Міністерство освіти і науки України Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Дегтерьова Радомира Павловича*

академічної групи 125-19-1

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему **Розробка комплексної системи захисту інформації в інформаційно-комунікаційній системі підприємства Ziber**

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи				
розділів:				
спеціальний				
економічний				

Рецензент				

Нормоконтролер				

Дніпро 2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту **Дегтерьову Р.П.** (прізвище та ініціали) **академічної групи** **125-19-1** (шифр)

спеціальності **Кібербезпека**

спеціалізації _____

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

на тему **Розробка комплексної системи захисту інформації в інформаційно-комунікаційній системі підприємства Ziber**

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _____№ _____

Розділ	Зміст	Термін виконання
Принципи побудови інформаційно-комунікаційної системи підприємства	розкрити основні можливості корпоративних інформаційно-комунікаційних систем та описати процес створення таких корпоративних інформаційних систем; привести особливості віртуальної мережі передачі даних та назвати технології, що використовуються в корпоративних інформаційно-комунікаційних системах; перелічити основні принципи захисту інформації при підключенні до мережі Інтернет;	
Розробка комплексної системи захисту корпоративної інформаційної системи підприємства Ziber на базі обладнання Keenetic	детально дослідити основні етапи проєктування комп'ютерної мережі на базі обладнання Keenetic; навести розрахунок необхідної кількості комп'ютерного устаткування корпоративної комунікаційної системи, зробити вибір і обґрунтування програмного забезпечення корпоративної комунікаційної системи, вибір серверного обладнання та комутаційного обладнання корпоративної комунікаційної системи (Keenetic Ultra, Giga, Viva і т.д.); зробити побудову корпоративної комунікаційної системи на основі вибраного обладнання та забезпечити захист створеної мережі; розробити програмний засіб захисту транспортування даних у мережі.	
Економічне обґрунтування запропонованих рішень	провести економічне обґрунтування запропонованих рішень	

Завдання видано _____ _____

(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ _____

(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Записка: 99 стор., 39 рис., 13 таблиць, 9 додатків, 61 джерело.

Метою дослідження в роботі є створення комплексного програмно-апаратного засобу захисту корпоративної комунікаційної системи на базі обладнання Keenetic.

Об'єктом дослідження є сукупність необхідних умов, що забезпечують найкращий підхід для розуміння порядку створення інформаційно-захищеної корпоративної комунікаційної системи.

Предметом дослідження є проєкт комплексного захисту корпоративної комунікаційної системи на базі обладнання Keenetic.

Методи дослідження: теоретичний аналіз наукової літератури; аналіз та узагальнення. Статистичні дані та порівняння. Класифікація теоретичного матеріалу та розробка рекомендацій. Проєктування.

Результати – розкрито основні можливості корпоративних інформаційно-комунікаційних систем та описати процес створення таких корпоративних інформаційних систем; наведено особливості віртуальної мережі передачі даних та назвати технології, що використовуються в корпоративних інформаційно-комунікаційних системах; окремо наведено особливості захисту інформації такими способами, як NAT-перетворення, можливість PAT, демілітаризована зона, антивірусний захист КМ, функція ACL та захист інформації за допомогою міжмережних екранів; детально досліджено основні етапи проєктування комп'ютерної мережі на базі обладнання Keenetic; розроблено програмний засіб захисту транспортування даних у мережі підприємства.

В економічній частині розраховано затрати на покупні вироби та витратні матеріали для створення локальної мережі підприємства, проаналізована основна заробітна плата та наведена калькуляція собівартості інформаційно-комунікаційної системи.

МАРШРУТИЗАТОР, МОДЕЛЮВАННЯ МЕРЕЖІ, ЗАХИСТ ІНФОРМАЦІЇ, БЕЗПЕКА, ЛОКАЛЬНА МЕРЕЖА, ПРОГРАМНИЙ КОД, ТРАНСПОРТУВАННЯ ДАНИХ, ІНФОРМАЦІЙНА СИСТЕМА.

ABSTRACT

The thesis consists of 99 pages, 39 figures, 13 tables, 9 appendices, and references to 61 sources.

The aim of this research is to develop a comprehensive software-hardware system for protecting a corporate communication system based on Keenetic equipment.

The object of our research is the set of necessary conditions that provide the best approach to understanding the process of creating an information-secure corporate communication system.

The subject of the research is the project of comprehensive protection of a corporate communication system based on Keenetic equipment.

The research methods include theoretical analysis of scientific literature, analysis and synthesis, statistical data and comparisons, classification of theoretical material, and development of recommendations. Design.

The results reveal the main capabilities of corporate communication systems and describe the process of creating such information systems. It discusses the features of virtual data transmission networks and technologies used in corporate communication systems. It specifically highlights the information protection features such as NAT transformation, PAT capability, demilitarized zone, antivirus protection, ACL function, and information protection using firewalls. The main stages of designing a computer network based on Keenetic equipment are examined in detail. A software tool for securing data transportation within the enterprise network has been developed.

The economic section includes calculations of expenses for purchasing products and consumables for creating a local enterprise network. The main salary expenses are analyzed, and the cost calculation of the communication system is provided.

ROUTER, NETWORK MODELING, INFORMATION SECURITY, SAFETY, LOCAL NETWORK, SOURCE CODE, DATA TRANSPORTATION, INFORMATION SYSTEM.

ЗМІСТ

ВСТУП

Однією з видимих тенденцій останнього часу став розвиток інтенсивний корпоративних інформаційно-комунікаційних систем виробничих підприємств. Причому ці зміни помітні не тільки у великих містах, але і в регіонах.

Актуальність дослідження. Зміст понять «корпоративна комунікаційна система» та «інформаційно-комунікаційна система» можна трактувати, як групу організацій, яка незалежно від організаційно-правової форми окремих одиниць або групи в цілому і незалежно від деталей системи управління, об'єднана наявністю спільних організаційних, матеріальних і технологічних ресурсів [4, с. 19]. Іншими словами, всередині такої інформаційно-комунікаційної системи відбувається досить вільний обмін інформацією, засобами, кадрами. У державних установах елементи мережевої структури можуть бути представлені у вигляді адміністративних і нормативних зв'язків між організаційними одиницями. Структура, що визначає характеристики мережі, є важливим параметром корпоративної комунікаційної системи. Саме тому структура мережі може розглядатися як об'єкт управління, вплив на який дозволяє управляти потоками даних, що є основним завданням управління мережею.

В даний час розроблено і використовується велика кількість потужних систем управління захистом корпоративних інформаційно-комунікаційних систем. Це дозволяє вивчити результати їх роботи і підкреслити загальні для них позитивні і негативні сторони. Пов'язано це з необхідністю враховувати особливість роботи корпоративної системи, що вимагає відповідних методів управління її роботою і налаштувань корпоративної комунікаційної системи. Таким чином, постійно поглиблюється розрив між зростаючими можливостями систем управління та реальними потребами при управлінні, спрямованим на конкретні докладання.

В наслідок цього розробляються нові концептуальні підходи до управління корпоративними мережами. Вони спрямовані на вирішення необхідного набору

прикладних завдань, які при застосуванні універсальних багатофункціональних систем управління забезпечують необхідну якість їх рішення. Рішення проблеми базується на розробці підходів до управління корпоративною мережею, що поєднує облік специфіки розв'язуваних завдань і можливості діючих систем управління. Представлене дослідження стосується створення захищеної корпоративної комунікаційної системи приватного підприємства на базі обладнання Keenetic.

Ступінь розробки теми. Комплексному дослідженню сутності корпоративних інформаційно-комунікаційних систем, розробці технологій реалізації та впровадження різного роду систем присвятили свої роботи такі вітчизняні та іноземні фахівці як: В. Г. Хоменко та М. П. Павленко [56], які запропонували новий аналітичний підхід до підготовки проєктів впровадження корпоративних інформаційних систем в організації. Питання створення захищеної корпоративної комунікаційної системи досліджувалися як українськими, так і зарубіжними вченими. Серед них можна виділити роботи В. М. Фурашев, Д. В. Ланде [55], І. Г. Тарахнов [50], В. І. Романчук, О. А. Лаврів, Р. І. Бак [41], К. В. Панфілов [37], Д. Куроуз, К. Росс [27], А. В. Зав'ялов [17], В. Л. Бурячок, А. О. Аносов [8].

Мета дослідження в роботі — створення комплексного програмно-апаратного засобу захисту корпоративної комунікаційної системи на базі обладнання Keenetic.

Об'єктом дослідження є сукупність необхідних умов, що забезпечують найкращий підхід для розуміння порядку створення інформаційно-захищеної корпоративної комунікаційної системи.

Предметом дослідження — проєкт комплексного захисту корпоративної комунікаційної системи на базі обладнання Keenetic.

Методи дослідження: теоретичний аналіз наукової літератури; аналіз та узагальнення. Статистичні дані та порівняння. Класифікація теоретичного матеріалу та розробка рекомендацій. Проєктування. Вирішення поставлених у роботі завдань здійснювалося з використанням системного підходу в доборі

матеріалу, методів індуктивного і логічного аналізу, статистичні методи аналізу літературних даних. У процесі роботи, залежно від поставлених цілей і завдань, використовувалися відповідні методи аналізу: структурного і системного, порівняльного і факторного аналізу, які ґрунтуються на застосуванні основних принципів логічних та статистичних методів оцінки первинного матеріалу.

Завдання дослідження полягає в:

- розкрити основні можливості корпоративних інформаційно-комунікаційних систем та описати процес створення таких корпоративних інформаційних систем;
- привести особливості віртуальної мережі передачі даних та назвати технології, що використовуються в корпоративних інформаційно-комунікаційних системах;
- перелічити основні принципи захисту інформації при підключенні до мережі Інтернет;
- окремо навести особливості захисту інформації такими способами, як NAT-перетворення, можливість PAT, демілітаризована зона, антивірусний захист КМ, функція ACL та захист інформації за допомогою міжмережних екранів;
- детально дослідити основні етапи проєктування комп'ютерної мережі на базі обладнання Keenetic;
- навести розрахунок необхідної кількості комп'ютерного устаткування корпоративної комунікаційної системи, зробити вибір і обґрунтування програмного забезпечення корпоративної комунікаційної системи, вибір серверного обладнання та комутаційного обладнання корпоративної комунікаційної системи (Keenetic Ultra, Giga, Viva і т.д.);
- зробити побудову корпоративної комунікаційної системи на основі вибраного обладнання та забезпечити захист створеної мережі;
- розробити програмний засіб захисту транспортування даних у мережі.

Новизна дослідження. Зроблено широкий літературний пошук з детальним аналізом наукової інформації. Проведено систематизацію та адаптацію отриманих літературних результатів. Зроблено рекомендації для покращення існуючої

системи формування доходів від реалізації продукції сільськогосподарських підприємств.

Джерелами інформації для вирішення перерахованих вище завдань є збірники наукових праць, монографії, періодична література, підручники та довідники, періодичні фахові журнали.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

1.1.1 Основні можливості інформаційно-комунікаційних систем

Як вже було сказано у вступі, корпоративна комунікаційна система – це складний комплекс взаємопов'язаних і узгоджено функціонуючих апаратних і програмних компонентів, що забезпечує передачу інформації між різними віддаленими додатками і системами, використовуваними на підприємстві. Через наявність декількох центрів обробки даних корпоративні мережі належать до децентралізованих (або розподілених) обчислювальним системам.

Корпоративну мережу необхідно розглядати з різних сторін: структурної, функціональної та системно-технічної. Із структурної точки зору корпоративна комунікаційна система – мережа змішаної топології, яка містить кілька локальних обчислювальних мереж. Корпоративна комунікаційна система об'єднує філії підприємства створюючи спільний інформаційний корпоративний простір. З цієї точки зору корпоративна комунікаційна система відображає структуру установи. З функціональної точки зору корпоративна комунікаційна система – це ефективне середовище передачі актуальної інформації необхідної для вирішення завдань [1, с. 45].

Сучасна корпоративна комунікаційна система – це не тільки мережа передачі даних, а складний комплекс, який здатний надавати різні сервіси з прогнозованими характеристиками. Завдяки корпоративним мережам результативно вирішуються завдання ключових процесів. Таких як:

- швидкий доступ до інформаційних масивів загального інформаційного простору;
- аналіз стану та управління бізнес-процесами з єдиного аналітичного центру;
- обмін інформаційними та розрахунковими документами;
- безперервне автоматизоване спостереження (моніторинг) і управління ресурсами інфокомунікаційної системи з Єдиного центру.

Основними перевагами впровадження корпоративних інформаційно-комунікаційних систем є:

- отримання точної та оперативної інформації про роботу всіх підрозділів компанії;
- зростання ефективності управління організацією;
- скорочення витрат робочого часу на виконання робітниками певних процесів;
- зростання результатів роботи за рахунок більш доцільної її організації.

До найбільш суттєвих особливостей корпоративних інформаційно-комунікаційних систем можна віднести наступні:

- масштабність системи, адже корпоративна комунікаційна система включає велику кількість комп'ютерів на великій території, які пов'язані між собою;
- гетерогенність – тобто неоднорідність обладнання, протоколів, операційних систем, додатків;
- використання глобальних зв'язків – корпоративна комунікаційна система для з'єднання віддалених локальних мереж і окремих комп'ютерів використовує всі типи глобальних зв'язків, в тому числі телефонні канали, радіоканали, супутниковий зв'язок, комерційні мережі з комутацією каналів і пакетів;
- Інтегрованість – неоднорідні частини і підмережі корпоративної комунікаційної системи повинні працювати як єдине ціле, надаючи користувачам по можливості прозорий доступ до всіх необхідних ресурсів. Незалежно від того, яке обладнання придбано, корпоративна комунікаційна система повинна бути здатна інтегрувати вже наявні на підприємстві комп'ютерні системи [6, с. 210];
- підвищені вимоги до надійності – в корпоративній мережі виконуються стратегічно важливі для роботи підприємства додатки і зберігаються такі ж важливі дані, тому така мережа повинна мати мінімально можливий час простоїв основних компонентів через збої і відмови, а критична інформація не повинна втрачатися;

- підвищені вимоги до керованості мережі – масштабність мережі вимагає розвинених багатофункціональних засобів управління мережею, інакше витрати експлуатації мережі з великим штатом фахівців набагато перевищать принесені вигоди. У корпоративних інформаційно-комунікаційних системах користувачі висувають дуже жорсткі вимоги до часу усунення відмови обладнання, тому апаратна надмірність і планування відновлення після відмов є дуже важливими. Адміністратори корпоративних інформаційно-комунікаційних систем потребують комплексних системах, що дозволяють їм не стільки оперативно реагувати на виникаючі відмови, скільки попереджати їх виникнення, наприклад, шляхом аналізу тенденцій в продуктивності мережі і виявлення проблем до того, як вони проявилися у вигляді відмов;
- універсальний характер розв'язуваних завдань – у той час як локальні мережі, як правило, мають спеціалізацію, для корпоративної комунікаційної системи звичайним є наявність найрізноманітніших завдань, таких як автоматизація діловодства і автоматизація технологічних процесів, розробка програмних додатків і інформаційний пошук [20, с. 195];
- широта охоплення технічних проблем – при проєктуванні корпоративної комунікаційної системи розробники мають справу з найширшим колом технічних питань (від мейнфреймів до ПК, від операційних систем до самих різних додатків, від вибору кабельної системи локальних мереж до вибору типу глобальних зв'язків, від питань сполучення різнорідних мережевих архітектур до проблем структуризації мережі з використанням всього різноманіття комунікаційного обладнання);
- потреба в наявності на підприємстві фахівців різних профілів високої кваліфікації – створення корпоративної комунікаційної системи та управління нею вимагає наявності проєктувальників мережі, інсталяторів мережі та адміністраторів мережі.

1.2 Постановка задачі

1.2.1 Процес створення корпоративної інформаційно-комунікаційної системи

Об'єднання офісних локальних мереж в єдину корпоративну мережу організації може здійснюватися:

- з використанням бездротових мереж передачі даних. Застосовується при побудові корпоративної комунікаційної системи між робочими майданчиками, розташованими в близько розміщених будівлях;
- з використанням Internet у якості транспортного середовища передачі даних, з використанням технології побудови VPN тунелів;
- з використанням орендованих каналів передачі даних. Можлива побудова мережі із застосуванням технології побудови VPN тунелів або без.

Об'єднання офісних мереж з використанням бездротового обладнання має такі переваги [12, с. 58]:II

- швидкість і простота розгортання локальної мережі;
- невисокі витрати на придбання обладнання;
- низька вартість експлуатації і відсутність абонентської плати;
- збереження інвестицій в локальну мережу при переїзді і зміні офісу.

Основними недоліками об'єднання офісних мереж з використанням бездротового обладнання є наявність «прямої видимості» між офісними майданчиками (у разі відсутності, необхідно проводити тестові випробування можливості підключення) та зниження швидкості передачі даних зі збільшенням відстані.

Використання Internet в якості транспортного середовища передачі даних, при побудові корпоративної комунікаційної системи підприємства має такі переваги:

- низька абонентська плата;
- простота реалізації.

Її недоліками є невисока надійність та відсутність гарантованої швидкості передачі даних.

Об'єднання локальних мереж підприємства в єдину корпоративну мережу на основі орендованих каналів передачі даних має такі переваги:

- висока якість наданих каналів передачі даних;
- високий рівень послуг і сервісів, що надаються провайдером;
- гарантована швидкість передачі даних.

Основна мета проєктування корпоративних інформаційно-комунікаційних систем полягає в тому, щоб визначити структуру, склад апаратно-програмних засобів та організацію корпоративної комунікаційної системи. І при заданих обмеженнях на витрати по проєктуванню, впровадженню та обслуговуванню вони будуть виконувати основні вимоги до якості інформаційних послуг, що надаються мережею [14, *с.* 33]. Процес будування відбувається на підставі характеристик корпоративних інформаційних потоків підприємства, параметрів споживачів і виробників інформації. Один з підходів до класифікації корпоративних інформаційно-комунікаційних систем наведено в додатку А роботи.

Враховуючи масштабність, використання глобальних зв'язків, високий ступінь різнорідності проєктування корпоративних інформаційно-комунікаційних систем є важко формалізуємими процесами. У сьогоднішній день відсутні універсальні методики проєктування корпоративних інформаційно-комунікаційних систем. Тому необхідно сформулювати деякі типові етапи виконання мережевих проєктів. Процес проєктування корпоративної комунікаційної системи складається з наступних етапів:

- аналіз вимог. На цьому етапі формулюються основні цілі підприємства (оперативний прийом замовлень, скорочення виробничого циклу, підвищення продуктивності праці). Аналізуються існуючі аналогічні системи, обґрунтовується необхідність у власних проєктах системи;
- розробка технічної моделі корпоративної комунікаційної системи (структурний синтез). Технічна модель являє собою сукупність технічних засобів, необхідних для реалізації проєкту корпоративної комунікаційної системи. На даному етапі визначаються технічні параметри компонентів

мережі, такі як повний функціональний набір необхідних програмних і апаратних засобів, але без конкретизації обладнання (марок і моделей);

- моделювання та оптимізація корпоративної комунікаційної системи. Моделювання проводиться на даному етапі з метою оцінки характеристик функціонування корпоративної комунікаційної системи та їх оптимізації [25, с. 420];
- установка і налагодження корпоративної комунікаційної системи. На цьому етапі мається на увазі управління конфігураціями, координування поставок від субпідрядників, інсталяцію та налагодження обладнання, навчання персоналу;
- тестування корпоративної комунікаційної системи. На цьому етапі повинні проводитися необхідні випробування, описані в контракті з інтегратором;
- супровід та експлуатація корпоративної комунікаційної системи. Останній етап не має чітких часових меж, він передбачає безперервний процес.

В даний час набирає популярність багаторівнева архітектура, з огляду на те, що вона має багато таких переваг перед архітектурами файл-серверу і клієнт-серверу як:

- масштабованість;
- конфігурованість – ізольованість рівнів один від одного робить можливим миттєво і легкими засобами переконфігурувати систему при виникненні неполадок або при плановому обслуговуванні на одному з рівнів;
- високий рівень безпеки та ступінь надійності;
- невисокі вимоги до швидкості каналу (мережі) між терміналами і сервером додатків;
- невисокі вимоги до продуктивності і технічним характеристикам терміналів, тим самим відбувається зменшення їх вартості.

Але слід наголосити, що наведена архітектура мережі не змогла скласти конкуренцію іншим мережам завдяки:

- виникаючим труднощам під час розробки систем, адже складно узгодити різні модулі, через те, що вони були спроєктовані різними класами

розробників. Як правило, зміна в одному плагіні призводить до обвальних змін в інших, виходячи з цього, неважко зробити висновок, що навіть саму елементарну систему, засновану на багаторівневій архітектурі, буде важче довести до ладу [30, с. 40];

- високим вимогам до ефективності роботи серверів додатків і сервера бази даних, що в свою чергу, збільшує вартість серверного обладнання;
- створеним завищеним умовам до забезпечення швидкості на лінії (мережі) між сервером бази даних і серверами додатків;
- існуванню великих труднощів по адмініструванню.

На даний час перспективною є технологія CASE (Computer Aided Software Engeneering). Початкове значення терміна CASE, яке було обумовлено питаннями автоматизації розробки виключно програмного забезпечення, в даний час отримало новий сенс, який охоплює процес розробки складних інформаційних систем. У порівнянні з традиційною технологією класичного проєктування CASE-технології володіють наступними перевагами:

- розвитком якості розроблюваного програмного продукту за рахунок засобів автоматичного контролю та генерації;
- можливістю використання елементів розробки повторно;
- підтриманням адаптивності та супроводу інформаційної системи;
- скороченням часу розробки системи – і це якраз те, що робить можливим на ранніх стадіях проєктування створення прототипу майбутньої системи.

1.2.2 Технології, що використовуються в інформаційно-комунікаційних системах підприємств

Побудова сучасних корпоративних інформаційно-комунікаційних систем ґрунтується на комплексному підході, що довів свою ефективність і надійність. Комплексний підхід орієнтований на створення захищеного середовища обробки інформації в корпоративних інформаційно-комунікаційних системах. Сюди відносяться правові, морально-етичні організаційні програмні і технічні способи забезпечення інформаційної безпеки. Основними технологіями, що

використовуються для побудови корпоративних інформаційно-комунікаційних систем, є Ethernet, Token Ring та FDDI. В технології Ethernet застосовується дуже простий алгоритм доступу, який дозволяє вузлу мережі передавати дані в ті моменти часу, коли він вважає, що розділене середовище вільне. Простота технології Ethernet визначила простоту та низьку вартість обладнання Ethernet. Негативним атрибутом алгоритму доступу технології Ethernet є ситуації, коли кадри, що передаються різними станціями, зіштовхуються одне з одним в загальному середовищі. Такі ситуації знижують ефективність розділеного середовища та надають роботі з мережею непередбачуваного характеру. Початковий варіант технології Ethernet був розрахований на коаксіальний кабель, який використовувався всіма вузлами мережі в якості загальної шини. Перехід на кабельні системи на концентраторах (хабах) суттєво підвищив експлуатаційні характеристики мереж Ethernet [33, с. 302].

В технологія Token Ring та FDDI підтримувались більш складні та ефективні алгоритми доступу до середовища, засновані на передачі одне одному токену – спеціального кадру, який дозволяє доступ. Однак цієї переваги не було достатньо для успішного конкурування з технологією Ethernet.

Серед популярних мережевих технологій побудови локальних мереж можна виокремити Token Ring та FDDI. Дані технології є функціонально складнішими технологіями, ніж всі інші. Розробники цих технологій намагались наділити корпоративні мережі багатьма позитивними якостями: створити механізм розділення середовища керованим та передбачуваним, забезпечити відмовостійкість мережі, організувати пріоритетне обслуговування для чутливого до затримок трафіку, наприклад, голосового. Механізм доступу в середовищі в мережах Token Ring та FDDI є більш детермінованим, ніж в мережах Ethernet. Зазвичай вузли в мережах Token Ring та FDDI зв’язані між собою у кільце, тобто одна станція може отримувати інформацію тільки від однієї станції – від тієї, яка є попередньою в кільці, а передавати дані може тільки наступному сусіду вниз по потоку даних. Швидкість передачі даних в перших мережах Token Ring,

розроблених компанією IBM, була всього 4 Мбіт/с, але згодомцей показник було підвищено до 16 Мбіт/с. Основним середовищем передачі даних є вита пара.

Для адресації мереж Token Ring та FDDI використовують MAC-адреси такого ж формату як і Ethernet. Метод доступу в технології Token Ring заснований на передачі від вузла до вузла спеціального кадру – токену, або маркеру доступу, при цьому тільки вузол, у якого знаходиться цей маркер, може передавати свої кадри в мережу, яка в цьому випадку стає розділеним середовищем. Існує певне обмеження на період монопольного використання середовища – так званий час утримання токену, по закінченню якого вузол повинен передати токен сусідньому по кільцю вузлу. В результаті такі ситуації, як невизначений час очікування доступу до середовища, які характерні для Ethernet, тут недопустимі (у випадках, коли мережеві адаптери станцій працюють без збоїв).

Мережу Token Ring за технологією FDDI (Fiber Distributed Data Interface, волоконно-оптичний розподілений інтерфейс даних) можна вважати покращеним варіантом Token Ring, оскільки в ній, як і в Token Ring, використовується доступ до середовища, що засноване на передачі токена, а також кільцева топологія зв'язків, але разом з цим FDDI працює на більш високій швидкості та має більш досконалий механізм відмовостійкості. Технологія FDDI стала першою технологією корпоративних інформаційно-комунікаційних систем, в якій оптичне волокно було використано в якості розділеного середовища передачі даних [36, с. 560].

За рахунок використання оптичних систем швидкість передачі даних вдалось підвищити до 100 Мбіт/с (пізніше з'явилось обладнання FDDI на витій парі, яке працює на такій ж швидкості). У тих випадках, коли потрібно було забезпечити високу надійність мережі FDDI, застосовувалось подвійне кільце. В нормальному режимі станції використовують для передачі даних і токену доступу первинне кільце, а вторинне простоює. У випадку відмови, наприклад, при обриві кабелю між станціями 1 і 2, первинне кільце об'єднується із вторинним, знову створюючи єдине кільце. Цей режим роботи мережі називається режимом

згортання кілець. Операція згортання виконується засобами повторювачів та мережевих адаптерів FDDI.

Для спрощення цієї процедури дані по первинному кільцю завжди передаються в одному напрямку, а по вторинному – у зворотному. Тому при створення спільного кільця із двох кілець передавачі станцій залишаються підключеними до приймачів сусідніх станцій, що дозволяє правильно передавати та приймати інформацію сусіднім станціям. Однією з базових технологій локальних комп'ютерних мереж з комутацією пакетів є технологія Ethernet. Ця технологія використовує протокол CSMA / CD (множинний доступ з контролем несучої та виявленням колізій). Цей протокол дозволяє в певний момент часу лише один сеанс передачі в логічному сегменті мережі. При появі двох і більше сеансів передачі одночасно виникає колізія, яка фіксується станцією, що ініціює передачу. Для передачі даних технологія Ethernet може використовувати:

- коаксіальний кабель з діаметром 0,5 дюйма, «товстий» коаксіал – стандарт 10Base – 5;
- коаксіальний кабель з діаметром 0,25 дюйма, «тонкий» коаксіал – стандарт 10Base – 2;
- неекранована вита пара (UTP, Unshielded Twisted Pair) – стандарт 10Base-T;
- оптоволоконний кабель – стандарт 10Base-F.
- Дана технологія лежить в основі кількох швидкісних технологій: Fast Ethernet (100 Мбіт/с), Gigabit Ethernet (1000 Мбіт/с), 10 Gigabit Ethernet (10 Гбіт/с). Порівняльна характеристика технологій побудови локальної мережі представлена в таб. 1.1.

Таблиця 1.1 - Порівняльна характеристика технологій побудови локальної мережі

Характеристика	Ethernet	Token Ring	FDDI
Бітова швидкість	10 (100) Мбіт/с	4, 16 Мбіт/с	100 Мбіт/с
Топологія	Загальна шина, зірка	Зірка, кільце	Подвійне кільце дерев
Метод доступу	CSMA / CD	Пріоритетна Система резервування	Доля від часу обороту маркера
Середовище передачі даних	Товстий коаксіал, тонкий коаксіал, вита пара, оптичне волокно	Екранована та неекранована вита пара, оптичне волокно	Оптичне волокно, неекранована вита пара 5 категорії
Максимальна довжина мережі (без мостів)	2500 м	4000 м	200 км (100 км на кільце)
Максимальна відстань між вузлами	2500 м	100 м	2 км (не більше 11 дБ втрат між вузлами)
Максимальна кількість вузлів	1024	260 – екранована витої пари 72 – неекранована вита пара	500 (1000 з'єднань)

Таким чином можна зробити такі висновки, що технології Token Ring та Ethernet є дешевшими для підключення клієнтських комп'ютерів та невеликих серверів. Token Ring забезпечує гарантовану затримку, а Ethernet не може забезпечити гарантованої затримки. Затримка в Ethernet зростає з ростом інтенсивності передачі. Довжина кадру Token Ring – 4500 байт, Ethernet – 1500 байт, тобто Token Ring ефективніше передає дані. Маркерний метод доступу Token Ring більш складний, ніж множинний доступ в Ethernet, тому мережеві адаптери Token Ring дорожчі за мережеві адаптери Ethernet, отже мережа Token Ring є дорожчою для встановлення. Token Ring в більшості випадків використовується в технологічних процесах, де важливим критерієм є не стільки швидкість, скільки надійність доставки інформації.

1.2.3 Основні принципи захисту інформації при підключенні до мережі Інтернет

Актуальність і важливість проблеми забезпечення інформаційної безпеки обумовлені наступними чинниками:

- сучасні рівні і темпи розвитку засобів інформаційної безпеки значно відстають від рівнів і темпів розвитку інформаційних технологій;
- високі темпи зростання парка персональних комп'ютерів, вживаних в різноманітних сферах людської діяльності. (Згідно даним досліджень компанії Gartner Dataquest в теперішній час у світі більше мільярда персональних комп'ютерів. А наступний мільярд буде досягнутий вже в 2009 році.);
- різке розширення кола користувачів, що мають безпосередній доступ до обчислювальних ресурсів і масивів даних [31, с. 95].

Під захистом інформації при підключенні до мережі інтернет розуміється можлива небезпека (потенційна або така, що реально існує) здійснення якого-небудь діяння (дії або бездіяльності), направленого проти об'єкту захисту (інформаційних ресурсів), що завдає збитку власникові або користувачеві. Реалізація тієї або іншої загрози безпеки може переслідувати наступні цілі:

- порушення конфіденційності інформації. Інформація, що зберігається і оброблюється в корпоративній мережі, може мати велику цінність для її власника, її використання іншими особами наносить значну шкоду інтересам власника;
- порушення цілісності інформації. Втрата цілісності інформації (повна або часткова компрометація, дезинформація) – загроза близька до її розкриття. Цінна інформація може бути втрачена або знецінена шляхом її несанкціонованого видалення або модифікації. Збиток від таких дій може бути багато більшим, ніж при порушенні конфіденційності;
- порушення (часткове або повне) працездатності корпоративної комунікаційної системи (порушення доступності). Вивід з ладу або некоректна зміна режимів роботи компонентів корпоративної комунікаційної системи (КМ), їх модифікація або підміна можуть привести до отримання невірних результатів, відмови КМ від потоку інформації або відмова при обслуговуванні. Тому забезпечення інформаційної безпеки комп'ютерних мереж є одним з ведучих напрямів розвитку інформаційних

технологій. Для підключення будь-якої організації до мережі Інтернет необхідно прийняти ряд певних організаційно-технічних заходів для її захисту.

При побудові захисту варто виходити з того, що будь-який захист ускладнює використання корпоративної комунікаційної системи, що за прямим призначенням обмежує функціональні можливості, споживає обчислювальні й трудові ресурси, вимагає фінансових витрат на створення та експлуатацію. Чим вище захист, тим дорожчою у побудові та обслуговуванні стає система і тим менш зручною для безпосередніх користувачів. Тому, захищаючи корпоративну мережу, варто виходити з доцільної вартості захисту. Тобто витрати на захист повинні бути пропорційні цінності ресурсу, що захищається [32, с. 613].

Firewall (Брандмауер). Основним загальновизнаним засобом такого захисту є міжмережний екран (Брандмауер). Міжмережний екран установлюється між мережею та Інтернет і виконує роль мережевого фільтра (Рисунок 1.1).

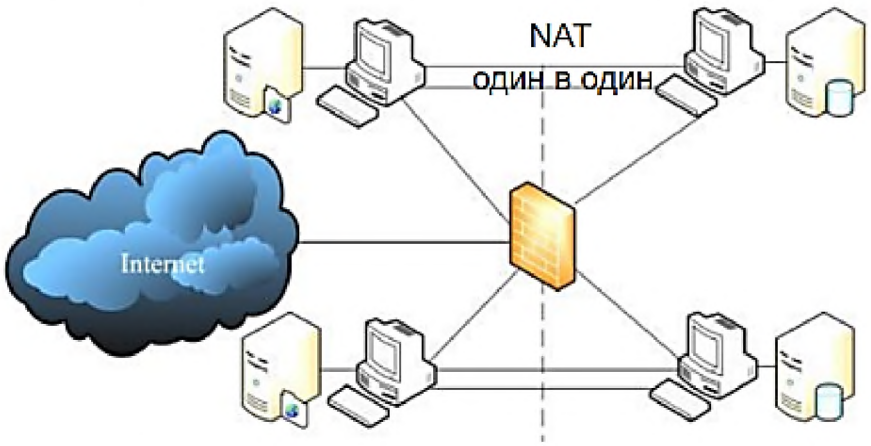


Рисунок 1.1 – Встановлення брандмауера у корпоративній мережі

Він налаштовується таким чином, щоб пропускати допустимий трафік від користувачів мережі до служб Інтернет і назад, і обмежити трафік з боку Інтернет до мережі, яка потребує захисту, тільки необхідними службами, наприклад: smtp, dns, ntp. Допустимість того або іншого трафіка визначається мережним адміністратором відповідно до політики інформаційної безпеки організації. Наприклад, може бути дозволений доступ із частини комп'ютерів мережі до web та ftp-серверів Інтернет і двонаправлений доступ між Інтернет та поштовим

сервером, але при цьому заборонені всі інші протоколи й напрями трафіка [45, с. 59].

Таким чином, міжмережний екран фізично розташовується на місці мережного шлюзу (маршрутизатора), логічним є сполучення їх функції в одному пристрої. Це дозволяє одним засобом захистити й локальну мережу і безпосередньо сам шлюз. Така опція передбачена для маршрутизаторів компанії Cisco Systems (Firewall Feature Set). Однак дане правило є необов'язковим і міжмережний екран може бути поданий окремим пристроєм.

У найпростішому випадку виконання функцій міжмережного екрана можна організувати за допомогою мережного фільтру на основі аркушів доступу (access-lists). Аркуші доступу визначають правила, за якими або дозволяється, або забороняється проходження трафіка з певними ознаками від одного мережного інтерфейсу маршрутизатора до іншого усередині самого маршрутизатора. Як ознаки можуть використовуватися IP-адреси або діапазон, IP-адреса джерела й приймача, тип протоколу, номер порту призначення або відправлення, ряд інших службових ознак IP-пакету.

Розглянемо комплексний підхід для забезпечення інформаційної безпеки корпоративної комунікаційної системи. До основних способів забезпечення інформаційної безпеки відносять: законодавчі (правові); морально-етичні; організаційні (адміністративні); технічні; програмні. Законодавчі заходи захисту визначаються законодавчими актами країни, якими регламентуються правила використання, обробки і передачі інформації обмеженого доступу і встановлюються заходи відповідальності за порушення цих правил.

Організаційні (адміністративні) засоби захисту – це організаційно-технічні і організаційно-правові заходи здійснювані, у процесі створення і експлуатації апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють всі структурні елементи апаратури на всіх етапах їх життєвого циклу (будівництво приміщень, проєктування системи, монтаж і наладка устаткування, випробування і експлуатація). Організаційні заходи передбачають [49, с. 670]:

- обмеження доступу в приміщення де відбувається обробка конфіденційної інформації;
- допуск до вирішення завдань на комп'ютері з обробки секретної, конфіденційної інформації перевірених посадових осіб, визначення порядку проведення робіт на комп'ютері;
- зберігання магнітних носіїв в ретельно захищених шафах;
- призначення одного або кількох комп'ютерів для обробки цінної інформації і подальша робота тільки на цих комп'ютерах;
- установка дисплея, клавіатури і принтера так, щоб виключити перегляд сторонніми особами змісту оброблюваної інформації;
- постійне спостереження за роботою принтера та інших пристроїв виводу на носії цінної інформації; знищення фарбувальних стрічок або інших матеріалів, що містять фрагменти цінної інформації;
- заборона ведення переговорів про безпосередній зміст конфіденційної інформації особами, зайнятими її обробкою.

Організаційно-технічні заходи захисту корпоративної комунікаційної системи припускають:

- обмеження доступу всередину корпуса комп'ютера шляхом встановлення механічних пристроїв замикання;
- знищення всієї інформації на вінчестері комп'ютера при відправці в ремонт з використанням засобів низькорівневого форматування;
- організацію живлення комп'ютера від окремого джерела живлення або від загальної (міської) електромережі через стабілізатор напруги (мережевий фільтр) або мотор-генератор;
- використання для відображення інформації рідкокристалічних або плазмових дисплеїв, а для друку – струменевих або лазерних принтерів;
- розміщення дисплея, системного блоку, клавіатури і принтера на відстані не менше 2,5–3,0 метрів від пристроїв освітлення, кондиціонування повітря, зв'язку (телефону), металевих труб телевізійної і радіоапаратури, а також

інших комп'ютерів, що не використовуються для обробки конфіденційної інформації;

- у час обробки цінної інформації на комп'ютері рекомендується виключати пристрої, що створюють додатковий шумовий фон (кондиціонери вентилятори), а також обробляти іншу інформацію на комп'ютерах, що стоять поряд. Ці пристрої повинні бути розташовані на відстані не менше 2,5–3,0 метрів [51, с. 253];
- знищення інформації безпосередньо після її використання.

Технічні засоби захисту корпоратвиної мережі реалізуються у вигляді механічних, електричних, електромеханічних і електронних пристроїв, призначених для перешкоди на можливих шляхах проникнення і доступу потенційного порушника до компонентів захисту. Програмні засоби представляють собою програмне забезпечення, що спеціально призначене для виконання функцій захисту інформації. Програмні засоби складають основу механізмів захисту на першій фазі розвитку технології забезпечення безпеки зв'язку в каналах телекомунікацій.

1.2.4 NAT-перетворення

На даному етапі захисту корпоративної комунікаційної системи існують такі підходи до захисту, як використання технології трансляції мережних адрес (Network Address Translation – NAT) для приховання від зовнішніх зловмисників діапазону IP-адрес організації та логічної структури мережі.

Протокол NAT використовується для передачі пакетів з IP-адрес, призначених тільки для внутрішнього використання, в зовнішні мережі і для вирішення задачі приховування внутрішньої логічної структури мережі від зовнішніх мереж. NAT транслює тільки той трафік, який проходить між внутрішньою і зовнішньою мережею і визначений для трансляції. Будь-який трафік, який не відповідає критеріям трансляції або той, який проходить між іншими інтерфейсами на маршрутизаторі, ніколи не транслюється і пересилається з використанням маршрутизації. Слід звернути увагу на те, що протокол NAT

виконує тільки трансляцію адрес і не виконує функції фільтрації. Для заборони проходження пакетів з зовнішніх мереж у внутрішню необхідно застосовувати відповідні списки доступу [44, с. 175].

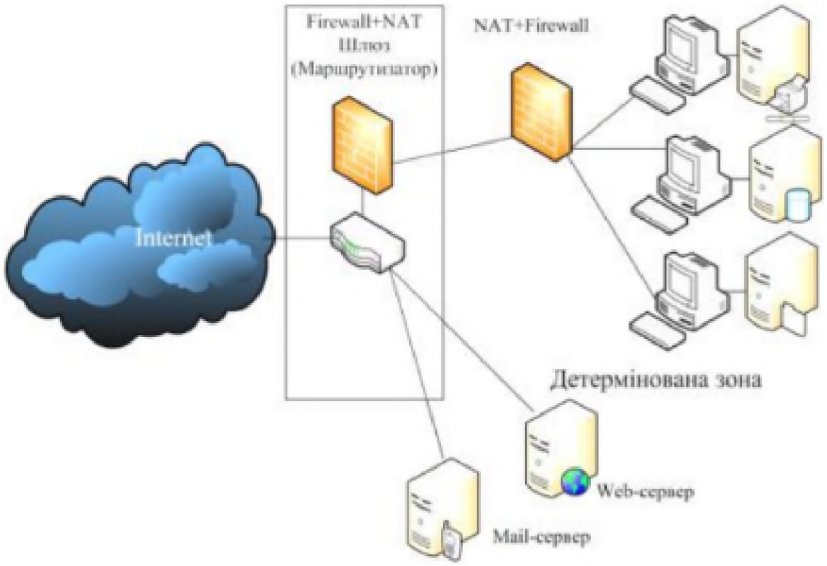


Рисунок 1.2 – Трансляція фіксованої внутрішньої адреси у фіксовану зовнішню мережу

В даний час існують наступні способи реалізації методики NAT:

- статичний NAT – відображення конкретної внутрішньої IP-адреси на конкретну зовнішню IP-адресу (можлива також заміна портів протоколів транспортного рівня при трансляції). Зазвичай статичний NAT використовують, коли до вузла внутрішньої мережі необхідно забезпечити доступ з зовнішніх мереж з використанням конкретних протоколів прикладного рівня;
- динамічний NAT – відображає адресу з блоку внутрішніх IP-адрес на одну з вільних адрес блоку зовнішніх адрес. Досить рідко використовується завдяки необхідності використання кількох зовнішніх IP-адрес та пов’язаній з цією ж особливістю низькою масштабованістю [48, с. 50];
- перевантаження (Overload) – форма динамічного NAT, який відображає адресу з блоку внутрішніх IP-адрес в єдину зовнішню IP-адресу, використовуючи різні порти (відома також як PAT-Port Address Translation). Дана методика є найбільш поширеною для організації виходу в Інтернет з внутрішніх вузлів корпоративної комунікаційної системи;

– списки контролю доступу (Access Control List – ACL) містять набір правил, де визначено дію над пакетами і параметри пакетів для фільтрації (адреси відправників та отримувачів, номера портів протоколів транспортного рівня тощо).

Перевірка пакетів проводиться точно в тому порядку, в якому задані правила в списку. Коли пакет потрапляє на інтерфейс, він перевіряється по першому правилу. Якщо параметри пакету відповідають першому правилу, то подальша перевірка припиняється, тоді пакет або буде передано далі або знищено. Якщо параметри пакету не відповідають першому правилу, то проводиться його аналіз на відповідність наступному правилу і так далі, поки не буде перевірено усі правила (якщо пакет не відповідав вимогам якогось з правил вище). Якщо параметри пакету не відповідають жодному з правил списку, то пакет просто знищується (в кінці кожного списку стоїть неявне правило, яке забороняє проходження усіх пакетів). ACL можуть бути застосовані до:

– фізичних або логічних інтерфейсів (в тому числі на інтерфейси VLAN-комутаторів 3-го рівня);
– термінальних ліній для обмеження доступу до пристрою по протоколам Telnet або SSH;
– VPN-тунелів (які пакети потрібно шифрувати);
– механізмів QoS (визначення пріоритетів для різних типів трафіку);
– шейперів для обмеження швидкості трафіку користувачів;
– протоколу NAT (визначають, які IP-адреси необхідно транслювати).

За допомогою списків доступу вирішується і задача захисту від нав'язування хибного маршруту. Така атака базується на властивості ICMP-протоколу «на льоту» змінювати маршрут просування пакетів (повідомлення «Перенаправлення маршруту» (Redirect) ICMP протоколу). В результаті зв'язок вузла з мережею буде розірваний.

Друга форма NAT – це трансляція групи внутрішніх адрес в одну зовнішню. При цьому всі внутрішні комп'ютери можуть працювати з Інтернетом одночасно, а маршрутизатор розрізняє, кому яка відповідь перетрансльовується за

службовими даними TCP-з'єднання. У зовнішній мережі створюється враження, що до неї звертається тільки один комп'ютер. Така заміна істотно ускладнює життя користувачу, який старається завдати шкоду корпоративній мережі, тому що повністю приховує внутрішні комп'ютери й перешкоджає «обчисленню» його адреси (рис. 1.3). Супротивник, навіть бачучи трафік, що виходить із внутрішньої мережі, не може визначити, від якого комп'ютера він виходить [46, с. 117].

Крім того, це виключає можливість ініціативного обігу ззовні до внутрішнього комп'ютера, тому що для маршрутизатора в цьому випадку відсутнє правило прив'язки зовнішньої адреси до внутрішньої. Зокрема виключається можливість сканування ззовні внутрішньої мережі.

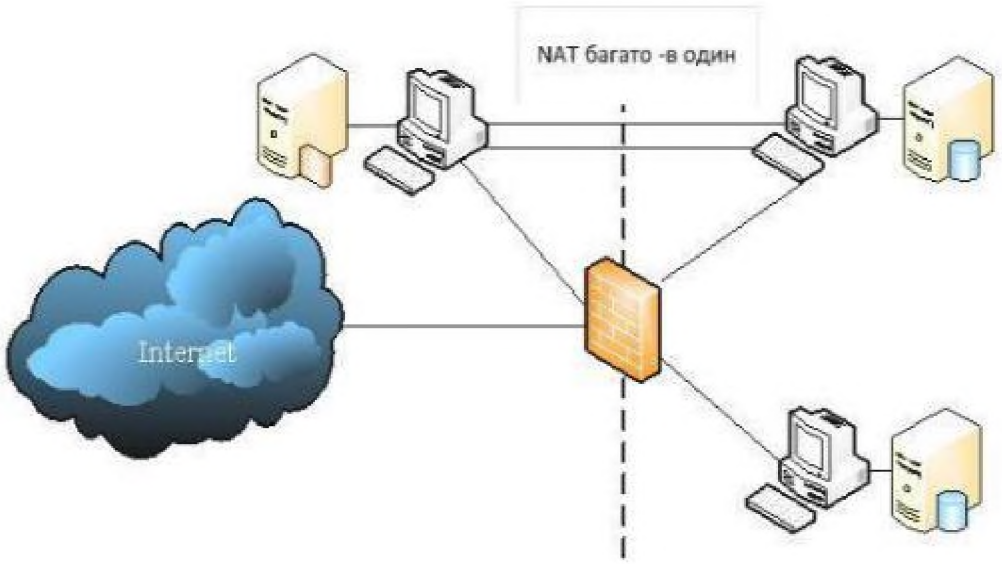


Рисунок 1.3 – Трансляція групи внутрішніх адрес в одну зовнішню

Третя форма NAT – використання для заміни внутрішніх адрес не однієї адреси, а будь-якої з виділених адрес. Тобто внутрішній комп'ютер, виходячи в Інтернет, одержує вільну у цей момент адресу з бази даних (БД). При цьому адреси підмінюються динамічно, і кожне нове TCP-з'єднання може бути встановлене з іншою IP-адресою. Це також створює додаткові труднощі супротивнику, тому що позбавляє його можливості атакувати будь-який внутрішній комп'ютер прицільно. Сказане відносно другої форми NAT є справедливим і для третьої форми. Якщо запит приходить ззовні, то маршрутизатор не в змозі зв'язати адресу з БД з адресою мережі. Тому такий запит не досягне мети [39, с. 48].

1.2.5 Демілітаризована зона

Як правило, організації потрібно мати у себе деякі мережні ресурси, до яких відкритий доступ з мережі Інтернет. Звичайно це поштовий, dns і web-сервери. Механізм їх роботи допускає, що до них повинен бути дозволений вільний або слабко обмежений доступ з Інтернету. Відповідно ймовірність їх зламу вища, ніж інших комп'ютерів мережі. Із цієї причини розміщати їх усередині зони, яка захищається, недоцільно з погляду безпеки, тому що у випадку зламу вони можуть стати воротами для атаки внутрішніх комп'ютерів [40, с. 245]. Для мінімізації ризику і збереження функціональності такі сервери встановлюють за основним шлюзом мережі, але перед міжмережним екраном, що забезпечує захист внутрішніх комп'ютерів. Логічну область їх розміщення називають демілітаризованою зоною (рис. 1.4).

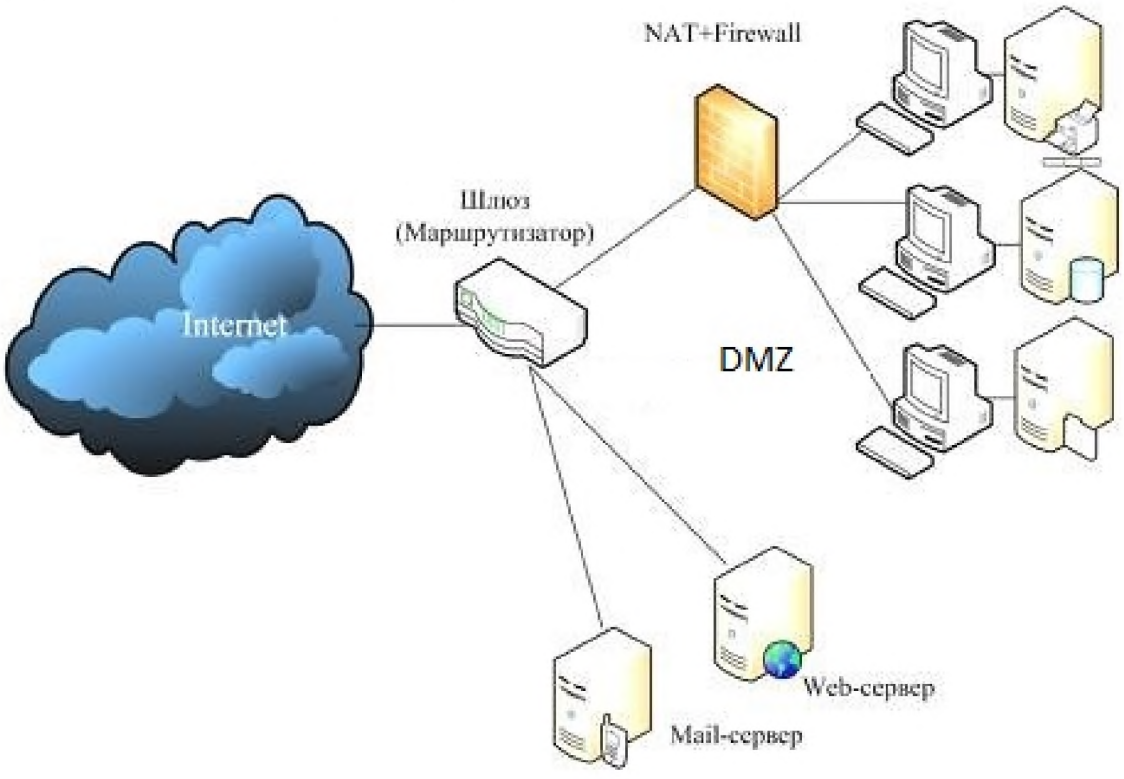


Рисунок 1.4 – Демілітаризована зона

З рис. 2.3 видно, що ніщо не заважає встановити другий Firewall на основному шлюзі корпоративної комунікаційної системи. Це є логічним рішенням і дозволяє одночасно підвищити рівень захисту внутрішньої мережі й захистити сервери демілітаризованої зони.

Наявність другого міжмережного екрана ускладнює конфігурування мережного устаткування й настроювання роботи всіх елементів мережі. Для додаткового підвищення захищеності можна використати Firewall-и різних виробників. Тоді якщо в одному з них буде виявлена вразливість, інший не дозволить користувачу, який старається завдати шкоду корпоративній мережі безперешкодно проникнути у мережу, як це мало б місце при використанні Firewall-ів одного типу [42, с. 43].

Особливо варто підкреслити, що можливість мережного доступу до шлюзів і до міжмережних екранів, щоб уникнути зловмисного використання, повинна бути відключена. З погляду безпеки пристрої, які знаходяться на сторожі мережі, повинні конфігуруватися й адмініструватися тільки через консольний порт локально (рис. 2.4).

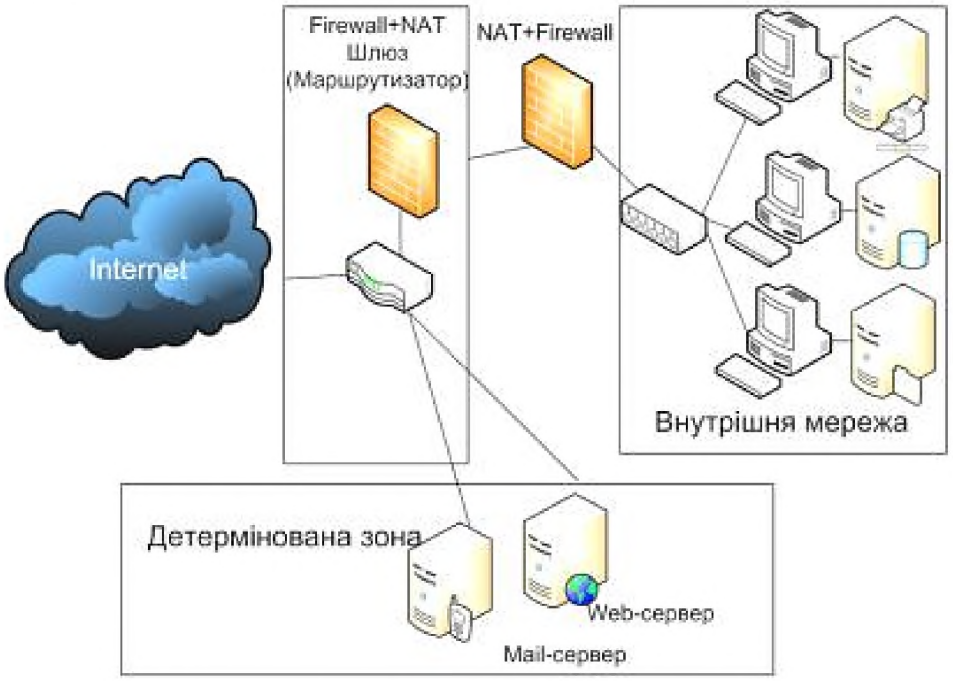


Рисунок 1.5 – Локально-консольний порт для серверів

Схема, запропонована на рис. 1.5, може бути дещо вдосконалена. Для цього необхідно використати граничний маршрутизатор із двома Ethernet-портами.

1.2.6 Антивірусний захист інформаційно-комунікаційної системи

На сьогодні відомі десятки тисяч різних комп'ютерних вірусів. Незважаючи на такий достаток, число типів вірусів, що відрізняються один від одного

механізмом поширення і принципом дії, досить обмежено. Існують і комбіновані 241 віруси, які можна віднести одночасно до декількох типів [43, с. 268].

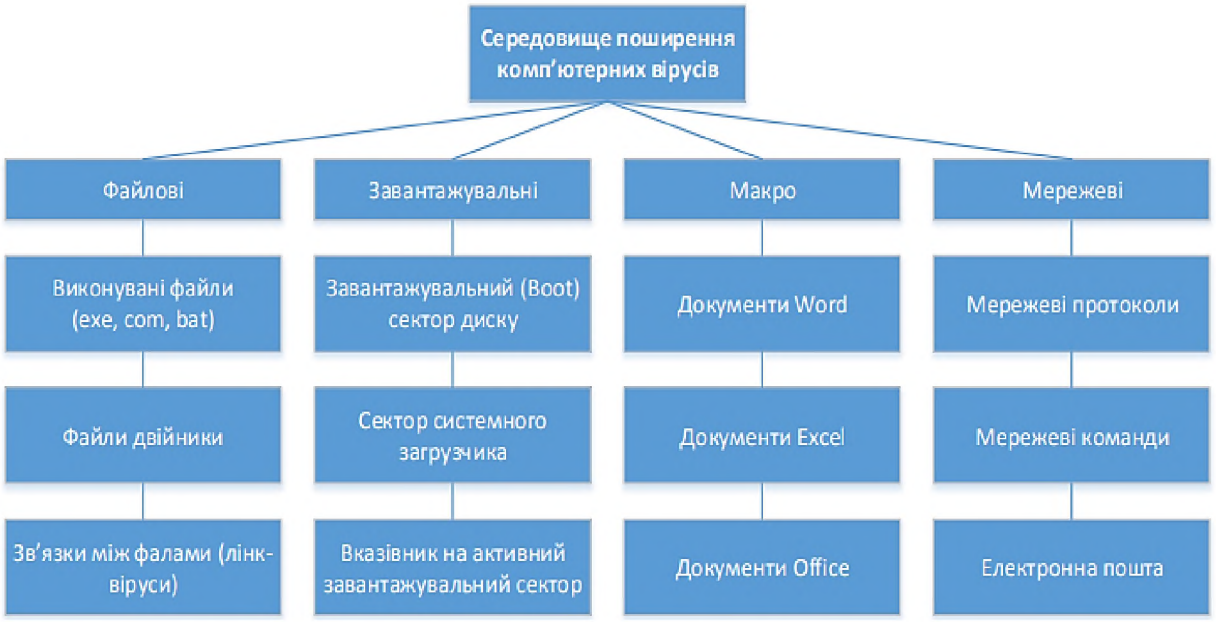


Рисунок 1.6 – Класифікація комп'ютерних вірусів за місцем існування

Мережеві віруси використовують для свого поширення протоколи або команди комп'ютерних мереж і електронної пошти. Іноді мережеві віруси називають програмами типу «черв'як». Мережеві черв'яки підрозділяються на Internet-черви (поширюються по Internet), LAN-черви (поширюються по локальній мережі), IRC-черви Internet Relay Chat (поширюються через чати). Існують також змішані типи, які поєднують в собі відразу кілька технологій.

Проблема антивірусного захисту – одна з пріоритетних проблем безпеки корпоративних інформаційних ресурсів організації. Її актуальність пояснюється:

- лавиноподібним зростанням числа комп'ютерних вірусів;
- незадовільним станом антивірусного захисту в існуючих корпоративних комп'ютерних мережах.

Сьогодні корпоративні мережі знаходяться в постійному розвитку. Проте разом з ним постійно росте і число точок проникнення вірусів в корпоративні мережі Інтернет. Поза всяким сумнівом, головною зброєю в боротьбі з вірусами завжди були антивірусні програми. Вони дозволяють не тільки виявляти віруси, що використовують різні методи маскування, але і видаляти їх з комп'ютера. Розрізняють наступні види антивірусних програм: вакцини; детектори; ревізори;

охоронці; монітори; поліфаги; евристичні аналізатори. Останнім часом, розробники антивірусних програм, пропонують користувачам комплексні рішення антивірусного захисту [38, с. 28].

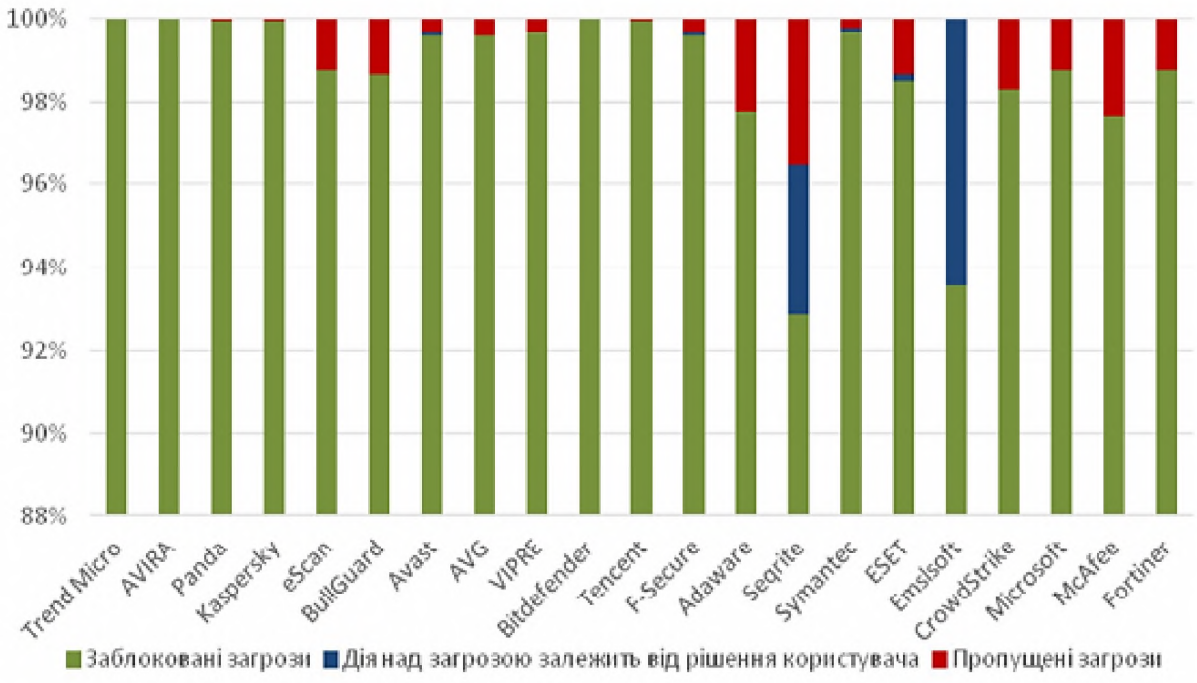


Рисунок 1.7 – Тест антивірусних засобів на захист від шкідливих програм

Як правило, такими точками є: шлюзи і сервери Інтернет, сервери файлових додатків, сервери групової роботи і електронної пошти, робочі станції. Для невеликих підприємств, що використовують до 10 вузлів, доцільні рішення по антивірусному захисту, що мають зручний графічний інтерфейс і допускають локальну конфігурацію без застосування централізованого управління. Для великих підприємств прийнятнішою є система антивірусного захисту з декількома консолями і менеджерами управління, що відносяться до єдиного загального центру. Такі рішення дозволяють забезпечити оперативне централізоване управління локальними антивірусними клієнтами і дають можливість при необхідності інтегруватися з іншими рішеннями в області безпеки корпоративних інформаційно-комунікаційних систем [35, с. 117].

Таким чином, на даний момент більшість рішень в області комп'ютерної безпеки корпоративної комунікаційної системи реалізуються, як комплекс декількох технологій. У класичних антивірусах сигнатурні детектування зазвичай використовується в парі з тією чи іншою реалізацією моніторингу системних

подій, емулятора. Перш за все, слід пам'ятати, що не існує ні універсального, ні найкращого рішення. У кожної технології є свої плюси і мінуси. Наприклад, моніторинг подій в системі постійно займає процесорний час, але його найважче обманути; процесу емуляції можна перешкодити використанням в коді певних команд, але при її використанні виявлення шкідливого коду виконується в попереджуючому режимі, система залишається захищеною.

Вибір технології – це вибір золотої середини з урахуванням конкретних потреб і обставин. Існує безліч методик виявлення невідомого шкідливого програмного засобу. Кожна з них має свої переваги, недоліки та особливості використання. Але на даний момент не існує методики, яка б повністю вирішувала завдання виявлення невідомого шкідливого програмного засобу з прийнятною ефективністю для будь-яких видів шкідливих програмних засобів і за будь-яких вимог до системи виявлення шкідливих програмних засобів. Теоретично об'єднання кількох методик може вирішити цю проблему.

1.2.7 Захист інформації за допомогою міжмережних екранів

Серед програмно-апаратних і програмних засобів забезпечення захисту інформації в корпоративній мережі можна виділити міжмережеві екрани (МЕ), засоби аналізу захищеності й засоби виявлення атак [34, с. 358].

Міжмережевий екран (МЕ) – це спеціалізований комплекс міжмережевого захисту, що називається також брандмауером або системою firewall. МЕ дозволяє розділити загальну мережу на дві частини (чи більше) і реалізувати набір правил, що визначають умови проходження пакетів з даними через кордон з однієї частини загальної мережі в іншу. Як правило, ця межа проводиться між корпоративною (локальною) мережею підприємства і глобальною мережею Internet. Зазвичай МЕ захищають внутрішню мережу підприємства від «вторгнень» з глобальної мережі Internet, хоча вони можуть використовуватися і для захисту від «нападів» з корпоративної інтрамережі, до якої підключена локальна мережа підприємства. Технологія МЕ одна з найперших технологій

захисту корпоративних інформаційно-комунікаційних систем від зовнішніх загроз.

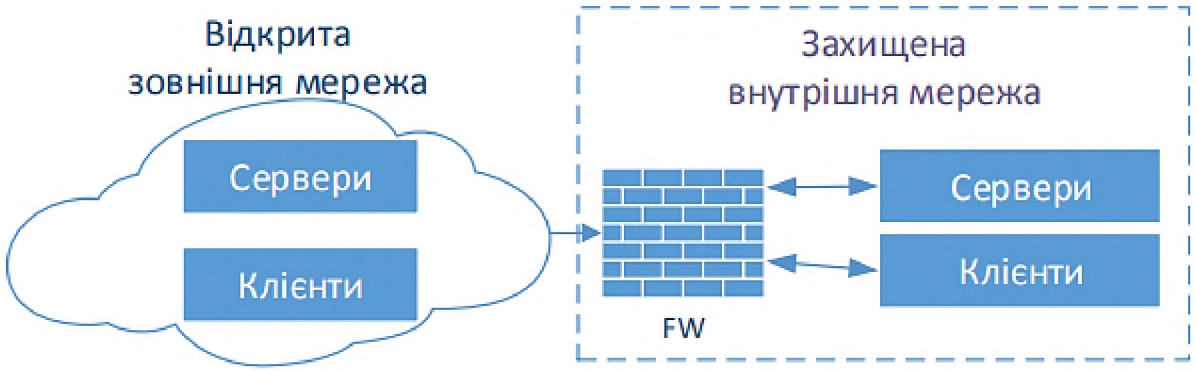


Рисунок 1.8 – Схема підключення міжмережевого екрану

Міжмережеві екрани (брандмауери, firewall) реалізують набір правил, які визначають умови проходження пакетів даних з однієї частини розподіленої КМ (відкритої) в іншу (захищену). Залежно від рівня взаємодії об'єктів мережі основними різновидами ММЕ є фільтруючі маршрутизатори, шлюзи сеансового й прикладного рівнів. Основною функцією фільтруючих маршрутизаторів, що працюють на мережному рівні еталонної моделі, є фільтрація пакетів даних, що входять у захищену частину мережі або вихідних з неї. Правила фільтрації визначають, дозволяється або блокується проходження через ММЕ пакета із правилами, що задаються цими параметрами.

Рисунок 1.9 – Структура міжмережевого екрану

До основних переваг фільтруючих маршрутизаторів відносяться простота їх створення, установка й конфігурування; прозорість для додатків користувачів КМ і мінімальний вплив на їх продуктивність; невисока вартість.

Недоліками фільтруючих маршрутизаторів є [26, с. 180]:

- відсутність автентифікації на рівні користувачів КМ; уразливість для підміни IP-адреси в заголовку пакета;
- незахищеність від погроз порушення конфіденційності й цілісності переданої інформації;
- сильна залежність ефективності набору правил фільтрації від рівня знань адміністратора ММЕ конкретних протоколів;
- відкритість IP-адрес комп'ютерів захищеної частини мережі.

Шлюзи сеансового рівня призначені для контролю віртуального з'єднання між робочою станцією захищеної частини мережі й хостом її незахищеної частини і трансляції IP-адрес комп'ютерів захищеної частини корпоративної комунікаційної системи.

У процесі виконуваного шлюзом сеансового рівня процедури трансляції IP-адрес відбувається їхнє перетворення в одну IP-адресу, асоційовану із ММЕ. Це виключає пряму взаємодію між хостами захищеної й відкритої мереж і не дозволяє порушнику здійснювати атаку шляхом підміни IP-адрес.

До переваг шлюзів сеансового рівня відносяться їх простота й надійність програмної реалізації. Недоліком є відсутність можливості перевіряти вміст переданої інформації. Це дозволяє порушнику намагатися передати пакети зі шкідливим програмним кодом і звернутися потім прямо до одного із серверів, що атакується КМ [28, с. 75].

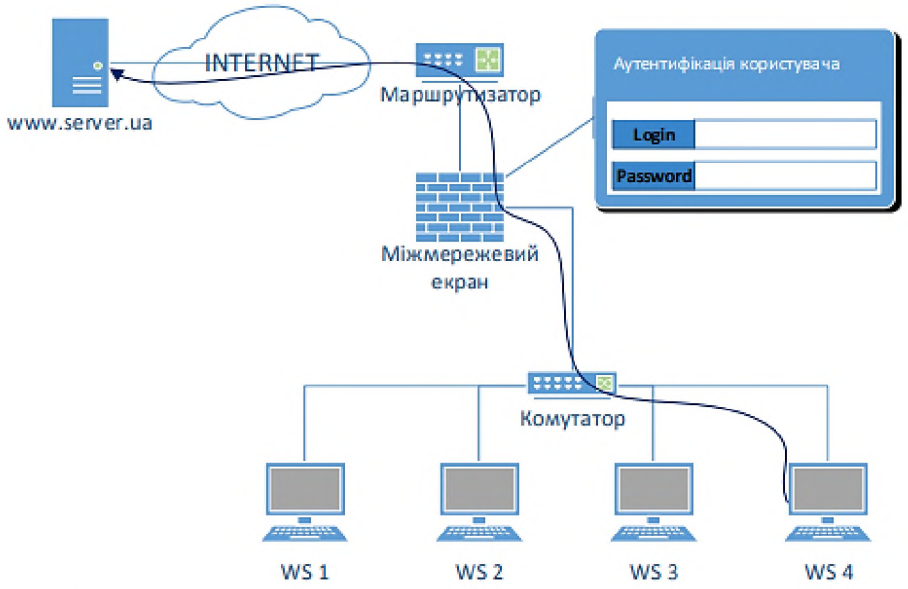


Рисунок 1.10 – Схема аутентифікації користувача по паролю

Шлюзи прикладного рівня не тільки виключають пряму взаємодію між уповноваженим користувачем із захищеної частини мережі й хостом з її відкритої частини, але й фільтрують усі вхідні й вихідні пакети даних на прикладному рівні (на основі аналізу змісту переданих даних).

Основні функції шлюзів прикладного рівня такі:

– ідентифікація й автентифікація користувача КМ при спробі встановити з'єднання;
– перевірка цілісності переданих даних; розмежування доступу до ресурсів захищеної й відкритої частин корпоративної комунікаційної системи, фільтрація і перетворення переданих повідомлень (виявлення шкідливого програмного коду, шифрування й розшифрування);
– реєстрація подій у спеціальному журналі; кешування запитуваних ззовні даних, розміщених на комп'ютерах внутрішньої мережі (для підвищення продуктивності КМ).
– Перевагами шлюзів прикладного рівня також є:
– прихованість структури захищеної частини мережі для інших хостів [29, с. 67];
– надійна автентифікація й реєстрація минаючих повідомлень;

- більш прості правила фільтрації пакетів на мережному рівні, відповідно до яких маршрутизатор повинен пропускати тільки трафік, призначений для шлюзу прикладного рівня, і блокувати весь інший трафік;
- можливість реалізації додаткових перевірок.

Основними недоліками шлюзів прикладного рівня є більш висока вартість, складність розробки, установки й конфігурування, зниження продуктивності КМ, «непрозорість» для додатків користувачів КМ.

Міжмережеві екрани є основою для створення віртуальних приватних мереж (Virtual Private Network, VPN), які призначені для приховання топології внутрішніх мереж організацій, що обмінюються інформацією з мережею Інтернет, і захисту трафіка між ними. При цьому використовуються спеціальні системи маршрутизації.

Загальним недоліком ММЕ будь-якого виду є те, що ці програмно-апаратні засоби захисту в принципі не можуть запобігти багатьох видів атак, наприклад, погрози несанкціонованого доступу до інформації з використанням неправильного сервера служби доменних імен мережі Інтернет, погрози аналізу мережного трафіка, погрози відмови в обслуговуванні. Порушнику реалізувати погрозу доступності інформації в КМ, що використовує ММЕ, може виявитися навіть простіше, тому що досить атакувати тільки хост із ММЕ для фактичного відключення від зовнішньої мережі всіх комп'ютерів захищеної частини мережі [21, с. 44].

1.2.8 Можливості адресного перетворення (PAT)

Порт адресного перетворення (PAT), також відомий як NAT overload або маскування адрес, є одним з методів мережевого трансляції мережних адрес. PAT є розширенням технології мережевої адресації (NAT), яка дозволяє приватним мережам з внутрішніми IP-адресами отримувати доступ до Інтернету через одну або кілька публічних IP-адрес.

PAT використовується для маскування внутрішніх IP-адрес з приватних мереж (наприклад, з діапазону IP-адрес 10.0.0.0 / 8, 172.16.0.0 / 12 або 192.168.0.0 /

16) і надання доступу до Інтернету для всіх пристроїв в цих мережах через одну або кілька публічних IP-адрес. Це досягається шляхом переписування інформації про порт та IP-адресу пакетів, що проходять через мережевий пристрій, який виконує PAT.

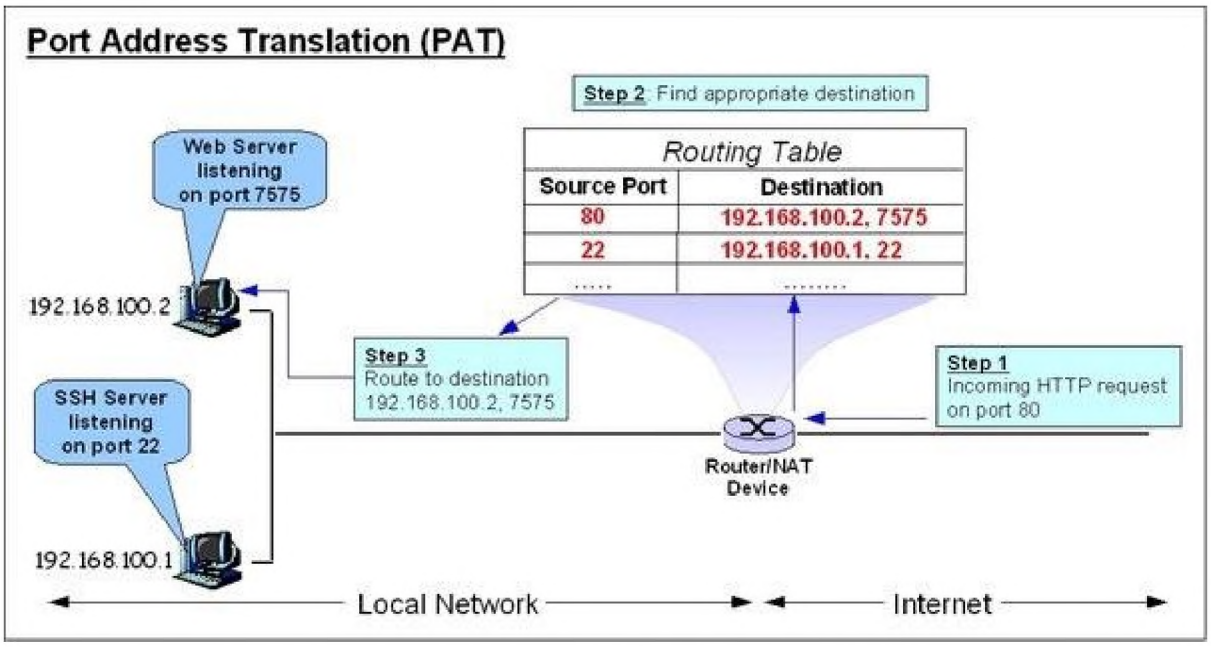


Рисунок 1.11 – Функціональність PAT

Основні переваги використання PAT включають:

1 Економія публічних IP-адрес: Завдяки PAT можна використовувати одну або кілька публічних IP-адрес для доступу до Інтернету для багатьох пристроїв в приватній мережі. Це економить кількість доступних публічних IP-адрес і дозволяє більш ефективно використовувати їх.

2 Захист приватної мережі: При використанні PAT внутрішні IP-адреси пристроїв в приватній мережі не відкриті для прямого доступу з Інтернету. Зовнішні пристрої бачать лише публічну IP-адресу маршрутизатора або мережевого пристрою, що виконує PAT. Це забезпечує певний рівень безпеки для внутрішніх пристроїв, ховаючи їхні IP-адреси від зовнішніх загроз.

3 Доступ до Інтернету для багатьох пристроїв: PAT дозволяє багатьом пристроям в приватній мережі одночасно використовувати Інтернет через одну або кілька публічних IP-адрес. Він використовує унікальні порти для ідентифікації пристроїв, що забезпечує правильну доставку пакетів з Інтернету до відповідних пристроїв в приватній мережі.

Використання PAT може бути особливо корисним для невеликих офісів або домашніх мереж, де кількість публічних IP-адрес обмежена або дорога. Він дозволяє об'єднувати декілька пристроїв в одну публічну IP-адресу, забезпечуючи їм доступ до Інтернету [21].

Keenetic – це серія мережевих пристроїв, що використовуються для створення локальних корпоративних інформаційно-комунікаційних систем та надання доступу до Інтернету. Деякі моделі пристроїв Keenetic підтримують функцію порт адресного перетворення (PAT) для ефективного маскування адрес у внутрішніх мережах.

За допомогою функції PAT на обладнанні Keenetic можна налаштувати перетворення IP-адрес та портів, що дозволяє використовувати одну або кілька публічних IP-адрес для доступу до Інтернету для всіх пристроїв у приватній мережі. Основна ідея полягає в тому, що пристрої з приватними IP-адресами в мережі Keenetic використовують одну публічну IP-адресу під час взаємодії з Інтернетом.

Існує кілька кроків для налаштування PAT на пристроях Keenetic:

1 Встановлення публічної IP-адреси: Почніть з призначення публічної IP-адреси, яку ви будете використовувати для доступу до Інтернету. Цю інформацію вам надасть ваш Інтернет-провайдер.

2 Встановлення внутрішньої мережі: Налаштуйте внутрішню мережу на пристрої Keenetic, використовуючи приватні IP-адреси. Ви можете налаштувати статичну IP-адресу для кожного підключеного пристрою або використовувати DHCP для автоматичного призначення IP-адрес.

3 Налаштування правил порт переадресації: Встановіть правила переадресації портів (port forwarding), які пересилають вхідний трафік з публічної IP-адреси до конкретного пристрою або служби у внутрішній мережі. Це дозволить зовнішнім пристроям отримувати доступ до внутрішніх ресурсів.

4 Активація PAT: Включіть функцію порт адресного перетворення (PAT) на пристрої Keenetic та налаштуйте правила перетворення IP-адрес та портів. Це

забезпечить правильну маршрутизацію пакетів і забезпечить доступ до Інтернету для всіх підключених пристроїв.

Точність процесу налаштування PAT на пристроях Keenetic може змінюватися в залежності від моделі та версії програмного забезпечення пристрою. Рекомендується використовувати документацію та ресурси, надані виробником, для отримання детальнішої інформації про налаштування PAT на конкретній моделі Keenetic [21].

1.2.9 Засоби функціоналу ACL

Функція Access Control List (ACL) (Список керування доступом) є важливим елементом налаштування безпеки в локальних корпоративних інформаційно-комунікаційних системах. ACL використовується для контролю доступу до ресурсів мережі, таких як пристрої, служби або сегменти мережі, шляхом встановлення правил для фільтрації трафіку.

ACL може бути налаштований на різних мережевих пристроях, включаючи комутатори, маршрутизатори або файєрволи. Він працює на рівні мережевого рівня (рівень 3 моделі OSI) та здатен контролювати трафік на основі різних параметрів, таких як IP-адреси джерела та призначення, номери портів, протоколи і т. д [21].

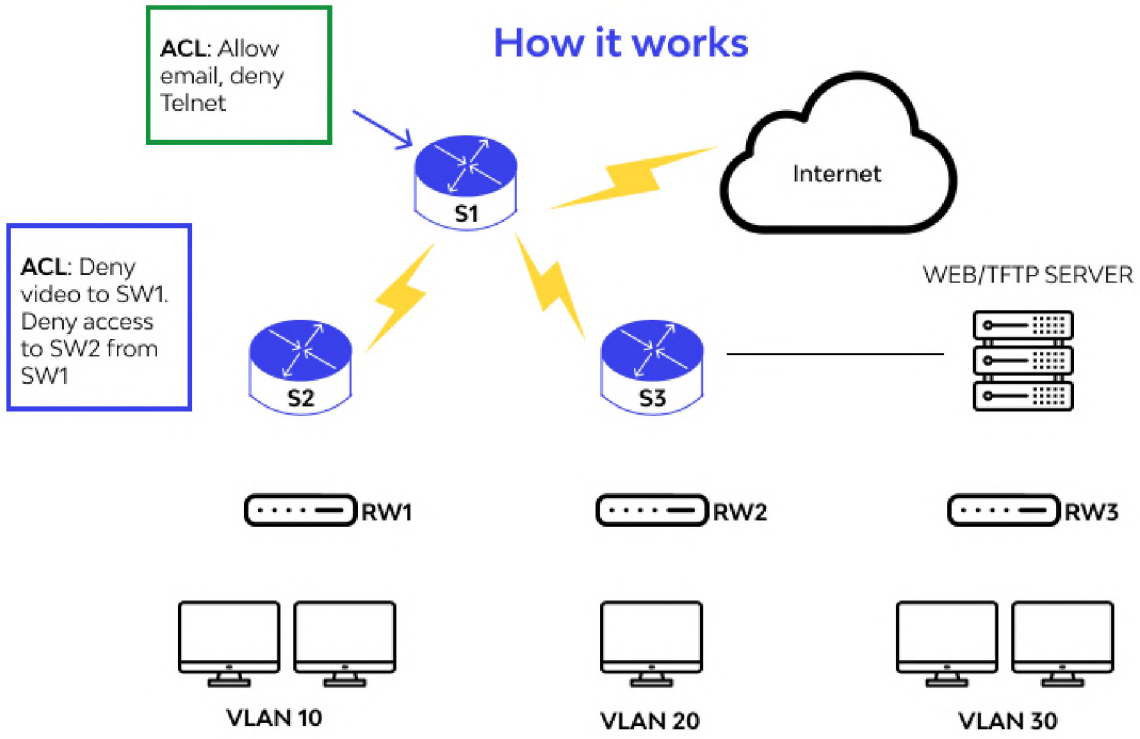


Рисунок 1.12 – Функціонал ACL

Основні аспекти функції ACL включають:

1. Фільтрація трафіку: ACL дозволяє встановлювати правила, які визначають, який тип трафіку може проходити через мережевий пристрій, а який повинен бути відхилений. Наприклад, ви можете налаштувати ACL, щоб дозволити лише певні IP-адреси або діапазони IP-адресів отримувати доступ до певних ресурсів мережі, а забороняти решту.

2 Керування безпекою: ACL використовується для забезпечення безпеки мережі шляхом контролю доступу до різних ресурсів. Ви можете налаштувати ACL для блокування небажаних або потенційно шкідливих підключень до мережі, запобігаючи атакам, шпигунству або несанкціонованому доступу.

3 Керування політикою: ACL дозволяє встановлювати політику доступу до мережі відповідно до вимог організації. Ви можете налаштувати ACL, щоб обмежити доступ до конкретних ресурсів або служб, встановити рівні пріоритету для різних типів трафіку або виконувати інші політики безпеки.

4 Маршрутизація: ACL може використовуватися для керування маршрутизацією трафіку в мережі. Ви можете налаштувати ACL, щоб вказати, які

маршрути повинні бути використані для певних типів трафіку або які маршрути повинні бути виключені.

5 Контроль бандвітду: ACL може бути використаний для керування пропускною здатністю мережі шляхом обмеження або пріоритезації певних типів трафіку. Наприклад, ви можете налаштувати ACL для обмеження шириною смуги для певних пристроїв або додатків, щоб забезпечити рівномірний розподіл ресурсів мережі.

Настройка ACL може варіюватися в залежності від типу обладнання та виробника. Рекомендується детально ознайомитися з документацією вашого пристрою Keenetic або звернутися до підтримки виробника для отримання конкретної інформації про налаштування ACL на вашому пристрої.

ACL є потужним інструментом для керування доступом та забезпечення безпеки в корпоративних інформаційно-комунікаційних системах. Правильне використання ACL допомагає контролювати трафік та забезпечувати безпеку вашої мережі.

1.2.10 Віртуальні мережі передачі даних

У 2012 році з'явилася технологія віртуалізації мережі (Network Virtualization, NV), що забезпечує можливість віртуалізації на принципово новому рівні – рівні мережевого сегменту. У випадку серверної віртуалізації з невеликими застереженнями операційна система (ОС) всередині віртуальних машин (ВМ) працює так, ніби була встановлена на фізичний сервер і була єдиною ОС на цьому обладнанні. За аналогією віртуалізація мережі призводить до того, що віртуальна, а точніше в даному контексті віртуалізована мережа, функціонує так, ніби вона була фізичною мережею [2, с. 205]. Даний рівень віртуалізації дозволяє створювати і використовувати кілька віртуальних мереж, можливо з перекриваємими або навіть повністю схожими просторами IP-адресів, на одній фізичній мережевій інфраструктурі. Ця мережева інфраструктура, може

включати в себе довільну кількість фізичних серверів і мережевого обладнання. Схематичне зображення віртуальної мережі передачі даних наведено в додатку Б.

Штатні засоби платформи VMware vSphere не надають переваг масштабованості, гнучкості налаштування мережі і не реалізують функції, що необхідні для безпечної роботи мережі. Внаслідок чого необхідно використовувати додаткові сторонні засоби для створення нової системи роботи мережі. Віртуальна локальна мережа (VLAN) являє собою логічний домен циркулярної розсилки, який може охоплювати безліч фізичних локальних мережевих сегментів. За кожним портом комутатора може бути закріплена конкретна VLAN, яка може бути логічно сегментована відповідно до її функцій і завдань. Порти однієї VLAN мають спільний домен циркулярної розсилки. Порти, що відносяться до різних VLAN, не можуть здійснювати циркулярну розсилку.

Можна підвищити рівень безпеки шляхом сегментування мережі на окремі домени циркулярної розсилки. Крім того, можна регулювати розмір і структуру домену шляхом регулювання розміру і структури VLAN. Віртуальна корпоративна комунікаційна система з віддаленим доступом наведена в додатку В.

VLAN дозволяють групувати порти комутатора таким чином, щоб трафік обмежувався тільки членами тієї чи іншої групи. Ця функція обмежує циркулярну, одноадресну і багатоадресну розсилку (лавинна адресація) тільки портами, що включені в конкретну VLAN. VLAN дозволяє ефективно розділяти трафік, забезпечуючи більш високу пропускну здатність. Можливі такі типи VLAN:

- VLAN на базі порту, який не має стандарту;
- на базі тільки одного комутатора;
- VLAN на базі MAC, який не має стандарту;
- VLAN на базі ознаки (tag-based), IEEE 802.1 q;
- Може бути між кількома комутаторами.

Внутрішньокорпоративні мережі VPN будуються з використанням Internet або мережевих інфраструктур, що розділяються між сервіс-провайдерами, які надають послугу. З'єднання вузлів мережі за допомогою технології Intranet VPN наведено в додатку Г. Основними перевагами Intranet VPN є:

- застосування потужних криптографічних протоколів шифрування даних для захисту конфіденційної інформації;
- надійність функціонування при виконанні таких критичних застосувань, як системи автоматизованого продажу і системи управління базами даних;
- гнучкість управління ефективним розміщенням швидко зростаючої кількості нових користувачів, нових офісів і нових програмних застосувань.
- Побудова Intranet VPN є найрентабельнішим способом реалізації VPN-технології. Проте в Internet рівні сервісу взагалі не гарантуються. Компанії, яким потрібно гарантовані рівні сервісу, повинні розглянути можливість розгортання своїх VPN з використанням мережевих інфраструктур, що розділяються між сервіс-провайдерами, які надають послугу [3, с. 16].
- Міжкорпоративна комунікаційна система VPN – це мережева технологія, яка забезпечує прямий доступ з мережі однієї компанії до мережі іншої компанії і, таким чином, сприяє підвищенню надійності зв'язку, підтримуваного в ході ділової співпраці. Міжкорпоративна комунікаційна система Extranet VPN наведена в додатку Д. Мережі Extranet VPN (ME) в цілому схожі на внутрішньокорпоративні віртуальні приватні мережі з тією різницею, що проблема захисту інформації є для них гострішою. VLAN на базі порту дозволяє створювати VLAN з різних портів одного моста. VLAN на базі MAC дозволяє об'єднувати в сегмент MAC адресу хост-машин, а VLAN на базі ознаки дозволяє створювати VLAN за якою-небудь ознакою. Ознака записується після MAC адреси джерела в кадрі Ethernet, що дозволяє ідентифікувати VLAN. На сьогодні рішення по віртуалізації мережі надають великі корпорації, а саме: VMware NSX – це платформа віртуалізації мережі для програмного ЦОД; Amazon Elastic Compute Cloud – Amazon EC2) – це веб-сервіс, що надає масштабовані обчислювальні ресурси в хмарі; Cisco

Application Centric Infrastructure – ACI) – інфраструктура, що орієнтована на додатки.

OpenFlow – протокол управління процесом обробки даних, що передаються по мережі маршрутизаторами і комутаторами, що реалізує технологію SDN. Протокол використовується для управління мережевими комутаторами і маршрутизаторами з центрального пристрою-контролера мережі. Як елемент управління роботою мережі може бути використана віртуальна машина з встановленим на ній OpenFlow-контролером floodlight. Задля передачі даних між користувачами в кожному ESXi-хості встановлюють OpenvSwitch (реалізація OpenFlow switch). Ізоляція інформації між ESXi-хостами може бути реалізована за рахунок створення GRE-тунелів. Правила роботи OpenFlow switch описані в таблицях потоків, які містяться в його пам'яті. Таблиця потоків складається із записів, в кожній з яких містяться поля порівняння, лічильники та інструкції. Коли пакет надходить в OpenFlow switch поля порівнянь записів таблиці потоків, то порівнюються з заголовком пакета в порядку пріоритету (одне з полів порівняння). Якщо знайдено схожий запис, то до пакету застосовуються інструкції, які асоційовані з цим записом, і при цьому, збільшується значення лічильника.

Таким чином, завдання зводиться до передачі таблиць потоків в відповідний Open vSwitch. Щоб визначити, який зміст таблиць повинен бути на кожному Open vSwitch-е, і яку необхідно зібрати інформацію про систему, (її MAC адресу, Vlan, на якому ESXi-хості і в якій зоні безпеки вона знаходитися). Для цього розроблений модуль збору інформації з vCenter з використанням засобів віддаленої командного рядка vSphere CommandLine Interface (програма на C++) [13, с. 185].

Xen – загальнодоступний гіпервізор, запропонований для роботи на товарних платформах апаратних засобів, які використовують метод паравіртуалізації. Xen дозволяє одночасно керувати багатофункціональними VMs на єдиній фізичній машині. Схематичне зображення архітектури Xen наведено в додатку Ж. Архітектура Xen складається з одного гіпервізора, розташованого

вище фізичних апаратних засобів і кількох VMs по гіпервізору. У кожного VM може бути свій власний ОС і додатки. Гіпервізор керує доступом до апаратних засобів, а також наявними ресурсами, розділеними між VMs. Крім того, драйвери пристроїв збережені в ізольованому VM, названому Доменом 0 (dom0) для забезпечення надійної і ефективної апаратної підтримки. Оскільки dom0 має повний доступ до апаратних засобів фізичної машини, то у нього існують також спеціальні привілеї в порівнянні з іншими VMs, так званими користувацькими доменами (domUs).

Vmware – компанія, яка надає машинні платформи віртуалізації клієнтам центру обробки даних і кінцевого користувача. Платформи віртуалізації VMware засновані на понятті повної віртуалізації. Воно оцінює рівень платформи віртуалізації центру обробки даних VMware під назвою vmware сервер ESX. Ізоляція VM і частота представлення ресурсу на основі політики розподілу ресурсів встановлюється системним адміністратором. Схематичне зображення архітектури Vmware наведено в додатку З.

Архітектура Vmware складається з компонентів інтерфейсу апаратних засобів, монітора віртуальної машини (VMM), VMkernel, менеджера ресурсів і сервісного управління. Компоненти інтерфейсу апаратних засобів відповідальні за здійснення визначених для апаратних засобів функцій і створюють надану VMs абстракцію апаратних засобів. Це робить незалежні апаратні засоби VM як VMM відповідальними за центральний процесор віртуалізації, надаючи vCPU кожному VM. VMkernel керує і стежить за основними апаратними засобами. VMM і VMkernel разом здійснюють шар віртуалізації. Управління ресурсами здійснюється VMkernel. Він ділить основні фізичні ресурси між VM, перерозподіляючи ресурси для кожного VM.

OpenVZ – загальнодоступний інструмент віртуалізації рівня ОС. Кожне ізольоване навколишнє середовище називають Virtual Private Server (VPS). VPS схожий на фізичний сервер, маючи власні процеси, файли, адреси Internet Protocol (IP), системну конфігурацію і забезпечуючи повний доступ до кореня [11, с. 52]. Головне місце використання цієї технології віртуалізації є веб-хостинг, де

надається кожному клієнту повне навколишнє середовище Linux, а так само вона використовується в освітніх інформаційних технологіях (IT). OpenVZ менш гнучкий, ніж інші інструменти віртуалізації, такі як VMware або Xen, тому що середовище для OpenVZ має бути Linux дистрибутивом, на основі того ж самого ядра ОС фізичного сервера. Схематичне зображення архітектури OpenVZ наведено в додатку Є.

Архітектура OpenVZ складається з зміненого ядра Linux, яке знаходиться вище апаратних засобів. OpenVZ – змінене ядро, що здійснює віртуалізацію та ізоляцію кількох підсистем, управління ресурсом і контрольно-пропускними пунктами. Крім того, механізми віртуалізації вводу / виводу забезпечені OpenVZ-зміненим ядром, у якого є драйвер пристрою для кожного пристрою введення / виводу. Це змінене ядро також здійснює дворівневий планувальник процесу, який відповідальний за перший рівень, визначаючи який VPS буде здійснюватися, і хто буде керувати процесами VPS.

1.3 Висновки

Отже, з цього розділу можна дізнатися, що інформаційно-комунікаційні системи це комплекс, який має такі переваги як швидкодія, оптимізація управління та виконання певних процессів, маштабність, гетерогенність, інтегрованість, надійність,гнучкість, широкий спектр охоплення та розв'язування технічних проблем, а також має такі способи підключення як бездротові мережі, Internet, VPN, орендовані канали передачі, у кожного з якого є свої переваги та недоліки. При проєктуванні системи можна виділити наступні єтапи: аналіз вимог, при якому виділяється спосіб підключення, який найбільше їм відповідає; структурний синтез майбутньої системи; моделювання для оцінки характеристик функціонування та її оптимізація; установка; тестування; єксплуатація.

Наразі все більш стають популярні багаторівневі системи через такі переваги як маштабованість, конфігурованість, високий рівень безпеки та невисокі вимоги до продуктивності, але такі системи також мають такі недоліки як труднощі під час розробки через складності при узгодженні різних модулей та

ризику обвалити всю систему при нагалодженні одного з них, високим вимогам до ефективності роботи, а також у труднощах адміністрування

Також в цьому розділі розглядаються такі технології, які використовуються в інформаційно-комунікаційних системах як Enternet, Token Ring та FDDI. Перша з них є найбільш проста та дешева, але має недоліки у вигяді ситуацій, коли кадри, що передаються різними станціями, зіштовхуються одне з одним в загальному середовищі, що знижують ефективність розділеного середовища. Інші більш складні, та у своєму початку мали перевагу над Enternet, бо не утворювали таких ситуацій, але цього було недостатньо для конкурування з Enternet. З часом через розвиток та пошвидшення швидкості передачі, системи токенів та кілець усі системи стали рівноконкурентноздатними між собою.

Зачеплена тема захисту інформації, чому ця тема завжди актуальна, цілі, які можуть переслідувати різні загрози. Браундмауер - міжмережний екран установлюється між мережею та Інтернет і виконує роль мережевого фільтра. Він налаштовується таким чином, щоб пропускати допустимий трафік від користувачів мережі до служб Інтернет і назад, і обмежити трафік з боку Інтернет до мережі, яка потребує захисту, тільки необхідними службами.

Розглянутий комплексний підхід для забезпечення інформаційної безпеки корпоративної комунікаційної системи, основні способи, а саме законодавчі, морально-етичні, організаційні та технічні і програмні, а також що вони передбачають, допускають та як реалізуються

Окремо розглянуті NAT-перетворення(а далі і більш розширена технологія PAT), як він працює та способи розміщення та захисту демілітарізованної зони, яку не логічно та небезпечно розміщувати за одним шлюзом з іншою інформацією, яка потребує вищого рівня безпеки.

Віруси, їх види, класифікація та проблеми антивірусного захисту. Головна зброя проти вірусів є антиірусні програми, які виявляють та видаляють віруси що використовують різні види маскування. Окрім них також існують міжмережеві єкрани, що дозволяють розділити загальну мережу на дві чи більше і реалізувати

набір правил, що визначають умови проходження пакетів з даними через кордон з однієї частини загальної мережі в іншу.

Розглянута технологія ACL(Access Control List), що є важливим елементом налаштування безпеки в локальних корпоративних інформаційно-комунікаційних системах та використовується для контролю доступу до ресурсів мережі і може бути налаштований на різних мережевих пристроях, включаючи комутатори, маршрутизатори або файєрволи.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Розробка комплексної системи захисту корпоративної інформації системи підприємства ZIBER на базі обладнання KEENETIC

2.1.1 Характеристика підприємства

В результаті вивчення розташування кабінетів підприємства «Ziber» побудовано план (рис. 2.1). Для відображення використано програмне забезпечення-MS Visio.

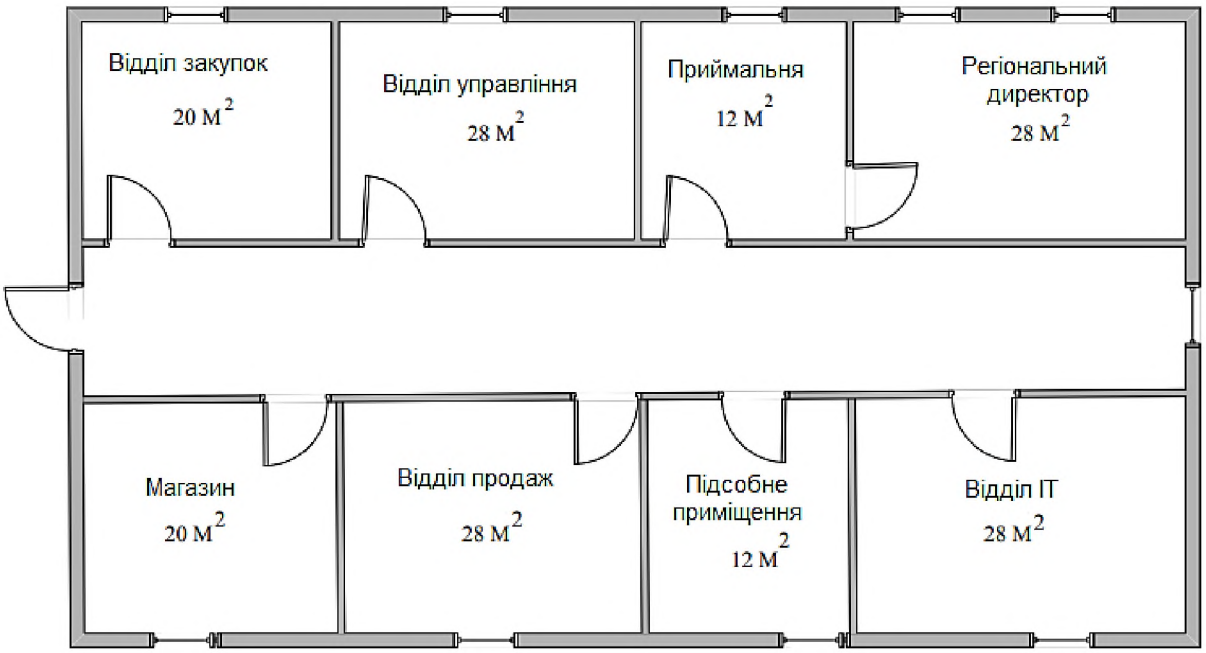


Рисунок 2.1 – Схематичне зображення кабінетів досліджуваного підприємства «Ziber»

В офісі виробничого підприємства «Ziber» працює всього кілька співробітників, причому використовують для своєї роботи мобільні пристрої та ноутбуки. Тому найправильнішим рішенням буде зробити корпоративну мережу за допомогою технології Wi-Fi. Для організації роботи десятка співробітників не потрібно купувати дороге мережеве обладнання. Сучасні Wi-Fi роутери відмінно підходять для організації мережі. Для даного проєкту обрана топологія «зірка». Ця топологія є найпопулярнішою і є основою для функціонування всіх сучасних мереж. Для з'єднання вузлів мережі потрібен пристрій-комутатор, до якого

підключаються всі комп'ютери мережі. Для бездротової мережі таким комутатором є бездротова точка доступу.

Для розробки логічної схеми майбутньої корпоративної системи необхідно вивчити категорії співробітників, що використовують обчислювальну техніку у своїй виробничій діяльності [22, с. 38]:

Регіональний директор: для організації трудової діяльності необхідний ноутбук, комплектуючі (монітор, клавіатура, миша) Бездротова гарнітура і багатобарвне багатофункціональний пристрій (далі – БФП).

Помічник директора: для організації трудової діяльності необхідний стаціонарний комп'ютер, комплектуючі, бездротова гарнітура і багатобарвне БФП.

Керівник проектів: для організації трудової діяльності необхідний ноутбук, комплектуючі, бездротова гарнітура і монохромне БФП.

Менеджер продажів: для організації трудової діяльності необхідний стаціонарний комп'ютер, комплектуючі, бездротова гарнітура, монохромний принтер.

Фахівець із закупівель: для організації трудової діяльності необхідний стаціонарний комп'ютер, комплектуючі, бездротова гарнітура, монохромний принтер.

Координатор: для організації трудової діяльності необхідний ноутбук, комплектуючі, бездротова гарнітура, монохромний принтер.

Інженер: для організації трудової діяльності необхідний ноутбук, бездротова гарнітура і монохромний принтер.

Продавець: для організації трудової діяльності необхідний, стаціонарний комп'ютер, бездротова гарнітура, монохромний принтер. Перерахованим співробітникам необхідний доступ до мережі Інтернет, загальним файлом і друкуючим пристроїв.

Розробка і впровадження корпоративної системи повинні забезпечити автоматизацію роботи підприємства «Ziber», дозволити підвищити точність і оперативність роботи з документацією, автоматизувати формування різних

звітних документів, що значно зменшить тимчасові, а відповідно і матеріальні витрати.

Отримання необхідної інформації в мережі Інтернет, а також за допомогою електронної пошти дозволить прискорити виробничий процес, а отже, збільшити обороти підприємства за рахунок зростання обсягів продажів продукції, що виготовляється [24, с. 170].

Економічна ефективність розробки корпоративної системи обумовлюється скороченням трудовитрат на організацію роботи з ведення бухгалтерського обліку та отримання інформації за необхідними формами, а також зниженням цін на закупівлю необхідних для виробництва матеріалів за рахунок пошуку в мережі Інтернет нових, більш вигідних, постачальників.

Проектована корпоративна комп'ютерна мережа повинна відповідати зростаючим потребам бізнесу:

- легко масштабуватися при збільшенні кількості робочих місць;
- підтримувати механізми забезпечення якості сервісу;
- бути безпечною та високопродуктивною;
- доступ до серверів корпоративної системи повинен здійснюватися на швидкості до 1 Гбіт/с;
- користувачі дротової мережі повинні мати доступ до її ресурсів на швидкості 100 Мбіт/с;
- користувачам бездротової мережі надається смуга пропускання 54 Мбіт/с;
- дротова і бездротова мережа повинні управлятися централізовано;
- передача даних по бездротовій мережі повинна задовольняти вимогам безпеки.

2.1.2 Розрахунок необхідної кількості комп'ютерного устаткування корпоративної системи

Враховуючи потреби співробітників підприємства «Ziber» у комп'ютерній техніці (рис. 2.2) продемонструємо логічну схему корпоративної системи. Всі комп'ютери і друкуюча мережева техніка об'єднані в одну підмережу за

допомогою комутатора. Задля була обрана топологія – «зірка». Перевага даної топології-висока продуктивність і легкий пошук несправностей і обривів мережі.

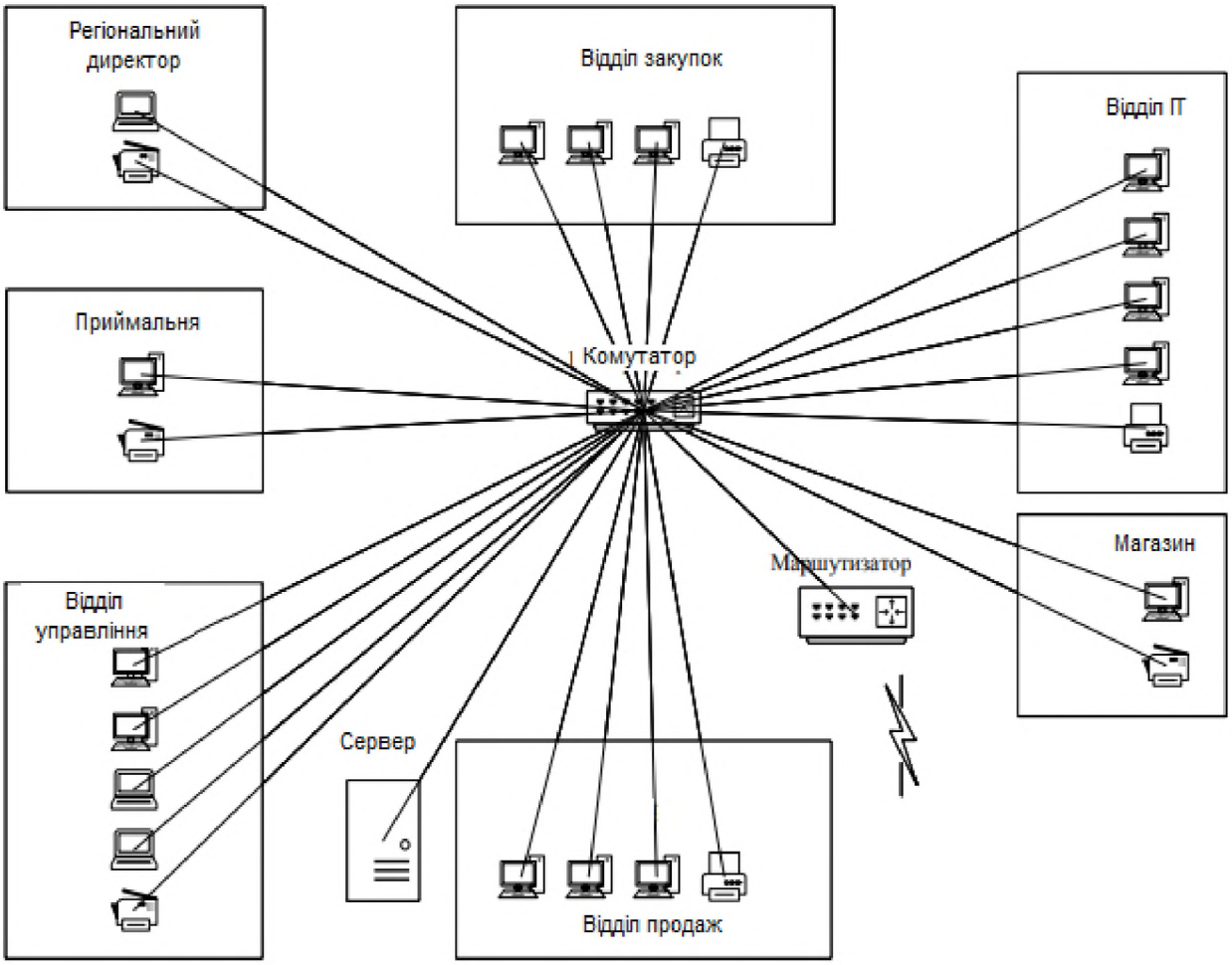


Рисунок 2.2 – Логічна схема об'єднання комп'ютерів підприємства «Ziber» в корпоративну мережу

Крім того, для розробки корпоративної системи нам потрібно Switch 10 / 100Mb 16 портів – 2 штуки, в одному з них обов'язково повинний бути BNC роз'єм для комутації сегмента з топологією «загальна шина». Ці два Switch комутуються між собою крученою парою; кручена пара – 350 метрів 10BaseFL; коаксіальний кабель – 150 метрів 10Base5; роз'єми: KJ45–32 штук (2 роз'єми на комутацію свічів, 2 роз'єми для підключення інтернет сервера, 2 роз'єми для підключення файлового сервера, 2 роз'єми для підключення принт-сервера).

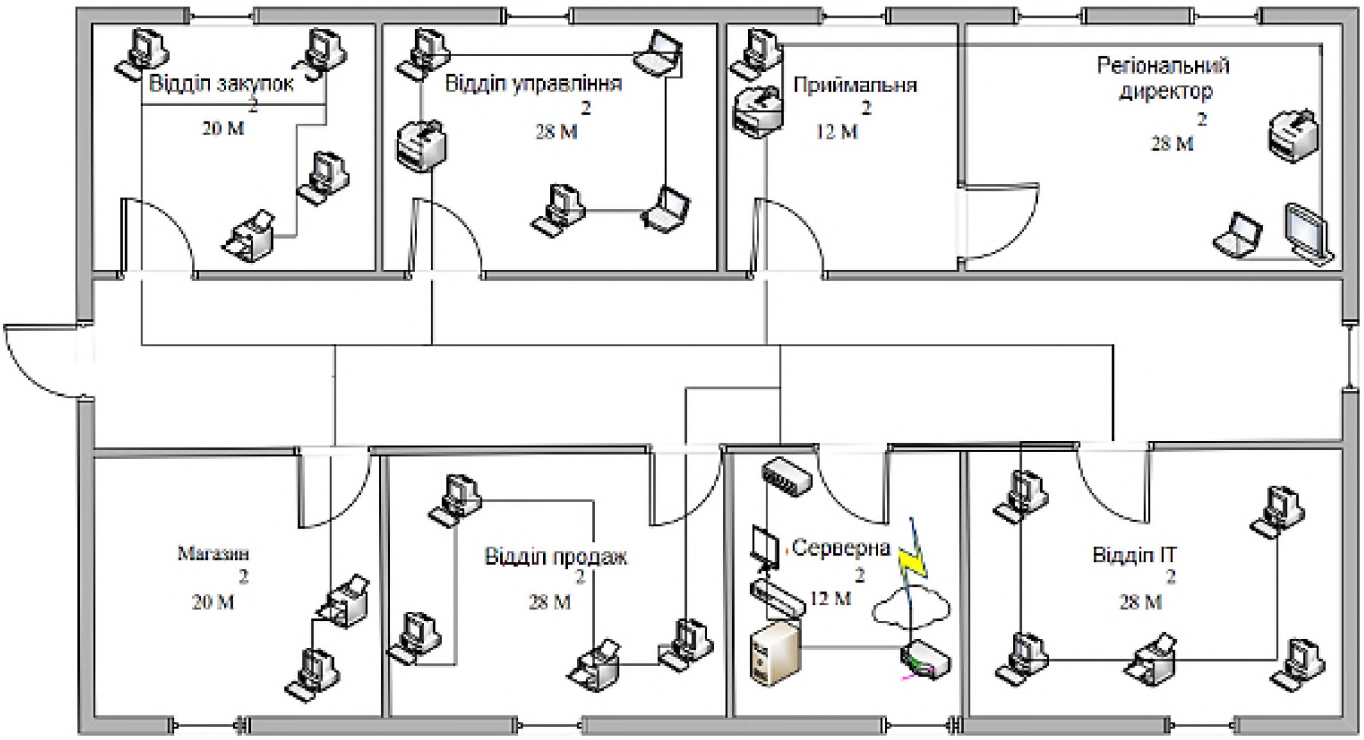


Рисунок 2.3 – Фізична схема організації корпоративної системи досліджуваного підприємства

Для монтажу мережі була використана кручена пара категорії CAT 5e [8]. Вибір якої обумовлений вимогою замовника.

Рисунок 2.4 – Зовнішній вигляд крученої пари категорії 5e

CAT 5 (смуга частот 100 МГц) – 4-х парний кабель, завдяки високій швидкості передачі, до 100 Мбіт/с при використанні 2-х пар і до 1000 Мбіт/с, при використанні 4-х пар, є найпоширенішим мережевим носієм, що використовується в комп'ютерних мережах досі. При прокладанні нових мереж використовують кілька вдосконалений кабель CAT5e (смуга частот 125 МГц), який краще пропускає високочастотні сигнали [23, с. 214]. Його перевагами є:

хороший радіус вигину; максимальна довжина 100 метрів без втрати сигналу; мідні жили та доступна ціна.

2.1.3 Вибір і обґрунтування програмного забезпечення корпоративної системи

На сервері досліджуваного підприємства буде розгорнута ОС-Microsoft Windows Server 2012 R2 Standard, на робочих станціях – Microsoft Windows 10 Enterprice.

Рисунок 2.4 – Логотип програмного продукту Microsoft, що планується використати в даній розробці

Windows Server 2012 R2. Аналізуючи програмне забезпечення Windows Server 2012 R2 слід сказати, що воно має 4 редакції:

- Datacenter – максимально повна по кількість функцій редакція, яка призначена для великих компаній, часто використовують віртуалізацію. Головна її перевага – можливість підключення необмеженої кількості віртуальних машин. Необхідна ліцензія на сервер і на клієнтський доступ (CAL). Datacenter покриває два фізичних процесори.
- Standart – не відрізняється від Datacenter по функціоналу, але дозволяє підключити до двох віртуальних машин. Зручна для тих компаній, які рідко використовують віртуалізацію. При необхідності збільшення кількості віртуальних машин, можна повторно купити Windows Server 2012 R2 Standart, адже кожна Ліцензія запускає дві віртуальні машини [22, с. 56].
- Essentials – редакція обмеженої функціональності, яка підійде для невеликих компаній. Вона не дозволяє запускати віртуальні машини. Також

важливо пам'ятати, що не можна замовляти Windows Server 2012 R2 Essentials для компанії з кількістю користувачів, що перевищують 25 осіб. Ліцензія CAL (Client access license) в даному випадку не потрібна, продукт ліцензується на сервер, Ліцензія покриває один-два процесори. Запуск Essentials може бути проведений як у фізичному, так і віртуальному середовищі.

- Foundation – сама обмежена за функціоналом редакція Windows Server 2012 R2, яку не можна купувати в коробковій версії або придбати корпоративний варіант ліцензії. Foundation поставляється тільки разом з готовими серверами і купується у виробника. Вона не дозволяє запускати віртуальні машини і не використовується у віртуальному середовищі, дозволяє підключити до 15 користувачів, і використовується тільки на серверах з одним процесором.

Серед головних нововведеннями в Windows Server 2012 R2 є:

- наявність загальних віртуальних дисків, що дозволяють проводити кластеризацію і зберігати інформацію без допомоги дорогого обладнання;
- можливість на ходу змінювати розмір VHDX дисків, навіть якщо запущена віртуальну машину (ВМ);
- автоматичне ліцензування кожної нової віртуальної машини завдяки новій системі ліцензування Automatic Virtual Machine Activation (AVMA). Цей тип ліцензії доступний для редакцій Datacenter, Standard або Essentials.

Перелічимо головні переваги Windows Server 2012 R2. Windows Server 2012 R2 призначений для створення хмарних середовищ і центрів даних, в яких можна зручно зберігати дані, що вимагають великих ресурсів. Приємним бонусом для кожної компанії стане можливість швидкого відновлення даних, адже платформа передбачає захист від перебоїв в мережі. У Windows Server 2012 R2 можна з легкістю розгорнути або масштабувати додатки, ефективно розподіляти навантаження між локальним вузлом і хмарним сервісом. Останній дозволяє постійно мати доступ до корпоративної інформації, додатків та інших ресурсів, а

просте управління посвідченнями в центрі обробки персональних даних забезпечує повну безпеку інформації [15, с. 60].

Microsoft Windows 10 Enterprice – корпоративна редакція операційної системи, яка орієнтована на використання у великих фірмах з власними серверами, локальними мережами та іншої IT-інфраструктурою. Це проявляється в двох аспектах. По-перше, з коробки в неї вбудовано кілька спеціальних служб, спрямованих на покращення внутрішньомережевої роботи. По-друге, вона продається за передплатою, а не одноразовим платежем за весь період використання. Унікальними службами версії Enterprise є: BranchCache – інструмент прискорення оновлення, коли кожен комп'ютер в локальній мережі виступає в якості «Сіда». Також він прискорює передачу файлів, якщо вони зберігаються більш ніж на одній «машині»; Device Guard – програмно-апаратний набір технологій, спрямований на підвищення захисту комп'ютера. Контролює цілісність коду, процес завантаження, роботу з оперативною пам'яттю і так далі.

Windows 10 Enterprise потрібна для професійних користувачів. І загальними для неї можливостями є:

- приєднання до домену. Це необхідно для роботи системи групового оновлення, розгортання додатків, автоматичного управління;
- управління груповою політикою. Дозволяє адміністратору мережі централізовано відключати і включати деякі налаштування на приєднаних до домену комп'ютерах;
- EMIE (Internet Explorer в режимі підприємства). Переводить вбудований браузер операційної системи в режим роботи, максимально сумісний з внутрішньо-корпоративними сайтами; розмежування доступу. Допомагає налаштовувати доступ для певних користувачів, в тому числі мережевих, до тих чи інших файлів, папок і так далі;
- режим віддаленого робочого столу. Дозволяє віддалено підключатися до ПК, що працює під управлінням Windows Enterprise, через нативний інструмент Remote Desktop. Комп'ютер з Windows 10 може виступати в якості клієнта – можна підключатися з нього, але не до нього;

- Клієнт Hyper-V. інструмент віртуалізації для 64-розрядних процесорів з підтримкою гостьових операційних систем сімейств Linux і Windows до «десятки» [16, с. 130];
- BitLocker. Інструмент шифрування жорсткого диска, який робить дані нечитабельним в разі підключення цього HDD до іншого комп'ютера або перевстановлення Windows;
- підтримка TPM2.0 – апаратно-програмної системи, яка перевіряє структуру завантажувального сектора жорсткого диска на предмет впровадження сторонніх вірусних додатків.

Credential Guard – програмний набір технологій, спрямований на захист облікового запису. Допомагає не тільки паролі зберегти, але і запобігти доступу до особистих файлів при хакерських або вірусних атаках;

Direct Access – утиліта для віддаленого управління операційною системою і комп'ютером.

Рішення дозволяє організувати комплексну інформаційну систему, відповідну корпоративним, українським і міжнародним стандартам і забезпечуючу фінансово-господарську діяльність підприємства. Прикладне рішення створює єдиний інформаційний простір для відображення фінансово-господарської діяльності підприємства, охоплюючи основні бізнес-процеси. В той же час чіткий розмежовується доступ до відомостей, що зберігаються, а також можливості тих або інших дій залежно від статусу працівників.

Внутрішній устрій прикладного рішення повністю відкрито для вивчення і налаштування під специфічні потреби підприємства. Для реалізації роботи використовуватимемо сервер HP Proliant DL380 G5 Server (458562–421) зі встановленою MS SQL Server 2008 і операційною системою MS Windows Server 2008 Standard Edition [18, с. 205].

2.1.4 Вибір серверного обладнання

Так як в корпоративній мережі використовується один сервер, необхідно підібрати продуктивне, сучасне обладнання яке забезпечить режим багатозадачності для роботи проєктованого програмного засобу [5, с. 61].

Таблиця 2.1 – Технічні характеристики сервера для корпоративної комунікаційної системи

Найменування	Комплектуючі	Характеристики/модель
Сервер ProLiant ML150G9 834607–421	Центральний процесор	Intel Xeon E5–2609v4
	Оперативна пам'ять	8 Т6 / DDR4 / 2400 МГц
	Підтримка RAID	0 / 1 / 10 / 5
	Блок живлення	1х550 Вт
	HDD	2х2 ТБ

Мобільна робоча станція в проєктуємій корпоративній мережі – ноутбук, призначений для керівника часто перебувають у відрядженнях або на ділових зустрічах.

Таблиця 2.2 **– Технічна характеристика ноутбуку для корпоративної комунікаційної системи**

Найменування	Комплектуючі	Характеристики/модель
Ноутбук HP Pavilion x360 13-u002ur	Центральний процесор	Core I5–6200U
	Оперативна пам'ять	4 г6 / DDR4 / 2133 МГц
	HDD	SSD 256 ГБ
	Дисплей	13,3

Таблиця 2.3 – Технічні характеристики стаціонарного комп'ютера

Найменування	Комплектуючі	Характеристики/модель
Комп'ютер HP ProDesk 400 G2 K8K74EA	Центральний процесор	Intel Core I3 7100
	Оперативна пам'ять	4 г6 / DDR4 / 2133 МГц
	HDD	SATA 500 ГБ
	Відеосистема	Intel HD Graphics

Стаціонарна робоча станція в проєктованій корпоративній мережі - комп'ютер, призначений для рядових співробітників, розташовані практично у всіх кабінетах офісу.

2.1.5 Вибір комутаційного обладнання корпоративної системи (KEENETIC Ultra, Giga, Viva і т.д.)

Для офісу був обраний роутер Інтернет-центр Keenetic Giga II. Він служить перш за все для підключення Інтернету, мережі провайдера і його сервісів. Вбудований міжмережевий екран Інтернет-центру захищає всі пристрої мережі від атак з Інтернету та має можливості налаштування функцій ACL та протоколів NAT і PAT.

Крім того, Keenetic Giga II обладнаний багатофункціональним 2-портовим хостом USB, завдяки якому можна організувати постійне підключення до Інтернету через USB-модем оператора мобільного зв'язку 3g / 4g, відкрити мережевий доступ до USB-накопичувача по FTP з Інтернету або з домашньої мережі по DLNA, а також забезпечити загальний доступ до USB-принтера з декількох мережевих пристроїв. Інтернет-центр Keenetic Giga II призначений для доступу в Інтернет по виділеній лінії Ethernet через провайдерів, що використовують будь-які типи підключення: VPN (PPTP і L2TP), PPPoE, 802.1 X, VLAN 802.1 Q, IPv4 / IPv6. Фірмова технологія ZyXEL Link Duo дозволяє комп'ютерам домашньої мережі отримати одночасно доступ і в Інтернет, і до локальних сервісів провайдера по одній виділеній лінії [7, с. 118].

Інтернет-центр дозволяє організувати високошвидкісну бездротову мережу для спільної роботи в Інтернеті і робочої мережі з ноутбуків, смартфонів і інших пристроїв Wi-Fi стандарту IEEE 802.11 n. Дві антени з коефіцієнтом посилення 5 дбі забезпечують широку зону покриття мережі Wi-Fi і висока бездротового зв'язку на швидкості до 300 Мбіт/с. Для гостьових пристроїв можна включити окрему мережу Wi-Fi, призначену для виходу в Інтернет без доступу до інформації в мережі.

Для філій і сервісного центру обрані Інтернет центри Keenetic Giga та Viva. Ці пристрої мають ті ж самі функції, що і Keenetic Giga II, але володіють меншим радіусом дії Wi-Fi. На роботу філій це не позначиться, оскільки площа приміщень по перевищує 20 м, проте дозволить скоротити витрати на покупку мережевого та Інтернет обладнання.

Контролер в корпоративній мережі працює на всіх нових моделях Keenetic (з індексом KH-XXXX) від початку до ультра і на пристроях попереднього покоління, для яких доступний реліз KeeneticOS 2.15 (Giga III, Ultra II, Air, Extra II, Start II, Lite III Rev. B и 4G III Rev. B). Для роботи не потрібно підключення Інтернету і хмарних сервісів.

Ретранслятором в корпоративній мережі може виступати будь-яка з нових моделей Keenetic (з індексом KH-XXXX) від початку до ультра, а також деякі моделі попереднього покоління, для яких доступний офіційний реліз KeeneticOS 2.15 і вище (Giga III, Ultra II, Air, Extra II, Start II, Lite III Rev. B и 4G III Rev. B).

Keenetic Ultra KN–1810. Апаратна конфігурація роутера частково збігається з Keenetic Giga: процесор MediaTek MT7621AT (два ядра MIPS1004Kc, 880 МГц, вбудовані контролери USB і гігабітний мережевий комутатор), 256 МБ оперативної пам'яті DDR3, 128 МБ Флеш-пам'яті NAND. Але є і важлива (втім, і єдина) відмінність – замість одного радіо MediaTek MT7615DN, обслуговуючого і діапазон 2,4 ГГц і діапазон 5 ГГц в режимі 2T2R кожен, тут встановлені дві мікросхеми MT7615N, так що обидва діапазони отримали схему 4T4R.

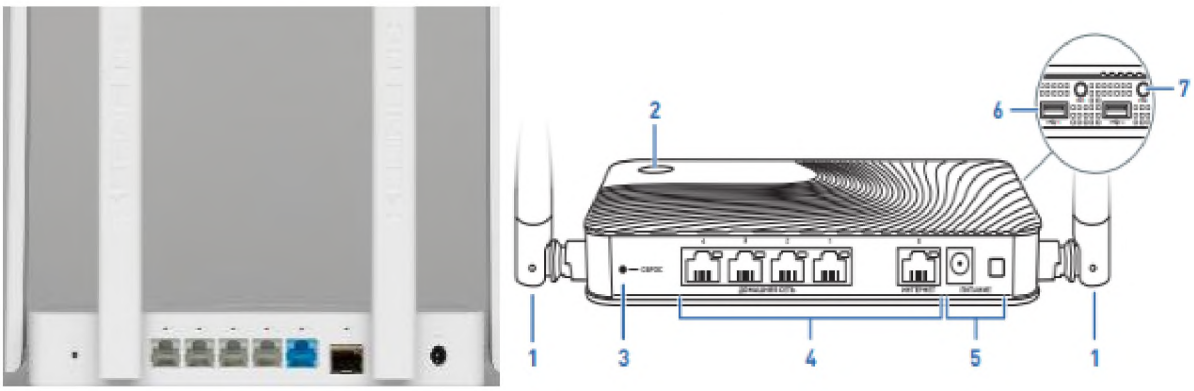


Рисунок 2.5 – Зовнішній вигляд Keenetic Ultra

1. Антени бездротової мережі Wi-Fi, 2. Кнопка управління бездротовою мережею Wi-Fi, 3. Кнопка «скидання» (скидання налаштувань Користувача), 4. Мережеві порти «0... 4» П'ять портів Ethernet для підключення домашніх пристроїв та інтернет-кабелю. 5. Вимикач і роз'єм «живлення». 6. Універсальні порти USB 2.0 і 3.0-і порти для підключення сумісних USB-пристроїв, таких, як Модеми 3G / 4G, принтери і зовнішні жорсткі диски з інтерфейсом USB 2.0 або USB 3.0. 7. Кнопки з призначуваними функціями «FN1» і «FN2».

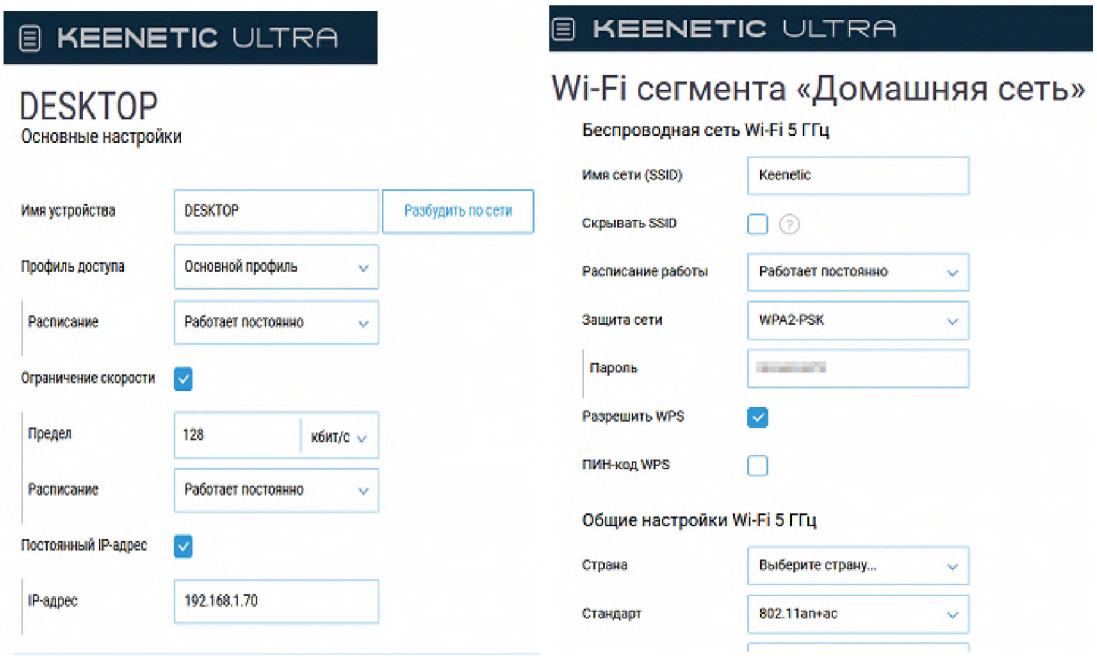


Рисунок 2.6 – Основні налаштування та підключення до бездротового інтернету Keenetic Ultra KN–1810

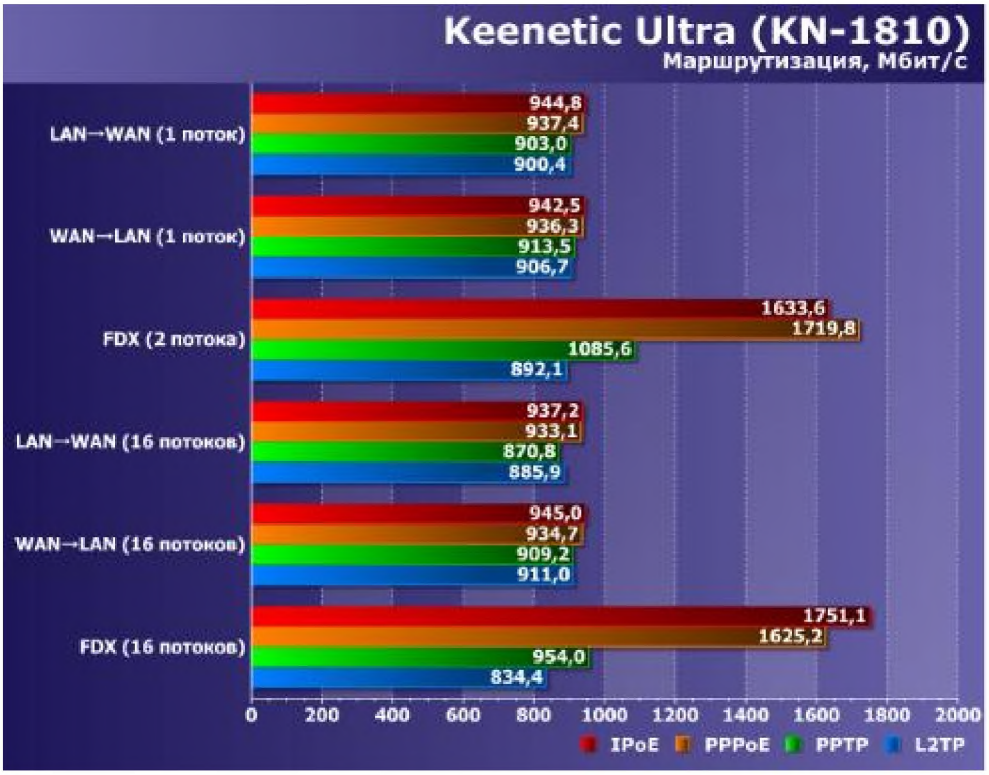


Рисунок 2.7 – Маршрутизації інтернет-трафіку для різних типів підключення Keenetic Ultra KN–1810

Пристрій здатний максимально ефективно працювати у всіх режимах – в разі передачі даних в одну сторону реальна швидкість становить близько 900 Мбіт/с. у дуплексі для PPTP і L2TP використовується тільки програмне

прискорення, так що тільки в IPoE і PPPoE, де є і апаратний прискорювач, ми бачимо тут швидкість помітно вище гігабіта [9, с. 120].

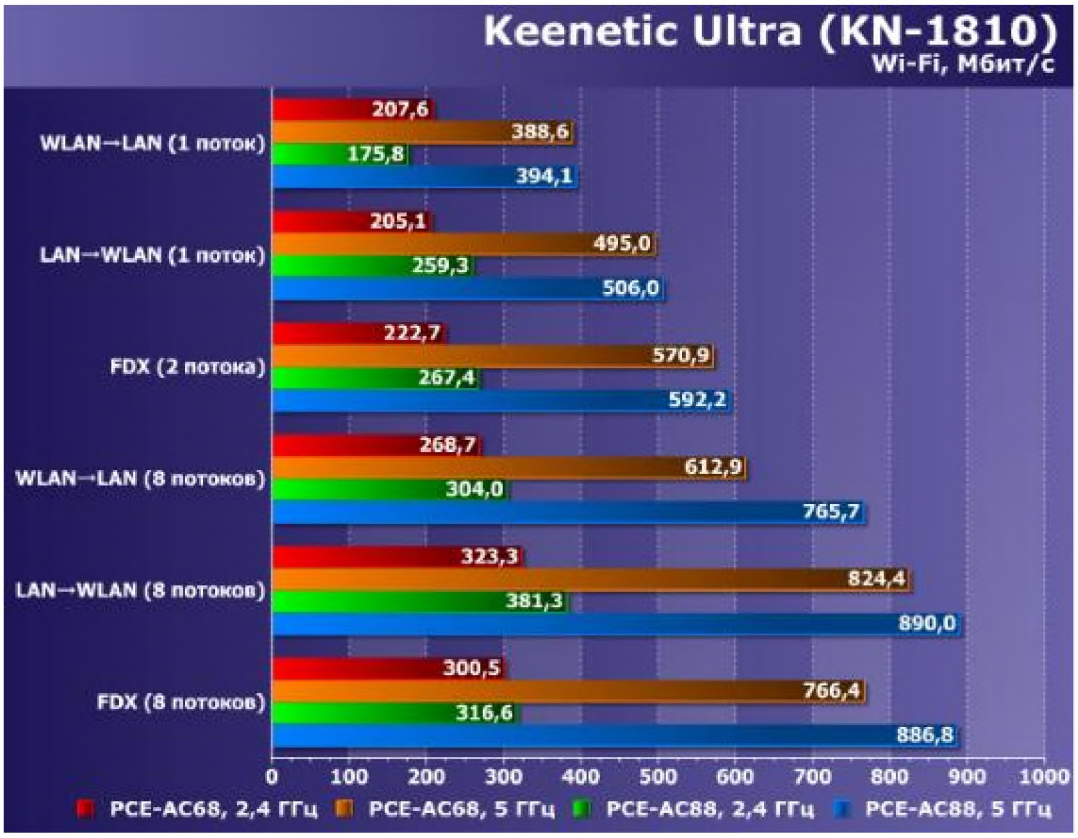


Рисунок 2.8 – Маршрутизації інтернет-трафіку (бездротового) для різних типів підключення Keenetic Ultra KN–1810

Keenetic Ultra KN–1810 здатний забезпечити близько 150 Мбіт/с для режимів PPTP і L2TP і майже 300 Мбіт/с для IPSec. Сервери SSTP і OpenVPN виключно реалізовані програмним чином і для них ми отримали тільки близько 25 Мбіт/с.

Keenetic Giga III призначений для надійного повнофункціонального підключення будинку до Інтернету і IP-телебачення по виділеній лінії Ethernet через провайдерів, що використовують будь-які типи підключення: IPoE, PPPoE, PPTP, L2TP, 802.1 X, VLAN 802.1 Q, IPv4 / IPv6. При цьому він дає повну швидкість за тарифами до 1000 Мбіт/с незалежно від виду підключення і характеру навантаження, а для IPoE / PPPoE – до 1800 Мбіт/с в дуплексі. Крім того, Keenetic Giga III може забезпечувати підключення до Інтернету через десятки популярних USB-модемів 3G / 4G, DSL-модем або провайдерський

Роптермінал з портом Ethernet, а також через провайдерський або приватний хот-спот Wi-Fi.

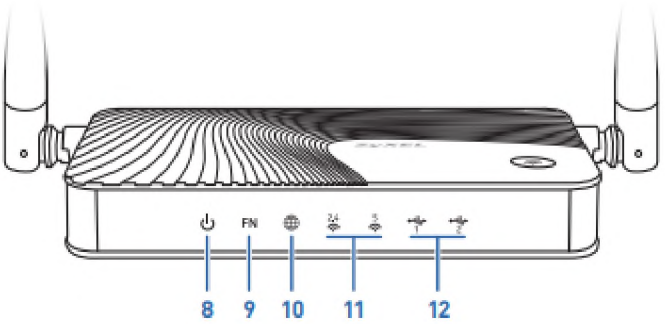


Рисунок 2.9 – Функціональне призначення основних виходів та індикаторів на пристрої Keenetic Giga III

8. Індикатор (Статус). 9. Індикатор FN-настроюваний індикатор індикатор реагує на вибрані вами події. 10. Індикатор (Інтернет / Авторизація). 11. Індикатори (бездротові мережі Wi Fi 2,4 ГГц і 5 ГГц). 12. Індикатори (підключення до роз'ємів «USB»).

При першому ж включенні Інтернет-центр розгортає максимально захищену за стандартом WPA2 дводіапазонну мережу Wi-Fi 802.11 n / ac для ноутбуків, смартфонів, планшетів та інших бездротових пристроїв.

Поворотні антени і спеціальні підсилювачі сигналу Wi-Fi дають максимально широку зону покриття і високу якість бездротового зв'язку на швидкості з'єднання до 867 + 300 Мбіт/с незалежно від положення Інтернет-центру. Для гостьових пристроїв передбачена окрема мережа Wi-Fi з виходом тільки в Інтернет без доступу до домашньої мережі. Оптимальний робочий канал вибирається автоматично на основі періодичного аналізу радіоефіру [10, с. 75].

Поряд з доступом в Інтернет через USB-модеми 3G / 4G, а також мережевим використанням USB-накопичувачів і USB-принтерів порти USB можуть використовуватися для підключення таких пристроїв, як DECT-станція Keenetic Plus DECT або ADSL2+ / VDSL2-модем Keenetic Plus DSL. Швидкість читання з підключених по USB 3.0 дисків становить не менше 40 Мбайт/с. Максимальна швидкість з'єднання в бездротовій мережі (867 Мбіт / с для діапазону 5 ГГц і 300 Мбіт / с для 2,4 ГГц) досягається за умови підключення пристроїв Wi-Fi стандарту IEEE 802.11 ac або 802.11 n, що використовують для прийому і передачі двох просторових потоків і канал шириною 80 МГц або 40 МГц відповідно.

Маршрутизатор Keenetic Viva (KN–1910) можна сміливо назвати спрощеною версією Giga (KN–1010).

Рисунок 2.9 – Зовнішній вигляд маршрутизатора Keenetic Viva KN–1910

Якщо орієнтуватися на ціни, представлені на сайті розробника, то різниця між Viva і Giga становить 1 600 грн: 8 190 грн і 6 590 грн. В нашому проєктуванні ми обрали Keenetic Giga III та Keenetic Viva KN–1910, адже різниця в їх ціні невелика в порівнянні з Keenetic Ultra KN–1810.

Таблиця 2.4 – Порівняння характеристик Keenetic Giga III та Keenetic Viva KN–1910

	Keenetic Viva (KN–1910)	Keenetic Giga (KN–1010)
Стандарти	IEEE 802.11 a / b / g / n / ac (2,4 ГГц + 5 ГГц); 802.11 k / r	
Чіпсет	MediaTek MT7621A (2 x MIPS1004KC 880 МГц)	
Контролер	MT7615D	
	-	Realtek RTL8211FS
RAM	128 Мбайт	256 Мбайт
ROM	128 Мбайт	
Антени	4 x зовнішні 5 dBi; довжина 175 мм	
	-	Підсилювачі прийому / передачі
Шифрування Wi-Fi	WPA / WPA2, WEP, WPS	
Макс, швидкість	802. Пас: до 867 Мбіт/с; 802.11п: до 400 Мбіт/с	
	5 x 10 / 100 / 1000 Мбіт/с RJ–45	
Інтерфейси	-	1 x 100 / 1000 Мбіт/с SFP
	2 x USB 2.0	1 x USB 2.0; 1 x USB 3.0
Індикатори	4 x на верхній кришці	6 x на верхній кришці (2 x FN)
	-	У кожного мережевого порту
Апаратні кнопки	Відключення Wi-Fi / запуск WPS, перезагрузка/скидування налаштувань, 2 x FN (програмовані)	
Розміри (ШхДхВ)	159 x 110 x 29 мм	214 x 153 x 33 мм

Перевага Viva заключаєтьсяу менших габаритах. Наприклад, вона набагато компактніше Giga / Ultra – 159 × 110 × 29 мм проти 214 × 154 × 33 мм – і приблизно вдвічі легше. Але даний пристрій гріється сильніше через іншу форму корпусу. Розміри зменшені завдяки відмові від SFP-порту і переносу одного USB-роз'єму: тепер вони знаходяться на протилежних бічних гранях. Однак загальний стиль оформлення корпусу залишився колишнім. Комплектний блок живлення у Viva інший, трохи більш компактний і менш потужний (18 Вт) [19, с. 73].

Таблиця 2.5

Можливості Keenetic Giga (KN–1010) та Keenetic Viva (KN–1910)

Доступ в Інтернет	Static IP, DHCP, PPPoE, PPTP, L2TP, SSTP, 802. lx; VLAN; KABiNET; DHCP Relay; IPv6 (6in4); Multi-WAN; пріоритети підключення (policy-based routing); резервне підключення + Ping checker; MSP; майстер налаштування NetFriend
Сервіси	Сервер DLNA, FTP, SMB, AFP; TimeMachine; прінт-сервер; BitTorrent-клієнт Transmission; VLAN; VPN-сервер (IPSec / L2TP, PPTP, Open VPN, SSTP); Entware; модулі Keenetic Plus; автообновлення прошивки; Captive-портал; NetFlow / SNMP; SSH-доступ
Захист	Батьківський контроль, фільтрація, захист від телеметрії і реклами: «Яндекс. DNS», SkyDNS, AdGuard, Norton ConnectSafe; HTTPS-доступ до веб-інтерфейсу
Проброс портів	Інтерфейс / УІЛМ+порт+протокол+IP; UPnP, DMZ; IPTV / VoIP LAN-Port, VLAN, IGMP / PPPoE Proxy, udpxy
QoS / Шейпинг	WMM, IntelliQoS; вказання пріоритету інтерфейсу / VLAN + DPI; шейпер
Сервіси Dynamic DNS	DNS-master (RU-Center), DynDns, NO-IP; KeenDNS
Режим роботи	Маршрутизатор, MSP-клієнт/медіа-адаптер, точка доступа, повторювач
Проброс VPN, ALG	PPTP, L2TP, IPSec; (T) FTP, H. 323, RTSP, SIP
Брандмауер	Фільтрація по порт / протокол / IP; Packet Capture; SPI; захист від DoS

Через обмеження порту версією 2.0 у Keenetic Viva (KN–1910) будуть працювати повільніше: в описі заявлена швидкість до 40 Мбайт/с. незмінний стендовий накопичувач Kingston SSDNow V+200 з одним NTFS-розділом, упакований у зовнішній бокс LanShuo INIC–3609, показав рівно ці цифри. Що по FTP, що по SMB можна отримати трохи більше 40 Мбайт/с при читанні і трохи менше 40 при записі.

Базові налаштування Keenetic Viva KN–1910 все ті ж, тобто це шифрування WPA2, 802.11 n + ширина каналу 20 / 40 МГц для 2,4 ГГц, 802.11 n / ac + ширина 20 / 40 / 80 МГц для 5 ГГц, всі базові опції MU-MIMO / Beamforming / 256-QAM /

TxBurst при наявності включені. Конфігурації стендів колишні. Перша машина: Intel Core i7–3770, 16 Гбайт RAM, ASUS PCE-AC88 на базі чіпсета Broadcom 4366, Realtek RTL8168, Windows 7 SP1 x64. Друга: Intel Xeon D–1540, 32 Гбайт ECC RAM, 2 x Intel I210 (у таблиці позначений як R), 2 x Intel I350, Devuan Jessie.

Таблиця 2.6 – Результати тестування маршрутизатора Keenetic Viva KN–1910

Потоки	1	2	4	8	16	32	64
Средняя скорость Wi-Fi 802.11ac 5 ГГц, Мбит/с							
A → R	415	546	559	671	673	657	607
R →A	268	537	607	669	681	658	627
A↔R	520	547	573	644	683	681	661
Средняя скорость Wi-Fi 802.1Ш 2,4 ГГц, Мбит/с							
A → R	171	209	193	214	169	141	151
R →A	173	195	202	211	226	190	193
A↔R	167	186	206	209	210	198	170

В цілому умови тесту ті ж, що і завжди. Згодом змінюється тільки стан навколишнього ефіру. Число видимих сусідських точок доступу не те щоб стрімко зростає, але важливо те, що все більше з них перебирається в діапазон 5 ГГц. Через це, зокрема, довелося примусово вибрати 64-й канал-лише тому, що він був далі від сторонніх ТД.

Рисунок 2.10 – Схематичне зображення результатів тестування маршрутизаторів

Сам же роутер (в таблиці 3.7 позначений як R) при автовиборі каналу стабільно йшов у верхню частину діапазону (за сотий канал). Keenetic Giga III та Keenetic Viva KN–1910 знаходилися в прямій видимості один від одного на відстані чотирьох метрів. В обох діапазонах істотних відмінностей між Giga і Viva немає. В 2,4 ГГц з Viva набагато рідше було видно швидкість 400 Мбіт/с і набагато частіше з'єднання йшло до 200 Мбіт/с [47, с. 205].

Keenetic Giga III, в свою чергу давала якщо вже не 400, то 300 Мбіт/с.

2.1.6 Розрахунок адресного простору IP-адрес

План IP-адресацій є фундаментом для реалізації всього проєкту мережі. Розумно складений IP план дозволяє знизити навантаження на обладнання у випадку великих територіально розподілених інсталяцій і спрощує розуміння інфраструктури обслуговуючим персоналом, що в свою чергу знижує ризики відмов елементів мережі через людський фактор.

Залежно від застосування IP-адреса версії 4 може бути ідентифікована як: унікальна IP-адреса (Unicast IP-Address); групова IP-адреса (Multicast IP-Address); широкомовна IP-адреса (Broadcast IP-Address). У повідомленні (IP-пакеті) унікальні IP-адреси можуть зазначатися як адреси відправника (Source IP-Address), так і як адреси отримувача (Destination IP-Address). Групові і широкомовні IP-адреси можуть зазначатися лише як адреси отримувача. IP-адреса отримувача визначає яким є IP-пакет: унікальним, груповим чи широкомовним. Поділ IP-адреси версії 4 на частини здійснюється з використанням двох підходів: класовий, класова IP-адресація (Classful IP-Addressing); безкласовий, безкласова IP-адресація (Classless IP-Addressing).

Таблиця 2.7 – IP-адресація проєктованої корпоративної комунікаційної системи

Назва відділу	Кількість хостів	IP-адрес підмережі або діапазон
Регіональний директор	2	172.205.0.0 / 24
Відділ закупок	4	172.205.2.0 / 24
Приймальня	2	172.205.3.0 / 24
IT-відділ	5	172.205.4.0 / 24
Магазин	2	172.205.5.0 / 24
Відділ продаж	4	172.205.6.0 / 24
Відділ управління	5	172.205.7.0 / 24
Склад	1	172.205.9.0 / 24 172.205.10.0 / 24

Для прикладу, наша корпоративна комунікаційна система має такі IP-адреси мережного адаптера / інтерфейсу – 172.205.14.1. Визначимо такі основні параметри IP-адресації, як клас IP-адреси; пряму класову маску мережі; інверсну класову маску мережі; класовий префікс мережі; IP-адресу (номер) мережі; IP-адресу (номер) вузла; мінімальну IP-адресу діапазону, що може використовуватися для адресації вузлів мережі; максимальну IP-адресу діапазону, що може використовуватися для адресації вузлів мережі; широкомовну IP-адресу мережі; кількість вузлів (IP-адрес вузлів), які можуть входити в мережу.

Як відомо, IP-адреса містить у собі як IP-адресу (номер) мережі, так і IP-адресу (номер) вузла. Кількості байтів, які виділяються на IP-адресу мережі та IP-адресу вузла, визначаються на основі таблиці класів. Задана IP-адреса 172.205.14.1 за даними таблиці класів належить до класу B. Класовою маскою для мереж класу B є маска: 255.255.0.0

Інверсною класовою маскою для мереж класу B є маска: 0.0.255.255

Класовим префіксом для мереж класу B відповідно є префікс: / 16

Для класу B на номер мережі виділяється два перших байти IP-адреси. Відповідно IP-адреса мережі матиме вигляд: 172.205.0.0

Для класу B на номер вузла і IP-адреса вузла матиме вигляд: 0.0.14.1

IP-адреса мережі і широкомовна IP-адреса (нульова й остання IP-адреси відповідно) не можуть призначатися вузлам. Тому мінімальною IP-адресою для діапазону, що може використовуватися для адресації вузлів, є IP-адреса, наступна

за IP-адресою мережі [53, с. 40]. У нашому випадку мінімальною IP-адресою вузла є адреса: 172.205.0.1

Максимальною IP-адресою вузла є адреса: 172.205.255.254

Широкомовною IP-адресою мережі є адреса: 172.205.255.255

Кількість вузлів (IP-адрес вузлів), які можуть входити в мережу, розраховується за формулою: $K_{вузлів} = 2^{(32-Класовий\ префікс)} - 2$

У нашому випадку кількість вузлів становить:

$$K_{вузлів} = 2^{(32-16)} - 2 = 2^{16} - 2 = 65536 - 2 = 65534 \text{ вузли.}$$

2.1.7 Побудова корпоративної системи на основі вибраного обладнання

На початку нашого дослідження перелічимо основні етапи розробки проєктованого програмного засобу для корпоративної комунікаційної системи (таб. 2.8).

Таблиця 2.8 – Основні етапи розробки корпоративної комунікаційної системи

Етап розробки інформаційно-комунікаційної системи	Назва роботи	Зміст роботи
1	2	3
1	Аналіз потреб в доступі до інформації та її обліку	Постановка задачі. Збір необхідних матеріалів. Вибір і обґрунтування критеріїв ефективності і надійності проєктуючої мережі. Обґрунтування необхідності її проведення.
2	Розробка і затвердження технічного завдання на мережу	Визначення основних вимог, що пред'являються до мережі. Освоєння та систематичне обґрунтування побудови мережі на основі вже існуючих ЛОМ
3	Вибір топології мережі і мережного методу доступу	Вивчення графічного проєкту будівлі, в якій буде реалізована локальна мережа та раціональне розташування робочих станцій та серверу. Ефективне фізико-логічне поєднання обладнання між собою, яке утворює мережу.
4	Вибір кабельної структури	Проводиться аналіз надійності та пропускної здатності середовища передачі даних.
5	Аналіз та вибір апаратної організації мережі	Проводиться вибір мережного устаткування на основі поставлених задач, що являються доповненням до вибору типу кабелю.

Продовження таблиці 2.8

1	2	3
6	Прокладка кабелю та установка Комунікації	Прокладання мережного кабелю між комп'ютерами, серверами та мережним обладнанням. Установка активного та пасивного мережного обладнання
7	Вибір мережних ОС	Аналіз існуючих мережних ОС та вибір операційної системи, яка задовольняє поставленим вимогам.
8	Аналіз та вибір програмної організації мережі	Порівнюються характеристики роботи різного програмного забезпечення і обирається найкраще 113.
9	Установка та настроювання мережі	Проведення робіт, направлених на створення логічних зв'язків компонентів мережі та їх правильної роботи.
10	Випробування мережі	Випробування мережі в робочому режимі
11	Створення програмного засобу захисту транспортування даних у мережі	Розробка програмного засобу, що буде функціонувати на обладнанні Keenetic з використанням функції ACL та протоколів NAT і PAT
12	Підготовка документації	Збір матеріалів та технічної документації на мережу для подальшого її розширення та монтажу.

Аналізуючи порядок побудови корпоративної комунікаційної системи на основі вибраного обладнання слід сказати, що контролер автоматично визначить версію операційної системи ретранслятора і при наявності оновлення, в процесі додавання в Wi-Fi-систему, виконає оновлення операційної системи пристрою до останньої актуальної версії. Потрібно натиснути кнопку «захопити», щоб додати ретранслятор до системи Wi-Fi. Дочекатися завершення процесу [54, с. 77].

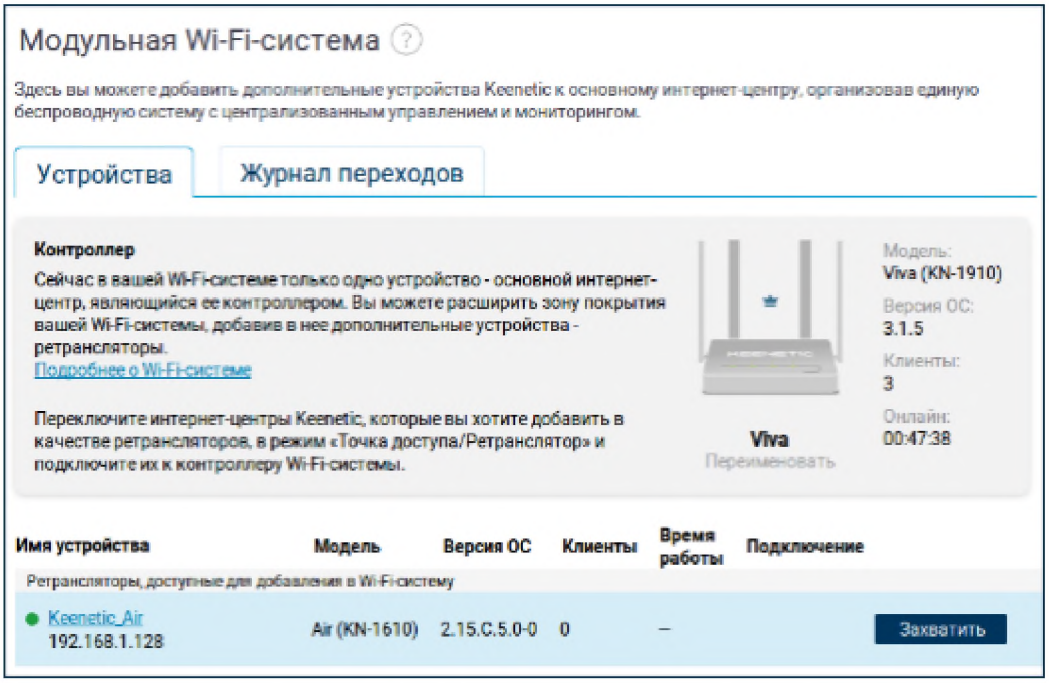


Рисунок 2.11 – Початок побудови мережі за допомогою обладнання Keenetic Viva KN–1910

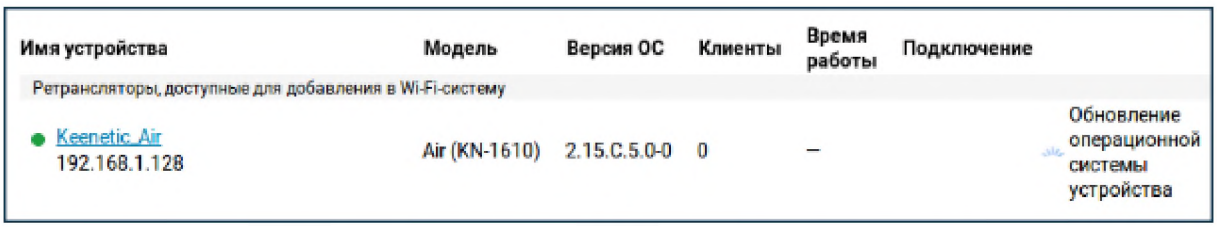


Рисунок 2.12 – Ідентифікація обладнання ОС

Після захоплення пристрою з’явиться в списку «Ретранслятори, що входять в Wi-Fi-систему» [61].

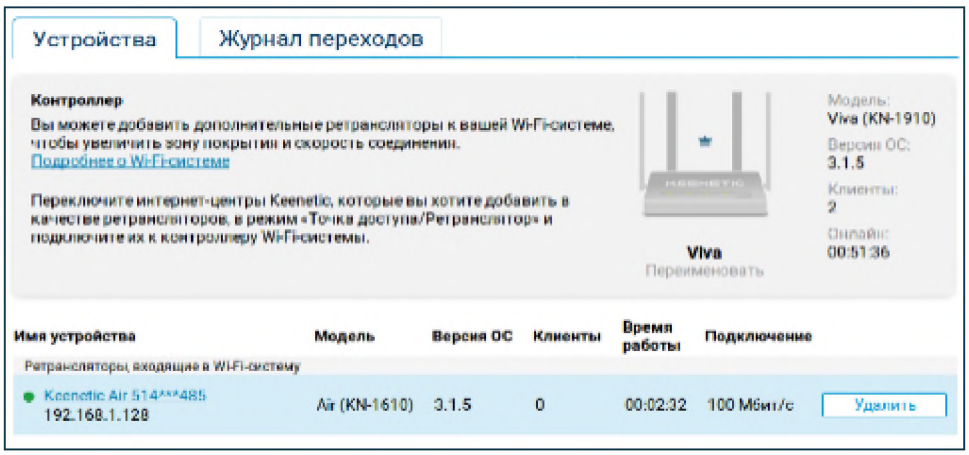


Рисунок 2.13 – Виявлення Wi-Fi-системою наявного підключеного обладнання

Якщо з якоїсь причини ретранслятор не з'являється в списку доступних для додавання або не захоплюється в Wi-Fi-систему, то потрібно виконати скидання налаштувань на заводські і потім повторити підключення. Після додавання ретранслятора в Wi-Fi-систему можна перейти до його веб-конфігуратору. Натисніть по посиланню в назві ретранслятора.

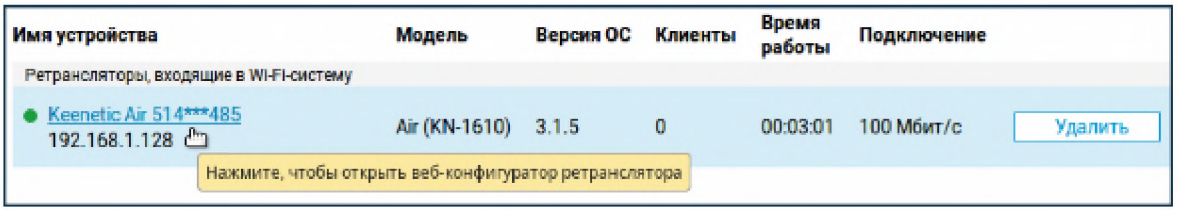


Рисунок 2.14 – Веб-конфігурація наявного підключеного обладнання

При підключенні до інтерфейсу ретранслятора потрібно використовувати пароль облікового запису адміністратора, який встановлений на контролері. Підключившись до веб-інтерфейсу ретранслятора можна побачити повідомлення «цей пристрій керується контролером Wi-Fi-системи».

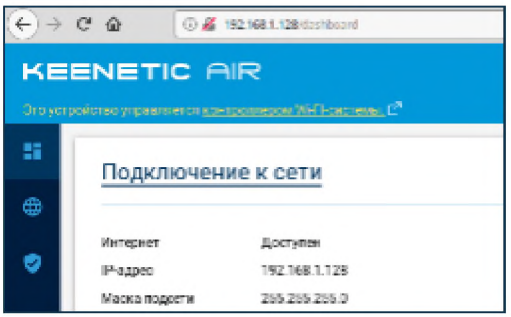


Рисунок 2.15 – Результат підключення до веб-інтерфейсу ретранслятора

На пристрої, який управляється контролером Wi-Fi-системи, основні налаштування бездротової мережі «Ім'я мережі – SSID)» захист мережі «(протокол безпеки)», «Пароль» (ключ безпеки), налаштування безшовного роумінгу, параметри IP, списки контролю доступу (Білий / Чорний) будуть недоступні для редагування. Змінити їх можна тільки на контролері (головному інтернет-центрі).

На сторінці «Модульна Wi-Fi-система «на вкладці» Пристрої» відображаються всі ретранслятори доступні для додавання і входять в Wi-Fi-систему.

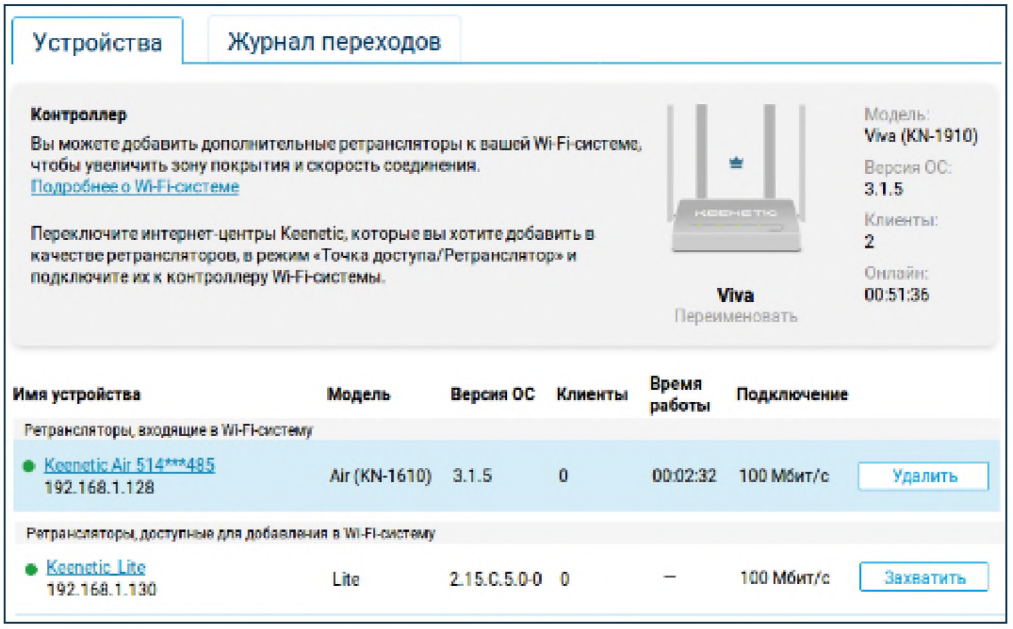


Рисунок 2.16 – Результат вивлення підключених користувачів

На вкладці «Журнал переходів» відображаються переходи бездротових пристроїв між вузлами Wi-Fi-системи. Реєструються події: підключення; відключення; перехід (стандартний перехід без «прискорювачів», клієнт просто відключився від однієї точки і підключився до іншої); перехід по PMK-кешу (швидкий перехід з використанням pmkid-кешу, ідентифікатора спарених майстер-ключів Pairwise Master Key Identifier); швидкий перехід (найшвидший перехід з 802.11 r і режимом Ft – Fast Transition).

Коли в журналі переходів багато записів, можна скористатися фільтром.

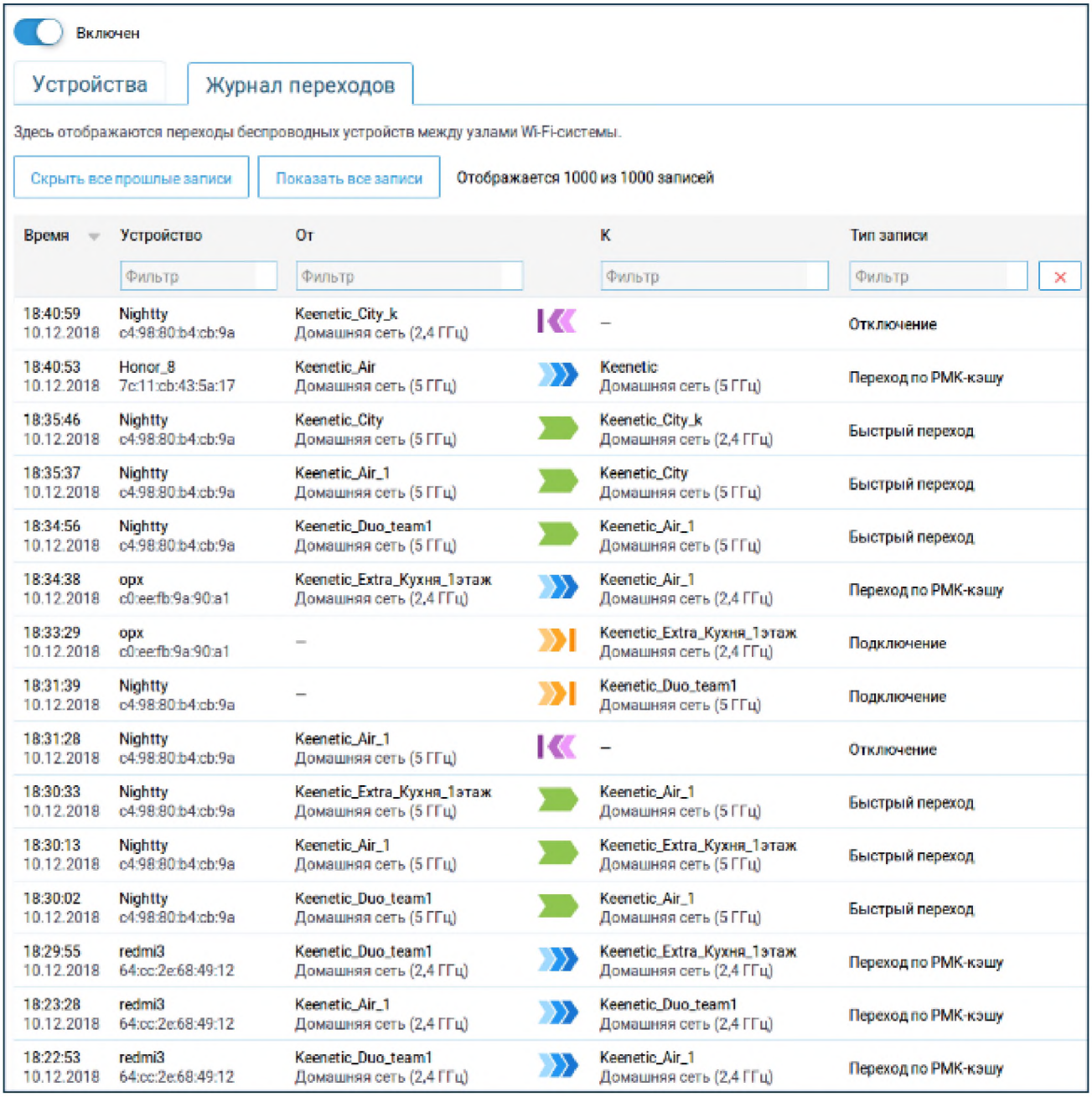


Рисунок 2.17 – Використання фільтрів для пошуку необхідних користувачів мережі

Якщо для підключення ретрансляторів використовується проміжний комутатор, то він повинен повністю прозоро пропускати трафік на рівні L2. При роботі Wi-Fi-системи використовується протокол STP, і якщо комутатор має підтримку MSTP / RSTP / STP, ці настройки потрібно відключити на портах, задіяних для Wi-Fi-системи. Для роботи гостьової мережі на ретрансляторах потрібна додаткова настройка Інтернет-центрів.

2.1.8 Особливості підключення інтернет-центру Keenetic Giga III та Keenetic Viva KN–1910

Інтернет-центр Keenetic Giga III, підключається до мережі Інтернет через встановлення компоненту серверу PPTP. У проєктуємій корпоративній мережі вихід в інтернет відбувається за допомогою Keenetic Giga 2 і Keenetic Viva. До VPN-сервера на Keenetic Giga 2 інтернет-центр автоматично встановлює з'єднання (в якості клієнта PPTP), що дозволяє користувачам в домашній мережі (доступ як безпосередньо на Keenetic (підключення до USB-накопичувачів і принтерів), так і до ресурсів, розташованим в його мережі комп'ютерів, серверів NAS [57, с. 65].

Для запуску програмного коду на налаштованому мережевому обладнанні Keenetic потрібно використовувати спеціальний інтерфейс.

Особливості налаштування Keenetic Giga III. У меню «Система → Користувач» встановлюють користувача, від імені якого буде виконуватися PPTP-підключення до сервера, права доступу-vpn.

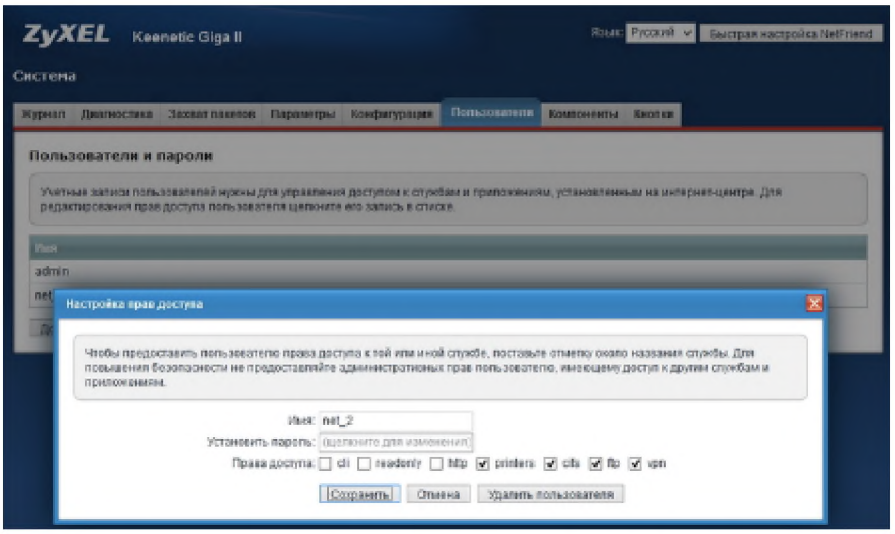


Рисунок 2.18 – Налаштування маршрутизатора Keenetic Giga III

При роботі пристрою в даній схемі не слід встановлювати від імені цього ж користувача підключення з інших розташувань (тобто обліковий запис з ім'ям net_2 буде використовуватися виключно для PPTP-підключень).

Потім в меню «програми > сервер VPN» потрібно включити прив'язку сервера до інтерфейсу «Мережа». Початковий IP-адрес пулу слід вибрати таким,

щоб не виникало перекриття з діапазонами IP-адрес робочих мереж. Рекомендується залишити в цьому полі значення за замовчуванням, а для клієнтського пристрою, що бере участь в схемі, вказати в списку користувачів статичну IP-адресу з цієї ж підмережі.

Рисунок 2.19 – Налаштування VPN для маршрутизатора Keenetic Giga III

Користувач net_2 буде при підключенні до VPN-сервера отримувати IP-адресу 172.205.1.2. Для настройки потрібно клацнути мишкою по потрібній облікового запису і в поле IP-адреса вказати адресу.

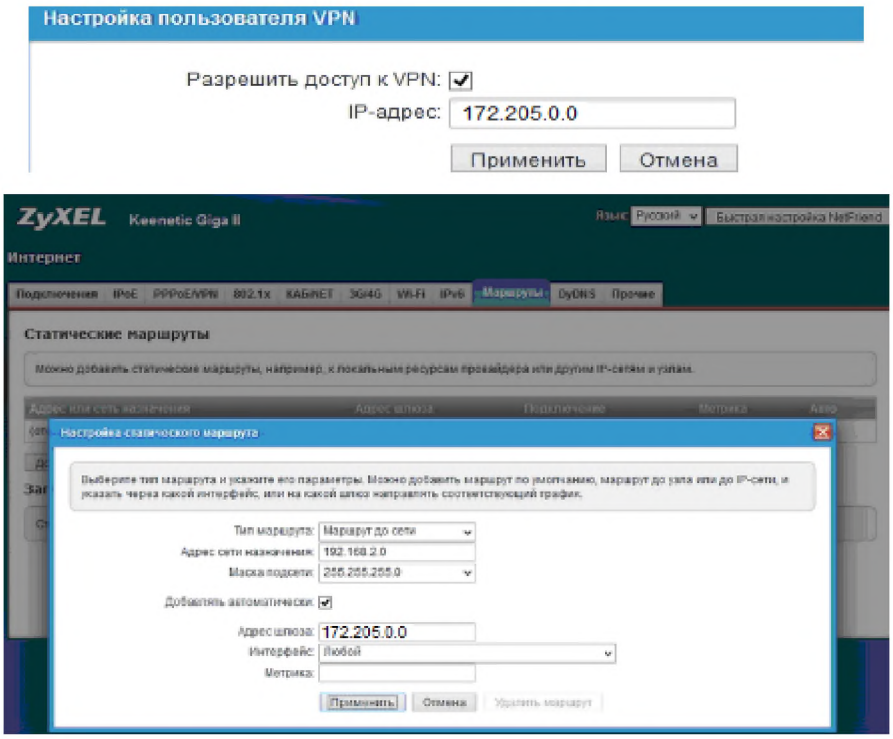


Рисунок 2.20 – Налаштування маршрутів Keenetic Giga III

Для того щоб клієнтам мережі офісу були доступні ресурси мережі Тпіо і сервісного центру, в меню Інтернет > маршрути потрібно створити статичний

маршрут, із зазначенням розташування мережі Тпіо і сервісного центру. Локальна мережа 192.168.2.0 / 255.255.255.0 стане доступна через IP-адресу, видану сервером підключився Клієнту (в нашому випадку це клієнт с ім'ям net_2 і з IP-адресою 172.205.0.0). При налаштуванні маршруту слід вказати опцію додавати автоматично і вибрати в полі інтерфейс будь-яке значення.

Проведемо аналіз порядку налаштування Keenetic Viva KN–1910. На цьому пристрої потрібно виконати дві основні налаштування.

1. Об'єднувані мережі мають різні адресні простори – 192.168.1.0 / 24 і 192.168.2.0 / 24 (маска 255.255.255.0) – мережа сервера і клієнта відповідно, оскільки в локальній мережі клієнта потрібно використовувати адресацію, відмінну від мережі сервера. Налаштувати параметри локальної адреси пристрою можна в меню «Мережа > параметри IP».

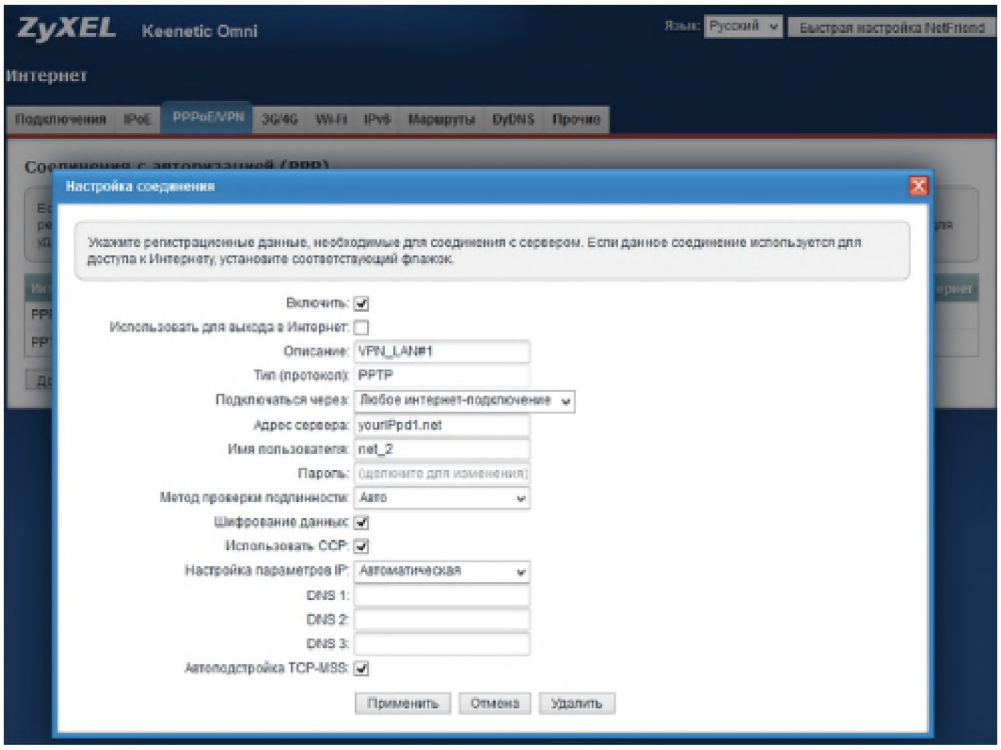


Рисунок 2.21 – Налаштування маршрутизатора *Keenetic Viva KN–1910*

2. Інтернет-центр Keenetic Viva KN–1910 буде працювати в якості PPTP-клієнта. Необхідне PPTP-підключення до VPN-сервера потрібно створювати в меню Інтернет > PPPoE / VPN.

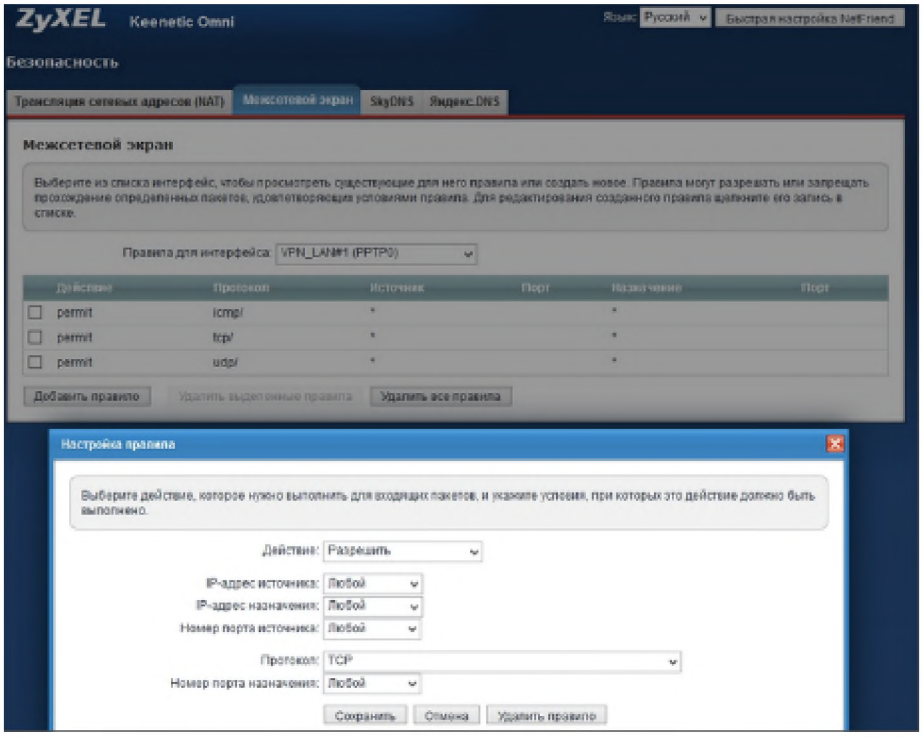


Рисунок 2.22 – Налаштування PPTP-підключення до VPN-сервера

На маршрутизаторі необхідно закрити доступ в Інтернет всім користувачам з бухгалтерії і декільком робочим станціям у відділі маркетингу в діапазоні адресів 172.205.1.3–72.205.1.8. Для цього виконуємо на маршрутизаторі наступні команди:

```
access-list extended INET deny 172.16.3.0 0.0.0.255 any
access-list extended INET deny host 172.16.1.3 0.0.0.255 any
access-list extended INET deny host 172.16.1.4 0.0.0.255 any
access-list extended INET deny host 172.16.1.5 0.0.0.255 any
access-list extended INET deny host 172.16.1.6 0.0.0.255 any
access-list extended INET deny host 172.16.1.7 0.0.0.255 any
access-list extended INET deny host 172.16.1.8 0.0.0.255 any
access-list extended INET allow ip any any
ip access-group INET out
```

Встановлюємо пароль на з’єднання. В результаті цих дій отримуємо такий набір команд:

```
Router>enable
Router#config terminal
Router (config)#hostname R0
Router (config)#ip domain-name some-dmn
Router (config)#crypto key generate rsa
Router (config)#line vty 0 4
Router (config-line)#transport input ssh
Router (config-line)#password secret password1
Команди для створення підінтерфейсів:
```

```
Router>enable
Router#configure terminal
Router (config)#int FastEthernet0 / 0
Router (config)#no shutdown
Router (config-if)#int fa0 / 0.10
Router (config-subif)#encapsulation dot1q 10
Router (config-if)#ip address 172.205.6.14 255.255.255.240
```

Список команд для налаштування інтерфейсу:

```
Switch>enable Switch#config terminal
Switch (config)#int fa3 / 1
Switch (config-if)#switchport mode trunk 58
Switch (config-if)#switchport trunk allowed vlan 10, 20, 30, 40, 50, 60, 100, 101
```

Зв'язок з центральним офісом здійснюватиметься через магістральний кабель, що матиме IP адресу у локальній мережі 0.0.0.0. На маршрутизаторі буде створений такий список доступу:

```
Router (config)#access-list 101 deny ip 172.18.6.0 0.0.0.15 0.0.0.0 0.0.0.0
Router (config)#access-list 101 deny ip 172.205.6.16 0.0.0.15 0.0.0.0 0.0.0.0
Router (config)#access-list 101 permit ip 172.205.6.32 0.0.0.7 0.0.0.0 0.0.0.0
Router (config)#access-list 101 deny ip 172.205.6.48 0.0.0.7 0.0.0.0 0.0.0.0
Router (config)#access-list 101 deny ip 172.205.6.56 0.0.0.7 0.0.0.0 0.0.0.0
Router (config)#access-list 101 deny ip 172.205.6.64 0.0.0.7 0.0.0.0 0.0.0.0
Router (config)#access-list 101 permit ip 172.205.6.72 0.0.0.7 0.0.0.0 0.0.0.0
Router (config)#access-list 101 deny ip 172.205.6.76 0.0.0.7 0.0.0.0 0.0.0.0
```

При налаштуванні з'єднання не потрібно встановлювати прапорець Використовувати для виходу в Інтернет, тоді клієнт отримає інформацію про локальну мережу офісу, розташованої за сервером, автоматично. Це позбавляє від необхідності налаштовувати статичну маршрутизацію. Вкажемо в поле Тип (протокол) значення PPTP, а в поле підключатися через можна залишити значення за замовчуванням. В поле Адреса сервера потрібно буде вказати публічну IP-адресу Інтернет-центру Keenetic Giga 3 [58, с. 405].

2.1.9 Забезпечення захищеності корпоративної системи

За способами здійснення всі заходи забезпечення безпеки комп'ютерних систем підрозділяють на: правові (діючі закони, укази та нормативні акти); морально-етичні (норми поведінки); організаційно-адміністративні (регламентація процесів функціонування інформаційних систем – ІС); апаратно-програмні [59, с. 6].

Для автоматизації завдання забезпечення безпеки корпоративної системи передбачається впровадження в систему захисту інформації компанії криптографічних систем. Криптографічні методи є найбільш ефективними засобами захисту корпоративної системи в автоматизованих системах. А при передачі інформації по протяжних лініях зв'язку вони є єдиним реальним засобом запобігання несанкціонованого доступу.

Метод шифрування з використанням датчика псевдовипадкових чисел найбільш часто використовується в програмній реалізації системи криптографічного захисту даних. Це пояснюється тим, що, він досить простий для програмування і дозволяє створювати алгоритми з дуже високою криптостійкістю. Крім того, ефективність даного метод шифрування досить високий. Системи, засновані на цьому методі, дозволяють зашифрувати в секунду від декількох десятків до сотень Кбайт даних.

Основною перевагою методу DES є те, що він – стандартний. Важливою характеристикою цього алгоритму є його гнучкість при реалізації та використанні в різних додатках обробки даних. Кожен блок даних шифрується незалежно від інших, тому можна здійснювати незалежну передачу блоків даних і довільний доступ до зашифрованих даних. Ні тимчасова, ні позиційна синхронізація для операцій шифрування не потрібна.

Алгоритм виробляє зашифровані дані, в яких кожен біт є функцією від всіх бітів відкритих даних і всіх бітів ключ. Різниця лише в одному Біті даних дає в результаті рівні ймовірності зміни для кожного біта зашифрованих даних. DES може бути реалізований апаратно і програмно, але базовий алгоритм все ж розрахований на реалізацію в електронних пристроях спеціального призначення.

Це властивість DES вигідно відрізняє його від методу шифрування з використанням датчика ПСЧ, оскільки більшість алгоритмів шифрування побудованих на основі датчиків ПСЧ не характеризуються всіма перевагами DES. Однак і DES володіє рядом недоліків. Найістотнішим недоліком des вважається малий розмір ключа. Стандарт в даний час не вважається невразливим, хоча і дуже важкий для розкриття (досі не були зареєстровані випадки несанкціонованої дешифрації). Ще один недолік DES полягає в тому, що однакові дані будуть однаково виглядати в зашифрованому тексті.

Оптимальним на даний момент для захисту інформації є метод RSA. Він є дуже перспективним, оскільки для зашифровування інформації не потрібно передачі ключа іншим користувачам. Але в даний час до цього методу відносяться з підозрілістю, оскільки не існує доказу, що немає іншого способу визначення секретного ключа за відомим, крім як визначення дільників цілих чисел [60, с. 7].

Традиційні vpn-рішення зазвичай концентруються переважно на захисті трафіку між двома віддаленими локальними мережами або між локальною мережею та віддаленими (або мобільними) користувачами.

Технологія ViPNet забезпечує створення безпосереднього і захищеного з'єднання «клієнт-клієнт». Також в усі компоненти ViPNet OFFICE інтегровані модулі IDS (intrusion detection system – система виявлення атак) і міжмережевий екран, тому ViPNet з рівним успіхом забезпечує захист трафіку як між віддаленими мережами, так і всередині локальної мережі. Ядром програмного забезпечення ViPNet є так званий ViPNet драйвер, основною функцією якого є фільтрація і шифрування / дешифрування вхідних і вихідних IP-пакетів. Кожен вихідний пакет обробляється драйвером відповідно до одним з наступних правил: переадресовується або відправляється у вихідному вигляді (без шифрування); шифрується і відправляється; шифрується і переадресується.

ViPNet драйвер працює між канальним рівнем і мережевим рівнем моделі OSI, що дозволяє здійснювати обробку IP-пакетів до того як вони будуть оброблені стеком протоколів TCP / IP і передані на прикладний рівень. Таким

чином, ViPNet драйвер захищає IP-трафік всіх додатків, не порушуючи звичний порядок роботи користувачів [62, с. 70].

Онлайн-сервіси пакету ViPNet OFFICE є такі функції:

– кільком ViPNet-клієнтам, що працюють в локальній мережі через ViPNet-координатор, використовувати одну зовнішню IP-адресу;
– тунелювати трафік від комп'ютерів локальної мережі, не оснащених програмним забезпеченням ViPNet, до інших об'єктів мережі VPN;
– перемаршрутизувати зашифрований трафік ViPNet-клієнтів на адресу їх координатора (проводиться підміна IP і MAC-адреси) і міжмережеві екрани (брандмауери, firewall) інших типів.

Щоб встановити ViPNet на проєктуєму корпоративну мережу потрібно:

– закрити всі відкриті програми;
– запустити програму установки ViPNet OFFICE. Буде запущений майстер «Установка ViPNet OFFICE», зображений на рис. 2.23;

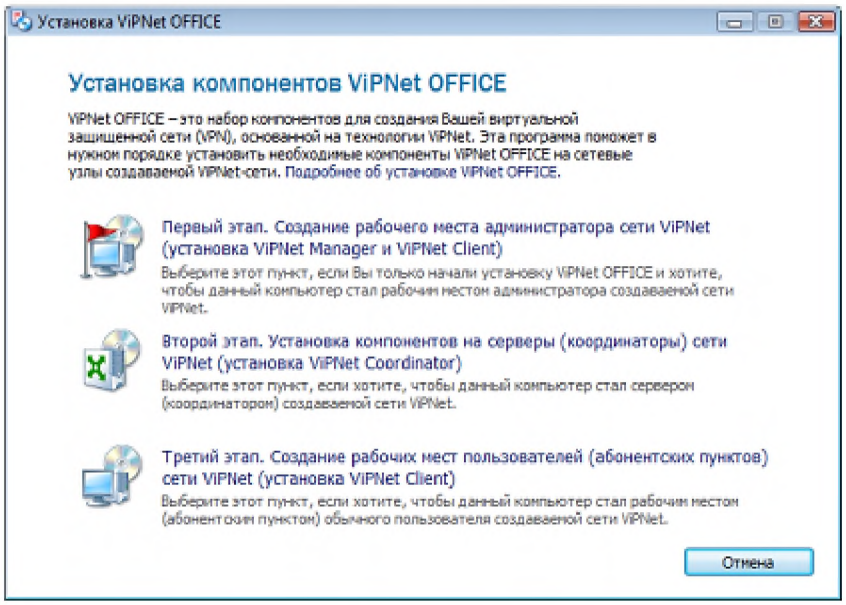


Рисунок 2.23 – Вибір компонентів для установки

– на сторінці «Установка компонентів ViPNet OFFICE» натискаємо посилання «Перший етап» «Створення робочого місця адміністратора мережі ViPNet» (установка ViPNet Manager і ViPNet Client);

– на сторінці створення робочого місця адміністратора мережі ViPNet (установка ViPNet Manager і ViPNet Client) натискаємо кнопку «Встановити ViPNet Manager». Буде запущений майстер «Установка ViPNet Manager», який зображено на Рисунок 2.24;

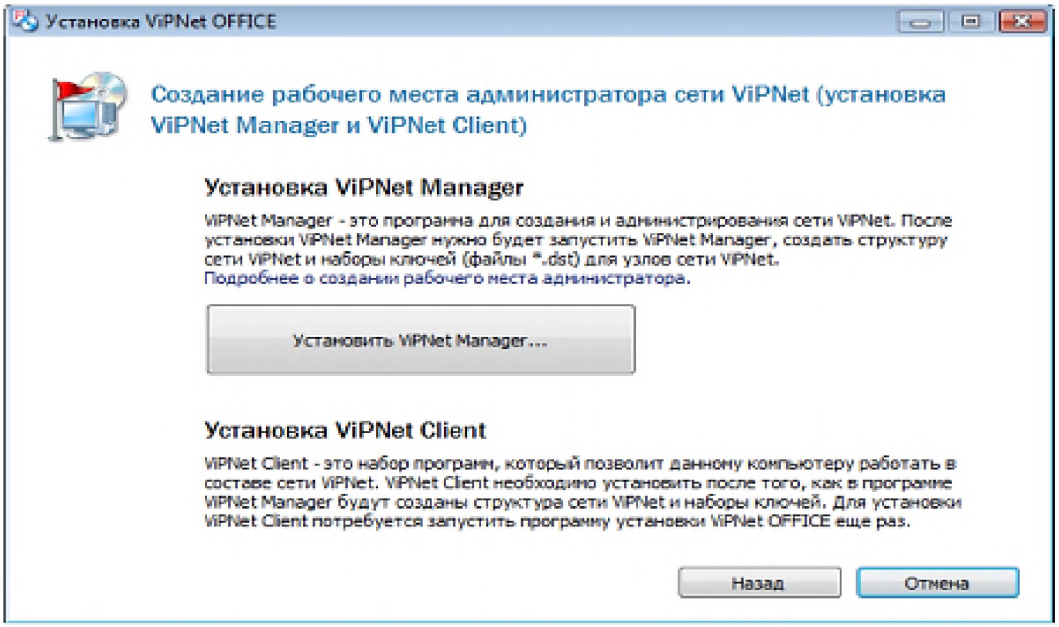


Рисунок 2.24 – Створення робочого місця адміністратора мережі ViPNet

– слідуємо інструкціям майстра. На сторінці «Ліцензійна угода» приймаємо угоду, інакше подальша установка ViPNet Manager буде неможливий;

– після закінчення установки з’явиться повідомлення про те, що установка успішно завершений. У вікні повідомлення натискаємо «ОК»;

– якщо потрібно перезавантажити комп’ютер, у вікні повідомлення про перезавантаження натискаємо «Перезавантажити зараз».

Опишемо порядок установки ViPNet Client на робочому місці адміністратора корпоративної системи. Для установки необхідно:

– закрити всі відкриті програми;

– запустити програму установки ViPNet OFFICE. Відкриється майстер «Установка ViPNet OFFICE» зображений на рис. 2.25.

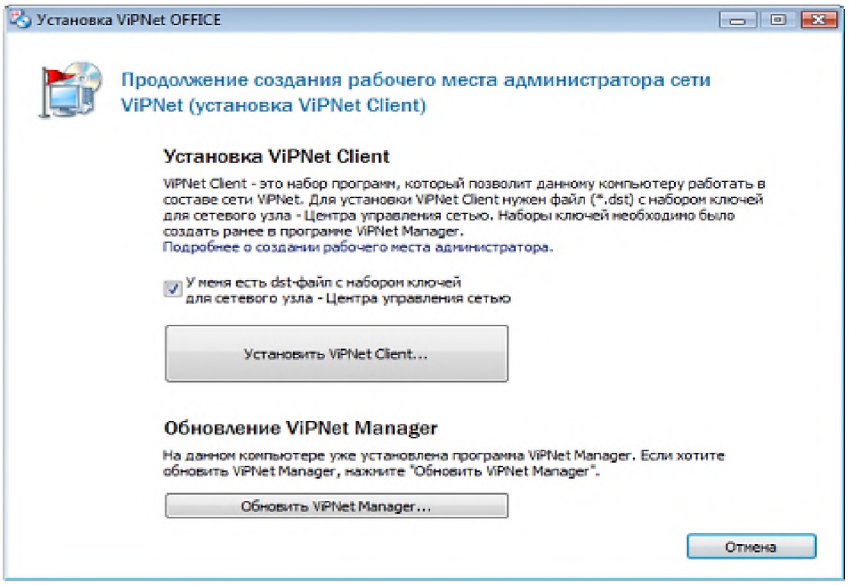


Рисунок 2.25 – Установка ViPNet Client на робочому місці адміністратора

– якщо раніше були створені Набори ключів для мережевих вузлів і є дистрибутив ключів для мережевого вузла-Центру управління мережею, встановлюємо прапорець «у мене є DST-файл з набором ключів для мережевого вузла-Центру управління мережею»;
– натискаємо кнопку «Встановити ViPNet Client», буде запущений майстер установка ViPNet Client;
– слідуємо інструкціям майстра. На сторінці «Ліцензійна угода» необхідно прийняти угоду, інакше подальша установка ViPNet Client буде неможлива;

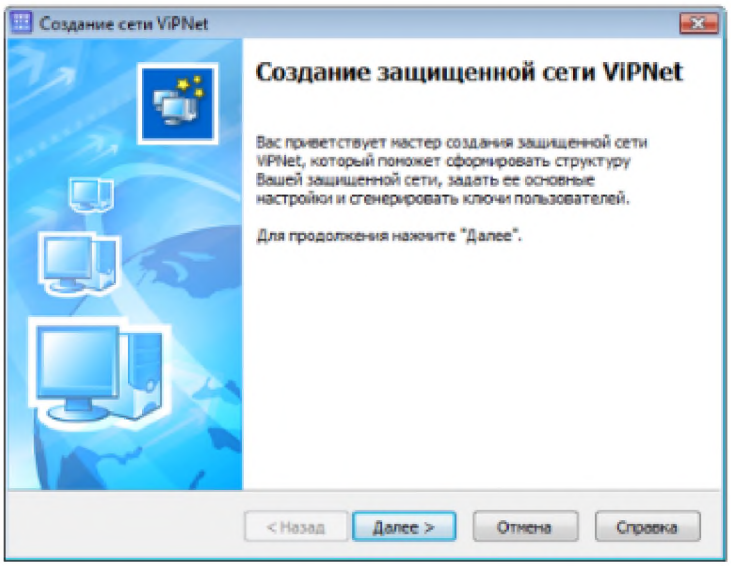


Рисунок 2.26 – Майстер захисту корпоративної системи ViPNet

– після закінчення установки програма видасть повідомлення, що установка успішно завершена. У вікні повідомлення натискаємо «ОК». Якщо буде потрібно перезавантажити комп'ютер, у вікні повідомлення про перезавантаження натискаємо «Перезавантажити пізніше»;
– відкриваємо папку, в якій знаходиться файл *.dst з набором ключів мережевого вузла-Центру управління мережею. Щоб встановити набір ключів, двічі клацаємо файл*.dst і слідуємо вказівкам майстра установки ключів;
– перезавантажуємо комп'ютер. Після перезавантаження робоче місце адміністратора буде готово до використання.

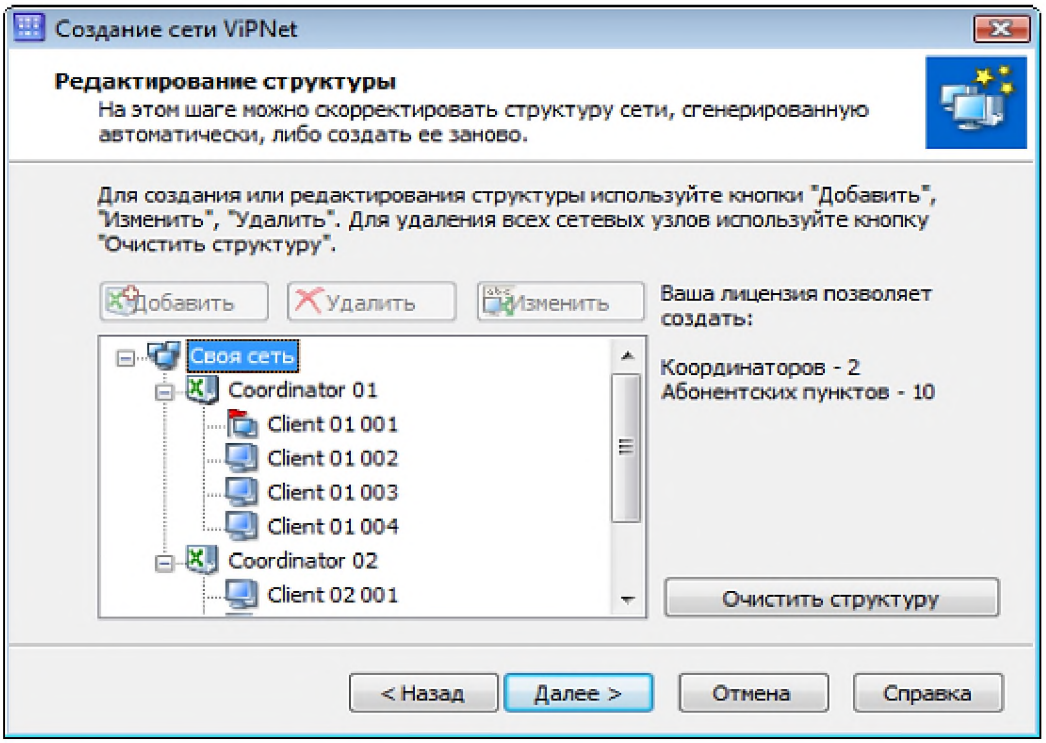


Рисунок 2.27 – Сторінка для редагування структури мережі

Програма ViPNet Client повинна бути встановлена на робочих місцях користувачів мережі ViPNet. Завдяки простоті установки, автоматичному визначення мережевих налаштувань, набору встановлених рівнів мережної безпеки і інтуїтивно зрозумілому інтерфейсу, з програмою ViPNet Client легко можуть працювати навіть недосвідчені користувачі.

ViPNet Client включає в себе:

- sнтегрований персональний мережевий екран з функціями виявлення атак (IDS) і контролю мережевої активності додатків;
- TCP / IP шифратор;
- ряд корисних захищених комунікаційних додатків.

Одна з найважливіших функцій по ViPNet Client – ефективний контроль Іртрафіка під час завантаження операційної системи (ОС). Цей контроль здійснюється завдяки безпосередній взаємодії між ViPNet. Драйверами та драйверами мережевих адаптерів. В ОС Windows для ініціалізації завантаження комп'ютера використовує тільки одна служба. Ініціалізація ViPNet Драйвера і ключів шифрування ViPNet виконується перед входом користувача у Windows, тобто до ініціалізації інших служб і драйверів операційної системи.

При перегляді інтернет-ресурсів ViPNet Client забезпечує [61, с. 10]:

- блокування найбільш поширених банерів, реклами, спливаючих вікон, які можуть відволікати користувача і приводити до збільшенню інтернет-трафіку. Список блокованих банерів може бути розширений;
- блокування різних інтерактивних елементів (ActiveX, Java додатків, Flash-анімації, сценаріїв JavaScript і VBScript), які можуть виконувати несанкціоновані користувачем дії;
- захист від несанкціонованого збору інформації про дії користувача в Інтернеті (шляхом блокування Cookie і Referer).

2.1.10 Розробка програмного засобу захисту корпоративної інформаційної системи

Розробимо програмний код, який демонструє, як можна використовувати JavaScript для налаштування захисту транспортування даних у мережі з використанням функції ACL, NAT і PAT на мережевому обладнанні Keenetic:

```
// налаштування ACL
function configureACL() {
// Підключення до мережевого пристрою Keenetic
const keenetic = connectToKeenetic();

// Налаштування правил ACL
keenetic. configureACL({
```

```
sourceIP: '192.168.0.0 / 24',
destinationIP: '10.0.0.0 / 24',
protocol: 'tcp',
action: 'allow',
});

// Збереження налаштувань
keenetic. saveConfiguration();
}

// Налаштування NAT
function configureNAT() {
// Підключення до мережевого пристрою Keenetic
const keenetic = connectToKeenetic();

// Налаштування правил NAT
keenetic. configureNAT({
internalIP: '192.168.0.100',
externalIP: '1.2.3.4',
});

// Збереження налаштувань
keenetic. saveConfiguration();
}

// Нналаштування PAT
function configurePAT() {
// Підключення до мережевого пристрою Keenetic
const keenetic = connectToKeenetic();

// Налаштування правил PAT
keenetic. configurePAT({
internalIP: '192.168.0.100',
internalPort: 8080,
externalPort: 80,
});

// Збереження налаштувань
keenetic. saveConfiguration();
}

// Виклик функцій для налаштування захисту
configureACL();
configureNAT();
configurePAT();
```

Наведемо опис кожної функції з коду на JavaScript:

1. *`configureACL()`*: Ця функція відповідає за налаштування правил ACL (Списку керування доступом). Вона викликає функцію `connectToKeenetic()`, яка встановлює з’єднання з обладнанням Keenetic. Потім вона викликає метод

`configureACL()` об'єкта `keenetic`, щоб налаштувати правила ACL, такі як діапазони IP-адрес, протоколи та дії (дозволити або заборонити).

2 *`configureNAT()`*: Ця функція відповідає за налаштування правил NAT (Network Address Translation). Вона також викликає функцію `connectToKeenetic()` для підключення до обладнання Keenetic. Потім вона викликає метод `configureNAT()` об'єкта `keenetic`, щоб налаштувати правила NAT, вказавши внутрішню IP-адресу та зовнішню IP-адресу для перетворення адрес.

3 *`configurePAT()`*: Ця функція відповідає за налаштування правил PAT (Port Address Translation). Вона також викликає функцію `connectToKeenetic()` для підключення до обладнання Keenetic. Потім вона викликає метод `configurePAT()` об'єкта `keenetic`, щоб налаштувати правила PAT, вказавши внутрішню IP-адресу, внутрішній порт та зовнішній порт для перетворення адрес.

4 *`connectToKeenetic()`*: Ця функція відповідає за підключення до обладнання Keenetic. У цьому прикладі вона може бути функцією, яка створює з'єднання з обладнанням Keenetic і повертає об'єкт `keenetic`, який представляє підключення до пристрою.

5 *`keenetic. configureACL()`*: Цей метод викликається на об'єкті `keenetic` і використовується для налаштування правил ACL на пристрої Keenetic. Він отримує параметри, такі як діапазони IP-адрес, протоколи та дії, і встановлює відповідні налаштування на пристрої.

6 *`keenetic. configureNAT()`*: Цей метод викликається на об'єкті `keenetic` і використовується для налаштування правил NAT на пристрої Keenetic. Він отримує параметри, такі як внутрішню IP-адресу та зовнішню IP-адресу, і встановлює відповідні налаштування на пристрої.

7 *`keenetic. configurePAT()`*: Цей метод викликається на об'єкті `keenetic` і використовується для налаштування правил PAT на пристрої Keenetic. Він отримує параметри, такі як внутрішню IP-адресу, внутрішній порт та зовнішній порт, і встановлює відповідні налаштування на пристрої.

8 *`keenetic. saveConfiguration()`*: Цей метод викликається на об'єкті `keenetic` і використовується для збереження налаштувань на пристрої Keenetic

після внесення змін. Він забезпечує збереження налаштувань, щоб вони були активними після перезавантаження або відновлення пристрою.

2.2 Висновки

Отже, у підсумок цього розділу можна сказати, що для підприємства «Ziber», де працює небагато людей, які використовують мобільні пристрої та ноутбуки, вистачить інформаційно-комунікаційної системи, базованної на мережі Wi-Fi, для організації якої вистачить сучасний Wi-Fi роутер та пристрій-комутатор для з'єднання всіх комп'ютерів в мережі. Для її розробки ми повинні вивчити техніку, яку використовують співробітники. Враховуючи потреби співробітників, була обрана топологія – «зірка» черещ свої переваги, а саме висока продуктивність та легкий пошук несправностей і обривів мережі.

В якості операційних систем була вибрана Windows Server 2012 R2 Standard для серверної частини та Microsoft Windows 10 Enterprice для робочих станцій.

Enterprice – це версія Windows 10, яка орієнтована на підприємства з власними серверами завдяки двум аспектам. В неї вбудовані спеціальні служби для покращення внутрішньомережевої роботи та вона продається за передоплатою. Унікальними службами версії Enterprise є: BranchCache – інструмент прискорення оновлення, коли кожен комп'ютер в локальній мережі виступає в якості «Сіда». Також він прискорює передачу файлів, якщо вони зберігаються більш ніж на одній «машині»; Device Guard – програмно-апаратний набір технологій, спрямований на підвищення захисту комп'ютера. Контролює цілісність коду, процес завантаження, роботу з оперативною пам'яттю.

Також у розділі підбирається та описується обладнання для комунікаційної системи, мобільної станції для відряджень та стаціонарних робочих станцій для кожного з співробітників.

Для офісу був обраний роутер Інтернет-центр Keenetic Giga II, який обладнаний міжмережевим екраном для захисту мережі від Інтернет-атаки, 2-портовим хостом USB, який розширює можливості для підключення, а також дозволяє включити окрему мережу Wi-Fi, призначену для виходу в Інтернет без доступу до інформації в мережі.

Для філій і сервісного центру обрані Інтернет центри Keenetic Giga та Viva. Ці пристрої мають ті ж самі функції, що і Keenetic Giga II, але володіють меншим радіусом дії Wi-Fi. На роботу філій це не позначиться, оскільки площа приміщень по перевищує 20 м, проте дозволить скоротити витрати на покупку мережевого та Інтернет обладнання.

Окремо розглянуті такі маршрутизатори як Keenetic Ultra KN–1810, Keenetic Giga III та Keenetic Viva KN–1910 як можливі варіанти, а далі у розділі йде їх порівняння, яке показує, що модель Viva дешевша і слабкіша, а також має обмеження у вигляді USB 2.0, але менша у габаритах та майже вдвічі легша.

Забезпечення захищеності корпоративної системи. Описані та порівняні такі методи як криптографічний, метод шифрування з використанням датчика псевдовипадкових чисел, DES, RSA, VPN та ViPNet. Після цього розробили програмний код, який демонструє, як можна використовувати JavaScript для налаштування захисту транспортування даних у мережі з використанням функції ACL, NAT і PAT на мережевому обладнанні Keenetic

РОЗДІЛ 3. ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ЗАПРОПОНОВАНИХ РІШЕНЬ

Для розробки інформаційно-комунікаційної системи підприємства «Ziber» задіяно дві людини: керівник проекту і виконавець. Керівник проекту формує завдання проекту (комплекс робіт), план виконання цих завдань, здійснює управління проектом розробки ПЗ, проводить необхідні консультації. Виконавець здійснює проектування архітектури інформаційно-комунікаційної системи, ПЗ, програмну реалізацію алгоритмів, розробку бази даних, розробку інтерфейсу, тестування програми та інші дії згідно з планом проекту. Вибір комплексу робіт щодо розробці проекту проводиться відповідно до стандарту ISO / IEC12207: 2008 «System and software engineering – Software life cycle processes», який встановлює стадії розробки програмних продуктів.

Проведемо розрахунок економічного ефекту проектованої інформаційно-комунікаційної системи підприємства «Ziber». Затрати на покупні вироби й напівфабрикати визначається аналогічно витратам на матеріали. Дані для розрахунків і результати зведені в таблицю 3.1.

Таблиця 3.1 – Затрати на покупні вироби та витратні матеріали для створення локальної мережі підприємства

Найменування	Кількість	Ціна, грн.	Сума, грн.
Сервер ProLiant ML150G9 834607–421			200000
Ноутбук HP Pavilion x360 13-u002ur			20000
Комп'ютер HP ProDesk 400 G2 K8K74EA			39000
Стійка монтування 19»	1	20000	15000
Кабель силовий	50 м	10	500
Провід 5Е	500 м		10000
Штекери RJ – 45	1000 шт	500	500
Програмне забезпечення			15000
Сума			300000
Транспортно-торгівельні затрати 5%			15000
Усього			315000

Проведемо розрахунок основної заробітної плати. Витрати за цією статтею розраховуються по кожному виду робіт залежно від норми часу й погодинної тарифної ставки робітників.

$$C_{З.О.} = \sum_{i=1}^{n} C_{Т_i} t_{Ш_i} \quad , \qquad (3.1)$$

де $C_{Ті.}$ – погодинна тарифна ставка, грн;

$t_{Ші}$ – норма годин на одну операцію.

Перелік робіт відповідає технологічному процесу складання виробу. Норми часу для монтажних і складальних робіт визначаються типовими нормами часу на складально-монтажні роботи, таблиця 3.2.

Таблиця 3.2 - Основна заробітна плата

	Назва робіт	Тариф. розряд	Годинна тарифна ставка, грн/год	Норма часу, ч	Сума зарплати, грн.
1	Підготовка	3	260	3	780
3	Монтажні	4	280	6	1680
4	Складальні	5	320	4	1280
Сума					3740
Доплати й надбавки (20% – 60%)					1870
Усього					5610

Додаткова зарплата робітників. Витрати за цією статтею визначаються у відсотках від основної заробітної плати. За орієнтовну величину можна прийняти норматив додаткової заробітної плати для приладобудівних підприємств у розмірі 30–40%.

$$С_{з.\ дод.} = 0{,}30 \cdot 5610 = 1683 \text{ грн.}$$

де $С_{з.\ о.}$ – основна заробітна плата.

Відповідно, повна зарплата буде дорівнювати:

$$С_{з.\ пов} = 5610 + 1683 = 7293 \text{ грн.}$$

Нарахування на заробітну плату. Норму нарахування на зарплату визначають за сумою основної й додаткової зарплат. Це нарахування в пенсійний фонд, фонд соціального страхування, фонд страхування на випадок безробіття й фонд страхування від нещасного випадку на виробництві (37,8%).

$$С_{с.\ с.} = 0{,}378 \cdot 7293 = 2757 \text{ грн.}$$

Загальновиробничі витрати. З огляду на те, що собівартість локальної мережі підприємства визначається на ранніх стадіях її проектування в умовах обмеженої інформації щодо технології виробництва і витрат на її підготовку, в загальновиробничі витрати включаються, крім власне цих витрат, витрати на:

освоєння основного виробництва, відшкодування зносу спеціальних інструментів і приладів цільового призначення, підтримку й експлуатацію устаткування. При цьому загальновиробничі витрати визначаються у відсотках до основної заробітної плати. При такому комплексному складі загальновиробничих витрат їхній норматив досягає 200–300%.

$$C_{з.\,в.} = (2...\,3) \cdot C_{з.\,про}\,, \qquad (3.2)$$

$$C_{з.\,в.} = 2 \cdot 5610 = 11220 \text{ грн.}$$

Адміністративні витрати. Ці витрати відносяться до собівартості мережі підприємства пропорційно основній заробітній платі і на приладобудівних підприємствах складають 100–200%:

$$C_{з.\,г} = 1 \cdot C_{з.\,об}\,, \qquad (3.3)$$

$$C_{з.\,г} = 1 \cdot 5610 = 5610 \text{ грн.}$$

Витрати на збут. Витрати по цій статті визначаються у відсотках до виробничої собівартості (звичайно 2, 5–5,0%).

$$C_{збуд.} = 0{,}04 \cdot 51794 = 1295.$$

Розрахунок повною собівартістю інформаційно-комунікаційної системи представлений у таблиці 3.3.

Таблиця 3.3 – Калькуляція собівартості інформаційно-комунікаційної системи

Витрати	Сума, грн
Сировина й матеріали + покупні вироби	315000
Основна заробітна плата	5610
Додаткова зарплата (30%)	1683
Нарахування на заробітну плату (37,8%)	2757
Витрати на збут (2,5%)	1295
Повна собівартість	326345

У таблиці представлені різні види витрат, які враховуються при розрахунку собівартості інформаційно-комунікаційної системи. Сировина й матеріали, включаючи покупні вироби, складають 315000 грн. Основна заробітна плата становить 5610 грн, додаткова зарплата (30%) – 1683 грн, нарахування на заробітну плату (37,8%) – 2757 грн, витрати на збут (2,5%) – 1295 грн. Загальна сума собівартості становить 326345 грн.

Проведемо розрахунок витрат на експлуатацію виробу.

Вартість електроенергії.

$C_{ел.}$ = Рспож. / 10000 · (24 · 365) · 0,27 (грн) = 0,05 · 8760 · 0,27 = 1180 грн.

Таблиця 3.4 - Річні експлуатаційні витрати користувача

Статті експлуатаційних витрат	Річні експлуатаційні витрати
Вартість електроенергії, грн.	1180
Витрати на обслуговування пристрою, грн.	100
Амортизаційні відрахування, грн.	650
Витрати на поточний ремонт, грн.	920
Всього	2850

Ця таблиця відображає річні експлуатаційні витрати користувача в розрізі окремих показників. Вартість електроенергії складає 1180 грн, витрати на обслуговування пристрою – 100 грн, амортизаційні відрахування – 650 грн, витрати на поточний ремонт – 920 грн. Загальні витрати складають 2850 грн.

ВИСНОВКИ

Отже, в роботі розкрито основні можливості корпоративних інформаційно-комунікаційних систем та описано процес створення таких корпоративних інформаційних систем. Корпоративна комунікаційна система об'єднує філії підприємства створюючи спільний інформаційний корпоративний простір. З цієї точки зору корпоративна комунікаційна система відображає структуру установи.

Проаналізовано особливості віртуальної мережі передачі даних та названо технології, що використовуються в корпоративних інформаційно-комунікаційних системах. Наголошено, що основна мета проєктування корпоративних інформаційно-комунікаційних систем полягає в тому, щоб визначити структуру, склад апаратно-програмних засобів та організацію корпоративної комунікаційної системи.

Перелічено основні принципи захисту інформації при підключенні до мережі Інтернет. Встановлено, що при побудові захисту варто виходити з того, що будь-який захист ускладнює використання корпоративної комунікаційної системи, що за прямим призначенням обмежує функціональні можливості, споживає обчислювальні й трудові ресурси, вимагає фінансових витрат на створення та експлуатацію. Чим вище захист, тим дорожчою у побудові та обслуговуванні стає система і тим менш зручною для безпосередніх користувачів. Тому, захищаючи корпоративну мережу, варто виходити з доцільної вартості захисту. Тобто витрати на захист повинні бути пропорційні цінності ресурсу, що захищається.

Окремо розглянуто особливості захисту інформації такими способами, як NAT-перетворення, PAT, ACL, демілітаризована зона, антивірусний захист КМ та захист інформації за допомогою міжмережних екранів. Дано їх обмеження та області застосування.

В практичній частині роботи розкриті основні етапи проєктування комп'ютерної мережі на базі обладнання Keenetic. Дано характеристику необхідного обладнання та розглянуто способи його компонування для створення

програмного засобу захисту транспортування даних у мережі з використанням функції ACL та протоколів NAT і PAT.

Зроблено розрахунок необхідної кількості комп'ютерного устаткування корпоративної комунікаційної системи, зроблено вибір серверного обладнання та комутаційного обладнання корпоративної комунікаційної системи (Keenetic Ultra, Giga, Viva і т.д.).

Розроблено програмний код, який демонструє, як можна використовувати JavaScript для налаштування захисту транспортування даних у мережі з використанням функції ACL, NAT і PAT на мережевому обладнанні Keenetic. Наведено опис кожної функції з коду на JavaScript. Для запуску програмного коду на налаштованому мережевому обладнанні Keenetic потрібно використовувати спеціальний інтерфейс.

Інтернет-центр Keenetic Giga III, підключається до мережі Інтернет через встановлення компоненту серверу PPTP. У проєктуємій корпоративній мережі вихід в інтернет відбувається за допомогою Keenetic Giga 2 і Keenetic Viva. До VPN-сервера на Keenetic Giga 2 інтернет-центр автоматично встановлює з'єднання (в якості клієнта PPTP), що дозволяє користувачам в домашній мережі (доступ як безпосередньо на Keenetic (підключення до USB-накопичувачів і принтерів), так і до ресурсів, розташованим в його мережі комп'ютерів, серверів NAS.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абдуллазаде Ф. З. Побудова IP-мережі на базі обладнання Cisco / Ф. З. Абдуллазаде; наук. кер. Л. Р. Чупахіна. Київ: Комп'ютер юніті, 2019. 73 с.
2. Азаров О. Д. Комп'ютерні мережі: навчальний посібник / О. Д. Азаров, С. М. Захарченко, О. В. Кадук. Вінниця: Вінницький Національний Технічний Університет, 2013. 371 с.
3. Альтман Е. А. Проєктування корпоративної комунікаційної системи [Текст] / Е. А. Альтман, А. Г. Малютин. Донецк: 2014. 22 с.
4. Альтман Е. А. Комп'ютерні мережі на базі обладнання компанії Cisco [Текст] / Е. А. Альтман. Донецк: 2013. 32 с.
5. Бабаш А. В. Інформаційна безпека. Лабораторний практикум: підручник / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. Київ: КноРус, 2013. 136 с.
6. Біячуєв Т. А. Безпека корпоративних інформаційно-комунікаційних систем / Т. А. Біячуєв. М.: 2014. 481 с.
7. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В. Л. Бурячок, Г. М. Гулак. Киев: ДУТ, 2015. 449 с.
8. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов. Киев: КУБГ, 2019. 218 с.
9. Волков І. О. Економіка підприємства: підручник / І. О. Волков. Київ: ИНФРАМ, 2015. 416 с.
10. Бєлов П. В. Організація захисту мережі від мережевих загроз [Текст] / П. В. Бєлов; наук. кер. А. Ю. Криштофович. Київ: Комп'ютер юніті, 2019. 99 с.
11. Виханов Д. А. Організація захисту корпоративної комунікаційної системи підприємства / Д. А. Виханов; науч. рука. А. Ю. Криштофович. Київ: Комп'ютер юніті, 2019. 81 с.
12. Гатчин Ю. А. Теорія інформаційної безпеки та методологія захисту інформації / Ю. А. Гатчин. Донецк, 2010. 98 с.
13. Гафнер В. В. Інформаційна безпека: підручник / В. В. Гафнер. Рн. Донецьк: Феникс, 2010. 324 с.

14. Гілленберг О. С. Розробка системи аналізу та підвищення захищеності корпоративної комунікаційної системи / О. С. Гілленберг. Київ: Комп'ютер юніті, 2019. 82 с.
15. Громов Ю. Ю. Інформаційна безпека та захист інформації: підручник / Ю. Ю. Громов. Київ: ТНТ, 2010. 384 с.
16. Дятибратов А. П.; Гудино, Л. П.; Кириченко, А. А. Обчислювальні системи, мережі та телекомунікації. Фінанси і статистика. Київ, 2013. 512 с.
17. Зав'ялов А. В. Моделювання мереж пакетної комутації на основі обладнання Cisco / А. В. Зав'ялов. Київ: Комп'ютер юніті, 2018. 48 с.
18. Зегжда Д. П. Основи безпеки інформаційних систем / Д. П. Зегжда, А. М. Івашко. Київ: Гаряча лінія – телеком, 2009. 452 с.
19. Ідіятулліна А. С. Застосування критеріїв згоди при аналізі мережевого трафіку / А. С. Ідіятулліна. Київ: Комп'ютер юніті, 2018. 94 с.
20. Комп'ютерні мережі. Навчальний курс: Офіційний посібник Microsoft із самостійного темпу навчання: [пер. з англ.] [Текст] – 5-е вид. Корпорація Майкорософт. Київ, 2015. 410 с.
21. Корнєв В. А. Проєктування захищеності фрагмента корпоративної комунікаційної системи Ethernet / В. А. Корнєв. Київ: Комп'ютер юніті, 2019. 73 с.
22. Кравець С. В. Розробка методу захисту корпоративної комунікаційної системи від використання користувачем глобальних ресурсів не за призначенням. Вінниця: ВНТУ, 2014. 80 с.
23. Кузін А. В. Комп'ютерні мережі / А. В. Кузін. Київ: 2015. 256 с.
24. Кузьменко Н. Г. Комп'ютерні мережі та мережеві технології / Н. Г. Кузьменко. Київ: Наука і техніка, 2013. 368 с.
25. Кульгин М. В. Корпоративні мережеві технології [Текст] / М. В. Кульгин. СПб.: «Питер», 2009. 704 с.
26. Кульгин М. Технологія корпоративних інформаційно-комунікаційних систем / М. Кульгин. Київ: Мережі, 2014. 541 с.

27. Куроуз Д. Комп'ютерні мережі. Спадний підхід / Д. Куроуз, К. Росс. Київ: Освіта, 2016. 912 с.
28. Курушин В. Д. Комп'ютерна злочинність та інформаційна безпека / В. Д. Курушин. Київ: Новий юрист, 2012. 256 с.
29. Малюк А. А. Впровадження в інформаційну безпеку в автоматизованих системах / А. А. Малюк, С. В. Пазинин. Київ: Освіта. 2001. 148 с.
30. Нугман М. Розробка методики аналізу трафіку локальної обчислювальної мережі / М. Нугман; науч. рука. В. Г. Карташевський. Київ: Освіта, 2018. 70с.
31. Оліфер В. Г. Стратегічне планування загальнокорпоративних інформаційно-комунікаційних систем [Текст] / В. Г. Оліфер, Н. А. Оліфер и др. 3-е вид. Київ: Освіта. 2010. 680 с.
32. Оліфер В. Г. Комп'ютерні мережі: принципи, технології, протоколи [Текст] / В. Г. Оліфер, Н. А. Оліфер и др. 4-е изд., Київ: Освіта, 2012. 958 с.
33. Оліфер В. Г. Нові технології та обладнання IP-мереж [Текст] / В. Г. Оліфер, Н. А. Оліфер. Київ: Освіта, 2012. 512 с.
34. Оліфер В. Г. Мережеві операційні системи / В. Г. Оліфер. Київ: Освіта, 2016. 544 с.
35. Основи комп'ютерних мереж / Б. Д. Виснадул, С. А. Лупин. С. В. Сидоров, П. Ю. Чумаченко / Під ред. Л. Г. Гагаріної. Київ: Програміст. 2007. 272 с.
36. Палмер М. Проєктування та впровадження комп'ютерних мереж / М. Палмер, Р. Б. Синклер. Київ: Програміст, 2004. 752 с.
37. Панфілов К. В. Аналіз систем моніторингу мережевого обладнання мережі передачі даних / К. В. Панфілов. Київ: Комп'ютер юніті, 2019. 96 с.
38. Прончев Г. Б. Комп'ютерні комунікації. Найпростіші обчислювальні мережі: Навчальний посібник / Г. Б. Прончев. Київ: Програміст, 2009. 64 с.
39. Редько В. Н.; Басараб, І. А. Бази даних та інформаційні системи; Знання, 2013. 150 с.
40. Ретана А. Принципи проєктування корпоративної IP-мережі [Текст] / А. Ретана, Д. Слайс, Р. Уайт, пер. з анг. Київ: Освіта, 2012. 368 с.

41. Романчук В. І. Дослідження імовірнісних властивостей трафіку корпоративної мультисервісної мережі / В. І. Романчук, О. А. Лаврів, В. В. Червенець, Р. І. Бак. Радіоелектроніка та телекомунікації. Львів: Видавництво Львівської політехніки, 2011. С. 128–134.
42. Севастьянов Е. Н. Проєктування захищених мереж зв'язку / Е. Н. Севастьянов. Київ: Комп'ютер юніті, 2019. 71 с.
43. Семенов А. Б. Проєктування та розрахунок структурованих кабельних систем та їх компонентів [Текст] / А. Б. Семенов. Київ: Освіта, 2014. 416 с.
44. Семенов А. Б. Структуровані кабельні системи [Текст] / А. Б. Семенов та ін. вид. 3-е перероб. і доп. Київ: Освіта, 2013. 607 с.
45. Семенов А. Б. Волоконна оптика в локальних і корпоративних інформаційно-комунікаційних системах / А. Б. Семенов. Київ: Програміст, 2016. 327 с.
46. Семенов А. Б. Структуровані кабельні системи Айті-СКС. / А. Б. Семенов. Київ: Програміст, 2014. 269 с.
47. Семенов М. І. Автоматизовані інформаційні технології в економіці: Підручник / М. І. Семенов. Донецьк: Фінанси і статистика, 2014. 476 с.
48. Соколов А. В. Захист від комп'ютерного тероризму / А. В. Соколов. СБП.: 2015. 380 с.
49. Таненбаум Е. Комп'ютерні мережі. 5-е видання. / Е. Таненбаум. Донецьк: Свічадо, 2012. 992 с.
50. Тарахнов І. Г. Проєктування і побудова бюджетної структурованої комп'ютерної мережі / І. Г. Тарахнов; наук. кер. І. В. Ротенштейн. Київ: Комп'ютер юніті, 2018. 84 с.
51. Титаренко Г. А. Автоматизовані інформаційні технології в економіці: Підручник / Г. А. Титаренко. Київ: Комп'ютер юніті, 2013. 400 с.
52. Шиндер Л. Д. Основи комп'ютерних мереж / Л. Д. Шиндер. Київ: Комп'ютер юніті: 2015. 152 с.
53. Федотов Е. Д. Аналіз характеристик сенсорних мереж / Е. Д. Федотов; наук. кер. Б. Я. Ліхтциндер. Донецьк: Свічадо, 2019. 135 с.

54. Філімонов А. Ю. Побудова мультисервісних мереж Ethernet: підручник [Текст] / А. Ю. Філімонов. Київ: Програміст, 2015. 248 с.
55. Фурашев В. М. Інформаційні операції крізь призму системи моніторингу та інтеграції Інтернет-ресурсів / В. М. Фурашев, Д. В. Ланде. *Правова інформатика.* 2009. № 2 (22). С. 49–57.
56. Хоменко В. Г., Павленко М. П. Комп'ютерні мережі: Навчальний посібник / В. Г. Хоменко, М. П. Павленко. Донецьк: ЛАНДОН-ХХІ, 2011. 316 с.
57. Шаньгін В. Захист інформації в комп'ютерних системах та мережах / Шаньгін Донецьк: Свічадо, 2013. С. 65.
58. Експлуатація об'єктів мережевої інфраструктури: підручник для школярів. [Текст] / А. В. Назаров, В. П. Мельников; під кер. А. В. Назарова. Київ: Освіта, 2014. 538 с.
59. Sukhov A. M. Active flows in diagnostic of troubleshooting on backbone links [Text] / A. A. Galtsev, A. M. Sukhov // Journal of High Speed Networks. 2011. Vol. 18. №. 1. P. 69–81.
60. Бездротова точка доступу. URL: https: // uk. wikipedia. org / wiki / Бездротова точка доступу. (дата звернення: 10.06.2023).
61. Keenetic – Центр підтримки URL: https: // help. keenetic. net / (дата звернення: 10.06.2023).

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Зміст	2	
3	А4	Вступ	4	
4	А4	Стан питання. Постановка задачі	39	
5	А4	Спеціальна частина	42	
6	А4	Економічний розділ	4	
7	А4	Висновки	2	
8	А4	Перелік посилань	5	
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	
13	А4	Додаток Д	1	
14	А4	Додаток Е	1	
15	А4	Додаток Ж	1	
16	А4	Додаток З	1	
17	А4	Додаток І	1	
18	А4	Додаток К	1	
19	А4	Додаток М	1	
20	А4	Додаток Н	1	
21	А4	Додаток Л	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Пояснювальна записка Дегтерьов Радомир Павлович.doxc
2. Пояснювальна записка Дегтерьов Радомир Павлович.pdf
3. Презентація Дегтерьов Радомир Павлович.pptx

ДОДАТОК В. Відгуки перівників розділів

Відгук керіввника економічного розділу:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук

на кваліфікаційну роботу бакалавра на тему:

Розробка комплексної системи захисту інформації в інформативно-комунікаційній системі підприємства Ziber

Дегтерьова Радомира Павловича

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 103 сторінках.

Метою дослідження в роботі є створення комплексного програмно-апаратного засобу захисту корпоративної комунікаційної системи на базі обладнання Keenetic.

Тема кваліфікаційної роботи: аналіз комплексного програмно-апаратного засобу захисту корпоративної комунікаційної системи на базі обладнання Keenetic.

Розроблено рекомендації для проведення ідентифікації інформаційних активів.

Позитивними рисами дипломної роботи є системність та послідовність викладення матеріалу, а також застосування прогресивного досвіду в сфері захисту інформації та його практичне застосування і вдосконалення.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Дегтерьов Р.П. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

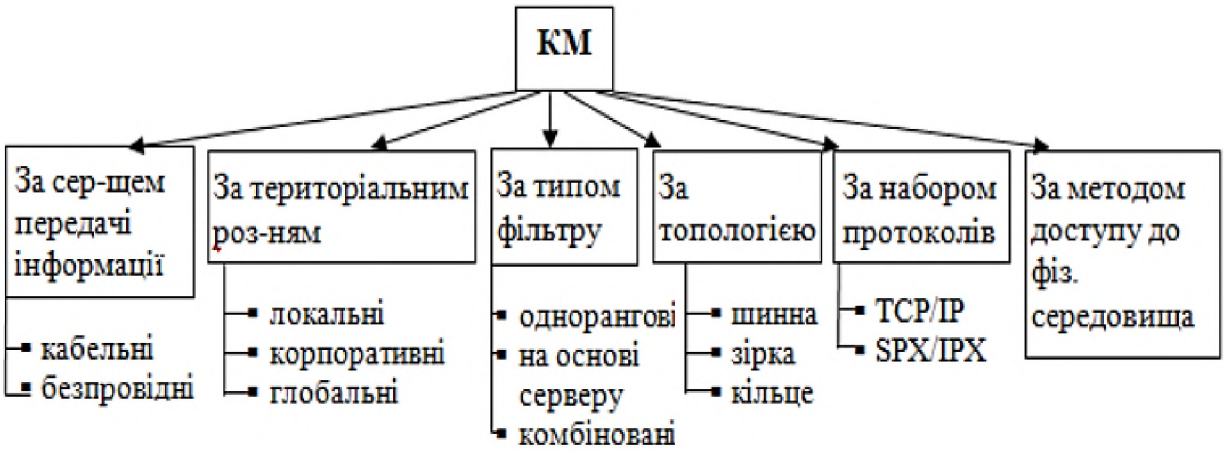
Рівень запозичень у кваліфікаційній роботі не перевищує вимог “Положення про систему виявлення та запобігання плагіату”.

Кваліфікаційна робота заслуговує оцінки «_____».

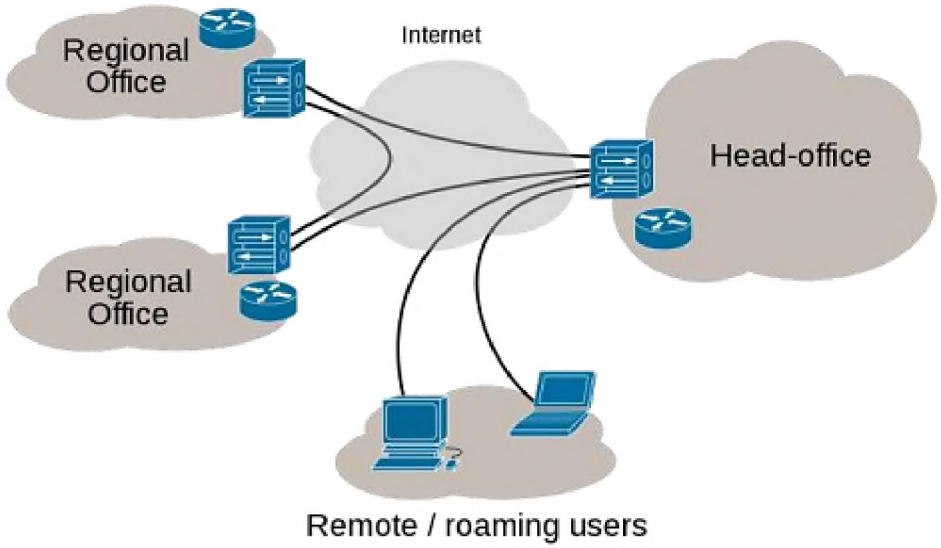
Керівник кваліфікаційної роботи

Керівник спец. Розділу

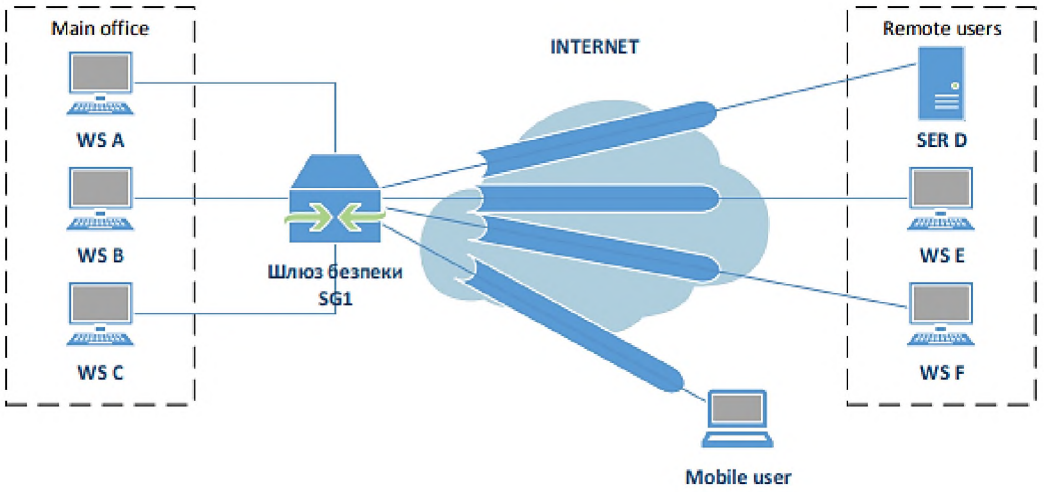
ДОДАТОК Д. Класифікація корпоративних інформаційно-комунікаційних систем



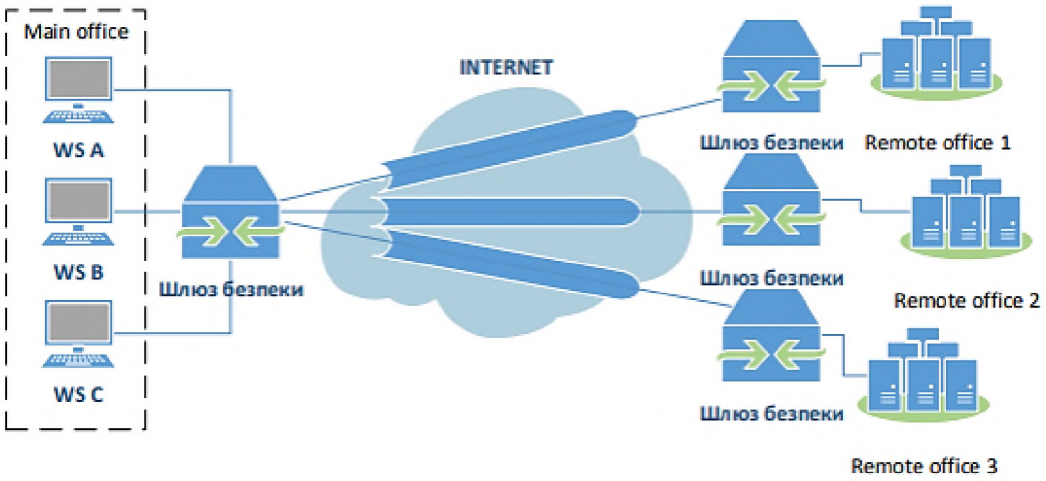
ДОДАТОК Е. Схематичне зображення віртуальної мережі передачі даних



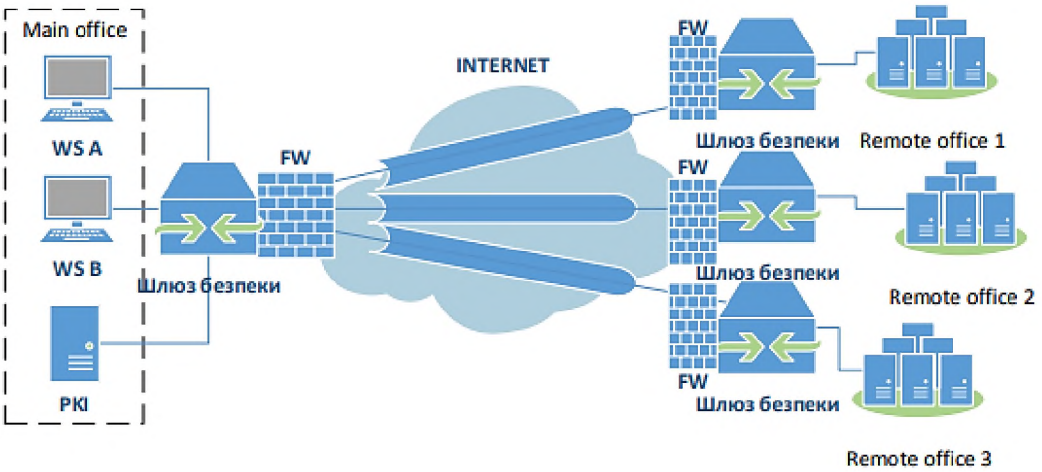
ДОДАТОК Ж. Віртуальна корпоративна комунікаційна система **з віддаленим доступом**



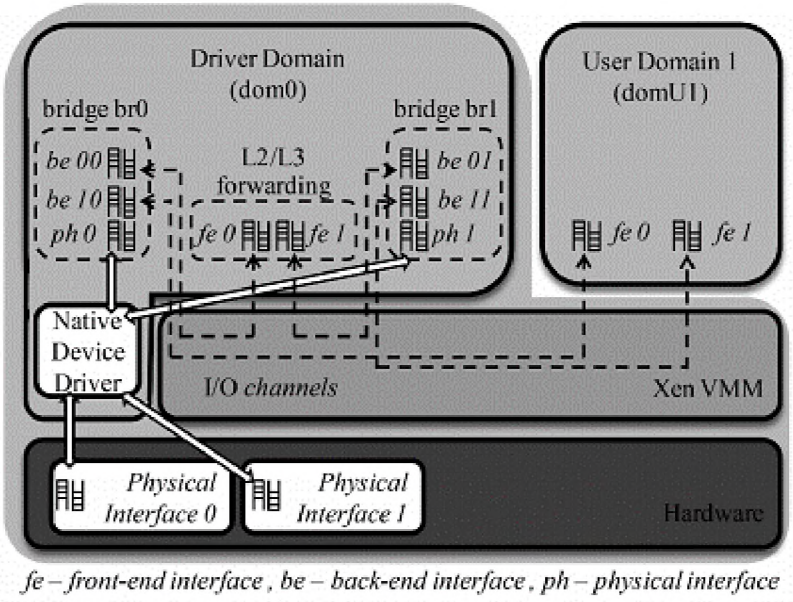
ДОДАТОК З. З'єднання вузлів мережі за допомогою технології Intranet VPN



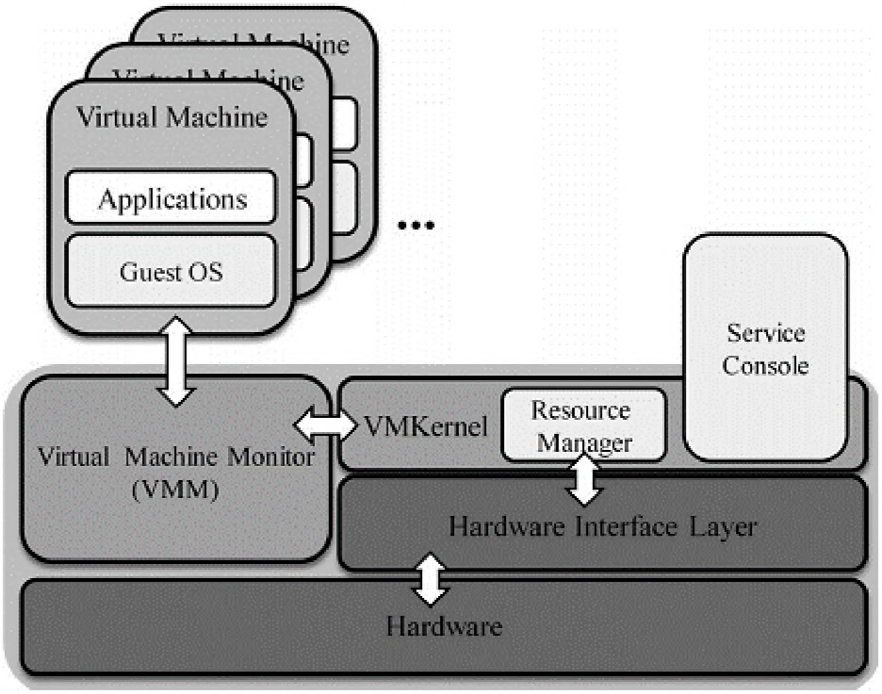
ДОДАТОК І. Міжкорпоративна комунікаційна система **Extranet VPN**



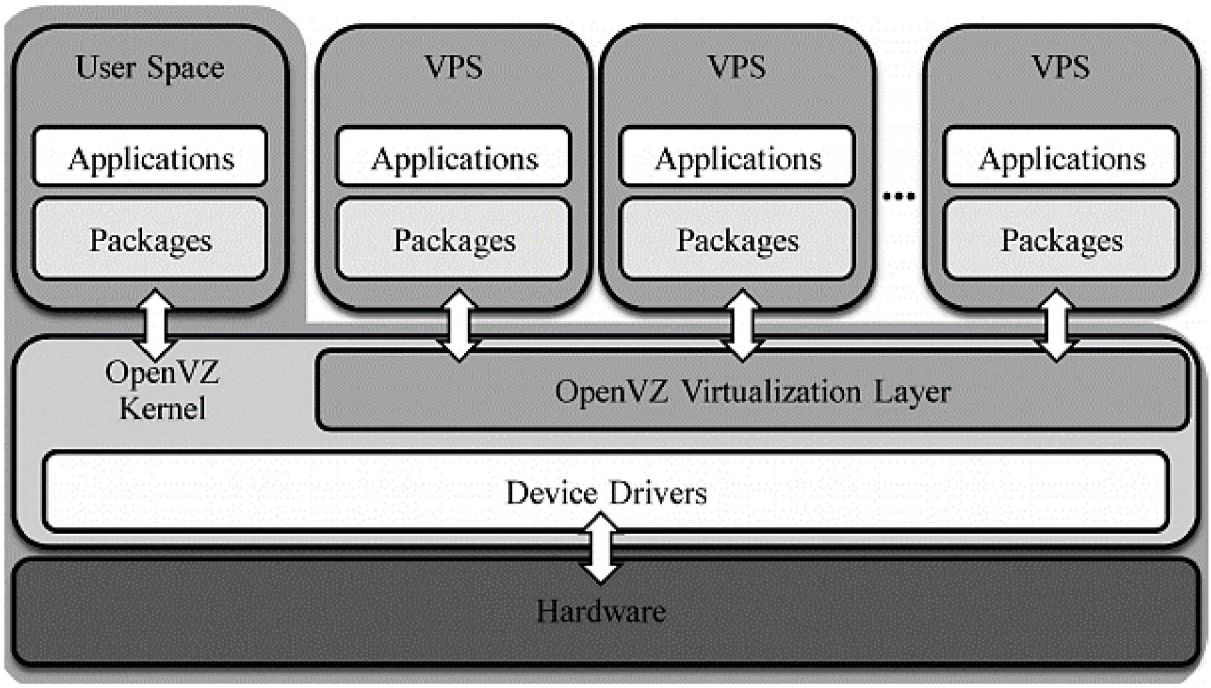
ДОДАТОК К. Схематичне зображення архітектури Xen



ДОДАТОК Л. Схематичне зображення архітектури VMware



ДОДАТОК М. Схематичне зображення архітектури OpenVZ



ДОДАТОК Н. Програмний код для налаштування захисту транспортування даних у мережі з використанням функції ACL, NAT і PAT на мережевому обладнанні Keenetic

```
// налаштування ACL
function configureACL() {
// Підключення до мережевого пристрою Keenetic
const keenetic = connectToKeenetic();

// Налаштування правил ACL
keenetic. configureACL({
sourceIP: '192.168.0.0 / 24',
destinationIP: '10.0.0.0 / 24',
protocol: 'tcp',
action: 'allow',
});

// Збереження налаштувань
keenetic. saveConfiguration();
}

// Налаштування NAT
function configureNAT() {
// Підключення до мережевого пристрою Keenetic
const keenetic = connectToKeenetic();

// Налаштування правил NAT
keenetic. configureNAT({
internalIP: '192.168.0.100',
externalIP: '1.2.3.4',
});
```

```
// Збереження налаштувань
keenetic. saveConfiguration();
}

// Нналаштування PAT
function configurePAT() {
// Підключення до мережевого пристрою Keenetic
const keenetic = connectToKeenetic();

// Налаштування правил PAT
keenetic. configurePAT({
internalIP: '192.168.0.100',
internalPort: 8080,
externalPort: 80,
});

// Збереження налаштувань
keenetic. saveConfiguration();
}

// Виклик функцій для налаштування захисту
configureACL();
configureNAT();
configurePAT();
```