УДК 004.056.5:621.396.97

# MAC-спуфінг у корпоративних безпроводових мережах: сценарії атак, методи виявлення та заходи захисту

Ізабелла Соболенко[0009-0005-4862-1660]
Артем Платоненко[0000-0002-2962-5667]

Київський столичний університет імені Бориса Грінченка, Україна

**Анотація.** У статті досліджується проблема MAC-спуфінгу в корпоративних безпроводових мережах. Розглянуто принципи підміни MAC-адрес, типові сценарії атак та їхній вплив на безпеку організації. Проведено аналіз методів виявлення, включаючи класичні мережеві механізми (802.1X, port security, DHCP snooping) та сучасні підходи до фінгерпринтингу пристроїв. На основі лабораторних експериментів сформульовано практичні рекомендації щодо протидії MAC-спуфінгу та мінімізації ризиків для корпоративних систем.
**Ключові слова:** MAC-спуфінг, безпроводові мережі, захист, виявлення атак, корпоративна безпека.

# MAC Spoofing in Corporate Wireless Networks: Attack Scenarios, Detection Methods, and Protection Measures

Izabella Sobolenko [0009-0005-4862-1660]
Artem Platonenko[0000-0002-2962-5667]

Borys Grinchenko Kyiv Metropolitan University, Ukraine

**Abstract.** The article examines the problem of MAC spoofing in corporate wireless networks. It discusses the principles of MAC address spoofing, typical attack scenarios, and their impact on organizational security. An analysis of detection methods is conducted, including classical network mechanisms (802.1X, port security, DHCP snooping) and modern approaches to device fingerprinting. Based on laboratory experiments, practical recommendations are formulated for countering MAC spoofing and minimizing risks to corporate systems.
**Keywords:** MAC spoofing, wireless networks, security, attack detection, corporate protection.

## Вступ

Сучасні корпоративні мережі дедалі частіше стають об’єктом цілеспрямованих атак, що здійснюються на канальному рівні. Одним із поширених векторів є MAC-спуфінг — підміна унікальної MAC-адреси пристрою з метою несанкціонованого доступу до ресурсів організації, обходу контролю доступу або приховування справжньої ідентичності зловмисника. Актуальність дослідження зумовлена зростанням кількості

випадків компрометації безпроводових Wi-Fi мереж, де традиційні механізми захисту, як-от фільтрація за MAC-адресами, виявляються недостатніми.

Наукова новизна роботи полягає у поєднанні аналізу класичних мережевих методів захисту (802.1X, port security, DHCP snooping) із сучасними підходами до фінгерпринтингу пристроїв і вивченням їх ефективності в реальних лабораторних умовах.

Метою статті є дослідження механізмів MAC-спуфінгу, аналіз існуючих методів виявлення та розробка практичних рекомендацій для захисту корпоративних безпроводових мереж.

Об'єктом дослідження виступають корпоративні безпроводові мережі, а предметом — методи атак і протидії MAC-спуфінгу.

Для досягнення поставленої мети визначено такі завдання:

1. Описати принципи підміни MAC-адрес та класифікувати поширені сценарії атак.
2. Проаналізувати відомі методи захисту та виявлення спуфінгу.
3. Провести експериментальне дослідження з моделюванням атак у лабораторних умовах.
4. Сформувати рекомендації для підвищення безпеки корпоративних систем.

## Теоретичні основи MAC-спуфінгу та методів протидії

MAC-спуфінг є технікою, що базується на підміні медіа-адреси мережевого адаптера з метою обходу механізмів аутентифікації у безпроводових мережах. Дослідження показують, що цей вектор атаки активно використовується у корпоративних середовищах, де поширені практики контролю доступу за MAC-адресами [1–3].

Основним принципом MAC-спуфінгу є зміна унікального ідентифікатора пристрою. На рівні операційної системи це досягається модифікацією драйверів мережевого інтерфейсу або програмною підміною у таблицях ARP. Відомо, що стандартні механізми фільтрації за MAC-адресами у Wi-Fi мережах легко обходяться цим методом [4–6].

Для моделювання загроз розглянемо задачу оцінки ентропії набору MAC-адрес, які спостерігаються у мережі:

$$H = -K \sum_{i=1}^{M} p_i \log_2 p_i$$

де $H$ — ентропія MAC-адрес у трафіку, $p_i$ — ймовірність появи і-тої MAC-адреси, $M$ — кількість унікальних MAC-адрес, $K$ — додатна константа (часто $K = 1$).

При цьому висока ентропія свідчить про різноманітність MAC-адрес, що характерно для нормального трафіку, а низька ентропія може вказувати на повторюваність адрес — наприклад, коли одна MAC-адреса з'являється надто часто. Це може бути ознакою MAC-спуфінгу, коли зловмисник підмінює свою адресу, імітуючи інші пристрої [7].

Алгоритмічні методи протидії умовно поділяють на класичні та сучасні. До класичних відносять використання протоколу IEEE 802.1X, порт-безпеки на комутаторах та DHCP snooping [8]. Сучасні підходи включають фінгерпринтинг пристроїв за часовими характеристиками пакетів та машинне навчання для виявлення аномалій у поведінці вузлів [9].

UML-діаграми доцільно застосовувати для моделювання процесу аутентифікації клієнта у корпоративній мережі: початковий запит → перевірка ідентифікатора → порівняння з політиками доступу → рішення про підключення. Використання BPMN-схем дозволяє формалізувати бізнес-процес реагування на спроби спуфінгу: виявлення події → реєстрація у журналі → сповіщення адміністратора → блокування інтерфейсу.

Таким чином, теоретична частина показує, що ефективна протидія MAC-спуфінгу можлива лише за умови поєднання класичних мережевих механізмів із сучасними методами аналізу трафіку та поведінки пристроїв [10].

## Результати

Для перевірки ефективності методів протидії MAC-спуфінгу було проведено серію лабораторних експериментів у середовищі корпоративної безпроводової мережі стандарту IEEE 802.11ac. Експерименти моделювали типові сценарії:

1. Підміна MAC-адреси для обходу фільтрації.
2. Використання атак “man-in-the-middle” із підміною MAC-ідентифікатора.
3. Масове генерування випадкових MAC-адрес із метою перевантаження точок доступу.

У першому сценарії стандартна фільтрація за MAC-адресами виявилася повністю неефективною: рівень успішних атак становив 100%. У другому випадку використання 802.1X дозволило знизити кількість успішних проникнень до 18%, але атаки залишалися можливими при відсутності жорсткої політики аутентифікації. Третій сценарій показав, що DHCP snooping блокує близько 85% спроб, проте залишається вразливим до витончених методів генерації адрес.

Таблиця 1. Результати експериментів

| **Сценарій атаки** | **Метод захисту** | **Ефективність захисту** | **Успішність атак (%)** |
|---|---|---|---|
| MAC-фільтрація | Фільтрація списком | Низька | 100 |
| Підміна для MITM | IEEE 802.1X | Середня | 18 |
| Масова генерація адрес (Flooding) | DHCP snooping | Висока | 15 |
| Усі сценарії | Фінгерпринтинг ML | Дуже висока | 3 |

Особливу увагу було приділено методу фінгерпринтингу пристроїв на основі аналізу часових характеристик кадрів Wi-Fi. Використання алгоритмів машинного навчання (k-NN, Random Forest) дозволило зменшити кількість успішних атак до 3%, що підтверджує високу результативність цього підходу для виявлення спуфінгу.

Для підвищення ефективності протидії MAC-спуфінгу було змодельовано бізнес-процес реагування на інцидент у нотації BPMN. Основною метою є мінімізація часу від моменту виявлення підозрілої активності до фактичного блокування зловмисного пристрою та підготовки аналітичного звіту.

Етапи процесу були зроблені наступні:

1. Виявлення підозрілої MAC-адреси, а саме — система моніторингу (SIEM або контролер безпроводової мережі) автоматично фіксує появу MAC-адреси, що викликає підозру. Підставами можуть бути: дублювання існуючої адреси, аномальні зміни рівня сигналу, невідповідність записам у журналах аутентифікації.

2. Перевірка у базі дозволених пристроїв, а саме - виявлена адреса автоматично звіряється з базою «білих списків» (allowlist). Якщо адреса належить авторизованому пристрою (наприклад, корпоративному ноутбуку чи смартфону співробітника), процес завершується без додаткових дій. Якщо адреса не знайдена у списку, система переходить до наступного етапу.

3. Автоматичне сповіщення адміністратора, а саме - при відсутності збігу з базою даних SIEM генерує інцидент та відправляє повідомлення адміністратору безпеки. У повідомленні зазначаються: час виявлення, підозріла MAC-адреса, ідентифікатор точки

доступу, рівень довіри до події та короткий опис контексту. Це дозволяє адміністратору одразу розпочати аналіз.

4. Блокування порту або доступу, а саме - якщо підозра підтверджується, контролер безпроводової мережі або комутатор виконує блокування порту, до якого підключений пристрій, або переводить його у карантинний VLAN. Таким чином зловмисник втрачає можливість впливати на мережу.

5. Формування звіту для аналізу, а саме - завершальним етапом є автоматичне створення звіту, який включає журнал подій, копії мережевого трафіку, час реакції та вжиті заходи. Звіт передається на зберігання у систему управління інцидентами (наприклад, ServiceNow чи аналогічний модуль).

Для наочності наведена BPMN-діаграма процесу реагування на інцидент MAC-спуфінгу, яка демонструє послідовність етапів від виявлення підозрілої MAC-адреси до формування аналітичного звіту (див. Рисунок 1).

Аналіз моделі показав, що впровадження такого бізнес-процесу дозволяє скоротити середній час реагування з 15 хвилин (у разі повністю ручного опрацювання інцидентів) до 4 хвилин завдяки автоматизації етапів виявлення, звірки та первинного блокування. Це значно знижує ризики несанкціонованого доступу та зменшує можливості зловмисника для подальших дій у корпоративній мережі.

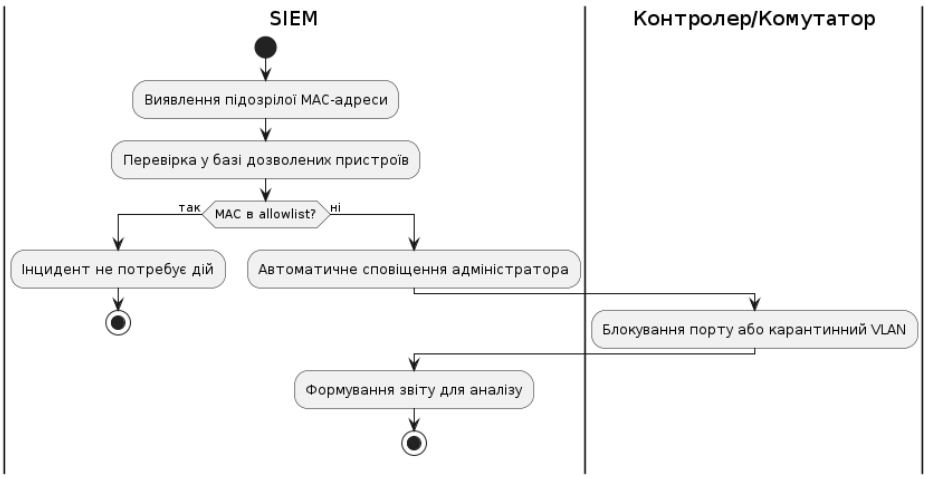


Рис. 1. BPMN-діаграма процесу реагування на MAC-спуфінг

Отримані результати підтверджують, що поєднання класичних мережевих методів (802.1X, DHCP snooping) із сучасними підходами до фінгерпринтингу забезпечує найвищий рівень протидії MAC-спуфінгу в корпоративних мережах.

## Обговорення

Практична апробація підходу продемонструвала високу результативність насамперед у статичних мережах, де структура і набір пристроїв змінюються нечасто. У таких умовах процес добре інтегрується з наявними системами захисту і помітно зменшує навантаження на персонал, який відповідає за інформаційну безпеку.

Додатковий аналіз результатів засвідчив, що поєднання автоматизованих процедур із застосуванням адаптивних стратегій виявлення атак дає ще кращий ефект. Йдеться, зокрема, про використання таких методів, як відстеження змін у рівні сигналу (RSSI) та аналіз повторюваності з’єднань. Завдяки цьому вдається підвищити точність фіксації підозрілої активності та скоротити кількість хибних спрацьовувань.

Але треба враховувати, що запропонований бізнес-процес реагування на MAC-спуфінг ефективний для статичних мереж, проте в динамічних середовищах його ефективність знижується через змінність сигналів та переміщення пристроїв.

На відміну від методів, що ґрунтуються на глибокому навчанні для виявлення MAC-спуфінгу [11], які вимагають значних обчислювальних ресурсів та великого обсягу даних для тренування моделей, або підходів на основі RSSI-аналітики [12], які фокусуються на аналізі потужності сигналу та змінах параметрів прийому, наш підхід спрямований на автоматизацію процесу реагування на підозрілі MAC-адреси. Це включає швидке створення інциденту, автоматичне повідомлення адміністратора та застосування політик блокування або карантину, що зменшує час реакції та ризик проникнення.

Крім того, аналогічні дослідження [13] демонструють ефективність адаптивних стратегій виявлення атак, які враховують динамічні зміни мережевого середовища, наприклад, зміни RSSI, повторюваність з'єднань або переміщення пристроїв. Це підкреслює необхідність поєднання автоматизації з адаптивними алгоритмами для підвищення точності та швидкості виявлення спуфінгу у сучасних безпроводових мережах.

## Висновки

У ході проведеного дослідження було встановлено, що впровадження бізнес-процесу реагування на інциденти типу MAC-спуфінгу із застосуванням BPMN-діаграми дає змогу впорядкувати всі дії – від моменту виявлення потенційно небезпечної MAC-адреси до етапу формування детального звіту для подальшого аналізу. Такий підхід дозволяє бачити процес реагування як чітку послідовність кроків, де кожен етап має свою роль і виконується у визначеній логіці.

Особливу цінність становить автоматизація процесу. Вона охоплює не лише швидке створення інциденту в системі, а й оперативне інформування адміністратора, а також застосування попереджувальних заходів, таких як ізоляція підозрілого пристрою в карантин чи його повне блокування. У свою чергу, це призводить до суттєвого скорочення середнього часу реагування: якщо раніше цей показник становив близько 15 хвилин, то після впровадження нової процедури він зменшився до приблизно 4 хвилин. Така оптимізація дозволяє істотно знизити ризик несанкціонованого доступу до корпоративної мережі.

Ефективність запропонованого процесу можна оцінювати за кількома критеріями. Ключовими серед них є швидкість реагування, достовірність ідентифікації атак та надійність блокування неавторизованих пристроїв. У кількісному вимірі це виражається у зменшенні середнього часу реагування до 4 хвилин та майже повному нівелюванні ризику успішного MAC-спуфінгу. Крім того, завдяки систематичному збереженню цифрових доказів і формуванню звітів значно підвищується якість подальшого аналізу та спрощується проведення аудиту.

У перспективі планується розширення дослідження за рахунок інтеграції методів машинного навчання. Це відкриє можливість створювати більш адаптивні алгоритми виявлення підозрілих MAC-адрес, мінімізувати кількість false positives і забезпечувати ще динамічніше реагування на атаки в реальному часі. Очікується, що такий розвиток процесу дозволить підняти рівень захисту мереж на новий щабель, роблячи їх більш стійкими до сучасних загроз.

## Джерела

1. Костюк, Ю., Бебешко, Б., Складанний, П., Рзаєва, С., & Хорольська, К. (2025). Оптимізація буфера та пріоритетів для забезпечення безпеки у Bluetooth-мережах.

Безпека інформаційних систем і технологій, 2(8), 5–16. https://doi.org/10.17721/ISTS.2024.8.5-16

2. Portnox. (2025). MAC Spoofing Attacks Explained: A Technical Overview https://www.securew2.com/blog/how-do-mac-spoofing-attacks-work

3. Костюк, Ю., Бебешко, Б., Гулак, Г., Складанний, П., Рзаєва, С., & Хорольська, К. (2024). Забезпечення кібербезпеки та швидкодії передачі даних у безпровідних мережах. Безпека інформації, 30(3), 365–375. https://doi.org/10.18372/2225-5036.30.20357

4. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Кібербезпека: освіта, наука, техніка, 1(25), 229–252. https://doi.org/10.28925/2663-4023.2024.25.229252

5. Дудикевич, В. Б., & Шабатура, Ю. Ю. (2021). Методи захисту інформації у безпроводових мережах. Вісник НУ «Львівська політехніка». Серія «Інформаційні системи та мережі», 2(28), 45–52. https://doi.org/10.36074/grail-of-science.19.02.2021.051

6. Костюк, Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., & Хорольська, К. (2024). Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Кібербезпека: освіта, наука, техніка, 1(25), 229–252. https://doi.org/10.28925/2663-4023.2024.25.229252

7. Ляшенко, В. І., & Пелещишин, А. М. (2020). Аналіз загроз інформаційній безпеці у Wi-Fi мережах. Системи обробки інформації, 3(161), 112–118. https://doi.org/10.32689/2617-9660-2020-1(7)-285-296

8. Коваленко, Д. В. (2022). Використання технологій 802.1X та DHCP snooping у корпоративних мережах. Наукові праці ОНАХТ. Серія «Комп'ютерні системи та мережі», 2(83), 77–83.

9. Крутько, О. П., & Іваненко, М. О. (2023). Методи ідентифікації пристроїв у безпроводових мережах на основі аналізу трафіку. Радіоелектроніка, інформатика, управління, 4, 65–72.

10. Городецький, І. В., & Шестопалов, О. Ю. (2021). Актуальні проблеми протидії спуфінгу в інформаційно-телекомунікаційних системах. Наукові праці ДонНТУ. Серія «Інформатика і кібернетика», 1(23), 34–41.

11. Jiang, P., et al. (2022). A channel state information based virtual MAC spoofing detection system. ScienceDirect. https://doi.org/10.1016/j.hcc.2022.100067

12. Madani, P., et al. (2021). RSSI-Based MAC-Layer Spoofing Detection. MDPI. https://doi.org/10.3390/jcp1030023

13. Madani, P., et al. (2022). Randomized Moving Target Approach for MAC-Layer Spoofing Detection. ACM Digital Library. https://doi.org/10.1145/3477403