МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних наук,
управління та адміністрування
Кафедра інформаційних технологій

Кваліфікаційна робота бакалавра

на тему: **Проектування мережі для організації, з аналізом спеціалізованого ПЗ для захисту даних**

Виконав студент групи **К-20і**
спеціальності 122 Комп'ютерні науки
Голосний Максим Андрійович

Керівник **асистент**
Клепатська Вікторія Вікторівна

Консультант **д.т.н., проф.**
Казакова Надія Феліксівна

Рецензент **Начальник відділу впровадження інформаційних технології Департаменту інформації та цифрових рішень Одеської міської ради**
Корчемний Павло Анатолійович

Одеса 2022

ЗМІСТ

ТЕРМІНИ, СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

Топологія – це конфігурація графа, вершинам якого відповідають кінцеві вузли мережі (комп'ютери та комунікаційне обладнання (маршрутизатори)), а ребрам – фізичні чи інформаційні зв'язки між вершинами. фізичної - описує реальне розташування та зв'язки між вузлами мережі.

Таблиця маршрутизації – це електронна таблиця (файл) або база даних, що зберігається на маршрутизаторі або мережному комп'ютері, яка описує відповідність між адресами призначення та інтерфейсами, через які слід надіслати пакет даних до наступного маршрутизатора. Є найпростішою формою правил маршрутизації.

Мережевий шлюз — апаратний маршрутизатор або програмне забезпечення для об'єднання комп'ютерних мереж, що використовують різні протоколи (наприклад, локальної та глобальної).

Маска підмережі – бітова маска для визначення IP-адреси адреси підмережі та адреси вузла (хоста, комп'ютера, пристрої) цієї підмережі. На відміну від IP-адреси, маска підмережі не є частиною IP-пакета.

Кручена пара – це такий вид кабелю зв'язку. Він являє собою одну або кілька пар ізольованих провідників, скручених між собою (з невеликою кількістю витків на одиницю довжини), покритих пластиковою оболонкою.

Інформаційна безпека – це стан захищеності систем обробки та зберігання даних, при якому забезпечені конфіденційність, доступність та цілісність інформації, використання та розвиток на користь громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства та держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (у цьому сенсі найчастіше використовують термін «захист інформації»)

Wi-Fi – це технологія бездротової локальної мережі із пристроями на основі стандартів IEEE 802.11. Під абревіатурою Wi-Fi (від англійського словосполучення Wireless Fidelity, яке можна дослівно перекласти як бездротова

точність). Основними діапазонами Wi-Fi вважаються 2.4 ГГц (2412 МГц-2472 МГц) та 5 ГГц (5160-5825 МГц). Сигнал Wi-Fi може передаватися навіть на кілометри і навіть при низькій потужності сигналу передачі, але для прийому Wi-Fi-сигналу зі звичайного Wi-Fi-маршрутизатора на далекій відстані потрібна антена з високим коефіцієнтом посилення (наприклад, параболічна антена або Wi-Fi- гармата).

VLAN – віртуальна локальна мережа, яка дозволяє розділити одну локальну мережу на окремі сегменти.

IP-адреса – це такий унікальний числовий ідентифікатор пристрою в комп'ютерній мережі, що працює за протоколом IP.

Internet – інформаційно-комунікаційна мережа та всесвітня система об'єднаних комп'ютерних мереж для зберігання та передачі інформації.

DNS-сервер – програма, призначена для відповідей на DNS-запити за відповідним протоколом. Також DNS-сервером можуть називати хост, на якому запущено відповідну програму.Fast Ethernet– це така загальна назва для набору стандартів передачі даних у комп'ютерних мережах, які працюють за технологією Ethernet зі швидкістю до 100 Мбіт/с, на відміну від початкових 10 Мбіт/с. Також FE позначається як 100BASE-X, де X має на увазі варіанти реалізації (наприклад, 100BASE-TX, 100BASE-FX). Варіанти для роботи з крученний пари мають загальне позначення 100BASE-T.

IC – інформаційна система.

VLAN – Virtual Local Area Network.

IP – Internet Protocol.

FE – Fast Ethernet.

DNS – Domain name server.

ВСТУП

В наш час, такі поняття як комп'ютерна мережа, Internet, комп’ютер стали буденністю та важливою частиною повсякденного життя. Світ швидко розвивається і стає насиченим новими технологіями.

Метою кваліфікаційної роботи є проектування мережі для організації з аналізом спеціалізованого програмного забезпечення для захисту даних, передачі даних із застосуванням сучасного обладнання.

Для вирішення поставленої мети у кваліфікаційної роботи вирішуються такі завдання:

- вибір мережевої архітектури для комп'ютерної мережі;
- метод доступу, топологія, тип кабельної системи;
- конфігурація мережного обладнання – серверів, концентраторів, мережевих принтерів, мережевих пристроїв;
- управління мережевими ресурсами та користувачами мережі;
- розгляд питань безпеки мережі.

Завдання кваліфікаційної роботи є розробка обґрунтованої та гнучкої схеми структури мережі, забезпечення моделі швидкого оновлення інформації, що працює на сервері, і вирішення проблеми забезпечення необхідного рівня захисту даних.

Передача даних (обмін даними, цифрова передача, цифровий зв'язок) – це фізичне перенесення даних (цифрового бітового потоку) у вигляді сигналів від точки до точки або від точки до кількох точок засобами електрозв'язку по каналу передачі даних, як правило, для подальшої обробки засобами обчислювальної техніки. Прикладами подібних каналів можуть бути мідні дроти, ВОЛЗ, бездротові канали передачі чи картка пам'яті.

Дана бакаларська кваліфікаційна робота складається зі вступу, 4-ьох розділів, висновків, переліку посилань з 18 найменувань. Повний обсяг роботи становить 55 сторінок та містить 6 таблиць і 8 рисунків.

1. ОПИС ПОНЯТТЯ КОМП'ЮТЕРНА МЕРЕЖА ТА АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПРОЕКТУВАННЯ МЕРЕЖІ

Комп'ютерні мережі – це системи комп'ютерів, об'єднаних каналами передачі даних, що забезпечують ефективне надання різних інформаційно-обчислювальних послуг користувачам за допомогою зручного та надійно-го доступу до ресурсів мережі [1].

Інформаційні системи, що використовують можливості комп'ютерних мереж, забезпечують виконання таких завдань:

- зберігання та обробка даних;
- організація доступу користувачів до даних;
- передача даних та результатів обробки даних користувачам.

Ефективність вирішення перелічених завдань забезпечується:

- дистанційним доступом користувачів до апаратних, програмних та інформаційних ресурсів;
- високою надійністю системи;
- можливістю оперативного перерозподілу навантаження;
- спеціалізацією окремих вузлів мережі для вирішення певного класу завдань;
- вирішенням складних завдань спільними зусиллями декількох вузлів мережі;
- можливістю здійснення оперативного контролю всіх вузлів мережі.

Основні показники якості комп'ютерних мереж включають такі елементи: повнота функцій, що виконуються, продуктивність, пропускна здатність, надійність мережі, безпека інформації, прозорість мережі, масштабованість, інтегрованість, універсальність мережі.

Існує безліч програм для проектування мереж, такі як Cisco Packet Tracer, GNS3 та інші, для розробки мережі у кваліфікаційному проекті використовувалась програма Cisco Packet Tracer.

Packet Tracer – це симулятор мережі передачі даних, що випускається фірмою Cisco Systems. Дозволяє робити працездатні моделі мережі, налаштовувати (командами Cisco IOS) маршрутизатори та комутатори[2].

У симуляторі реалізовані серії маршрутизаторів Cisco. Бездротові пристрої представлені маршрутизатором Linksys WRT300N, точками доступу та стільниковими вежами. Крім того є сервери DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP та EMAIL, робочі станції, різні модулі до комп'ютерів та маршрутизаторів, IP-фони, смартфони, хаби, а також хмара, що емулює WAN. Об'єднувати мережні пристрої можна за допомогою різних типів кабелів, таких як прямі та зворотні патч-корди, оптичні та коаксіальні кабелі, послідовні кабелі та телефонні пари.

Успішно дозволяє створювати складні макети мереж, перевіряти на працездатність топологію мережі. Проте реалізована функціональність пристроїв обмежена і надає всіх можливостей реального устаткування.

Було надано перевагу цьому програмному забезпеченню з причин:

- актуальності програми та постійної підтримки;
- наявність безлічі функцій та пристроїв при моделюванні;
- зручного та інтуїтивно зрозумілого інтерфейсу;
- існує безліч курсів як безкоштовних так і платних;
- програму можна отримати безкоштовно, якщо реєструватися на курс Cisco Academy.

З недоліків програмного забезпечення:

- реалізований функціонал пристроїв має обмеження, порівняно з реальним обладнанням;
- неможливість навідріз відкривати проекти новіших версій у пізніх версіях.

Graphical Network Simulator. Якщо перекладати буквально – графічний симулятор мережі. Він дозволяє створювати різні мережеві топології прямо на вашому комп'ютері. Найчастіше GNS використовується як лабораторний стенд, де можна перевірити ту чи іншу технологію або схему.

Насправді GNS3 не симулятор, а емулятор! Варто розуміти різницю між цими поняттями.

Емулятор дозволяє створити модель комп'ютера або іншого пристрою та запускати всередині оригінальне програмне забезпечення. Емулюються всі основні компоненти пристрою, включаючи процесор, пам'ять та пристрої введення/виводу. У випадку з Cisco емулятор створює модель маршрутизатора і запускає всередині реальну операційну систему Cisco IOS. Таким чином ми отримуємо повнофункціональний маршрутизатор.

Симулятор імітує поведінку системи та її інтерфейсу. Яскравий приклад – Cisco Packet Tracer. Програмісти цього програмного забезпечення просто створили пристрої зі схожим інтерфейсом і схожими командами.

Переваги:

- повний функціонал емульованих пристроїв, тобто. запустивши той же маршрутизатор Cisco, будуть доступні практично всі функції, які працюють на реальному маршрутизаторі (якщо згадати Cisco Packet Tracer, то там значна частина функціоналу недоступна, тому що це лише симулятор);
- можливість побудови гетерогенних мереж (мається на увазі, що можна зібрати схему, де будуть не тільки пристрої Cisco, але і Juniper, Mikrotik, CheckPoint і т.д.);
- додавання в мережу повноцінних робочих станцій і серверів, згадуючи Cisco Packet Tracer, то там як кінцеві пристрої були доступні клієнтські комп'ютери або сервери з дуже обмеженим функціоналом, в GNS3 можна додати повноцінний комп'ютер з Windows 7 або Ubuntu.

Недоліки:

- відсутність можливості емулювати комутатори;
- дуже високі вимоги до системних ресурсів, проблема пристроїв, що запускаються в ньому, які споживають дуже багато ресурсів (GNS3 на відміну від Cisco Packet Tracer працює з реальними прошивками

пристроїв. Для прикладу, щоб запустити Cisco ASA потрібен 1Гб оперативної пам'яті. У разі створення кластера буде споживатися ще більше оперативної пам'яті, на сьогоднішній день, мінімальні системні вимоги для GNS3 – це 4Гб оперативної пам'яті, але краще мати хоча б 8, у разі проектування досить великих схем);

– баги або глюки (У GNS3 їх досить багато).

2. ХАРАКТЕРИСТИКИ ЗАХИСТУ ІНФОРМАЦІЇ У МЕРЕЖІ

Дослідження та аналіз численних випадків впливів на інформацію та несанкціонованого доступу до неї показують, що їх можна розділити на випадкові та навмисні.

Для створення засобів захисту інформації необхідно визначити природу загроз, форми та шляхи їх можливого прояву та здійснення в системі. Для вирішення поставленої задачі все різноманіття загроз і шляхів їх впливу наводиться до найпростіших видів і форм, які були б адекватні їх безлічі в системі. Дослідження досвіду проектування, виготовлення, випробувань та експлуатації систем говорять про те, що інформація в процесі введення, зберігання, обробки та передачі піддається різним випадковим впливам.

Причинами таких впливів можуть бути:

- неуважність та недбалість співробітників;
- використання піратського ПЗ;
- DDoS-атаки. Distributed-Denial-of-Service;
- віруси;
- загрози з боку співвласників бізнесу;
- законодавчі перипетії;
- інші дії.

Навмисні загрози завжди потенційно пов'язані з діяльністю людини, причинами яких може бути певне невдоволення своїм матеріальним добробутом чи життєвої ситуацією чи просте розвага з перевіркою своїх здібностей, як і хакерів, тощо. Немає жодних сумнівів, що на підприємстві відбудуться випадкові чи навмисні спроби зламування мережі ззовні. У зв'язку з цим обставиною потрібно ретельно передбачити захисні заходи.

Для обчислювальних систем характерні такі штатні канали доступу до інформації[3]:

- термінали користувачів, найдоступніші з яких це робочі станції;
- термінал адміністратора системи;

- термінал оператора функціонального контролю;
- засоби відображення інформації;
- засоби завантаження програмного забезпечення;
- засоби документування інформації;
- носії інформації;
- зовнішні канали зв'язку.

2.1 Загальні рекомендації щодо захисту мережі

Постійно встановлюйте оновлення для комп'ютера[4].

Щоб підвищити безпеку комп'ютерів у мережі, необхідно вмикати на кожному з них автоматичне оновлення. Windows може автоматично встановити важливі та рекомендовані оновлення або лише важливі оновлення.

Важливі оновлення забезпечують значне покращення захисту та надійності комп'ютера. Рекомендовані оновлення можуть стосуватися некритичних проблем та покращити роботу комп'ютера. Необов'язкові оновлення автоматично не завантажуються та не встановлюються.

Служба Windows Update містить програмні засоби, які перевіряють дані про комп'ютер (модель, версія Windows) та інше програмне забезпечення Microsoft, яке використовується на комп'ютері. Майкрософт використовує цю інформацію для встановлення лише необхідних для комп'ютера оновлень.

Використання брандмауера Windows

За допомогою брандмауера можна запобігти проникненню на комп'ютер хакерів або шкідливих програм (наприклад, черв'яків) через мережу або інтернет. Крім того, брандмауер запобігтиме відправленню шкідливих програм з комп'ютера на інші.

Без встановлення брандмауера, онлайн-доступ до комп'ютера схильний до кількох видів загроз, які можуть стати причиною злому інформації для кіберзлочинців.

Проблеми можуть включати (але не обмежуватися):

Бекдор доступ: Бекдор відноситься до вразливостей у системі безпеки або помилок, які при експлуатації допускають несанкціонований контроль за програмою. Навіть цілі операційні системи, такі як Windows, можуть мати бекдор, і досвідчений хакер знає, як ними скористатися.

Злам віддаленого доступу: Віддалений робочий стіл дозволяє підключатися до комп'ютера та керувати ним з іншого місця через Інтернет.

Атака через e-mail: Цей вид атаки націлений на людину, якій зловмисник надсилає тисячі електронних листів, щоб забити поштову скриньку жертви. Спам електронною поштою є досить популярним видом атаки. Хоча більшість спаму просто викликає роздратування, але деякі листи можуть містити віруси.

Переадресація маршруту: Коли пакети даних проходять через онлайн-мережу, вони, як правило, передаються декількома маршрутизаторами до досягнення пункту призначення. Деякі хакери використовують цю систему, створюючи враження, що шкідливі пакети даних надходять із надійного джерела. З цієї причини багато брандмауерів замінюють основну маршрутизацію.

Існує багато переваг для запуску брандмауера на комп'ютері. Підвищена безпека, яку вони забезпечують, коштує кілька зайвих повідомлень та спливаючих попереджень.

Переваги:

- брандмауер забезпечує моніторинг та перевірку онлайн-доступу будь-якої запущеної програми (мережевий трафік, який може сигналізувати про незахищену передачу конфіденційних даних, контролюватиметься через брандмауер);
- багато рішень повідомляють про заблоковані пакети даних і показують спливаючі повідомлення щоразу, коли брандмауер відфільтровує будь-які з'єднання. Таким чином, користувач завжди знає, якщо щось трапиться;
- деякі брандмауери постачаються з додатковими функціями для підвищення кібербезпеки.

Недоліки:

- брандмауер виступає як контрольна точка безпеки для пакетів даних, що входять і виходять з вашої мережі (як і в будь-якій точці контролю безпеки, іноді виникають помилкові спрацьовування. Користувач може виявити, що брандмауер випадково блокує захищену вебсторінку, до якої хоче отримати доступ);
- ця проблема також не є унікальною для окремих користувачів (провайдер інтернет-безпеки McAfee провів бізнес-опитування, яке показало, що третина організацій відключають функції безпеки брандмауера, щоб запобігти перериванню робочого процесу через помилкові спрацьовування. Деякі компанії відключають певні функції, тому що вони використовують дуже багато обчислювальної потужності).

Брандмауери допомагають захистити комп'ютер від хробаків та хробаків, але вони не призначені для захисту від вірусів, тому слід також встановити антивірусне програмне забезпечення.

Віруси можуть міститись у вкладеннях електронної пошти, файлах на компакт-дисках та DVD-дисках або у файлах, завантажених з інтернету. Слід переконатися, що антивірусне програмне забезпечення оновлено та настроєно на періодичне сканування комп'ютера.

Використання маршрутизатора для спільного доступу до Інтернету. Ці пристрої зазвичай мають вбудовані брандмауери, перетворювачі мережевих адрес (NAT) та інші засоби, які можуть покращити захист мережі від хакерів.

Не варто входити до системи як адміністратор.Якщо використовується програма, яка потребує доступу до Інтернету, наприклад браузер або поштова програма, рекомендується входити до системи за допомогою стандартного облікового запису, а не адміністратора.

Багато вірусів та хробаків не можуть зберігатися та запускатися на комп'ютері, якщо вхід до системи виконаний без прав адміністратора.

Адміністратори Windows можуть змінювати параметри безпеки, інста-

лювати програмне забезпечення та інсталювати обладнання, а також отримувати доступ до всіх файлів, що зберігаються на комп'ютері. Адміністратори також можуть змінювати установки інших облікових записів.

2.2 Причини виникнення загроз в інформаційній безпеці

1. Загрозу інформаційної безпеки компанії, як не дивно, можуть представляти цілком звичайні співробітники, які навіть не думають про злий намір про крадіжку важливих даних. Ненавмисна шкода конфіденційним відомостям відбувається через простий недбалість або непоінформованість працівників про важливі теми інформаційної безпеки. Завжди є можливість того, що хтось відкриє фішинговий лист та впровадить вірус із особистого ноутбука на сервер компанії. Або, наприклад, скопіює файл з конфіденційними відомостями на планшет, флешку або КПК для відрядження. І жодна компанія не застрахована від пересилання неуважним співробітником важливих файлів за тією адресою. У такій ситуації інформація виявиться легкою здобиччю для різних зловмисників.

2. Іноді керівники компаній намагаються заощадити придбання ліцензійного ПЗ. Але слід знати, що неліцензійні програми не дають захисту від шахраїв, які зацікавлені в крадіжці інформації за допомогою вірусів. Власник неліцензійного програмного забезпечення не отримує технічної підтримки, своєчасних оновлень, що надаються компаніями-розробниками. Разом з ним він купує і віруси, здатні завдати шкоди системі комп'ютерної безпеки. За даними дослідження Microsoft, у 7% вивчених неліцензійних програм було знайдено спеціальне програмне забезпечення для крадіжки паролів та персональних даних.

3. DDoS-атаки (Distributed-Denial-of-Service) – «розподілена відмова від обслуговування» – це потік помилкових запитів від сотень тисяч географічно розподілених хостів, які блокують обраний ресурс одним із двох шляхів. Перший шлях–це пряма атака на канал зв'язку, який повністю блокується безліччю

марних даних. Другий – атака безпосередньо на сервер ресурсу. Недоступність або погіршення якості роботи публічних веб-сервісів внаслідок атак може тривати досить тривалий час, від кількох годин до кількох днів.

Традиційно подібні атаки застосовуються в ході конкурентної боротьби, шантажу підприємств або для відвернення уваги системних адміністраторів від деяких протиправних дій на кшталт викрадення коштів з рахунків. На думку фахівців, саме крадіжки є головним мотивом DDoS-атак. Мішенню зловмисників частіше стають сайти банків, у половині випадків було порушено саме вони.

4. Однією з найнебезпечніших на сьогодні загроз інформаційної безпеки є комп'ютерні віруси. Це підтверджується багатомільйонним збитком, який зазнають компанії внаслідок вірусних атак. Останніми роками суттєво збільшилася їх частота та рівень збитків. На думку експертів, можна пояснити появою нових каналів проникнення вірусів. На першому місці, як і раніше, залишається пошта, але, як показує практика, віруси здатні проникати і через програми обміну повідомленнями, такі як telegram, viber та інші. Збільшилася кількість об'єктів для можливих вірусних атак. Якщо раніше атакам піддавалися переважно сервери стандартних веб-служб, то сьогодні віруси здатні впливати і на міжмережні екрани, комутатори, мобільні пристрої, маршрутизатори.

Останнім часом особливо активними стали так звані віруси-шифрувальники. Навесні та влітку 2017 року мільйони користувачів постраждали від атак вірусів WannaCry, Petya, Misha. Епідемії показали, що жертвою вірусної атаки можна стати навіть якщо не відкривати підозрілі листи. За інформацією Intel вірусом WannaCry заразилися 530 тисяч комп'ютерів, а загальні збитки компаній склали понад 1 млрд доларів.

5. Загрози з боку співвласників бізнесу. Саме легальні користувачі є однією з основних причин витоків інформації в компаніях. Такі витоки фахівці називають інсайдерськими, а всіх інсайдерів умовно поділяють на кілька груп:

«Порушники» – середня ланка та топ-менеджери, які дозволяють собі

невеликі порушення інформаційної безпеки – грають у комп'ютерні ігри, роблять онлайн-покупки з робочих комп'ютерів, користуються особистою поштою. Така безладність здатна викликати інциденти, але найчастіше вони є ненавмисними. До речі, більшість зовнішніх атак відбуваються саме через особисті поштові скриньки чи месенджери працівників.

"Злочинці". Найчастіше інсайдерами є топ-менеджери, які мають доступ до важливої інформації та зловживають своїми привілеями. Вони самостійно встановлюють різні програми, можуть відсилати конфіденційну інформацію зацікавленим у ній третім особам тощо.

"Кроти"–співробітники, які навмисне крадуть важливу інформацію за матеріальну винагороду від компанії-конкурента. Як правило, це дуже досвідчені користувачі, які вміло знищують всі сліди своїх злочинів. Впіймати їх через це буває дуже непросто.

Ще одна категорія – це звільнені та ображені на компанію співробітники, які забирають із собою всю інформацію, до якої вони мали доступ. Зазвичай вкрадена інформація використовується на новому місці роботи.

6. Законодавчі перипетії. Державні органи наділені правом конфіскувати під час перевірок обладнання та носії інформації. Оскільки більшість важливих даних компанії зберігається в електронному вигляді на серверах, то у разі їх вилучення компанія на якийсь час просто зупиняє свою діяльність. Простои цьому ніхто не компенсує, і якщо перевірка затягується, великі збитки можуть призвести до припинення діяльності фірми. Вилучення обладнання – одна з найгостріших проблем сучасного бізнесу, при цьому приводом для нього може бути все, що завгодно – від рішення слідчого до рішення суду в рамках будь-якої кримінальної справи.

2.3 Поняття інформаційної безпеки

Під інформаційною безпекою підприємства чи компанії розуміють ком-

плекси заходів організаційного та технічного характеру, спрямованих на збереження та захист інформації та її ключових елементів, а також обладнання та системи, що використовуються для роботи з інформацією, її зберігання та передачі. Цей комплекс включає технології, стандарти та методи управління інформацією, які забезпечують її ефективний захист.

Засоби забезпечення інформаційної безпеки допомагає захистити інформацію та саму інформаційну інфраструктуру підприємства від злоякісних впливів. Такі дії можуть мати випадковий або навмисний, внутрішній або зовнішній характер. Результатом таких втручань може стати втрата важливої інформації, її несанкціонована зміна чи використання третіми особами. Тому інформаційна безпека – це важливий аспект захисту бізнесу та забезпечення його безперервності [6].

Принципи ефективного впровадження у компанії систем інформаційної безпеки:

- конфіденційність;
- цілісність;
- доступність.

Конфіденційність розуміють організацію та підтримку ефективного контролю для забезпечення достатнього ступеня безпеки даних, активів та інформації на різних етапах бізнес-процесів для виключення несанкціонованого або небажаного розкриття. Підтримка конфіденційності обов'язково застосовується при збереженні та транзиті інформації у будь-якому форматі.

Цілісність охоплює елементи управління, які забезпечують внутрішню та зовнішню послідовність інформації. Забезпечення цілісності дає змогу виключити можливість спотворення даних на будь-якому з етапів ділових операцій.

Доступність підтримує повноцінний та надійний доступ до інформації для посадових осіб, які мають відповідні повноваження. Ключовим моментом тут є передбачуваність процесів, що протікають у мережному середовищі, щоб користувачі мали можливість доступу до необхідних даних у потрібний час.

Одним із важливих факторів доступності інформації є можливість швидкого та повного відновлення системи після збоїв, щоб не допустити його негативного впливу на функціонування компанії.

2.4 Здійснення контролю інформаційної безпеки підприємства

Забезпечити повноцінну та надійну інформаційну безпеку підприємства можна лише за умови застосування комплексного та системного підходу. Система інфобезпеки має бути побудована з урахуванням усіх актуальних загроз та вразливостей, а також з урахуванням тих загроз, які можуть виникнути в майбутньому. Тому важливо забезпечити підтримку безперервного контролю, який має діяти щодня та цілодобово. Необхідною умовою є забезпечення контролю на кожному з етапів життєвого циклу інформації, починаючи з моменту її надходження до інфраструктури компанії та закінчуючи втратою її актуальності чи знищенням даних.

Існує кілька видів контролю інформаційної безпеки, впровадження яких дозволяє компанії знижувати ризики у цій сфері та підтримувати їх на прийнятному рівні. У тому числі розрізняють:

- адміністративний контроль;
- логічний контроль;
- фізичний контроль.

Адміністративний контроль інформаційної безпеки–це система, що складається з комплексу встановлених стандартів, принципів та процедур. Цей вид контролю визначає межі для здійснення бізнес-процесів та управління персоналом. Він включає законодавчі та нормативні акти, прийняту на підприємстві політику корпоративної безпеки, систему найму працівників, дисциплінарні та інші заходи.

Логічний контроль передбачає використання засобів управління (засобів технічного контролю), що захищають інформаційні системи від небажаного доступу. Ці засоби поєднують спеціальне ПЗ, брандмауери, паролі тощо.

Фізичний контроль зосереджений серед робочих місць і засобах обчислення. У тому числі він передбачає забезпечення ефективного функціонування інженерних систем будівель підприємства, робота яких може вплинути на зберігання та передачу інформації. До таких систем відносяться опалення та кондиціювання, протипожежні системи. Іншою важливою складовою фізичного контролю є системи контролю та управління доступом на об'єкти.

2.5 Засоби захисту інформації

Засобами захисту інформації називають пристрої, прилади, пристрої, програмне забезпечення, організаційні заходи, які запобігають витоку інформації та забезпечують її збереження в умовах впливу всього спектра актуальних загроз.

Залежно від способів реалізації, засоби захисту інформаційної безпеки бувають наступних типів:

Організаційні – комплекс заходів та засобів організаційно-правового та організаційно-технічного характеру. До перших відносять законодавчі та нормативні акти, локальні нормативні документи організації. Другий тип – це заходи щодо обслуговування інформаційної інфраструктури об'єкта.

Апаратні (технічні) – спеціальне обладнання та пристрій, що запобігає витоку, що захищає від проникнення в IT-інфраструктуру.

програмні. Спеціальне програмне забезпечення, призначене для захисту, контролю, зберігання інформації.

Програмно-апаратні – спеціальне обладнання із встановленим програмним забезпеченням для захисту даних.

Найширше поширення сьогодні набули програмні засоби захисту інформації. Вони повністю відповідають вимогам ефективності та актуальності, регулярно оновлюються, ефективно реагуючи на актуальні загрози штучного характеру.

Для захисту даних у сучасних мережах використовується широкий

спектр спеціалізованого програмного забезпечення. Можна виділити такі типи програмних засобів захисту:

Спеціалізований софт для виявлення, нейтралізації та видалення комп'ютерних вірусів. Виявлення може виконуватися під час перевірок за розкладом або запущених адміністратором. Програми виявляють та блокують підозрілу активність програм у «гарячому» режимі. Крім того, сучасні антивіруси можуть відновлювати файли, заражені шкідливими програмами.

Хмарні антивіруси (CloudAV) – поєднання можливостей сучасних антивірусних програм із хмарними технологіями. До таких рішень відносяться сервіси Crowdstrike, Panda Cloud Antivirus, Immunet та багато інших. Весь основний функціонал ПЗ розміщений у хмарі, а на комп'ютері, що захищається, встановлюється клієнт – програма з мінімальними технічними вимогами. Клієнт вивантажує хмарний сервер основну частину аналізу даних. Завдяки цьому забезпечується ефективний антивірусний захист за мінімальних ресурсних вимог до обладнання. Рішення CloudAV оптимально підходять для захисту ПК, які не мають достатньої вільної обчислювальної потужності для стандартного антивірусу.

Рішення DLP (Data Leak Prevention) – спеціальні програмні рішення, що запобігають витоку даних. Це комплекс технологій, які ефективно захищають підприємства від втрати конфіденційної інформації з різних причин. Впровадження та підтримка DLP – вимагає досить великих вкладень та зусиль з боку підприємства. Однак цей захід здатний значно зменшити рівень інформаційних ризиків для IT-інфраструктури компанії.

Системи криптографії (DES–Data Encryption Standard, AES–Advanced Encryption Standard) – перетворюють дані, після чого розшифровка може бути виконана тільки з використанням відповідних шифрів. Крім цього, криптографія може використовувати інші корисні програми для захисту інформації, у тому числі дайджести повідомлень, методи автентифікації, зашифровані мережеві комунікації, цифрові підписи. Сьогодні нові програми, що використову-

ють зашифровані комунікації, наприклад, Secure Shell (SSH), поступово витісняють застарілі рішення, що не забезпечують у сучасних умовах необхідний рівень безпеки, такі як Telnet та протокол передачі файлів FTP. Для шифрування бездротового зв'язку широко використовуються сучасні протоколи WPA/WPA2. Також використовується досить старий протокол WEP, який поступається з безпеки. ITU-T G.hn та інші провідні комунікації шифруються за допомогою AES, а автентифікацію та обмін ключами в них забезпечує X.1035. Для шифрування електронної пошти використовують такі програми як PGP та GnuPG.

Міжмережеві екрани (МСЕ), забезпечують фільтрацію та блокування небажаного трафіку, контролюють доступ до мережі. Розрізняють такі види фаєрволів, як мережеві та хост-сервери. Мережеві фаєрволи розміщуються на шлюзових ПК LAN, WAN та в інтрамережах. Міжмережевий екран може бути виконаний у форматі програми, встановленої на звичайний комп'ютер, або мати програмно-апаратне виконання. Програмно-апаратний фаєрвол–це спеціальний пристрій на базі операційної системи з встановленим МСЕ. Крім основних функцій, міжмережеві екрани пропонують низку додаткових рішень для внутрішньої мережі. Наприклад, виступають як сервер VPN або DHCP.

Віртуальні приватні мережі VPN (Virtual Private Network) – рішення, що використовує у межах загальнодоступної мережі приватну мережу передачі та прийому даних, що дає ефективний захист підключених до мережі додатків. За допомогою VPN забезпечується можливість віддаленого підключення до локальної мережі, створення спільної мережі для головного офісу с філій. Безпосередньо для користувачів VPN дає можливість приховувати розташування та захист дій, що виконуються в мережі.

Проксі-сервер – виконує функцію шлюзу між комп'ютером та зовнішнім сервером. Запит, який надсилається користувачем на сервер, спочатку надходить на proxy і від його імені надходить на сервер. Повернення відповіді проводиться також із проходженням проміжної ланки–proxy. Перевагою є те, що кеш проксі-сервера доступний для всіх користувачів. Це підвищує зручність у

роботі, оскільки найчастіше запитані ресурси перебувають у кеші.

Рішення SIEM – системи моніторингу та управління інформаційною безпекою. Спеціалізоване ПЗ, яке перебирає функцію управління безпекою даних. SIEM забезпечує збирання відомостей про події з усіх джерел, що підтримують безпеку, у тому числі від антивірусного ПЗ, IPS, фаєрволів, а також від операційних систем тощо. Також SIEM виконує аналіз зібраних даних та забезпечує їх централізоване зберігання в журналі подій. На підставі аналізу даних система виявляє можливі збої, атаки хакерів, інші відхилення і можливі інформаційні загрози.

Враховуючи широке розповсюдження мобільних пристроїв, які співробітники часто використовують за межами підприємства з корпоративною метою, у системі інформаційної безпеки обов'язково має враховуватися і цей фактор. Для контролю мобільних пристроїв персоналу та захисту інформації підприємства можуть використовуватись такі програмні продукти, як Blackberry Enterprise Mobility Suite, IBM MaaS360, VMware AirWatch та інші.

3. ДОСЛІДЖЕННЯ ТА АНАЛІЗ ПРОГРАМНИХ ПРОДУКТІВ

SIEM (Security Information and Event Management) – системи збирання та управління інформацією про безпеку, а також аналізу подій інформаційної безпеки. Саме це ПЗ не призначене для захисту та запобігання витоку даних та інших кібер–проблем. Його завдання – збирати інформацію від DLP, IDS, антивірусу, маршрутизатора та інших, аналізувати її та повідомляти про відхилення, підозрілі дії тощо.

Подібних програм досить багато, тому наведено кілька варіантів для прикладу.

IBM QRadar Security Intelligence – платформа, в рамках якої реалізовано відразу кілька продуктів для виявлення загроз мережевої безпеки, оцінки та протидії їм. ПЗ забезпечує можливість управління подіями, інтеграцію інформації про безпеку, виявлення аномальних ситуацій, управління журналами та реалізацію інших завдань. Саме комплексність та велика кількість можливостей – головні переваги цієї системи.

Основні можливості:

- єдина архітектура аналізу загроз, журналів, подій та інших маркерів;
- розрахунок кореляції, і навіть аномальних обставин практично як реального часу;
- великі можливості аналізу мережної активності;
- великі можливості аналізу дій користувачів та запущених програм;
- визначення інцидентів із високим рівнем пріоритетності;
- автоматизована система складання звітів;
- збір та узагальнення інформації про зафіксовані загрози;
- масштабований контроль активності у межах підприємства;
- проведення детального аналізу виходячи з технологій великих даних.

Недоліки:

- деяким подіям, що реєструються, не присвоюється категорія;

– це масштабна система, що може спричинити деякі складнощі з інтеграцією.

Доступний 14-денний пробний період, а також можливість безкоштовного використання програмного забезпечення з обмеженим функціоналом. Вартість ліцензії – від 800 $ на місяць.

Splunk Enterprise Security є ще одним потужним інструментом, призначеним для аналітики подій інформаційної безпеки на підприємствах. Його основна відмінна риса – орієнтованість насамперед на сучасні загрози та адаптивність із новими програмно-апаратними рішеннями. Завдяки цьому ПЗ відрізняється високою оперативністю виявлення загроз та оповіщення про них.

Основні можливості:

– моніторинг загроз у режимі реального часу;
– перевірка користувачів, програм та мережевих ресурсів;
– виявлення складних загроз, зокрема визначення взаємозв'язків між різними подіями;
– виявлення внутрішніх загроз, у тому числі зловмисних дій з боку співробітників;
– розслідування інцидентів, зокрема встановлення їх масштабів.
– автоматизація управління та вивантаження даних;
– виявлення шахрайства виходячи з виявлення аномалій у діях.

Недоліки:

– корпоративна версія відрізняється певною складністю установки;
– відсутня українська локалізація нових версій ПЗ.

Вартість ліцензії – від 1800 $ на рік залежно від конфігурації.

Розробники McAfee Enterprise Security Manager називають свою систему одним з лідерів за швидкістю та повнотою обробки інформації. Це програмне забезпечення доступне для розгортання, як у хмарних, так і в локальних мережах. Добре підходить для підприємств та організацій, де потрібна обробка великих обсягів даних. Також продукт відрізняється високим рівнем інтеграції з

програмним забезпеченням сторонніх розробників без API, що дозволяє створювати корпоративні системи інформаційної безпеки, використовуючи найбільш підходяще з власного погляду програмне забезпечення.

Основні можливості:

- наявність готових конфігурацій із попередньо налаштованими сценаріями;
- вбудовані пакети матеріалів з базової поведінки користувачів;
- окремий пакет функцій моніторингу внутрішніх служб Windows.
- виявлення загроз у реальному часі;
- система інформування про загрози;
- моніторинг даних у хмарних та локальних мережах;
- збір та кластеризація подій;
- формування автоматичних звітів про події.

Недоліки:

- система вимоглива до обсягу обчислювальних ресурсів;
- не завжди оперативне усунення виявлених багів.

Вартість однієї безстрокової ліцензії – від 500 грн. Для всіх нових користувачів доступний 14-денний безкоштовний тестовий період.

DLP-система (розшифровка абревіатури – Data Leak Prevention) – спеціалізоване ПЗ, призначене для захисту від витоків та крадіжки конфіденційної корпоративної інформації. Такі програми використовують технології блокування передачі через різні канали, пропонують функціонал для моніторингу поведінки співробітників та всіх учасників мережі, надають деякі можливості відстеження активностей персоналу. Ринок DLP-систем великий, але на ньому можна виділити два лідируючі продукти.

Система InfoWatch Traffic Monitor розроблена для роботи під великим навантаженням.

При необхідності обробки значних обсягів інформації. Це масштабоване ПЗ, яке однаково добре підходить для великих організацій та невеликих офісів. Основні функції – моніторинг та блокування даних. Особливість – здатність

виявляти документи та мультимедійні дані, блокувати їх навіть у разі їх значної видозміни користувачем.

Основні можливості:

- виявлення трафіку конфіденційної інформації всіх типів;
- блокування передачі конфіденційної інформації;
- виявлення несумлінних працівників;
- виявлення шахрайських схем;
- виявлення неочевидних загроз;
- контролює шляхи поширення інформації всередині компанії.

Недоліки:

- недостатній функціонал контролю за активністю користувачів;
- відсутність кейлоггера;
- модульна інфраструктура із розміщенням модулів на окремих серверах.

Вартість залежить від обраної конфігурації та надається розробником за запитом. Продукт продається з річною відновлюваною ліцензією.

DeviceLock DLP – хостова DLP-система, призначена для моніторингу інформації та блокування її несанкціонованого розповсюдження. Надає великі можливості налаштування сценарій та політик контролю, що дозволяє інтегрувати її в організаціях різних типів для вирішення більшості завдань, пов'язаних із захистом конфіденційних даних.

Основні можливості:

- блокування доступу користувачів до даних;
- блокування доступу користувачів до серверів та периферійних пристроїв;
- індивідуальне налаштування параметрів моніторингу та блокування;
- контроль доступу та взаємодії користувачів із мережевими сервісами.

Недоліки:

- обмежені можливості моніторингу працівників;
- необхідна точна настройка сценаріїв для коректного спрацювання блокування.

Вартість річної ліцензії – від 80 доларів. Точна ціна залежить від вибраної версії та конфігурації.

Ще одна категорія корисних програм – ПЗ, що дозволяє виявити людину, яка викрала документи. У різних рішеннях реалізовано різні методи досягнення такого результату. Але справді ефективною можна назвати лише одну систему.

EveryTag – програма, яка дозволяє з дуже високою ймовірністю виявити співробітника, який викрав інформацію. ПО особливо маркує документи, причому маркування візуально непомітна. У разі витоку інформації та появи несанкціонованої копії, її достатньо завантажити в систему, щоб дізнатися, хто зі співробітників вчинив розкрадання. Підхід простий, але ефективний.

Основні можливості:

- захист документів у електронному форматі;
- захист від несанкціонованого фотографування роздрукованих документів;
- захист від крадіжки методом несанкціонованих знімків екрана;
- захист від розкрадання роздрукованих документів.

Недоліки:

- це цільове ПЗ, функціонал якого дозволяє лише виявляти співробітників, які викрадають документи.

Вартість залежить від конфігурації ПЗ. Прайс-лист розробник надає лише за запитом клієнта.

Система інформаційної безпеки компанії не буде повною без впровадження хорошого корпоративного антивірусу. Це програмне забезпечення для захисту інформації та обладнання від шкідливого програмного забезпечення, вірусних загроз та кібер–атак. Ринок пропонує багато хороших програм такого типу. Розглянемо деякі з них.

Kaspersky Small Office Security – надійний антивірус із швидким оновленням баз даних та гарним рівнем захисту від загроз. ПЗ оптимально підходить для невеликих компаній, але може використовуватися і у великих організаціях. Безперечна перевага – розширений функціонал, що охоплює майже всі аспекти цифрової взаємодії компанії із зовнішніми мережами.

Основні можливості:

– файловий антивірус;
– веб-антивірус;
– захист від збирання даних;
– контроль оновлення програм;
– захист веб-камер;
– фільтрування активності користувачів;
– контроль встановлених програм;
– захист фінансової інформації;
– блокування реклами;
– шифрування інформації.

Недоліки:

– ПЗ більшою мірою орієнтоване на малі офіси;
– обмежений функціонал управління у веб-панелі.

Вартість річної ліцензії – від 23 долари для конфігурації із захистом на 1 ПК.

McAfee Endpoint Protection Essential – ще один популярний корпоративний антивірус. Також відрізняється гарним набором інструментів для захисту від мережевих та програмних загроз. Оптимізований для вирішення завдань компаній та організацій, відрізняється простотою налаштування та керування, а також високою частотою оновлення баз даних. Ключові переваги – висока ефективність виявлення загроз та протидії їм, великі можливості налаштування звітів.

Основні можливості:

– брандмауер;
– моніторинг у режимі реального часу;
– захист від вірусів-здирників;
– мережевий захист ПК;
– контроль веб-трафіку;
– автоматична реакція на можливі небезпеки.

недоліки:

– ускладнена установка та налаштування;
– вимоги до ресурсів обладнані при повному скануванні системи.

Вартість річної ліцензії – від 100 доларів. Точна ціна залежить від вибраної конфігурації.

Системи обліку робочого часу (СОРВ) – ще одна категорія програмного забезпечення, без якого не обійтися, налагоджуючи комплексний захист корпоративних даних. Щоправда, слід розглядати лише СОРВ, функціонал яких доповнено інструментами контролю співробітників, які працюють за ПК. І тут поза конкуренцією програма Kickidler, оскільки серед усього доступного на ринку ПЗ саме вона має найбільший набір інструментів для моніторингу працівників та їх дій.

Винахідливість несумлінних співробітників у прагненні до скоєння корпоративних злочинів не можна недооцінювати. Вони регулярно винаходять нові методи обходу уваги ПЗ для контролю та блокування руху інформації. Але можливі проломи у захисті можна закрити, контролюючи як рух корпоративних даних, а й дії самого працівника.

Kickidler з його функціями запису відео з моніторів співробітників, кейлоггера, онлайн-моніторингу та контролю часу перебування за ПК у цьому відношенні дуже гарний. До речі, компанія має реальний кейс з виявлення інсайдера, що краде клієнтську базу, що підтверджує ефективність такого контролю.

До речі, співробітник, знаючи, що кожна його дія реєструється та зберігається, зі значно меншою ймовірністю спробує викрасти дані або вчинити інший корпоративний злочин. Особливо з урахуванням того, що суперечливі або спірні моменти можна уточнити на підставі показників відразу кількох інструментів (наприклад, перевіривши дані кейлоггера та запис відео з екрана).

Основні можливості:

- онлайн-моніторинг ПК працівників – можливість дивитися екрани працівників у реальному часі;
- кейлоггер – запис усіх натискань на клавіатуру;
- запис відео – у безперервному режимі записується відеосигнал із екрана співробітника;
- реєстрація часу початку та завершення роботи, а також пауз та простоїв;
- віддалений доступ до пк працівників;
- автосповіщення про порушення на робочому місці – нагадування про постійний контроль для попередження серйозних провин.

Недоліки:

- відсутність мобільних версій;
- відсутність інтеграції із хмарними сервісами.

ПЗ доступне у безкоштовній версії (підключення до 6 ПК). Доступний 2-тижневий безкоштовний тестовий період для повної версії. Вартість ліцензії – 4 долари на місяць за кожен підключений ПК.

Підбиваючи підсумки, SIEM-система контролює інформацію, шукає загрози та попереджає про них. DLP-система контролює обмін даними та перешкоджає їх крадіжці. ПЗ для захисту документів виключає можливість їх крадіжки будь-яким способом. Корпоративний антивірус протидіє шкідливого ПЗ. СУРВ контролює поведінку та дії співробітників. А разом усі ці системи складають надійний контур кібер-безпеки, який у такій конфігурації пробити практично неможливо.

4. РОЗРОБКА ТА ПОБУДОВА КОРПОРАТИВНОЇ МЕРЕЖІ

Вихідні дані прийняті для прикладу виконання даної курсової роботи:

1) Кількість робочих станцій мережі – $N = 45$;

2) Кількість підмереж робочих станцій – $H = 8$;

3) Доступний адресний простір для підмереж маршрутизаторів S_R –10.7.0.0/24;

4) Доступний адресний простір для підмереж робочих станцій S_H –192.168.0.0/24;

Топологія ядра мережі представлена на рис.1.

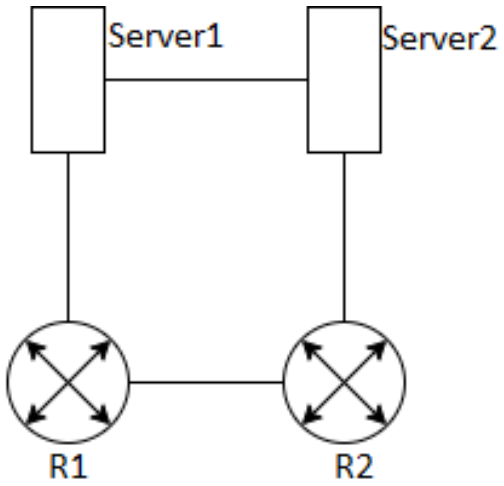

Рисунок 1 – Топологія ядра єдиної мережі передачі даних

4.1 Розподіл підмереж робочих станцій SH єдиної мережі передачі даних

Згідно з вихідними даними, єдина мережа передачі даних має забезпечити роботу як мінімум 45 робочих станцій (N = 45), які треба розділити на 8 підмереж.

4.2 Побудова графа єдиної мережі передачі

Розподіливши робочі станції за підмережами, починається с додавання графа єдиної мережі передачі даних.

Об'єднання всіх робочих пристроїв у кожній з підмереж буде здійснюватися за допомогою некерованого L2-комутатора (комутатор Cisco Catalyst WS-C2960-24) з 24 фізичними портами FastEthernet.

Кожна робоча станція підключається до комутатора за допомогою кабелю UTP (некранована кручена пара) категорії 5, утворюючи сегментоване повнодуплексне підключення.

З 24 фізичних портів комутатора частина портів використовується для об'єднання робочих станцій і один порт для підключення до маршрутизатора R ядра єдиної мережі передачі даних.

Порти комутатора, що залишилися, можна використовувати для ка-скадного підключення іншого комутатора при можливому розширенні підмережі або як технічний резерв, в нашому випадку всі технічні засоби залишаються під резерв. З метою техніки безпеки їх слід відключити за допомогою інтерфейсу командного рядка (Command Line Interface, CLI).

Згідно з вихідним графом єдиної мережі передачі даних, експлуатаційне навантаження мережі має забезпечувати 2 маршрутизатори R. Кожен із даних маршрутизаторів має по 10 інтерфейсів FastEthernet. Коректна маршрутизація пакетів між будь-якими підмережами надійно забезпечуватиметься за наявності 8 підмереж. Головним фактором належної роботи мережі передачі даних є стабільна робота обох маршрутизаторів, вони обслуговують не тільки свою підмережу, а також є транзитним вузлом для зв'язку з іншими підмережами (дані підмережі з'єднані за допомогою відповідних маршрутизаторів).

А також у мережі є 2 маршрутизатори R, для бездротового сегмента мережі, маршрутизатор WRT300N – Work призначений для підключення бездротових пристроїв працівників до мережі, крім робочої бездротової мережі, є

другий маршрутизатор WRT300N – Visitors який призначений для підключення бездротових пристроїв гостей. WRT300N використовує технологію Wi-Fi для передачі сигналу бездротовим шляхом

Розширений граф єдиної мережі передачі представлений на рис.2. На графі єдиної мережі передачі даних нанесені такі літерно-цифрові найменування:

– H1-H51 – робочі станції єдиної мережі передачі;
– R1-R2 – маршрутизатори єдиної мережі передачі;
– R3-R4–бездротові маршрутизатори єдиної мережі передачі;
– SW1-SW8 – комутатори підмережі робочих станцій.

На графі також позначені відповідні номери інтерфейсів маршрутів-пробок

R та порти комутаторів SW.

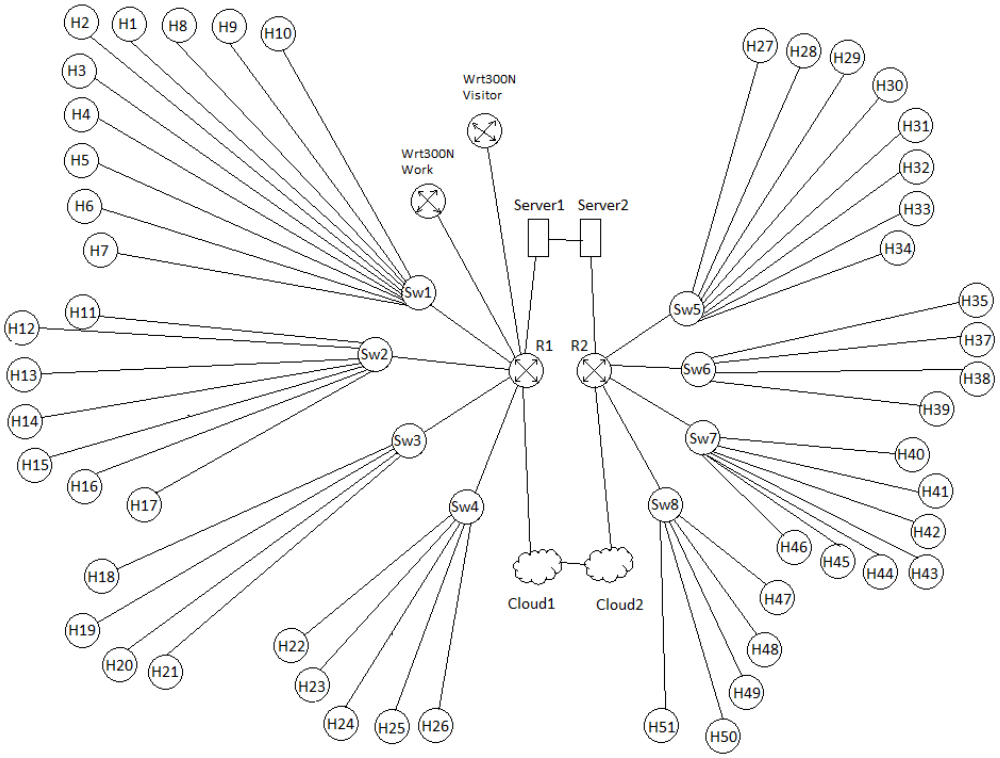

Рисунок 2 – Розширений граф єдиної мережі передачі даних

4.3 Список технічних засобів

За отриманим графом єдиної мережі передачі даних можна підрахувати загальну кількість технічних засобів, що витрачаються: комп'ютерів, маршрутизаторів і т.д. Для коректного функціонування мережі, що проектується, необхідний наступний набір обладнання:

1) 4 маршрутизатори (2 маршрутизатори з 10 інтерфейсами FastEthernet, а також 2 маршрутизатори бездротових);

2) 8 некерованих комутаторів (24 фізичних портів на кожному пристрої, повнодуплекс, автоузгодження), що підтримують мережу FastEthernet на кабелі UTP5e;

3) по 1 мережній карті на кожну робочу станцію (51 мережева карта стандарту FastEthernet, повнодуплекс, автоузгодження);

4) Бездротова точка доступу (WiFi AP), що підтримує стандарти 802.11b/g/n;

5) Опорна технологія мережі FastEthernet 100Мбі/с, тип ліній зв'язку між усіма пристроями – неекранована кручена пара.

4.4 План IP-адресації підмереж робочих станцій SH

Для адресації підмереж робочих станцій SH виділено адресний простір мережі 192.168.0.0/24. IP-адреса (24+4=28 біт). Виділена мережа 192.168.0.0/28 використовує 2 байти для адресації мережі, що залишилися 2 байти вільні. Запис мережі в двійковій нотації виглядатиме:

192.168.0.0 – 11000000.10101000.0000000.00000000

255.255.255.0 – 11111111.11111111.11111111.00000000

До цього слід враховувати, що кожна підмережа підключається до відповідного маршрутизатора єдиної мережі передачі даних. Тому для коректної маршрутизації та обміну інформацією між вузлами підмережі потрібно 14 IP-адрес на кожну підмережу робочих станцій SH, з яких деяка кількість IP-адрес

призначаються відповідним комп'ютерам, а одна IP-адреса призначається маршрутизатору R, підключеному через вказаний інтерфейс до даної підмережі. Крім цього, не слід також забувати про необхідність наявності адреси самої підмережі та широкомовної адреси та обліку резервних адрес.

Для адресації 8 вузлів достатньо 4 біти необхідно використовувати 4 біти, які дозволять адресувати 16 вузлів (24 = 16 IP-адрес). Додаткові адреси можна використовувати під час розширення підмережі або як резерв.

Використовуючи нотацію CIDR та безперервне виділення блоків IP-підмереж, виділимо 8 IP-підмереж з 16 доступними IP-адресами в кожній підмережі. Слід пам'ятати, що перші 2 байти мережі 192.168.0.0/28 не зміняться, а для виділення підмереж можна використовувати тільки останні 2 байти. Застосуємо маску підмережі довжиною 28 біт (32-4=28 біт адресації мережі, 4 біта адресації вузлів).

Таблиця 1 – Адресація під мереж робочих станцій S_H

Підмережа	Пул IP-адрес	Двійкова нотація	Призначення
S_H1	192.168.0.0\28	11000000.10101000.00000000.00000000	Адреса підмережі
	255.255.255.240	11111111.11111111.11111111.11110000	Маска підмережі
	192.168.0.1	11000000.10101000.00000000.00000001	R1, інтерфейс 2
	192.168.0.2	11000000.10101000.00000000.00000010	H1
	192.168.0.3	11000000.10101000.00000000.00000011	H2
	192.168.0.4	11000000.10101000.00000000.00000100	H3
	192.168.0.5	11000000.10101000.00000000.00000101	H4
	192.168.0.6	11000000.10101000.00000000.00000110	H5
	192.168.0.7	11000000.10101000.00000000.00000111	H6
	192.168.0.8	11000000.10101000.00000000.00001000	H7
	192.168.0.9	11000000.10101000.00000000.00001001	H8
	192.168.0.10	11000000.10101000.00000000.00001010	H9
	192.168.0.11	11000000.10101000.00000000.00001011	H10
	192.168.0.12	11000000.10101000.00000000.00001100	Резерв

	……		
	192.168.0.14	11000000.10101000.00000000.00001110	Резерв
	192.168.0.15	11000000.10101000.00000000.00001111	Широкомов. адр.
S_H2	192.168.0.16\28	11000000.10101000.00000000.00010000	Адреса підмережі
	255.255.255.240	11111111.11111111.11111111.11110000	Маска підмережі
	192.168.0.17	11000000.10101000.00000000.00010001	R1, інтерфейс 3
	192.168.0.18	11000000.10101000.00000000.00010010	H1
	192.168.0.19	11000000.10101000.00000000.00010011	H2
	192.168.0.20	11000000.10101000.00000000.00010100	H3
	192.168.0.21	11000000.10101000.00000000.00010101	H4
	192.168.0.22	11000000.10101000.00000000.00010110	H5
	192.168.0.23	11000000.10101000.00000000.00010111	H6
	192.168.0.24	11000000.10101000.00000000.00011000	H7
	192.168.0.25	11000000.10101000.00000000.00011001	Резерв
	……		
	192.168.0.30	11000000.10101000.00000000.00011110	Резерв
	192.168.0.31	11000000.10101000.00000000.00011111	Широкомов. адр.
S_H3	192.168.0.32	11000000.10101000.00000000.00100000	Адреса підмережі
	255.255.255.240	11111111.11111111.11111111.11110000	Маска підмережі
	192.168.0.33	11000000.10101000.00000000.00100001	R1, інтерфейс 4
	192.168.0.34	11000000.10101000.00000000.00100010	H1
	192.168.0.35	11000000.10101000.00000000.00100011	H2
	192.168.0.36	11000000.10101000.00000000.00100100	H3
	192.168.0.37	11000000.10101000.00000000.00100101	H4
	192.168.0.38	11000000.10101000.00000000.00100110	Резерв
	……..		
	192.168.0.46	11000000.10101000.00000000.00101110	Резерв
	192.168.0.47	11000000.10101000.00000000.00101111	Широкомов. адр.
	192.168.0.48	11000000.10101000.00000000.00110000	Адреса підмережі
	255.255.255.240	11111111.11111111.11111111.11110000	Маска підмережі
	192.168.0.49	11000000.10101000.00000000.00110001	R1, інтерфейс 5
	192.168.0.50	11000000.10101000.00000000.00110010	H1
	192.168.0.51	11000000.10101000.00000000.00110011	H2

S_H4	192.168.0.52	11000000.10101000.00000000.00110100	Н3
	192.168.0.53	11000000.10101000.00000000.00110101	Н4
	192.168.0.54	11000000.10101000.00000000.00110110	Н5
	192.168.0.55	11000000.10101000.00000000.00110111	Резерв
	……..		
	192.168.0.62	11000000.10101000.00000000.00111110	Резерв
	192.168.0.63	11000000.10101000.00000000.00111111	Широкомов. адр.
S_H5	192.168.0.64	11000000.10101000.00000000.01000000	Адреса підмережі
	255.255.255.240	11111111.11111111.11111111.11110000	Маска підмережі
	192.168.0.65	11000000.10101000.00000000.01000001	R2, інтерфейс 2
	192.168.0.66	11000000.10101000.00000000.01000010	Н1
	192.168.0.67	11000000.10101000.00000000.01000011	Н2
	192.168.0.68	11000000.10101000.00000000.01000100	Н3
	192.168.0.69	11000000.10101000.00000000.01000101	Н4
	192.168.0.70	11000000.10101000.00000000.01000110	Н5
	192.168.0.71	11000000.10101000.00000000.01000111	Н6
	192.168.0.72	11000000.10101000.00000000.01001000	Н7
	192.168.0.73	11000000.10101000.00000000.01001001	Н8
	192.168.0.74	11000000.10101000.00000000.01001010	Резерв
	……..		
	192.168.0.78	11000000.10101000.00000000.01001110	Резерв
	192.168.0.79	11000000.10101000.00000000.01001111	Широкомов. адр.
S_H6	192.168.0.80	11000000.10101000.00000000.01010000	Адреса підмережі
	255.255.255.240	11111111.11111111.11111111.11110000	Маска підмережі
	192.168.0.81	11000000.10101000.00000000.01010001	R2, інтерфейс 3
	192.168.0.82	11000000.10101000.00000000.01010010	Н1
	192.168.0.83	11000000.10101000.00000000.01010011	Н2
	192.168.0.84	11000000.10101000.00000000.01010100	Н3
	192.168.0.85	11000000.10101000.00000000.01010101	Н4
	192.168.0.86	11000000.10101000.00000000.01010110	Резерв
	……		
	192.168.0.94	11000000.10101000.00000000.01011110	Резерв
	192.168.0.95	11000000.10101000.00000000.01011111	Широкомов. адр.

S_H7	192.168.0.96	11000000.10101000.00000000.01100000	Адреса підмережі
	255.255.255.240	11111111.11111111.11111111.11110000	Маска підмережі
	192.168.0.97	11000000.10101000.00000000.01100001	R2, інтерфейс 4
	192.168.0.98	11000000.10101000.00000000.01100010	H1
	192.168.0.99	11000000.10101000.00000000.01100011	H2
	192.168.0.100	11000000.10101000.00000000.01100100	H3
	192.168.0.101	11000000.10101000.00000000.01100101	H4
	192.168.0.102	11000000.10101000.00000000.01100110	H5
	192.168.0.103	11000000.10101000.00000000.01100111	H6
	192.168.0.104	11000000.10101000.00000000.01101000	H7
	192.168.0.105	11000000.10101000.00000000.01101001	Резерв
	……		
	192.168.0.110	11000000.10101000.00000000.01101110	Резерв
	192.168.0.111	11000000.10101000.00000000.01101111	Широкомов. адр.
S_H8	192.168.0.112	11000000.10101000.00000000.01110000	Адреса підмережі
	255.255.255.240	11111111.11111111.11111111.11110000	Маска підмережі
	192.168.0.113	11000000.10101000.00000000.01110001	R2, інтерфейс 5
	192.168.0.114	11000000.10101000.00000000.01110010	H1
	192.168.0.115	11000000.10101000.00000000.01110011	H2
	192.168.0.116	11000000.10101000.00000000.01110100	H3
	192.168.0.117	11000000.10101000.00000000.01110101	H4
	192.168.0.118	11000000.10101000.00000000.01110110	H5
	192.168.0.119	11000000.10101000.00000000.01110111	Резерв
	……		
	192.168.0.126	11000000.10101000.00000000.01111110	Резерв
	192.168.0.127	11000000.10101000.00000000.01111111	Широкомов. адр.

4.5 План IP-адресації підмереж маршрутизаторів SR

Таблиця маршрутизації зазвичай містить:

– адресу мережі або вузла призначення, або вказівку, що маршрут є маршрутом за промовчанням;

- маску мережі призначення (для IPv4-мереж маска /32 (255.255.255.255) дозволяє вказати одиничний вузол мережі);
- шлюз, що позначає адресу маршрутизатора в мережі, на яку необхідно надіслати пакет, що настає до вказаної адреси призначення;
- інтерфейс, через який доступний шлюз (залежно від системи, це може бути порядковий номер, GUID або символьне ім'я пристрою;
- інтерфейс може бути відмінний від шлюзу, якщо шлюз доступний через додатковий мережевий пристрій, наприклад, карту мережі);
- метрику–числовий показник, що задає перевагу маршруту (чим менше число, тим кращий маршрут (інтуїтивно представляється як відстань)).

У таблиці може бути один, а в деяких операційних системах кілька шлюзів за замовчуванням. Такий шлюз використовується в мережах, для яких немає конкретніших маршрутів у таблиці маршрутизації.

Складемо план адресації для підмереж маршрутизаторів SR. Для адресації підмереж SR виділено адресний простір мережі 192.168.10.1/30. . Мережа 192.168.10.0/30 використовує 2 байти для адресації мережі:

192.168.10.0 – 11000000.10101000.00001010.00000000

255.255.255.252 – 11111111.11111111.11111111.11111100

З розширеного графа мережі відомо, що маршрутизація пакетів між будь-якими підмережами забезпечується за наявності 2 IP-підмереж. Використовуючи маршрутизатор R1, можна організувати набір резервних зв'язків між підмережами робочих станцій та підмережами маршрутизаторів мережі. Враховуючи цю пропозицію, використовуємо 2 підмережі маршрутизаторів.

Кожна підмережа маршрутизаторів SR об'єднує по 1 маршрутизатору.

Врахуємо, що перші 2 байти мережі 192.168.10.0/30 не змінюються, а для виділення підмереж можна використовувати тільки останній байт. Застосуємо маску підмережі завдовжки 30 біт (32 – 2 = 30 біт адресації мережі, 2 біта адресації маршрутизаторів).

Таблиця 2 – Адресація під мереж маршрутизаторів S_R

Підмережа S_R	Пул IP-адрес	Двійкова нотація	Призначення
S_R1	192.168.10.0/30	11000000.10101000.00001010.00000000	Адреса підмережі
	255.255.255.252	11111111.11111111.11111111.11111100	Маска підмережі
	192.168.10.1	11000000.10101000.00001010.00000001	R1, інтерфейс 9/0
	192.168.10.2	11000000.10101000.00001010.00000010	Широкомовна адреса
S_R2	192.168.10.3/30	11000000.10101000.00001010.00000011	Адреса підмережі
	255.255.255.252	11111111.11111111.11111111.11111100	Маска підмережі
	192.168.10.4/30	11000000.10101000.00001010.00000100	R2, інтерфейс 9/0
	192.168.10.5	11000000.10101000.00001010.00000101	Широкомовна адреса

4.6 Маршрутизація пакета

Маршрутизація пакетів відбувається за допомогою IP адрес. Маршрутизація здійснюється в кінцевих пристроях, що посилають TCP/IP, і в маршрутезаторах. В обох випадках на інтернет-рівні кінцеві пристрої та маршрутизатори повинні приймати рішення, куди відсилати пакет. Для вирішення цього завдання інтернет-рівень отримує інформацію зі спеціальних таблиць маршрутеризації. Записи в таблиці створюються автоматично при ініціалізації цього TCP/IP, і це можна зробити і вручну.

При доставці IP пакетів можливі два варіанти доставки:

- пряма доставка (Direct delivery), це коли один IP кінцевий пристрій посилає пакети іншому пристрою, що належить тому самому сектору, за допомогою MAC адресу приймаючого пристрою;
- непряма доставка (Indirect delivery) вона відбувається через проміжні установки або маршрутизатори до мети, яка не відноситься до сектора локальної мережі. У цьому випадку комп'ютер, що посилає, адресує пакет даних, використовуючи MAC адресу маршрутизатора.

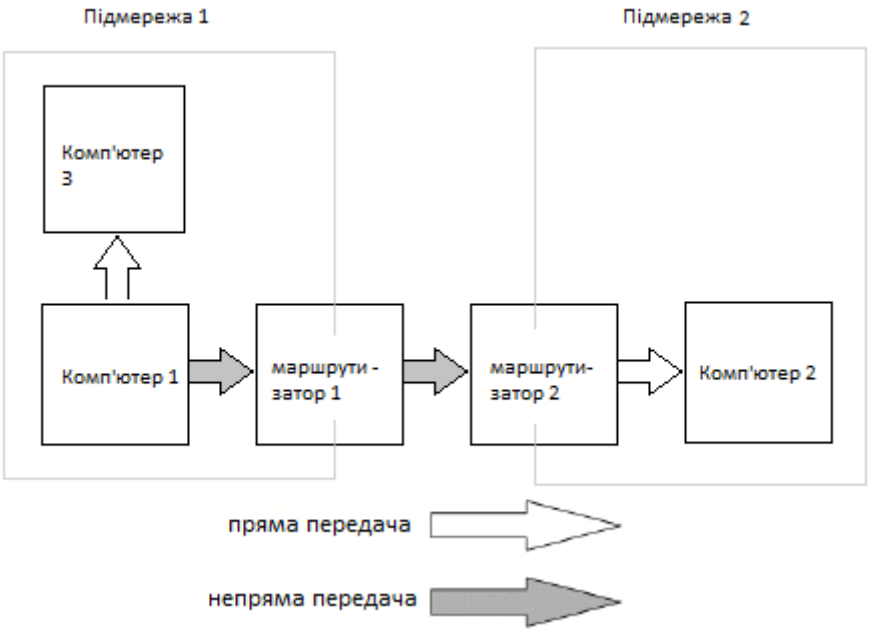

Рисунок 3 – Різні варіанти маршрутизації

Таблиця машрутизації є у всіх IP кінцевих пристроях. Така таблиця містить інформацію про IP мереж призначення і як пакети можуть бути доставлені в ці мережі та різні оцінки, завдяки яким на інтернет-рівні можна прийняти рішення про найбільш доцільний шлях доставки.

Візьмемо довільний комп'ютер, наприклад, пристрій з IP-адресою 192.168.0.3, який знаходиться в одній із сусідніх поосетей 192.168.0.1/28. Взлом призначення довільно призначимо робочу станцію з IP-адресою

192.168.0.50 з іншої підмережі підмережі 192.168.0.49/28

Згідно умови покажу, що мережею відправника дійсно є вказана мережа, зробивши множення IP-адреси відправника та маски підмережі відправника:

192.168.0.3 – 11000000.10101000.0000000.00000011

255.255.255.240 – 11111111.11111111.11111111.11110000

192.168.0.1 – 11000000.10101000.0000000.00000001

Дійсно IP-адреса належить вказаній мережі.

Накладемо маску підмережі на IP-адресу відправника і перевіримо, чи належить ця IP-адреса тієї ж мережі:

192.168.0.50 – 11000000.10101000.0000000.00110010

255.255.255.240 – 1111 1111.1111 1111.1111 1111.1111 0000

192.168.0.49 – 11000000.10101000.0000000.00110001

IP-адреса одержувача належить іншій мережі. Тобто підсіти відправника та підсіти одержувачі не співпадають, отже необхідно маршрутизувати пакет.

4.7 Налаштування VLAN на комутаторах

Локальні мережі давно перестали складатися з кількох абонентських пристроїв, які розташовані всередині одного приміщення. Сучасні мережі підприємств є розподілені системи, які з більшої кількості пристроїв різного призначення. Ситуація змушує розділяти такі великі мережі на автономні підмережі, у результаті логічні структури мережі від фізичних топологій. Подібні системи створюються за допомогою технології VLAN.

Технологія VLAN забезпечує:

Гнучка побудова мережі – VLAN дозволяє зробити сегментацію локальної мережі на підмережі за функціональною ознакою незалежно від територіального розташування пристроїв. Тобто, пристрої однієї підмережі VLAN можуть бути підключені до різних комутаторів, віддалених один від одного. І навпаки, до одного комутатора можуть бути підключені пристрої, що належать до різних підмереж VLAN

Збільшення продуктивності – VLAN поділяє підсіть на окремі широкомовні домени. Це означає, що широкомовні повідомлення будуть отримувати лише пристрої, що знаходяться в одній мережі VLAN. Побудова системи з використанням технології VLAN дозволяє зменшити широкомовний трафік усередині мережі, тим самим знижується навантаження на мережні пристрої та покращується продуктивність системи загалом.

Покращення безпеки – Пристрої з різних підмереж VLAN не можуть спілкуватися один з одним, що зменшує шанси на несанкціонований доступ до пристроїв системи. Зв'язок між різними підмережами можливий лише через маршрутизатор. Крім того, використання маршрутизатора дозволяє настроїти

політики безпеки, які можуть бути застосовані відразу до всієї групи пристроїв, що належать до однієї підмережі.

Кожна VLAN-підмережа має свій ідентифікатор, за яким визначається належність тієї чи іншої підмережі. Інформація про ідентифікатор міститься в тезі, який додається в тіло Ethernet-фрейму мережі, в якій введено розділення на підмережі VLAN.

Найпоширеніший стандарт, який описує процедуру тегування трафіку, – це відкритий стандарт 802.1 Q. Крім нього є пропрієтарні протоколи, але менш популярні.

Формат Ethernet – кадр після тегування (рис.4).

Рисунок 4 – Кадр після тегування

Access-port – порт доступу, який передає нетегований трафік. Використовується для підключення кінцевих пристроїв, які не підтримують технологію VLAN.

Тип Access призначається порту комутатора, якого підключено або одиничний абонентський пристрій, або група пристроїв, що у однієї підмережі. Крім вибору режиму роботи порту Access, необхідно вказати ідентифікатор VLAN-підмережі, до якої належатиме обладнання, що знаходиться за цим портом.

Комутатор, отримавши в порт Access дані від підключених до нього абонентських пристроїв, додасть всім Ethernet-кадрам загальний тег із заданим ідентифікатором підмережі і далі оперуватиме вже тегованим пакетом. Навпаки, приймаючи з основної мережі дані, призначені Access-порту, комутатор звірить ідентифікатор VLAN пакета з номером VLAN-підмережі цього порту.

Якщо вони співпадуть, дані будуть успішно передані в порт, а тег видалений, таким чином, підключені до порту пристрої продовжать працювати без необхідності підтримки VLAN. Якщо ідентифікатор не дорівнює номеру підмережі, кадр буде відкинуто, не дозволивши передати пакет із «чужої» підмережі VLAN.

Trunk-port – магістральний порт, який передає теговані пакети даних. Використовується для підключення мережевих пристроїв із підтримкою VLAN, найчастіше для з'єднання комутаторів між собою.

Крім завдання режиму роботи та ідентифікатора VLAN, при конфігуруванні Trunk-портів створюється список дозволених для передачі підмереж VLAN, з яким комутатор звіряється при отриманні пакетів. Завдяки цьому через Trunk-порти можуть передаватися пакети кількох VLAN-підмереж.

Комутатор, отримавши порт Trunk нетегированные дані, надійде аналогічно Access-порту, тобто. промаркує пакети ідентифікатором VLAN-підмережі, який присвоєний цьому порту, і передасть далі в мережу. При отриманні пакета з таким же ідентифікатором VLAN, як і в порту, тег буде знято і дані відправлені на абонентський пристрій без тега. У разі отримання тегованого пакета з ідентифікатором VLAN, який відрізняється від номера, присвоєного порту, комутатор порівняє ідентифікатор зі списком дозволених VLAN-підмереж. Якщо номер буде вказано у списку, дані будуть передані по мережі на наступний пристрій без зміни тега. У випадку, якщо ідентифікатор вказує на належність незнайомої підмережі VLAN, пакет буде відкинуто.

У кваліфікаційному проекті був створен VLAN для відділу кадрів та відділу бухгалтерії, для того щоб вони могли взаємодіяти між собою та безпечно передавати дані див.рис.5

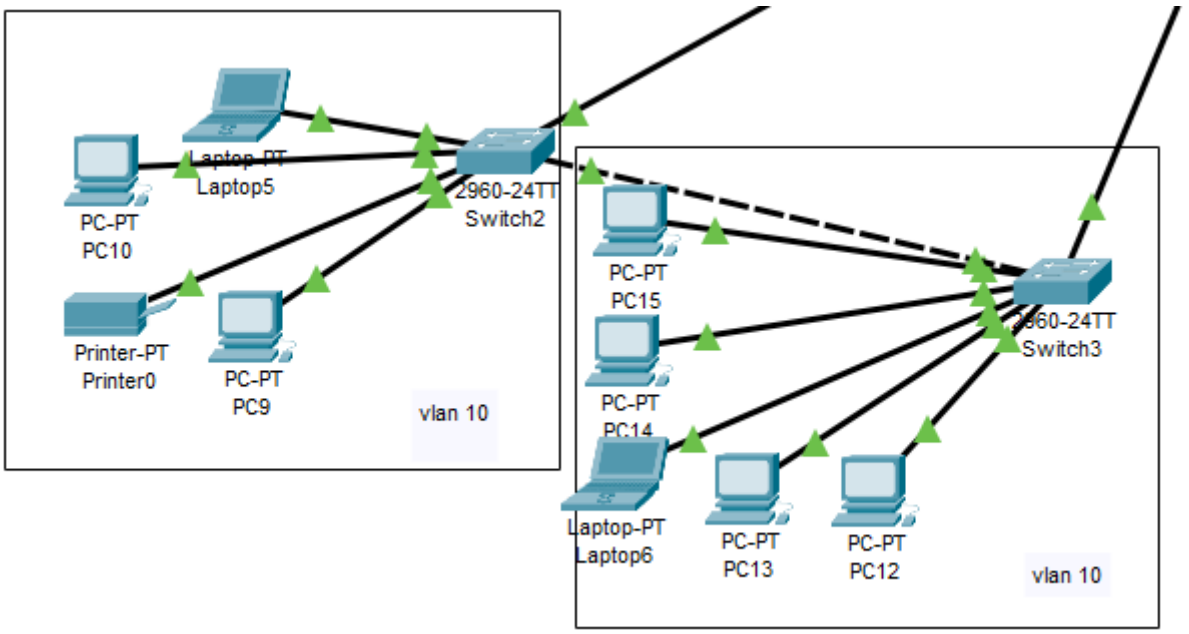

Рисунок 5 – окремий VLAN

4.8 Організація бездротового доступу до комп'ютерної мережі передачі даних

Для забезпечення бездротового доступу до інформаційно-обчислювальних ресурсів проектованої мережі необхідно підключити бездротову точку доступу, що організує міст між провідною мережею Ethernet і бездротовою зоною WiFi. При проектуванні мережі, зображеної на рис.2, були використані 10-портові комутатори FastEthernet, на кожному з яких один фізичний порт зарезервований для розширення. Таким чином підключення точки доступу можна зробити до будь-якого комутатора SWi мережі. У такому випадку бездротові станції можуть використовувати резервні IP-адреси з кожного діапазону (див.табл.2). Таке рішення досить просто при реалізації, але має ряд помітних недоліків: обмежений адресний простір, складність контролю доступу бездротових клієнтів, змішання мережевого трафіку від довірених станцій і тимчасових клієнтів. З цих наведених причин буде інший варіант структуризації мережі бездротового доступу.

Враховуючи територіальне розташування об'єктів мережі та ступінь концентрації бездротових станцій у центральній області, найбільш доцільним видається підключення точки доступу до окремого інтерфейсу (6 та 7) маршрутизатора R1.

Буде дві бездротові мережі, одна для робітників, а друга для відвідувачів. Виходячи з розрахунків проведених у попередніх розділах, адресний простір мережі, що проектується, має достатню глибину, для виділення окремої IP-підмережі, призначеної для організації доступу бездротових клієнтів. Припускаючи наявність одночасно не більше 50 бездротових клієнтів у зоні доступу можна розрахувати діапазон адресного простору.

Таблиця 3 – Адресація бездротового сегмента мережі для працівників

Пул IP-адрес	**Двійкова нотація**	**Призначення**
192.168.1.0/24	11000000.10101000.00000001.00000000	Адреса підмережі
255.255.255.0	11111111.11111111.11111111.00000000	Маска підмережі
192.168.1.1	11000000.10101000.00000001.00000001	R1, інтерфейс Fa6/0
192.168.1.2	11000000.10101000.00000001.00000010	Точка доступу
192.168.1.100	11000000.10101000.00000001.01100100	Бездрот. клієнт 1
192.168.1.101	11000000.10101000.00000001.01100101	Бездрот. клієнт 2
192.168.1.102	11000000.10101000.00000001.01100110	Бездрот. клієнт 3
192.168.1.103	11000000.10101000.00000001.01100111	Бездрот. клієнт 4
192.168.1.104	11000000.10101000.00000001.01101000	Бездрот. клієнт 5
192.168.1.105	11000000.10101000.00000001.01101001	Бездрот. клієнт 6
192.168.1.106	11000000.10101000.00000001.01101010	Бездрот. клієнт 7
192.168.1.107	11000000.10101000.00000001.01101011	Бездрот. клієнт 8
192.168.1.108	11000000.10101000.00000001.01101100	Бездрот. клієнт 9
192.168.1.109	11000000.10101000.00000001.01101101	Бездрот. клієнт 10
192.168.1.110	11000000.10101000.00000001.01101111	Бездрот. клієнт 11
……		
192.168.1.149	11000000.10101000.00000001.10010101	Бездрот. клієнт 50
192.168.1.150	11000000.10101000.00000001.10010111	Широкомовна адреса

Таблиця 4 – Адресація бездротового сегмента мережі для відвідувачів

Пул IP-адрес	**Двійкова нотація**	**Призначення**
192.168.2.0/24	11000000.10101000.00000010.00000000	Адреса підмережі
255.255.255.0	11111111.11111111.11111111.00000000	Маска підмережі
192.168.2.1	11000000.10101000.00000010.00000001	R1, інтерфейс Fa6/0
192.168.2.2	11000000.10101000.00000010.00000010	Точка доступу
192.168.2.100	11000000.10101000.00000010.01100100	Бездрот. клієнт 1
192.168.2.101	11000000.10101000.00000010.01100101	Бездрот. клієнт 2
192.168.2.102	11000000.10101000.00000010.01100110	Бездрот. клієнт 3
192.168.2.103	11000000.10101000.00000010.01100111	Бездрот. клієнт 4
192.168.2.104	11000000.10101000.00000010.01101000	Бездрот. клієнт 5
192.168.2.105	11000000.10101000.00000010.01101001	Бездрот. клієнт 6
192.168.2.106	11000000.10101000.00000010.01101010	Бездрот. клієнт 7
192.168.2.107	11000000.10101000.00000010.01101011	Бездрот. клієнт 8
192.168.2.108	11000000.10101000.00000010.01101100	Бездрот. клієнт 9
192.168.2.109	11000000.10101000.00000010.01101101	Бездрот. клієнт 10
192.168.2.110	11000000.10101000.00000010.01101111	Бездрот. клієнт 11
……	……	……
192.168.2.149	11000000.10101000.00000010.10010101	Бездрот. клієнт 50
192.168.2.150	11000000.10101000.00000010.10010111	Широкомовна адреса

У табл.5-6 зведені основні дані конфігурації бездротової точки доступу: ідентифікатор бездротової мережі, частотний діапазон, спосіб шифрування, секретна фраза та ін.

Таблиця 5– Конфігурація бездротової точки доступу для працівників

Параметр	Значення
Місце включення	R1, інтерфейс 6
IP-адреса	192.168.1.1
Адресний простір	192.168.1.150/24
MAC-адреса точки доступу	BF:CC:1A:1E:AA:09
Підтрим. стандарти	802.11b/g/n, 2.4, 2.5, 5 GHz
Аутентифікація	WPA-PSK
SSID	EKSPD

Таблиця 6 – Конфігурація бездротової точки доступу для відвідувачів

Параметр	Значення
Місце включення	R1, інтерфейс 7
IP-адреса	192.168.2.1
Адресний простір	192.168.2.150/24
MAC-адреса точки доступу	FT:C5:2C:1E:3T:08
Підтрим. стандарти	802.11b/g/n, 2.4, 2.5, 5 GHz
Аутентифікація	WPA-PSK
SSID	EKSPD

4.9 Готовий проект

Готова топологія циско наведена рис. 6.

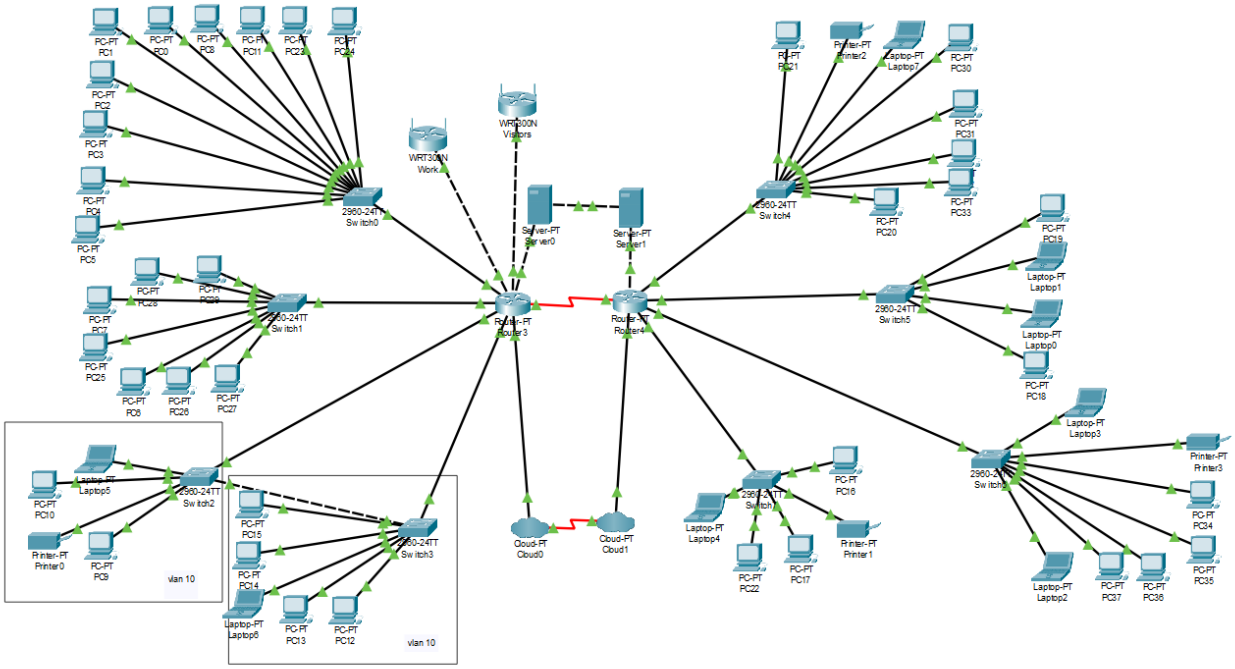

Рисунок 6 – Топологія Cisco

На рис. 7 показано приклад виконання команди ping від PC2 до PC30 який знаходиться в іншій підмережі, пакети відправлені успішно.

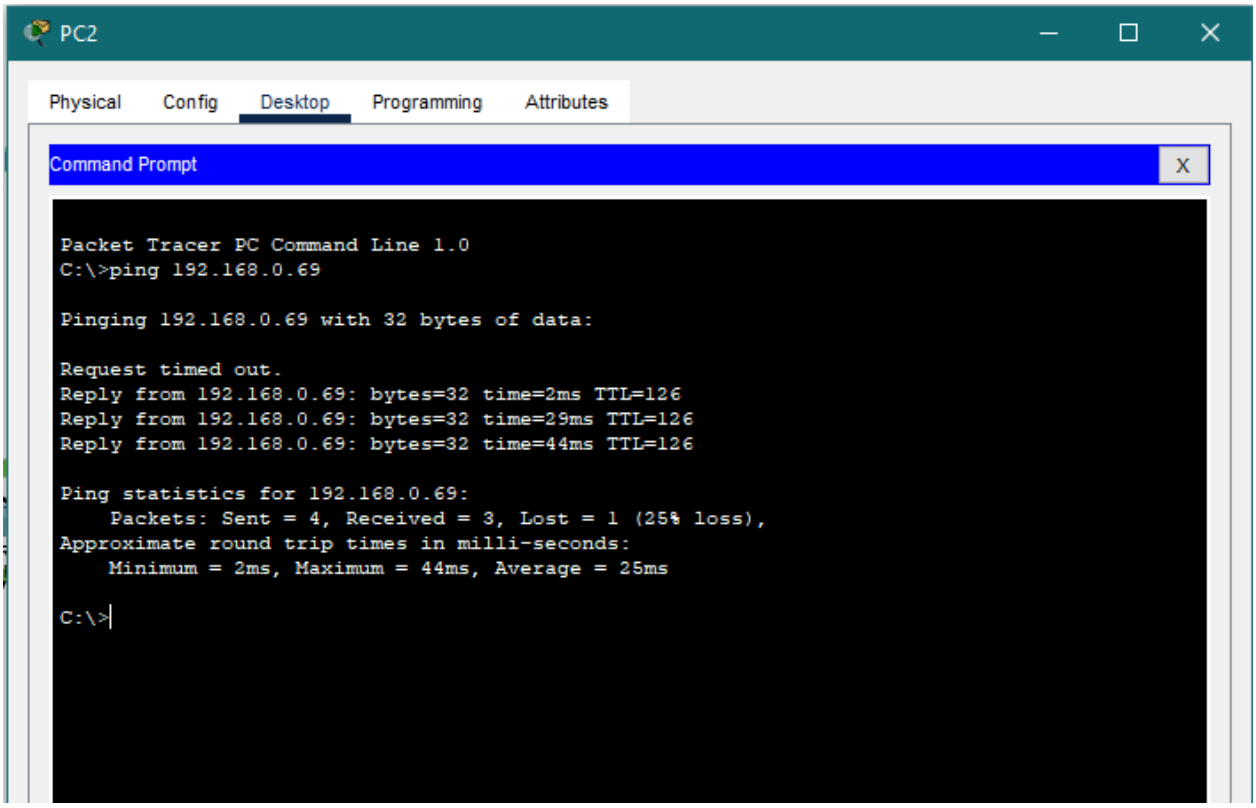

Рисунок 7 – Ping між PC2 до PC30

Виконуємо команду tracert, яка показує трасування маршруту до вказаного віддаленого хоста. У ході трасування буде показано весь маршрут проходження пакетів (див. рис 8).

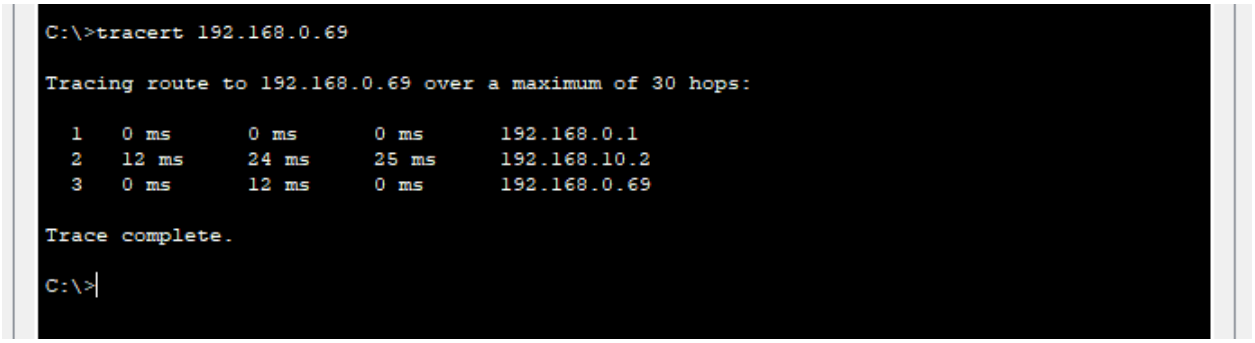

Рисунок 8 – Tracert між PC2 до PC30

ВИСНОВКИ

На сьогоднішній день розробка та впровадження локальних інформаційних систем є одним із найцікавіших та найважливіших завдань у галузі інформаційних технологій. Виникає потреба у використанні нових технологій передачі. Інтенсивне використання інформаційних технологій вже зараз є найсильнішим аргументом у конкурентній боротьбі, що розгорнулася на світовому ринку.

Безпека мережі – це широкий термін, який охоплює безліч технологій, пристроїв і процесів. Простіше кажучи, це набір правил і конфігурацій, призначених для захисту цілісності, конфіденційності та доступності комп'ютерних мереж і даних за допомогою програмних і апаратних технологій. Кожній організації, незалежно від розміру, галузі чи інфраструктури, потрібен певний рівень мережевих рішень, щоб захистити її від кіберзагроз.

Сучасна мережева архітектура є складною і стикається з середовищем загроз, яке постійно змінюється, і зловмисниками, які завжди намагаються знайти та використати вразливі місця. Ці вразливості можуть існувати в багатьох областях, включаючи пристрої, дані, програми, користувачів і місця розташування. З цієї причини сьогодні використовується багато інструментів і програм керування безпекою мережі, які вирішують окремі загрози та експлойти, а також невідповідність нормативним вимогам. Коли лише кілька хвилин простою можуть спричинити масові зриви та серйозну шкоду прибутку та репутації організації, важливо, щоб ці заходи захисту були на місці.

Вирішуючи питання безпеки мережі в організації, слід враховувати багато рівнів. Атаки можуть відбуватися на будь-якому рівні в моделі рівнів безпеки мережі, тому обладнання, програмне забезпечення та політики безпеки мережі повинні бути розроблені для кожної області.

Безпека мережі зазвичай складається з трьох різних елементів контролю: фізичного, технічного та адміністративного.

Під час виконання кваліфікаційної роботи бакалавра були розглянуті

питання організації локальної обчислювальної мережі, проектування топології для подальшої реалізації в організації та методи захисту даних при побудові комп’ютерної мережі.

Безпека мережі має бути пріоритетом для будь-якої організації, яка працює з мережевими даними та системами. На додаток до захисту активів і цілісності даних від зовнішніх експлойтів, мережева безпека може також ефективніше керувати мережевим трафіком, підвищити продуктивність мережі та забезпечити безпечний обмін даними між співробітниками та джерелами даних. Існує багато доступних інструментів, програм та утиліт, які можуть допомогти захистити мережу від атак і непотрібних простоїв.

Були поставлені та успішно вирішені завдання вибору мережевої архітектури, конфігурації мережного обладнання, розглянуті питання управління мережевими ресурсами та користувачами мережі, питання безпеки мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Поняття і види комп'ютерних мереж. URL: http://ni.biz.ua/9/9_6/9_68246_ponyatie-i-vidi-kompyuternih-setey.html (дата звернення: 12.05.2022)
2. Cisco Packet Tracer. URL: https://en.wikipedia.org/wiki/Packet_Tracer (дата звернення: 12.05.2022)
3. Задачи и уровни обеспечения защиты информации. URL: https://studbooks.net/2271473/informatika/zadachi_urovni_obespecheniya_zaschity_informatsii (дата звернення: 01.03.2022)
4. Как повысить безопасность компьютерной и беспроводной сети. URL: https://windows-school.ru/publ/winfaq/shifrseti/sposoby_povyshenie_bezopasnosti_kompjuternoj_i_besprovodnoj_seti/8-1-0-76 (дата звернення: 01.03.2022)
5. Программная и аппаратная защита информации. URL: http://detektor.ru/prod/common/protect/ (дата звернення: 01.03.2022)
6. Защита доступа к информации. Программная защита информации URL: http://rus.safensoft.com/security.phtml?c=882 (дата звернення: 01.03.2022)
7. Что такое брандмауэр и зачем он нужен. URL: https://ru.safetydetectives.com/blog/%D1%87%D1%82%D0%BE-%D1%82%D0%B0%D0%BA%D0%BE%D0%B5-%D0%B1%D1%80%D0%B0%D0%BD%D0%B4%D0%BC%D0%B0%D1%83%D1%8D%D1%80/(дата звернення: 01.03.2022)
8. Информационная безопасность предприятия: ключевые угрозы и средства защиты. URL: https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html (дата звернення: 01.03.2022)
9. Технология VLAN. URL: https://moxa.ru/tehnologii/ethernet_network/tech-vlan/#:~:text=%D0%A2%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F%20VLAN%20%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B8%D0%B2%D0%B0%D0%B5%D1%82%3A,%D0%BD%D0%B5%D0%B7%D0%B0%D0

%B2%D0%B8%D1%81%D0%B8%D0%BC%D0%BE%20%D0%BE%D1%82%20%D1%82%D0%B5%D1%80%D1%80%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE%20%D1%80%D0%B0%D1%81%D0%BF%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F%20%D1%83%D1%81%D1%82%D1%80%D0%BE%D0%B9%D1%81%D1%82%D0%B2 (дата звернення: 01.03.2022)

10. Информационная безопасность предприятия: ключевые угрозы и средства защиты. URL: https://www.smart-soft.ru/blog/informatsionnaja-bezopasnost/ (дата звернення: 07.05.2022)
11. Настройка VLAN на коммутаторах Cisco под управлением IOS. URL: https://linkas.ru/articles/vlan-v-cisco/(дата звернення: 07.05.2022)
12. What are your network diagram needs? URL: https://www.lucidchart.com /pages/network-diagram (дата звернення: 11.05.2022)
13. Інтернет. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82 (дата звернення: 13.05.2022)
14. Wi-Fi. URL: https://uk.wikipedia.org/wiki/Wi-Fi (дата звернення: 15.06.2022)
15. VLAN. URL: https://uk.wikipedia.org/wiki/VLAN (дата звернення: 15.06.2022)
16. DNS. URL: https://uk.wikipedia.org/wiki/DNS-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80 (дата звернення: 15.06.2022)
17. IP-адреса. URL: https://uk.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D0%B0 (дата звернення: 15.06.2022)
18. Інформаційна безпека. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0 (дата звернення: 15.06.2022)