптичного волокна. Скляна оболонка відображає світло, і веде його вздовж оптичного волокна. Внутрішня оболонка скла забезпечує необхідну жорсткість і стійкість до розтріскування, перегріву або переохолодження. Гель та армована серцевина надати більше укриття від механічних впливів та впливу навколишнього середовища. Кабель може містити світло провідне оптичне волокно, але зазвичай їх кілька.

Сигнал на оптичному волокні може поширюватись таким чином, тобто у вигляди досить тонкого пучка або у вигляді декількох пучків. Світловод одномодового кабелю набагато тонші волокна ніж в багатомодового кабелю. Сигнал в одномодовому кабелі генерується лазерним джерелом світла. Вибираючи лазерний діод в якості джерела світла , його можна перемикати з частотою в кілька десятків МГц, забезпечуючи дуже високу швидкість цифрових сигналів.

Оптичне волокно достатньо гнучке, що може дозволити розміщувати оптоволоконні кабелі майже по тому ж каналі, що й скручена пара. За належної технології виготовлення оптоволоконного кабелю , навіть якщо оптоволоконний кабель скручений, світло може поширюватись вздовж оптичного волокна і не випромінюватись назовні. Близько з високою швидкістю передачі, оптоволокно є значно тонкішим і легшим від звичайного. Характеристики кабелю наведені в

таблиці 1.2. Перевагою цього кабелю включають стійкість до електронних перешкод, що дозволяє використосувати його з джерелами сильного електромагнітного поля, такими як електрозварювальний апарат.

Ціна оптоволоконного обладнання та його монтаж на сьогоднішній день не надто відрізняються від вартості мідних кабелів, тому зростає популярність рішень на базі волоконно-оптичних кабелів.

Таблиця 1.2 - Характеристики волоконно-оптичних кабелів

Характеристика	одномодовий	багатомодовий
діаметр серцевини	10 мкм	50; 62,5; 100; 140 мкм
генератор світла	лазер	діоди або лазер
довжина хвилі	1,3; 1,55 мкм	1,3; 0,85 мкм
смуга пропускання	2 ГГц	800-900 МГц
ширина смуги пропускання	залежить від довжини кабеля	
затухання сигналу	0,7 дБ/км	0,5-0,7 дБ/км
макс. Відстань	110 км	до 5 км

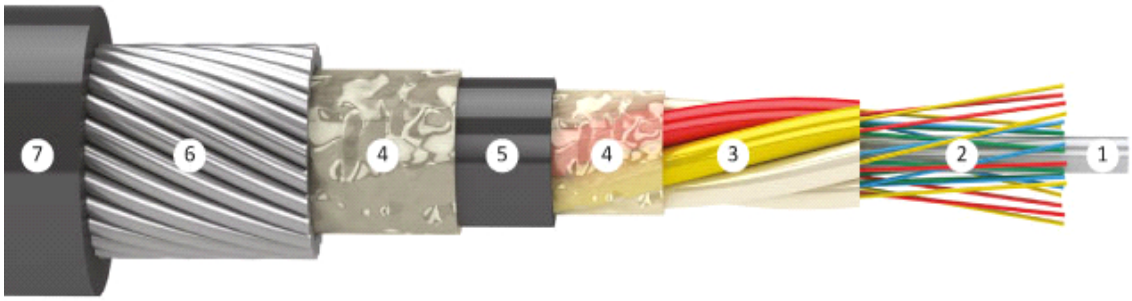


Рисунок 1.1 - Конструкція кабелю

1. Центральний силовий елемент.
2. Оптичне волокно.
3. Оболонка оптичного модуля.
4. Гідрофобний заповнювач.
5. Проміжна оболонка з полімерного матеріалу.

6. Броня із сталевого дроту.
7. ПВХ оболонка.

Виходячи з вище наведених прикладів топологій з’єднання локальних та глобальних мереж, та різновидів кабелів, пропонується для вирішення питання, що постає в данній кваліфікаційнійроботі, використовувати топологію розширена зірка, в якій буде використано скручену пару UTP 5e.

Кодування логічне 8B/10B. Використовується швидкість від 800Мбіт/с до 1Гбіт/с при тактовій частоті до 1,25ГГц.

1000BaseLX – оптичне волокно. Довжина хвилі лазерного датчика становить 1310нм. Для міжміського зв’язку. [3]

1000BaseLH – оптоволокно з довжиною хвилі 1310 нм. Використовується для зв’язку на дуже великі відстані.[3]

1000BaseT – відстань передачі на витій парі категорії 5e, 6,7 становить 100м і знаходиться в повно дуплексному режимі передач. [3]

Виходячи з описаних стандартів для мережі обрано специфікацію 1000BaseT стандарту технології Gigabit Ethernet.

1.2 Технічне завдання

1.2.1 Найменування та область застосування

Темою кваліфікаційного проекту є “Розробка та дослідження інфлрмаційно-управляючої системи Костільницької ЗОШ І-ІІ ст”.

Даний проект розробляється для покращення обслуговування та роботи Костільницької ЗОШ І-ІІ ст. Бучацького р-ну. Розроблена мережа повинна забезпечити доступ до інформації учням та вчителям школи, зокрема доступ до мережі Інтернет, а також покращити електронний документообіг в школі. Також повинна сприяти покращенню навчання учнів в школі інформаційним технологіям і добавити інтерактивності в вивчення інших предметів.

1.2.2 Призначення розробки

Проект мережі буде застосований для Костільницької ЗОШ І-ІІ ст. Бучацького р-ну. Впровадження цього проекту спрямоване на створення локальної мережі з забезпечення захисту та високої швидкості передачі даних. Також має забезпечуватися доступ до мережі Інтернет як для вчителів так і для учнів школи.

1.2.3 Вимоги до програмного і апаратного забезпечення

Для створення майбутньої мережі, необхідне наступне апаратне забезпечення:

– Персональний комп’ютери, обладнані мережними платами з пропускною здатністю в100- 1000 Мбіт/с;

– Інтелектуальні комутатори та маршрутизатори, які підтримували б швидкість передачі даних в 1000 Мбіт/с.

Що до програмного забезпечення. На всіх машинах повинна бути однакова операційна система. Тобто, одним з варіантів може бути Windows 10, тому що вона добре себе зарекомендувала в роботі з мережами та Інтернетом. Також є можливим варіант встановлення операційної системи Linux, яка не потребує ліцензії, є безкоштовною, а саме головне те що Linux має самий менший процент по ураженні вірусними програмами. Інші програмні засоби, які можливо стосуватимуться роботи фірми, чи до коректності роботи мережі, розглядаються на місці.

1.2.4 Вимоги до документації

Потрібно вказати вимоги до документування мережі, на основі єдиних стандартів. Також потрібно розробити (адаптувати) стандартний бланк(и) для документування мережі. Зокрема мають бути розроблені фізична та логічна

топології, створено кабельний журнал з маркованими входами та виходами та розроблено таблицю IP адресації.

1.2.5 Технічні показники

Рекомендовані техніко-економічні показники:

1 Логічна топологія - гібридна

2 Тип мережі - Gigabit Ethernet

3 Швидкість передачі інформації - 1000 Мбіт/с

4 Кількість серверів - 2

5 Програмне забезпечення - бекоштовне

6 Тип під’єднання до Інтернет - ADSL

1.2.6 Стадії та етапи розробки

При організації мережі, всі роботи можна поділити на 4 етапи:

– Збір інформації.

– Створення і затвердження проекту.

– Фізична реалізація мережі.

– Експлуатація та моніторинг мережі.

– При зборі інформації, необхідно визначитись у наступних питаннях:

– Який тип організації і чи планується її зростання

– Чи є існуючі комп’ютерні мережі

– Побажання керівництва

– Яке програмне забезпечення буде використовуватись в мережі

– Побажання користувачів

– Сума, яка планується до вкладання в мережу

– Визначити тип мережі, топологію, провідники та інше обладнання 1-го рівня

– Визначити необхідність повторювачів, концентраторів для робочих груп

– Визначити кількість і потребу магістралей (вертикального кабелювання) і горизонтальних кабелів

– Кількість і потреба в головному та проміжних комутаційних вузлах

– Визначити необхідність встановлення мостів, комутаторів або заміни іншого обладнання на них

– Визначити необхідність встановлення маршрутизаторів

– Тип підключення до глобальної мережі

– Наявність спеціального обладнання для підключення до глобальних мереж

– Необхідний захист і процедури керування

1.2.7 Порядок контролю та прийому

Контролюється при побудові мережі декілька етапів :

– розробка проектної частини;

– розробка проектної документації;

– закупка обладнання для мережі;

– прокладка та монтаж мережі;

– запуск та експлуатація мережі;

При прийомці проекту перевіряється наявність усієї документації , схем та планів. При прийомі в експлуатацію мережі виконується перевірка наявності та функціонування усього необхідного обладнання. Для тестування використовуються стандартні утиліти такі як ping, tracert, ipconfig.

2 ТЕХНОЛОГІЧНА ЧАСТИНА

2.1 Постановка задачі на розробку проекту, для якого створюється проект мережі

Метою даної кваліфікаційної роботи є розробка та дослідження інформаційно-управляючої системи Костільницької ЗОШ І-ІІ ст. Бучацького р-ну.

Основна задача розробки полягає в забезпеченні достатньої швидкодії як окремих вузлів, так і всієї мережі із врахуванням кадрових та фінансових можливостей та керування доступом до інформаційних ресурсів ЛКМ.

Школа розташована в с. Костільниця, вул Шкільна 12 і займає двоповерхову будівлю, план якої представлено в (листі 1)

Розвиток сучасних технологій, вимоги сьогодення щодо покращення процесу навчання поставили задачу побудови локальної комп’ютерної мережі з доступом до інтернет в даній школі.

Для ефективної реалізації нашого завдання, необхідно провести детальний аналіз структури приміщень школи, де і буде розміщуватися ЛКМ.

Реалізація запропонованого проекту збільшить продуктивність праці, скоротити час на обробку інформації, забезпечити оперативний інформацією між комп’ютерами, скоротити документообіг у школи, забезпечити доступ школі до глобальної інформаційної систем, що знаходяться в Internet, покращити рівень проведення уроків в школі, добавить в них інтерактивність через використання різних інформаційних ресурсів.

Процес створення обчислювальної локальної мережі повинен містити в собі не тільки рішення загальних задач побудови й організації мережі в школі, але і комплексно забезпечувати рішення проблем, які виникають з появою мережі в школі і її експлуатації. До них відносять організацію доступу до інформації і її захист, забезпечення взаємодії клієнтів мережі з Internet.

2.2 Опис та обґрунтування вибору логічного та фізичного типу мережі

Топологія «розширена зірка». Складається при об’єднанні декількох сегментів мережі, кожен сегмент організований відповідно до «зіркової» топології. Між сегментний зв’язок здійснюється між концентратором і комутатором, один з них є центральний.

Деревовидна або ієрархічна топології. Подібні до топології (розширена зірка), але різниця полягає в тому, що не всі сегменти під’єднанні до центрального концентраторів, чи комутаторів, створюючи окремі гілки дерева.

Топологія «подвійного кільця» відрізняється від «кільцевого» тим, що фізичне з’єднання створює два кільця і кожен ПК одночасно підключається до двох кілець. Це дозволяє високу надійність, гнучкість в використанні і обслуговуванні.

Характеристика певної топології полягає в тому, що кожен мережевий пристрій безпосередньо підключений до всіх інших пристроїв.

Нерегульована топологія немає точних визначених правил підключення мережевих пристроїв. Таку топологію допускати не варто.

Комірчаста топологія. Усі ПК підключено з іншим, зазвичай за допомогою радіо модемів, які знаходяться в зоні дії йо зв’язку.[8]

Фізична і логічна топологія незалежні одна від одної. (продовження у додатоку 1)

Детально схеми IP адресації та поділу на віртуальні мережі наведено в (листі 3).

В результаті аналізу логічної та фізичної топологій мережі для подальшого впровадження необхідно підібрати наступне мережеве обладнання, представлене в таблиці 2.1.

Підмережева маска вибрана для IP адрес класу C 255.255.255.0.

Таблиця 2.1 – Потреби в обладнанні по його типах

№ п.п.	Назва	Кількість, шт

Продовження таблиці 2.1

1.	Керований комутатор 16 портів	1
2.	Керований комутатор 24 порти	2
3.	Точка доступу	1
4.	Сервери мережі	2
5.	Робочі станції	41

2.3 Розробка схеми фізичного розташування кабелів та вузлів

2.3.1 Типи кабельних з’єднань та їх прокладка

Перед вибором типу кабелю було враховано усі особливості самого об’єкту, для якого розробляється мережа та характеристики кабельної системи розроблюваної мережі. Кабельна лінія складає фундамент будь-якої комп'ютерної мережі. Від її якості залежать всі основні властивості мережі. (продовження в додатку 2)

При монтажі скрученої пари необхідно особливо відзначити, що існує два різновиди з’єднань кабелів – пряме (див. рис. 2.4) (контакти 1-2 і 3-6 першого роз’єми з'єднуються з контактами 1-2 і 3-6 другого) і перехресне (див. рис. 2.5) (контакти 1-2 і 3-6 першого роз’єми з'єднуються з контактами 3-6 і 1-2 другого). Базовим для під’єднання є роз’єм RJ-45 в який в залежності від призначення встановлюються провідники в певному порядку.

Рисунок 2.4 Пряме з’єднання

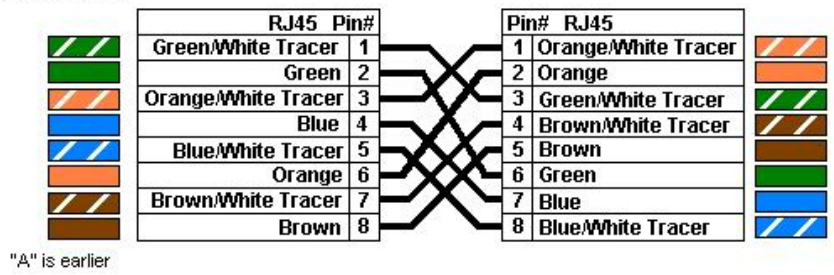


Рисунок 2.5 - Перехресне з’єднання

Фізичний зміст тут досить простий - передавач одного пристрою повинний бути з'єднаний із приймачем іншого. Тому, для з'єднання однакових пристроїв (наприклад, двох комп'ютерів) потрібно використовувати перехресний кабель. У габах, комутаторах і подібному устаткуванні конструктивно закладена перехресне розведення, і для їхнього з'єднання з комп'ютером використовується прямий варіант кабелю. [5]

Для даної мережі з врахуванням майбутніх затрат і можливостей модернізації мережі обрано кабелю скрученої пари категорії 6.

Прокладка кабельного з’єднання у кабінетах відбувається по плінтусу в захисних коробах, міжкабінетні - прокладені через спеціальні отвори в стінах на рівні плінтуса. З’єднання між поверхами виконується через кабельні шахти.

3 КОНСТРУКТОРСЬКА ЧАСТИНА

3.1 Будова вузлів та необхідність їх застосування

Топологія з’єднання нами вибрана гібридна. Використовуємо у локальній мережі 2 сервери, 41 робочу станцію, 3 комутатори, 1 безпровідний маршрутизатор.

В мережі буде один головний комутаційний вузол, розташований в окремій кімнаті (серверній) на 2 поверсі, що пов’язано з специфікою призначення кабінетів та кабелів. В комутаційному вузлі буде розташовано комутатор, модем, 2 сервери і робоче місце адміністратора мережі.

Також в комутаційному вузлі буде розташовано комутаційну шафу, яка допоможе оптимізувати кабельне господарство.

Проміжні комутаційні вузли розташовуються в настінних комутаційних шафах, відповідно на 1 поверсі в кабінеті іноземних мов та на 2 поверсі в кабінеті інформатики.

Також вузлами мережі є робочі станції та сервери мережі і інше активне комутаційне обладнання.

В приміщеннях буде розташовано комутаційні шафи розміром 12U CMS 12U, UA-MGSWL1235B (див. рис. 3.1).

Рисунок 3.1 – Комутаційна шафа CMS 12U

В серверній буде розташована напідложна версія комутаційної щафи висотою 24U (див.рис.3.2) CMS 19" 24U, UA-MGSE2468MB. В даній шафі буде монтуватися мережеве обладнання, зокрема головний комутатор, сервери та модем для доступу до інтернет.

Рисунок 3.2 – Напідложна шафа, висотою 24U UA-MGSE2468MB

3.2 Обґрунтування вибору обладнання для мережі (пасивного та активного).

Виходячи із потреб обладнання для мережі описаних в таблиці 3.1 виконаємо підбір необхідного обладнання для мережі.(продовження в додатку 3)

Для мережі вибрано сервери Dell PowerEdge T20 (T20v04) (див. рис. 3.3) виходячи із технічних характеристик, зокрема процесорів і жорстких дисків.

Рисунок 3.3 - сервери Dell PowerEdge T20

В якості комутаційного обладнання для мережі будуть використовуватися інтелектуальні комутатори. Дані пристрої набули досить широкого поширення і мають ряд переваг, не вимагаючи, при цьому, затрати значних ресурсів та часу на встановлення.

В даній мережі будуть використовуватися 1 16-ти портовий комутатор , і 2 24 портові гігабітні комутатори.

Для порівняння взято комутатори різних фірм, проте важливим фактором при виборі було дотримання технології Гігіабіт Ethernet та керованості комутаторів. Також важливим фактором є підтримка технології віртуальних мереж, оскільки в даному проекту передбачається їх використання, як було описано вище, зокрема стандарту 802.1Q.

Порівняльні характеристики вибору 16 портових гігабітних комутаторів наведені в таблиці 3.2.

Таблиця 3.2 – Порівняльні характеристики комутаторів

№ п/п	**Характеристики обладнання**	Модель пристрою			
		TP-LINK TL-SG1016D	D-Link DGS-1100-16.	TP-Link TL-SG2216 WEB	Cisco SRW2016
1.	Кількість портів	16	16	16	16

Продовження таблиці 3.2

2.	Швидкість портів	10/100/ 1000	10/100/ 1000	10/100/ 1000	10/100/ 1000
3.	Автовизн. швидкості	так	так	так	так
4.	Інтерфейс передачі даних	10/100/1000 Base-T RJ-45	10/100/1000Base-T RJ-45	10/100/1000Base-T RJ-45	10/100/1000Base-T RJ-45
5.	MAC-адреси, Кбайт	8	8	8	8
6.	Web інтерфейс	Ні	так	так	так
7.	Гарантія, міс	12	12	24	60

В результаті проведенного аналізу обрано коммутатор D-Link DGS 1100-16 (див.рис.3.4), який забезпечить високу швидкість та можливість керування мережею в цілому при відносно не високій ціні.

Рисунок 3.4 - Комутатор D-link DGS-1100-16

Комутатори серії DGS-1100- це недорогі рішення для SOHO і малих та середніх підприємств, також для організаційних ділових мереж таких як філії та бізнес-приміщення де потрібне просте управління. Усі моделі відправляються в малій металевій стільниці і оснащена 5, 6, 18 або 24 гігабітним портам. [16]

Комутатор DGS-1100 є стандартом IEEE802.3az Energy Efficient Ethernet, низьке споживання енергії при маленькому трафіку. Встановлення обладнання EEE забезпечує малим і середнім бізнесам економію грошей, зменшуючи витрати, пов'язані із придбанням охолоджуваного обладнання. Свіч серії DGS-1100 підтримує технологію D-Link Green, яка надає автоматичне зменшення

споживання енергії. Якщо автоматично визначено, що довжина підключеного кабелю менше 20-ти метрів, цей комутатор змешнить споживання енергії. Крім того, комутатор визначатиме стан підключення кожного порту та автоматично відключатиме живлення неактивних портів [16].

Перемикачі EasySmart підтримує управління через утиліти SmartConsole або Web-інтерфейс. Утиліта SmartConsole позволяє користувачам знайти перемекачі лінійки D-Link Smart в тому ж розділі мережі L2. Для використання цієї утиліти немає необхідності змінювати IP-адрес комп’ютера, і ви можете легко встановити комутатори серії Smart. На екрані зображений комутатор, що належить до того ж сегменту мережі і підключений до локального комп'ютера користувача, і доступ до нього може бути завжди. Користувачі можуть отримати доступ до розширеної конфігурації та основних налаштувань виявленого пристрою, таких як зміна пароль і оновлення програмного забезпечення. Зручний графічний веб-інтерфейс дозволяє адміністраторам мережі віддалено керувати мережею на рівні порту [16].

Для забезпечення кращої сумісності та зручності керування прийнято рішення про використання комутаторів одного виробника і однієї серії з різною кількістю портів, таким чином окрім описаного для мережі використовуються комутатори DGS-1100-24.

Радіомережеву точку доступу - маршрутизатор обрано для даного проекту виходячи із порівняльної таблиці 3.3

Таблиця 3.3 - Вибір маршрутизатора (точки доступу)

Модель	Linksys E2500	D-Link DIR-615s	TPLINK TL-WR840N
1	2	3	4
Тип	Для дому і малого офісу	Для дому малого офісу	Для дому і малого офісу
WAN-порт	Ethernet	Ethernet	Ethernet

Продовження таблиці 3.3

Інтерфейси	4 x 100M Ethernet WAN-порт	4 x RJ-45 10/100BASE-TX	4 x Fast Ethernet RJ-45
Бездротові можливості	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
Підтримує протоколи	—	PPTP, L2TP, IPsec, PPPoE	PPTP, L2TP, IPsec, PPPoE
Кількість антен	3, внутрішні	2, знімні	2, знімні
Функції безпеки	WEP, WPA, WPA2 128-біте шифрування Фільтрація по MAC адресі	WEP- 64/128-біт WPA/WPA2 NAT Stateful (SPI) Фільтр MAC/IP-адрес DMZ	Захист від атак DoS Wi-Fi Protected Access (WPA2-PSK, WPA-PSK) 64- и 128-разрядне шифрування (WEP)
Інші функції	—	WAN: Static IP Dynamic IP PPPoE L2TP	Підтримує Quality of Service (QoS) на базі Wi-Fi Multimedia

Розглянемо точку доступу - маршрутизатор D-Link DIR-615s, зображений (на рисунку 3.5).

Даний пристрій має функції роутера та підтримує радіомережі стандарту 802.11a/b/g/n, що дає додаткові можливості по підключенню мобільних клієнтів на 2 поверсі школи.

Детальні технічні характеристики обраного модему можна отримати з офіційного сайту D-Link.

Бездротовий модем 802.11n D-Link DIR-615 надає хорошу якість бездротового сигналу, ніж існуючою технологія 802.11g. Маршрутизатор DIR-615 покращує продуктивність існуючої домашньої мережі та організувати спільний доступ до інтернету, документації, файлів. 802.11n D-Link не тільки

збільшує діапазон роботи, но і дозволяє підключатися до існуючих бездротових пристроїв 802.11g і 802.11b. [18]

Рисунок 3.5 - Точка доступу-маршрутизатор D-Link DIR-615

Просте встановлення

За допомогою майста з швидкого встановлення D-Link, користувач може налаштувати бездротовий DIR-615 за декілька хвилин. Покрокова інструкція позволяє самому встановити Інтернет-з'єднання, та виконати налаштування.

Крім того цей роутер оснащений (SPI і NAT) для запобігання дудос атак.[18]

Для забезпечення доступу до Інтернет використовується ADSL модем

Вибір виконувався виходячи із порівняльної таблиці 3.4.

Таблиця 3.4 - Порівняння характеристик ADSL модемів

Виробник	**ZyXEL**	**ASUS**	**D-Link**
Модель	Zyxel Keenetic Extra II	Asus DSL-N12E	D-Link DSL-2650U
Інтерфейси	Ethernet 10/100BaseT, RJ-45, ADSL, RJ-11, USB, USB 3G, USB 4G	Ethernet 10/100BaseT, RJ-45, ADSL2+, RJ-11, USB 2.0	Ethernet 4x10/100BaseT, RJ-45, 1 порт ADSL с раз'ємом RJ-11, 1x802.11n

Продовження таблиці 3.4

Індикатори	- активне з’єднання - електроживлення; - з’єднання зі швидкістю 10/100 Мб/с; - стан з’єднання.	- активне з’єднання; - електроживлення; - з’єднання зі швидкістю 10/100 Мб/с.	- активне з’єднання ; -електро-живлення.

Зовнішній вигляд приведено (на рисунку 3.6)

Рисунок 3.6 – Модем DLINK DSL-2650U BRU

Даний модем забезпечує використання технології ADSL для забезпечення зв’язку з провайдером «Укртелеком» на швидкості до 24Mbit/c.

ADSL (Asymmetric Digital Subscriber Line) - Асиметрична цифрова абонентська лінія, високої передачі даних, відомих які позначаються xdsl.

В розроблюваній мережі планується підключення до інтернет через провайдера «Укртелеком», послуга «Ого». Оскільки відстань до райценту більше 25км підключення буде виконуватися через АТС розташовану в Золотому Потоці, тому максимальна швидкість не буде перевищувати 4Мбіти/с.

Отримані результату вибору а також супутнє обладнання, яке вибиралося без порівняльних таблиць а тільки з огляду на його функціональність і ціну наведені в таблиці 3.5.

Таблиця 3.5 – Таблиця необхідного обладнання

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів
1	2	3	4
1	D-Link DGS-1100-16	шт	1
2	D-Link DGS-1100-24	шт	2
3	Кабель UTP cat 5e	м	857
4	Патч-корд RJ45 UTP 2м кат.5e	шт	41
5	Роз’єм RJ-45	шт	86
6	Розетка RJ45	шт	43
7	Комутаційна шафа 24U	шт	1
8	Комутаційна шафа 12U	шт	2
9	Dell PowerEdge T20	шт	2
10	ББЖ PowerCom BNT-1500AP	шт	1
11	ББЖ PowerCom BNT-600AP	шт	4
12	D-LINK DIR-615s	шт	1
13	DLINK DSL-2650U BRU	шт	1

3.3 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій в мережі.

При виборі операційних систем для сервера та робочих станцій враховувалось:

- профіль роботи організації;
- апаратне забезпечення;
- наявність існуючого програмного забезпечення;
- вартість програмних продуктів;

Детально проаналізувавши кожен з вищенаведених пунктів було обрано наступні програмні рішення. В якості файлового сервера S1 буде ОС Ubuntu Server 16.04LTS+Samba 3, а на сервері S2 для доступу до інтернет в ролі шлюзу буде встановлена ОС Ubuntu Server 16.04LTS+squid.

Для робочих станцій встановлюємо операційну Ubuntu Mint, інсталяція даних програмних продуктів відрізняється лише налаштуванням конфігурації.

Використання Лінукс на серверах оправдане з точки зору надійності та вартості даного рішення, що є ключовим при розробці даного проекту.

Також і решта програмного забезпечення будуть встановлюватися із огляду на їх безкоштовність, зокрема LibreOffice, ClamAV та інші.

3.4 Особливості монтажу мережі

Монтаж мережі виконується згідно стандарту EIA/TIA-569:

Оскільки у нас одне приміщення, то для мережі вибрано один головний комутаційний вузол, розташований в кімнаті 306.

Відстані між головним комутаційним вузлом, проміжним комутаційним вузлом та горизонтальні кабелі повинні мати довжини, котрі не перевищують значень, наведених в таблиці 3.6.

Приміщення відповідають технічним стандартам і є пожежобезпечними. Температура в приміщенні – 21С, вологість – 30-50%, освітлення – 500 Люкс при висоті 2,6 м по номіналу. Розетки живлення – подвійні, кожних 1,8 м.

Таблиця 3.6 – Базові довжини кабелів

№	Тип середовища	Між гориз. кабелем і гориз. комут. вузлом	Між гориз. кабелем і проміж. комут. вузлом	Між проміж. комут. вузлом і гориз. каб. вузлом
1.	UTP (голос)	800 м	500 м	300 м
2.	UTP (дані)	90 м	90 м	90 м

Забезпечений доступ до кабелів, монтажних шаф, проміжних, головного та комутаційного вузлів.

Двері в комутаційному вузлі 90 см в ширину, відкриваються назовні і забезпечують необхідне обмеження для доступу.

Обладнання від стіни встановлюється на відстані не менше 50см (19”). Монтажна шафа стандартна розміром 500х620х610,12U, чорна, MG. Перед нею забезпечено мінімум 80 см диспетчерського простору.

Кабелі захищені коробами АСКО-УКРЕМ.

Кількість коробу в розрізі січень наведена в таблиці 3.7

Таблиця 3.7 – Таблиця потреби в кабелях

№ п/п	Січення коробу	Од. виміру	Факт. витрачено матеріалів
1	Короб 16х16	м	58
2	Короб 25х16	м	40
3	Короб 40х16	м	22
4	Короб 40х25	м	8
4	Короб 40х40	м	12

3.5 Обґрунтування вибору засобів захисту мережі

Оскільки в мережі школи є маршрутизатор безпровідного доступу то необхідно організувати захист мережі від несанкціонованого доступу. Серед багатьох протоколів можна виділити WPA.

Слід відзначити, що WPA має спрощений режим. Він отримав назву Pre-Shared Key (WPA-PSK). При застосуванні режиму PSK необхідно ввести один пароль для кожного окремого вузла бездротової мережі (бездротові маршрутизатори, точки доступу, мости, клієнтські адаптери). Якщо паролі збігаються з записами в базі, користувач отримає дозвіл на доступ в мережу.

WPA2 визначається стандартом IEEE 802.11i, прийнятим у червні 2004 року, і покликаний замінити WPA. У ньому реалізовано CCMP і шифрування AES, за рахунок чого WPA2 став більш захищеним, ніж свій попередник.

З 13 березня 2006 підтримка WPA2 є обов'язковою умовою для всіх сертифікованих Wi-Fi пристроїв. Саме його і буде використано для захисту мережі.

Захист проводового доступу через модем ADSL буде виконуватися засобами даного модему а також з допомогою проксі серверу та файєрвола ОС Лінукс.

Також захист буде організовуватися з використанням антивірусного програмного забезпечення ClamAV, та спеціалізованого програмного забезпечення для моніторингу роботи мережі.

Для організації захисту інформації на жорстких дисках серверу буде використовуватися створення програмного рейд масиву RAID1.

3.6 Тестування та налагодження мережі

Загально відомо, що більшість простоїв у мережі виникає через проблеми з кабелями. Інколи, причиною цього стають раніше використовувані кабельні сегменти, або недотримання виробниками вимог стандартів.

Кожен раз, при переміщенні робочої станції з місця на місце, підвищується ймовірність виникнення неполадок. Тоді, дуже корисною буде схема мережі.

При прокладці кабелів, потрібно впевнитись, що вони не здавлені і ніяким чином не натягнуті (це може призвести до пошкодження кабелю всередині). В мережах типу 1000Base-T і 100BaseTx, неполадки, пов’язані з кабелем легше визначити, оскільки до одного кабелю підключена лише одна робоча станція. Проте, якщо неполадки виникли в кабелях, які з’єднують концентратори, то їх важче локалізувати (щоб запобігти цьому, слід дотримуватись стандартів при прокладці кабелів).

Іншим важливим елементом при прокладці кабелів є використання якісних роз’ємів.

На роботу мережі впливає наявність різних видів завад. До них відносяться: електромагнітні і радіочастотні. Чим вища частота роботи кабелів, тим більш вони чутливі до цих видів завад. Причиною їх виникнення можуть бути:

- Флуоресцентні лампи.
- Кабелі живлення.
- Прилади, які містять електродвигуни.
- Трансформатори.
- Радіопередавачі (включаючи мобільні телефони).

Виходячи із описаного в приміщеннях прокладка мережі та розташування обладнання оптимізовані з точки зору внесення завад в мережу.

Несправності, пов’язані з мережевим адаптером.

Для локалізації несправностей, що виникли при встановленні (заміні) мережевого адаптера, необхідно перевірити декілька параметрів:

1. Несправність може бути викликана несправністю апаратної частини мережевого адаптера, самого комп’ютера, концентратора або мережевого кабелю.

2. Несправність може бути результатом неправильної настройки адаптера (портів, переривань).

Мережеві адаптери, як правило, мають світлодіодний індикатор. Якщо в процесі роботи він світиться, це означає, що мережева карта здатна вести обмін даними з концентратором (більшість концентраторів також мають світлодіодну індикацію для кожного свого порта). В іншому випадку, потрібно витягнути адаптер і вставити його в інший слот на материнській платі. Крім того, варто скористатись діагностичними програмами, які також поставляються з мережевими картами.

Результатом некоректної роботи мережевого адаптера можуть бути:

- Помилки FCS

- Формування кадрів, не доповнених до стандартної довжини – виникають в результаті дії електромагнітних коливань або колізій.

Несправності, пов’язані з комутаторами.

Оскільки в комутаторі сходяться кабелі від багатьох робочих станцій мережі, то досить важко визначити причину несправності. Наприклад, в мережі є станція, яка не може взаємодіяти з мережею. Причиною цієї проблеми може бути порт комутатора або кабель. Необхідно здійснити наступні кроки:

- Візуальна перевірка комутатора (світлодіодних індикаторів).
- Якщо світлодіод не горить, потрібно включити кабель в інший порт (робочий). Якщо проблема зникла, це означає, що несправним був порт комутатора.
- У випадку, коли робоча станція не здатна вести обмін даними і через робочий порт комутатора, необхідно здійснити перевірку кабелю (за допомогою тестера) і мережевої карти.

Інколи, проблеми, які виникають, можуть бути зв’язані не з відмовою обладнання, а з його неправильною настройкою. Тому, потрібно завжди настроювати порт комутатора у відповідності із можливостями мережевого адаптера.

4 СПЕЦІАЛЬНИЙ РОЗДІЛ

4.1 Інструкція з інсталяції програмного забезпечення серверів

Оскільки на серверах буде встановлено ОС Ubuntu Server 16.04 LTS, то нижче буде розглянуто встановлення та налаштування даної ОС.

Встановлення.

Для установки (1604) Server качаємо iso образ на офіційній сторінці, записуємо на DVD і завантажуємося з нього.

Перше вікно, вибираємо мову установки, в нашому випадку вибираємо Українська.

Запускаємо установку (1604)

Вибираємо країну - Україна

Не погоджуємося з автоматичним визначенням клавіатури

Вибираємо мову розкладки English, даний варіант зручніший для початку роботи, пізніше можна добавити роботу ще і з українською.

Вибираємо спосіб перемикання клавіатури, віддамо перевагу Ctrl + Shift.

Пишемо назву сервера, в нашому випадку стандартне ім'я S_1 і S_2

Пишемо ім'я користувача: Admin

Повторюємо введення користувача

Вводимо пароль, попередньо записавши його в блокнот. Пароль складного типу з буквами різних регістрів та цифрами і символами, для забезпечення достатньої захищенності мережі.

Повторюємо введення пароля, пароль складаємо із символів латинської розкладки, чергуючи верхній і нижній регістр, а також у випадковому порядку вставляємо цифри всередині пароля. Пароль повинен складатися мінімум з 8 символів.

Не погоджуємося з шифруванням домашнього каталогу, інакше доведеться вводити пароль при завантаженні сервера, а якщо доведеться перевантажити сервер віддалено, сервер на завантажиться без введення пароля для підключення шифрованого розділу:

Приступаємо до розбивки вінчестера вручну.

Переходимо на вінчестер і натискаємо Enter, і на питання створити нову порожню таблицю розділів - погоджуємося і натискаємо на Так й натискаємо Enter

Створилася нова таблиця розділу, переходимо на Вільне місце, натискаємо Enter і створюємо новий розділ / boot.

Стаємо на Створити новий розділ і натискаємо Enter.

Вводимо розмір розділу / boot - 250mb.

Вибираємо тип / boot розділу Первинний.

Натискаємо Enter стоячи на Початок.

Файлову систему встановлюємо - ext4.

Точка монтування - / boot

Мітка розділу завантажувальний – включено.

Стаємо на Налаштування розділу закінчена і натискаємо Enter.

Створюємо розділ підкачки:

- Переходимо на Створити новий розділ;
- Вказуємо розмір розділу підкачки - 16gb (це об’єм оперативної памяті)
- Переходимо на Початок і натискаємо Enter
- Вибираємо в файлової системі замість ext4 - розділ підкачки
- Вказуємо Налаштування розділу закінчено і натискаємо Enter

Установка (1604) Server, створюємо розділ / tmp для тимчасових файлів

- Створюємо розділ / tmp з розміром в 2Гб
- Вказуємо розмір розділу
- Тип розділу / tmp вибираємо Логічний і натискаємо Enter
- Вибираємо точку монтування / tmp і натискаємо Enter
- Відкриваємо параметри приєднання розділу /tmp і пропуском відзначаємо параметр noexec
- Натискаємо Enter після вибору параметра noexec
- Стаємо на Налаштування розділу закінчено і натискаємо Enter, настройка розділу tmp закінчена.

Нам залишилося тільки створити кореневий розділ / з розміром на все інше місце.

Вибираємо Логічний тип розділу

Вибираємо файлову систему ext4 для кореневого розділу /

Після розбивки та створення всіх розділів на вінчестері, закінчуємо розбивку вінчестера натиснувши на Закінчити розмітку і записати зміни на диск і натискаємо Enter

Погоджуємося з Записом змін на диск і натискаємо Enter. На питання про проксі сервер – залишаємо без серверу.

Вибираємо спосіб оновлення системи: Без автоматичного оновлення У вікні вибору програмного забезпечення вибираємо і ставимо галочку пропуском навпроти OpenSSH server і натискаємо Enter.

Йде процес установки програмного забезпечення. Погоджуємося з установкою системного завантажувача GRUB на жорсткий диск у головний завантажувальний запис і натискаємо Enter. Після натискання Продовжити відкриється CD-DVD привід, необхідно витягнути з приводу інсталяційний диск з дистрибутивом (1604) Server.

Установка завершена, (1604) Server встановлений.

Налаштування серверу: Веб-інтерфейс. Для управління системою через веб-інтерфейс є пакет webmin, але його на жаль в репозитарії немає, тому викачаємо підготовлений акет вручну:

Wget http://prdownloads.sourceforge.net/webadmin/webmin_1.840_all.deb

Для установки webim потрібні деякі залежні пакети, в нашому випадку це такий список, можливо, вам буде потрібно включити ще що-небудь. (продовження в додатку 4)

Налаштування доступу за допомогою squid еластично реалізовувати підходи доступу до інтернет ресурсів на основі інтервалів часу, кешування інформації для доступу до деяких сайтів.

Контроль доступу в Squid базується на двох різних компонентах: ACL-елементах та списку доступу (access list). Список для вхожу дозволяє або забороняє вхід до послуг.(продовження в додатку 5)

4.2 Інструкція з інсталяції та налаштування активного комутаційного обладнання

Налаштування комутатора

Для збору інформації про стан комунікаційних пристроїв, підтримуючих Gigabit Ethernet, і управління цими пристроями по мережі використовується протокол SNMP і агенти, вбудовані в пристрої.

Агенти більшості виробників підтримують в даний час як класичну для мереж TCP/IP базу управляючої інформації MIB II (RFC-1213), так і базу RMON MIB, спеціально орієнтовану на протоколи нижнього рівня Ethernet. База MIB II орієнтована в основному на збір статистики про протоколи мережного і транспортного рівнів стека TCP/IP, особливо протоколам фізичному і канальному рівнів, таким як Fast,Gigabit Ethernet.

Для керування через веб інтерфейс необхідно в браузері набрати адресу комутатора (http:// 10.90.90.90 *)*, після чого ввести логін і пароль і тоді відкриється вікно налаштування комутатора (див. рис. 3.2).

В подальшому в нашому випадку необхідно налаштувати VLAN, для розмежування доступу по портах таким чином, щоби всікомп’ютери мали спільний доступ до Інтернет серверу та файл –серверу і не мали доступу один до одного поза межами власної робочої групи. Це виконується за допомогою конфігурування VLAN по відповідних портах (див. рис. 4.2) При цьому для всіх робочих груп встановлюється спільний доступ до 1 та 2 портів, на яких підключено сервери мережі.

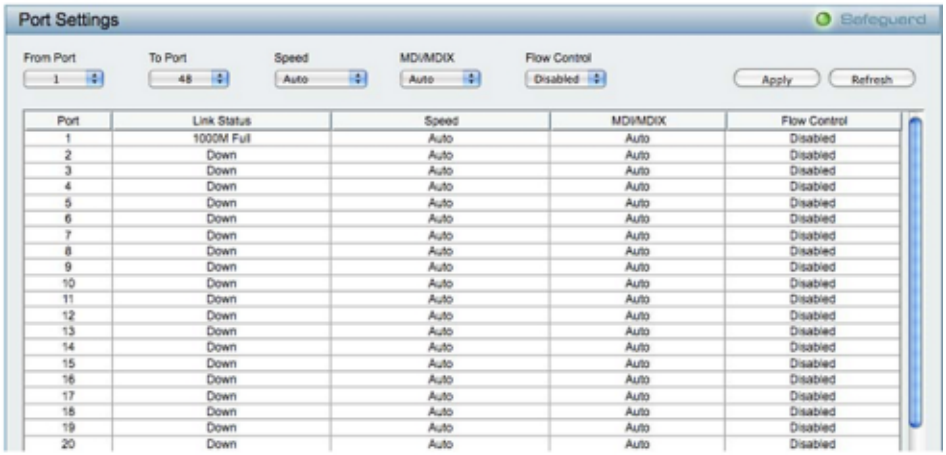


Рисунок 4.2 - Вікно налаштувань портів комутатора

Для налаштування Vlan необхідно ввімкнути функціїю 802.1Q VLAN, після чого слід створити нову VID групу, вибравши Add VID (див.рис. 4.3) і встановити порти в один із станів Untagged, Tagged or Not Member. При цьому слід пам’ятати що Untagged порт може бути тільки в одній Vlan групі. Після цього слід сконфігурувати PVID для доступу до Vlan групи.

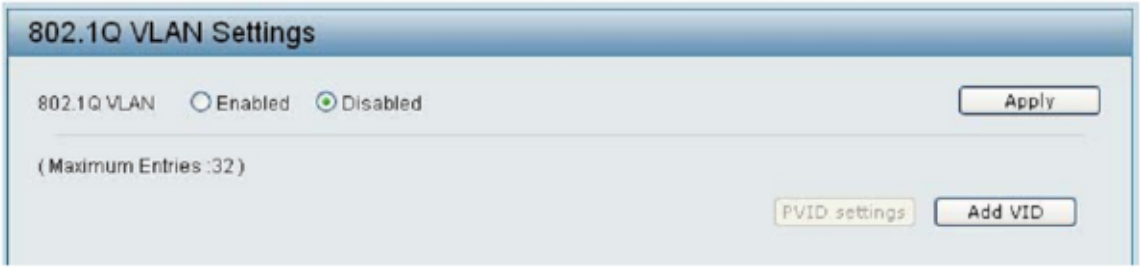


Рисунок 4.3 – Підключення нової VLAN

Наприклад для SW3 де перший порт ми використовуємо для підключення до комутатора SW2, решта портів діляться на дві VLAN – 4,5 (див.рис. 4.4) та присвоюємо PVID (див.рис. 4.5)

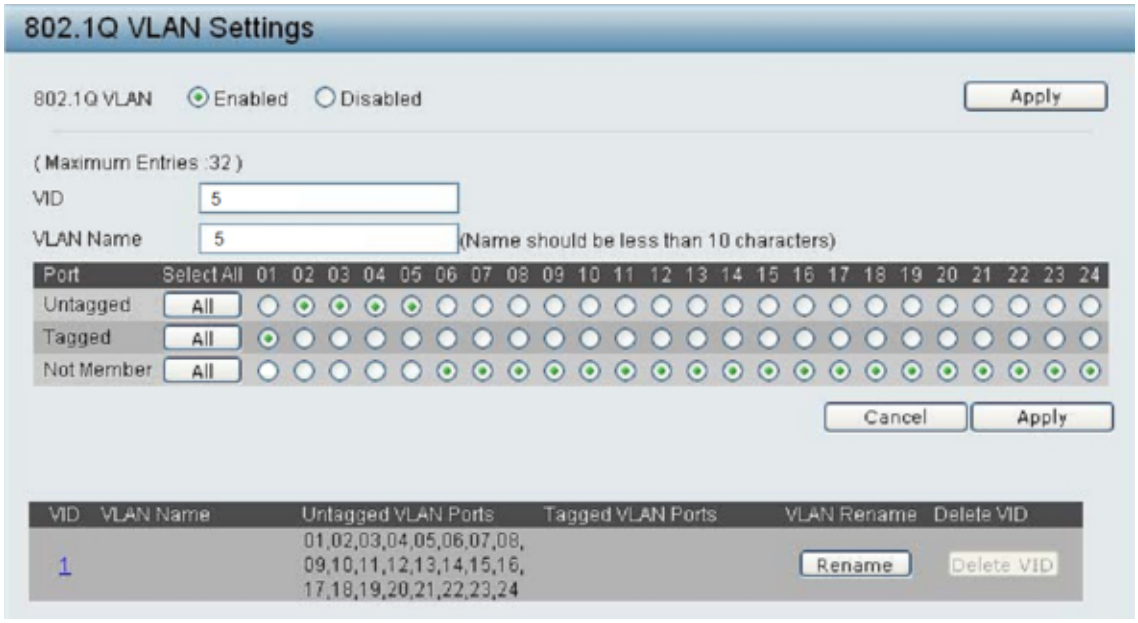


Рисунок 4.4 – Виділення портів в VLAN

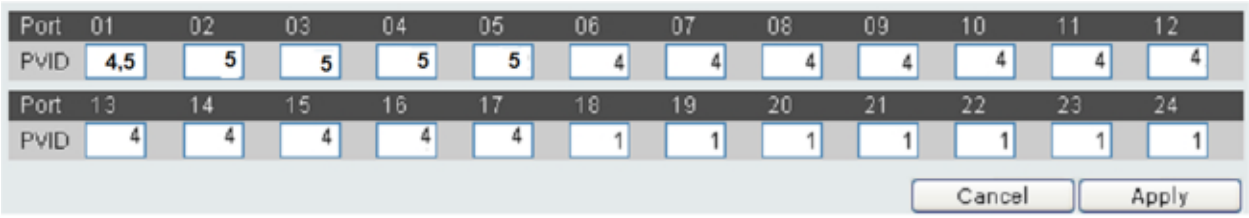


Рисунок 4.5 – Присвоєння PVID

Аналогічним чином виконуємо налаштування адресації портів для решти пристроїв у відповідності з таблицею IP адресації, яка представлена на листі 4

Можна також задати ім’я комутатору та IP адресу , для зручності доступу із власної мережі (див. рис. 4.6)

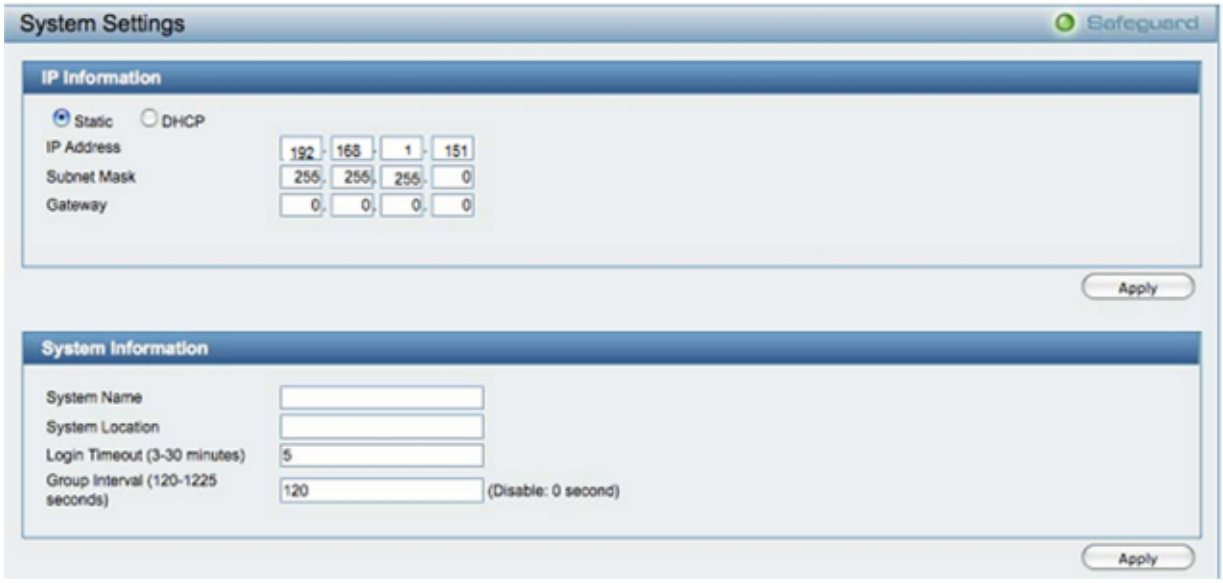


Рисунок 4.6 - Налаштування параметрів комутатора

4.3 Інструкція з використання тестових наборів та тестових програм

Апаратне тестування

Для тестування мереж використовують найрізноманітніше тестове обладнання. Найбільш використовуваним пристроєм для аналізу кабельної системи є рефлектометр Time Domain Reflectometer (TDR). Він виробляє та передає особливий сигнал у кабель і аналізує його відбиття, порівнюючи його з сигнальними сигнатурами відомих несправностей і визначає можливий тип несправності та її місце. Існує також ряд пристроїв для діагностики кабелів, котрі орієнтовані на конкретний тип мережі (наприклад, Ethernet та TokenRing).

Також для тестування мережі використовують тестери пробники, призначені для тестування кабелів витої пари. На рисунку 4.7 зображено один з таких тестерів.

Рисунок 4.7 - Тестер UTP/STP

Програмне тестування

Команда PING

PING – це програма призначена для перевірки з’єднання мереж. Він застосовує ICMP для обміну даними із далекою системою пінгу.

Команда PING тестує мережеве з'єднання шляхом передачі діагностичних пакетів конкретному вузлові в мережі. У свою чергу вузол, що одержав такий пакет, повинен відповісти і підтвердити прийом. Якщо відповідь отримана, то система працездатна. На даний момент існує дві версії цієї команди: оригінальна, що просто повідомляє про те, чи відбувся процес передачі прийому діагностичного пакета, і удосконалена, що видає розгорнуту інформацію про процес передачі-прийому.

Оригінальний варіант команди PING має наступний формат:

PING hostname, де hostname - машина, з'єднання з якої тестується.

Удосконалений варіант команди має більш складний формат:

PING [-fnqrv] [-c count] [-i wait] [-l] [-p pattern] [-s packetsize] hostname.

Таблиця 4.1 - Ключі команди PING

Ключ	Призначення
-c count	Команда закінчує роботу після count передач-прийомів діагностичного пакета. Якщо ключ **c** не зазначений, то ко-манда буде виконуватися до натискання CTRL^C.
-i wait	Ключ, що задає часовий інтервал wait між посилками. За замовчуванням цей інтервал задається рівним 1 секунді. Цей ключ не сполучимий з ключем f.
-p patter n	За допомогою ключа p користувач може наповнити 16 байт пакета, тобто задати дані, що будуть передаватися. Це використовується для діагностики проблем, пов'язані з пересиланням інформації.
-s pa-cket size	Ключ s задає число байт для пересилання packetsize**.** За замовчуванням задається розмір у 56 байт, а вся посилка займає 64 байта, тому що до даних додається 8-ми байтовий заголовок ICMP протоколу.
-f	Команда посилає черговий пакет як тільки одержує відповідь на попередній. Цей ключ може використовувати тільки адміністратор.
-l	Команда використовує вільний шлях для передачі тестових пакетів.
-n	Числовий вивід. Команда не буде виводити символьні імена адрес.
-q	На екран не буде виводитися нічого, крім рядків з інформацією про початок і завершення роботи команди.
-R	Ключ R говорить команді про необхідність запису шляхів тестових пакетів. Але необхідно пам'ятати, що IP - заголовок може зберігати тільки 9 імен вузлів. Інші будуть зігноровані .
-r	У цьому випадку команда посилає тестовий пакет прямо на host, оминаючи нормальний шлях. Якщо host не є прямо під’єднаним до

	мережі то команда повертає помилку.

Приклади використання команди

Для розуміння роботи команди Ping, необхідно розглянути кілька прикладів.

1. Приклад використання оригінального варіанта команди.

ping 192.168.1.20

У результаті дії цієї команди у випадку удалого виконання на екран буде виведено:

68 bytes from 192.168.1.20: icmp_seq=0 time=12 ms

68 bytes from 192.168.1.20: icmp_seq=1 time=11 ms

68 bytes from 192.168.1.20: icmp_seq=2 time=11 ms

68 bytes from 192.168.1.20: icmp_seq=3 time=10 ms

5 packets transmitted, 5 packets received, 0% packets loss round - trip (ms) min/avg/max = 9/11/12

Число icmp_seq говорить про порядковий номер посилки (у нашому випадку від 0 до 3).

Число time показує час, що пройшов з моменту відправлення пакета до одержання відповіді.

Дані після пунктирної лінії є підсумковими:

Кількість відправлений і отриманих, а також відсоток загублених пакетів - перший рядок.

Другий рядок - Мінімальний/Середній/Максимальний час за даними time.

Таблиця 4.2 - Розширені приклади використання утиліти Ping

Питання	Відповідь
1	2
1. Визначити, чи функціонує машина з IP-адресою 192.168.1.1	ping 192.168.1.1

Продовження таблиці 4.2

2. Перевірити працездатність вузла 192.168.1.1 за допомогою 6-и 60-ти байтних пакетів, що посилаються через 4 сек. з заповненням їхнім словом "HELLO"	ping -c 6 -i 4 -p HELLO -s 60 192.168.1.1
3. Провести тестування вузла 192.168.1.1без виводу поточної інформації на екран. Тестування проводити до натискання клавіш CTRL^C	ping -f -q 192.168.1.1
4.Провести перевірку працездатності вузла 192.168.1.1 с записом шляху до нього.	ping -R 192.168.1.1
5.Визначити середній час передачі прийому тестових пакетів 60-ти байтової довжини на вузол 192.168.1.1Використовувати 8 посилок.	ping -c 8 -s 60 192.168.1.1

Команда tracert

TRACERT – команда діагностики, схожа на ping . За допомогою ICMP ідентифікує всі пристрої, через які проходить пакет даних, щоб дістатись до вузла призначення.

Має наступний синтаксис:

tracert [-d] [-h макс число] [-j список вузлів] [-w інтервал] ім’я

Параметри:

-d – використовувати ім'я в замін IP адресу;

Використовуючи цю програму, ви можете здійснити діагностику мережі, щоб можна було знайти і помилки.

Інші утиліти

Ipconfig- Перевіряє форму протоколу TCP/IP, вносячи адреси серверів DHCP, DNS і WINS;

Finger- Одержує системну інформацію з вилученого комп'ютера, що підтримує сервіс Finger;

Nslookup- Дозволяє переглядати запису в базі даних сервера DNS, що відносяться до того або іншого вузла або домену;

Hostname- відає ім'я локальному пк для входу в систему ;

Netstat- показує статистику та яке підключення TCP/IP;

Route- дивиться або замінює локальну таблицю роутера;

Tracert- слідкує за маршрутом від роутера до віддаленого вузла;

Arp (Address Resolution Відображає локальний кэш відповідностей IP-адрес адресам Protocol) мережевих адаптерів.

4.4 Інструкція з експлуатації та моніторингу в мережі

Моніторинг та мережеметрія – це постійна перевірка інформаційних та комунікаційних процесів у системі.

Моніторинг дає можливість відслідковувати діяльність окремих користувачів з метою дотримання безпеки даних. Сама процедура моніторингу виконується на багатьох рівнях мережі з використання спеціального технічного забезпечення, протоколів, баз даних, служб.

Давайте детальніше розглянемо загальну характеристику способів організації моніторингу в КМ. Зрозуміло, що якщо вести моніторинг лише на одному з рівнів протоколу, то про ефективність таких процедур говорити не доводиться. Саме тому моніторинг доцільно проводити на різних рівнях:

- на фізичному рівні досліджуються параметри кабельної системи;
- на канальному та мережевому рівнях аналізуючи трафік, декодують та перехоплюють кадри і пакети;
- на верхніх рівнях проводиться вивчення взаємодії станцій з використанням конкретних протоколів та властивостей їх параметрів;

- на рівні застосувань можливий аналіз взаємодії застосувань (напрямку клієнта і сервера, бази даних)

Адміністратору передусім слід відслідковувати параметри взаємодії на рівні застосувань. Однак, як показує досвід, причини неефективності роботи слід шукати і у функціонуванні протоколів нижчих рівнів.

Давайте детальніше розглянемо особливості моніторингу на деяких рівнях.

На фізичному рівні найважливіше місце займає аналіз кабельної системи. В кабелях можуть виникати наступні несправності:

- обрив;
- коротке замикання;
- затиснення кабелю;
- погане навантаження;
- інші дефекти (згини, петлі тощо)

На вищих рівнях застосовують аналіз роботи сегмента, використовуючи аналізатор протоколу, що являє собою програмно-апаратний блок, який переймає весь потік інформаційного сегменту, аналізує, декодує та інтерпретує його.

Тут можлива реалізація найважливіших функцій:

Фільтрування – в загальному потоці виділяється пакет з певними ознаками.

Ініціалізація – відбувається зв'язок між режимами перехоплення і відображення з конкретними подіями. В даному випадку визначена подія (надходження кадру, визначення протоколу певної довжини чи звертання до вказаного сервера) запускає перехоплення протоколу.

Генерування тестових даних – в мережі створюється тестовий потік вказаного типу пакетів заданої інтенсивності.

Можливість використання розподіленої системи керувань мережею із застосуванням агентів моніторингу та аналізу, бази даних параметрів стандарту MIB, протоколів SNMP та RMON, систем моніторингу та аналізу дає змогу

значно підвищити ефективність збору інформації про функціонування окремих вузлів ЛКМ із врахуванням часових затрат.

Також для моніторингу можна використовувати засоби комутаторів.

Зокрема комутатор D-Link DGS-1100-16 дозволяє переглядати детальну статистику по портах. Яким же чином відстежити, який пристрій або користувач дуже інтенсивно використовує канал або генерує трафік (наприклад, вірус або додаток типу Торрент-клиента)? Все що потрібне, це перевірити статистику порту (port statistic). У даних моделях це налаштування знаходиться на сторінці L2 Features > Statistics (див. рис. 4.8).

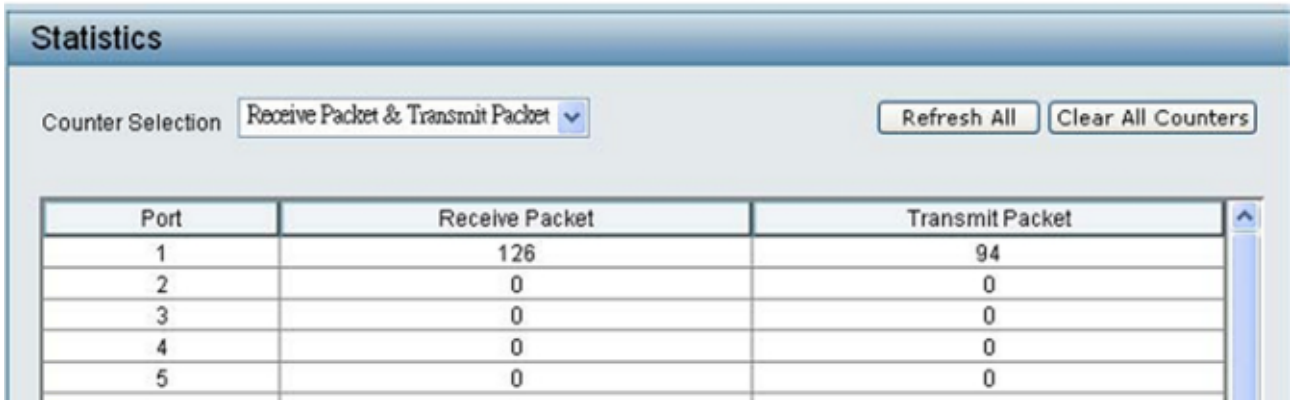


Рисунок 4.8 — Вікно статистики комутатора

Сторінка System > Port Settings одночасно відображає стан порту (Link Status), швидкість(Port Speed), контроль трафіку (Flow Control) і дозволяє вибирати і змінювати доступні значення. Так само на цій сторінці можна встановити пріоритет за умовчанням (Default Priority) для нетегованих пакетів, що приходять на порт.

4.5 Інструкція по налаштуванню засобів захисту мережі

Ubuntu Linux ядро включає в себе підсистему Netfilter. Всі сучасні засоби міжмережевого захисту Linux використовують цю систему для фільтрації пакетів.

Далі приведена інструкція по покращенню безпеки в Linux і в (1604) LTS server зокрема. Для цього слід виконати наступні кроки:

1. Установка і налаштування Firewall - ufw
2. Налаштування shared memory - fstab
3. SSH - відключення root login, зміна порту і ін.
4. Обмеження su тільки для групи admin (за умовчанням)
5. Налаштування мережевих параметрів sysctl
6. Відключення Open DNS Recursion і Version Info - Bind9 DNS server
7. Запобігання IP Spoofing
8. Захист від DDOS (Denial of Service) атак за допомогою ModEvasive
9. Сканування логів і заборона підозрілих IP - DenyHosts і Fail2Ban
10. Виявлення вторгнень - PSAD
11. Перевірка на RootKits - RKHunter і CHKRootKit
12. Сканування портів - Nmap
13. Аналіз системних логв - LogWatch
14. SELinux - Apparmor
15. Аудит системи безпеки - Tiger
16. Контроль - SUID
17. Контроль цілісності - Aide
18. IPS – Suricata

Розглянемо детальніше деякі із пунктів:

1. Установка і налаштування Firewall - ufw

Спершу встановимо Firewall. У Ubuntu передустановлено UFW - Ubuntu FireWall, який є надбудовою над IPtables. За бажання можна відключити роботу з протоколом ipv6. У файлі /etc/default/ufw міняємо "yes" на "no":

IPV6=no

Дозволяємо доступ до SSH і Http сервісів:

sudo ufw allow ssh sudo ufw allow http

Активація файрвола:

sudo ufw enable

Виведення детальної статистики:

sudo ufw status verbose

Непогано б додати до цих правил обмеження з'єднань (rate limit), яке може бути корисне для захисту від атак "в лоб" (brute - force). UFW заборонятиме з'єднання з IP адресами які намагаються встановити більше 6 з'єднань на протязі 30 секунд.

Типове використання:

ufw limit ssh/tcp

Додаємо правила при необхідності. Наприклад, що б дозволити доступ на порт 8080 з локальної мережі:

ufw allow to 192.168.0.10 port 8080 from 192.168.0.0/24 proto tcp

і включаємо логування: ufw logging on , що включить ведення журналу усіх з'єднань відповідно до рівня подробиць логу. Наприклад,тільки для дозволу журналювання.

Журналювання (LOGGING)

Ufw підтримує декілька рівнів деталізації журналювання. За умовчанням рівень журналювання встановлений в 'low'. Користувачі можуть встановити рівень деталізації командою : ufw logging LEVEL де LEVEL може набувати значень 'off ', 'low ', 'medium ', 'high' і 'full ':

– off журналювання відключено;

– low реєструються усі пакети, що блокуються, не відповідні політиці за умовчанням (включаючи rate limiting), так само як і пакети, що відповідають правилам, для яких включений log;

– medium як і low, плюс усі дозволені пакети, що не відповідають політиці за умовчанням, усі invalid пакети і усі нові з'єднання. А так само записи rate limiting.

– high як і medium (без rate limiting), плюс усі пакети з rate limiting;

– full як і high, але без rate limiting.

Рівні деталізації журналів вище medium генерують велику кількість повідомлень і можуть швидко заповнити ваш диск. У разі, якщо журналювання

було відключене, то при його включенні з опцією 'on ', включається журналювання рівня low.

Подивитися список правил: ufw status numbered

Один із способів видалити правило : ufw delete 1

Вставити правило по номеру рядка (старе правило зсувається вниз, на номер більше) :

ufw insert 1 reject from 192.168.0.67

2. Налаштування shared memory - fstab

Розділ /dev/shm може бути використаний в атаці на сервіс, такий як, наприклад, httpd. Відредагуйте /etc/fstab, що б зробити його безпечнішим: sudo vi /etc/fstab

Додайте наступний рядок і збережіть файл. Для того, що б зміни набули чинності необхідно перезавантажитися. tmpfs /dev/shm tmpfs defaults, noexec, nosuid 0 0

3. SSH - відключення root login, зміна порту і ін.

Простий спосіб підвищити безпеку SSH заборонити логінитися під root 'ом і поміняти стандартний 22 порт на будь-якій іншій. Перш ніж забороняти підключення суперкористувачеві root створіть іншого користувача і включіть його в групу admin . Якщо ви поміняли порт SSH, не забудьте відкрити його у файрволі і закрити 22 порт. У командному рядку виконайте:

sudo vi /etc/ssh/sshd_config

Змініть або додайте наступне:

Port

Protocol 2

PermitRootLogin no

DebianBanner no

Перезавантажите SSH сервер: sudo /etc/init.d/ssh restart

4. Обмеження su тільки для групи admin (за умовчанням)У Ubuntu цю команду виконувати немає необхідності.

5. Налаштування мережевих параметрів sysctl

Усі зміни мають бути внесені до файлу /etc/sysctl.conf:

sudo vi /etc/sysctl.conf

Розкоментуйте або додайте рядки: (продовження в додатку 6)

Також IPS можуть виконувати дефрагментацію пакетів, переупорядковування пакетів TCP для захисту від пакетів із зміненими SEQ і ACK номерами.

Також, оскільки в мережі присутня точка доступу слід налащтувати доступ по шифрованому каналу, для цього використовуємо шифрування WPA2-PSK і встановлюємо бажаний пароль (див.рис.4.8).

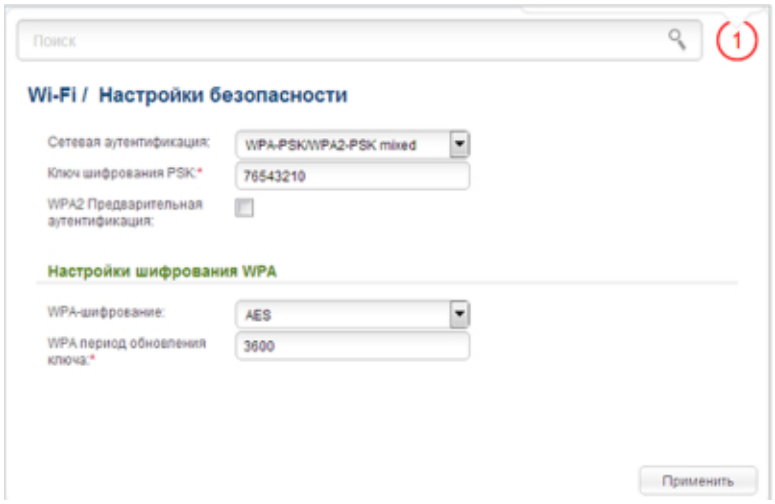


Рис.4.8 – Встановлення захисту безпровідного доступу

Також встановимо захист доступу ззовні в нашу мережу, відкривши тільки 80-й порт на модемі, в якому на сторінці «Межсетевой экран / Триггер портов» можна встановити правила для функції Port Triggering, шляхом встановлення значення для відного порту 80, т.т. доступ ззовні дозволетільки по порту 80. В разі виникнення потреби в інших портах їх можна також увімкнути, проте по замовчуванню вони вимкнені.

5 НАУВО-ДОСЛІДНА ЧАСТИНА

5.1 Модель дослідження

Метою цього дослідження є вивчення використання інформаційних систем в управлінні школою та з’ясування ідей керівників щодо управлінських інформаційних систем.

Населення цього дослідження формується із керівників шкіл, які працюють у 170 школах Тернопільської області. Однак керівники 98 шкіл відповіли на анкети. Серед керівників шкіл, включених у дослідження, 24 з них працювали 1-7 років (23,7%), 26 з них 6 -11 (22,1%), 16 з них 13-17 (15,5%), 9 з них їх за 18 -22 (8,4%), а 12 з них працювали 23 і більше років (17,5%). 23 учасників (23,6%) є студентами, 69 (26,2%) з них є аспірантами, і лише один із них (28,7%) є аспірантом. Серед керівників шкіл, включених у дослідження, шість з них не відповіли на питання про професійний досвід, а троє з них не відповіли на питання про рівень освіти.

5.1.1 Збір та аналіз даних

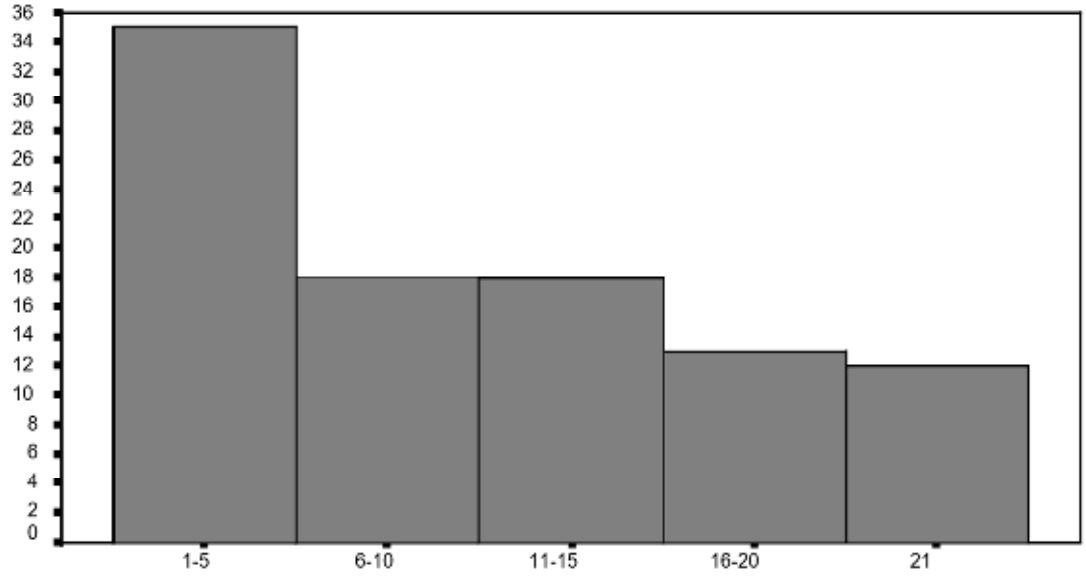
Розроблено анкету як інструмент збору даних. У першій частині анкети було кілька пунктів про особисту інформацію керівників шкіл, таких як професійний досвід та рівень освіти. У другій частині стосувались засобів інформаційних технологій, пов’язаних з інформаційними системами школи, та думки керівників шкіл щодо технологічних об’єктів. Елементи про кількість комп'ютерів у школі та кількість комп'ютерів, підключених до Інтернету, були відкритими, а пізніше їх класифікували після вивчення їх розподілу. Очікувалось, що учасники обиратимуть серед представлених варіантів пункти про місця комп’ютерів та підключених до Інтернету, а також програмне забезпечення, що використовується.

У третій частині опитування були предмети, пов’язані з дослідженнями, проведеними в школі, яка керує інформаційними системами, та предмети, за

якими проводились ці дослідження. Ці пункти були розділені на дві частини, як підготовка різних документів, списків та статистичних даних та введення даних. Четверта частина складалася з внеску управління інформаційними системами в управління школою та виниклих проблем. Ці предмети мали форму п'ятибальної шкалі.

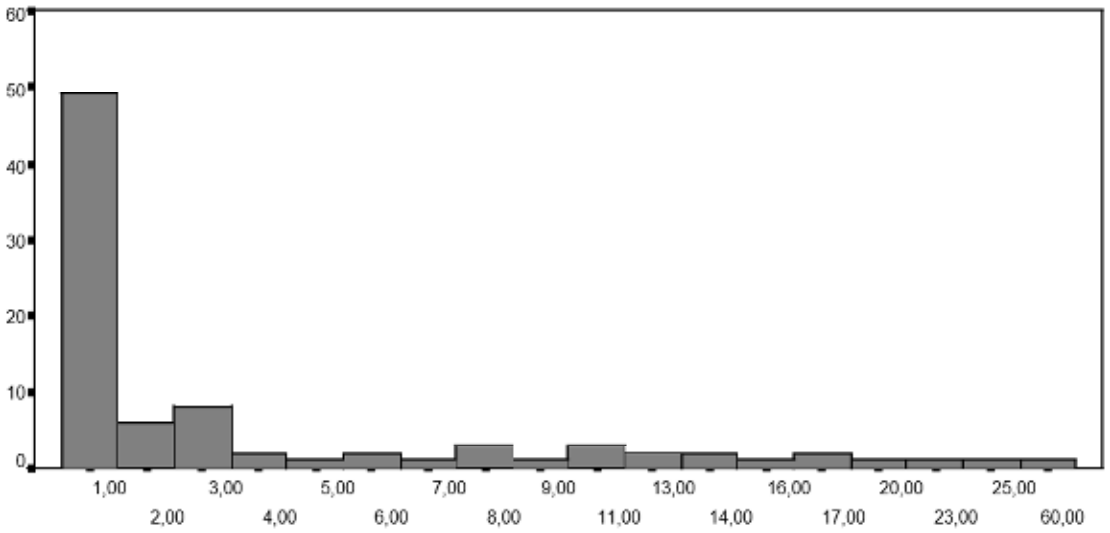
5.2 Інформаційні технології у школах

Під цією назвою були представлені засоби інформаційних технологій у школах та думки керівників шкіл щодо технологічних об'єктів. Кількість комп'ютерів підключених до Інтернету, їх розташування та програмне забезпечення, що використовується в школах, та думки керівників шкіл щодо програмного забезпечення були представлені нижче в графіках та таблицях.



Графік 5.1-Кількість комп’ютерів у школах

Коли було досліджено кількість комп’ютерів у школах, що потрапили в обсяг дослідження, було виявлено, що 35 (35,5%) із 96 шкіл мали 1-5 комп’ютерів, 18 (18,1%) школи мали 6-10, 13 шкіл (13,1%) мали 16-20 та 12 шкіл (12,5%) мали 21 і більше комп’ютерів. Як видно з графіку 5.1, (53%) шкіл, які були охоплені дослідженням, мали менше 10 комп'ютерів.



Графік 5.2 - Кількість комп’ютерів, підключених до інтернету в школах

Як видно на графіку 5.2, кількість підключених до Інтернету комп’ютерів була значно бідною. Крім того, лише 27,6% з цих шкіл мали веб-сторінку.

Таблиця 5.1 - Розташування комп’ютерів та комп’ютерів, під’єднаних до Інтернету в школах

	Комп’ютер		Інтернет	
Розташування	f	%	f	%
Кімната менеджера	85	86.7	70	71.4
Заступник керівника кімнати	74	75.5	51	52
Кімната для вчителя	56	57.1	34	34.7
Комп’ютерна лабораторія для студентів	62	63.3	33	33.7
Служба наведення	15	15.3	12	12.2
Бібліотека	15	15.3	6	6.1

85 (86,7%) менеджерів із 98, які були включені в дослідження, мали комп’ютер у своїх кімнатах, а 70 (71,4%) з них мали з’єднання з Інтернетом. Після цього прийшли заступники менеджерів із 74 кімнатами (75,5%). Лише 51 (52%) комп’ютерів мав з’єднання з Інтернетом у кімнатах заступників керівника. 56 вчителів (57,1%) мали комп’ютери, 34 з них були підключені до Інтернету (34,7%) у 98 школах. З іншого боку, лише 15 (15,3%) бібліотек та служб орієнтації мали комп’ютери. (Таблиця 5.1)

Таблиця 5.2 - Програмне забезпечення, що використовується в школах.

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ		N	Y
Пакет програмного забезпечення для управління школою	f	45	50
	%	45.9	51.0
Бюджетні програми	f	47	48
	%	48.0	49.0
Текстовий процесор (Microsoft Office-Word vb.)	f	15	81
	%	15.3	82.7
Електронна таблиця (Microsoft Office-Excel)	f	17	79
	%	17.3	80.6
Презентація (Microsoft Office-Power Point vb.)	f	30	66
	%	30.6	67.3
Програмне забезпечення	f	41	55
	%	41.8	56.1
Бібліотечна програма	f	90	5
	%	91.8	5.1

Як видно з таблиці 5.2, найбільш використовуваними програмними продуктами керівників шкіл у школах були програмне забезпечення для обробки текстів (82,7%) та електронних таблиць (80,6%). У 51% усіх шкіл програмне забезпечення для управління школами готували приватні компанії. Найменш використовуваним програмним забезпеченням була бібліотечна програма (5,1%).

Таблиця 5.3-Запобіжні заходи щодо безпеки інформації

ЗАПОБІЖНІ ЗАХОДИ		N	Y
Антивірусні програми	f	70	28
	%	71.4	28.6
Пароль	f	71	27
	%	72.4	27.6

Продовження таблиці 5.3

Резервне копіювання	f	63	35
	%	64.3	35.7

Хоча 75,5% шкіл, які брали участь у дослідженні, вживали заходів обережності, 25,5% з них не вживали жодних запобіжних заходів. Для безпеки програм у 28,6% шкіл використовували антивірусні програми, у 27,6% шкільних шифрах та у 35,7% резервних копій (табл. 5.3).

Як показано в таблиці 5.4, (що знаходиться у додатку А) найбільш інтенсивними введенням даних до інформаційних систем у школах були, відповідно, такі: інформація про інституції, інформація про учнів, оцінки учнів та відвідуваність. Найменший доступ до даних спостерігався в бібліотеках шкіл.

Коли було перевірено, хто вводив дані в школи, було зрозуміло, що найважливішу частину цієї роботи виконували директори шкіл та їх помічники. Директор школи зазвичай вводив дані про інформацію про установи (70,4%), інформацію про викладачів (52%), приналежності (39%), бюджет (29,6%), фонд оплати праці (26,5%) та нарахування (26,5%); а також помічників директорів внесли дані про відвідуваність (59,2%), інформацію про учнів (56,1%), оцінки (55,1%), навчальну програму та курси (48%) та бібліотеку (12,2%) у школах в рамках цього дослідження. Очевидно, що роль вчителів у введенні даних була дуже мізерною. Лише в 26 із 98 шкіл вчителям було призначено вносити в систему оцінки учнів, з 13 шкіл (13,3%) їм було призначено вводити навчальну програму та курси, а в 22 школах (21,4%) дані бібліотеки.

5.2.1 Внесок інформаційних систем в управління школою та проблеми, що виникають

Внесок інформаційних систем управління школою було подано в таблиці 5.5, а проблеми, що виникають, у таблиці 5.6 нижче.

Таблиця 5.5 - Внесок інформаційних систем у управління школою

ВНОСИ	**N**	**X**	**CC**
Підготовка документів стала простішою	97	4.43	72
Вести записи стало простіше	97	4.40	73
Листування стало легшим	97	4.39	72
Можна зробити набагато більше операцій порівняно з минулими часами	97	4.38	77
Виправити помилки легше	96	4.34	58
Інформація, яку запитують вищі установи, може бути передана в короткий час.	98	4.33	88
Частота помилок майже дорівнює нулю.	98	4.32	86
Виявити помилки легко	98	4.32	88
Інформація, що стосується учнів, може бути легко передана батькам.	96	4.04	92

Можна помітити, що рівень внеску інформаційних систем в управління школою був на високому рівні. Було зазначено, що найважливішим внеском інформаційних систем в управління школою був саме такий підготовка документа стала простішою (X= 4,43). За цим слідувала простота ведення записів (X = 4,40), простота листування (X = 4,39), виконано більше операцій порівняно з минулим (X = 4,38), простота виправлення помилок (X = 4,34), легкість передачі інформації, яку запитують вищі установи, за короткий час (X = 4,33), частота помилок найменша (X = 4,32), простота виявлення помилок (X = 4,32), простота інформації, що стосується учнів, яка легко передається батькам (X = 4,04) (Таблиця 5.5)

Таблиця 5.6 - Проблеми, що виникають, пов’язані з інформаційними системами управління

ПРОБЛЕМИ	**N**	***X***	**CC**
У разі відключення електроенергії ми повинні зробити перерву.	93	3.66	1.23
Збільшується ризик втрати даних (відключення електроенергії, колапс системи)	97	2.93	1.24
У нас є деякі проблеми, пов’язані з програмним забезпеченням.	95	2,87	1.13
Споживач постійно перевіряє електронні листи постійно.	97	2.24	1.01

Ми не можемо виконати необхідну роботу, коли відповідальні люди поза школою.	92	2.15	81

Продовження таблиці 5.6

У нас було достатньо часу, щоб підготувати навчання, яке вимагали вищі навчальні заклади (для вступу	96	1,97	88

Як видно з таблиці 5.6, керівники шкіл заявили, що той факт, що їм довелося призупинити роботу у разі відключення електроенергії (X = 3,66) була найбільш частою проблемою щодо інформаційних систем, і хоча той факт, що вони не могли регулярно оновлювати дані (X = 1,89) був найменш частим.

5.3 Аналіз і узагальнення отриманої інформації

За результатами цього дослідження, яке стосувалося використання інформаційних систем управління школою в початкових школах і яке має на меті визначити точки зору керівників шкіл, пов’язані з інформаційними системами управління, було помічено, що кількість комп’ютерів недостатня і існує у більшості шкіл було лише три комп’ютер підключений до інтернету. Крім того, у декількох із цих шкіл була веб-сторінка школи.

У дослідженні, проведеному у 2018 році в Тернопільській області, було виявлено, що однією з найважливіших перешкод у застосуванні управлінських інформаційних систем є недостатність чисельності комп'ютерів. З цієї причини можна сказати, що існувала важлива інфраструктурна проблема реалізації інформаційних систем управління школою в сучасних школах. Послідовність технологічних удосконалень зростала із використанням технологій. З цієї причини обов’язковим є надання викладачам, особливо керівникам шкіл, достатньо технологічних можливостей, щоб змусити їх прийняти та узгодити вдосконалення.

Більше того, було помічено, що все ще є деякі керівники шкіл, які не мають комп’ютера у своїх кабінетах у школах, що входять в обсяг цього дослідження. Серед керівників шкіл та помічників керівників шкіл, які мають комп’ютер у своїх кабінетах, деякі з них використовують комп’ютер без доступу до Інтернету. До того ж є деякі школи, вчителі яких не мають

можливості використовувати інформаційні технології. Вбачається, що мета Міністерства освіти, яка забезпечує кожен кабінет персоналу принаймні двома комп'ютерами; Постачання служб орієнтування, бібліотеки, керівників шкіл доступом до інтернету.

Хоча керівники шкіл заявляли, що найчастішою проблемою, яку вони страждають від інформаційних систем, є те, що їм доводиться припиняти роботу у таких випадках, як відключення електроенергії, найменшою проблемою була відсутність систематичного оновлення даних. Керівники шкіл сказали, що відсутність інфраструктури такі як відключення електроенергії, відсутність технічної підтримки та проблеми із забезпеченням безпеки даних заважали ефективному використанню системи. Подібним чином, найважливішою перешкодою на шляху ефективного використання управлінських інформаційних систем тут є відсутність інфраструктури, отже, відсутність планування.

Найважливішим відносним впливом інформаційних систем на їхню управлінську ефективність є те, що вона дозволяє легко отримати інформацію, необхідну для зміни проблем, і що дані, що вводяться в комп'ютер, є ефективними для прийняття управлінських рішень. Частіше, у сучасних школах приймаються більш складні та швидкі рішення. Для прийняття рішення потрібні більше даних та складні взаємозв'язки між цими даними, які слід враховувати. Більше того, ці рішення необхідно базувати на поточних-останніх даних.

На закінчення, дослідження з довгостроковими планами, започатковане заповненням недостатності в інфраструктурі, необхідне для ефективного використання інформаційних систем управління школою.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДХВИЧАЙНИХ СИТУАЦІЯХ

Охорона праці – це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних та лікувально-профілактичних заходів і засобів, спрямованих на збереження здоров’я та працездатності людини в процесі праці.

Метою даного розділу кваліфікаційного проекту є розгляд проблем, що пов’язані із розробкою, впровадженням та використанням локальної комп’ютерної мережі.

Основні особливості роботи користувачів комп’ютерів, електробезпека при роботі з комп’ютерним обладнанням та вимоги до режимів праці та відпочинку, що висуваються до користувачів ВДТ.

6.1 Заходи по покращенню питань з ОП та ТБ з мережевим обладнанням на підприємстві

Вимоги безпеки під час експлуатації мережевого обладнання

- Користувачі ЕОМ повинні слідкувати за тим, щоб мережеве обладнання та устаткування для його обслуговування, ремонту та налагодження були справними і випробуваними відповідно до чинних нормативних документів.

- Щоденно перед початком роботи необхідно проводити очищення екрана відеотермінала від пилу та інших забруднень.

- Після закінчення роботи мережеве обладнання та персональна ЕОМ повинні бути відключені від електричної мережі.

- У разі виникнення аварійної ситуації необхідно негайно відключити мережеве обладнання та ЕОМ від електричної мережі.

- При використанні з ЕОМ та мережевим обладнанням лазерних принтерів треба дотримуватись вимог Санітарних норм та правил устрою та експлуатації лазерів № 5804-91, затверджених Міністерством охорони здоров'я СРСР в 1991 р.

- При потребі, для захисту від електромагнітних, електростатичних та інших полів можуть застосовуватися спеціальні технічні засоби, що мають відповідний сертифікат або санітарно-гігієнічний висновок акредитованих органів щодо їх захисних властивостей.

- Є неприпустимими такі дії:

- виконання обслуговування, ремонту та налагодження мережевого обладнання безпосередньо на робочому місці користувача ЕОМ;

- зберігання біля мережевого обладнання та носіїв інформації, запасних блоків, деталей тощо, якщо вони не використовуються для поточної роботи;

- відключення захисних пристроїв, самочинне проведення змін у конструкції та складі мережевого обладнання або їх технічне налагодження;

Вимоги безпеки під час обслуговування, ремонту та налагодження мережевого обладнання

- Монтаж, обслуговування, ремонт та налагодження мережевого обладнання, заміна деталей, пристроїв, блоків повинні здійснюватись тільки при повному відключенні живлення.

- Забороняється з'єднувати та роз'єднувати кабелі при підключеній напрузі.

У тих випадках, коли монтаж, обслуговування, ремонт та налагодження мережевого обладнання або його блоків при відключеному живленні неможливі, виконання цих робіт допускається за умови додержання таких вимог:

- устаткування, допоміжна апаратура та прилади повинні бути заземлені;

- роботи виконуються не менше ніж двома працівниками;

- працівники повинні виконувати роботу інструментом з ізольованими ручками, стоячи на діелектричному килимку, або бути в діелектричних калошах.

Засоби захисту та інструмент необхідно щоразу перед застосуванням оглянути і при виявленні несправностей негайно заміняти.

Користування несправними захисними засобами та інструментом є

неприпустимим.

Під час виконання ремонтних робіт слід користуватись електроінструментом, напруга живлення якого не перевищує 36 В.

Особам, що виконують ремонтні роботи, забороняється працювати в ручному годиннику, що має металевий браслет.

Ремонтувати або настроювати мережеве обладнання під напругою дозволяється тільки в тих випадках, коли іншим способом виконати роботу неможливо.

Паяння деталей повинно проводитись відповідно до СП 952-72.

Промивання і знежирення деталей, блоків, плат повинні проводитись за допомогою етилового спирту або спеціальних негорючих промивних рідин.

Промивання, знежирення деталей, блоків і плат повинно проводитись в окремому приміщенні у спеціально обладнаних шафах з місцевою витяжною вентиляцією у вибухопожежобезпечному використанні при швидкості руху повітря в робочій зоні 0,7 м/хв. Промивати, знежирювати деталі, блоки, плати дозволяється тільки при працюючій вентиляції.

Приміщення, де здійснюється промивання і знежирення деталей, повинно бути забезпечене протипожежними засобами за узгодженням з органами державного пожежного нагляду.

Працівникам, що виконують обслуговування, ремонт та налагодження мережевого обладнання, не дозволяється:

- працювати поблизу відкритих струмовивідних частин;
- залишати без догляду увімкнуте в мережу живлення устаткування, прилади, що використовуються при проведенні робіт;
- • залишати на устаткуванні, приладах запобіжники, з'єднувачі, провід, залишки флюсу, припою тощо;
- проводити всередині мережевого обладнання операції, що виконуються тільки двома руками, без попереднього вимкнення з мережі живлення та зняття залишкових зарядів з конденсаторів фільтрів випрямлячів.

Вимоги до виробничого персоналу

Усі працівники, які виконують роботи, пов'язані з експлуатацією,

обслуговуванням, налагодженням та ремонтом ЕОМ, підлягають обов'язковому медичному огляду — попередньому під час оформлення на роботу та періодичному протягом трудової діяльності - в порядку, з періодичністю та медичними протипоказаннями відповідно до Положення про медичний огляд працівників певних категорій, затвердженого наказом Міністерства охорони здоров'я України від 31 березня 1994 р. № 45 і зареєстрованого в Міністерстві юстиції України 21.06.94 за МІ 36/345, та Сангін 3.3.2-007-98.

До роботи безпосередньо на ЕОМ допускаються особи, які не мають медичних протипоказань.

Працівники, що виконують роботи з профілактичного обслуговування, налагодження і ремонту ЕОМ при включеному живленні, та при інших роботах, передбачених Переліком робіт з підвищеною небезпекою, затвердженим наказом Держнаглядохоронпраці від 30.11.93 № 123, зареєстрованим в Міністерстві юстиції України 23.12.93 за № 196, зобов'язані проходити попереднє спеціальне навчання та один раз на рік перевірку знань відповідних нормативним актам з охорони праці.

Допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці та пожежної безпеки, забороняється.

Забороняється допускати осіб, молодших 18 років, до самостійних робіт в електроустановках та на електрообладнанні під час профілактичного обслуговування., налагодження, ремонту ЕОМ та при інших роботах, передбачених Переліком важких робіт та робіт зі шкідливими та небезпечними умовами праці, на яких забороняється застосовувати працю неповнолітніх, затвердженим наказом Міністерства охорони здоров'я України від 31.03.94 № 46, зареєстрованим у Міністерстві юстиції України 28.04.94 за № 176/385.

До робіт з обслуговування, налагодження та ремонту ЕОМ допускаються особи, що мають кваліфікаційну групу з електробезпеки не нижче III.

Працівники, які виконують роботи з експлуатації, обслуговування, налагодження та ремонту ЕОМ, згідно зі статтею 10 Закону України «Про охорону праці» забезпечуються належними засобами індивідуального захисту

відповідно до чинних норм.

Обов'язки, права та відповідальність за порушення правил

Відповідно до Закону України «Про охорону праці» керівник підрозділу:

- на підставі нормативно-правових актів про охорону праці, примірних інструкцій, інструкцій з експлуатації обладнання розробляє та затверджує інструкції з охорони праці за професіями або на окремі види робіт з урахуванням фактичних умов проведення робіт, технології, наявності обладнання й інструменту, засобів захисту та рівня

- підготовки виконавців, проводить відповідне навчання та Інструктажі з працівниками;

- вживає необхідних заходів з тим, щоб робочі місця та засоби виробництва протягом усього часу їх використання підтримувались у справному та безпечному стані, а виявлені недоліки, що впливають на охорону праці та захист здоров'я працівників, були своєчасно усунуті;

- відповідно до Порядку проведення атестації робочих місць за умовами праці проводить атестацію робочих місць для оцінки умов праці. На підставі аналізу проведеної атестації вживає заходів для унеможливлення виникнення небезпечних та шкідливих чинників;

- організовує роботу працівника таким чином, щоб повсякденна робота з мережевим обладнанням регулярно переривалась паузами або іншими видами діяльності, що знижують навантаження, обумовлене роботою з відеотерміналом, відповідно до вимог розділу 3.8.3 даних правил;

- забезпечує даними Правилами підприємство, керівників служб та структурних підрозділів, безпосередніх керівників робіт, робочі місця яких обладнані відеотерміналами та ЕОМ, та/або які виконують обслуговування, ремонт та налагодження комп'ютерної техніки.

Співробітник має право:

- на інформацію про всі важливі питання його здоров'я та безпеки, пов'язані з перебуванням за робочим місцем.

- Відповідно до Закону України «Про охорону праці» співробітник

зобов'язаний:

- знати та виконувати вимоги нормативно-правових актів про охорону праці, даних Правил, інструкцій з охорони праці, інструкцій щодо експлуатації застосовуваного обладнання, правила поводження з устаткуванням, інструментом та іншими засобами виробництва;

- додержуватись зобов'язань з охорони праці, передбачених колективним договором (угодою, трудовим договором) та правилами внутрішнього трудового розпорядку підприємства, проходити в установленому порядку попередні та періодичні медичні огляди;

- негайно повідомляти власника або безпосереднього керівника робіт про кожну виявлену серйозну та безпосередню небезпеку, про будь-яке пошкодження захисних пристроїв та засобів захисту, про не справності устаткування, інструменту та інших засобів виробництва;

- не відключати захисні пристрої, не проводити самовільних змін конструкції і складу устаткування або його технічного налагоджування.

За безпечність експлуатації, обслуговування, ремонту та налагодження ЕОМ, а також за відповідність обладнання, виробничих приміщень, робочих місць даним Правилам відповідає керівник експертно-криміналістичного підрозділу.

Особи, винні в порушенні цих Правил, несуть дисциплінарну, адміністративну, матеріальну або кримінальну відповідальність згідно з чинним законодавством.

6.2 Забруднення повітря на робочих місцях користувачів ВДТ

Важливо підкреслити, що концентрації різних речовин лише у рідкісних випадках перевищували гранично допустимі концентрації (ГДК) В той же час, у більшості досліджень серед речовин, у яких було виявлено перевищення ГДК у повітрі біля робочих місць з ВДТ найчастіше називалися озон, оксиди азоту, пил.

Особливу небезпеку щодо впливу на здоров'я представляє підвищені концентрація озону — високотоксичного подразнюючого газу. З ці* причини він був внесений у список речовин, максимальні значення концентрації яких на робочих місцях обмежені та строго визначені Надзвичайна небезпека озону для здоров'я людини пов'язана з тим, що вії належить до так званих радіоміметичних речовин — хімічних сполук, що викликають в живих організмах зміни, схожі з тими, які виникають після дії іонізуючого випромінювання. Тому озон вважається не лише подразнюючою, а й канцерогенною речовиною.

Початкові ознаки впливу озону можна визначити суб'єктивно. Так, його можна виявити за запахом, або за сухістю та подразненням слизових оболонок. При більших концентраціях появляються головні болі, недомагання.

Основними джерелами озону на комп'ютеризованих місцях є ЕПТ ВДТ та лазерні принтери. З огляду на це, необхідно виключати ВДТ у випадках, коли він не використовується, а лазерний принтер бажано розташувати подалі від робочого місця оператора. Однак, це додаткові заходи, основним же заходом щодо запобігання несприятливого впливу озону та інших шкідливих речовин на здоров'я операторів є забезпечення функціонування припливно-витяжної вентиляції. Для того, щоб шкідливі речовини не проникали із сусідніх приміщень в приміщеннях з ВДТ необхідно створити деякий надлишковий тиск.

Відповідно до ГОСТ 12.1.005-88 вміст озону в повітрі робочої зони не повинен перевищувати 0,1 мг/м^2; вміст оксидів азоту — 5 мг/м^2; вміст пилу — 4 мг/м^2.

Оскільки найбільш біологічно активними у приміщеннях з ВДТ є частки, які здатні накопичувати електричний заряд, доцільно розглядати наявність дрібних часток. Ці частки звичайно створюються у результаті коагуляції більш дрібних первинних часток.

Група дослідників перевіряла загальну масу завис лих у повітрі часток у деяких обладнаних ВДТ офісах, відбираючи тільки частки менше 10 мкм у діаметрі[1] (аеродинамічний діаметр). За даними 60 вимірювань концентрація

часток вкладала від 10 до 450 мкг/м^3, Виявлено, що у всіх випадках значення вище 150 мкг/м^3 стосувалися приміщень, у яких курили. Там, де не курили, концентрація часток становила 12—40 мкг/м^3. Ці результати знаходяться у повній відповідності з даними інших дослідників, які не виявили будь-якого виливу електростатичних полів ВДТ ні на концентрацію респірабельних часток у повітрі приміщення, ні на зникнення тютюнового диму.

Джерела аерозольних забруднень вельми численні. Звичайно вони зустрічаються у районах, де у повітрі при сутні продукти реакції двооксиду сірки, продукти окислення вуглеводнів» нітрати і т. п., причому склад та концентрації забруднювачів здебільшого залежать від близь кості водоймищ з солоною водою, інтенсивності метеорологічних процесів та ін». Наявність інших забруднювачів залежить від специфічних антропогенних джерел в тому або іншому регіоні (метали, оксиди металів, багато органічних сполук і т, п.). Окрім того, внутрішні джерела суттєво доповнюють концентрацію аерозолів у приміщенні. Одним з основних забруднювачів повітря у приміщеннях, зокрема оксидами вуглецю є тютюновий дим.

Аналіз динаміки бактеріального обсіменіння повітря у приміщеннях з ВДТ показав, що кількість мікроорганізмів помітно збільшується тільки через відсутність вентиляції. Проте слід відзначити, що збільшення вмісту бактеріальної флори також залежить від тривалості роботи користувача з ВДТ. Особливо кількість мікроорганізмів збільшується при безперервній роботі протягом 3 — 4 год (до 2100-2500 мікробних тіл на м^3). Періодичне включення вентиляції у приміщеннях з ВДТ значно знижує кількість бактерій.

Слід зазначити, що у випадках, коли робота користувачів пов'язана з прийняттям відвідувачів у приміщеннях з ВДТ, вміст мікроорганізмів у повітрі приміщень значно зростає і досягає, залежно від числа та тривалості перебування відвідувачів, 7000 та більше мікробних тіл на 1 м^3. Тому при такому режимі роботи необхідно залучати додаткові заходи оздоровлення, повітряного середовища (застосовувати додаткову вентиляцію, обмежувати число та тривалість перебування відвідувачів, конструювати робочі місця,

оснащені загороджувальними стінами з невеликими віконцями для спілкування з відвідувачами).

Згідно з діючими нормативними документами повітря, що надходить у робоче приміщення має бути очищене від забруднень, у тому числі від мікроорганізмів (ВСНиПРВЦ) Запиленість повітря не повинна перевищу вати вимог, викладених у СН 512-78.

Загальна кількість колоній на 1 $м^3$ повітря не повинна перевищувати 1000 та повністю виключається на явність патогенної мікрофлори.

6.3 Класифікація надзвичайних ситуацій

Надзвичайні ситуації (НС) прийнято класифікувати за сферою виникнення, характером протікання, масштабом і ступенем завданого збитку, а також за відомчою приналежністю. За сферою виникнення надзвичайні ситуації поділяються на техногенні, природні, біолого- соціальні і соціальні, екологічні і надзвичайні ситуації військового характеру (рис. 6.1).

Техногенні надзвичайні ситуації

Можуть виникають на основі подій техногенного характеру внаслідок конструктивних недоліків об'єкту (споруди, комплексу, системи, агрегату тощо), зношування устаткування, низької кваліфікації персоналу, порушення техніки безпеки в ході експлуатації об'єкту і так далі. НС техногенного характеру можуть протікати із забрудненням довкілля або без нього.

Забруднення довкілля може відбуватися при аваріях на промислових підприємствах з викидом радіоактивних, хімічно небезпечних, біологічно небезпечних речовин. До аварій з викидом або загрозою викиду радіоактивних речовин (РВ) відносяться аварії, що відбуваються на атомних станціях, ядерних науково-дослідних реакторах, підприємствах ядерно-паливного циклу, атомних судах, при падінні літальних апаратів з ядерними енергетичними установками на борту, а також на підприємствах ядерно-збройного комплексу. В результаті таких аварій може виникнути сильне радіоактивне забруднення місцевості або акваторії.

До НС техногенного характеру відноситься також електро- магнітне забруднення довкілля при функціонуванні техногенних джерел електромагнітного випромінювання (EMI), що створюють електромагнітні поля підвищеної інтенсивності.

До НС без забруднення довкілля відносять аварії, що супроводжуються вибухами, пожежами, руйнуванням будівель (споруд), порушенням систем життєзабезпечення, руйнуванням гідротехнічних систем, порушенням транспортних комунікацій і тому подібне.

Надзвичайні ситуації природного характеру

Виникають як правило, в результаті катастроф стихійних лих та інших природних явищ, викликаних як зовнішніми, так і внутрішніми причинами дії різних сил природи на біосферу. Зовнішні дії обумовлені впливом далекого космосу (Галактика, Сонячна система), накладенням процесів ближнього космосу (магнітосфери, атмосфери), а також процесами, що виникають безпосередньо на поверхні Землі.

Рис. 6.1. Класифікація надзвичайних ситуацій

Внутрішні процеси Землі пов'язані з диференціацією речовини і розшаруванням її за фізико-механічними властивостями, вони супроводжуються такими явищами, як інверсія магнітного поля, магматична і тектонічна активність, рух літосферних плит, вулканізм, сейсмічність тощо. Усі ці процеси з різною періодичністю в часі діють на біосферу і сприяють виникненню катастроф. Статистичний аналіз показує, що з природних явищ, з

точки зору нанесення збитку і ураження людей, на першому місці стоять повені. Далі йдуть землетруси, виверження вулканів, кліматичні зміни, погодні дії. При цьому існує небезпечна тенденція збільшення числа природних катастроф, зараз їх відбувається в п'ять разів більше, ніж в 60-х роках, а економічний збиток від них зріс більш, ніж у 8 разів.

Крім того, швидкий розвиток продуктивних сил, безконтрольне освоєння вільних територій, праця в районах з кліматичними умовами, де зберігається постійна небезпека виникнення природних катаклізмів збільшують ступінь ризику і масштаби втрат і збитку для населення і економіки. Нерідко природні явища стають прямою або непрямою причиною аварій і катастроф техногенного характеру.

Природні НС поділяються за підгрупами відповідно до небезпечності, і типу стихії, що їх викликає, на: геофізичні, геологічні, метео- і агрометеорологічні, морські гідрогеологічені, гідрологічно небезпечні явища і природні пожежі.

Кожна група стихійних лих класифікується по характеру явищ, які визначають особливості дії властивих їм вражаючих (руйнівних) чинників на населення, природу і об'єкти економіки.

До стихійних лих, пов'язаних з геофізично небезпечними явищами, відносяться землетруси, виверження вулканів і тому подібне. До геологічних небезпечних явищ відносяться зсуви, селі, осипи, лавини. Такі природні явища, як селеві потоки і лавини

найчастіше виникають в гірських районах.

Стихійні лиха, пов'язані з метеорологічними і агрометео- рологічними небезпечними явищами підрозділяються на лиха, що викликаються вітром (бурі, урагани, шквали і смерчі), сильним дощем (при кількості опадів 50 мм протягом 12 год і менше), великим градом (при діаметрі градин 20 мм і більше), сильними снігопадами (при кількості опадів 20 мм і більше за 12 год і менше), сильними завірюхами (при швидкості вітру 15 м/с); сильною ожеледдю, заморозками і суховіями.

Стихійні лиха, пов'язані з морськими гідрологічними небезпечними явищами, підрозділяються на лиха, що викликаються сильним хвилюванням на морях (при висоті хвиль, особливо небезпечних для мореплавання і берегових споруд), цунамі (при затопленні населених пунктів і об'єктів економіки) тощо. Гідрологічні небезпечні явища можуть бути викликані високими рівнями води, повенями і низьким рівнем води на судноплавних ріках, селями, що утворилися при прориві загат, завальних і морених озер із загрозою населеним пунктам та іншим важливим обьектам.

Природні пожежі, в першу чергу лісові і торфяні, є найпоширенішими лихами для населення, економіки і природного середовища.

До біолого-социальних НС відносяться інфекційні захворювання людей, сільськогосподарських тварин і ураження сільськогосподарських рослин різного масштабу. До соціальних НС відносяться: падіння репродукції населення, масові заворушення серед населення, тероризм в різних сферах його прояву, негативна обстановка в творчих і виробничих колективах тощо.

До надзвичайних ситуацій екологічного характеру відносять зміни стану атмосфери, суші, гідросфери і біосферу в цілому. НС екологічного характеру найчастіше виникають в результаті несприятливого впливу техногенної діяльності людини на довкілля, хоча часто їх причиною можуть бути стихійні явища, а також комплексна дія техногенних і природних чинників, В результаті порушень стану атмосфери можлива зміна клімату, виникнення гострого кисневого голодування у великих містах, утворення великих зон "кислотних дощів", руйнування озонового шару над населеними територіями та інші подібні явища. Несприятливі зміни в стані суші можуть призводити до деградації грунтів, втрати корисних площ і виснаження невідновлюваних запасів корисних копалини.

ВИСНОВКИ

У данній кваліфікаційній роботі було розроблено комп’ютерну мережу Костільницької ЗОШ І-ІІ ст. Бучацького р-ну з можливістю виходу в Internet.

Зроблено аналітичний огляд існуючих рішень в сфері проектування та встановлення провідних та безпровідних мереж, описано стандарти передачі даних.

Розроблено логічну та фізичну топології мережі, вибрано активне і пасивне комутаційне обладнання для мережі.

Описано процедуру інсталяції операційної системи ОС Ubuntu Server 16.04 LTS та розроблено інструкцію з налаштування параметрів роботи комутатора DGS-1100-16. Також організовано захист мережі від несанкціонованого доступу.

Результати дослідження були представлені під заголовком засобів інформаційних технологій шкіл і досліджень, проведених у школах, внеском управління інформаційними системами, а також проблемами, що виникають у досвіді роботи інформаційних систем керівників шкіл.

Робота містить детальний аналіз використаних технологій та опис побудови проекту і всіх його складових. Результатом виконання є повний пакет документації та 4-х листів графічної частини, які дозволять легко впровадити проект.

ПЕРЕЛІК ПОСИЛАНЬ

1. Буров Є. Комп'ютерні мережі. Львів: БаК, 2006.-468с.
2. Ватаманюк А.И. Беспроводная сеть своими руками. - СПб.:Питер, 2006.-192с.
3. Гук М. Аппаратние средства локальних сетей. Енциклопедия - СПб: Издательство "Питер" , 2000. - 576 с.
4. Жидецький В.Ц. Охорона праці користувачів комп'ютерів. Навчальний посібник. - Вид. 2-ге, доп. - Львів: Афіша, 2000. - 176с.
5. Кульгин М.В. Компьютерные сети. Практика построения. Для профессионалов. 2-е изд.- СПб.:Питер, 2003.-462с.:ил.
6. Москальова В. М. Основи охорони праці. Підручник. - Київ: ВД Професіонал, 2005.-666 с.
7. Оглтри Терри Модернизация и ремонт сетей, 4-е изд. : Пер с англ. - М.:Издательский дом "Вильямс", 2005. - 1328с.
8. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. - СПб.: Питер, 2006 - 958с.:ил.
9. Олтри Терри Модернизация и ремонт сетей, 2-е изд. : Пер с англ.: Учюпос. - М.:Издательский дом "Вильямс", 2000. - 928с.
10. Стивен Браун. Виртуальные частные сети. - М.:Лори, 2001.-504с.
11. Таненбаум Э. Компьютерные сети. 4-е изд. - СПб.: Питер, 2003. - 992 с: ил.
12. Холмогоров В. Компьютерная сеть своими руками. Самоучитель. - СПб.: Питер, 2003.- 171с.:ил.
13. Шкарабана С.І., Сапачова М.І. "Економічний аналіз діяльності промислових підприємств" - Тернопіль, ТАНГ 2009. 405с.
14. Сервер Impression Web Server NetNavigator H 1215 [Електронний ресурс] - Режим доступу до ресурсу: http://rozetka.com.ua/ua/impression_web_server_netnavigator_h_1215 - Дата доступу: 11.06.2020. - Заголовок з екрану.

15. RFC [Електронний ресурс] - Режим доступу до ресурсу: http://www.rfc-editor.org/ - Дата доступу: 12.09.2020. - Заголовок з екрану.

16. D-Link [Електронний ресурс] - Режим доступу до ресурсу: www.dlink.ua - Дата доступу: 10.08.2020. - Заголовок з екрану.

17. opennet [Електронний ресурс] - Режим доступу до ресурсу: www.opennet.ru - Дата доступу: 1.08.2020. - Заголовок з екрану.

18. price.ua [Електронний ресурс] - Режим доступу до ресурсу: http://price.ua / - Дата доступу: 12.10.2020. - Заголовок з екрану.

19. Ubuntu [Електронний ресурс] - Режим доступу до ресурсу: https://www.ubuntu.com/- Дата доступу: 06.10.2020. - Заголовок з екрану.

20. Оглтри Т. Модернизация и ремонт сетей. Пер. с .англ. -М.: QUE, 2000. –928с.,іл.

21. Ю. Шафрин, «Основы компьютерной технологии». М., АБФ, 1997

22. Э.А. Якубайтис, «Информатика – электроника - сети». М., «Финансы и статистика», 1989

23. Протоколы информационно-вычислительных сетей. Справочник под ред. И. А. Мизина, А. П. Кулешова. М., "Радио и связь" 1991.

24. К. Ги Введение в локальные вычислительные сети . М., "Радио и связь" 1986.

25. Д.А. Богданова, «Телекоммуникации в школе». «Информатика и образование», №№ 1-3, 1996

26. Спесивцев А.В. «Защита информации в персональных ЭВМ», М., Радио и связь, 1992

27. Жидецький В.Ц. Охорона праці користувачів комп’ютерів. Навчальний посібник. - Вид. 2-ге, доп. – Львів: Афіша, 2000 – 176 с.

28. Ніконенко Ю.В., Віденко М.М., Шегда А.В. Основи економічної теорії. К.: - Либідь, 1994, - 270с.

29. Основи охорони праці: Підручник. 3-тє видання, доповнене та перероблене. / К. Н. Ткачук, М. О. Халімовський, В. В. Зацарний, Д. В. Зеркалов, Р. В. Сабарно, О. І. Полукаров, В. С. Коз'яков, Л. О. Мітюк, Ю. О. Полукаров. – К.: Основа, 2011. – 480 с.