Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: Засоби захисту сучасного комунікаційного обладнання

Виконавець: студент IV курсу, групи КБ-41

_____ **Юрій ЖЕЛІБА**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Юрій ЩЕБЛАНІН	

Нормоконтроль	Олена БОГУСЛАВСЬКА	

Київ 2023

Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-41** (група) **Желібі Юрію Володимировичу** (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Засоби захисту сучасного комунікаційного обладнання

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Літературні джерела, сучасні методи захисту комунікаційного обладнання.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з сучасним комунікаційним обладнанням, вразливостями з боку безпеки даних, оцінити методи захисту від найпоширеніших загроз, розробити власні рекомендації щодо захисту сучасного комунікаційного обладнання.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність полягає в розробці рекомендацій щодо підвищення рівня захищеності комплексу засобів захисту для комунікаційного обладнання.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Юрій ЖЕЛІБА (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 27.01.2023	*виконано*
2	Аналіз літератури	28.01.2023 – 11.02.2023	*виконано*
3	Обґрунтування вибору рішення	12.02.2023 – 24.03.2023	*виконано*
4	Дослідження сучасного комунікаційного обладнання	25.03.2023 – 07.04.2023	*виконано*
5	Аналіз української та міжнародної законодавчої бази	08.04.2023 – 20.04.2023	*виконано*
6	Дослідження вразливостей та загроз	21.04.2023 – 05.05.2023	*виконано*
7	Вироблення рекомендацій щодо захисту комунікаційного обладнання	06.05.2023 – 20.05.2023	*виконано*
8	Оформлення пояснювальної записки	21.05.2023 – 30.05.2023	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	31.05.2023 – 12.06.2023	*виконано*

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Юрій ЖЕЛІБА (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 57 сторінок основного тексту, 10 рисунків, 1 таблицю. Список використаних джерел містить 32 найменування і займає 4 сторінки.

Об'єктом дослідження є процес захисту сучасного комунікаційного обладнання.

Предметом дослідження є методи та засоби захисту сучасного комунікаційного обладнання.

Методи дослідження використанні при підготовці кваліфікаційної роботи:

- аналіз наукової літератури;
- аналіз міжнародних стандартів та нормативно-правової бази України;
- порівняння державної та міжнародної практики;
- порівняння та синтез.

В роботі проаналізовані технології та методи інформаційної безпеки сучасного комунікаційного обладнання; запропоновано рекомендації щодо комплексу засобів захисту сучасного комунікаційного обладнання.

Результати досліджень можуть застосовуватися в сфері інформаційної безпеки, які дають можливість розробникам і користувачам обрати ефективний, найбільш вдалий та дієвий спосіб захисту інформації, яка обробляється комунікаційним обладнанням.

Практична цінність отриманих результатів полягає в розробці рекомендацій щодо підвищення рівня захищеності комплексу засобів захисту для комунікаційного обладнання.

Напрямки подальших досліджень: розробка програмного модулю для підвищення рівня захищеності операційної системи комунікаційного обладнання.

Ключові слова: комунікаційне обладнання, мережа, зв’язок, комутатор, протокол, атака, засоби захисту, методи захисту, зловмисник, інформаційні системи, програмне забезпечення.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

NAT	–	Network Address Translation
IP	–	Internet Protocol
OSI	–	The Open Systems Interconnection model
ARP	–	Address Resolution Protocol
MAC	–	Media Access Control
STP	–	Spanning Tree Protocol
MITM	–	Man-in-the-middle attack
CAM	–	Content Addressable Memory
VLAN	–	Virtual Local Area Network
IPsec	–	Internet Protocol Security
IETF	–	Internet Engineering Task Force
AH	–	Authentication Header
ESP	–	Encapsulating Security Payload
DES	–	Data Encryption Standard
AES	–	Advanced Encryption Standard
SIEM	–	Security Information And Event Management
IEEE	–	Institute of Electrical and Electronics Engineers
EAP	–	Extensible Authentication Protocol
BPDU	–	Bridge Protocol Data Units
CSA	–	Cisco Security Agent
DAI	–	Dynamic ARP Inspection
SNMP	–	Simple Network Management Protocol
DHCP	–	Dynamic Host Configuration Protocol
DoS	–	Denial-of-Service
DNS	–	Domain Name System
WINS	–	Windows Internet Naming Service
ACL	–	Access Control List
SNMP	–	Simple Network Management Protocol
КСЗІ	–	Комплексна система захисту інформації
ПЗ	–	Програмне забезпечення
КЗЗ	–	Комплекс засобів захисту

ЗМІСТ

ВСТУП

Актуальність дослідження методів захисту сучасного комунікаційного обладнання є надзвичайно важливою в контексті сучасного цифрового світу. Оскільки зростає кількість підключених до мережі пристроїв, обсяги інформації і рівень загроз безпеці, необхідно забезпечити належний рівень захисту для комунікаційного обладнання.

Одна з основних причин актуальності дослідження полягає у постійному зростанні кількості кібератак та загроз кібербезпеці. Зловмисники використовують різні методи і техніки для отримання незаконного доступу до комунікаційного обладнання з метою викрадення, руйнування або модифікації конфіденційної інформації. Відповідно, необхідно провести дослідження та розробити ефективні методи та засоби захисту для запобігання таким загрозам. Важливо мати надійні заходи безпеки, щоб захистити комунікаційне обладнання від несанкціонованого доступу, перехоплення та втручання. Ці заходи безпеки передбачають використання різноманітних інструментів та технік, таких як шифрування, аутентифікація, контроль доступу та виявлення та запобігання вторгнень.

Метою роботи є проаналізувати технології та методи інформаційної безпеки сучасного комунікаційного обладнання; запропонувати рекомендації щодо засобів комплексу засобів захисту сучасного комунікаційного обладнання.

Для досягнення даної мети необхідно вирішити такі завдання :

- проаналізувати основні поняття інформаційної безпеки комунікаційного обладнання;
- дослідити сучасні методи захисту комунікаційного обладнання;
- запропонувати власні висновки та рекомендації щодо комплексу засобів захисту сучасного комунікаційного обладнання.

Об’єктом дослідження є процес захисту сучасного комунікаційного обладнання.

Предметом дослідження є методи та засоби захисту сучасного комунікаційного обладнання.

Методи дослідження використанні при підготовці кваліфікаційної роботи:

- аналіз наукової літератури;
- аналіз міжнародних стандартів та нормативно-правової бази України;
- узагальнення державної та міжнародної практики;
- порівняння та синтез.

РОЗДІЛ 1
АНАЛІЗ ПОНЯТЬ ТА ПІДХОДІВ ДО ЗАХИСТУ КОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

1.1 Загальна характеристика сучасного комунікаційного обладнання

Комунікаційне обладнання – пристрої, що забезпечують функціонування комп'ютерних мереж.

Серед всіх пристроїв можна виділити:

• пристрої доступу до мережі, що призначені для під’єднання кінцевих пристроїв до локальної комп’ютерної мережі: комутатор (switch), концентратор (hub), точка доступу (access point);

• пристрої для з’єднання між собою локальних мереж: маршрутизатор (router);

• комунікаційні сервери і модеми для обслуговування глобальних мереж;

• пристрої безпеки (security appliance), найбільш відомим з яких є брандмауер (firewall).

У сучасних мережах передачі даних використовуються два основних типи середовищ: кабельні і бездротові. Бездротові канали особливо корисні там, де потрібна мобільність, наприклад, у громадських місцях, готелях, аеропортах або для підключення мобільних пристроїв, таких як смартфони чи планшети.

Кабельні середовища, такі як оптичні лінії зв'язку та мідні кабелі, використовуються для швидких магістралей та локальних мереж. Обидва типи середовищ використовуються залежно від конкретних потреб і умов мережі [1, с. 15].

Маршрутизатор - це електронний пристрій, який виконує функцію поєднання двох або більше мереж і керує процесом маршрутизації. На рисунку 1.1 зображено вигляд цього пристрою. Його головна задача полягає в прийнятті рішень щодо пересилання пакетів на мережевому рівні (рівень 3 моделі OSI) між різними сегментами мережі на основі інформації про топологію мережі та встановлених правилах [2, с. 5].

Рисунок 1.1 - Маршрутизатор Cisco C921-4P

Маршрутизатори виконують багато функцій, не обмежуючись простим пересиланням даних між інтерфейсами. Вони забезпечують захист локальної мережі від зовнішніх загроз, контролюють доступ користувачів до ресурсів Інтернету, виконують функції трансляції адреси, фільтрації трафіку та шифрування даних. Маршрутизатори працюють на мережному рівні моделі OSI та використовують таблицю маршрутизації для визначення шляху пересилання пакетів. Вони також можуть забезпечувати пріоритетний порядок обслуговування пакетів та сприяти зменшенню завантаження мережі.

Маршрутизатори використовуються для об'єднання різних типів мереж і забезпечення доступу до Інтернету. Вони можуть бути як спеціалізованим апаратним обладнанням, так і звичайним комп'ютером, який виконує функції маршрутизатора. За допомогою програмного забезпечення, такого як пакети на основі ядра Linux, звичайний комп'ютер може бути перетворений на високопродуктивний і багатофункціональний маршрутизатор. Маршрутизаторні функції можуть також виконуватись робочими станціями або серверами з кількома мережними інтерфейсами та спеціальним програмним забезпеченням.

Отже, маршрутизатори виконують важливі завдання у мережному середовищі, забезпечуючи безпеку, ефективність та доступ до ресурсів. Вони можуть бути реалізовані як апаратне обладнання або програмне забезпечення, що дозволяє

широкий спектр застосувань для задоволення потреб у різних мережних сценаріях [2, с. 6].

Комутатор – це мережевий пристрій вигляд якого ми можемо побачити на рисунку 1.2, який з’єднує кілька комп’ютерів в одну єдину локальну мережу.

Сучасні комутатори пропонують широкий спектр функцій, які значно спрощують роботу адміністратора. Вибір правильного комутатора має велике значення для ефективної роботи локальної мережі та підприємства в цілому.

Рисунок 1.2 - Комутатор Cisco Catalyst 3650 24

Комутатори працюють на другому рівні моделі OSI, являючись мостами з багатьма портами. Вони передають дані тільки безпосередньо до призначеного отримувача, за винятком широкомовного трафіку, який розсилається до всіх вузлів мережі. У порівнянні з концентраторами, які пересилають трафік від одного підключеного пристрою до всіх інших, незалежно від типу трафіку, комутатори підвищують продуктивність і забезпечують безпеку мережі, оскільки вони дозволяють вузлам обробляти лише призначені для них дані.

Комутатор зберігає таблицю комутації в своїй пам'яті, яка вказує, які MAC-адреси знаходяться на яких портах комутатора. Початково, коли комутатор вмикається, таблиця комутації порожня, і комутатор працює в режимі навчання.

У режимі навчання, коли кадр надходить через будь-який порт комутатора, він пересилається на всі інші порти. Комутатор аналізує кадри і записує MAC-адресу відправника в таблицю комутації. Пізніше, якщо комутатор отримує кадр,

призначений для хоста, чий MAC-адрес вже є в таблиці, він пересилає цей кадр тільки через відповідний порт, вказаний в таблиці. Якщо MAC-адреса хоста-одержувача немає в таблиці комутації, то кадр буде розісланий на всі порти.

З часом, комутатор будує повну таблицю комутації для всіх своїх портів, і в результаті трафік локалізується. Це означає, що комутатор знає, до якого порту передавати кадри для конкретного MAC-адресу, що прискорює передачу даних і зменшує навантаження на мережу [3, с. 24].

Концентратор (hub) –це багато-портовий повторювач призначений для фізичного з'єднання декількох сегментів мережі вигляд якого ми можемо побачити на рисунку 1.3. Фізична структуризація мережі за допомогою концентраторів дозволяє змінити структуру мережі, її топологію, збільшити діаметр та число доданих до мережі комп'ютерів, зробити кращою надійність передавання даних [4].

Концентратор - це пристрій, який передає електронні сигнали одного порту на всі інші порти без визначення конкретного призначення повідомлення. Він просто ретранслює отримані сигнали для всіх підключених пристроїв. Концентратори належать до пристроїв першого рівня (фізичного рівня) в моделі OSI, оскільки їх головна функція полягає у регенерації сигналу та його повторному поширенні на всіх портах [5].

Рисунок 1.3 - Концентратор TP-LINK UH700

Концентратор це пристрій із загальною пропускною здатністю, оскільки всі вузли в ньому працюють на одній смузі одного каналу. Мережевий адаптер вузла приймає тільки повідомлення, адресовані на правильну MAC-адресу, вузли ігнорують

повідомлення, які адресовані не їм. Тільки вузол, якому адресовано дане повідомлення, обробляє його і відповідає відправнику [5].

1.2 Найбільш поширені загрози безпеці комунікаційного обладнання

Загрози безпеці інформації можуть бути ненавмисними або навмисними. Ненавмисні загрози виникають через помилки в програмному забезпеченні, відмову апаратного забезпечення, некоректні дії користувачів тощо. Навмисні загрози мають на меті завдати шкоди. Забезпечення безпеки є важливим для будь-якої організації, незалежно від її розмірів та форми діяльності. Тому необхідно забезпечити захист і контроль на всіх рівнях, включаючи фізичний та програмний.

Основні технічні загрози безпеці комунікаційного обладнання включають:

1. Помилки в програмному забезпеченні (ПЗ): Помилки в ПЗ можуть бути результатом роботи конкретних людей з їхніми особливостями та кваліфікацією. Більшість помилок не призводить до небезпечних ситуацій, але деякі можуть мати серйозні наслідки, такі як незаконне отримання прав доступу до сервера зловмисником або несанкціоноване використання ресурсів. Для усунення таких загроз необхідно регулярно оновлювати системи безпеки за допомогою випуску виробниками програмного забезпечення оновлень. Крім того, для забезпечення належної роботи систем безпеки важливо використовувати останні стабільні версії програмного забезпечення, випущені виробником.

2. Spanning Tree Protocol (STP) Attacks

Протокол STP використовується в мережах з комутацією LAN. Його основною функцією є усунення потенційних петель у мережі. Без STP локальні мережі другого рівня просто перестали б функціонувати, оскільки петлі, створені в мережі, переповнили б комутатори трафіком. Оптимізована робота та конфігурація STP гарантує, що локальна мережа залишається стабільною та що трафік проходить через мережу найбільш оптимізованим шляхом. Якщо зловмисник вставляє в мережу новий пристрій STP і намагається змінити роботу STP, ця атака потенційно може вплинути

на те, як трафік протікає через локальну мережу, значно вплинувши на зручність використання та безпеку трафіку, що проходить через мережу [6].

3. Address Resolution Protocol (ARP) Attacks

Протокол ARP використовується всіма мережевими пристроями, які підключаються до мережі Ethernet. Пристрої використовують ARP, щоб знайти MAC адресу для пристрою призначення, використовуючи лише відому IP-адресу цільового пристрою. ARP сам по собі є незахищеним, оскільки пристроям наказано довіряти отриманим відповідям.

Отже, якщо пристрій A запитує MAC-адресу пристрою B, а пристрій C відповідає замість пристрою B, пристрій A надсилатиме весь трафік, призначений для пристрою B, на пристрій C це називається атакою «людина посередині» (MITM).

4. Media Access Control (MAC) Spoofing

У атаці спуфінгу, один пристрій у мережі використовує MAC-адресу іншого пристрою з метою перенаправлення всього трафіку цільового пристрою на атакуючий пристрій. У контексті телефонної мережі, ця атака може бути порівняна з тим, коли хтось незаконно отримує доступ до вашого номера телефону і перенаправляє всі майбутні дзвінки на свій власний пристрій. Цей метод може бути використано для маскування одного пристрою під інший для декількох цілей, зокрема для того, щоб діяти як цей пристрій, або для виконання атаки типу « відмова в обслуговуванні» на цьому пристрої.

5. Переповнення таблиці Content Addressable Memory (CAM)

Таблиці CAM, які також називаються таблицями MAC-адрес , на комутаторах використовуються для відстеження, куди надсилати трафік для певних отриманих MAC-адрес. Щоб зрозуміти справжній ефект цієї атаки, вам потрібно зрозуміти основну роботу таблиці CAM і те, як вона оптимізує поведінку пересилання комутатора.

Коли перемикач увімкнено, він має порожню таблицю CAM. Він не знає, які пристрої підключені до яких інтерфейсів, і тому спочатку надсилає отриманий трафік на всі інтерфейси. Оскільки CAM-таблиця отримує трафік у кожному інтерфейсі,

вона створює записи для кожної MAC-адреси, яку вона бачить, пов’язуючи кожну адресу з її конкретним інтерфейсом.

Якщо комутатор має запис для певної MAC-адреси призначення в таблиці CAM, він не пересилає трафік на всі інтерфейси, замість цього він надсилає трафік для цієї адреси до свого спеціального навченого інтерфейсу. Після того, як MAC-адреси всіх підключених пристроїв будуть розпізнані, трафік майже не передаватиметься; трафік буде надіслано на вивчений інтерфейс кожного пункту призначення. Цей результат значно оптимізує поведінку комутатора при перенаправленні та збільшує пропускну здатність, доступну через комутатор (за умови, що комутатор зайнятий).

Кожен перемикач обмежує кількість MAC-адрес, які може містити таблиця адрес CAM. Якщо ліміт таблиці досягнуто, весь трафік з невідомих MAC-адрес буде залито. Атака переповнення таблиці CAM працює, коли один пристрій (або кілька пристроїв) підробляє велику кількість MAC-адрес і надсилає трафік через комутатор. Таблиця CAM комутатора буде заповнена, а весь інший трафік (зазвичай трафік від легальних пристроїв) буде переповнений, що призведе до того, що комутатор стане дуже зайнятим і потенційно перевантаженим. В результаті мережа швидко гальмує і з часом стає непридатною для використання [6].

6. Перемикання віртуальної локальної мережі

- Перехідна атака на комутатор. Під час цієї атаки зловмисник підробляє роботу комутатора в мережі з метою перехоплення, перенаправлення або маніпуляції мережевого трафіку. У разі успішної атаки трафік із кількох мереж VLAN може надсилатися до несанкціонованого комутатора та через нього, дозволяючи зловмисникові переглядати трафік і потенційно маніпулювати ним. Ця атака може бути виконана шляхом зламування аутентифікаційних механізмів комутатора, використання вразливостей в програмному забезпеченні комутатора або маніпуляції мережевими протоколами, такими як Spanning Tree Protocol (STP).

- Double tagging це тип атаки, який використовується для обходу захисних механізмів в мережах VLAN (Virtual Local Area Network). В цій атаці зловмисник створює підроблені маркери (теги) VLAN у мережевому трафіку, щоб обдурити

комутатор і отримати доступ до інших VLAN або отримати несанкціонований доступ до даних. На рисунку 1.4 розглянуто приклад атаки Double tagging.

Зловмисник, наприклад, розташований у VLAN 1, надсилає кадри, які мають подвійні теги, ніби використовується trank 802.1Q. Природно, зловмисник не підключений до транка; він використовує підробку комутатора , щоб перевести свій інтерфейс комутатора в транкінговий режим. Він використовує інкапсуляцію магістралі, щоб обдурити комутатор і змусити кадри перейти до іншої VLAN.

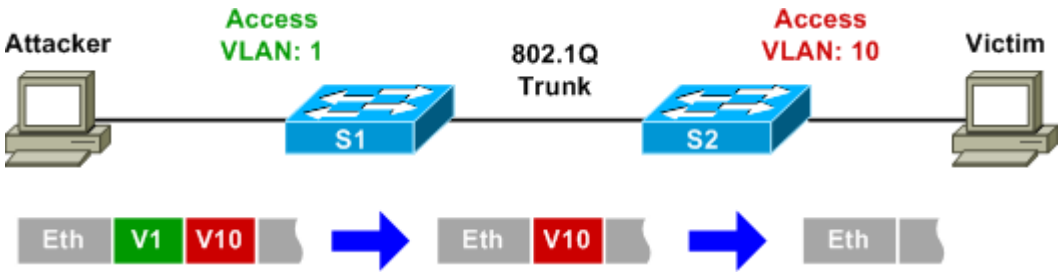


Рисунок 1.4 – Схема реалізації атаки типу Double tagging

Справжньому кадру, можливо, з деякими зловмисними даними, спочатку надається тег 802.1Q з ідентифікатором VLAN цільової VLAN, у цьому випадку VLAN 10. Потім додається другий фіктивний тег 802.1Q з ідентифікатором VLAN доступу зловмисника – VLAN 10 у нашому прикладі.

Коли локальний комутатор ліворуч отримує подвійний тегований кадр, він вирішує переслати його через інтерфейс магістралі. Це пояснюється тим, що перший тег «VLAN 10» має той самий ідентифікатор VLAN, що й власна VLAN транка. Тег «VLAN 10» видаляється, коли кадр надсилається по транку.

Комутатор надсилає всі кадри з рідної VLAN без тегів, це нормально. Тепер другий тег «VLAN 20» розміщено на магістралі. Коли перемикач з правого боку отримує кадр, він знаходить другий тег 802.1Q.

Підроблений тег для VLAN 20 знайдено, тег видаляється, а кадр пересилається до VLAN 20. У цей момент зловмисник успішно надіслав кадр із VLAN 10 і отримав кадр, вставлений у VLAN 20, не використовуючи маршрутизатор. Він зробив це через комутацію рівня 2 [7].

1.3 Аналіз стандартів безпеки комунікаційного обладнання

Оцінка засобів що гарантують інформаційну безпеку комунікаційного обладнання є на сьогоднішній день актуальною, що підтверджується аналізом вітчизняних та зарубіжних стандартів у цій галузі. Важливим елементом оцінки стану безпеки є тестування та підтвердження того, що засоби захисту відповідають стандартам даної галузі.

Стандарти встановлюють норми, вимоги, процедури та методики, які використовуються для захисту комунікаційного обладнання від різноманітних загроз і забезпечення надійності, конфіденційності та цілісності передачі інформації. Крім того, стандарти встановлюють процедури і методики, які допомагають в організації ефективного управління безпекою комунікаційного обладнання. Вони включають в себе рекомендації щодо розробки політик безпеки, процедур контролю доступу, аудиту безпеки та реагування на інциденти. Як основні стандарти в галузі формування вимог до засобів захисту комунікаційного обладнання, їх оцінки та тестування можна виділити такі документи:

1. IEEE 802.1X є протоколом автентифікації мережевого доступу, який забезпечує контроль доступу до комунікаційного обладнання в мережі. Цей стандарт описує процедури і повідомлення, які використовуються для взаємодії між комутатором і зазвичай кінцевим пристроєм для встановлення достовірності ідентифікації пристрою та контролю доступу до мережі.

За допомогою стандарту IEEE 802.1X можна встановити вимогу автентифікації до кожного пристрою, що підключається до комутатора. Це дозволяє забезпечити, щоб лише авторизовані користувачі або пристрої мали можливість комунікувати в мережі. Крім того, стандарт IEEE 802.1X підтримує різні методи автентифікації, такі як EAP (Extensible Authentication Protocol), що дозволяє використовувати різноманітні механізми автентифікації, такі як використання логіну та пароля, сертифікатів або біометричних даних.

2. IPsec (Internet Protocol Security) — це структура яку ми можемо побачити на рисунку 1.5, яка допомагає нам захистити IP-трафік на мережевому рівні. Інженерна

робоча група Інтернету (IETF) розробила протоколи IPsec у середині 1990-х років для забезпечення безпеки на рівні IP шляхом автентифікації та шифрування мережевих пакетів IP.

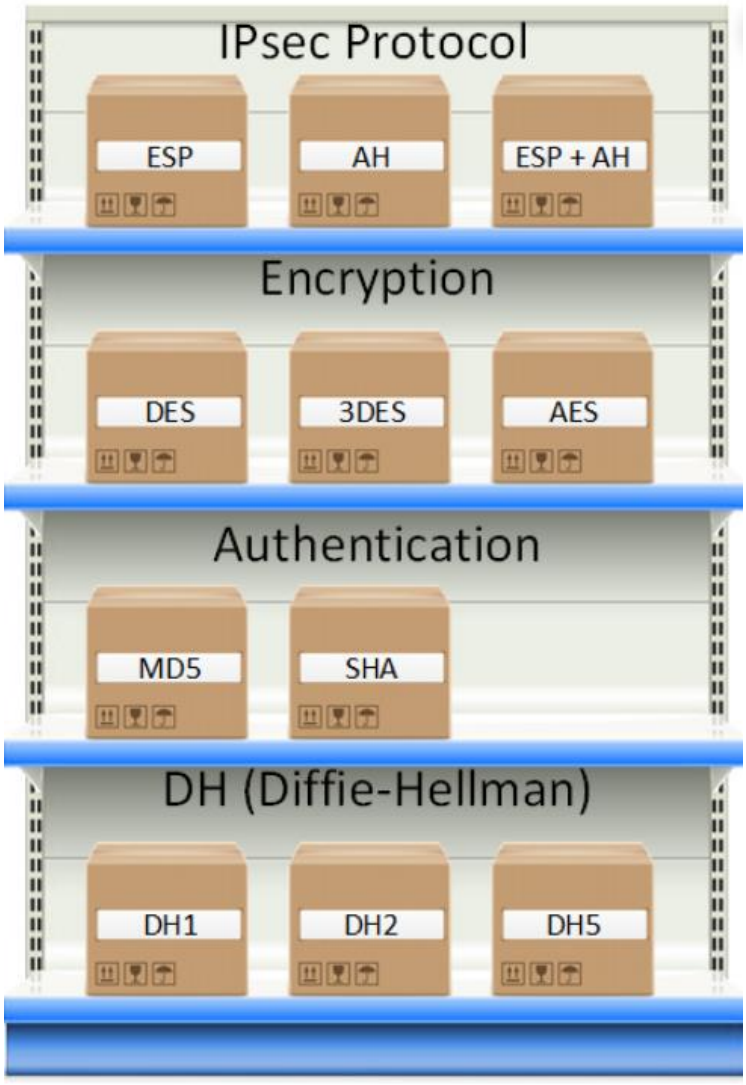


Рисунок 1.5 - структура різноманітних протоколів IPsec розбита по функціям які вони виконують

IPsec спочатку визначив два протоколи для захисту IP-пакетів: Authentication Header (AH) і Encapsulating Security Payload (ESP). Перший забезпечує цілісність даних і послуги захисту від повторів, а другий шифрує та перевіряє автентичність даних. IPsec може захистити наш трафік за допомогою таких функцій:

Конфіденційність : завдяки шифруванню наших даних ніхто, крім відправника та одержувача, не зможе прочитати наші дані.

Цілісність : обчисливши хеш-значення, відправник і одержувач зможуть перевірити, чи були внесені зміни в пакет.

Автентифікація : відправник і одержувач автентифікують один одного, щоб переконатися, що ми справді розмовляємо з пристроєм, який маємо намір.

Захист від повторного відтворення : навіть якщо пакет зашифровано та автентифіковано, зловмисник може спробувати перехопити ці пакети та надіслати їх знову. Використовуючи порядкові номери, IPsec не передаватиме жодних дублікатів пакетів.

3. IEEE 802.11: Стандарт IEEE 802.11 визначає технічні вимоги до бездротових локальних мереж (WLAN) і встановлює протоколи та процедури для передачі даних між бездротовими пристроями. Крім того, стандарт IEEE 802.11 визначає процедури автентифікації, які забезпечують перевірку ідентичності бездротових пристроїв перед дозволом їм підключатися до мережі. Цей стандарт також описує механізми керування мережею, такі як розділення каналів і керування потужністю передачі сигналу. Вони дозволяють забезпечити ефективну роботу бездротових мереж, зменшити вплив перешкод і забезпечити стабільну передачу даних між комунікаційним обладнанням.

4. NIST SP 800-57 Section 10 Key Management Specifications for Cryptographic Devices or Applications в даному розділі наведено вимоги і рекомендації для впровадження ефективної системи управління ключами в криптографічних пристроях або програмах.

5. ISO/IEC 27001: Цей стандарт визначає систему управління інформаційною безпекою, яка включає політики, процедури та технічні заходи для захисту комунікаційного обладнання та інших інформаційних ресурсів.

6. Посібник із тестування мережевої безпеки NIST 800-42

Цей стандарт дає практичні рекомендації щодо організації процесу тестування мережевої безпеки. Стандарт визначає ролі, стадії життєвого циклу, інструменти за допомогою яких необхідно виконувати тестування. Об'єктами мережевої безпеки, згідно з документом, є міжмережеві екрани, маршрутизатори та комутатори, сервери.

У документі розглядаються такі підходи щодо оцінки мережевої безпеки сканування мережі, сканування вразливості, злом пароля, аналіз лог-журналів, перевірка цілісності файлів, тестування на проникнення.

7. Закон України "Про захист інформації в інформаційно-комунікаційних системах" є основним законодавчим актом, що регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Згідно з цим законом, власник інформації визначає порядок доступу до неї. Для інформації, що є власністю держави або має обмежений доступ, а також для інформації, захист якої передбачено законом, перелік користувачів та їх повноваження регулюються законодавством. Захист інформації в системі покладається на власника цієї системи. Інформація, що є власністю держави або має обмежений доступ, а також інформація, захист якої передбачено законом, повинна оброблятися у системі з комплексною системою захисту інформації. Для цього необхідно мати підтвердження відповідності комплексних систем захисту інформації (КСЗІ), яке здійснюється через державну експертизу. Власник такої системи повинен створити службу захисту інформації або призначити відповідних осіб, які будуть забезпечувати захист інформації та контролювати цей процес. [12, с. 160].

Висновки до першого розділу

Отже, з проведеного нами дослідження в першому розділі, можемо зробити такий висновок, сучасне комунікаційне обладнання відіграє важливу роль в інформаційній інфраструктурі, забезпечуючи передачу даних та зв'язку. Велике різноманіття мережевого обладнання, та велика кількість такого роду пристроїв які використовуються на підприємствах вимагає особливої уваги до проблем безпеки.

Загрози безпеці комунікаційного обладнання є розмаїтими і постійно зростають. Серед них можна виділити атаки на рівні фізичної безпеки, зловживання привілеями, викрадення даних, впровадження шкідливого програмного забезпечення та інші. Ці загрози можуть призвести до втрати конфіденційної інформації, порушення цілісності даних і обмеження доступності мережі.

Аналіз стандартів безпеки комунікаційного обладнання виявив їх важливість і значення для забезпечення ефективного захисту. Стандарти встановлюють вимоги та

рекомендації щодо застосування відповідних заходів безпеки. Вони регулюють такі аспекти, як аутентифікація, шифрування, управління ключами, контроль доступу та інші аспекти безпеки. Ефективність і практичність стандартів безпеки комунікаційного обладнання залежить від їх відповідності сучасним технологіям і загрозам, а також від їх прийняття та використання відповідними організаціями. Вони забезпечують стандартизований підхід до захисту, полегшують інтеграцію різних пристроїв та систем і сприяють взаємній сумісності та взаємодії компаній виробників комунікаційних пристроїв.

Враховуючи постійний розвиток технологій і ускладнення рівня загроз, важливо постійно оновлювати стандарти безпеки комунікаційного обладнання та пристосовувати їх до нових викликів з боку зловмисників, відповідно впроваджуючи їх до систем безпеки конкретних секторів організацій.

РОЗДІЛ 2 ЗАСОБИ ЗАХИСТУ СУЧАСНОГО КОМУНІКАЦІЙНОГО ОБЛАДНАННЯ ВІД НАЙПОШИРЕНІШИХ АТАК

2.1 Засоби захисту комунікаційного обладнання

Комунікаційне обладнання є невід'ємною частиною сучасних мереж і відіграє важливу роль у передачі, обміні та обробці інформації. Однак, зростаючі загрози від кібератак та несанкціонованого доступу ставлять під загрозу безпеку цих комунікаційних засобів. Тому виникає необхідність у комплексних засобах захисту комунікаційного обладнання. Комплексний захист передбачає застосування широкого спектру заходів, методів і технологій, які спрямовані на запобігання вторгнень, виявлення та реагування на загрози, забезпечення конфіденційності, цілісності та доступності комунікаційного обладнання. Це охоплює використання фізичних, логічних, криптографічних і мережевих засобів захисту, а також впровадження політик безпеки та процедур управління, забезпечуючи надійну та безпечну роботу комунікаційного обладнання у сучасних мережах.

Засоби захисту інформації виконують важливі логічні та інтелектуальні функції, які можуть бути реалізовані як в складі програмного забезпечення автоматизованих інформаційних систем, так і в апаратних комплексах та системах контролю. Програмні засоби захисту є найпоширенішими і мають декілька переваг, таких як універсальність, гнучкість, простота реалізації, можливість змін та розвитку. Проте, саме через їх широке поширення, вони стають найбільш вразливими компонентами в системах захисту інформації підприємств.

Міжмережеві екрани (firewalls) відіграють найважливішу роль у захисті інформації при роботі в мережі Інтернет. Вони виконують контроль мережевого трафіку, який входить і виходить з мережі організації. Завдяки налаштуванням профілів доступу міжмережевого екрана, кожен користувач може мати власний профіль, який визначає не лише його права доступу до Інтернету, але й права доступу до нього з боку зовнішнього середовища. Міжмережевий екран може блокувати недозволений трафік і здійснювати перевірку передачі даних. Ефективно

налаштований міжмережевий екран здатний нейтралізувати більшість відомих комп'ютерних атак. Він забезпечує захист окремих протоколів та програмних продуктів, а також контролює доступ зовні до внутрішньої мережі і окремих сегментів на основі вмісту переданих даних між пристроями мережі. [13, с.38]. На рисунку 2.1 показано Cisco Secure Firewall 3100 середнього класу, який чудово підходить для невеликих організацій.

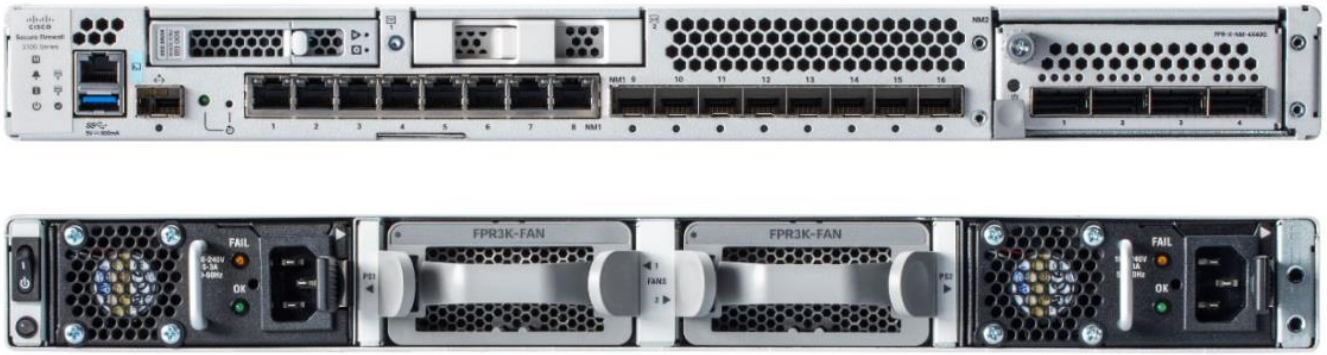


Рисунок 2.1– Cisco Secure Firewall 3100

Використання антивірусних засобів є невід'ємною та необхідною умовою при підключенні до Інтернету. Вони виконують важливу функцію у захисті інформації шляхом запобігання зараженню комп'ютерів шкідливими програмами. Антивірусні засоби виявляють, блокують та нейтралізують шкідливі програми, такі як віруси, троянські програми, шпигунське ПЗ та інші загрози безпеки. Їх використання дозволяє значно знизити ризик втрати інформації, запобігти несанкціонованому доступу до системи та зберегти приватні дані користувачів. Антивірусні засоби постійно оновлюються, щоб розпізнавати нові види загроз та забезпечувати надійний рівень захисту під час роботи в Інтернеті.

На комунікаційному обладнанні можуть використовуватись різні операційні системи, залежно від типу та функцій обладнання. Основні операційні системи, які застосовуються на комунікаційному обладнанні, включають:

1. Cisco IOS (Internetwork Operating System): Це операційна система, що використовується на маршрутизаторах та комутаторах Cisco. Вона надає широкі можливості управління мережею та реалізацію різних мережевих протоколів.

2. Junos OS: Ця операційна система розроблена компанією Juniper Networks і використовується на їх маршрутизаторах та комутаторах. Вона забезпечує високу масштабованість, надійність та широкі можливості управління мережею.

3. Huawei VRP (Versatile Routing Platform): Ця операційна система використовується на комунікаційному обладнанні компанії Huawei, такому як маршрутизатори та комутатори. Вона підтримує різні мережеві протоколи та має розширені функціональні можливості.

4. Arista EOS (Extensible Operating System): Ця операційна система використовується на комутаторах компанії Arista Networks. Вона пропонує високу швидкодію, масштабованість та розширюваність, а також підтримує різні мережеві протоколи.

5. MikroTik RouterOS: Ця операційна система використовується на маршрутизаторах та комутаторах компанії MikroTik. Вона надає широкий спектр функцій маршрутизації, комутації та безпеки.

У кожної операційної системи є власні агенти безпеки наприклад Cisco Security Agent (CSA) є потужною системою попередження на рівні хоста, призначеною для операційних систем Windows, Solaris та Linux. Її головна мета полягає в виявленні аномалій та небезпечних дій на комп'ютері шляхом моніторингу поведінки застосунків, виконуваного коду та мережевих з'єднань. Однією з великих переваг CSA є те, що вона не використовує сигнатури атак, що дозволяє їй ефективно виявляти нові загрози.

Після встановлення CSA на кінцеву систему, вона починає відстежувати та реєструвати події, що відбуваються в системі. За допомогою цих записів CSA перевіряє виконання попередньо заданих правил поведінки системи. Розташовуючись між ядром операційної системи та системними викликами, CSA здійснює контроль і спостереження за будь-якою активністю системи, запобігаючи відомим та невідомим атакам.

Juniper Networks Sky ATP (Advanced Threat Prevention) є рішенням з передовою захисту від загроз, розробленим компанією Juniper Networks. Цей продукт

використовує хмарні технології для виявлення та блокування шкідливих загроз у реальному часі.

Sky ATP працює на основі аналізу мережевого трафіку та інтелектуального сканування файлів з використанням різноманітних методів детектування загроз. Він виявляє нові та невідомі загрози, такі як віруси, шпигунське програмне забезпечення, троянські програми та інші види шкідливого програмного забезпечення.

Sky ATP може працювати як самостійний продукт або в поєднанні з мережевим обладнанням Juniper Networks, наприклад, мережевими файерволами серії SRX. Це забезпечує інтегрований підхід до захисту мережі, що поєднує периметральну безпеку з передовим виявленням загроз на рівні хмари.

Крім того, використання проксі-серверів та анонімних серверів може значно знизити ризики, пов'язані з використанням інтернету. Це дозволяє користувачам залишатися відносно анонімними під час взаємодії в мережі та зменшує ймовірність збирання та моніторингу мережевої інформації третіми особами. Використання проксі-серверів також може фільтрувати небажану та шкідливу інформацію, що надходить до системи, забезпечуючи більшу безпеку та контроль в мережі Інтернет.

Використання систем обмеження доступу співробітників до мережевих ресурсів Інтернету, використання маршрутизаторів та надійних постачальників мережевих послуг, а також короткочасних каналів зв'язку, допомагає знизити збір та моніторинг мережевої інформації на користь третіх осіб, а також обмежити потік небажаної та шкідливої інформації. Одним із методів захисту інформації в мережі є шифрування, яке ґрунтується на використанні криптографічних алгоритмів та ключів.

Для захисту інформації, що передається через незахищений канал, застосовуються IP-шифратори - пристрої криптографічного захисту інформації, які призначені для захисту IP-трафіку локальних мереж, терміналів і автоматизованих робочих місць. Також для захисту інформації використовуються різноманітні протоколи. Ці протоколи можна класифікувати в залежності від того, що саме вони захищають - з'єднання або програми. Наприклад, протоколи SSL і IPSec (IP Security) призначені для захисту комунікацій в Інтернеті, а протоколи S-HTTP і S/MIME спрямовані на забезпечення автентифікації та конфіденційності веб-додатків та

електронної пошти. Протокол SET (Secure Electronic Transaction) забезпечує захист трансакцій в електронній комерції. Застосування цих заходів допомагає забезпечити надійний захист інформації в мережі та зменшити ймовірність несанкціонованого доступу та втрати даних.

2.2 Сценарій проведення атаки STP та організація захисту від неї

Атаки Spanning Tree Protocol використовують вразливості в протоколі, щоб створити мережеві петлі або вивести мережу з ладу. Зловмисники можуть використовувати різноманітні методи, як-от надсилання зловмисних блоків даних протоколу Bridge (BPDU) , щоб втрутитися в обчислення STP і змусити мережу використовувати неоптимальний шлях або навіть створити петлю. Атаки STP можуть спричинити перевантаження мережі, широкомовні шторми та навіть призвести до збоїв в мережі, що може мати серйозні наслідки для організацій.

Короткий опис того як проходить STP атака:

1. Спочатку зловмисник отримує доступ до мережі.

2. По-друге, зловмисник надсилає шкідливі пакети Bridge Protocol Data Units (BPDU).

3. По-третє, пакети BPDU змінюють інформацію про топологію STP.

4. По-четверте, мережа змушена використовувати неоптимальний шлях або навіть створювати петлю.

5. Зрештою, мережа відчуває перевантаження, шторм трансляції або навіть збій. Атаки STP можуть мати серйозні наслідки для організацій, зокрема втрату даних і простої. Щоб запобігти атакам STP, мережеві адміністратори повинні вимкнути невикористовувані порти комутаторів, увімкнути безпеку портів і використовувати засоби захисту BPDU та кореневих засобів захисту[14].

Існує два основні механізми захисту від атак на процес STP: захист за допомогою Root Guard і захист рівня 2 за допомогою BPDU Guard.

Root Guard — це функція комутатора Cisco Catalyst, яка дозволяє адміністраторам визначати правильне розташування кореневого комутатора в мережі

рівня 2. Функція Root Guard налаштована на всіх інтерфейсах, які не є кореневими портами. Кореневий порт у реалізації протоколу Spanning-Tree – це будь-який порт на комутаторі, найближчий до кореневого мосту домену з комутацією Spanning-Tree. На рисунку 2.2 показано, як буде реалізовано функцію Root Guard, щоб запобігти тому, щоб некореневі порти стали кореневими комутаторами [15].

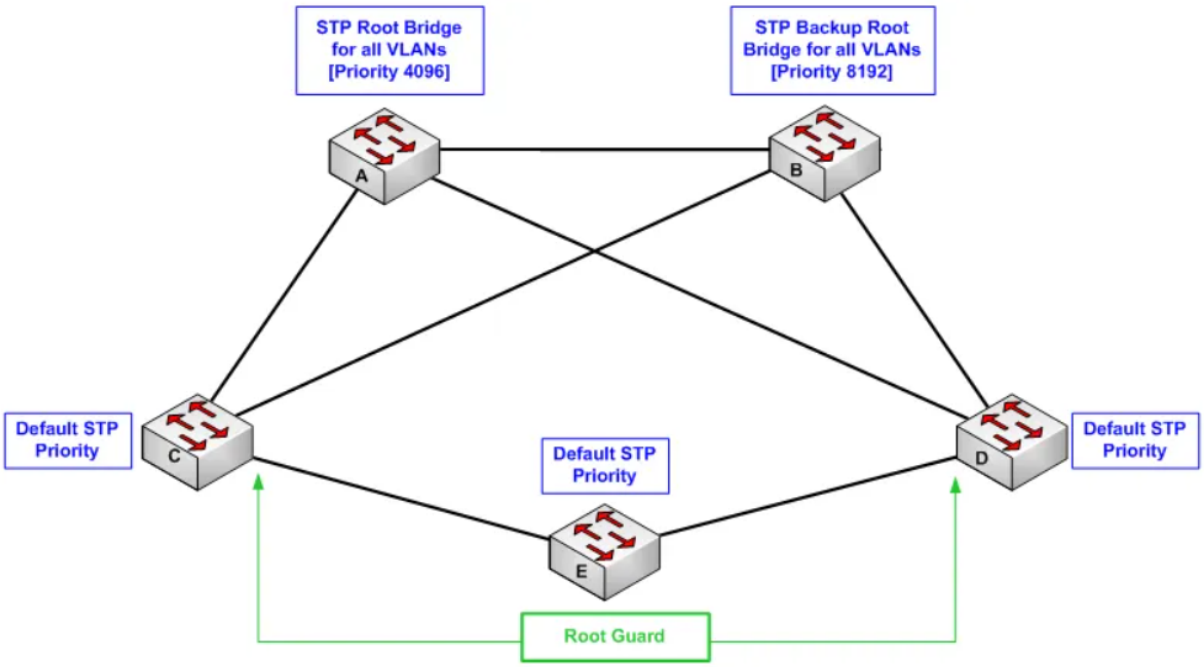


Рисунок 2.2 – реалізація функції Root Guard

На рисунку вище зображено мережу з комутацією рівня 2, яка складається з п’яти комутаторів: від комутатора A до комутатора E. Адміністратори мережі вирішили запровадити передбачувану мережу STP і налаштували комутатор A як кореневий міст STP, призначивши значення пріоритету 4096 для усіх налаштованих VLAN. Для резервування мережеві адміністратори налаштували комутатор B зі значенням пріоритету STP 8192. Всі комутатори C, D і E використовують значення пріоритету STP за замовчуванням 32, 768.

У цій топології немає причин, щоб комутатор E став кореневим мостом мережі STP. Таким чином, функцію Root Guard можна ввімкнути на інтерфейсах комутатора C і комутатора D, підключених до комутатора E. Це встановлює ці інтерфейси як призначені порти, і якщо будь-який пристрій через ці порти стає кореневим мостом, можливо, через неправильну конфігурацію, що призводить у вищих BPDU або через

STP-атаку інтерфейс буде переведено в кореневий несумісний стан. Поки порт знаходиться в цьому стані, весь трафік буде заблоковано комутатором. Крім того, порт залишатиметься в цьому стані, доки вихідні BPDU, отримані на цих портах, більше не будуть прийматися [16].

Функція BPDU Guard розроблена для збереження передбачуваності активної топології STP і підвищення надійності мережі за допомогою встановлення кордонів домену STP. Цю функцію можна ввімкнути глобально (тобто для всього комутатора) або на основі кожного інтерфейсу. Класичний процес конвергенції STP є повільним для сучасних мереж. Перш ніж порт перейде в стан пересилання, STP переводить порт у стан блокування на 20 секунд, стан прослуховування на 15 секунд, стан навчання на інші 15 секунд, а потім, нарешті, переводить порт у стан пересилання. Усе це тому, що протокол STP має бути впевнений, що цей порт не створюватиме петлю рівня 2, коли переходить у стан пересилання.

Логіка PortFast полягає в тому, що порт, який підключається до пристрою кінцевого користувача, не має потенціалу для створення петлі топології. З цієї причини порт може стати активним раніше, пропускаючи стани прослуховування та навчання STP. Оскільки ці порти PortFast підключено до пристроїв кінцевих користувачів, вони ніколи не повинні отримувати BPDU (BPDU надсилається лише комутаторами). Таким чином, якщо порт, увімкнений для BPDU Guard, отримує BPDU, порт вимикається, а порушення цієї політики повідомляється та припиняється.

Отримання BPDU на інтерфейсі, увімкненому для PortFast, вказує на недійсну конфігурацію або можливий стан безпеки, тобто підключення неавторизованого пристрою. Функція BPDU Guard переводить усі порти з увімкненим PortFast, які отримують BPDU, у стан вимкнення через помилку. Після того, як інтерфейс переведено в стан вимкнення через помилку, адміністратор має ввімкнути його вручну, забезпечуючи додатковий рівень безпеки, а також безпечну відповідь на недійсні конфігурації або можливі умови безпеки[17].

У таблиці 1 підсумовано функції BPDU Guard і Root Guard, а також типи атак STP наслідки яких вони допомагають зменшити:

Таблиця 1

Функції BPDU Guard і Root Guard

Тип атаки STP	Техніка зменшення впливу	Операція зменшення впливу
Зловмисник намагається підключити неавторизований мережевий пристрій, наприклад інший комутатор, до порту доступу, щоб отримати доступ до мережі з комутацією рівня 2	BPDU Guard, який увімкнено глобально або на основі кожного інтерфейсу для всіх інтерфейсів із увімкненим PortFast	BPDU Guard через помилку вимкне інтерфейс, налаштований для PortFast, який отримує BPDU
Зловмисник намагається маніпулювати кореневим мостом STP, щоб увесь трафік перенаправлявся на його чи її комутатор	Root Guard, який увімкнено на основі кожного інтерфейсу для всіх некореневих портів комутатора	Root Guard блокуватиме всі пересилання пакетів на інтерфейсі, який отримує вищий BPDU, для якого ввімкнено цю функцію

2.3 Сценарій проведення атаки ARP-spoofing та організація захисту

Підробка ARP відбувається в локальній мережі (LAN) за допомогою ARP. ARP — це протокол зв’язку, що з’єднує адресу динамічного Інтернет-протоколу (IP) із адресою фізичної машини. Остання називається адресою керування доступом до середовища (MAC). Протокол ARP керує зв'язком у локальній мережі.

Кожен мережевий пристрій має як IP-адресу, так і MAC-адресу. Щоб надсилати й отримувати повідомлення, хости в мережі повинні знати адреси інших хостів у цій мережі. При цьому хост підключатиме (зазвичай динамічну IP-адресу до фізичної MAC-адреси).

Наприклад, хост A в комп’ютерній мережі хоче з’єднати свою IP-адресу з MAC-адресою хоста B. Тому він надсилає ARP-запит усім іншим хостам у локальній мережі. Після цього запиту він отримує відповідь ARP від хоста B з його MAC-адресою. Хост, який запитує, зберігає цю адресу у своєму кеші ARP, який схожий на

список контактів. Цей кеш іноді називають таблицею ARP, оскільки адреси зберігаються у формі таблиці.

ARP-спуфінг означає, що зловмисник, який має доступ до локальної мережі, видає себе за хост В. Зловмисник надсилає повідомлення на хост А з метою змусити хост А зберегти адресу зловмисника як адресу хоста В. Хост А зрештою надсилатиме зловмисникові повідомлення, призначені для хосту Б. Після того, як зловмисник стане цим посередником, кожного разу, коли хост А спілкується з хостом В, цей хост фактично буде спілкуватися першим із зловмисником. Хост В зазвичай буде шлюзом за замовчуванням або маршрутизатором.

Щоб визначити, чи вас обманюють, перевірте свою програму автоматизації завдань і керування конфігурацією. Тут ви зможете знайти свій кеш ARP. Якщо є дві IP-адреси з однаковою MAC-адресою, ви можете стати жертвою атаки. Хакери зазвичай використовують програмне забезпечення для підробки, яке надсилає повідомлення про те, що його адреса є шлюзом за замовчуванням.

Однак також можливо, що це програмне забезпечення обманом змушує свою жертву замінити MAC-адресу шлюзу за замовчуванням своєю власною. У цьому випадку вам доведеться перевірити трафік ARP на наявність чогось незвичайного. Незвичайною формою трафіку є, як правило, небажані повідомлення, які стверджують, що володіють IP- або MAC-адресою маршрутизатора. Таким чином, небажані повідомлення можуть бути ознакою атаки ARP-спуфінгу [18].

Існує кілька підходів до запобігання атакам ARP Poisoning:

Статичні таблиці ARP

Можна статично зіставити всі MAC-адреси в мережі з їхніми належними IP-адресами. Це дуже ефективно для запобігання атакам ARP, але створює величезний адміністративний тягар. Будь-які зміни в мережі вимагатимуть ручного оновлення таблиць ARP на всіх хостах, що робить статичні таблиці ARP неможливими для більшості великих організацій. Тим не менш, у ситуаціях, коли безпека має вирішальне значення, виділення окремого сегмента мережі, де використовуються статичні таблиці ARP, може допомогти захистити критичну інформацію.

Перемикач безпеки

Більшість керованих комутаторів Ethernet мають функції, призначені для пом’якшення атак ARP. Ці функції, зазвичай відомі як динамічна перевірка ARP (DAI), оцінюють дійсність кожного повідомлення ARP і відкидають пакети, які здаються підозрілими або шкідливими. DAI також зазвичай можна налаштувати для обмеження швидкості, з якою повідомлення ARP можуть проходити через комутатор, ефективно запобігаючи DoS-атакам.

DAI і подібні функції колись були винятковими для мережевого обладнання високого класу, але тепер поширені майже на всіх комутаторах бізнес-класу, включно з тими, що є в невеликих компаніях. Зазвичай вважається найкращою практикою вмикати DAI на всіх портах, крім тих, які підключені до інших комутаторів. Ця функція не має значного впливу на продуктивність, але її, можливо, потрібно буде ввімкнути разом з іншими функціями, такими як DHCP Snooping.

Увімкнення захисту портів на комутаторі також може допомогти пом’якшити атаки кешу ARP. Port Security можна налаштувати так, щоб дозволити лише одну MAC-адресу на порту комутатора, позбавляючи зловмисника шансу зловмисно присвоїти кілька мережевих ідентифікаторів.

Фізична безпека

Належний контроль фізичного доступу до вашого офісу може допомогти пом’якшити атаки ARP. Повідомлення ARP не направляються за межі локальної мережі, тому потенційні зловмисники повинні перебувати у фізичній близькості від мережі жертви або вже мати контроль над машиною в мережі. Зауважте, що у випадку бездротових мереж близькість не обов’язково означає, що зловмиснику потрібен прямий фізичний доступ; Сигнал поширюється на вулицю або стоянку може бути достатнім. Незалежно від того, чи дротовий, чи бездротовий, використання технології, як-от 802.1x, може гарантувати, що лише надійні або керовані пристрої зможуть підключатися до мережі [19].

Ізоляція мережі

Як зазначалося раніше, повідомлення ARP не виходять за межі локальної підмережі. Це означає, що добре сегментована мережа може бути менш чутливою до отруєння кешу ARP загалом, оскільки атака в одній підмережі не може вплинути на

пристрої в іншій. Концентрація важливих ресурсів у виділеному сегменті мережі, де є підвищена безпека, може значно зменшити потенційний вплив атаки ARP Poisoning.

2.4 Сценарій проведення атаки MAC-spoofing та організація захисту

MAC спуфінг — це тип атаки, який використовується для використання недоліків у механізмі автентифікації, реалізованому апаратним забезпеченням дротової та бездротової мережі. З точки зору неспеціаліста, підробка MAC-адреси — це коли хтось або щось перехоплює, маніпулює або іншим чином змінює контрольні повідомлення, якими обмінюється мережевий пристрій, і його унікальну MAC-адресу . Це можна зробити різними способами, наприклад модифікацією апаратного забезпечення із вбудованим перемикачем для пересилання повідомлень з однієї MAC-адреси на іншу, підробки ідентифікаційної інформації цього пристрою шляхом пересилання повідомлень із пристрою невинного спостерігача («жертва підробки»), підробки повідомлень, надісланих із законних точок доступу, або перехоплення пакетів, які містять дані відповіді, якими остаточно маніпулюють до того, як вони досягнуть місця призначення.

Спуфінг MAC-адрес найбільш широко відома як метод атаки, який використовується під час злому бездротової мережі. Спуфінг MAC-адрес зазвичай використовується для проникнення в бездротові мережі та викрадення облікових даних бездротової мережі. Його також можна використовувати для встановлення неавторизованої точки доступу або імітації точки доступу за допомогою аналізатора пакетів у тій самій операційній системі, не перебуваючи в одному сегменті мережі [20].

На рисунку 2.3 показано 3 кроки реалізації атаки з спуфінгу MAC-адреси. Крок перший демонструє три виявлені пристрої (пристрої A, B і C) у таблиці CAM. Пристрій C є зловмисником. Після підробки MAC- адреси пристрою A (пам’ятайте, що початковий кадр, коли таблиця CAM порожня, надсилається на всі порти, крім порту джерела), пристрій C надсилає кадр із вихідною адресою MAC A з новою підробленою IP-адресою. На 2 кроці комутатор повторно запам’ятовує MAC-

адресу та змінює записи таблиці CAM. Тепер на кроці 3, коли пристрій B хоче зв'язатися з пристроєм A, комутатор надсилає пакет відповідно нової таблиці CAM, яка тепер є портом 3 або атакуючим ПК. Поки пристрій A не надішле пакети повторно, потік даних зберігатиметься, а зловмисник отримуватиме та переглядатиме актуальні дані. Забезпечивши відповіді на будь-які ARP-запити, зловмисник буде підтримувати з'єднання доки адміністратор мережі вручну не втрутиться та не виправить помилки.

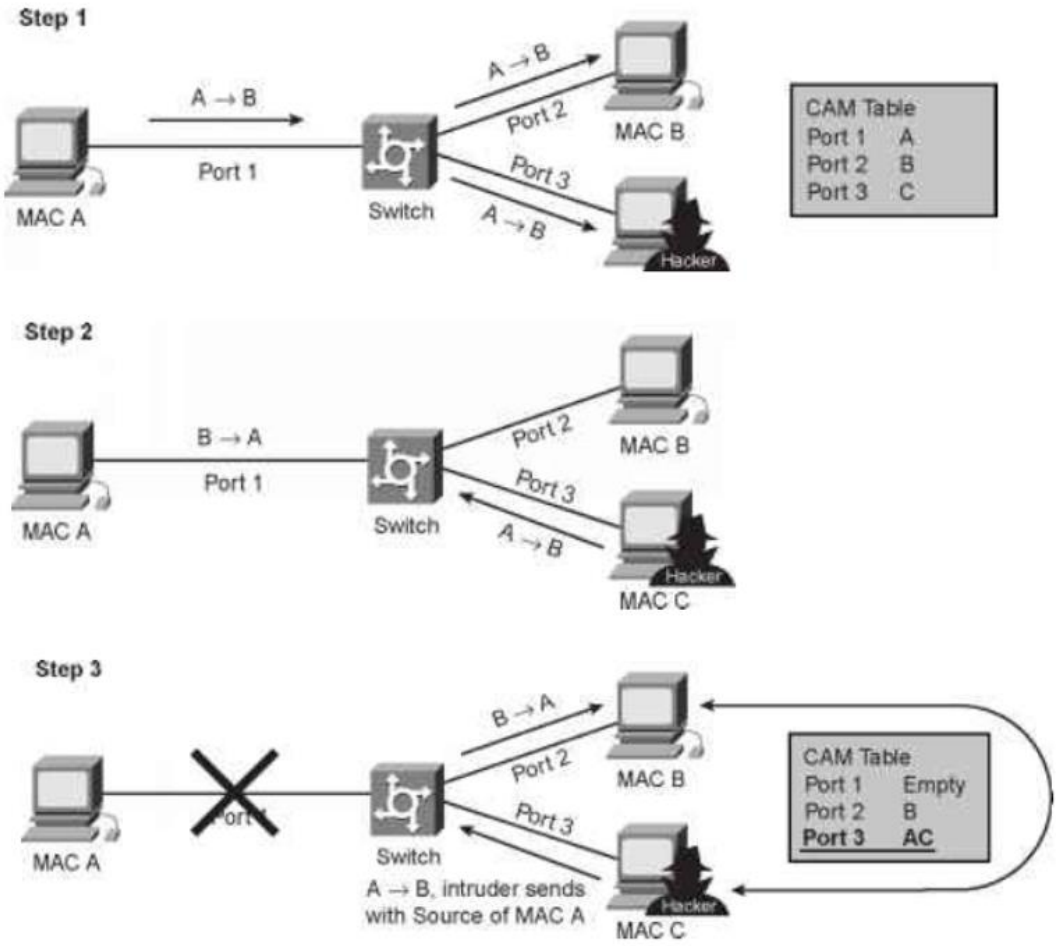


Рисунок 2.3 – Кроки реалізації атаки спуфінгу MAC-адреси

Простий метод, який використовують багато адміністраторів, щоб захиститись від такої атаки, полягає в тому, щоб вимкнути всі невикористовувані порти на комутаторі. Безпеку порту можна налаштувати так, щоб дозволити одну або кілька MAC-адрес. Якщо кількість MAC-адрес, дозволених на порту, обмежена однією, то лише пристрій із цією конкретною MAC-адресою може успішно підключитися до

порту. Якщо порт налаштовано як захищений і досягнуто максимальної кількості MAC-адрес, будь-які додаткові спроби підключитися за невідомими MAC-адресами призведуть до порушення безпеки.

Також у поєднанні з безпекою портів слід використовувати механізми відстеження DHCP, щоб переконатися, що у вашій мережі ввімкнено лише дійсні сервери DHCP. Один із механізмів відстеження DHCP полягає в тому, щоб дозволити лише довіреним повідомленням DHCP перетікати між клієнтським ПК і авторизованими серверами DHCP.

Коли клієнт надсилає широкомовне повідомлення для IP-адреси, ПК зловмисника також бачить запит, звичайно, оскільки широкомовні повідомлення надсилаються на всі інтерфейси чи порти, крім вихідного порту. Таким чином, по суті, мережа не повинна дозволяти надсилання пропозицій DHCP, підтверджень або негативних підтверджень із ненадійних джерел [21].

2.5 Сценарій проведення атаки переповнення CAM-таблиці комутатора та організація захисту

Усі моделі комутаторів використовують таблицю MAC-адрес для комутації рівня 2. Таблиця MAC-адрес у комутаторі містить MAC-адреси, пов’язані з кожним фізичним портом, і відповідну VLAN для кожного порту. Коли кадр надходить на порт комутатора, MAC-адреса джерела записується в таблицю MAC-адрес. Потім комутатор перевіряє отриману MAC-адресу призначення та дивиться в таблицю MAC-адрес, щоб побачити, чи містить вона MAC-адресу призначення. Якщо запис для MAC-адреси призначення вже існує, комутатор пересилає кадр на правильний порт. Якщо MAC-адреса призначення не існує в таблиці MAC-адрес, комутатор переливає кадри з усіх портів комутатора, окрім порту, через який було отримано кадр.

Поведінка MAC-адреси перемикача для невідомих адрес може бути використана для атаки на комутатор. Цей тип атаки називається атакою переповнення

таблиці MAC-адрес. Атаки переповнення таблиці MAC-адрес іноді називають атаками переповнення MAC-адрес і атаками переповнення таблиці CAM.

На рисунку 2.4 показано як зловмисник відправляє множинні ARP-запити з випадковими MAC-адресами. Реакція комутатора цілком очікувана: таблиця комутації миттєво заповнюється MAC-адресами, займаючи весь обсяг вільної пам'яті.

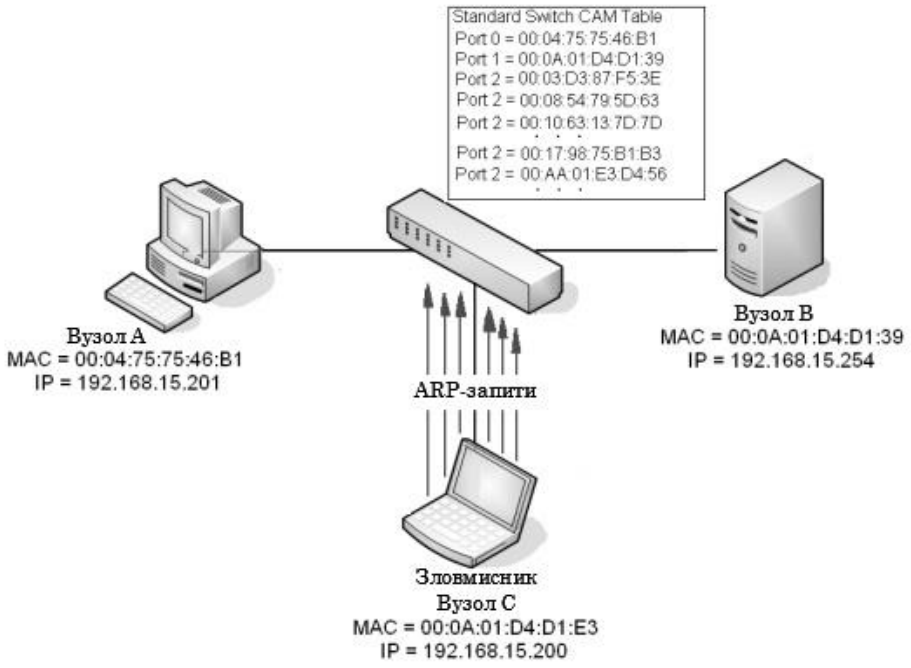


Рисунок 2.4 - – Схема організації атаки переповнення CAM-таблиці комутатора

З перших моментів атаки, комутатор починає показувати погану реакцію на спроби віддаленого управління. Індикація відбувається повільно, а відгук на команди займає надто багато часу. Проте, це не впливає на основну функцію комутатора і його пропускна здатність не страждає. Загроза спрямовується лише на систему управління, а не на основний функціонал пристрою. Крім того, через обмежений обсяг пам'яті комутатору, який не дозволяє зберегти всю кореспонденцію MAC-адрес, він переходить в режим хаба, що дозволяє зловмиснику переглядати дані. Таким чином, зловмисник отримує повний обсяг обміну трафіком між клієнтом з адресою 192.168.15.201 і сервером 192.168.15.254.

Слід зазначити, що існує два можливих сценарії розвитку ситуації, залежно від того, чи відбувався обмін трафіком між клієнтом і сервером до початку атаки.

У першому сценарії, де атака розпочинається до "спілкування" між сервером і клієнтом, комутатор не встигає записати їх MAC-адреси в таблицю комутації і під напливом флуду переходить в режим хаба перед тим, як клієнт надсилає запит на сервер. В результаті всі запити клієнта та відповіді сервера з'являються на всіх портах і стають доступними для зловмисника в повному обсязі.

У другому сценарії, атака починається після того, як MAC-адреси клієнта і сервера записані в таблицю комутації, що означає, що прослуховування стає неможливим. Проте, оскільки термін "життя" записів в таблиці комутації обмежений, коли цей термін закінчується, комутатор втрачає останні дані про "правильну" комутацію і не може їх отримати через переповнення пам'яті. Далі розвиток подій відбувається за першим сценарієм.

Щоб захиститися від такої атаки слід використовувати функцію безпеки порту, щоб обмежити вхід до інтерфейсу, обмеживши та ідентифікувавши MAC-адреси станцій, яким дозволено доступ до порту.

Існує три типи безпечних MAC-адрес:

Статичні безпечні MAC-адреси: вони налаштовуються вручну за допомогою команди налаштування інтерфейсу switchport port-security mac-address та зберігаються в таблиці адрес і додаються до запущеної конфігурації комутатора.

Динамічні захищені MAC-адреси: вони динамічно вивчаються, зберігаються лише в таблиці адрес і видаляються під час перезавантаження комутатора.

Закріплені безпечні MAC-адреси: їх можна динамічно вивчати або налаштовувати вручну, зберігати в таблиці адрес і додавати до поточної конфігурації. Якщо ці адреси збережено у файлі конфігурації, інтерфейсу не потрібно динамічно вивчати їх під час перезапуску комутатора.

Тоді, коли до таблиці адрес було додано максимальну кількість захищених MAC-адрес і станція, MAC-адреси якої немає в таблиці адрес, намагається отримати доступ до інтерфейсу, виникає порушення безпеки [22].

Комутатор може реагувати на порушення безпеки трьома різними способами:

• захист: коли кількість захищених MAC-адрес досягає обмеження, дозволеного для порту, пакети з невідомими адресами джерела відкидаються, доки ви не видалите достатню кількість захищених MAC-адрес або не збільшите кількість максимально допустимих адрес. Ви не отримуєте сповіщення про порушення безпеки.

• обмеження: коли кількість захищених MAC-адрес досягає обмеження, дозволеного на порту, пакети з невідомими адресами джерела відкидаються , доки ви не видалите достатню кількість захищених MAC-адрес або не збільшите кількість максимально допустимих адрес. У цьому режимі ви отримуєте сповіщення про порушення безпеки. Зокрема, надсилається перехоплення SNMP, реєструється повідомлення системного журналу, а лічильник порушень збільшується.

• вимкнення: у цьому режимі порушення безпеки порту призводить до негайного вимкнення інтерфейсу через помилку та вимикання індикатора порту. Він також надсилає пастку SNMP , реєструє повідомлення системного журналу та збільшує лічильник порушень. Коли захищений порт перебуває в стані вимкнення через помилку, ви можете вивести його з цього стану, ввівши команду глобальної конфігурації errdisable recovery cause psecure-violation, або ви можете повторно ввімкнути його вручну, ввівши конфігурацію інтерфейсу завершення роботи та відсутності вимкнення команди. Це режим за замовчуванням [22].

2.6 Сценарії проведення атак на DHCP-сервер та організація захисту

DHCP — це протокол, який автоматично призначає хосту дійсну IP-адресу з пулу DHCP. DHCP завжди був основним протоколом, який використовувався для призначення IP-адрес клієнтам. Проти комутованої мережі можна здійснити два типи атак DHCP: атаки DHCP starvation і DHCP spoofing. Під час атаки DHCP starvation зловмисник переповнює сервер DHCP запитами DHCP REQUEST, щоб використовувати всі доступні IP-адреси, які може видати сервер DHCP. Після видачі цих IP-адрес сервер не може видавати більше адрес, що призведе до виснаження пулу DHCP, і ця ситуація створює атаку відмови в обслуговуванні (DoS), оскільки нові

клієнти не можуть отримати доступ до мережі. DoS-атака — це будь-яка атака, яка використовується для перевантаження певних пристроїв і мережевих служб нелегітимним трафіком, таким чином перешкоджаючи законному трафіку досягти цих ресурсів.

Під час атак DHCP spoofing зловмисник налаштовує фальшивий сервер DHCP у мережі для видачі адрес DHCP клієнтам. Ціль цієї атаки змусити клієнтів використовувати помилкові сервери системи доменних імен (DNS) або Windows Internet Naming Service (WINS) і змусити клієнтів використовувати машину під контролем зловмисника як своїх шлюз за замовчуванням.

DHCP starvation часто використовується перед атакою DHCP-спуфінгу, щоб відмовити в обслуговуванні законного сервера DHCP, що полегшує введення підробленого сервера DHCP у мережу [23].

Для боротьби з такими атаками найкраще використовувати DHCP Snooping

DHCP Snooping — це технологія безпеки рівня 2, вбудована в операційну систему потужного мережевого комутатора, яка не пропускає трафік DHCP, що визнаний неприйнятним. DHCP Snooping запобігає неавторизованим (шахрайським) серверам DHCP, які пропонують IP-адреси клієнтам DHCP. Функція DHCP Snooping виконує такі дії:

- Перевіряє повідомлення DHCP з ненадійних джерел і фільтрує недійсні повідомлення.
- Створює та підтримує базу даних прив’язки DHCP Snooping, яка містить інформацію про ненадійні хости з орендованими IP-адресами.
- Використовує базу даних прив’язки DHCP Snooping для перевірки наступних запитів від ненадійних хостів.

В технології DHCP snooping використовується розрізнення між довірчими і недовірчими портами (довіреними і ненадійними відповідно). Довірчі порти вказуються вручну і дозволяють отримати відповіді DHCP, такі як DHCPOFFER. Недовірчі порти, натомість, не можу підтримувати відповіді DHCPOFFER.

Щоб вказати порти як довірчі, ця конфігурація створюється вручну. Усі порти, які не були визначені як довірчі, автоматично стають недовірчими. Зазвичай, порт,

який одночасно підключений до DHCP-сервера, встановлюється як довірчий порт (trust port), потім з нього очікується отримання відповіді DHCP.

Нижче кроки які ілюструють, як налаштувати DHCP snooping на комутаторі Catalyst 2960:

Крок 1. Увімкніть відстеження DHCP за допомогою команди режиму глобальної конфігурації ip dhcp snooping .

Крок 2. Увімкніть відстеження DHCP для певних VLAN за допомогою команди ip dhcp snooping vlan number .

Крок 3. Визначте порти як надійні на рівні інтерфейсу, визначивши надійні порти за допомогою команди ip dhcp snooping trust .

Додатково Обмежте швидкість, з якою зловмисник може постійно надсилати фальшивий DHCP

Крок 4. запити через ненадійні порти до сервера DHCP за допомогою команди ip dhcp snooping limit rate rate [23].

На рисунку 2.5 показано якщо комутатор отримує повідомлення DHCP від хоста, якого немає в його таблиці прив’язки, це повідомлення відхиляється, а хосту не надається доступ до мережі. Це запобігає від підробки повідомлень DHCP і отримання несанкціонованого доступу до мережі зловмисними хостами.

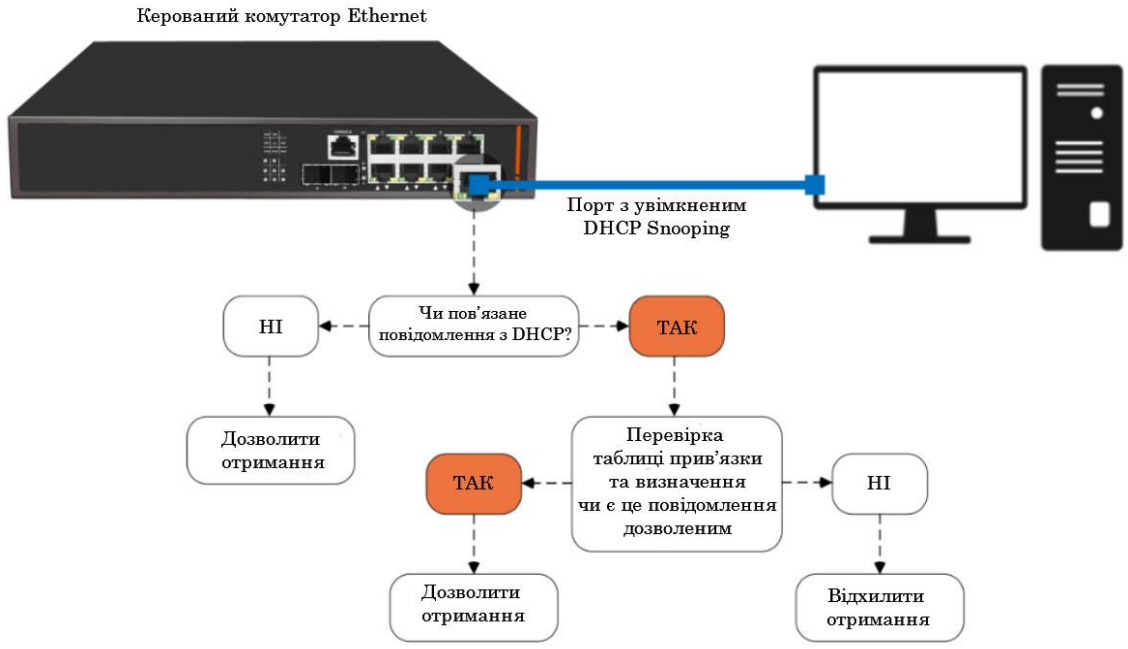


Рисунок 2.5 - Процес перевірки повідомлень DHCP

У таблиці прив'язки DHCP зберігаються (інформація зберігається тільки про ненадійні порти):

- MAC-адреса клієнта;
- орендована IP-адреса клієнта;
- час оренди в секундах;
- ідентифікатор VLAN;
- ідентифікатор порту до якого приєднаний клієнт.

Алгоритм роботи комутатора з встановленими функціями DHCP snooping і DAI наведено в Додатку А.

Висновки до другого розділу

У даному розділі було розглянуто сценарії проведення атак на комунікаційне обладнання, а також надано рекомендації щодо організації захисту від цих атак. Наслідками таких атак можуть бути порушення безпеки мережі, недоступність сервісів, витрати часу та ресурсів на відновлення роботи системи, а також втрата конфіденційності та цілісності даних.

Атака STP розкриває потенційну загрозу, пов'язану зі зміною топології мережі, що може призвести до відмови в обслуговуванні або отримання несанкціонованого доступу. Для організації захисту рекомендується використовувати Root Guard і захист рівня 2 за допомогою BPDU Guard.

Атака ARP-спуфінгу показує загрозу, пов'язану зі перехопленням мережевого трафіку. Для організації захисту рекомендується використовувати механізми захисту ARP, такі як статичні ARP-записи, DAI, а також використовувати шифрування трафіку.

Атака MAC-спуфінгу показує загрозу, коли зловмисник підробляє свою MAC-адресу для здійснення атаки. Для захисту від таких атак рекомендується використовувати функцію блокування портів MAC-адрес, аутентифікацію пристроїв, а також контроль доступу до комутатора.

Атака переповнення CAM-таблиці комутатора показує загрозу витоку інформації та перебоїв у роботі мережі. Для організації захисту рекомендується обмежувати доступ до комутатора, налаштовувати правила фільтрації MAC-адрес, а також використовувати протоколи безпеки, наприклад, 802.1X.

Атака на DHCP-сервер показує загрозу зміни налаштувань мережевих пристроїв та перехоплення трафіку. Для організації захисту рекомендується використовувати функцію DHCP snooping, а також використовувати механізми автентифікації та шифрування.

РОЗДІЛ 3
РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ КОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

3.1 Вибір методів захисту комунікаційного обладнання

Для забезпечення безпеки інформаційних ресурсів, які обробляються комунікаційним обладнанням, можна використовувати багаторівневий підхід до захисту. Ця потреба виникає з відсутності універсальних засобів захисту та необхідності комбінування декількох компонентів для забезпечення належного рівня безпеки мережі. Ефективний захист досягається шляхом використання компонентів, які працюють у взаємодії, ускладнюючи або навіть унеможливлюючи здійснення атак. Отже, для досягнення надійного захисту інформаційних ресурсів, що обробляються комунікаційним обладнанням, необхідно використовувати комплексний підхід, поєднуючи різні компоненти та механізми захисту, щоб створити непроникну систему, яка ускладнюватиме або навіть унеможливить зловмисний доступ до мережі та її ресурсів [24].

Для забезпечення безпеки комунікаційної мережі необхідно використовувати комплекс засобів захисту, який забезпечує виконання основних функціональних властивостей безпеки інформаційних ресурсів, відповідно до вимог Нормативних документів Системи технічного захисту інформації. Ці вимоги включають конфіденційність, цілісність і доступність інформації.

У Додатку Б наведена узагальнена структура можливих засобів і механізмів захисту комунікаційної мережі. Цей додаток надає огляд різних компонентів та можливих методів захисту, які можуть бути використані для забезпечення безпеки комунікаційної мережі.

На основі результатів дослідження найпопулярніших атак на комунікаційне обладнання можна створити загальну характеристику політики захисту. Політика захисту описуватиме технологію і процедури, що використовуються для моніторингу

стану захисту системи та контролю активності в мережі, що може виявити спроби компрометації системи і допоможе виконати аналіз атак.

Щоб забезпечити безпеку на комутаторах та маршрутизаторах, першим кроком рекомендується активувати функцію Port Security. Port Security є функцією на канальному рівні, яка має на меті запобігти несанкціонованій зміні MAC-адреси мережевого підключення. Крім того, ця функція захищає комутатор від атак, таких як переповнення таблиці MAC-адрес, атаки MAC-спуфінг та атаки ARP-спуфінг.

Також у поєднанні з безпекою портів слід використовувати механізми відстеження DHCP. DHCP snooping — це функція, яка визначає, які пристрої, підключені до портів комутатора, можуть відповідати на запити DHCP. DHCP snooping можна використовувати для запобігання неавторизованим повідомленням DHCP, які містять таку інформацію, як дані, пов'язані з IP-адресою, які надсилаються законним мережевим пристроям. У рамках процесу конфігурації DHCP порти комутатора можна ідентифікувати як надійні та ненадійні. Довірені порти можуть надсилати повідомлення DHCP будь-якого типу; ненадійні порти можуть надсилати лише запити DHCP. Ця конфігурація захищає мережу від атаки на пристрій, діючи як фальшивий сервер DHCP.

Далі для захисту від атак на процес STP слід використати одне з рішень Root Guard чи BPDU Guard. BPDU guard вимикає порт після отримання BPDU, якщо на порту ввімкнений PortFast. Вимкнення фактично забороняє пристроям з такими портами брати участь у STP. Root Guard дозволяє пристрою брати участь у STP до тих пір, поки пристрій не намагається стати root. Якщо root Guard блокує порт, подальше відновлення відбувається автоматично. Відновлення відбувається, як тільки пристрій-порушник припиняє надсилати вищий BPDU. Root Guard найкраще розгортати до портів, які підключаються до комутаторів, які не повинні бути кореневим мостом. Root Guard захищає кореневий міст від зміни іншого комутатора без дозволу адміністратора, BPDU Guard блокує порти, призначені для доступу користувачів, від підключення до несанкціонованих комутаторів [25].

Таким чином, BPDU Guard більше нагадує стандартний варіант безпеки для звичайних периферійних портів, тоді як Root Guard більш імовірний для конкретних сценаріїв.

Для ефективного запобігання DoS-атакам пов'язаним з ARP протоколом я рекомендую використовувати динамічну перевірку ARP (DAI). DAI — це функція безпеки, яка перевіряє пакети протоколу розпізнавання адрес у мережі. DAI дозволяє адміністратору мережі перехоплювати, реєструвати та відхиляти ARP-пакети з недійсними прив'язками MAC-адреси до IP-адреси. Крім того, DAI також може перевіряти ARP-пакети на відповідність налаштованим користувачем ARP-спискам ACL, щоб обробляти хости, які використовують статично налаштовані IP-адреси.

DAI також можна налаштувати на видалення пакетів ARP, якщо IP-адреси в пакеті недійсні або коли MAC-адреси в тілі пакета ARP не збігаються з адресами, указаними в заголовку Ethernet [28].

Також важливим аспектом КЗЗ є правильний час у мережі. Для точного відстеження мережевих подій, таких як порушення безпеки, необхідні правильні мітки часу. Протокол мережевого часу (NTP) — це протокол, який використовується для синхронізації годинника комп'ютерних систем у мережах передачі даних із комутацією пакетів і змінною затримкою. Протокол NTP дозволяє мережевим пристроям синхронізувати налаштування часу з сервером NTP. Група клієнтів NTP, які отримують інформацію про час і дату з одного джерела, матимуть узгодженіші налаштування часу. Безпечним методом забезпечення синхронізації для мережі є впровадження адміністраторами мережі власних приватних мережевих головних годинників, синхронізованих з UTC, за допомогою супутника чи радіо. Однак, якщо мережеві адміністратори не хочуть впроваджувати власні головні годинники через вартість або з інших причин, інші джерела годинника доступні в Інтернеті [22].

Для того щоб маршрутизатор не пропускав трафік наосліп між внутрішньою мережею та зовнішньою мережею без механізму фільтрації, слід використовувати брандмауер. Як правило, брандмауери можуть захистити локальні мережі від зовнішніх атак і запобігти зламу важливих даних, коротше кажучи, його робота — це антивірус, запобігання вторгненням, фільтрація URL-адрес, фільтрація файлів,

фільтрація вмісту, контроль поведінки додатків, фільтрація пошти, захист від поширених DDoS-атак, традиційних одно-пакетних атак.

Деякі комутатори рівня 3 можна налаштувати за допомогою правил ACL: правила контролю доступу, фільтрування пакетів на інтерфейсі відповідно до заданих умов, керування поведінкою та інші часткові функції брандмауера. У випадках, коли вимоги до безпеки мережі невисокі, можна повністю ігнорувати брандмауери [31].

На рівні фізичної безпеки також необхідно забезпечити захист пристроїв. Фізичний доступ до комунікаційного обладнання може дати порушнику повний контроль над ним. Також, фізичний доступ до каналів зв'язку дозволяє перехоплювати повідомлення або відтворювати додаткові дані. Навряд чи будуть ефективні складні програмні засоби захисту, якщо не забезпечено контроль доступу до мережного обладнання та каналів зв'язку. Захист мережного обладнання має включати правильну конфігурацію обладнання і політику контролю, обмеження доступу до обладнання, забезпечення надійності електроживлення та охолодження, контроль прямого доступу до всього мережного обладнання, захист каналів зв'язку та розробку плану відновлення системи у разі катастрофи [32].

Адміністративний інтерфейс маршрутизаторів, серверів мережного доступу і брандмауерів є привабливою мішенню для зловмисників. Якщо зловмисник отримує несанкціонований доступ до адміністративного інтерфейсу, він може вносити зміни в конфігурацію пристрою, здійснити несанкціоновані операції або отримати повний контроль над пристроєм. Це може призвести до компрометації безпеки мережі або навіть недоступності мережних сервісів. Для забезпечення безпеки адміністративного інтерфейсу необхідно вжити певні заходи. Перш за все, слід використовувати шифрування паролів для запобігання простому перехопленню і використанню адміністративних облікових записів. Крім того, впровадження багаторівневої системи привілеїв доступу дозволить обмежити права користувачів, що мають доступ до адміністративного інтерфейсу, та запобігти несанкціонованим діям. Загалом, захист адміністративного інтерфейсу передбачає використання шифрування паролів, впровадження багаторівневої системи привілеїв доступу, управління доступом SNMP

та інші заходи, які допоможуть убезпечити пристрої від несанкціонованого доступу та зберегти безпеку мережі.

3.2 Рекомендації щодо комплексу засобів захисту сучасного комунікаційного обладнання

Базовий захист комунікаційного обладнання не зупиняє зловмисні атаки. Безпека – це багаторівневий процес, який, по суті, ніколи не завершується. Чим більше спеціалісти в організації обізнані щодо атак на безпеку та загроз, які вони несуть, тим краще. На основі проведеного дослідження було сформовано власні висновки та рекомендації щодо комплексу засобів захисту сучасного комунікаційного обладнання:

1. Детально вивчайте вбудовані функції захисту комунікаційного обладнання та налаштовуйте їх відповідно до інструкцій наданих виробниками. Більшість сучасних виробників надають покрокові інструкції з ілюстраціями по налаштуванню, а також в більшості є цілодобова служба підтримки якій можна поставити питання при виникненні різного роду проблем.

2. Підтримуйте актуальне програмне забезпечення. Регулярно оновлюйте програмне забезпечення на комунікаційному обладнанні. Це включає оновлення операційних систем, мережевих драйверів і патчів безпеки. Оновлення допомагають виправити виявлені вразливості та контролювати актуальність бази шкідливих програм. Встановлюйте оновлення щотижня або щодня, якщо це можливо.

3. Використовуйте мережеві фаєрволи: Встановлюйте мережеві фаєрволи для контролю трафіку, який входить і виходить з вашої мережі. Налаштуйте правила фаєрволу для блокування небажаного трафіку, а також для контролю доступу до адміністративних інтерфейсів комунікаційного обладнання.

4. Контролюйте фізичний доступ до комунікаційного обладнання. Такий доступ може значно полегшити завдання зловмиснику та надати йому можливість повного контролю над вашою системою.

5. Забезпечення безпеки мережі також передбачає закриття невикористовуваних служб та портів. Відкриті порти та служби, які не використовуються, можуть стати точкою входу для зловмисників та потенційно вразливими для атак. Тому важливо перевіряти активні порти та служби на мережному обладнанні та серверах і закривати ті, які не є необхідними.

6. Впроваджуйте шифрування: Застосовуйте шифрування для захисту конфіденційної інформації, яка передається через мережу. Використовуйте протоколи шифрування, такі як SSL/TLS, для захисту комунікації між клієнтами і серверами.

7. Регулярно проводьте аудит комунікаційної інфраструктури. Інструменти безпеки дозволяють адміністратору мережі виконувати перевірку безпеки, що виявляє тип інформації, яку може зібрати зловмисник, просто відстежуючи мережевий трафік.

8. Встановіть систему моніторингу, яка буде виявляти підозрілий трафік, спроби несанкціонованого доступу та аномальну активність у вашій мережі. Це дозволить вчасно виявляти та реагувати на потенційні загрози.

9. За необхідності можна проводити тести на проникнення, але вони проводяться в дуже контрольованих умовах, дотримуючись задокументованих процедур, детально викладених у комплексній політиці безпеки. Ідеальним варіантом може бути тестовий стенд, який імітує фактичну роботу комунікаційного обладнання. Проте це не буде актуальним для невеликих організацій.

10. Регулярно проводьте навчання персоналу. Забезпечте навчання свого персоналу щодо безпеки комунікаційного обладнання. Навчайте їх розпізнавати підозрілу активність, обережно ставитися до невідомих посилань та завантажувати оновлення з надійних джерел.

Дані рекомендації можна назвати відправною точкою для управління безпекою комунікаційної системи. Організації повинні постійно залишатися пильними та відслідковувати появу нових загроз, щоб бути захищеними від будь-яких спроб зловмисного впливу.

3.2 Перспективи подальших досліджень

Вивчення нових перспектив дозволить покращити захист комунікаційного обладнання і вдосконалити стратегії захисту від нових загроз. Отримані результати можуть бути використані для розробки нових методів, стандартів та інструментів, спрямованих на підвищення безпеки комунікаційного обладнання. Ось список перспектив подальших досліджень в сфері захисту комунікаційного обладнання:

1. Розвиток нових методів виявлення атак: Важливо постійно вдосконалювати методи виявлення вразливостей в комунікаційному обладнанні. Дослідження в цій області можуть спрямовуватися на розробку нових алгоритмів аналізу мережевого трафіку, машинного навчання та штучного інтелекту для виявлення підозрілої активності та атак.

2. Вивчення нових загроз та вразливостей: Технології швидко розвиваються, і з'являються нові типи атак та вразливостей. Подальші дослідження можуть бути спрямовані на вивчення нових методів атак, таких як атаки з використанням штучного інтелекту, розробку захисних стратегій та протоколів, що забезпечують стійкість комунікаційного обладнання до таких загроз.

3. Аналіз захисту в хмарних середовищах: Захист комунікаційного обладнання в хмарних середовищах викликає особливі виклики та проблеми. Подальші дослідження можуть спрямовуватися на розробку ефективних методів захисту в хмарних середовищах, включаючи розумний контроль доступу, шифрування даних та моніторинг безпеки.

4. Вивчення соціально-інженерних атак: Соціально-інженерні атаки стають все більш поширеними та складними. Подальші дослідження можуть бути спрямовані на аналіз методів соціально-інженерної маніпуляції та розробку стратегій протидії таким атакам.

5. Розробка стандартів та нормативів: Розробка стандартів та нормативів є важливим кроком у забезпеченні безпеки комунікаційного обладнання. Дослідження можуть бути спрямовані на розробку нових стандартів та нормативів щодо захисту комунікаційного обладнання, які враховують сучасні технології та загрози.

Висновки до третього розділу

На основі проведеного нами дослідження в третьому розділі, ми можемо зробити наступні висновки. В ході вибору методів захисту комунікаційного обладнання було виявлено, що ефективний захист вимагає комплексного підходу, оскільки загрози та атаки постійно еволюціонують.

Виходячи з чого були сформовані такі рекомендації: детально вивчайте вбудовані функції захисту комунікаційного обладнання та налаштовуйте їх відповідно до інструкцій наданих виробниками, підтримуйте актуальне програмне забезпечення, використовуйте мережеві фаєрволи, контролюйте фізичний доступ до комунікаційного обладнання, закрийте служби та порти, які не використовуються, застосовуйте шифрування для захисту конфіденційної інформації, яка передається через мережу, регулярно проводьте аудит комунікаційної інфраструктури, встановіть систему моніторингу, за необхідності проводьте тести на проникнення, регулярно проводьте навчання персоналу.

Також в даному розділі було розглянуто перспективи подальших досліджень, а саме: розвиток нових методів виявлення атак, вивчення нових загроз та вразливостей, аналіз захисту в хмарних середовищах, вивчення соціально-інженерних атак, розробка стандартів та нормативів. Загалом же захист комунікаційного обладнання є невід’ємною складовою сучасної мережі і вимагає постійного вдосконалення та вивчення нових методів та технологій для забезпечення безпеки та надійності.

ВИСНОВКИ

У рамках кваліфікаційної роботи було проведено детальне дослідження захисту комунікаційного обладнання, яке виявилося дуже актуальним у сучасному світі інформаційних технологій. Захист комунікаційного обладнання є критичним завданням для безпеки та надійності мережі.

Проаналізовано найпопулярніші сценарії проведення атак на комунікаційне обладнання таких як атака STP, ARP-спуфінг, MAC-спуфінг, переповнення CAM-таблиці комутатора, атака на DHCP-сервер. Відповідно яким були сформовані найкращі методи запобігання та захисту комунікаційного обладнання. Серед яких Root Guard, BPDU Guard, DAI, шифрування трафіку, блокування портів MAC-адрес, аутентифікація пристроїв, контроль доступу до комутатора та інших пристроїв, правила фільтрації MAC-адрес, DHCP snooping.

Було виявлено, що загрози та атаки на комунікаційне обладнання постійно зростають і еволюціонують. З метою ефективного захисту необхідний комплексний підхід, що включає в себе різноманітні методи та технології. Виходячи з чого були сформовані наступні рекомендації: детально вивчайте вбудовані функції захисту комунікаційного обладнання та налаштовуйте їх відповідно до інструкцій наданих виробниками, використовуйте мережеві фаєрволи, контролюйте фізичний доступ до комунікаційного обладнання, закрийте служби та порти, які не використовуються, застосовуйте шифрування для захисту конфіденційної інформації, яка передається через мережу, регулярно проводьте аудит комунікаційної інфраструктури, встановіть систему моніторингу, за необхідності проводьте тести на проникнення, регулярно проводьте навчання персоналу, важливим етапом є також регулярне оновлення програмного забезпечення комунікаційного обладнання для усунення вразливостей та багів, здійснення резервного копіювання конфігурацій і даних комунікаційного обладнання сприятиме відновленню роботи у разі виникнення проблеми.

Перспективи подальших досліджень у цій галузі включають розробку та впровадження нових алгоритмів машинного навчання та штучного інтелекту для

виявлення та прогнозування нових типів загроз. Також розробка стандартів і протоколів для безпеки Інтернет-речей, оскільки збільшується кількість підключених пристроїв, які створюють нові ефективні точки для атаки.

Комунікаційне обладнання утворює своєрідний міст між користувачами та їхніми комп’ютерами, з одного боку, і ресурсами, які їм потрібні, з іншого. І цей міст та його фундамент необхідно обслуговувати та постійно контролювати, щоб переконатися, що все працює належним чином і без помилок. Кожен компонент стратегії безпеки зміцнює та захищає організацію в цілому від збою будь-якого окремого компонента. Тож слід розуміти у міру того, як організація росте та скорочується, комунікаційне обладнання та засоби безпеки, які його захищають, повинні розвиватися та відповідати новим викликам з боку зловмисників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комп'ютерні мережі: підручник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.]. − Вінниця : ВНТУ, 2020. – Режим доступу до ресурсу: http://pdf.lib.vntu.edu.ua/books/IRVC/Azarov_2020_378.pdf

2. Аналіз мережевого обладнання для побудови мережі інтернет-провайдера [Електронний ресурс] / С. С. Волошко, А. Ю. Фролов – Режим доступу до ресурсу: http://reposit.nupp.edu.ua/bitstream/PoltNTU/4575/1/%D0%A1%D1%82%D0%B0%D1%82%D1%82%D1%8F%20%D0%9D%D0%86%D0%A1%D0%A2%20%D0%A4%D1%80%D0%BE%D0%BB%D0%BE%D0%B2.pdf

3. Основи інфокомунікаційних технологій: Навчальний посібник [А.П. Бондарчук, Г.С. Срочинська, М.Г. Твердохліб]. – Київ, 2015 – Режим доступу до ресурсу: http://kist.ntu.edu.ua/textPhD/osnovInfComTeh.pdf

4. Особливості побудови локальних мереж [Електронний ресурс]. – Режим доступу до ресурсу: https://studfile.net/preview/7194624/page:2/

5. Мережеві пристрої. Властивості мережевих пристроїв та їх функції. [Електронний ресурс]. – Режим доступу до ресурсу: https://gazik.ua/blog/porady-pokuptsyam/merezhevi-prystroyi-vlastyvosti-merezhevykh-prystroyiv-ta-yikh-funktsiyi/

6. 7 Popular Layer 2 Attacks [Електронний ресурс]. – Режим доступу до ресурсу: https://www.pearsonitcertification.com/articles/article.aspx?p=2491767

7. VLAN hopping attack – Switch Spoofing and Double tagging [Електронний ресурс]. – Режим доступу до ресурсу: https://howdoesinternetwork.com/2012/vlan-hopping-attack/

8. 802.1X-2020 - IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control [Електронний ресурс]. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/9018454

9. IPsec (Internet Protocol Security) [Електронний ресурс]. – Режим доступу до ресурсу: https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security#IPsec_Protocols

10. 802.11-2020 - IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications [Електронний ресурс]. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/9363693

11. NIST SP 800-57 Part 1 Rev. 5 Recommendation for Key Management: Part 1 – General [Електронний ресурс]. – Режим доступу до ресурсу: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

12. Безпека інформаційно-комунікаційних систем: підручник / [Грайворонський М. В.; Новіков О. М]. − Київ : Видавнича група BHV, 2009 – Режим доступу до ресурсу: http://www.is.ipt.kpi.ua/pdf/Graivorovskyi_Novikov.pdf

13. ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ: підручник / [В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний]. − Київ : КУБГ, 2019 – Режим доступу до ресурсу: https://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBMI.pdf

14. What is STP (Spanning Tree Protocol) And its attack? [Електронний ресурс]. – Режим доступу до ресурсу: https://securiumsolutions.com/blogs/spanning-tree-protocol/

15. Prevent STP Attacks [Електронний ресурс]. – Режим доступу до ресурсу: https://www.howtonetwork.com/technical/security-technical/prevent-stp-attacks/

16. Address resolution protocol (arp) spoofing: what it is and how to prevent an arp attack [Електронний ресурс]. – Режим доступу до ресурсу: https://www.crowdstrike.com/cybersecurity-101/spoofing-attacks/arp-spoofing/

17. MAC Spoofing Attack [Електронний ресурс]. – Режим доступу до ресурсу: https://www.ccexpert.us/ccie-security/mac-spoofing-attack.html

18. Protecting against MAC flooding attack [Електронний ресурс]. – Режим доступу до ресурсу: https://www.ciscozine.com/protecting-against-mac-flooding-attack/

19. ARP Poisoning: What it is & How to Prevent ARP Spoofing Attacks [Електронний ресурс]. – Режим доступу до ресурсу: https://www.varonis.com/blog/arp-poisoning

20. What is MAC Spoofing Attack? [Електронний ресурс]. – Режим доступу до ресурсу: https://www.geeksforgeeks.org/what-is-mac-spoofing-attack/

21. Cisco Networking Academy's Introduction to Basic Switching Concepts and Configuration [Електронний ресурс]. – Режим доступу до ресурсу: https://www.ciscopress.com/articles/article.asp?p=2181836&seqNum=7

22. IPsec (Internet Protocol Security) [Електронний ресурс]. – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/IPsec-Internet-Protocol-Security

23. Захист інформації в комп'ютерних системах: підручник / [Гапак О.М., Балога С.І.]. – Ужгород, 2021

24. Варіанти захисту від загроз в комунікаціях розподілених мереж [Електронний ресурс]. – Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/10600/1/15_p104.pdf

25. Enhance Spanning Tree Protocol with Root Guard [Електронний ресурс]. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html#diff

26. Chapter: Understanding and Configuring Dynamic ARP Inspection [Електронний ресурс]. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html

27. What Is The Difference Between Switches and Firewalls? [Електронний ресурс]. – Режим доступу до ресурсу: https://www.utepo.net/article/detail/What_Is_The_Difference_Between_Switches_and_Firewalls?.html

28. Network Protection: How to Secure a Network [Електронний ресурс]. – Режим доступу до ресурсу: https://www.esecurityplanet.com/networks/how-to-secure-a-network/

29. 7 Tips for Office Network Security [Електронний ресурс]. – Режим доступу до ресурсу: https://carbidesecure.com/resources/7-tips-for-office-lan-security/

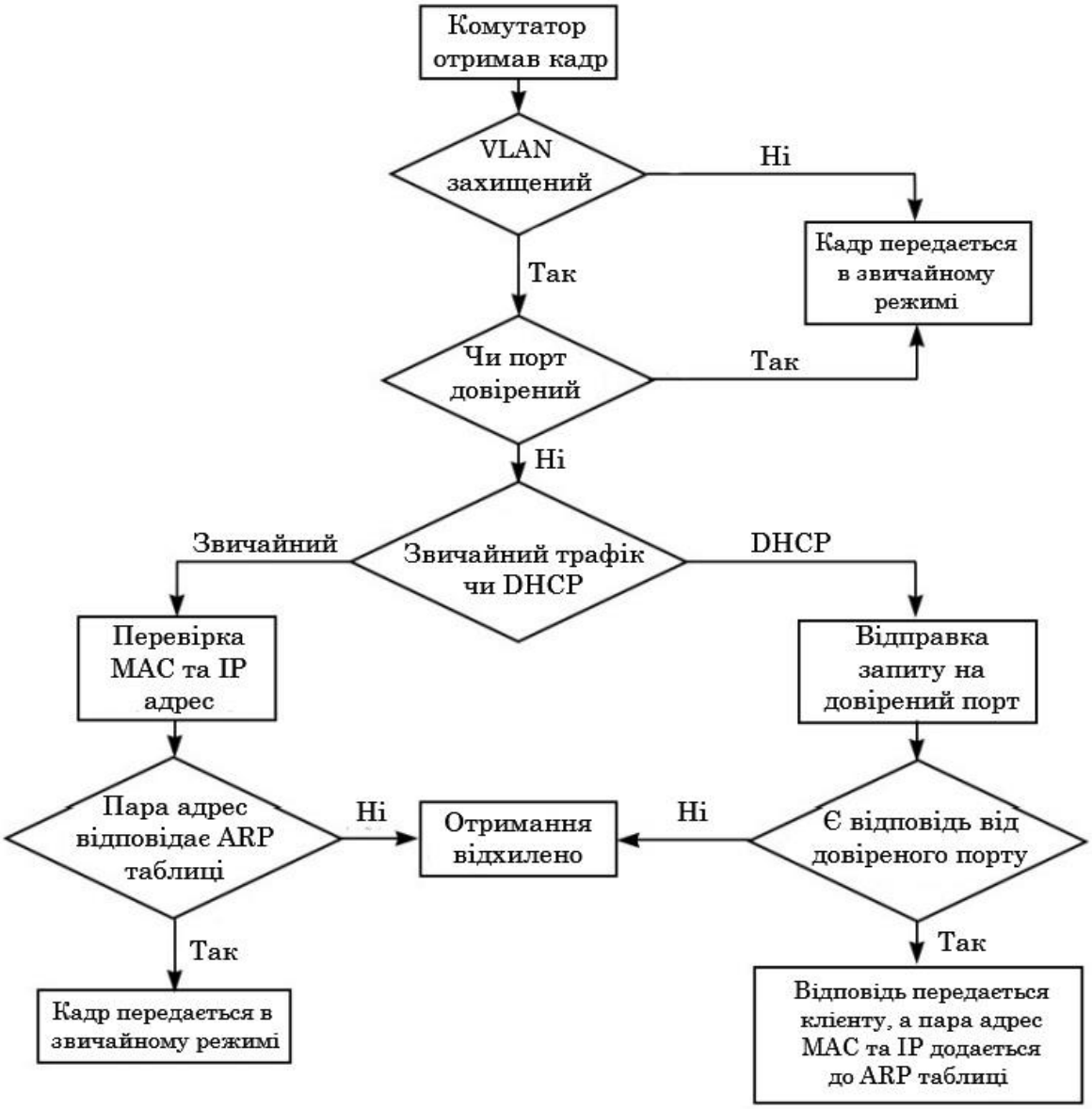
30. Буточнов О. М., Гончар Г. В., Деревянко С. М., Короленко М. П. Захист інформації в комунікаційній мережі зв'язку ЄДАПС. // К.: Вісті Академії інженерних наук України. 2005, № 2, с. 37 − 58;

31. Захист інформації в телекомунікаційних системах: Навчальний посібник.(лист МОНУ №1.4/18 – Г – 183 від 02.06.2009р.). –К.: НАУ,2009. – Режим доступу до ресурсу: https://tks.nau.edu.ua/wp-content/uploads/2016/05/Zahyst-informatsiyi-v-telekomunikatsijnyh-systemah.pdf

32. Solutions for LAN and WAN Protection [Електронний ресурс]. – Режим доступу до ресурсу: https://www.alliedtelesis.com/ua/en/solution-guide/solutions-lan-wan-protection

ДОДАТОК А

АЛГОРИТМ РОБОТИ КОМУТАТОРА З ВСТАНОВЛЕНИМИ ФУНКЦІЯМИ DHCP SNOOPING І DAI



ДОДАТОК Б

УЗАГАЛЬНЕНА СТРУКТУРА МОЖЛИВИХ ЗАСОБІВ І МЕХАНІЗМІВ ЗАХИСТУ КОМУНІКАЦІЙНОЇ МЕРЕЖІ