Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Навчально-науковий центр заочної форми навчання*

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

Дослідження методів апаратно-технічного захисту локальної мережі
(тема)

Виконав: студент 2 курсу, групи *ІМІзм-19-2*

Діль А.В
(прізвище, ініціали)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)

Тип програми *освітньо-науковий*

Освітня програма *Інформаційні мережі зв'язку*

Керівник *к.т.н., доц. Золотарьов В.А.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *проф. Безрук В.М.*
(підпис) (прізвище, ініціали)

2021 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ Діль А.В.

Керівник _____ Золотарьов В.А.

Харківський національний університет радіоелектроніки

Факультет *Навчально-науковий центр заочної форми навчання*

Кафедра *Інформаційно-мережної інженерії*

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 Телекомунікації та радіотехніка*
Тип програми *освітньо-наукова*
Освітня програма *Інформаційні мережі зв'язку*

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«25» березня 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Діль Андрію Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження методів апаратно-технічного захисту локальної мережі

затверджена наказом по університету від 25 *березня* 2021 р. № *33 стз*
2. Термін подання студентом роботи до екзаменаційної комісії *16 травня 2021* р.
3. Вихідні дані до роботи: *Об'єкт дослідження – інфокомунікаційна локальна мережа. Провести аналіз найпопулярніших атак на локальні мережі у 2020 р. Розробити модель інформаційних загроз локальній мережі. Розробити стандартні засоби захисту локальної мережі: організаційні, технічні, програмні, апаратно-програмні. Дослідити безпеку мереж зберігання даних: основні типи технологій і інтерфейсов SAN. Розробити алгоритм безпечного підключення локальної мережі до Інтернету. Дослідити та обгрунтувати вибір безпечних методів налаштування маршрутизаторів і точок доступу Wi-Fi для інфокомунікаційної локальної мережі*

4. Перелік питань, що потрібно опрацювати в роботі: *Перелік умовних скорочень. Вступ. 1. Захист інформації в локальних інфокомунікаційних мережах 2. Дослідження мереж зберігання даних 3. Розробка алгоритму безпечного налаштування локальної мережі. 4.Висновки. Перелік використаних джерел. Додаток А: слайди презентації*

5. Перелік графічного матеріалу із зазначенням комп'ютерних ілюстрацій (слайдів)

Слайди у форматі Power Point: *мета роботи; інформаційні ризики використання маршрутизаторів; дослідження методів безпечного налаштування маршрутизаторів і точок доступу Wi-Fi локальної мережі. Переваги та недоліки NAT; переваги та недоліки WWM*

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Основна	*доц. Золотарьов В.А.*		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	26.03.2021	
2	*Аналіз завдання та літературних джерел.*	01.04.2021	
3	*Написання першого розділу*	08.04.2021.	
4	*Написання другого розділу*	15.04.2021	
5	*Написання третього розділу*	28.04.2021	
6	*Написання четвертого розділу*	08.05.2021	
7	*Написання вступу та висновків*	11.05.2021	
8	*Оформлення презентаційного матеріалу та підготовка до захисту у ДЕК*	12.05.2021	

Дата видачі завдання 25 березня 2021 р.

Студент _____ Діль А.В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ к.т.н., доц. Золотарьов В.А.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 94 сторінки, 16 рисунків, 26 таблиць, 75 джерел, 1 додаток

Атестаційна робота присвячена апаратно-технічному захисту сучасних інфокомунікаційних локальних мереж. Проблема вельми актуальна в наш час, оскільки це пов’язано насамперед з забезпеченням безпеки в мережі Інтернет. Заходи безпеки використовують як організації так і окремі користувачі. Це дозволяє персоналу в час пандемії працювати віддалено, не опасаючись витоку інформації. В роботі розроблений алгоритм безпечного доступу в Інтернет. Проведено аналіз існуючих систем контролю управління доступом, наведені типи та рівні мережевої взаємодіє між її блоками. Досліджена безпека мереж зберігання даних. Досліджені методи безпечного налаштування для маршрутизаторів і точок доступу Wi-Fi локальної мережі

ЗАХИСТ ЛОКАЛЬНОЇ МЕРЕЖІ, СПЕЦІАЛІЗОВАНІ МЕРЕЖІ ЗБЕРІГАННЯ ДАНИХ, АПАРАТНО-ПРОГРАМНІ МЕТОДИ ЗАХИСТУ

ABSTRACT

Explanatory note: 94 pages, 16 figures, 16 tables, 57 sources, 1 appendix

Certification work is devoted to modern VPN networks. This problem is very relevant at the present time. This is mainly due to the security of the Internet. Security measures are used by both companies and ordinary users. This allows personnel to work remotely and use company data without fear of information leakage. The aim of the study is to develop an algorithm for the organization of a secure connection of a distributed corporate network to the Internet. The analysis of existing systems of control of access control is conducted, types and levels of network interaction between its blocks are given.

PROTECTION OF LOCAL AREA NETWORK, STORAGE AREA NETWORK

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АРМ – автоматизоване робоче місце
БД – база даних
ІБ – інформаційна безпека
ІТ – інформаційні технології
ЛІКМ – локальна інфокомунікаційна мережа;
НСД – несанкціонований доступ
ПЗ – програмне забезпечення
ПК -персональний комп’ютер
СКУД – система керування доступом
ШПЗ – шкідливе програмне забезпечення
DAS - Direct-attached storage — система зберігання даних з прямим підключенням
LAN - Local Area Network – локальна комп’ютерна мережа
SAN - Storage Area Network – спеціалізовані мережі зберігання
VPN – Virtual Private Network – віртуальні приватні мережі

ВСТУП

Однією з основних проблем при розробці системи безпеки інформації в локальних розподілених мережах стає необхідність зв'язати в одну систему безліч комп'ютерів, серверів, мереж і вузлів. Вибір правильної топології дозволяє мінімізувати кошти, виділені на захист даних.

Топологія системи повинна дозволяти витрачати мінімальні ресурси на обробку критично важливої інформації. Під цим терміном розуміється інформація, необхідна для загального управління мережею, а також інформація з найвищим рівнем секретності. Основною проблемою стає те, що при розробці систем безпеки рідко використовуються засоби криптографічного захисту інформації, так як вони суттєво уповільнюють швидкість обробки даних. Швидкість протікання бізнес-процесів виявляється важливіше, ніж надійний захист даних. Далеко не завжди, навіть при виборі засобів криптографічного захисту, рішення приймається на користь інноваційних технологій, а придбання застарілих не гарантує того, що вони не будуть розшифровані за допомогою більш сучасних і методів.

Ще однією складним завданням при розробці систем безпеки для розподілених мереж стає недостатня підготовка не тільки рядових користувачів, але і системних адміністраторів до роботи з сучасними способами шифрування, архівування, іншими методами захисту інформації.
Архітектура мереж часто є безліч різнорідних елементів, доданих за першої необхідності. Це не дає можливості створити цілісну систему захисту інформації.

Забезпечення безпеки інформації також вимагає виділення додаткових ресурсів на підготовку і навчання персоналу.

Доступ до інформації не може бути надано в рівній мірі кожному користувачеві, це є аксіомою захисту даних в розподілених мережах. Захист від несанкціонованого доступу спрямована на те, щоб убезпечити масиви інформації не тільки від навмисного розкриття, а й від випадкового знищення. З'єднання апаратних, програмних, організаційних заходів захисту має вирішувати задачу збереження даних в повному обсязі.

1 ЗАХИСТ ІНФОРМАЦІЇ В ЛОКАЛЬНИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Завдання захисту від несанкціонованого доступу інформації стає актуальною для багатьох компаній. Відомості, які можуть зацікавити третіх осіб, знаходяться в базах даних і медичних установ, і виробничих підприємств, і державних структур. При цьому охорона персональних даних - вимога закону, інші масиви інформації охороняються виходячи з внутрішніх політик підприємства, спрямованих на створення зручної і ефективної системи захисту.

1.1 Поняття локальної інфокомунікаційної мережі

Під локальної інфокомунікаційною мережею (ЛІКМ) розуміється невелика за розмірами комп'ютерна мережа, яка служить інтересам обмеженої кількості користувачів, покриваючи одне або декілька будівель, наприклад, офіси або приміщення інститутів [1, 41].

ЛІКМ класифікуються за способом адміністрування:

- локальні;
- розподілені;
- міські.

У ЛІКМ комп'ютери об'єднуються за допомогою мідних або оптоволоконних кабелів або по супутниковому зв'язку. Об'єднання персональних комп’ютерів (ПК) в мережу дає можливість [3]:

- передавати інформацію без знімних носіїв;
- спільно працювати в програмі, встановленої на одному комп'ютері, декільком користувачам;
- спільно користуватися пристроями, наприклад, принтером;
- застосовувати одне рішення для захисту конфіденційної інформації на декількох робочих станціях.

З іншими мережами ЛІКМ з'єднується через шлюзи. Вона може підключатися до Інтернету або бути автономною, у другому випадку вирішити задачу забезпечення безпеки даних простіше [2].

1.2 Аналіз найпопулярніших загроз ЛІКМ 2020 року

Аналіз найпопулярніших загроз інфокомунікаційним мережам різних підприємств у 2019 – 2020 рр. дав такі результати [1].

Порушення регламентів інформаційної безпеки (ІБ) виявлені абсолютно у кожної організації (100%). Серед них - використання про програмного забезпечення (ПЗ) для віддаленого доступу та використання незахищених протоколів.

Таблиця 1.1 – Порушення регламентів ІБ

Вид атаки	%
Застосування протоколів LLMNR і NetBios	69
Застосування ПЗ для віддаленого доступу	67
Використання незахищених протоколів передачі даних	64
Використання BitTorrent	36
Завантаження та встановлення потенційно небезпечного стороннього ПЗ	10

Одним з найбільш використовуваним порушенням регламентів ІБ - використання ПЗ для віддаленого доступу. У більшості компаній (59%) застосовується TeamViewer, в 21% компаній - Ammyy Admin. Також були помічені LightManager, Remote Manipulator System (RMS), Dameware Remote Control (DWRC), AnyDesk і інші [4].

Підозріла мережева активність , була виявлена в більшості компаній (90%). До неї відносяться приховування трафіку, запуск інструментів сканування мережі, спроби віддаленого запуску процесів. Перехід підприємств під час локдаунів коронвірусу на віддалену роботу вплинув і на мережеву активність - зросла частка підключень в зовнішню мережу по протоколу віддаленого доступу RDP: в 2019 році становила 3%, в 2020 році досягла 18%. Очевидно, що такі підключення повинні ретельно контролюватися. Так, наприклад, в одному промисловому організації PT NAD зафіксував підключення по RDP на зовнішній ресурс, що містить хмарне сховище. На його адресу за протоколами RDP і HTTPS в цілому було передано 23 ГБ даних. Зловмисники могли застосувати техніку T1071 - використання

протоколів прикладного рівня за класифікацією MITRE ATT & CK. Її суть полягає в тому, що порушники або шкідливі програми здійснюють потайливу передачу вкрадених даних на підконтрольні сервери, використовуючи поширені протоколи прикладного рівня.

Таблиця 1.2 – Підозріла мережева активність (частки компаній)

Активність	%
Приховування трафіка (тунелювання, проксирування)	59
Отримання даних з контролера домену	36
Численні, невдалі спроби автентифікації	31
Запуск інструментів для адміністрування та проведення атак	31
Сканування внутрішньої мережі	23
Спроби підключення до внутрішніх вузлів	21
Підозрілі підключення по протоколам віддаленого доступу	18
Спроби віддаленого запуску процесів	18

У половині промислових компаній було зафіксовано отримання даних з контролера домену. Сама по собі ця активність легітимна, проте вивантаження складу доменних груп або списку адміністраторів може говорити про активність зловмисників в інфраструктурі компанії і бути частиною розвідки.

Активність шкідливого ПЗ - ще одна популярна загроза. Вона виявлена в 68% організацій. У кожної четвертої організації виявлені спроби підключення до засінкхоленних доменів (доменних адресами, які були раніше помічені у шкідливих кампаніях, а тепер звернення до них перенаправляються на спеціальні sinkhole-сервери для недопущення зв'язку шкідливого програмного забезпечення (ШПЗ) з командними серверами). У кожній п'ятій компанії відзначені спроби віддаленого запуску процесу. Така мережева активність може свідчити про дії шкідливого ПЗ.

В ході написання атестаційної роботи автор знайшов відомості про активність 36 сімейств ШПЗ. Серед них були і такі як шифрувальник WannaCry, банківські трояни RTM, Ursnif і Dridex. Шпигунське ПЗ AgentTesla було виявлено в трьох організаціях. Навесні 2020 року ШПЗ Agent Tesla зустрічався в фішингових кампаніях, пов'язаних з COVID-19. ШПЗ було

змінено для крадіжки облікових даних електронної пошти з клієнта Outlook, а також паролів від Wi-Fi.

Таблиця 1.3 – Найпопулярніше ШПЗ 2020 року

Вид шкідливого програмного забезпечення	%
ШПЗ для віддаленого доступу	29
Майнери	27
Шифрувальник	24
Рекламне ПЗ	12
Банківський троян	12
Завантажувач	10
Шпигунське ПЗ	10

У кожної четвертої компанії виявлена активність кріптомайнеров. Як правило, PT NAD виявляв запити на дозвіл доменних імен, що відносяться до відомих Майнінг-пулів, таким як antpool.com, supportxmr.com, minexmr.com, nanopool.org, xmrpool.eu, monerohash.com, io.litecoinpool.org . Зловмисники можуть встановлювати Майнер в навантаження до основного ШПЗ або після виконання своєї мети, наприклад, крадіжки даних. Крім того, Майнер можуть використовувати до 80% вільної потужності комп'ютера, що загрожує компаніям істотним зниженням їх продуктивності.

Виявлення будь-якого ШПЗ в інфраструктурі - це привід для проведення ретельного розслідування. Наявність ШПЗ може свідчити про серйозні недоліки в системі безпеки компанії.

Спроби експлуатації вразливостей в ПЗ були помічені в кожній третій компанії. Це і спроби атак всередині мережі, так і успішні атаки для систем, розташованих на периметрі. Більше половини випадків пов'язано з уразливістю CVE-2017-0144 в реалізації протоколу SMBv1.

Проблема CVE-2017-0144 була виявлена в TeamViewer 14.2.2558. Для оновлення продукту від імені користувача без прав адміністратора необхідно ввести облікові дані адміністратора в графічний інтерфейс. Згодом ці облікові дані обробляються в Teamviewer.exe, що дозволяє будь-якому додатком, що працює в тому ж контексті користувача, який не є адміністратором, перехоплювати їх у вигляді відкритого тексту в пам'яті процесу.

Використовуючи цей метод, локальний зловмисник може отримати реєстраційні дані адміністратора для підвищення привілеїв. Цією уразливістю можна скористатися шляхом впровадження коду в Teamviewer.exe, який перехоплює виклики GetWindowTextW і реєструє оброблені облікові дані [2]. CVE-2017-0144 експлуатувалася відомим шифрувальником WannaCry, і була усунена ще в 2017 році. Однак зловмисники продовжують її активно використовувати, вишукуючи в мережі комп'ютери, на яких за 3,5 року так і не було встановлено оновлення. У 2019 році спроби експлуатації уразливості CVE-2017-0144 зустрічалися також часто і були виявлені в кожній п'ятій компанії.

Крім того, за допомогою ПЗ для віддаленого доступу зловмисники можуть непомітно підключатися до вузлів інфраструктури компанії. Тому якщо немає можливості повністю відмовитися від використання ПЗ для віддаленого доступу, то рекомендуємо обмежитися тільки одним інструментом і обов'язково встановити актуальні оновлення. 69% компаній використовують застарілі протоколи LLMNR і NetBios. Цей недолік конфігурації зловмисники можуть використовувати для перехоплення значень NetNTLMv2 challenge-response, що передаються по мережі, і подальшого підбору облікових даних.

Спроби підбору паролів (26%) також виявлені за допомогою систем аналізу трафіку. Так, наприклад, в одній компанії зловмисники намагалися підібрати пароль до системи управління базою даних, веб-інтерфейс якої був доступний через інтернет. У разі успіху атакуючі змогли б отримати доступ до бази даних веб-сайту, в тому числі до облікових даних користувачів.

1.3 Модель інформаційних загроз локальній мережі

При вирішенні задачі захисту інформації в локальній мережі на першому етапі необхідно скласти релевантну модель загроз, щоб оцінити ступінь ризиків, до яких схильні дані. При складанні моделі загроз передбачається, що несанкціонований доступ буває двох видів:

1. Непрямий, який здійснюється без прямого фізичного доступу до даних;

2. Прямий, з фізичним доступом до мережі.

Перелік способів нелегітимного отримання відомостей широкий. Загрозу для системи створюють навіть ті, що використовуються рідко.

Основні способи організації несанкціонованого доступу до інформації в ЛІКМ:

- фотографування екрану;
- зчитування електромагнітних хвиль моніторів;
- заборонене копіювання, стає в останні роки основною загрозою для безпеки інформації;
- розкрадання носіїв даних;
- проникнення в комп'ютери інших користувачів для отримання інформації обмеженого доступу, іноді з використанням чужих коштів ідентифікації (логінів, паролів, смарт-карт);
- застосування програмних пасток;
- отримання даних за допомогою серії дозволених запитів;
- використання недоліків програм і операційних систем для отримання відомостей;
- застосування шкідливих програм;
- нелегітимне підключення до мережі.

З кожним з цих способів розкрадання даних можна боротися. За статистикою, до 80% випадків несанкціонованого доступу до даних пов'язані з діями внутрішніх користувачів. Зовнішні атаки на корпоративні мережі відбуваються рідше, особливо якщо в цілях захисту інформації ЛІКМ не підключена до Інтернету.

Отримання несанкціонованого доступу до інформації може привести до серйозних інцидентів:

- розголошення, поширення даних. Цьому ризику особливо схильні до документи, що мають характер комерційної таємниці, і інтелектуальні активи. Їх потрапляння до третіх осіб, конкурентам може заподіяти компанії фінансовий збиток. Розголошення відомостей, що відносяться до персональних даних, тягне за собою відповідальність за нормами чинного законодавства;
- навмисне спотворення, підміна достовірної інформації неправдивою;

- знищення через злий намір третіх осіб або через поломки обладнання, носіїв інформації або в результаті ненавмисного зараження робочої станції за допомогою комп'ютерних вірусів.

Складно розрахувати, який саме збиток може принести компаніям недостатня турбота про захист інформації. Поява на ринку інсайдерської інформації може вплинути на курс акцій компанії, знизити її капіталізацію. Так, витік в 2020 році 87 млн облікових записів користувачів Facebook істотно знизила вартість компанії. Зараження мереж компанії A.P.Moller-Maersk вірусом-шифрувальником призвело до збитків в 300 млн доларів і необхідності протягом десяти днів контролювати розвантаження і завантаження сотень морських суден без використання ПЗ.

1.4 Стандартні заходи безпеки ЛІКМ

Використання різних засобів захисту інформації потрібно враховувати на етапі розробки архітектури мережі.

Захисні методи діляться на чотири групи:

1. організаційні;
2. технічні або апаратні;
3. програмні;
4. апаратно-програмні.

Всі названі засоби покликані створити складності для несанкціонованого доступу в ЛІКМ.

Основні бар'єри для зловмисників:

- фізичне перешкода, що виключає можливість дотику третьої особи з елементами мережі;
- система контролю і управління доступом, яка регламентує рівні прав користувачів;
- використання криптографічних засобів захисту інформації (шифрування даних);
- регламентація дій персоналу;
- застосування заходів дисциплінарного, цивільно-правового та навіть кримінально-правового впливу з метою захисту конфіденційної інформації.

1.5 Системи контролю і управління доступом до ЛІКМ

Системою контролю та управління доступу називають сукупність програмно-апаратних технічних засобів безпеки, що мають на меті: обмеження і реєстрацію входу-виходу об'єктів (людей, транспорту) на заданій території через «точки проходу»: двері, ворота, контрольно-пропускні пункти. Також, СКУД використовують для збору різноманітної інформації про працівників, їх пересування територією підприємства, термінів і часу знаходження в підрозділах та ін. Сучасні СКУД складаються з ідентифікаторів, зчитувачів, керуючого пристрою [56], призначення яких наведено в таблиці 1.4:

Таблиця 1.4 – Призначення складових СКУД [57]

Складова	Призначення
Індикатор	пристрій, який дозволяє системі розпізнати людину. На цій посаді часто використовуються популярні зараз безконтактні карти, контактні карти (з чорної магнітної смужкою), електронні брелоки. Ще в ролі ідентифікатора може виступати спеціальний код, який вводить людина під час входу в зону, що охороняється або біометричні дані — відбитки пальців або долоні, відбиток сітківки очей, розпізнавання голосу і т. п.
Зчитувач	пристрій для розпізнавання і передачі даних на керуючий блок.
Керуючий блок	Виконує функцію прийняття рішень щодо можливості визначити, чи потрібен доступ до приміщення для власника конкретного ідентифікатора. Якщо доступ дозволяється — надсилається сигнал на відкриття електронного замка (турнікета, шлагбаума, двері). У мережевих СКУД додатково до керуючого блоку підключається комп'ютер

В сучасних ЛІКМ, на наш погляд, доцільніше використовувати для ідентифікації користувачів – спеціальні картки, характеристики та типи яких наведені у таблиці 1.5.

Таблиця 1.5 – Карти – ідентифікатори користувачів [6]

Тип	Характеристика
Безконтактні радіочастотні (PROXIMITY) карти	Найбільш перспективний і вживаний зараз тип карт. Безконтактні картки спрацьовують на відстані і не вимагають чіткого позиціювання, що забезпечує їх стійку роботу і зручність використання, високу пропускну здатність системи. Зчитувач генерує електромагнітне випромінювання певної частоти і, при внесенні карти до зони дії зчитувача, це випромінювання через вбудовану в карті антену живить чіп картки. Отримавши необхідну енергію для роботи, карта пересилає на зчитувач свій ідентифікаційний номер за допомогою електромагнітного імпульсу певної форми і частоти.
Магнітні картки	менш поширений варіант, володіє декількома недоліками - малий термін служби, необхідність чіткого позиціонування. Існують карти з низько коерцитивною і високо коерцитивною магнітною смугою і з записом на різні доріжки. Використовується як правило для ідентифікаторів з дуже обмеженим терміном дії.
Карти Віганд	названі по імені вченого, який відкрив магнітний сплав, що володіє прямокутною петлею гистерезису. Всередині карти розташовані відрізки дроту з цього сплаву, які, при переміщенні повз них голівки, що зчитує, дозволяють отримувати інформацію. Ці карти довговічніші, ніж магнітні, але й дорожчі. Один з недоліків - те, що код в карту заноситься при виготовленні раз і назавжди.
Штрих-кодові карти	на карту наноситься штриховий код. Існує складніший варіант - штрих-код закривається матеріалом, прозорим тільки в інфрачервоному світлі, зчитування відбувається в ІЧ-області спектру.

На сьогодні для контролю доступу до мережі використовують автономні, мережеві та комбіновані СКУД, характеристики яких наведені у таблиці 1.6. [56]

Таблиця 1.6 - Контролери СКУД

Тип	Характеристика
Автономні	Призначені для обслуговування, як правило, однієї точки проходу. Зустрічаються найрізноманітніші варіації: контролери, суміщені зі зчитувачем, контролери, вбудовані в електромагнітний замок і так далі. Автономні контролери розраховані на застосування різних типів зчитувачів. Розраховані на обслуговування невеликої кількості користувачів, звичайно до п'ятисот.
Мережеві	Працюють під управлінням комп'ютера з встановленим спеціалізованим програмним забезпеченням. Мережеві контролери застосовуються для створення СКУД будь-якого ступеня складності. При цьому адміністрація одержує величезну кількість додаткових можливостей: дозволу або заборони проходу; отримання звіту про наявність чи відсутність співробітників на роботі; миттєво дізнатися, де конкретно знаходиться співробітник; вести автоматичний табель обліку робочого часу; отримати звіт про те, хто і куди ходив практично за будь-який період часу; сформувати часовий графік проходу співробітників, тобто хто, куди і в який час може ходити; можливість ведення бази даних співробітників (електронної картотеки
Комбіновані	Поєднують в собі функції мережних і автономних контролерів. При наявності зв'язку з керуючим комп'ютером (on line) контролери працюють як мережний пристрій, при відсутності зв'язку - як автономні. Найкраще рішення для сучасних інтегрованих систем безпеки, дозволяють побудувати відмовостійку на гнучку СКУД.

Стуктурно-логічну схему автономної СКУД наведено на рис.1.1.

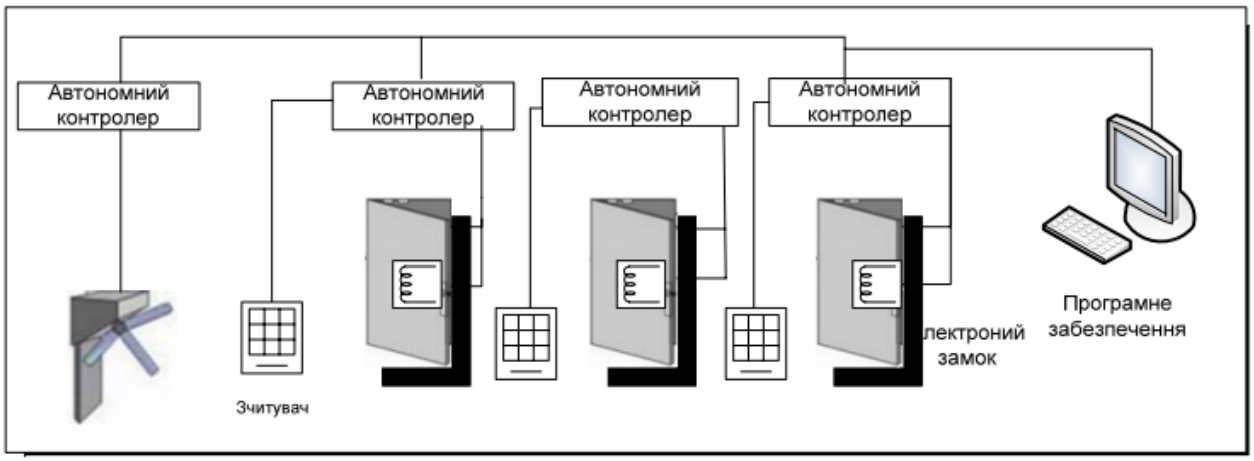


Рисунок 1.1 – Структурно-логічна схема автономної СКУД [56]:

Вимоги до інтеграції СКУД з іншими системами безпеки організації наведені в таблиці 1.7

Таблиця 1.7 – Інтеграція СКУД з іншими системами безпеки організації

Система безпеки	Мета інтеграції
відеоспостереження	для суміщення архівів подій систем, передачі системі відеоспостереження повідомлень про необхідність стартувати запис, повернути камеру для запису наслідків зафіксованого підозрілого події
охоронної сигналізації	для обмеження доступу в приміщення, або для автоматичного зняття і постановки приміщень на охорону;
пожежної сигналізації	для отримання інформації про стан пожежних сповіщувачів, автоматичного розблокування евакуаційних виходів і закривання протипожежних дверей в разі пожежної тривоги

Засоби контролю доступу в приміщення з локальною мережею з метою захисту інформації включають:

- механізми ідентифікації користувачів і елементів системи, засновані на текстових (логін, пароль) або технічних (смарт-карта, токен) принципах;
- роздачу повноважень на доступ в залежності від службового рангу користувача;

- регламентування дозволених робіт в мережі для кожної категорії користувачів;
- фіксацію дій користувачів;
- певні реакцій (відключення системи, сигналізація) при виявленні спроб несанкціонованого доступу [7].

При побудові мережевих СКУД використовуються чотири рівні мережевої взаємодії [56], особливості яких наведені у таблиці 1.8:

Таблиця 1.8 – Рівні мережевої взаємодії СКУД

Рівень	Конструкція	Призначення
1 (вищий)	комп'ютерна мережа типу клієнт/сервер на основі мережі ETHERNET, з протоколом обміну TCP/IP і з використанням мережевих операційних систем Windows NT або Unix	забезпечує зв'язок між сервером і робочими комп'ютерами підсистем.
2	зв'язок між контролерами і комп'ютерами підсистем	використовується інтерфейс RS 232
3	зв'язок між контролерами і зчитувачами пристроями	застосовується інтерфейс RS 485 або, що стали вже стандартом, інтерфейси зчитувачів або магнітних карт
4	рівень сповіщувачів пожежної сигналізації і ланцюгів управління — збалансовані і незбалансовані радіальні і адресні шлейфи, релейні вихідні ланцюга управління	застосовуються нестандартні спеціалізовані інтерфейси і протоколи обміну інформацією

Контролери, що працюють в мережевому режимі, повинні забезпечувати:
- обмін інформацією по лінії зв'язку між контролерами і керуючим комп'ютером або провідним контролером [56],;
- збереження пам'яті, установок, кодів ідентифікаторів у разі обриву зв'язку з керуючим комп'ютером, відключення живлення і при переході на резервне живлення [56],;
- контроль ліній зв'язку між окремими контролерами і між контролерами і керуючим комп'ютером [56].

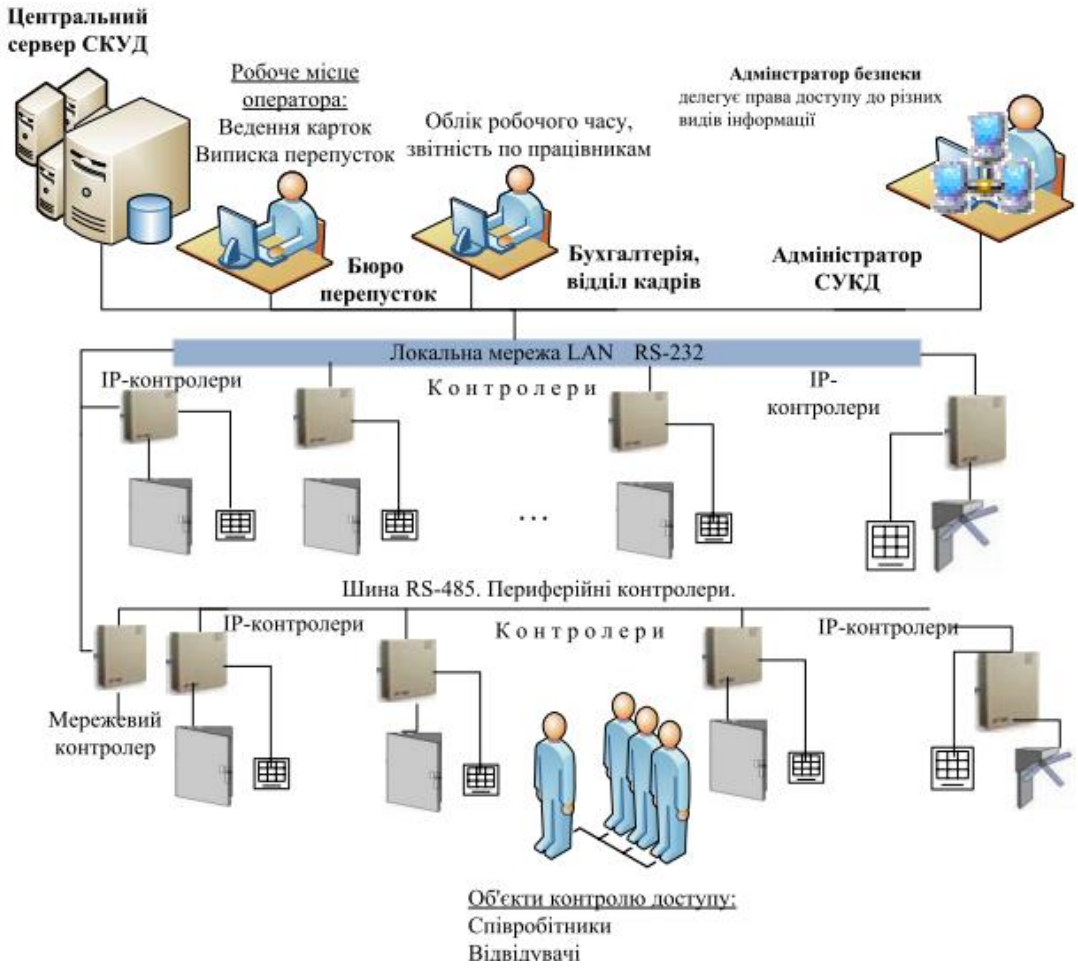


Рисунок 1.2 – Структурно-логічна схема мережевої СКУД [56]

Протоколи обміну інформацією і інтерфейси повинні бути стандартних типів. Види і параметри інтерфейсів повинні бути встановлені в паспортах та/або інших нормативних документах на конкретні засоби [56].

Таблиця 1.9 - Рекомендовані типи інтерфейсів

Розташування	Тип
між контролерами	RS 485
між контролерами і керуючим комп’ютером	RS 232

Основну роль у діяльності мережевої системи відіграє програмне забезпечення, яке має виконувати наступні функції:

- заносити коди до пам’яті системи різноманітних ідентифікаторів для розпізнавання користувачів;

- встановлювати часові інтервали доступу (робочий день, перерва)
- встановлювати різні рівні доступу користувачів (індивідуально для кожного або за групами);
- вести журнал подій дій користувачів;
- вести різноманітні бази даних користувачів та забезпечувати її цілісність після збоїв.

1.6 Організаційні методи захисту ЛІКМ

До організаційних методів традиційно відносять внутрішні нормативні акти, які регламентують порядок роботи з інформацією. Це положення про комерційну таємницю, про порядок роботи з інформаційними ресурсами, про порядок доступу до документів. Але тільки положеннями та іншими нормативними актами організаційні заходи не обмежуються, вони можуть носити і характер дій.

До організаційних засобів захисту інформації відносять:

- обмеження доступу в робочі приміщення, введення системи перепусток;

розмежування прав користувачів в роботі з масивами інформації;

- виділення для обробки цінної інформації спеціальних автоматичних робочих місць (АРМ) без підключення до Інтернету;
- особливий порядок обліку та зберігання знімних носіїв інформації;
- розміщення АРМ таким чином, щоб екран комп'ютера і клавіатура не виявлялися в зоні видимості інших співробітників і сторонніх;
- контроль за виведенням інформації на принтер, створення захищених зон для друку;
- контроль за роздрукованими примірниками документів, що містять критичну інформацію;
- в разі поломки обладнання - знищення даних на жорстких дисках перед його відправкою в ремонт;
- встановлення запірних пристроїв на корпусі комп'ютера.

Для регламентування дій користувачів доцільно:

- ввести на підприємстві режим комерційної таємниці, склавши вичерпний перелік конфіденційних даних;

- включити в трудові договори умова про відповідальність за розголошення комерційної таємниці або персональних даних;
- проводити тренінги, присвячені способам захисту інформації.

При виявленні випадків недбалого ставлення до інформації, що міститься в локальних обчислювальних мережах, потрібно публічно притягати винних до відповідальності. Це запобіжить нові випадки розкриття цінних відомостей. Політика безпеки кожної корпорації повинна своєчасно доводитися до відома кожного співробітника, систематично оновлюватися і діяти в щоденному режимі. Контроль за цим повинен бути покладений на служби персоналу і безпеки.

1.7 Технічні методи захисту ЛІКМ

Технічні засоби захисту інформації, незважаючи на високу вартість, дуже популярні, оскільки дозволяють захистити дані найбільш надійно. Вони стійкі до зовнішнього впливу, захищені від втручання в конструкцію, гарантують обмеження несанкціонованого доступу в повному обсязі.

Технічні засоби поділяються на дві групи:

1. Апаратні, вони вбудовуються в комп'ютери або сумісні з ними через певний інтерфейс (канал передачі даних - USB, Wi-Fi);

2. Фізичні, що представляють собою обладнання або архітектуру приміщень, які захищають ЛІКМ і їх елементи від несанкціонованого доступу.

Крім названих, широко використовуються такі варіанти вирішення завдань, як генератори акустичних перешкод, покликані запобігти підслуховування, використання м'яких підкладок під обладнання, що також знижує ризики витоку інформації по акустичному каналу. Використання мережевих фільтрів або стабілізаторів напруги, які продовжують життя обладнанню, що побічно відбивається на збереження даних.

Система віброакустичного зашумлення (маскування) призначена для запобігання прослуховування приміщення шляхом створення шумового сигналу в діапазоні звукових частот. Така система складається, як правило, з генератора шуму та комплекту акустичних і вібраційних випромінювачів [6].

Таблиця 1.10 – Генератори віброакустичного зашумлення

	Назва	Призначення
1	Генератор шумових сигналів "МАРС-ТЗО-4-2"	Генерація шумових сигналів при використанні у складі технічних засобів активного захисту мовної інформації від витоку акустичним і віброакустичним каналами
2	Прилад віброакустичного захисту інформації "ОЦЗІ-ВА"	Генерація шумових сигналів при використанні у складі технічних засобів активного захисту акустичної (мовної) інформації від витоку акустичним і віброакустичним каналами
3	Генератори акустичного шуму стаціонарні „РІАС-2ГС”	Захист інформації з обмеженим доступом на об’єктах інформаційної діяльності від її витоку акустичними та віброакустичними каналами шляхом генерації шумового сигналу (шумової завади)
4	Генератори акустичного шуму мобільні „РІАС-2ГМ”	Захист інформації з обмеженим доступом на об’єктах інформаційної діяльності від її витоку акустичним та віброакустичним каналами шляхом генерації шумового сигналу (шумової завади)
5	Пристрій захисту „Базальт-4ГА”	Генерація шумових сигналів при використанні у складі технічних засобів активного захисту мовної інформації від витоку акустичним і віброакустичним каналами

Проведемо порівняльну характеристику найпопулярніших генераторів віброакустичного шуму за технічними характеристиками та зведемо всі дані до таблиці 1.11.

Таблиця 1.11 – Порівняльна характеристика сертифікованих генераторів віброакустичного зашумлення

Характеристика	Марс-ТЗО-4.2	Базальт – 4ГА	PIAC
Діапазон частот шумового сигналу	від 180 Гц до 5600 Гц	від 170 Гц до 5700 Гц	від 180 Гц до 5600 Гц
Кількість каналів виходів всього, у т.ч на: акустичні випромінювачі віброакустичні випромінювачі	222	211	211
Індикація рівня вихідного сигналу	по 10 сегментному індикатору	відсутня	відсутня
Максимальна вихідна потужність на кожний канал у т.ч.	≥ 10 Вт		
Віброакустичний (п'єзоелектричний) канал			≥ 10 Вт
Вихідне середнеквадратична напруга акустичного(електромагнітного) каналу при навантаженні 4 Ом			≥ 5 Вт
Максимальні ефективні напруги вихідних шумових сигналів в смузі частот (170 … 5700) Гц по:			
низьковольтному виходу на мінімальному опорі навантаження 1 Ом, В		≥ 2	
високовольтному виходу на мінімальному опорі навантаження 50 Ом, В		≥ 15	
Глибина регулювання рівнів шумових сигналів на виходах	≥ 20 Дб	≥ 20 Дб	≥ 20 Дб
Регулювання рівня сигналу по верхнім и нижнім частотам (по октавах) на глибину		≥ 25 Дб	≥ 20 Дб
Живлення генератора	від 100 В до 240 В частотою 50, 60 Гц	від 198 до 240 В	220 В частотою 50 (±1) Гц акумулятор або бортова мережа

1.8 Програмні методи захисту ЛІКМ

У міру вдосконалення шкідливих програм вдосконалюються і методи боротьби з ним. Сьогодні шкідливе ПЗ може тривалий час переховуватися в мережах і не виявлятися антивірусами. Такі програми стали дешевше на чорному ринку, вони доступні навіть для невеликих хакерських угруповань, а кількість можливих каналів зараження суттєво зросла.

Крім зовнішніх інформаційних загроз, існують і внутрішні, пов'язані з людським фактором. Захисне ПЗ діє і проти них.

Залежно від розв'язуваних завдань програмні методи захисту даних діляться на наступні типи:

- міжмережеві екрани, що ставлять бар'єр для трафіку в вузлах обчислювальної мережі або в місці її з'єднання з зовнішніми мережами;
- антивіруси, що виявляють шкідливі програми;
- засоби криптографічного захисту інформації, що дозволяють шифрувати дані як на дисках, так і в момент їх передачі;
- технології електронного підпису, що забезпечують справжність документів;
- засоби виявлення вторгнення, що сигналізують про спроби несанкціонованого доступу в обчислювальну мережу;
- засоби довіреної завантаження, контролюючі завантажуються користувачами в мережу файли;
- утиліти для контролю знімних носіїв, що дозволяють уникнути несанкціонованого копіювання;
- засоби ідентифікації копій документів, що дозволяють виявити, хто саме з користувачів роздрукував секретну інформацію;
- системи контролю управління доступом (СКУД);
- рішення для аудиту даних в інформаційній системі.

Програмні засоби захисту інформації в Україні проходять обов'язкову сертифікацію в Державній службі спеціального зв’язку та захисту інформації України і це свідчить про їхню надійність. Програмні засоби зазвичай застосовуються в комплексі, з опорою на вироблену при розробці архітектури системи модель загроз.

Для великих і середніх компаній одним з кращих засобів захисту інформації в локальної обчислювальної мережі є DLP-системи. Це комплексне рішення, що дозволяє відстежувати дані всередині мережі та на виході з неї. Ядро DLP-системи складає текстовий аналізатор - фільтр для аналізу інформації, що передається, який однозначно визначає категорію конфіденційності документа. Щоб текстовий аналізатор почав працювати, його наповнюють відомостями, що дозволяють виявляти файли, що містять конфіденційну інформацію. Якщо певним чином впливати в системі не дозволено для конкретного користувача, воно буде заблоковано. Інформація про подію також буде передана до підрозділу інформаційної безпеки з метою вжиття заходів реагування.

DLP-системи також сертифікуються, крім іншого, в них визначають в тому числі на ступінь вмісту незадекларованих можливостей. Така перевірка сертифікація показує, наскільки безпечно програмне рішення, чи не міститься в ньому прихованих функцій, наприклад, кейлоггера або опції крадіжки паролів.

1.9 Апаратно-програмні засоби захисту ЛІКМ

Окрему групу методів захисту даних в ЛІКМ становлять апаратно-програмні засоби, що включають в себе технічну частину і програмний код, що дозволяє нею керувати. До таких засобів відносять:

апаратні засоби контролю доступу (електронні замки, пристрої ідентифікаційних ознак);

спеціалізовані мережі зберігання (SAN - Storage Area Network). Вони призначені для консолідації дискового простору на спеціально виділених зовнішніх дискових сховищах, що збільшує продуктивність системи;

дискові сховища даних, наприклад, RAID-масиви;

стрічкові накопичувачі, для резервного зберігання даних, що, захищає їх від втрати.

Вибір програмно-апаратного засобу забезпечення інформаційної безпеки має здійснюватися усвідомлено. На відміну від програмних засобів захисту інформації, його складніше поміняти на нове у міру розвитку кібертехнологій.

1.10 Дослідження методів і технологій захисту ЛІКМ на фізичному та канальному рівнях

Найпоширенішими атаками на ЛІКМ на фізичному рівні насьогодні є:

- навмисне фізичне пошкодження ліній зв'язку;
- несанкціоноване внесення змін у функціональному середовищі;
- несанкціоноване відключення фізичних каналів зв'язку
- навмисне зашумлення зловмисником всієї полоси пропускання каналу.

Таблиця 1.12 – Методи та технології захисту канального рівня

Метод захисту	Загрози, яким протидіють	Наслідки дії методу
Функція Portsecurity	Внутрішні загрози несанкціонованого підключення до мережі або зміни MAC- адреси	При несанкціонованому підключенні вузла порт блокується або відкидаються кадри з недозволеною MAC-адресою відправника
Функція DHCP Snooping	Внутрішні загрози додавання несанкціонованого DHCP-серверу, DoS-атаки на DHCP-сервер.	Автоматичне створення прив'язок IP-MAC-порт з подальшим відкиданням кадрів від вузлів, які не відповідають прив'язкам
Функція Dynamic ARP Inspection	Внутрішні загрози, пов'язані з підміною MAC-адрес в ARP-записах (атака ARP-spoofing)	Відкидання кадрів з незаконними ARP-повідомленнями
Функція IP SourceGuard	Внутрішні загрози, пов'язані з підміною IP-адрес	Відкидання кадрів від вузлів, які не відповідають прив'язці IP-MAC-порт
Сегментація на VLAN	Внутрішні загрози широкомовних штормів та НСД до вузлів та інформації	Передача кадрів з будь-якими MAC-адресами отримувача тільки між вузлами окремих VLAN
Авторизація по протоколу 802.1x	Внутрішні загрози несанкціонованого підключення вузлів до мережі та доступу до сервісів та інформації	Передача кадрів від вузла тільки після проходження автентифікації та авторизації кінцевого пристрою або користувача

Найоптимальніший метод захисту – застосування оптоволоконного кабелю. Для ліній зв'язку з довжиною до 100 метрів інколи можна використовувати екрановану віту пару для знешкодження електромагнітних наведень на канали передачі даних [54, 55].

Найпоширеніші атаки на ЛІКМ на канальному рівні зловмисники здійснюють для перевантаження каналів зв’язку та різноманітного комутаційного обладнання шляхом генерації широкомовних кадрів або влаштовуючи широкомовні шторми. Зловмисники також підмінюють MAC адрес вузлів та атакують протоколи Spanning-Tree і ARP.

2 ДОСЛІДЖЕННЯ БЕЗПЕКИ МЕРЕЖ ЗБЕРІГАННЯ ДАНИХ

Мережа зберігання даних (SAN) - це виділена високошвидкісна мережа або підмережа, яка з'єднує між собою і представляє спільні пули пристроїв зберігання даних для декількох серверів.

Доступність і висока готовність систем зберігання даних є ключовими показниками для корпоративних додатків. Традиційне розгортання систем зберігання з прямим підключенням до окремих серверів може бути простим і недорогим варіантом для багатьох корпоративних додатків, але диски і важливі дані, що містяться на них, прив'язані до фізичного сервера через виділений інтерфейс, такий як SAS. Сучасні корпоративні середовища часто вимагають набагато більш високого рівня організації, гнучкості та контролю. Ці потреби стимулювали розвиток мережі зберігання даних (SAN).

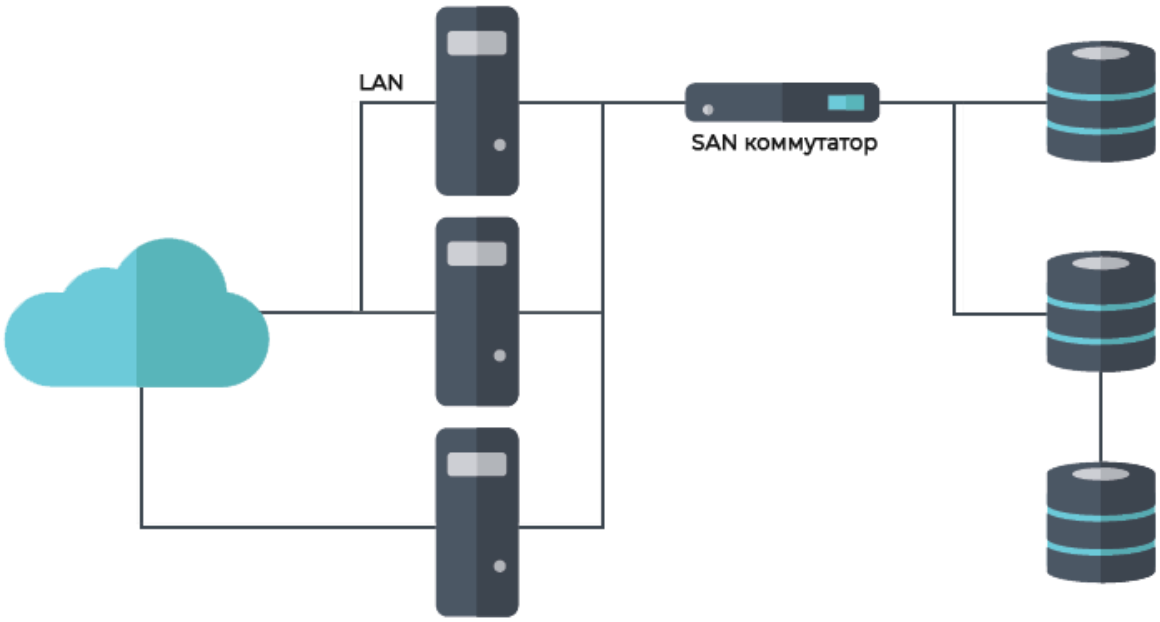


Рисунок 2.1 – Мережа зберігання даних

Технологія SAN задовольняє передові потреби корпоративного сховища, надаючи окрему, виділену, добре масштабується у високопродуктивну мережу, призначену для з'єднання безлічі серверів з масивом пристроїв зберігання. Сховище можна організувати і керувати ним як

єдиним пулом ресурсів. SAN дозволяє організації розглядати сховище як єдиний колективний ресурс, який також можна централізовано реплицирувати і захищати, в той час як додаткові технології, такі як дедуплікація даних і RAID, можуть оптимізувати ємність сховища і значно підвищити відмовостійкість сховища - в порівнянні з традиційним сховищем з прямим підключенням (DAS).

2.1 Призначення SAN

SAN - це мережа накопичувачів, до якої звертається мережу серверів. Існує кілька популярних застосувань мереж SAN в корпоративних обчисленнях. SAN зазвичай використовується для консолідації сховищ. Наприклад, зазвичай комп'ютерна система, така як сервер, включає в себе одне або декілька локальних пристроїв зберігання даних. Але розглянемо центр обробки даних з сотнями серверів, на кожному з яких запущені віртуальні машини, які можна розгортати і переміщати між серверами за бажанням. Якщо дані для кожної робочої навантаження зберігаються на тому ж локальному сховищі, то їх також потрібно буде переміщати, якщо робоче навантаження переноситься на інший сервер або відновлюється, якщо сервер виходить з ладу. Замість того щоб намагатися організувати, відстежувати і використовувати фізичні диски, розташовані на окремих серверах, компанія може перемістити дані на виділену підсистему зберігання з можливістю колективного доступу до сховища, управління і захисту.

SAN також може підвищити доступність сховища. Оскільки SAN, по суті, являє собою мережеву структуру взаємопов'язаних комп'ютерів і пристроїв зберігання, порушення одного мережевого шляху зазвичай може бути компенсовано за рахунок включення альтернативного шляху через структуру SAN. Таким чином, несправність одного кабелю або пристрою не робить сховище недоступним для корпоративних робочих навантажень. Крім того, можливість розглядати сховище як єдиний ресурс може поліпшити використання сховища, виключивши «забуті» диски на недо використовуваних серверах. Замість цього, SAN пропонує центральне місце для всіх сховищ і дозволяє адміністраторам поєднувати пристрої зберігання в пули і управляти ними спільно.

Всі ці приклади використання можуть поліпшити відповідність нормативним вимогам організації, а також аварійне відновлення (DR) і забезпечення безперебійного функціонування за рахунок поліпшення здатності IT-фахівцями підтримувати корпоративні робочі навантаження. Але щоб оцінити цінність технології SAN, важливо зрозуміти, чим SAN відрізняється від традиційних DAS.

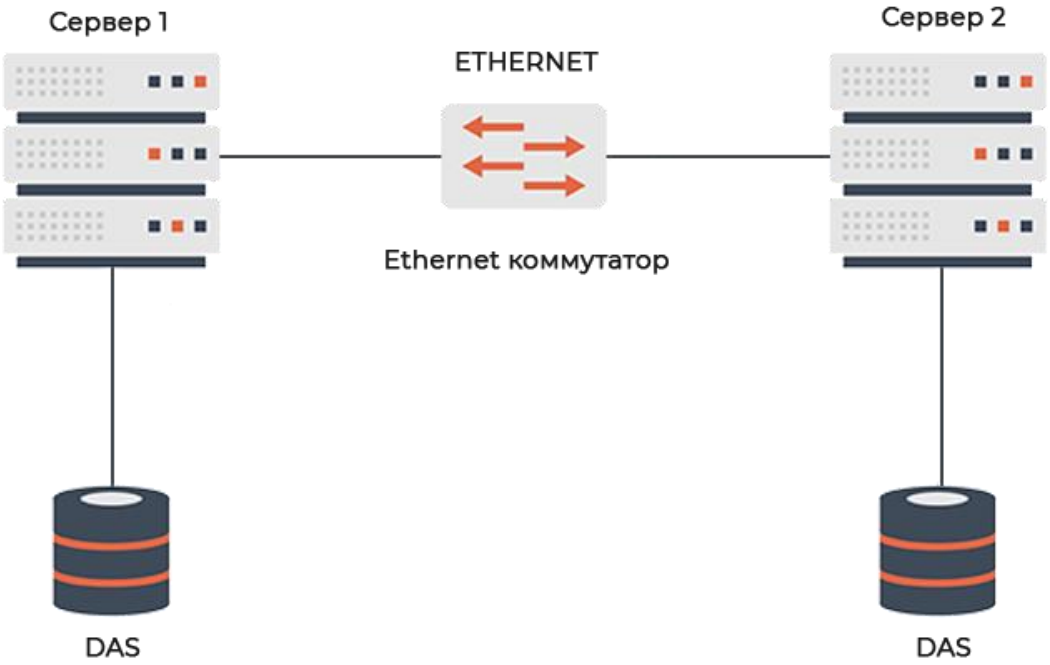


Рисунок 2.2 – Сховище з прямим підключенням

За допомогою DAS один або декілька дисків безпосередньо підключаються до конкретного сервера через спеціальний інтерфейс зберігання, такий як SATA або SAS. Диски часто використовуються для зберігання додатків і даних, призначених для роботи на цьому конкретному сервері. Хоча до пристроїв DAS на одному сервері можна отримати доступ з інших серверів, зв'язок здійснюється через загальну IP-мережу - LAN - разом з трафіком інших додатків. Доступ до великих обсягів даних і їх переміщення через звичайну IP-мережу може займати багато часу, а вимоги до смуги пропускання при переміщенні великих обсягів даних можуть впливати на продуктивність додатків на сервері.

SAN працює зовсім по-іншому. SAN об'єднує всі диски в виділену мережу зберігання даних. Ця виділена мережа існує окремо від загальної LAN. Такий підхід дозволяє кожному з серверів, підключених до SAN, отримати доступ до будь-якого з дисків, підключених до SAN, ефективно використовуючи сховище як єдиний загальний ресурс. Ніякі дані сховища SAN не проходять через локальну мережу - це знижує потребу в пропускної здатності локальної мережі і зберігає її продуктивність. Оскільки SAN - це окрема виділена мережа, її можна спроектувати так, щоб забезпечити високу продуктивність і відмовостійкість, що особливо важливо для корпоративних додатків.

Таблиця 2.1 – Характеристика мереж

Мережі	*Характеристика*
SAN	Високопродуктивна мережа, яка добре масштабується, та з'єднує хости із загальним пулом пристроїв зберігання даних на рівні блоків.
NAS	Підключається до одного хосту і керується ним. Сховище складається з дисків в хості і / або зовнішніх дискових полицях, які безпосередньо підключені до контролерів в хості.
DAS	Сховище із загальним доступом, яке зберігає і дозволяє спільно використовувати файли за стандартними протоколами - в основному, за протоколами Network File System і Server Message Block - по IP-мереж.

SAN може підтримувати величезну кількість пристроїв зберігання, а масиви зберігання - спеціально розроблені підсистеми зберігання - які підтримують SAN, можуть масштабуватися для зберігання сотень або навіть тисяч дисків. Будь-сервер з відповідним інтерфейсом SAN може отримати доступ до SAN і його величезному потенціалу зберігання, а SAN може підтримувати безліч серверів.

2.2 Основні типи мережевих технологій і інтерфейсів

У мережах SAN використовуються два основні типи мережевих технологій і інтерфейсів: Fibre Channel і iSCSI.

2.2.1 Fibre Channel

FC - це високошвидкісна мережа відрізняється високою пропускною здатністю і малою затримкою, яка пропонує швидкість передачі даних до 128 Гбіт / с на відстанях до 10 км - при використанні оптоволоконних кабелів і інтерфейсів. Такий вид виділеної мережі дозволяє консолідувати блочне сховище в одному місці, в той час як сервери можуть бути розподілені по будівлях кампусу або міста. Традиційні мідні кабелі і відповідні інтерфейси FC також можуть використовуватися, коли сховище і сервери знаходяться в одному місці і відстань не перевищує 10 метрів. FC реалізується шляхом установки адаптерів FC (HBA) на кожному сервері, сховище, мережевих комутаторах FC або інших мережевих пристроях. Кожен HBA включає один або кілька портів, через які відбувається обмін даними. Порти можуть бути віртуальними або фізичними, а фізичні порти з'єднані між собою кабелями, дозволяючи HBA і комутаторів утворювати мережеву структуру в різних топологіях.

2.2.2 ISCSI

ISCSI - це ще один тип мережі, призначений для з'єднання серверів із загальним сховищем. Він може працювати зі швидкістю до 100 Гбіт / с і забезпечує кілька спрощень для операторів центрів обробки даних. FC пропонує унікальний і вузькоспеціалізований структуру мережі, а iSCSI об'єднує традиційні блоки даних SCSI і пакети команд зі звичайними мережевими технологіями Ethernet і TCP / IP. Це дозволяє мереж зберігання iSCSI використовувати ті ж кабелі, мережеві адаптери, комутатори і інші мережеві компоненти, які використовуються в будь-якій мережі Ethernet. У багатьох випадках iSCSI може працювати в одній і тій же локальній мережі Ethernet і обмінюватися даними по локальній мережі, глобальної мережі і навіть через Інтернет. Операційна система кожного сервера розглядає доступ до даних iSCSI як до локально підключеному диску.

2.3 Принцип роботи SAN

SAN - це, по суті, мережа, яка призначена для з'єднання серверів з СГД. Мета будь-якої SAN - витягти пристрої зберігання з окремих серверів і розмістити їх в загальному сховищі, ресурсами якого можна централізовано

керувати і захищати. Така централізація може бути виконана фізично, наприклад, шляхом розміщення дисків в виділену підсистему зберігання. Однак централізація також може виконуватися логічно за допомогою програмного забезпечення (наприклад, VMware vSAN), яке використовує віртуалізацію для пошуку і об'єднання доступних ресурсів зберігання.

За рахунок підключення загального сховища до серверів через окрему мережу - крім традиційної LAN - продуктивність сховища може бути оптимізована і прискорена, оскільки трафіку системи зберігання більше не потрібно конкурувати за пропускну здатність локальної мережі, необхідну для серверів і їх робочих навантажень. Таким чином, корпоративні робочі навантаження потенційно можуть отримати більш швидкий доступ до величезних обсягів зберігання.

Зазвичай SAN сприймається як сукупність трьох груп або шарів: серверів - споживачів дискових ресурсів, мережевої інфраструктури - фабрик і дискових масивів (систем зберігання даних) - сховищ.

2.3.1 Хост-шар

Він являє собою сервери, підключені до SAN. У більшості випадків серверах виконуються корпоративні робочі навантаження, такі як бази даних, яким потрібен доступ до сховища. Хости зазвичай використовують традиційні компоненти LAN - Ethernet, щоб сервер і його робоче навантаження могли взаємодіяти з іншими серверами, а також з користувачами. Однак хости SAN також включають в себе окремий мережевий адаптер, призначений для доступу до SAN. Мережевий адаптер, який використовується для більшості мереж FC SAN, називається хост-адаптером (HBA - host bus adapter). Як і в більшості мережевих адаптерів, FC HBA використовує вбудоване програмне забезпечення для роботи обладнання HBA, а також драйвер пристрою, який пов'язує HBA з операційною системою сервера. Ця конфігурація дозволяє робочому навантаженні передавати команди і дані сховища через операційну систему в мережу SAN і її ресурси зберігання. FC є не єдиною, але однією з найбільш популярних і потужних технологій SAN.

2.3.2 Шар фабрики

Він являє собою кабелі та мережеві пристрої, що становлять мережеву структуру, яка з'єднує вузли SAN і сховище SAN. Мережеві пристрої SAN на рівні фабрики можуть включати комутатори SAN, шлюзи і маршрутизатори.

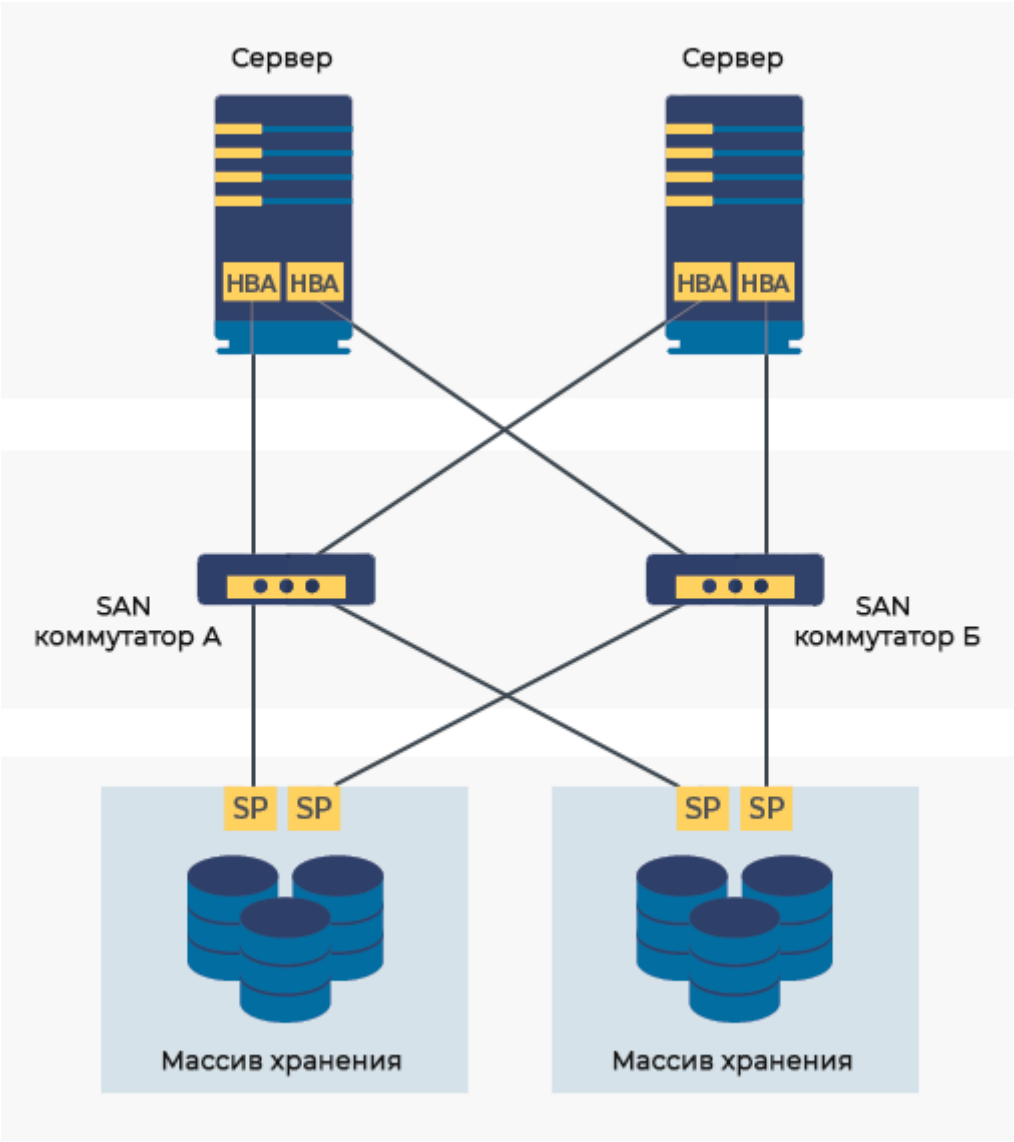


Рисунок 2.3 – Масиви зберігання

Кабелі та відповідні порти пристроїв SAN можуть використовувати оптоволоконні з'єднання або традиційні мідні кабелі. Різниця між мережею та фабрикою- це надмірність: доступність декількох альтернативних шляхів від хостів до сховища через фабрику. При побудові фабрики SAN зазвичай реалізується кілька з'єднань для забезпечення декількох шляхів. Якщо один шлях пошкоджений, для зв'язку SAN буде використовуватися альтернативний шлях.

2.3.3 Шар зберігання

Він складається з різних пристроїв зберігання, зібраних в різні пули зберігання даних. Зазвичай для зберігання використовуються традиційні магнітні жорсткі диски, але також можуть використовуватися твердотільні накопичувачі, а також стрічкові накопичувачі. Більшість пристроїв зберігання в мережі SAN організовані в фізичні групи RAID, які можна використовувати для збільшення ємності сховища, підвищення надійності пристрою зберігання або того й іншого. Логічним об'єктів зберігання, таким як групи RAID або навіть розділів диска, призначається унікальний LUN, який служить тієї ж мети, що і буква диска, наприклад C або D. Таким чином, будь-який хост SAN потенційно може отримати доступ до будь-якого LUN SAN через фабрику SAN.

2.3.4 Особливості SAN

SAN використовує ряд протоколів, що дозволяють програмному забезпеченню обмінюватися даними або готувати дані для зберігання. Технології SAN часто підтримують декілька протоколів, допомагаючи забезпечити ефективну взаємодію всіх рівнів, операційних систем і додатків.

Основу SAN становить її фабрика: масштабується, високопродуктивна мережа, яка об'єднує хости - сервери - і пристрої зберігання даних. Структура фабрики безпосередньо впливає на надійність і функціональність SAN. У найпростішому варіанті, FC SAN може просто підключити порти HBA на серверах безпосередньо до відповідних портів в масивах зберігання даних.

Але такі прості схеми підключення віддаляють справжню міць SAN. На практиці тканину SAN призначена для підвищення надійності та доступності систем зберігання даних за рахунок усунення окремих точок відмови. Основна ідея при створенні SAN полягає в використанні як мінімум двох з'єднань між будь-якими елементами SAN. Мета полягає в тому, щоб між хостами SAN і сховищем SAN завжди був доступний хоча б один робочий мережевий шлях.

Однією фабрики недостатньо для забезпечення надійність при зберіганні даних. На практиці системи зберігання повинні включати набір внутрішніх технологій, в тому числі RAID - групи дисків. У систему зберігання зазвичай додаються додаткові технології для ефективного використання сховища,

включаючи тонке виділення ресурсів, моментальні знімки або клонування сховища, дедуплікація даних і стиснення даних.

2.4 Переваги SAN

Незалежно від того, традиційна або віртуальна, SAN пропонує ряд переконливих переваг, життєво важливих для робочих навантажень корпоративного класу.

2.4.1 Висока продуктивність

SAN використовує окрему мережеву структуру, призначену для вирішення завдань зі зберігання даних. Мережевою інфраструктурою традиційно є FC для забезпечення максимальної продуктивності, хоча також доступні iSCSI і конвергентні мережі.

2.4.2 Висока масштабованість

SAN може підтримувати надзвичайно великі розгортання, що охоплюють тисячі хост-серверів і пристроїв зберігання. При необхідності можуть бути додані нові хости і сховище для побудови SAN відповідно до конкретних вимог організації.

2.4.3 Висока доступність

Традиційна SAN заснована на ідеї мережевої структури, яка - в ідеалі - пов'язує все з усім. Це означає, що в повнофункціональному розгортанні SAN немає єдиної точки відмови між хостом і пристроєм зберігання, а використання фабрик підтримує високу доступність сховища для робочого навантаження.

2.4.4 Розширені можливості управління

SAN підтримує ряд корисних функцій сховища корпоративного класу, включаючи шифрування даних, Дедуплікація даних, реплікацію сховища і технології самовідновлення, призначені для максимального збільшення ємності сховища, безпеки і стійкості даних. Функції повністю централізовані і можуть бути легко застосовані до всіх ресурсів зберігання в SAN.

2.5 Недоліки SAN

Незважаючи на переваги, SAN навряд чи ідеальний, і є ряд потенційних недоліків, які IT-керівники повинні враховувати перед розгортанням або модернізацією SAN.

2.5.1 Складність

Хоча сьогодні для SAN існує більше варіантів конвергенції, таких як FCoE і уніфіковані варіанти, традиційні SAN представляють собою додаткову складність у вигляді другої мережі - в комплекті з дорогими HBA на хост-серверах, комутаторами і кабелями в складній і надлишкової структурі. Такі мережі повинні проектуватися і підтримуватися з обережністю. Ця складність стає все більш проблематичною для IT-організацій з невеликою кількістю персоналу і обмеженим бюджетом.

2.5.2 Масштаб

З огляду на вартість, SAN зазвичай ефективна тільки в більших і складних середовищах, де є багато серверів і значний обсяг сховища. Звичайно, можна реалізувати SAN в невеликих масштабах, але буде важко виправдати вартість і складність. У невеликих розгортання часто можна досягти задовільних результатів з використанням iSCSI SAN, конвергентної SAN в єдиній загальній мережі, такий як FCoE, або розгортання HCI, яке здатне об'єднувати і виділяти ресурси.

2.5.3 Управління

З урахуванням того, що складність зосереджена на апаратному забезпеченні, існує серйозна проблема в управлінні SAN. Налаштування функцій, таких як зіставлення LUN або зонування, може бути проблематичною. Налаштування RAID і інших технологій самовідновлення, а також відповідне ведення журналу і звітність - не кажучи вже про безпеку - можуть зайняти багато часу, але неминучі для підтримки відповідності вимогам організації.

2.6 SAN і NAS

Мережеве сховище (NAS) - це альтернативний спосіб зберігання і доступу до даних, заснований на файловому протоколі, такому як SMB і NFS, на відміну від блокових протоколів, таких як FC і iSCSI, використовуваних в SAN. Якщо SAN використовує мережу для підключення серверів і сховища, NAS покладається на виділений файловий сервер, розташований між серверами і сховищем.

Хоча обидва підходи зберігають дані, вибір системи буде залежати від типу оброблюваних даних. SAN - кращий вибір для блочного сховища даних, яке зазвичай добре підходить для структурованих даних, наприклад сховища для додатків реляційних баз даних корпоративного класу. Для порівняння, NAS - з його файловим підходом - краще підходить для неструктурованих даних, таких як файли документів, електронні листи, зображення, відео та інші поширені типи файлів.

Як і у випадку з SAN, NAS консолідує сховище в єдиному просторі і може підтримувати завдання управління і захисту даних, такі як архівування та резервне копіювання даних. Проте NAS використовує загальну мережу і забезпечує набагато меншу вартість і складність, ніж SAN. Однак мережі SAN відрізняються продуктивністю і масштабованість, здатними забезпечити найвищу продуктивність для найвимогливіших корпоративних додатків.

SAN і NAS не виключають один одного. SAN і NAS можуть співіснувати в одному центрі обробки даних, де потрібно як блочне, так і файлове сховище даних. Системи SAN, як і NAS можна модернізувати для підвищення продуктивності, оптимізації управління, боротьби з обмеженням ємності сховища. У деяких випадках окремі системи зберігання можна замінити уніфікованою системою зберігання або спростити мережу SAN за допомогою iSCSI SAN [9].

2.7 Безпека в мережах передачі даних

Сучасні корпорації накопичують терабайти даних і для їх зберігання використовують системи NAS і SAN. Однак в силу своєї конструкції дане обладнання не передбачає вбудованих засобів розмежування доступу до даних між окремими користувачами або їх групами. Інформація при цьому

сконцентрована в одному місці, і потенційна ступінь її уразливості досить висока.

Високий ступінь консолідації обертається небезпекою несанкціонованого доступу по відкритих каналах, так як всі вузли знаходяться в єдиній мережі. Злом одного або декількох вузлів в корпоративній мережі зберігання даних може привести до катастрофічних наслідків для бізнесу.

У зв'язку з тим, що 50-80% атак починаються всередині мережі, більшість організацій визнають, що їх найбільш критична інформація "за замовчуванням" знаходиться під загрозою. Такі рішення, як міжмережеві екрани або віртуальні приватні мережі забезпечують загальну захист периметра корпоративної мережі, а центральні сховища даних залишаються уразливими для внутрішніх і зовнішніх атак.

SAN являє собою відокремлену мережу, відділену від локальної, з можливістю зберігання величезних обсягів інформації, які можна нарощувати практично нескінченно. Типова SAN включає ряд дискових масивів, підключених до комутатора, який, в свою чергу, з'єднаний з серверами, що служать для організації доступу до збережених даних. Технічну основу мережі зберігання даних складають волоконно-оптичні з'єднання, адаптери шини вузла FC HBA і FC-комутатори, в даний час забезпечують швидкість передачі 200 Мбайт / с і віддаленість між сполучаються об'єктами до 10 км (до 120 км за допомогою спеціальних рішень). SAN дозволяє з будь-якого сервера отримати доступ до будь-якого накопичувача, не завантажуючи при цьому ні інші сервери, ні локальну мережу компанії. Крім того, можливий обмін даними між системами зберігання без участі серверів.

Істотним недоліком SAN є висока ціна. Вартість обладнання і проекту по впровадженню мережі може становити до декількох сотень тисяч доларів. Однак досвід показує, що такі суми витрачаються не марно, адже мережеве зберігання даних дозволяє створювати інформаційні системи високої готовності та безвідмовності в роботі.

Завдяки використанню в SAN Fibre Channel вдалося домогтися максимального захисту інформації. Набір вбудованих в SAN інструментів включає аутентифікацію хостів шляхом процедур Fabric Login і Process Login, управління доступом хостів до цілей за допомогою розбиття на зони і списків доступу, і, що не менш важливо, технологію VSAN. Остання ділить SAN на безліч віртуальних комутуючих структур.

Найбільш очевидна перевага SAN - зменшення навантаження на локальну мережу. У мережі зберігання можна запустити процедуру повного резервного копіювання, при цьому не побоюватися негативного впливу на трафік додатків. Як відомо, резервне копіювання помітно уповільнює роботу інших додатків, а оскільки мережа зберігання використовує дуже швидкий мережевий протокол, то це значно скорочує час для створення резервної копії. Більш того, ємність SAN відносно легко збільшити, додаючи нові дискові масиви. Останнім часом в SAN стали застосовувати технології віртуалізації пам'яті. По суті, за допомогою віртуалізації сервери можуть використовувати кілька жорстких дисків (або їх певну ємність) як один логічний том. Безпека в SAN реалізується на рівні сервера SAN, в той час як в NAS застосовується безпеку на рівні доступу до файлів. І в тому і в іншому випадку додаткові засоби керування даними забезпечують реплікацію даних, моментальні знімки даних, високошвидкісне архівування та відновлення.

2.7.1 Інформаційні ризики

Серед можливих загроз щодо мереж зберігання даних можна виділити наступні:

- фізичне знищення;
- розкрадання;
- несанкціоноване спотворення даних;
- порушення автентичності даних;
- підміна даних;
- блокування доступу до масиву даних.

Джерела загроз можуть бути як зовнішніми, так і внутрішніми. Сама по собі загроза - наслідок вразливостей в конкретних вузлах мережі зберігання. Можливі уразливості визначають складові елементи і властивості архітектурних рішень мереж зберігання, а саме:

- елементи архітектури;
- протоколи обміну;
- інтерфейси;
- апаратні платформи;
- системне програмне забезпечення;
- умови експлуатації;

- територіальне розміщення вузлів мережі зберігання.

Розглянемо проблему безпеки за рівнями надання необхідних служб. Доцільно виділити чотири рівня, щодо яких ми спробуємо викласти основні аспекти безпеки для NAS і SAN:

- рівень пристроїв;
- рівень даних;
- рівень мережевої взаємодії;
- рівень управління і контролю.

2.7.2 Рівень пристроїв

Стосовно до SAN в першу чергу загроза несанкціонованого доступу до пристрою може виникнути внаслідок слабкої пральний захисту і непродуманої схеми авторизації користувачів. В цьому випадку несанкціонований доступ із захопленням всіх прав дає абсолютний контроль над цим вузлом (комутатором або шлюзом), в результаті чого виникає реальна загроза порушення цілісності архітектури і збережених даних.

Інша небезпека може виникнути внаслідок вразливості на рівні програмно-апаратних засобів пристрою, де зберігаються дані, або через відсутність уваги до питань безпеки щодо використовуваного микрокода. Зловмисник отримує можливість використовувати даний пристрій для віддаленої атаки на інші вузли мережі зберігання (сервери, робочі станції, шлюзи, комутатори).

Для авторизації користувачів слід задіяти схему із застосуванням списків контролю доступу (Access Control List). Найчастіше необхідно обмежити доступ до пристрою за допомогою багатофакторної ідентифікації.

На цьому рівні NAS працюють як файлові сервери. Однак крім традиційних каналів, для доступу до пристроїв зберігання (в тому числі до зовнішніх по відношенню до самого сервера NAS) можуть бути задіяні елементи архітектури SAN. Як правило, це жорсткі диски, підключені до сервера по оптичних лініях з використанням протоколів Fibre Channel або FC-AL. В такому випадку на даний сегмент повинні поширюватися вимоги, аналогічні тим, що висуваються до архітектури SAN.

Які типи вразливостей притаманні даному рівню? Наявність налаштувань за замовчуванням, а також обмеженість функцій з

адміністрування призводить до підвищення ймовірності використання слабкостей схеми авторизації при недостатній пральний захисту. В силу закритості операційної системи і включених фабричних настройок існує загроза можливих атак на незадіяні служби, DNS, Telnet і т. п.

2.7.3 Рівень даних

В архітектурі SAN при не авторизованому доступі з адміністративними правами користувач отримує повний або частковий контроль над даними, в зв'язку з чим виникає небезпека блокування доступу, спотворення або модифікації, а також знищення даних. Великий ризик встановлення контролю доступу до блоків даних на рівні самих серверів. Незважаючи на те що для архітектури SAN характерний блоковий доступ до збережених даних, самі обчислювальні вузли в разі активізації відповідних служб можуть виступити в ролі серверів NAS з наданням доступу за протоколами CIFS / SMB, а також NFS. Архітектура SAN передбачає підключення серверів і робочих станцій з єдиної зоною доступу до пристроїв зберігання. Тому вимога безпеки при доступі до даних має застосовуватися в рівній мірі як до серверів, так і до робочих станцій. Таким чином виключається виконання серверами додатків невластивою їм ролі вузлів NAS, через які зловмисник міг би отримати несанкціонований доступ до конфіденційної інформації.

З огляду на, що доступ до даних на серверах NAS здійснюється за протоколами CIFS / SMB і NFS, саме вони будуть розглядатися з точки зору можливих загроз. Згадані протоколи передбачають лише слабкий захист переданих паролів, особливо це стосується NFS. Коли це можливо, від використання NFS необхідно відмовитися, відключивши відповідну службу. Якщо ж до конфіденційності даних пред'являються високі вимоги, щоб уникнути компрометації паролів повинні бути передбачені додаткові заходи по авторизації користувачів із застосуванням необхідних програмно-апаратних засобів.

Уже на етапі опрацювання архітектурного рішення слід ввести жорстку класифікацію збережених даних за ступенем їх важливості і конфіденційності, причому не варто забувати про інші ефективні засоби безпеки, зокрема організації виділених вузлів криптографічного захисту.

2.7.4 Рівень мережевої взаємодії

Історично склалося так, що архітектура SAN розвивалася завдяки впровадженню оптичних каналів з використанням протоколу Fibre Channel. Основним їх перевагою є висока швидкість передачі, відсутність взаємних перешкод між прокладені кабелі і низька затримка сигналу. Вирішення питань безпеки щодо переданої по каналах інформації не було пріоритетним. І тільки в даний час питань захищеності стали приділяти більше уваги. З точки зору безпеки на рівні мережного взаємодії слід зазначити загрози несанкціонованого підключення до каналів з підміною адрес, що в рівній мірі відноситься до обладнання та каналів як в самих центрах обробки даних, так і у філіях. В силу відкритості архітектури і взаємної віддаленості пристроїв, що комутують і конвертують, пристрої можуть стати об'єктами атаки з подальшою втратою контролю над каналами і отриманням зловмисником несанкціонованого доступу до переданих даних. Невірно сконфігуровані кінцеві пристрої мережі зберігання також стають привабливою мішенню для атаки.

Оскільки мережевий рівень серверів NAS в більшості випадків організований па базі протоколу TCP / IP, основна загроза виходить від можливих атак через мережу: DoS, перехоплення сеансів, підміна адрес і т.п. Внаслідок відкритості архітектур пристрої NAS можуть бути підключені як всередині корпоративного мережевого сегмента, так і за його межами. Останнє відбувається досить часто при наявності великої кількості філій всередині однієї компанії. Якщо трафік виходить за межі контрольованого мережного сегмента, обов'язково повинні бути встановлені брандмауери, а також кошти IDS. Для підвищення ступеня безпеки можна задіяти віртуальні локальні мережі, забезпечивши тим самим незалежність трафіку всередині кожного з створених сегментів і виключивши ризик його прослуховування і дістування несанкціонованого контролю над ним.

2.7.5 Рівень управління доступом

Всі засоби управління доступом до збережених даних повинні задовольняти вимогам безпеки в максимальному ступені - це стосується як конкретних пристроїв, так і архітектури в цілому (щоб виключити будь-яке неавторизоване вторгнення). Для цього необхідно, зокрема, забезпечити

постійний моніторинг користувачів, що мають права доступу, і здійснювати централізований контроль за роботою пристроїв. Рішення завдання безпечного управління доступом спрощує спеціалізоване програмне забезпечення.

Парольний захист слід посилити шляхом контролю мінімальної довжини слова і введенням примусової періодичної зміни паролів. Більш того, доступ до вузлів SAN необхідно розмежовувати за допомогою завдання відповідної політики, де враховувалися б роль кожного користувача і ступінь конфіденційності даних, що зберігаються. З цією метою можна використовувати і списки контролю доступу.

На відміну від SAN, доступ до даних на вузлах NAS здійснюється на рівні файлів. При цьому сам вузол функціонує як файловий сервер, а потреба в його конфігурації і налаштувань мінімальна. Найчастіше виробники серверів NAS (в силу досить вузької спеціалізації) більшу частину налаштувань виконують до поставки сервера до замовника, і згодом за замовчуванням використовуються саме вони. Цю обставину необхідно враховувати при інтеграції серверів NAS як в локальну мережу, так і в мережу зберігання даних.

Одна з найбільш частих атак на сервери NAS - несанкціонований доступ з використанням слабкого захисту при передачі паролів по мережі за допомогою протоколів Telnet і HTTP.

Як і на всіх розглянутих раніше рівнях, важливо здійснювати строгий контроль за системними журналами [10].

3 РОЗРОБКА АЛГОРИТМУ ОРГАНІЗАЦІЇ БЕЗПЕЧНОГО ПІДКЛЮЧЕННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ДО ІНТЕРНЕТУ

На будь-якому підприємстві, в ЛІКМ якого обробляється конфіденційна інформація, виникає необхідність її захисту. Постійно йде створення більш досконалих каналів передачі даних, способів захисту цих каналів, їхньої технології і програмного вдосконалення системи передачі даних. Залежно від каналів передачі даних, в яких циркулює інформація, застосовуються різні методи її захисту і потрібні концептуально різні підходи до захисту.

Для підприємств, які мають віддалені офіси, найбільш оптимальним стане використання віртуальних приватних мереж. Віртуальні приватні мережі (VPN – Virtual Private Network) це захищене з'єднання, яке створюється всередині незахищеною мережі з використанням відкритих каналів зв'язку шляхом створення зашифрованого каналу. Простіше кажучи, таке з'єднання можна уявити як тунель, прокладений через інтернет.

Віртуальні мережі набули великого поширення за рахунок економічності і високої безпеки, особливо при використанні розподілених обчислювальних мереж. В технології VPN для захисту комп'ютерних мереж використовуються технології, що включають в себе елементи міжмережевого екранування і механізми криптографічного захисту мережевого трафіку [11].

VPN за допомогою спеціальних програм об'єднує окремі комп'ютери і локальні мережі для захисту інформації, що передається. При з'єднанні з сервером, що знаходяться в мережі загального доступу VPN, технологія утворює канал захищається інформацію за допомогою алгоритмів шифрування. Таким чином всередині незахищеною мережі утворюється захищений тунель для передачі даних. Простіше кажучи, VPN дозволяє віртуально підключити одну мережу до іншої таким чином, як ніби вони з'єднані проводами, при цьому весь вихідний і вхідний трафік шифрується, що робить цю технологію безпечною.

Для розробки алгоритму необхідно представити типову структуру організації мережі підприємства. За основу взято підприємство малого чи середнього бізнесу, що має центральний офіс і кілька віддалених, і для якого потрібно здійснювати обмін конфіденційної інформації між офісами. Внаслідок обмеженості бюджету зміст виділених провайдером каналів не

представляється можливим, тому обмін інформацією забезпечується через відкриті канали інтернету.

Потрібно розробити архітектуру, що включає наступні компоненти:

структуру головного і віддалених офісів, що мають можливість здійснювати інформаційний обмін між собою;

організацію безпечної мережевої інфраструктури, характерної для мереж будь-якого масштабу і забезпечує захист від основних загроз інформаційній безпеці;

гнучкі можливості мережевих налаштувань.

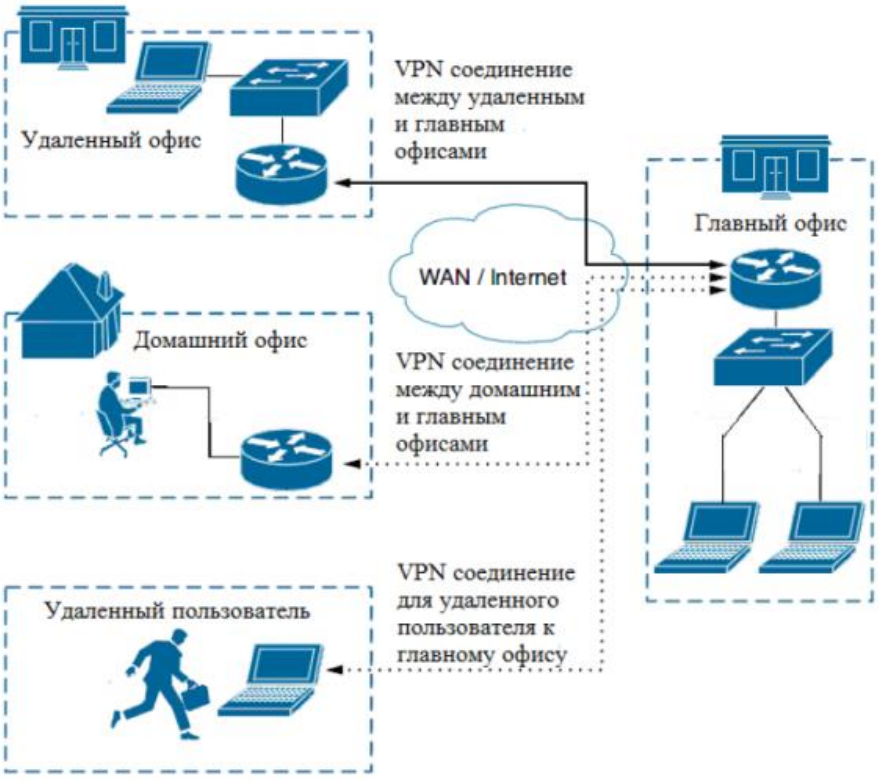
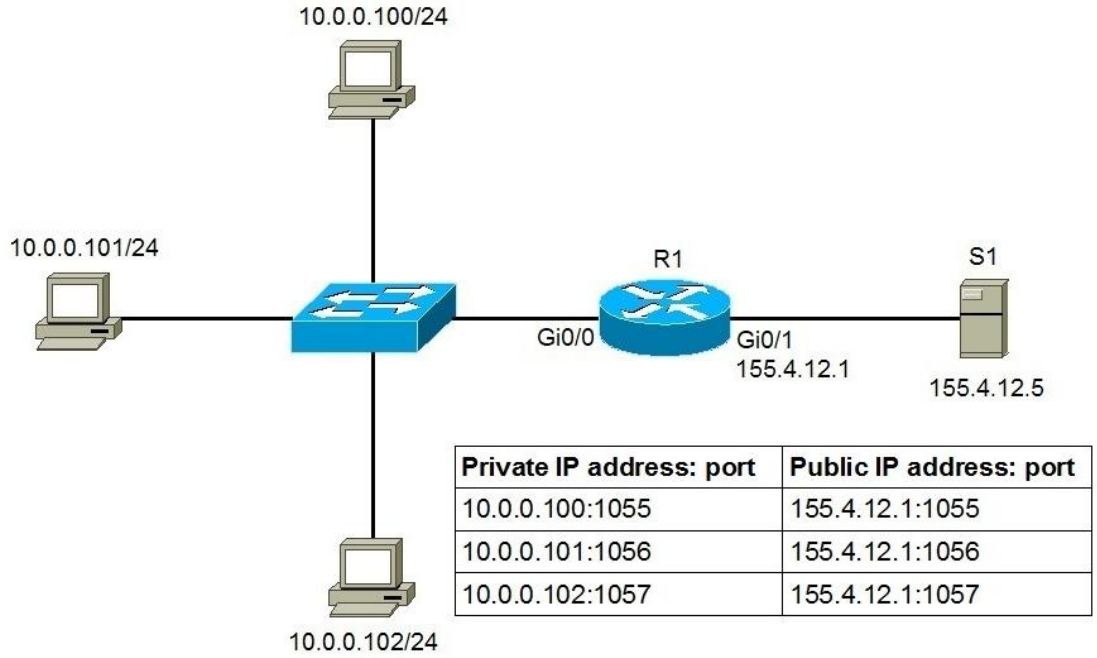


Рисунок 3.1- Високорівнева мережева діаграма

На рис. 3.1 представлена високорівнева мережева діаграма, що демонструє різні типи бізнес-підключень, які можуть бути реалізовані з використанням розробляється архітектури, що включає в себе центральний офіс і два віддалених офісу. Мережа побудована за допомогою WAN-маршрутизаторів (Cisco 2811) і LAN-комутаторів (Cisco Catalyst 2960). Для організації та підтримки даних можливостей при розробці архітектури будуть використані наступні технології.

Standard Cisco IPSec, що забезпечує VPN з'єднання між офісами підприємства; динамічна маршрутизація на основі протоколу OSPFv2. IP Security - це комплект протоколів, що стосуються питань шифрування, аутентифікації і забезпечення захисту при транспортуванні IP-пакетів; до його складу зараз входять майже 20 пропозицій по стандартам і 18 RFC. Продукти Cisco для підтримки VPN використовують набір протоколів IPSec, є на сьогодні промисловим стандартом забезпечення широких можливостей VPN. IPSec пропонує механізм захищеної передачі даних в IP-мережах, забезпечуючи конфіденційність, цілісність і достовірність даних, що передаються через незахищені мережі типу Internet [37].



Private IP address: port	Public IP address: port
10.0.0.100:1055	155.4.12.1:1055
10.0.0.101:1056	155.4.12.1:1056
10.0.0.102:1057	155.4.12.1:1057

Рисунок 3.2 - Технологія PAT [44]

Технологія PAT для трансляції приватних IP-адрес в публічний IP-адреса. PAT (Port Address Translation) - технологія трансляції адрес з використанням портів. Дана технологія вирішує проблему доставки зворотних пакетів. Оскільки кількість білих IP обмежена нам необхідно економити ці адреси. Для цього була створена технологія PAT. Вона дозволяє локальним хостам використовувати приватні IP-адреси і встановити один зареєстровану адресу на маршрутизатор доступу. В технології перетворення адрес PAT використовується особливість роботи протоколу TCP: з точки зору сервера абсолютно все одно, здійснюються з'єднання з трьома різними хостами з

різними адресами або з'єднання встановлюються з одним хостом на один IP-адреса, але з різними портами. Отже, щоб підключити до Інтернету безліч хостів невеликого офісу за допомогою одного тільки зареєстрованого публічного IP адреси, служба PAT транслює приватні адреси локальних хостів в один наявний зареєстрований. Щоб правильно пересилати пакети зворотного комунікації локальним хостам, маршрутизатор зберігає у себе таблицю IP адрес і номерів портів для протоколів TCP і UD [34].

Рисунок 3.3 - Списки доступу ACL [45]

Списки доступу ACL для обмеження доступу до ресурсів мережі підприємства. ACL (Access Control List) - це набір текстових виразів, які щось дозволяють, або щось забороняють. Зазвичай ACL дозволяє або забороняє IP-пакети, але крім усього іншого він може заглядати всередину IP-пакета, переглядати тип пакету, TCP і UDP порти. Також ACL існує для різних мережевих протоколів (IP, IPX, AppleTalk і так далі). В основному застосування списків доступу розглядають з точки зору пакетної фільтрації, тобто пакетна фільтрація необхідна в тих ситуаціях, коли у вас коштує обладнання на кордоні Інтернет і приватної мережі і потрібно відфільтрувати непотрібний трафік. Ви розміщуєте ACL на вхідний напрямку і блокуєте надлишкові види трафіку [35, 36].

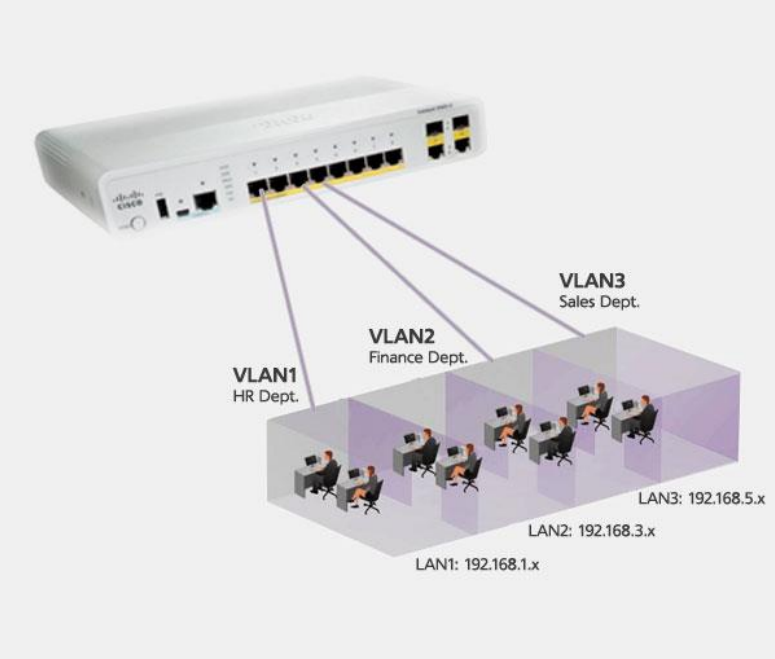


Рисунок 3.4 - Технологія VLAN

Технологія VLAN для розмежування доступу всередині широкомовного домену локальної мережі. Це мережа віртуального типу, налаштувати її можна на світче (смарт або керованому) другого рівня. По-іншому вона називається широкомовним доменом. По суті, VLAN являє собою мітку в кадрі, передану по мережі. У неї є ID. Під нього відводиться 12 біт, тобто мітка може мати нумерацію від 0 до 4095. Важливо враховувати, що зарезервовані 1-й і останній номери, використовувати їх не можна. Вілани - прерогатива не робочих станцій, а комутаторів. На портах таких пристроїв зазначено, в який віртуальної мережі вони знаходяться: весь трафік, що виходить через порт, буде відзначатися міткою - VLANом. Завдяки цьому він надалі зможе йти і через інші інтерфейси світчей, що працюють під цією позначкою. При цьому інші порти цей трафік приймати не будуть. Таким чином, створюється окрема підмережа, що не вступає у взаємодію з іншими підмережами без використання комутатора або роутера. VLAN дозволяє: 1. Побудувати мережу з незалежної логічною структурою. Побудова її топології не буде залежати від того, де фізично знаходяться компоненти мережі; 2.Розбити один такий домен на кілька: трафік широкомовного типу, який належить одному домену, не буде проходити через інший. Це дозволяє менше навантажувати мережеве обладнання. 3.Захистити мережу від стороннього втручання. Порт світча

зможе ігнорувати і відкидати кадри, які надходять з інших VLAN, причому незалежно від початкового IP. 4.Групувати ПК, які входять в одну підмережу, і застосовувати політики на всю групу. 5. Здійснювати маршрутизацію за допомогою використання віртуальних портів [39].

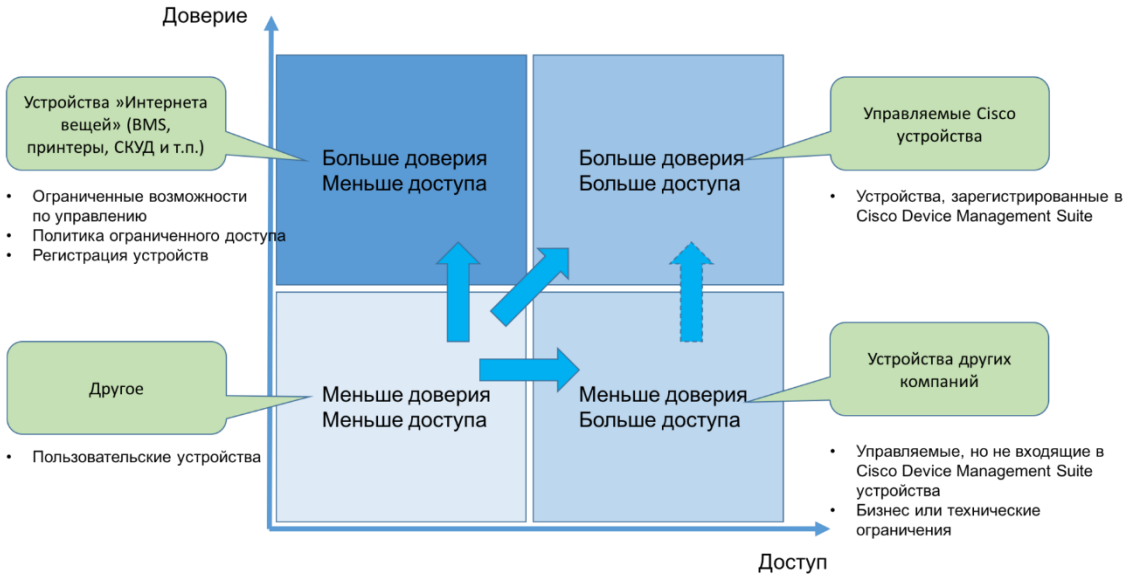


Рисунок 3.5 – Принцип контролю доступу

Контроль доступу до мережевих пристроїв на основі парольної аутентифікації з використанням списку привілеїв. Контроль доступу в мережу розроблено для допомоги в забезпеченні достатнього захисту від загроз безпеки на всіх провідних і бездротових кінцевих пристроях (зокрема, на ПК, лептопах, серверах,), які отримують доступ до мережевих ресурсів. NAC дає компаніям можливість проаналізувати і проконтролювати всі пристрої, які звертаються до мережі. Стежачи за тим, щоб на кожному кінцевому пристрої дотримувалася корпоративна політика безпеки і діяли оновлені і найбільш підходящі механізми захисту, компанії можуть значно скоротити або взагалі звести до нуля кількість кінцевих пристроїв, які виступають традиційним джерелом зараження або злому мереж. Контроль доступу в мережу (Network Admission Control, NAC) - це набір технологій і рішень, фундаментом яких є загальногалузева ініціатива, реалізована під патронажем Cisco Systems. NAC використовує інфраструктуру мережі для контролю над дотриманням політики безпеки на всіх пристроях, які прагнуть отримати доступ до ресурсів мережі. Цим шляхом знижується збиток, який можуть заподіяти виникаючі загрози безпеки. Використовуючи NAC, клієнти

отримують можливість надавати мережевий доступ тільки дотримують запропоновані вимоги, безпечним кінцевим пристроям (наприклад, комп'ютерів, серверів і КПК) і обмежувати доступ для пристроїв, які не відповідають вимогам. NAC - елемент із самозахистом мережі Cisco, стратегії, яка істотно підвищує здатність мережі автоматично ідентифікувати і запобігати виникаючі загрози безпеки, а також адаптуватися до них. Cisco пропонує підходи до впровадження NAC на базі пристроїв (NAC Appliance) і на базі архітектури (NAC Framework), які відповідають функціональним та операційним запитам будь-якої компанії. При цьому компаніям може бути необхідна як найпростіша політика безпеки, так і підтримка складних структур безпеки, в яких інструменти забезпечення безпеки від різних розробників об'єднані з корпоративним рішенням з управління настільними пристроями. Пристрій NAC (NAC Appliance) на базі лінійки продуктів Cisco Clean Access забезпечує швидке розгортання з автономними сервісами експертизи кінцевих пристроїв, управління політикою та прийняття корегувальних заходів. Пристрій NAC - автономна, виконана "під ключ" версія NAC, комплексне повнофункціональним рішенням. В архітектурі NAC (NAC Framework) реалізований підхід на базі архітектури з інтеграцією систем різних розробників. Тут для вирішення проблеми контролю доступу в мережу застосовуються мережева інфраструктура Cisco і рішення сторонніх розробників. Інтелектуальна інфраструктура мережі об'єднана з рішеннями понад 60 розробників провідних антивірусних програм та іншого програмного забезпечення в області безпеки і управління [40].

Віддзеркалення трафіку на комутуючі пристрої для контролю активності мережі [41].

Віддалене управління мережевими пристроями на основі захищеного протоколу SSH (англ. Secure SHell - захищена оболонка) - мережевий протокол прикладного рівня, призначений для безпечного віддаленого доступу до UNIX-системам. Даний протокол ефективний тим, що шифрує всю інформацію, що передається по мережі, на відміну від протоколу telnet. В основному він потрібен для віддаленого управління даними користувача на сервері, запуск утиліт команд, роботи в командному режимі з базами даних [42] Щоб забезпечити SSH доступ користувачеві необхідні SSH-клієнт і SSH-сервер. Кожна операційна система має свій набір програм, що забезпечують з'єднання. Так, для Linux це lsh (server і client), openssh (server і client). Для Mac

OS часто використовується NiftyTelnet SSH. А в ОС Windows для реалізації з'єднання через SSH протокол найчастіше використовується додаток PuTT. Для використання PuTTY необхідно завантажити та інсталювати додаток, після чого в графічному інтерфейсі можна здійснити настройку програми. Додаток має 4 вкладки: Session. У цій вкладці здійснюється настройка підключення до сервера. Terminal. Тут можна коригувати налаштування роботи терміналу, через який і здійснюється вся робота. Connection. У цій вкладці можна задати параметри підключення, вибрати алгоритм шифрування і задати інші настройки з'єднання. Window. У цьому вікні користувач може вибрати зовнішній вигляд програми, змінити шрифт і колір тексту [43].

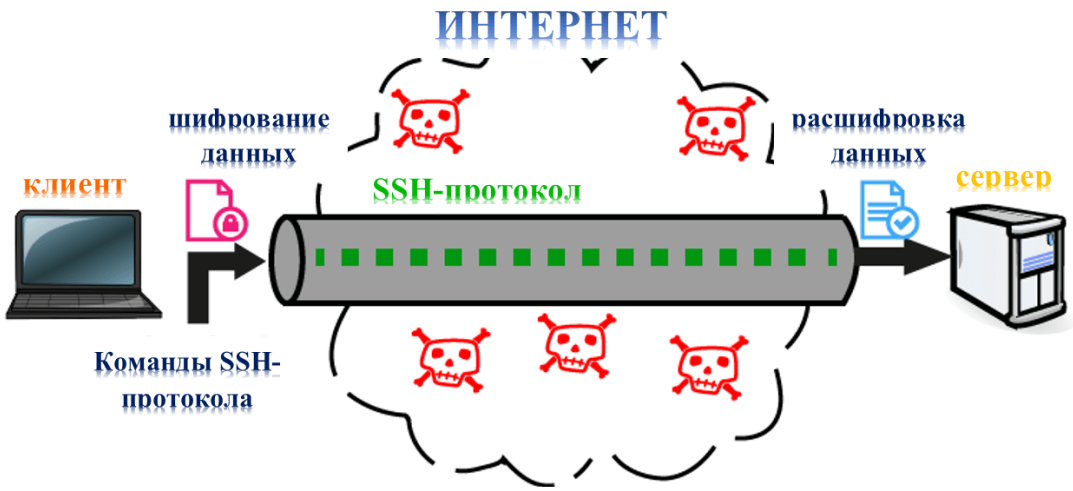


Рисунок 3.6 – Передача даних за SSH протоколом через небезпечну мережу

Для реалізації алгоритму необхідно було вибрати середовище моделювання, що відповідає вимогам організації локальної розподіленої мережі підприємства. Для даної мети було запропоновано використовувати офіційне середовище моделювання Cisco Packet Tracer v 6.2, в якій була побудована і налаштована розподілена локальна мережа, яка використовує канали загального доступу для організації взаємодії між офісами (рис. 3.2)

Перед підключенням локальної мережі офісу до інтернету необхідно забезпечити внутрішню безпеку локальної мережі, тому була обрана представлена черговість дій [12]:

1. Забезпечення безпеки локальної мережі (розмежування доступу до мережевих пристроїв, настройка віддаленого управління мережевими

пристроями, настройка контролю додавання нових пристроїв, конфігурація VLAN).

2. Організація безпечного підключення до мережі інтернет (налаштування дзеркалювання трафіку на центральному комутаторі, настройка списків доступу до локальних і віддалених ресурсів, реалізація VPN-з'єднання Standard Cisco IPSec між віддаленими офісами, настройка PAT).

3. Перевірка функціонування і захищеності мережі.

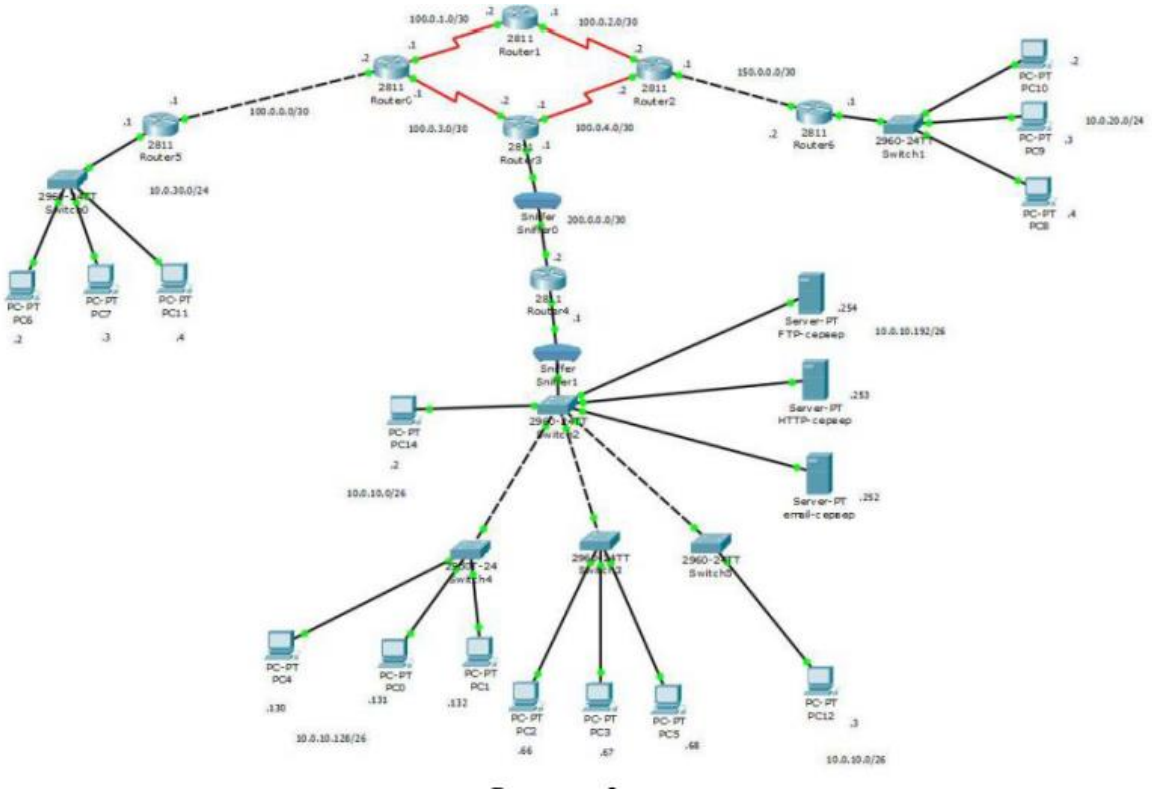


Рисунок 3.7 – Розподілена локальна мережа

Розмежування доступу до мережевих пристроїв розглядається як необхідний захід, що обмежує доступ до зміни налаштувань мережевого обладнання і є обов'язковою мірою для прикордонного мережевого обладнання [13]. для коректного використання мережевих пристроїв і поділу обов'язків потрібно ввести привілейований доступ до пристроїв:

- користувач не може застосовувати зміни і дивитися файли конфігурації;

Таблиця 3.1 – Характеристика запропонованих сервісів

Сервіс	Характеристика
Контроль додавання пристроїв	Реалізується за рахунок налаштування безпеки портів на комутаторах доступу. Кожному інтерфейсу комутатора ставиться у відповідність MAC-адреса дозволеного для цього інтерфейсу мережевого адаптера. Дане рішення також здатне захистити локальну мережу від атак типу «відмова в обслуговуванні», які реалізуються з допомогою переповнення таблиці MAC-адрес.
Конфігурація VLAN	Кожен підрозділ прив'язаний до свого комутатора доступу і знаходиться у власній VPN, інтерфейси даних комутаторів асоціюються з номером цієї віртуальної мережі. Інтерфейси комутаторів, які повинні передавати трафік декількох VPN, позначаються як trunk-інтерфейси; на прикордонному маршрутизаторі виділяються кілька підінтерфейсів для кожного VLAN.
Віддзеркалення трафіку на центральному комутаторі	Використовується для контролю, приходить з мережі інтернет трафіку за допомогою IDS або аналізатора трафіку, який встановлений на робочої станції, контрольованої системним адміністратором. З використанням віддзеркалення здійснюється приховування контролю трафіку для звичайних користувачів мережі і зловмисників.
Налаштування списків доступу ACL.	Основними є списки доступу до загальних ресурсів мережі - серверів. Дані списки частково виконують функції брандмауера, оскільки здатні фільтрувати трафік за адресою призначення, джерела, типу протоколу. Внаслідок того, що контроль адрес здійснюється на прикордонному маршрутизаторі, завданням для списків доступу до серверів є контроль допустимих для використання портів.
Реалізація VPN-з'єднання між віддаленими офісами.	Налаштування прикордонних маршрутизаторів характеризується методом обміну ключами (ISAK.MP), методом шифрування (AES), алгоритмом хешування (SHA-1), методом аутентифікації (обмін ключами коли ви створюєте з'єднання), обмін ключами методом Діффі-Хеллмана другої групи (1024 біта).
Налаштування PAT	ускладняються використанням технології VPN для правильної конфігурації, якій необхідно виключення з транслювання трафіку між віддаленими офісами, так як протокол IPSec вже виробляє трансляцію для зазначеного в його списках доступу трафіку.
Перевірка працездатності і захищеності мережі	Перевірка працездатності і захищеності мережі, реалізованої за допомогою запропонованого алгоритму, проводиться поетапно. Першим етапом є перевірка працездатності та захищеності мережевого обладнання локальної мережі. другим етапом вважається перевірка працездатності та захищеності доступу в інтернет і взаємодії з віддаленими офісами.

- агент підтримки також має можливості користувача і доступ до команди ping;

- помічник адміністратора має можливості агента підтримки і можливість перезавантаження обладнання;
- адміністратор має повний доступ до конфігурації пристрою;
- підключення по протоколу telnet (настройка віддаленого доступу) вкрай небезпечно, оскільки передає паролі по мережі у відкритому вигляді; для захисту даного конфіденційного трафіку використовується протокол SSH.

Таким чином, в результаті застосування запропонованого нами алгоритму налаштування VPN можуть бути протестовані на коректність і відповідність вимогам безпеки. Змодельована захищена локальна мережа здатна протидіяти основним загрозам безпеки і може бути застосована на практиці.

4 ДОСЛІДЖЕННЯ МЕТОДІВ БЕЗПЕЧНОГО НАЛАШТУВАННЯ ДЛЯ МАРШРУТИЗАТОРІВ І ТОЧОК ДОСТУПУ Wi-Fi ЛОКАЛЬНОЇ МЕРЕЖІ

4.1 Інформаційні ризики використання маршрутизаторів

Маршрутизатор - це пристрій, який працює на мережевому рівні моделі OSI, основною функцією якого є вибір шляху і пересилання пакетів. Маршрутизатор можуть бути основним мережевим обладнанням в будь-якій організації, тому безпека маршрутизатора викликає серйозне занепокоєння. Існують різні типи атак маршрутизатора, про які повинні знати мережеві фахівці.

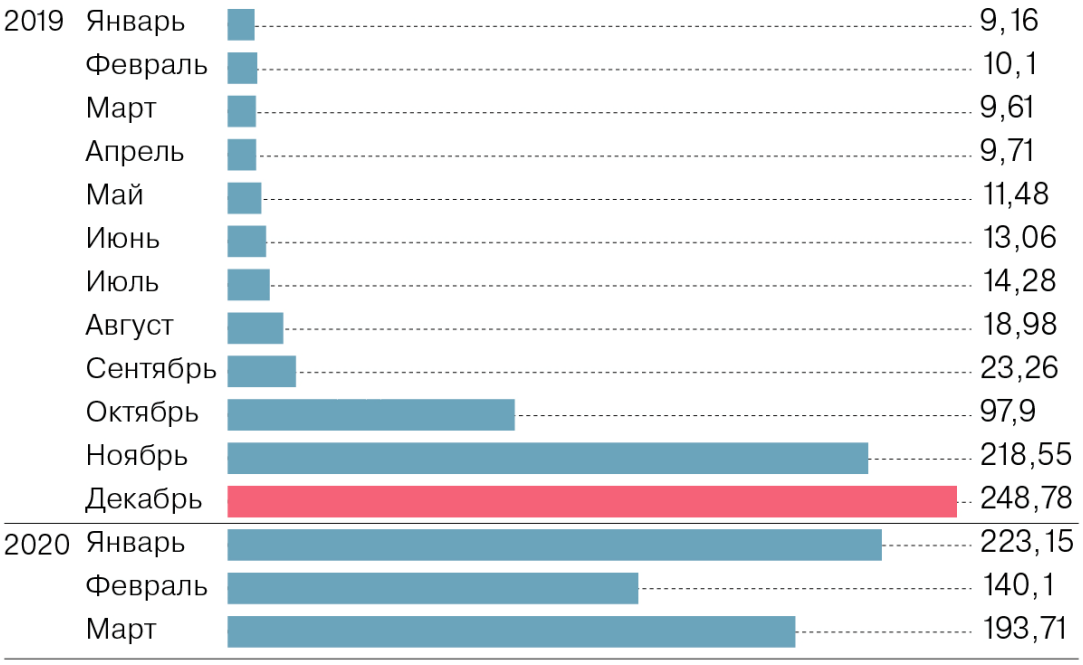


Рисунок 4.1 – Кількість спроб «жорсткого зламу» паролів маршрутизаторів (в мільйонах, дані Trend Micro) [49]

Компанія Trend Micro, що займається розробкою програмного забезпечення в сфері кібербезпеки, опублікувала доповідь, згідно з яким хакери стали набагато частіше атакувати маршрутизатори (роутери). Причому в першу чергу атакам піддаються домашні пристрої. За даними Trend Micro, різке зростання спроб злому роутерів спостерігається з жовтня 2019 року. Якщо на початку 2019 року фіксувалося по 9-10 млн спроб в місяць, то у

вересні - вже 23 млн, в жовтні це число підскочило майже до 100 млн, а в грудні досягло піку в майже 250 млн спроб. Як наголошується в доповіді, це тільки цифри «грубого злому», коли хакери намагаються підібрати пароль до пристрою за допомогою програмного забезпечення, яке просто перебирає всі найбільш поширені варіанти. «У випадку з інтернет-пристроями на зразок роутерів, цей процес займає досить мало часу, так як на багатьох роутерах за замовчуванням встановлені загальновідомі паролі», - йдеться в доповіді [49].

Атаки маршрутизаторів мережі типу «Відмова в обслуговуванні» - DoS-атака виконується зловмисником, у якого є мотивація на відправку величезної кількості пакетів (flooding) маршрутизатора або інших пристроїв, що впливає на доступність. Відправка більшої кількості ICMP-пакетів з декількох джерел робить маршрутизатор нездатним обробляти трафік. Якщо маршрутизатор не може обробляти трафік, він не може надавати послуги в мережі, а вся мережа відключається, що впливає на повсякденну діяльність організації.

Атаки роутерів з використанням некоректних пакетів - у цьому типі атаки після того, як відбувається зараження системи шкідливим кодом, маршрутизатор просто неправильно обробляє звичайний мережевий потік. Роутер не може організувати процес маршрутизації і починає неправильно обробляти пакети. Заражений пристрій не може правильно обробити пакети і створює в мережі петлі, відмову в обслуговуванні, перевантаження і т.п. Цей тип атаки дуже важко виявити і знешкодити.

«Отруєння» таблиці маршрутизації - маршрутизатор використовує таблицю маршрутизації для відправки пакетів в мережу. Маршрутизатор переміщує пакети, переглядаючи таблицю маршрутизації. Таблиця маршрутизації формується шляхом обміну інформацією про маршрути між мережевими пристроями. «Отруєння» таблиці маршрутизації означає небажану або шкідливе зміна в таблиці маршрутизації маршрутизатора. Це робиться шляхом редагування пакетів оновлення інформації маршрутизації, які поширюються пристроями. Ця атака може завдати серйозної шкоди в мережі, ввівши неправильні записи таблиці маршрутизації в таблицю маршрутизації.

Атаки Hit-and-Run - ця атака також називається тестової атакою, де зловмисник відправляє шкідливі пакети маршрутизатора і дивиться на результат, чи працює мережа коректно чи ні. Якщо мережа все ще працює,

зловмисник відправляє ще більше шкідливих пакетів, щоб вивести з ладу маршрутизатор. Ця атака може привести до того, що маршрутизатор буде виконувати незвичайні дії, які залежать від коду, введеного зловмисником. Цей тип атаки важко ідентифікувати і може завдати серйозної шкоди роботі маршрутизатору.

Стійкі атаки на маршрутизатор - на відміну від попереднього типу атаки, в цій атаці зловмисник неодноразово вводить шкідливі пакети в маршрутизатор, виявляючи уразливості маршрутизатора. Ця атака дуже сувора за своєю природою і може завдати великої шкоди. Маршрутизатор може перестати працювати від безперервної ін'єкції шкідливих пакетів. Цей тип атаки легше виявити в порівнянні з іншими атаками маршрутизатора.

Після інфікування загрозою роутер може: перенаправляти на веб-сторінки, які викрадають облікові дані; заманювати вас встановлювати шкідливі програми; проводити MITM-атаки; використовуватися для атак на інші пристрої; стати частиною ботнету для запуску DDoS-атак на веб-сайти або навіть на інфраструктуру Інтернету; бути інструментом для шпигування через Інтернет речей (IoT); використовуватися для прихованого майнінгу криптовалют [48].

Щоб запобігти перерахованим типам атак на маршрутизатори, мережевий адміністратор повинен реалізувати в мережі інший варіант безпеки. Моніторинг активності користувачів та використання шифрування там, де це можливо, необхідно. Брандмауер повинен бути встановлений для фільтрації вхідного і вихідного трафіку. Аналогічним чином, різне управління доступом має бути налагоджене для різних користувачів. Слід змінити настройки за замовчуванням журналу мережевого пристрою, необхідно регулярно робити резервні копії в мережі

4.2 Підготовка до налаштування маршрутизатора

По-перше, створіть резервну копію налаштувань вашого маршрутизатора на випадок, якщо буде потрібно відновити їх.

По-друге, здійсніть оновлення програмного забезпечення на своїх пристроях. Вкрай важливо встановити останні оновлення системи безпеки, щоб ваші пристрої максимально ефективно працювали разом. Спочатку

встановіть останні оновлення прошивки для вашого маршрутизатора. Потім поновіть програмне забезпечення на інших пристроях

По-третє, на кожному пристрої, яке ви раніше підключали до мережі, може знадобитися забути мережу, щоб пристрій використовувало нові настройки маршрутизатора при підключенні до мережі.

4.3 Безпечне налаштування маршрутизаторів

Налаштування безпеки визначають тип аутентифікації і шифрування, що використовуються вашим маршрутизатором, а також рівень захисту конфіденційності даних, що передаються по відповідній мережі. Яку б настройку ви не вибрали, завжди встановлюйте надійний пароль для підключення до мережі.

WPA3 Personal - це найбезпечніший на сьогоднішній день протокол, доступний для підключення пристроїв до мережі Wi-Fi. Він працює з усіма пристроями, що підтримують Wi-Fi 6 (802.11ax), а також деякими пристроями попередніх моделей. Найважливіша зміна в протоколі WPA3, це використання нового методу одночасної рівноправній аутентифікації SAE (Simultaneous Authentication of Equals), що надає додатковий захист від брутфорс-атак. SAE повинен замінити простий метод обміну загальними ключами PSK (Pre-Shared Key), який використовується в WPA2. Завдання SAE максимально захистити процес установки з'єднання від хакерських атак. SAE працює на підставі припущення про рівноправність пристроїв. Будь-яка зі сторін може відправити запит на з'єднання, і потім вони починають незалежно відправляти засвідчує їх інформацію, замість простого обміну повідомленнями по черзі, як у випадку з методом обміну ключами PSK. У SAE застосовується спеціальний варіант встановлення зв'язку (dragonfly handshake), який використовує криптографію для запобігання вгадування пароля зловмисником. Крім вищесказаного, SAE використовує метод прямої секретності (perfect forward secrecy, PFS) для додаткового посилення безпеки, якого не було в PSK. Припустимо, зловмисник отримує доступ до зашифрованих даних, які маршрутизатор відправляє і отримує з Інтернету. Раніше атакуючий міг зберегти ці дані, а потім, в разі успішного підбору пароля, розшифрувати їх. З використанням SAE при кожному новому з'єднанні встановлюється новий шифрує пароль, і якщо хакер в якийсь момент

проникне в мережу, він зможе вкрасти тільки пароль від даних, переданих після цього моменту [24].

WPA2 / WPA3 Transitional - це змішаний режим, при якому використовується WPA3 Personal з пристроями, що підтримують даний протокол, при цьому для пристроїв більш ранніх моделей доступний протокол WPA2 Personal (AES) [25].

WPA2 Personal (AES) підійде вам, якщо у вас немає можливості використовувати один з більш безпечних режимів. У цьому випадку також рекомендуємо вибрати AES в якості типу шифрування, якщо він доступний [26].

Виберіть значення *WPA3 Personal*, щоб забезпечити максимальний рівень безпеки.

Виберіть значення *WPA2 / WPA3* Transitional для сумісності зі старими пристроями

4.4 Уникнення слабких параметрів безпеки на маршрутизаторі

Не створюйте і не об'єднуйте мережі, що використовують старі або застарілі протоколи безпеки. Вони перестають бути захищеними, знижують надійність і пропускну здатність мережі і можуть призводити до відображення попереджень, пов'язаних з безпекою вашого пристрою :

1. Змішані режими WPA / WPA2. WPA / WPA2 - Personal (PSK) - це звичайний спосіб аутентифікації. Коли потрібно задати тільки пароль (ключ) і потім використовувати його для підключення до Wi-Fi мережі. Використовується один пароль для всіх пристроїв. Сам пароль зберігається на пристроях. Де його при необхідності можна подивитися, чи змінити. WPA / WPA2 - Enterprise - більш складний метод, який використовується в основному для захисту бездротових мереж в офісах і різних закладах. Дозволяє забезпечити більш високий рівень захисту. Використовується тільки в тому випадку, коли для авторизації пристроїв встановлений RADIUS-сервер (який видає паролі) [16];

2. WPA Personal. Даний режим підходить для більшості домашніх мереж. Коли на бездротовий маршрутизатор або на точку доступу встановлюється пароль, його потрібно вводити користувачами при підключенні до мережі Wi-Fi [17].

Рисунок 4.2 - WPA Personal

У режимі PSK бездротовий доступ не може управлятися індивідуально або централізовано. Один пароль поширюється на всіх користувачів, і він повинен бути вручну змінено на кожному бездротовий пристрій перебуває після того, як він вручну змінюється на бездротовому маршрутизаторі або на точці доступу. Даний пароль зберігається на бездротових пристроях. Таким чином, кожен користувач комп'ютера може підключитися до мережі, а також побачити пароль;

3.WEP, в тому числі WEP Open, WEP Shared, WEP Transitional Security Network або Dynamic WEP (WEP з підтримкою 802.1X). WEP (Wired Equivalent Privacy) - застарілий і небезпечний метод перевірки автентичності. Це перший і не дуже вдалий метод захисту. Зловмисники без проблем отримують доступ до бездротових мереж, які захищені за допомогою WEP. Не потрібно встановлювати цей режим в налаштуваннях свого роутера, хоч він там і присутній (не завжди) [16];

4. TKIP, включаючи будь-які значення параметрів безпеки, що містять слово TKIP. Існує два способи шифрування TKIP і AES. Рекомендується використовувати AES. Якщо у вас в мережі є старі пристрої, які не підтримують шифрування AES (а тільки TKIP) і будуть проблеми з їх підключенням до бездротової мережі, то встановіть "Авто". Тип шифрування TKIP не підтримуються в режимі 802.11n.) [16].

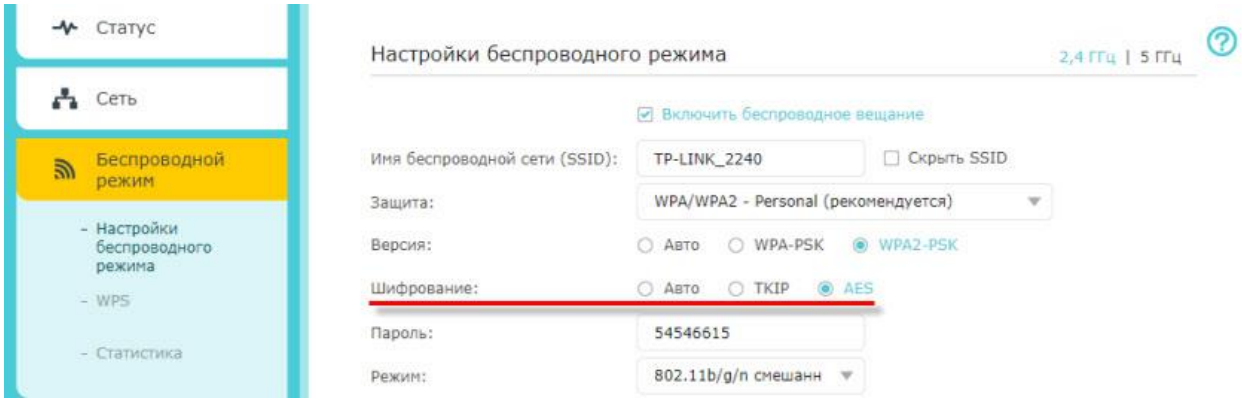


Рисунок 4.3 – Налаштування бездротового режиму

Крім того, не рекомендуємо використовувати параметри, що відключають функції захисту мережі, такі як «Без захисту», «Відкрита» або «Незахищена». Деактивація функцій захисту відключає аутентифікацію і шифрування і дозволяє будь-якого пристрою підключатися до вашої мережі, отримувати доступ до її загальних ресурсів (включаючи принтери, комп'ютери і інтелектуальні пристрої), використовувати ваше інтернет-з'єднання, стежити за тим, які веб-сайти ви відвідуєте, і контролювати інші дані, що передаються через вашу мережу або інтернет-з'єднання. Таке рішення пов'язане з ризиком, навіть якщо функції безпеки відключені тимчасово або для гостьової мережі.

4.5 Ім’я мережі

Ім'я мережі Wi-Fi або SSID (ідентифікатор набору послуг) - це ім'я, яке ваша мережа використовує для повідомлення про свою доступність інших пристроїв. Те ж ім'я знаходяться поблизу користувачі бачать в списку доступних мереж свого пристрою [18].

За рівнем безпеки ідентифікатор мережі SSID складно назвати безпечним. Навіть якщо він прихований в налаштування точки доступу і не транслюється в широкомовному форматі, то зловмисник все одно може не особливо вагаючись його «виловити» використовуючи спеціалізоване програмне забезпечення для аналізу переданого «по повітрю» трафіку [19].

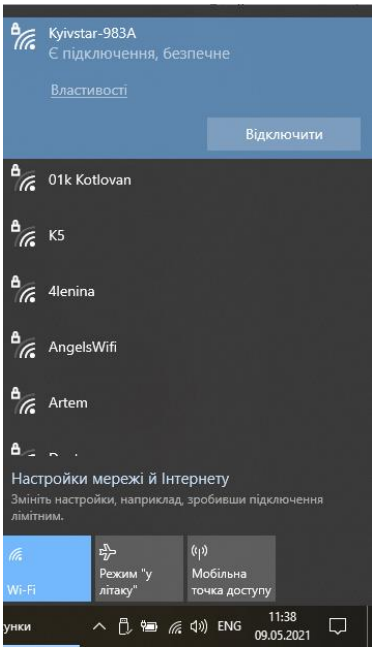


Рисунок 4.4 – Ім’я мережі

Використовуйте унікальне для вашої мережі ім'я і переконайтеся, що всі маршрутизатори в вашій мережі використовують одне і те ж ім'я для кожного підтримуваного ними діапазону. Наприклад, не рекомендується використовувати такі поширені імена або імена за замовчуванням, як linksys, netgear, dlink, wireless або 2wire, а також привласнювати різні імена діапазонів 2,4 ГГц і 5 ГГц.

Якщо ви не скористаєтеся цією рекомендацією, пристрої не зможуть належним чином підключитися до вашої мережі, всім маршрутизаторів у вашій мережі або всім доступним діапазонами ваших маршрутизаторів. Більш того, пристрої, які підключаються до вашої мережі, можуть виявити інші мережі з таким же ім'ям, а потім автоматично намагатися підключитися до них.

Рекомендація - задайте єдине, унікальне ім'я (з урахуванням регістру).

4.6 Прихована мережа

Маршрутизатор можна налаштувати так, щоб він приховував своє ім'я мережі (SSID). Параметр «Прихована мережа» задається в настройках роутера, щоб додатково убезпечити мережу від сторонніх підключень. Також це може бути зроблено, щоб не афішувати наявність бездротової мережі або

щоб не «захаращувати» список доступних мереж для користувачів. Ця практика, наприклад, широко поширена в торгових центрах. Зазвичай в таких місцях значно більше мереж, ніж бачать в своїх смартфонах користувачі. Там приховані мережі потрібні для роботи касового обладнання або внутрішнього користування співробітниками [20]. Ваш маршрутизатор може некоректно використовувати позначення «закрита» замість «прихована» і «транслюється» замість «не сховатися». Приховування імені мережі не запобігає її виявлення і не захищає її від несанкціонованого доступу. У зв'язку з особливостями алгоритму, який пристрою використовують для пошуку мереж Wi-Fi і підключення до них, використання прихованої мережі може призвести до розголошення ідентифікуючої інформації про вас і використовуваних вами прихованих мережах, таких як ваша домашня мережа. При підключенні до прихованої мережі на вашому пристрої може відображатися попередження про загрозу конфіденційності.

З метою забезпечення безпеки доступу до вашої мережі рекомендуємо використовувати відповідні налаштування безпеки.

4.7 Фільтрація MAC-адрес, аутентифікація, контроль доступу

MAC-фільтр - визначає список MAC-адрес пристроїв, які матимуть доступ до вашої мережі, або для яких доступ до мережі буде заборонений. MAC-фільтр поряд з шифруванням, аутентифікацією і ключем шифрування (паролем від Wi-Fi мережі) є додатковим заходом захисту бездротової мережі. Наприклад, якщо ви хочете обмежити доступ стороннім особам до вашої мережі, або дозволити доступ тільки своїм пристроям. Іноді його використовують в якості опції «батьківський контроль» і забороняють підключення до мережі пристроїв дитини [21].

MAC-адреси можна легко підробити в багатьох операційних системах, тому будь-який пристрій може прикидатися одним з тих дозволених унікальних MAC-адрес. MAC-адреси також легко отримати. Вони відправляються в ефір з кожним пакетом даних, що йде на пристрій і з пристрою, оскільки MAC-адресу використовується для забезпечення того, щоб кожен пакет потрапляв на потрібний пристрій. Щоб підключитися до вашого роутеру, зловмиснику docnfnymj простежити за трафіком Wi-Fi, перехопити пакет даних, вивчити пакет, щоб знайти MAC-адресу дозволеного

пристрою, змінити MAC-адресу свого пристрою на цей дозволений MAC-адресу і підключитися до нього. Часто користувачі думають, що це не можливо, ви думаєте, що це буде неможливо, тому що він вже увімкнений. Втім за допомогою атаки «deauth» або «deassoc», яка примусово відключає пристрій від мережі Wi-Fi, дозволить зловмисникові відновити з'єднання на своєму місці. Зловмисник з набором інструментів, наприклад, Kali Linux (в якому йде все з коробки), може використовувати Wireshark для підслуховування пакета даних, може перехопити даних, в яких буде вказано як раз ваш дозволений MAC-адресу, для підключення до мережі. Весь цей процес може зайняти менше 30 секунд. І це всього лише ручний метод, який включає в себе виконання кожного кроку вручну. Але є ще і автоматизовані інструменти, які можуть зробити це швидше. Фільтрація MAC-адрес, правильно використовувана, скоріше є функцією мережевого адміністрування, ніж функцією безпеки. Це не захистить вас від сторонніх, які намагаються активно зламати ваше шифрування і потрапити в вашу мережу. Проте, це дозволить вам вибрати, які пристрої дозволені в Інтернеті. [22].

Увімкніть цю функцію для настройки маршрутизатора таким чином, щоб він допускав підключення до мережі виключно пристроїв з певними MAC-адресами (управління доступом до середовища). Включення цієї функції не гарантує захисту мережі від несанкціонованого доступу з наступних причин. Вона не перешкоджає мережевим спостерігачам відстежувати чи перехоплювати трафік мережі. MAC-адреси можна легко скопіювати, підробити (імітувати) або змінити. Щоб захистити конфіденційність користувачів, деякі пристрої Apple використовують різні MAC-адреси для кожної мережі Wi-Fi. З метою забезпечення безпеки доступу до вашої мережі рекомендуємо використовувати відповідні налаштування безпеки [23].

Рекомендуємо задавати значення: «Відключено».

4.8 Автоматичне оновлення прошивки

Зазвичай автоматичне оновлення включається не відразу після випуску релізу. Це може статися через досить довгий термін і залежить від завантаження сервера і кількості оновлюються пристроїв. Зазвичай частота випуску автооновлення відбувається приблизно 6 раз на рік. Завдання автооновлення не в тому, щоб всі інтернет-центри швидко отримали нову

версію ПЗ, як тільки вона вийшла, а в тому, щоб пристрої не залишалися на старих версіях операційної системи, в яких є виправлення відомих і вирішених в нових версіях проблем [27]. Якщо можливо, налаштуйте маршрутизатор таким чином, щоб вироблялася автоматична установка оновлень програмного забезпечення та прошивки в міру їх появи. Оновлення прошивки можуть вплинути на доступні вам налаштування безпеки і забезпечують оптимізацію стабільності, продуктивності та безпеки вашого маршрутизатора.

Рекомендація - задайте значення: «Увімкнено».

4.9 Радіорежим

Ці параметри, доступні окремо для діапазонів 2,4 ГГц і 5 ГГц, визначають, які версії стандарту Wi-Fi маршрутизатор використовує для бездротового зв'язку. Новіші версії пропонують оптимізовану продуктивність і підтримують одночасне використання більшої кількості пристроїв. У більшості випадків оптимальним рішенням є включення всіх режимів, доступних для вашого маршрутизатора, а не якогось обмеженого набору таких режимів. У такому випадку всі пристрої, в тому числі пристрої більш пізніх моделей, зможуть підключатися до найбільш швидкісного підтримуваного ними радіо режиму. Це також допоможе скоротити перешкоди, створювані застарілими мережами і пристроями, що знаходяться поблизу [25].

Задайте значення: «Все» (рекомендується), або «Wi-Fi 2 - Wi-Fi 6» (802.11a / g / n / ac / ax).

4.10 Діапазони

Діапазон Wi-Fi подібний вулиці, по якій переміщаються дані. Чим більше діапазонів, тим більше обсяг переданих даних і продуктивність вашої мережі. Додайте всі діапазони, підтримувані вашим маршрутизатором.

4.11 Канал

Кожен діапазон вашого маршрутизатора розділений на кілька незалежних каналів зв'язку, подібних смугах руху на проїжджій частині. Коли встановлено автоматичний вибір каналу, ваш маршрутизатор вибирає

оптимальний канал Wi-Fi за вас. Якщо ваш маршрутизатор не підтримує автоматичний вибір каналу, виберіть той канал, який найкраще працює у вашій мережевому середовищі. Це залежить від перешкод Wi-Fi у вашому мережевому середовищі, в тому числі від перешкод, створюваних будь-якими іншими маршрутизаторами і пристроями, що використовують той же канал. Якщо у вас кілька маршрутизаторів, налаштуйте кожен так, щоб він використовував окремий канал, особливо якщо маршрутизатори розташовані близько один до одного.

Задайте значення: «Авто».

4.12 Ширина каналу

Задайте значення: «Авто» або «канали будь-якої ширини (20 МГц, 40 МГц, 80 МГц)» для діапазону 5 ГГц. Налаштування ширини каналу визначає ширину смуги пропускання, доступну для передачі даних. Ширші канали відрізняються більш високою швидкістю, проте вони більшою мірою схильні до перешкод і можуть заважати роботі інших пристроїв. 20 МГц для діапазону 2,4 ГГц допомагає уникнути проблем з продуктивністю і надійністю, особливо поблизу інших мереж Wi-Fi і пристроїв 2,4 ГГц, включаючи пристрої Bluetooth. Режими «Авто» або «Канали будь-якої ширини» для діапазону 5 ГГц забезпечують найкращу продуктивність і сумісність з усіма пристроями. Перешкоди, створювані бездротовими пристроями, не є актуальною проблемою в діапазоні 5 ГГц.

Задайте значення: «20 МГц» для діапазону 2,4 ГГц.

4.13 DHCP

DHCP (протокол динамічної конфігурації хоста) призначає IP-адреси пристроїв у вашій мережі. Кожен IP-адреса ідентифікує пристрій в мережі і дозволяє йому обмінюватися даними з іншими пристроями в мережі і через Інтернет. Мережевому пристрою потрібен IP-адреса, подібно до того як телефону потрібен номер телефону. У вашій мережі може бути тільки один DHCP-сервер. Якщо DHCP-сервер включений більш ніж на одному пристрої (наприклад, на кабельному модемі і маршрутизатор), конфлікти адрес можуть

перешкодити деяким пристроям підключатися до Інтернету або використовувати мережеві ресурси [33].

DHCP використовує протокол дейтаграм користувача. Це система зв'язку без встановлення з'єднання і тому вона не включає шифрування. Оскільки майже всі типи повідомлень в протоколі призначені для трансляції в кожен режим в мережі, snoopers можуть отримати великий контроль над мережевими операціями і створити руйнівний порушення, просто отримавши доступ до мережі і прослуховуючи широкомовні передачі DHCP. Ось чому DHCP рідко реалізується ізольовано. Існує ряд проблем з координацією, які необхідно враховувати при розподілі IP-адрес. На ці адреси також повинен посилатися DNS-сервер. Існує ймовірність того, що зловмисник може вставити віртуальний підроблений DNS або DHCP-сервер в мережу. Безпека мереж і правильність адрес виконуються диспетчером IP-адрес. Це ключовий елемент в наборі DDI [33].

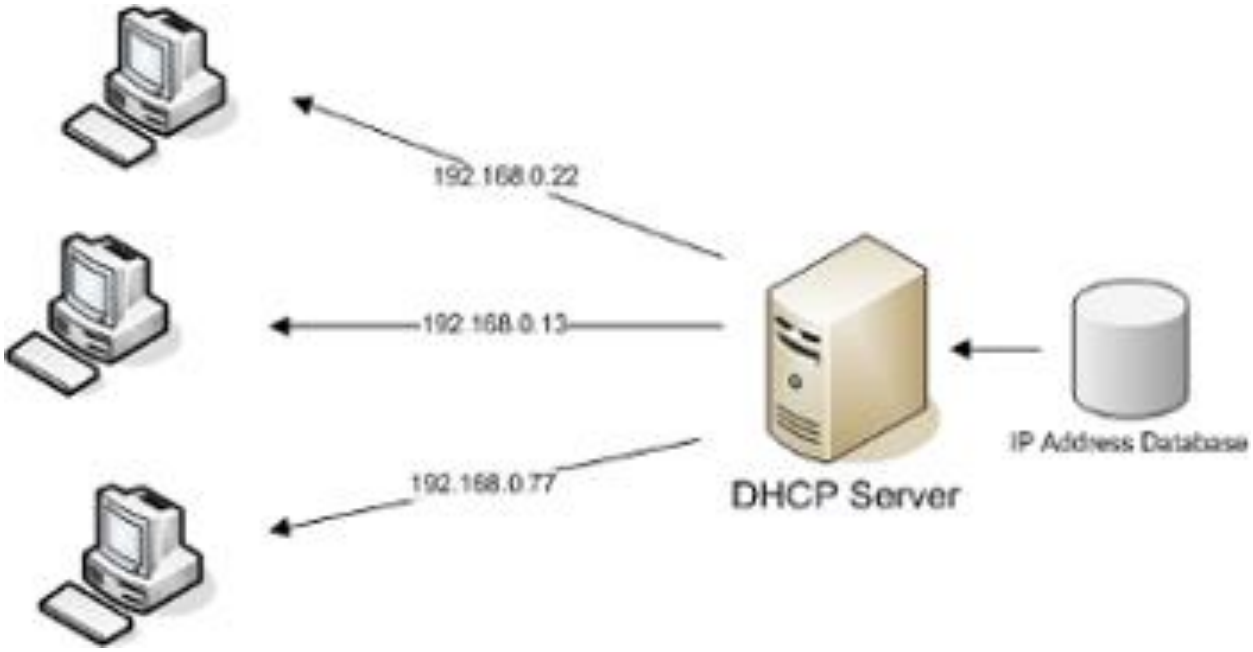


Рисунок 4.5 - Принцип дії DHCP

Задайте значення: «Увімкнено», якщо ваш маршрутизатор є єдиним DHCP-сервером в мережі.

4.14 Час оренди DHCP

Час оренди DHCP - це час, протягом якого IP-адреса, призначений пристрою, зарезервований для цього пристрою. Маршрутизатор Wi-Fi зазвичай мають обмежену кількість IP-адрес, які вони можуть призначати пристроям в мережі. Якщо це число вичерпано, маршрутизатор не може призначати IP-адреси нових пристроїв, і ці пристрої не можуть зв'язуватися з іншими пристроями в мережі і в Інтернеті. Скорочення часу оренди DHCP дозволяє маршрутизатора швидше відновлювати і перепризначувати старі IP-адреси, які більше не використовуються.

Задайте значення: «8 годин" для домашніх або офісних мереж; «1 + час» для точок доступу або гостьових мереж.

4.15 NAT

NAT (перетворення мережевих адрес) - це перетворення адрес в Інтернеті в адреси у вашій мережі. NAT можна порівняти з поштовим відділом компанії, який розподіляє відправлення на адресу співробітників, спрямовані на поштову адресу компанії, по кабінетах цих співробітників всередині будівлі. У більшості випадків NAT потрібно включити тільки на маршрутизаторі. Якщо функція NAT включена більш ніж на одному пристрої (наприклад, на кабельному модемі і маршрутизатор), «дублювання NAT» може привести до втрати пристроями доступу до певних ресурсів в локальній мережі або в Інтернеті.

При проектуванні мереж зазвичай застосовуються приватні IP-адреси 10.0.0.0/8, 172.16.0.0/12 і 192.168.0.0/16. Їх використовують всередині мережі майданчики або організації для підтримки локального взаємодії між пристроями, а не для маршрутизації у всесвітній мережі. Щоб пристрій з адресою IPv4 могло звернутися до інших пристроїв або ресурсів через інтернет, його приватну адресу повинен бути перетворений в публічний і загальнодоступний. Таке перетворення - це головне, що робить NAT, спеціальний механізм перетворення приватних адрес в загальнодоступні [29]. Підтримка NAT в поєднанні з приватними IPv4 адресами стала ефективним способом збереження загальнодоступних адрес IPv4.

Таблиця 4.1 – Переваги та недоліки NAT [30]

Переваги	Недоліки
1. NAT допомагає зберегти адресний простір IPv4, коли користувач використовує NAT перевантаження 2. NAT підвищує надійність та гнучкість взаємозв'язків із глобальною мережею шляхом розгортання декількох пулів джерел, пулу балансування навантажень та резервних пулів. 3. NAT має відомий метод мережевої адресації. Якщо є використання глобальної IP-адреси, то адресний простір повинен бути належним чином призначений. Тому що при розбудові мережі може знадобитися багато IP-адрес 4. NAT надає додатковий рівень безпеки в мережі, тому що хост, вбудований в мережу NAT, недоступний для інших мережевих пристроїв відповідно до уподобань користувача.	1. Коли запрошення гостя на віддалений доступ, він повторно перевірить, чи належать з'єднання від маршрутизатора до NAT. Але деякі гості встановили з'єднання з іншим хостом, якщо конкретний користувач не відповість на правильний хост, то він отримає запит, інший хост. Цей критерій призведе до погіршення продуктивності мережі 2. Якщо існує декілька додатків і протоколів, на які покладаються цілі функції, то мережа користувача не може бути доступною для інших користувачів. Оскільки хост вбудований всередині мережі NAT, яка недоступна, як обговорювалося вище 3. Якщо є необхідність усунення неполадок у мережі з віддалених районів, то усунення несправностей буде важким і призводить до втрати відстеження від кінця до кінця. 4. Застосування протоколів тунелювання створює більше ускладнень через значення перекладених NAT у заголовках IP, а також перериває перевірку цілісності, зроблені IPsec та лівими протоколами тунелювання. 5. Послуги, для яких потрібні з'єднання з встановленням UDP або TCP з глобальної сторони, можуть бути порушені та, можливо, часом недоступні.

Рисунок 4.6 – Принцип дії NAT

Механізм дає можливість численним пристроїв, кожне з яких має власний приватний адресу, використовувати єдиний загальнодоступний адреса IPv4. Додатковим плюсом NAT є підвищення рівня безпеки та конфіденційності мережі, за рахунок того, що він приховує приватні адреси IPv4. Маршрутизатор NAT можна налаштувати з одним або декількома загальнодоступними IPv4-адресами, які називають пулом NAT. При відправці трафіку пристроєм з внутрішньої мережі в зовнішню мережу, маршрутизатор перетворює його внутрішній IPv4-адрес в один з адрес, що входять до складу пулу.

В результаті дії такого механізму весь, що виходить із мережі трафік зовнішні пристрої «бачать» з загальнодоступним адресою IPv4, який можна назвати NAT IP адресою. Дія маршрутизатора NAT здійснюється на кордоні тупикової мережі, що отримала назву Stub-мережі. Вона пов'язана з сусідньою мережею одним з'єднанням, має один вхід і один вихід. При встановленні зв'язку між пристроями всередині і зовні Stub-мережі пакет відправляється прикордонному маршрутизатора, який виконує процес NAT. В результаті цього процесу внутрішній приватний адресу пристрою перетвориться в публічний зовнішній адресу, піддається маршрутизації [28].

Задайте значення: «Увімкнено», якщо ваш маршрутизатор є єдиним пристроєм, що реалізує функцію NAT в мережі.

4.16 WMM

WMM (Wi-Fi multimedia) визначає пріоритет мережевого трафіку для підвищення продуктивності різних мережевих додатків, таких як відео і голосовий зв'язок. На всіх маршрутизаторах, що підтримують Wi-Fi 4 (802.11n) або більш пізньої версії, функція WMM повинна бути включена за замовчуванням. Відключення WMM може вплинути на продуктивність і надійність пристроїв в мережі.

Таблиця 4.2 - Переваги та недоліки WMM [31]

Переваги	Недоліки
1. Все сучасне мережеве обладнання працює за стандартом WMM. 2. Ефективно працює для медіа (IPTV) і голосового (VoIP) трафіку. 3. За її рахунок акумулятори мобільних пристроїв економлять до 30% заряду.	1. Пріоритет ставить на голос і відео, і вибрати тільки між ними не можна. 2. Старі пристрої не працюють з даним стандартом.

Задайте значення: «Увімкнено».

ВИСНОВКИ

У ході виконання магістерської атестаційної роботи автором був:

- Проведений аналіз найпопулярніших атак на локальні мережі, з’ясовано що зловмисники найчастіше використовують шпигунське програмне забезпечення для здійснення віддаленого доступу та майнінгу криптовалют;
- Розроблені модель інформаційних загроз локальній мережі
- Розглянуті стандартні заходи безпеки локальної мережі: організаційні, технічні, апаратно-програмні;
- Докладно розглянута СКУД до ЛІКМ: з’ясовано призначення її складових, описані карти-ідентифікатори користувачів, розглянуті види контролерів СКУД і їх призначення, побудовано структурно-логічну схему автономної і мережевої СКУД, описані рівні взаємодії останньої та визначені вимоги до програмного забезпечення;
- При розгляді технічних засобів захисту локальної мережі були описані вітчизняні віброакустичні генератори зашумлення та проведений їхній порівняльний аналіз;
- Досліджені методи і технології захисту ЛІКМ на фізичному та канальному рівнях;
- Досліджені безпекові питання мереж зберігання даних;
- Розроблений алгоритм безпечного підключення локальної мережі підприємство;
- Досліджені методи безпечного налаштування для маршрутизаторів і точок доступу Wi-Fi локальної мережі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Локальні мережі та IT- інфраструктура [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://infotel.ua/ua/local-aria-network-data-transfering/.
2. Локальні комп'ютерні мережі [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://stud.com.ua/53333/informatika/lokalni_kompyuterni_merezhi.
3. Типи локальних мереж і їх характеристики [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://ukr.kagutech.com/4130394-types-of-local-networks-and-their-characteristics.
4. Топ угроз ИБ в корпоративных сетях, 2021 [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/top-ugroz-ib-v-korporativnyh-setyah-2021/.
5. CVE-2019-11769 Подробности [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://nvd.nist.gov/vuln/detail/CVE-2019-11769.
6. Система контролю доступу [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.elvis.com.ua/ua/access-ua.html.
7. Контроль доступу [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://expert112.com.ua/kontrol-dostupa/index_ua.html.
8. Загальний огляд систем віброакустичного зашумлення [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://tzi.com.ua/zagalnij-oglyad-sistem-vbroakustichnogo-zashumlennya.html.
9. Сеть хранения данных (SAN — Storage Area Network) [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.itc.by/storage-area-network/
10. Безопасность в сетях хранения данных [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: http://www.ishodniki.ru/art/net/storing/1026.html.
11. Запечников С.В. Основы построения виртуальных частных сетей / С.В. Запечников, Н.Г. , Милославская, А.И. Толстой. – М: Горячая Линия - Телеком, 2011. – 248 с.

12. Семенов Ю.А. Алгоритмы телекоммуникационных сетей. В 3 частях. Часть 3. Процедуры, диагностика, безопасность / Ю.А. Семенов - М.: БИНОМ. Лаборатория знаний, 2007. – 512 с.
13. Лэммл Т. Настройка коммутаторов. Учебное руководство / Т. Лэммл, К. Хейлзю – М.: Лори, 2015. – 464 с.
14. Наполова Е. И. Защита компьютерных сетей на основе технологии VIRTUAL PRIVATE NETWORK. / Е. И. Наполова, С. В. Кожевников. // Экономика и качество систем связи. – 2018. – №2. – С. 80–85.
15. Организация надежных каналов связи [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://rascom.ru/information/blog/organizaciya-nadezhnykh-kanalov-svyazi/.
16. Тип безопасности и шифрования беспроводной сети. Какой выбрать? [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://help-wifi.com/nastrojka-zashhity-wi-fi-setej/tip-bezopasnosti-i-shifrovaniya-besprovodnoj-seti-kakoj-vybrat/.
17. В чем разница между режимами WPA-Personal и WPA-Enterprise [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://www.tp-link.com/ru-ua/support/faq/500
18. SSID Wi-Fi сети на роутере. Что это и зачем он нужен? [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://help-wifi.com/poleznoe-i-interesnoe/ssid-wi-fi-seti-na-routere-chto-eto-i-zachem-on-nuzhen/.
19. Имя сети SSID в WiFi — что это такое и где его найти [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://set-os.ru/imya-seti-ssid-wifi/.
20. Находим и подключаемся к скрытой Wi-Fi сети [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://blog.maxnet.ua/2019/02/nakhodim-i-podklyuchayemsya-k-skrytoy-wi-fi-seti/.
21. Что такое MAC-фильтр, для чего он нужен и как его настроить? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.dlink.ru/ru/faq/110/1631.html.

22. Почему нельзя использовать фильтрацию MAC-адресов на своем Wi-Fi роутере [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://svyat.tech/%D0%9F%D0%BE%D1%87%D0%B5%D0%BC%D1%83-%D0%BD%D0%B5%D0%BB%D1%8C%D0%B7%D1%8F-%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D1%8C-%D1%84%D0%B8%D0%BB%D1%8C%D1%82%D1%80%D0%B0%D1%86/.
23. Контроль доступу по MAC-адресах для бездротової мережі Wi-Fi [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://help.keenetic.com/hc/uk/articles/213969309-%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C-%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D1%83-%D0%BF%D0%BE-MAC-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D0%B0%D1%85-%D0%B4%D0%BB%D1%8F-%D0%B1%D0%B5%D0%B7%D0%B4%D1%80%D0%BE%D1%82%D0%BE%D0%B2%D0%BE%D1%97-%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96-Wi-Fi.
24. Keenetic Руководство пользователя Мои сети и Wi-Fi Новые механизмы защиты беспроводной сети WPA3 и OWE [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://help.keenetic.com/hc/ru/articles/360005697520-%D0%9D%D0%BE%D0%B2%D1%8B%D0%B5-%D0%BC%D0%B5%D1%85%D0%B0%D0%BD%D0%B8%D0%B7%D0%BC%D1%8B-%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B-%D0%B1%D0%B5%D1%81%D0%BF%D1%80%D0%BE%D0%B2%D0%BE%D0%B4%D0%BD%D0%BE%D0%B9-%D1%81%D0%B5%D1%82%D0%B8-WPA3-%D0%B8-OWE.
25. Рекомендуемые настройки для маршрутизаторов и точек доступа Wi-Fi [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://support.apple.com/ru-ru/HT202068.
26. Безопасность Wi-Fi: следует ли использовать WPA2-AES, WPA2-TKIP или оба? [Електронний ресурс]. – 2017. – Режим доступу до ресурсу:

https://greatech.ru/2017/10/15/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/.

27. Автоматическое обновление операционной системы [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://help.keenetic.com/hc/ru/articles/360000922779-%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5-%D0%BE%D0%B1%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9-%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B.
28. Технология преобразования сетевых адресов (NAT) [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.smart-soft.ru/blog/tehnologija_preobrazovanija_setevyh_adresov_nat/.
29. Kholodnitska M. Що таке NAT? Для чого використовую даний стандарт? [Електронний ресурс] / Mariia Kholodnitska. – 2020. – Режим доступу до ресурсу: https://hyperhost.ua/info/uk/shcho-take-nat-dlya-chogo-vikoristovuyu-daniy-standart.
30. Що таке NAT? [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://uk.photo-555.com/7513995-what-is-nat.
31. Что такое Wi-Fi WMM и как включить в настройках роутера и ПК? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://wifigid.ru/sovety-po-nastrojke-routerov/wi-fi-wmm.
32. Що означає режим WMM на роутері і як його активувати [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://teknikmark.com/27-what-does-wmm-mode-on-the-router-mean-and-how-to-activate-it.
33. DHCP [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://lanmarket.ua/entsiklopediya/telekommunikatsionnye-tekhnologii/dhcp.html

34. Линков В. Что такое PAT? Лабораторная работа в Packet Tracer [Електронний ресурс] / Валерий Линков. – 2018. – Режим доступу до ресурсу: https://habr.com/ru/post/351332/.
35. ACL: списки контроля доступа в Cisco IOS [Електронний ресурс]. – 2011. – Режим доступу до ресурсу: https://habr.com/ru/post/121806/.
36. Списки доступа (Access Lists) в Cisco IOS (cisco acl firewall) [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.opennet.ru/base/cisco/access_list_intro.txt.html.
37. Технологии используемые в IPSEC (ipsec vpn tunnel cisco) [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.opennet.ru/base/cisco/ipsec_tech.txt.html.
38. Cisco IPsec VPN setup for iPhone and iPad [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://support.apple.com/ru-ru/guide/deployment-reference-ios/ior03a622a9f/web.
39. Что такое VLAN: логика, технология и настройка. Реализация VLAN в устройствах CISCO [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://e-server.com.ua/sovety/chto-takoe-vlan-logika-tehnologija-i-nastrojka-realizacija-vlan-v-ustrojstvah-cisco.
40. Решение Cisco по контролю доступа в сеть для беспроводных LAN [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.cisco.com/web/RU/netsol/ns466/netbr0900aecd80355b2f.html.
41. Олещенко Л. М. Організація комп'ютерних мереж. Конспект лекцій / Л. М. Олещенко. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 225 с.
42. Что такое SSH [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://beget.com/ru/kb/how-to/ssh/chto-takoe-ssh#.
43. Что такое SSH? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://freehost.com.ua/faq/wiki/chto-takoe-ssh/.
44. Port Address Translation (PAT) configuration [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://technoworldmittal.wordpress.com/2019/08/20/port-address-translation-pat-configuration/.
45. Николаев А. Сетевая безопасность: Рефлексивные списки доступа Reflexive ACL [Електронний ресурс] / Алексей Николаев. – 2018. –

Режим доступу до ресурсу: https://blog.learncisco.ru/setevaya-bezopasnost-refleksivnyie-spiski-dostupa-reflexive-acl/.

46. Как реализуется контроль сетевого доступа внутри компании Cisco? [Електронний ресурс] // 2016 – Режим доступу до ресурсу: https://habr.com/ru/company/cisco/blog/308472/.
47. Смирнов А. Маршрутизатор — определяем типы атак [Електронний ресурс] / Андрей Смирнов. – 2021. – Режим доступу до ресурсу: https://14bytes.ru/marshrutizator-opredelyaem-tipy-atak/.
48. Безпека домашньої мережі: як забезпечити захист роутера від атак [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://eset.ua/ua/news/view/655/bezopasnost-domashney-seti-kak-obespechit-zashchitu-routera-ot-atak.
49. Сараханьянц К. В вашем роутере боты водятся Домашние маршрутизаторы стали любимой целью хакеров [Електронний ресурс] / Кирилл Сараханьянц. – 2020. – Режим доступу до ресурсу: https://www.kommersant.ru/doc/4423665.
50. Як захистити свій Wi-Fi роутер від сусідів — 11 методів [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://e-server.com.ua/uk/poradi/jak-zahistiti-svij-wi-fi-router-vid-susidiv-11-metodiv.
51. Захит роутера від несанкціонованого втручання [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://www.teviant.com.ua/%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82-%D1%80%D0%BE%D1%83%D1%82%D0%B5%D1%80%D0%B0-%D0%B2%D1%96%D0%B4-%D0%BD%D0%B5%D1%81%D0%B0%D0%BD%D0%BA%D1%86%D1%96%D0%BE%D0%BD%D0%BE%D0%B2%D0%B0%D0%BD%D0%BE%D0%B3/.
52. Захист Wi-Fi мережі: 5 найважливіших порад [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.neologic.com.ua/info/articles/2020/zakhyst_wi_fi_merezhi_5_nayvazhlyvishykh_porad/.

53. 10 лайфхаків для Wi-Fi-роутера, про які ви не знали [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.lanet.ua/instructions/10-laifkhakiv-dlia-wi-fi-routera/.
54. Стецюк В. І. Методи контролю інформаційних потоків в телекомунікаційних системах / В. І. Стецюк, В. В. Мішан, О. В. Боженок. // Вісник Хмельницького національного університету. – 2018. – С. 209–216.
55. Технічні канали витоку інформації. Порядок створення технічних коплексів захисту інформації / С. О.Іваненко, О. В. Гавриленко, О. А. Липський, А. С. Шевцов. – Київ: ІССЗІ НТУ "КПІ", 2016. – 104 с
56. Юдін О. К. Аналіз та класифікація систем контролю та управління доступом на підприємстві / О. К. Юдін, О. М. Веселовська. // Науково-ємні технології. – 2018. – №2. – С. 220–225.
57. Волхонский В. В. Системы контроля и управления доступом / В. В. Волхонский. — СПб. : Университет ИТМО. — 2015.