resilience to variability in input data. The article presents the operational algorithm, mathematical formulation of the modules, the principle of decision integration, and scalability potential. The proposed solution shows promise for practical implementation in mobile devices, access control systems, and online identity verification platforms.

Key words: *technical information protection; biometric authentication; machine learning; liveness detection; computer vision; multi-layered protection; anti-spoofing.*

Отримано: 9.06.2025

УДК 004.85
DOI: 10.32626/2308-5916.2025-27.102-121

В. В. Палагін, д-р техн. наук, професор,
О. В. Івченко, канд. техн. наук,
О. А. Палагіна, канд. техн. наук,
В. В. Філіпов, канд. техн. наук,
А. В. Байрак,
О. А. Проценко

Черкаський державний технологічний університет, м. Черкаси

МЕТОД МАШИННОГО НАВЧАННЯ ДЛЯ АНАЛІЗУ ШКІДЛИВОГО МЕРЕЖЕВОГО ТРАФІКУ НА ПРИКЛАДНОМУ РІВНІ (DHCP SPOOF)

DHCP (Dynamic Host Configuration Protocol) є критично важливим елементом мережевої інфраструктури, що забезпечує автоматичну видачу IP-адрес і параметрів конфігурації клієнтам. Проте через відсутність механізмів аутентифікації в базовому протоколі він є вразливим до атак типу DHCP spoofing, коли зловмисник імітує роботу легітимного сервера та видає клієнтам шкідливі налаштування. У цій роботі запропоновано підхід до виявлення таких атак із використанням методів машинного навчання, що дозволяє ідентифікувати як типові варіанти атак із фальшивими IP-адресами, так і складніші – із підміною MAC-адрес при справжньому IP сервера.

У межах дослідження розроблено інструмент для генерації DHCP-трафіку з різноманітними сценаріями поведінки, включно з нормальними сесіями, атаками з різними IP-адресами зловмисників та маскуванням під легітимного сервера. Запропоновано застосування методів машинного навчання (*Machine learning – ML*) для аналізу даних про трафіку, які отримані в режимі реального часу. На основі отриманого PCAP-файлу було автоматизовано процес побудови датасету зі стисненим, але інформативним набором ознак (кількість унікальних IP/MAC-адрес, перший MAC-відповідач, відповідність IP до MAC тощо). Побудована модель

класифікації на основі дерева рішень продемонструвала високу точність і здатність виявляти обидва типи атак.

Запропонований підхід має перевагу над класичними методами, такими як DHCP Snooping, які потребують ручного налаштування та не виявляють атак із підміною MAC-адрес і можуть бути застосовані тільки в мережах з дротовим з'єднанням. Розроблена модель та метод демонструють винятковку надійність, досягаючи 100% точності виявлення DHCP – спуфінгу, що має вирішальне значення для підтримки швидкості реагування мережі. Результати роботи засвідчують ефективність застосування поведінкового аналізу DHCP-сесій у поєднанні з машинним навчанням для виявлення аномалій, що відкриває перспективи впровадження моделі в практичні системи моніторингу та захисту мережевого трафіку.

Ключові слова: *кіберзагрози, атаки на інфраструктуру, штучний інтелект, мережева безпека, DHCP spoofing, IDS аналіз, машинне навчання.*

Вступ. У сучасних комп'ютерних мережах забезпечення безпеки служб автоматичної конфігурації є одним із ключових завдань, особливо з урахуванням широкого використання протоколу DHCP (Dynamic Host Configuration Protocol) для динамічної видачі IP-адрес. У відкритих чи слабко контрольованих мережах (університети, корпоративні Wi-Fi-зони, IoT-середовища) цей протокол часто стає мішенню атак, зокрема DHCP spoofing, які можуть спричинити повну втрату контролю над трафіком користувача [1-3]. Такий тип атак дозволяє зловмиснику видавати себе за легітимний DHCP-сервер, надсилаючи клієнтам підроблені IP-адреси хосту, шлюзу або DNS-серверу, що уможливлює перехоплення, підміну або перенаправлення трафіку, ініціюючи атаку через посередника.

Класичні рішення щодо виявлення або запобігання DHCP spoofing-атакам базуються на механізмах DHCP Snooping, фільтрації портів або ручному визначенні довірених зон у комутаторах [1]. Хоча такі методи досить ефективні в ізольованих або строго контрольованих середовищах, вони мають низку суттєвих обмежень. Зокрема, вони не дозволяють виявляти маскувальні атаки, коли зловмисник використовує IP-адресу легітимного сервера, змінюючи лише MAC-адресу, або діє у VLAN без правильних конфігурацій і можуть бути задіяні тільки в мережах з дротовим з'єднанням [4].

Окрім технічної складності впровадження у великих масштабах, класичні підходи часто не здатні виявити аномальні поведінкові патерни або сценарії, які не були явно передбачені системним адміністратором. Це створює критичну потребу в автоматизованих та адаптивних механізмах виявлення, здатних навчатися на основі структури трафіку, виявляти нетипові шаблони DHCP-повідомлень і відокремлювати нормальні сеанси від потенційно шкідливих.

У цьому контексті надзвичайно актуальними є методи машинного навчання (ML), що дозволяють моделювати поведінку мережевих протоколів на основі реальних даних та виявляти аномалії без необхідності жорстко заданих правил. Дослідження останніх років демонструють високу ефективність ML у сфері аналізу мережевого трафіку, зокрема для задач інтелектуального виявлення атак типу ARP poisoning, DNS spoofing, DoS/DDoS тощо [5-11]. Проте напрям виявлення DHCP spoofing з використанням AI/ML досі залишається недостатньо дослідженим, що визначає наукову новизну цієї роботи.

У межах даного дослідження запропоновано метод виявлення DHCP spoofing-атак на основі моделювання поведінки DHCP-серверів із використанням моделей класифікації. Основу системи становить комбінований набір ознак, що включає аналіз множинних OFFER-відповідей, їх MAC-ідентифікаторів, першого відповідача та кількості унікальних IP-адрес у межах сесії. Побудований синтетичний датасет охоплює як прості, так і складні сценарії атак, що дозволяє моделі виявляти навіть ті випадки, які залишаються непоміченими традиційними методами. Отримані результати підтверджують доцільність та ефективність застосування ML-підходів для задач безпеки DHCP-середовищ.

Мета роботи полягає у підвищенні безпеки виявлення атак на DHCP з використанням методів штучного інтелекту для аналізу мережевого трафіку в режимі реального часу, що включає автоматичне виявлення як класичних spoofing-атак із фальшивими IP-адресами, так і складніших сценаріїв з підміною MAC-ідентифікаторів, шляхом побудови поведінкової моделі на базі машинного навчання.

1. Протокол DHCP та його вразливості. DHCP (Dynamic Host Configuration Protocol) – це мережевий протокол, який автоматично надає пристроям у мережі необхідні налаштування для підключення до неї. Цей протокол дозволяє централізовано керувати конфігурацією мережевих пристроїв без необхідності вручну налаштовувати кожен з них. DHCP відносить до прикладного рівня моделі OSI і використовується в більшості великих мереж TCP/IP [1].

DHCP spoofing (DHCP-атака) – це тип атаки на мережу, в якій зловмисник намагається підробити DHCP-сервер для того, щоб маніпулювати процесом надання IP-адрес або інших налаштувань мережі клієнтам.

До основних функцій DHCP можна віднести [12]:

- автоматичне призначення IP-адрес: DHCP надає пристроям, що підключаються до мережі, унікальну IP-адресу з попередньо визначеного діапазону (пул IP-адрес);
- конфігурація інших параметрів мережі:
  - маска підмережі (Subnet Mask);
  - основний шлюз (Gateway) – IP-адреса пристрою, через який трафік виходить за межі локальної мережі;

- DNS-сервери – сервери для перетворення доменних імен у IP-адреси;
- часове обмеження (Lease Time) – період, на який пристрій отримує IP-адресу, після чого може бути вимушене оновити свою конфігурацію.

На рис. 1 показаний типовий обмін повідомленнями між хостом і DHCP-сервером при запиті мережевих налаштувань.

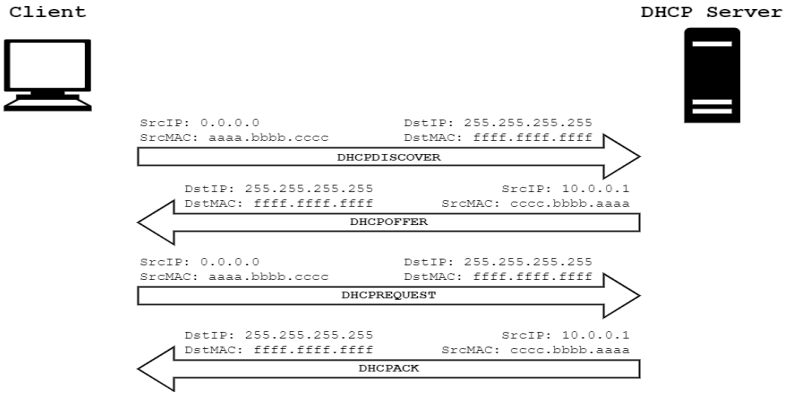

Рис. 1. *Мережеві повідомлення між DHCP-сервером і DHCP-клієнтом*

Основними учасниками обміну повідомленнями за протоколом DHCP є:

DHCP-сервер – це пристрій (як правило, маршрутизатор або окремий сервер), який надає налаштування пристроям у мережі;

DHCP-клієнт – це пристрій (наприклад, комп'ютер, смартфон або принтер), який запитує ці налаштування для підключення до мережі.

Трафік між DHCP-сервером і DHCP-клієнтом можна розділити на окремі повідомлення.

DHCP Discover (запит на пошук DHCP-серверів): коли клієнт приєднується до мережі (наприклад, вмикається новий комп'ютер), він посилає широкомовний DHCP Discover запит, щоб знайти доступні DHCP-сервери.

DHCP Offer (пропозиція IP-адреси та інших налаштувань): DHCP-сервери, що отримали запит, відповідають DHCP Offer. У цьому повідомленні вказано:

- призначена IP-адреса;
- інші мережеві налаштування (маска підмережі, шлюз тощо);
- часове обмеження (час оренди адреси).

DHCP Request (запит на отримання налаштувань): клієнт вибирає одну з отриманих пропозицій (як правило, першу) і посилає сер-

веру DHCP Request, підтверджуючи свій вибір і вказуючи серверу, що він хоче отримати вказану адресу.

DHCP Acknowledgment (DHCPPACK-підтвердження налаштувань): після отримання запиту DHCP-сервер надсилає клієнту DHCP Acknowledgment (підтвердження), яке містить остаточні налаштування (IP-адреса, шлюз, DNS і т.д.). Клієнт отримує адресу на визначений час, після чого, якщо пристрій ще підключений до мережі, він повинен продовжити оренду адреси, відправивши запит на продовження оренди (DHCP Request) до закінчення часу оренди.

DHCP NAK – відмова, якщо IP-адреса або налаштування вже недійсні.

DHCP Release – повідомлення про звільнення IP-адреси.

Приклад трафіку, який виникає при запиті клієнтом нових мережевих налаштувань показаний на рис. 2, який отриманий при застосуванні популярного інструменту Wireshark, призначеного для аналізу мережевого трафіку, який дозволяє детально досліджувати пакети даних у режимі реального часу або збережених у форматі PCAP [13].

Time	Source	Destination	Protocol	Length	Info
2024-12-20 16:29:04,468396	192.168.31.51	192.168.31.1	DHCP	342	DHCP Release - Transaction ID 0x1d8685eb
2024-12-20 16:30:12,367231	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xd78c0bc4
2024-12-20 16:30:12,369835	192.168.31.1	255.255.255.255	DHCP	373	DHCP Offer - Transaction ID 0xd78c0bc4
2024-12-20 16:30:12,370883	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xd78c0bc4
2024-12-20 16:30:12,373443	192.168.31.1	255.255.255.255	DHCP	393	DHCP ACK - Transaction ID 0xd78c0bc4
2024-12-20 16:31:16,758219	192.168.31.51	192.168.31.1	DHCP	342	DHCP Release - Transaction ID 0xd50db018
2024-12-20 16:31:42,327523	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0x16da55b8
2024-12-20 16:31:42,330095	192.168.31.1	255.255.255.255	DHCP	373	DHCP Offer - Transaction ID 0x16da55b8
2024-12-20 16:31:42,330962	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x16da55b8
2024-12-20 16:31:42,333950	192.168.31.1	255.255.255.255	DHCP	393	DHCP ACK - Transaction ID 0x16da55b8

Рис. 2. *Приклад мережевого трафік між DHCP-сервером і DHCP-клієнтом*

На рис. 3-5 показаний вміст повідомлень DHCP Offer, Request, ACK між DHCP-сервером і DHCP-клієнтом.

```
> Frame 710: 373 bytes on wire (2984 bits), 373 bytes captured (2984 bits)
> Ethernet II, Src: 28:d1:27:8d:13:f2, Dst: ff:ff:ff:ff:ff:ff
> Internet Protocol Version 4, Src: 192.168.31.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x65dd7baf
    Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.31.51
    Next server IP address: 192.168.31.1
    Relay agent IP address: 0.0.0.0
    Client MAC address: 00:e0:4c:36:40:18
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (192.168.31.1)
  > Option: (51) IP Address Lease Time
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (28) Broadcast Address (192.168.31.255)
  > Option: (3) Router
```

Рис. 3. *Мережевий трафік між DHCP-сервером і DHCP-клієнтом (повідомлення DHCP Offer)*

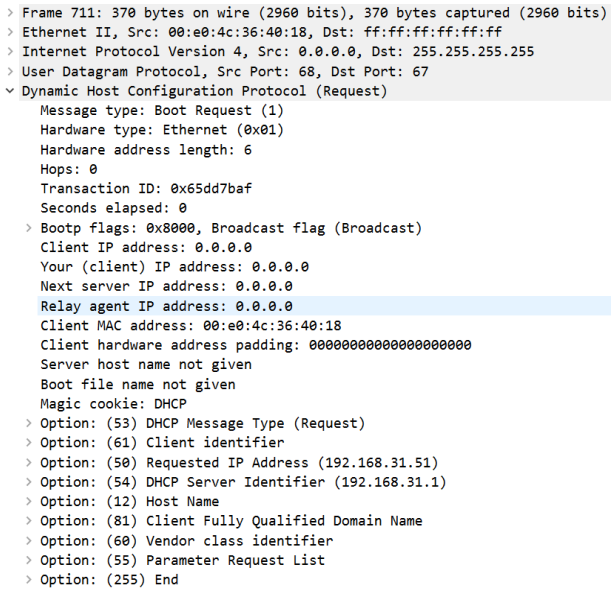

Рис. 4. *Вміст повідомлення DHCP Request, яке надіслав клієнт до DHCP сервера*

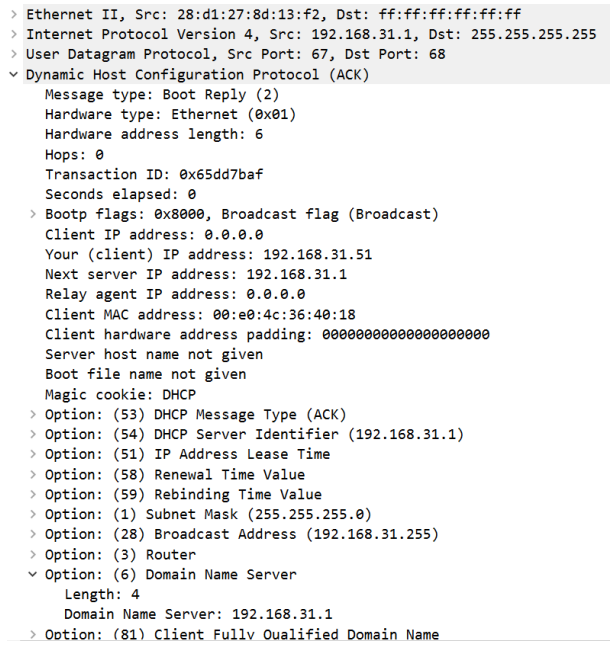

Рис. 5. *Вміст повідомлення DHCP ACK, яке надіслав DHCP сервер*

2. Мережева атака типу DHCP SPOOF. З аналізу трафіку (рис. 2-5), який виникає в процесі обміну повідомленнями між DHCP-клієнтом і DHCP-сервером видно, що клієнт не володіє інформацією про правдиві параметри DHCP-сервера (тому використовує широкомовні адреси мережевого (255.255.255.255) і канального (FF:FF:FF:FF:FF:FF) рівнів, щоб виявити сервери DHCP. В IP-заголовку в полі адреси джерела IP-пакета вказується 0.0.0.0, оскільки клієнт ще не отримав цей параметр. У полі джерела повідомлення на канальному рівні вказується MAC-адреса клієнта (рис.6).

```
> Frame 709: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) o
v Ethernet II, Src: 00:e0:4c:36:40:18, Dst: ff:ff:ff:ff:ff:ff
  > Destination: ff:ff:ff:ff:ff:ff
  > Source: 00:e0:4c:36:40:18
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 330
    Identification: 0x5910 (22800)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
```

Рис. 6. *Широкомовний трафік від клієнта, який містить запит мережевих налаштувань (DHCP Discover)*

Оскільки це повідомлення є широкомовним кадром, комутатор передаватиме повідомлення на всі інтерфейси, тобто одна копія надсилається на правдивий DHCP-сервер, а інша – на фальшивий DHCP-сервер (рис. 7) [14].

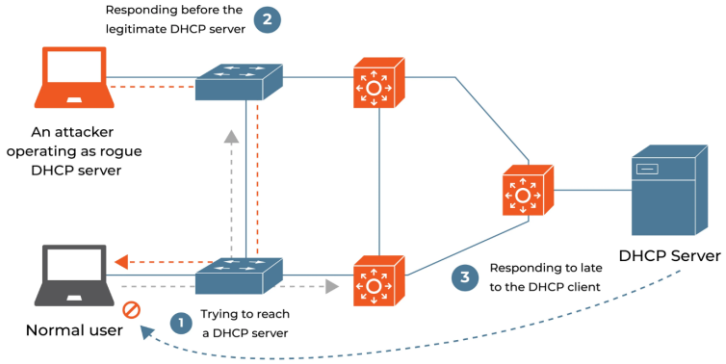

Рис. 7. *Передача широкомовних запитів DHCP-клієнтом*

При отриманні повідомлення DHCPDISCOVER від потенційного клієнта, DHCP-сервер пропонує вільну IP-адресу. Це повідомлення, адресоване від сервера клієнту, називається DHCPOFFER. На час пропозиції адреса резервується DHCP-сервером і не пропонується

іншим клієнтам. Якщо підроблений DHCP сервер зловмисника відповість першим, то весь зв'язок DHCP продовжуватиметься лише з цим сервером, а повідомлення про пропозицію DHCP від законного сервера DHCP буде відхилено.

Припустимо, клієнт отримав повідомлення DHCPOFFER від DHCP-сервера. Тоді він відправляє широкомовне повідомлення DHCPREQUEST, в якому міститься IP-адреса сервера, що видав пропозицію. Таке широкомовне повідомлення інформує інші DHCP-сервери про те, що клієнт вже прийняв пропозицію від одного з серверів. У такому випадку інші сервери DHCP звільняють зарезервовані IP-адреси, і в подальшому вони можуть бути запропоновані іншим клієнтам.

Коли сервер отримує повідомлення DHCPREQUEST, він вказує обрану клієнтом IP-адресу в поєднанні DHCPACK і відсилає його в сторону клієнта. Після цього клієнт фіксує отримані налаштування і використовує їх при мережевому обміні пакетами.

Внаслідок того що протокол DHCP не має вбудованої перевірки автентичності це може викликати атаки, такі як DHCP-спуфінг [3, 4, 10], коли зловмисник підміняє сервер для надсилання підроблених повідомлень DHCP з метою перенаправлення трафіку хостів до шкідливих серверів DHCP, контрольованих зловмисником. Це може призвести до того, що хости не зможуть підключитися до мережі або будуть перенаправлені на шкідливі веб-сайти для подальших атак. Наприклад, комбінована з DHCP-спуфінг атака, яка спрямована на підробку DNS-записів в зонах Active Directory Integrated DNS (ADIDNS) [15]. У результаті зловмисник може здійснити атаку типу «людина посередині», призначивши себе шлюзом за замовчуванням або сервером DNS у відповідях DHCP, які надсилаються клієнтам DHCP. Це дозволяє зловмиснику перехопити IP-зв'язок між налаштованими клієнтами та рештою мережі.

Важливим для виконання атаки DHCP SPOOF є виявлення активних DHCP серверів в мережі. Визначити активні DHCP-сервери в мережі реалізується зазвичай тим, що зловмисник може надіслати широкомовне повідомлення DHCP Discover і перевірити відповіді на пропозиції від серверів.

Щоб надсилати повідомлення DHCP, можна запустити утиліту dhclient Linux – настроюваний клієнт DHCP, який дозволяє взаємодіяти з серверами DHCP. Якщо проаналізувати трафік і перевірити повідомлення DHCP Offer, то можна ідентифікувати всі активні сервери DHCP (рис. 8).

	Time	Source	Destination	Protocol	Length	Info
1	0.0000…	0.0.0.0	255.255.255.255	DHCP	290	DHCP Discover
2	0.0114…	172.25.14.123	255.255.255.255	DHCP	342	DHCP Offer
3	0.0121…	172.25.14.101	255.255.255.255	DHCP	342	DHCP Offer

Рис. 8. *Надсилання DHCP Discover для визначення активних серверів DHCP у мережі*

3. Рішення для захисту від атаки DHCP SPOOF. Існує два рішення для захисту від атаки спуфінгу DHCP. Перше рішення – налаштувати IP-інформацію вручну на всіх кінцевих точках мережі, що буде майже неможливо у великих середовищах. Друге рішення полягає в застосуванні функції відстеження DHCP на комутаторах.

Відстеження DHCP – це функція безпеки рівня 2, яку можна застосувати на комутаторі, щоб певною мірою запобігти підробці DHCP і атаці голодування DHCP. Основна ідея цієї функції полягає в тому, щоб комутатор міг створювати та підтримувати таблицю прив'язки DHCP Snooping.

Кожен запис у цій базі даних міститиме інформацію про всі інтерфейси комутатора та MAC- та IP-адреси клієнта, доступні на них, а також додаткову інформацію, таку як асоціація VLAN, ідентифікатор порту тощо.

Після того, як інтерфейси налаштовані як довірені або ненадійні, комутатор відфільтровує повідомлення DHCP і дозволяє або забороняє їх на основі записів даних у таблиці зв'язування відстеження DHCP.

Попри наявність базових механізмів захисту від DHCP spoofing, традиційні підходи мають істотні обмеження у масштабованості та гнучкості. Зокрема, ручне налаштування IP-параметрів на кожному кінцевому пристрої є вкрай трудомістким і практично нездійсненним у великих або динамічних мережах із сотнями чи тисячами хостів. Використання механізму DHCP Snooping на комутаторах дійсно дозволяє обмежити доступ ненадійних клієнтів до DHCP-трафіку, але ефективність цього методу напряму залежить від типу середовища(може бути задіяні тільки в мережах з дротовим з'єднанням), правильності та повноти конфігурації, а також від довіри до інфраструктури доступу, що не завжди гарантовано.

Крім того, відстеження DHCP є пасивним захистом, який не здійснює глибокого аналізу вмісту трафіку та не враховує поведінкових ознак, що можуть свідчити про складні або замасковані атаки. Така система не виявляє, наприклад, ситуацій, коли зловмисник використовує справжню IP-адресу сервера, але підмінює MAC-адресу – що дозволяє обійти перевірки на рівні IP. Ці недоліки створюють передумови для впровадження більш гнучкого та адаптивного підходу на основі методів машинного навчання, здатного виявляти аномалії в поведінці DHCP-сесій на основі реального трафіку, навіть за відсутності попередньо заданих правил.

4. Архітектура запропонованої моделі ML для аналізу DHCP SPOOF атак в реальному часі. В роботі пропонуються спеціалізовані програмні рішення, які базуються на застосуванні моделей машинного навчання, які своєчасно класифікують і виділяють DHCP

SPOOF атаки. Розробка та застосування таких моделей *ML дозволяє автоматизувати аналіз* мережевого трафіка та підвищити безпеку комп'ютерних мереж. Запропоноване рішення може працювати в режимі моніторингу широкомовного DHCP трафіку і сигналізувати про виявлення не законного DHCP-сервера.

Як вже зазначалося, одним із найбільш очевидних випадків DHCP-атаки є ситуація, коли в мережі, крім легітимного DHCP-сервера (10.0.0.1), з'являється інший сервер із *іншою IP-адресою* (10.0.0.95). Такий сервер, часто працюючи на рівні користувача або фізичного пристрою, перехоплює запити *DHCP Discover* і відповідає *DHCP Offer* раніше за легітимний сервер. Якщо клієнт приймає цю відповідь, він отримає IP-адресу від зловмисника, а також змінені маршрути або DNS-сервери. Для виявлення такого роду атак можна аналізувати множинні відповіді на DHCP Discover з різних IP-адрес, що не відповідають дозволеним DHCP-серверам (рис. 9).

0.0.0.0	255.255.255.255	DHCP	286 DHCP Discover
10.0.0.95	255.255.255.255	DHCP	310 DHCP Offer
10.0.0.1	255.255.255.255	DHCP	310 DHCP Offer
0.0.0.0	255.255.255.255	DHCP	298 DHCP Request
10.0.0.95	255.255.255.255	DHCP	310 DHCP ACK

Рис. 9. *Ілюстрація множинної відповіді DHCP Offer від легітимного та атакуючого сервера з різними IP-адресами*

Більш витонченою і небезпечною є атака, при якій зловмисник *імітує IP-адресу справжнього DHCP-сервера* (10.0.0.1), залишаючи у полях DHCP-повідомлень правильне значення *server_id*, але використовуючи *фальшиву MAC-адресу* як джерело повідомлення (рис. 10).

0.0.0.0	255.255.255.255	DHCP	286 DHCP Discover
10.0.0.1	255.255.255.255	DHCP	310 DHCP Offer
10.0.0.1	255.255.255.255	DHCP	310 DHCP Offer
0.0.0.0	255.255.255.255	DHCP	298 DHCP Request
10.0.0.1	255.255.255.255	DHCP	310 DHCP ACK

Рис. 10. *Ілюстрація множинної відповіді DHCP Offer від легітимного та атакуючого сервера з однаковими IP-адресами*

У такому випадку класичні методи захисту, які перевіряють лише IP-адресу сервера, можуть бути неефективними, адже трафік виглядає легітимним. Для виявлення таких атак необхідно враховувати не лише IP-поля, а й апаратні адреси відправників у DHCP-пакетах типу Offer.

Таким чином, постає задача виявлення DHCP spoofing-атак двох типів: *прості атаки з несанкціонованими IP та маскувальні атаки з підміною MAC-адреси при справжньому IP.* Оскільки класичні методи захисту (наприклад, DHCP Snooping) можуть не покривати обидва сценарії водночас, актуальним є підхід, який поєднує аналіз IP, MAC та поведінкових патернів відповіді DHCP-серверів. Завдання полягає у створенні узагальненої моделі ML, здатної ідентифікувати ознаки аномального DHCP-трафіку незалежно від конкретного сценарію атаки.

Для реалізації системи виявлення DHCP spoofing-атак запропоновано метод ML, що базується на створеному трафіку, який моделює як нормальні DHCP-сеанси, так і різні типи атак. Було розроблено генератор DHCP-пакетів, що дозволяє створювати сценарії з одним або кількома відповідями DHCP Offer на один запит DHCP Discover. У випадку нормальної сесії лише легітимний сервер (з фіксованою IP- та MAC-адресою) відповідає клієнту. Для моделювання атаки використовуються два підходи: відповіді з фейкових IP-адрес (*спрощений spoofing*) та відповіді зі справжньої IP-адреси, але фальшивою MAC-адресою (*маскування*).

Побудова простого методу машинного навчання для виявлення DHCP SPOOF атак в реальному часі на локальному комп'ютері або мережі має свої переваги порівняно з застосуванням спеціалізованих контролерів та ручних налаштувань. До таких переваг можна віднести:

- простота і швидкість впровадження;
- незалежність від інфраструктури;
- гнучкість і адаптивність;
- ефективність в розподілених середовищах.

У той час, як ручне налаштування безпеки може надавати розширені можливості управління та моніторингу мережі, їх впровадження і підтримка можуть бути витратними і складними. Отже, побудова простого та ефективного методу машинного навчання для виявлення DHCP SPOOF атак може бути доступним рішенням для забезпечення необхідного рівня безпеки мережі без значних інвестицій.

В роботі пропонуються спеціалізовані програмні рішення на мові Python, які базуються на застосуванні моделей машинного навчання, які своєчасно класифікують і виділяють DHCP SPOOF атаки та створюють керуючі сигнали для оповіщення, що сприяє підвищенню безпеки комп'ютерних мереж. Для розробки та застосуванні таких моделей *ML пропонується проводити аналіз* мережевого трафіка в реальному часі використовуючи дані платформи *Wireshark*, хоча джерелом інформації про трафік може виступати і інша платформа.

На рис. 11 наведена загальна структура підготовки даних для побудови моделі ML. Попередня обробка даних є важливою процедурою для забезпечення якості та надійності результатів аналізу даних і роботи моделей машинного навчання. Добре оброблені дані допомагають покращити точність та інтерпретованість моделей, а також зменшити можливість виникнення помилок під час аналізу. Для отримання моделі ML, яка буде завантажуватися і використовуватися для аналізу даних в реальному часі, потрібно виконати декілька підготовчих етапів.

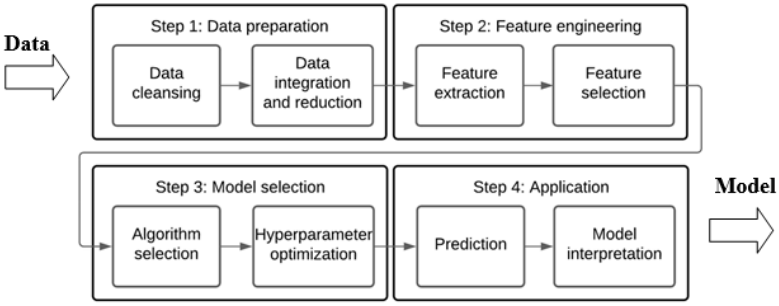

Рис. 11. *Узагальнена структура підготовки даних для синтезу моделі ML*

Підготовка даних (Step 1). Це перший крок, де данні (Data) можуть збиратися з різних джерел, зокрема з платформи *Wireshark.* На основі збереженого трафіку у форматі.CSV формується DataFrame. На цьому етапі відбувається очищення даних (Data Cleaning), видаляються або коригуються неправильні, відсутні або непотрібні дані (Missing value), відбувається фільтрація DHCP -пакетів і залишаються тільки ті, які належать до протоколу DHCP.

Конструювання ознак (Step 2). На цьому етапі відбувається вилучення зайвих ознак (*Feature Extraction*) і виділення необхідних (*Feature Selection*), в тому числі можуть створюватися нові. Якщо датасет містить багато ознак, які не є важливими для аналізу або моделювання, вони можуть бути видалені, щоб спростити аналіз, зменшити розмірність та обчислювальні витрати. Даний етап реалізується різноманітними методами аналізу даних, в тому числі кореляційними підходами.

Вибір і підготовка моделі (Step 3). На цьому етапі відбувається кодування категоріальних ознак (*Encoding Categorical Features*) для переведення їх в числовий формат, масштабування ознак (*Feature Scaling*) для забезпечення однакового діапазону значень і покращення швидкості навчання моделей. Окрім того, на цьому етапі відбувається вибір алгоритму (класифікатора) для побудови моделі та визначення оптимальних гіперпараметрів.

Останній етап (Step 4) призначений для формування моделі ML, збереження цієї моделі або декількох в залежності від потреб аналізу атак. Отримані моделі використовуються для прогнозування різноманітних атак, на які вони були налаштовані та навчанні.

Згенерований трафік зберігається у форматі. PCAP, після чого обробляється інструментом, який витягує ключові ознаки для кожної DHCP-сесії. Зокрема, фіксуються усі IP-адреси серверів, які надіслали DHCP Offer, MAC-адреси відповідних джерел, адреса сервера, якого клієнт зрештою обрав (r*equest_server_ip*), та MAC першого відповідача (*first_offer_mac*). Ці дані агрегуються у форматі CSV, що

дозволяє подальшу машинну обробку та побудову моделі виявлення аномалій. Отриманий датасет має структуру, представлену на рис. 12.

	xid	offer_ips	offer_macs	first_offer_mac	request_server_ip	label
0	453525	['10.0.0.1']	['aa:bb:cc:dd:ee:01']	aa:bb:cc:dd:ee:01	10.0.0.1	normal
1	288430	['10.0.0.1']	['aa:bb:cc:dd:ee:01']	aa:bb:cc:dd:ee:01	10.0.0.1	normal
2	867043	['10.0.0.1']	['aa:bb:cc:dd:ee:01']	aa:bb:cc:dd:ee:01	10.0.0.1	normal
3	142946	['10.0.0.90', '10.0.0.1']	['aa:bb:cc:dd:ee:fa', 'aa:bb:cc:dd:ee:01']	aa:bb:cc:dd:ee:fa	10.0.0.90	spoofed
4	989267	['10.0.0.1']	['aa:bb:cc:dd:ee:01']	aa:bb:cc:dd:ee:01	10.0.0.1	normal
5	745001	['10.0.0.1']	['aa:bb:cc:dd:ee:01']	aa:bb:cc:dd:ee:01	10.0.0.1	normal
6	826507	['10.0.0.1', '10.0.0.1']	['aa:bb:cc:dd:ee:fa', 'aa:bb:cc:dd:ee:01']	aa:bb:cc:dd:ee:fa	10.0.0.1	spoofed
7	762676	['10.0.0.90', '10.0.0.1']	['aa:bb:cc:dd:ee:fa', 'aa:bb:cc:dd:ee:01']	aa:bb:cc:dd:ee:fa	10.0.0.90	spoofed
8	784662	['10.0.0.1', '10.0.0.1']	['aa:bb:cc:dd:ee:fa', 'aa:bb:cc:dd:ee:01']	aa:bb:cc:dd:ee:fa	10.0.0.1	spoofed
9	358428	['10.0.0.1']	['aa:bb:cc:dd:ee:01']	aa:bb:cc:dd:ee:01	10.0.0.1	normal

Рис. 12. *Представлення датасета для отримання моделі ML аналізу DHCP Snooping*

На рис. 12 представлені наступні позначення:

- *offer_ips* – всі IP-адреси OFFER-повідомлень у порядку надходження;
- *offer_macs* – MAC-адреси серверів, хто надіслав OFFER;
- *first_offer_mac* – MAC-адреса першого відповідача;
- *request_server_ip* – IP-адреса, яку обрав клієнт;
- l*abel* – мітка про нормальний ('*normal*') або аномальний ('*spoofed*') трафік.

Основна гіпотеза моделі полягає в тому, що у звичайному середовищі відповіді DHCP Offer повинні надходити лише від авторизованих серверів з відомими IP- та MAC-адресами. Всі відхилення – наявність кількох різних IP, різних MAC-адрес при однаковому IP, або перші відповіді від несанкціонованих адрес – класифікуються як потенційно шкідливі. Таке представлення дозволяє не тільки виявляти класичні spoofing-атаки, а й складніші варіанти маскування, які можуть обходити традиційні механізми на основі IP-фільтрації.

Запропонований підхід забезпечує гнучкість у виявленні DHCP spoofing у широкому спектрі варіацій атак та може бути легко адаптований до реальних мережевих середовищ. На відміну від статичних правил, модель дозволяє враховувати контекст – наприклад, послідовність відповідей, множинність джерел або невідповідність MAC-адрес. Це створює підґрунтя для інтеграції моделі в системи виявлення аномалій, засновані на машинному навчанні, що у перспективі підвищує рівень захищеності мережевої інфраструктури.

5. Результати дослідження та обговорення. Система *автоматизованої підтримки ML моделі* складається з застосування декількох нових методів.

1. **Метод перетворення**. *pcap* файлів з платформи *Wireshark* у табличний формат.*csv* в режимі реального часу за наступним алгоритмом:

- підготовка середовища – визначення шляхи до папок з вхідними. *pcap* та вихідними *.csv* файлами;
- визначається файл.csv, який буде виключено з обробки у разі відсутності у трафіку з DHCP пакетів;
- аналіз пакетів – функція читає вхідний *.pcap* файл та аналізує пакети для виявлення різних типів протоколів (Ethernet, ARP, IP, DHCP);
- збирання інформації про кожен пакет (джерело, призначення, тип протоколу, довжина та інші деталі);
- запис зібраної інформацію у вихідний *.csv* файл.

Основні операції даного методу полягають у:

- отриманні списку всіх *.pcap* файлів з вхідними файлами;
- визначення не оброблених файлів;
- перевірка папки на наявність нових файлів, які з'являються автоматично;
- для кожного нового файлу *.pcap,* який з'являється, викликається функція обробки та збереження результатів у.*csv* файл;
- додавання оброблених файлів до списку для уникнення повторної обробки;
- видалення файлів після їх обробки для уникнення перевантаження пам'яті.

2. **Метод обробки DataFrame**.*csv* файла і формування заданих фітчів (ознак) для застосування підготовленої моделі ML, який полягає в наступному.

Для отримання моделей ML вхідні дані мережевого трафіка (*Network Traffic*) утворюють Dataset, який підлягає попередній обробці (*Preprocessing*) згідно загальної структури на рис.11.

Після формування структурованого датасету у форматі CSV для кожної DHCP-сесії було виділено набір ключових ознак (*features*), що забезпечують максимальну інформативність з точки зору виявлення атак. До таких ознак належать: кількість DHCP Offer у межах однієї сесії, список IP-адрес серверів, що відповіли, список MAC-адрес, що надіслали відповіді, а також MAC-адреса першого відповідача (*first_offer_mac*) і IP-адреса, до якої звернувся клієнт (*request_server_ip*). Основним критерієм при побудові ознак було те, що атаки на DHCP характеризуються аномаліями у кількості та джерелах відповідей, а також у їхній послідовності.

Для кожної сесії було сформовано вектор ознак, включаючи кількість унікальних IP (*n_unique_ips*), кількість унікальних MAC (*n_unique_macs*), логічний прапорець *first_offer_legit*, що вказує, чи

першим відповів легітимний сервер, та ознаку *ip_has_multiple_macs*, яка сигналізує про маскування. Всі категоріальні значення (наприклад, MAC-адреси) були закодовані або у вигляді бінарних прапорців, або числових індексів. Після векторизації ознак набір даних було розділено на тренувальну (*X_train, y_train*) – 70%, та тестову вибірки (*X_test, y_test*) – 30%.

Модель навчається розпізнавати з врахуванням наступних логічних правил:

- *якщо n_unique_ips* > *n* → підозра на spoofing, де *n* – кількість легітимних DHCP серверів;
- якщо *first_offer_legit == 0* → зловмисник відповів першим;
- якщо *під однією IP є кілька MAC* → класична ознака маскування.

Модель дуже ефективна при роботі з датасетом, що містить як прості, так і складні атаки, і добре узагальнює правила без потреби ручного налаштування кожного варіанту атаки.

Для побудови класифікатора було використано базову модель *DecisionTreeClassifier*, що добре підходить для інтерпретованих задач без необхідності складної обробки ознак. Модель навчалась на маркованих даних загальним обсягом 1000 записів при вкладення двох типів атак загальною чисельність 10 кожного типу. Кожна сесія мала мітку label, як «*normal*» або «*spoofed*», визначену на основі правил виявлення атаки (наявність фейкових IP або MAC). Після навчання модель була протестована на незалежній вибірці для оцінки здатності виявляти як прості, так і маскувальні атаки.

3. **Аналіз трафіка в режимі онлайн** із застосуванням запропонованої моделі ML:

- зчитування даних з.*csv* файлу і додавання додаткових даних з підготовленого файлу на той випадок, якщо у поточній сесії відсутній DHCP протокол для нормального функціонування моделі ML;
- завантаження підготовленої моделі ML для класифікації трафіка для кожного окремого підготовленого *.csv* файлу;
- виводяться кількісні характеристики аномального трафіку на екран з подачею звукового повідомлення чи передачею інформації на електронну пошту (при потребі).

У процесі тестування було використано класичні метрики *accuracy, precision, recall* та *f1-score*, з особливою увагою до класу *spoofed*, оскільки саме атаки є цільовими для виявлення (рис. 13).

Всі показники ефективності на тестовому наборі показали максимальний результат – *1.0*, тобто сто відсоткову відповідність. Така характеристика, як *Confusion Matrix* дає чітке уявлення про помилки моделі і показує, наскільки добре модель класифікує трафік для кожного класу. У нашому випадку модель класифікує DHCP-сесії як:

- **normal** (нормальні);
- **spoofed** (з атакою).

```
=== Confusion Matrix ===
[[300   0]
 [  0   6]]

=== Classification Report ===
              precision    recall  f1-score   support

      normal       1.00      1.00      1.00       300
     spoofed       1.00      1.00      1.00         6

    accuracy                           1.00       306
   macro avg       1.00      1.00      1.00       306
weighted avg       1.00      1.00      1.00       306
```

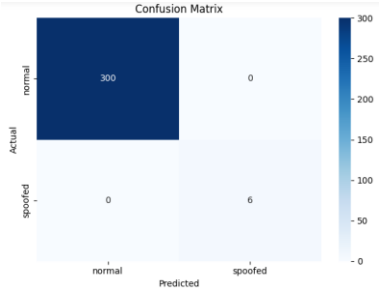

***Рис. 13**. Результат оцінювання якості запропонованої моделі виявлення DHCP атак*

Для бінарної класифікації *Confusion Matrix* має наступну структуру, де фігурують наступні позначення:

	Predicted Normal	Predicted Spoofed
Actual Normal	TN = True Negative	FP = False Positive
Actual Spoofed	FN = False Negative	TP = True Positive

TP (True Positive) – модель вірно виявила атаку (атакуючий трафік «spoofed» було передбачено як «spoofed»);

TN (True Negative) – модель вірно виявила нормальний трафік (справжнє «normal», передбачено «normal»);

FP (False Positive) – хибне спрацювання **(**нормальний трафік «normal» визначено як атакуючий «spoofed»);

FN (False Negative) – пропущена атака **(**атакуючий трафік «spoofed» визначено нормальний «normal»).

Задачею добре натренованої моделі є:

- максимізувати **TP** – для виявлення якомога більше атак;
- мінімізувати **FN** – тому що пропущені атаки є критично небезпечними;
- контролювати **FP –** хибні спрацювання можуть знизити довіру до моделі;
- контролювати **TN –** не варто надмірно оптимізувати під «normal», якщо це шкодить «spoofed».

Основні метрики оцінювання ефективності моделі виражаються наступними виразами:

$$Accuracyy = \frac{TP + TN}{Total},\ \Pr ecision = \frac{TP}{TP + FP},\ \mathrm{Re}call = \frac{TP}{TP + FN}.$$

На практиці найчастіше використовують не самі ці величини, а так звані оцінки *f1* – це гармонічне середнє значення влучності та повноти. Це метрика, яка дає оцінку точності моделі, оскільки вона враховує наскільки модель робить правдиві прогнози, які насправді є істинними, так і скільки загальних правдивих прогнозів, які модель правильно передбачила:

$$f1 = \frac{2 * \Pr ecision * \mathrm{Re}\, call}{\Pr ecision + \mathrm{Re}\, cal}.$$

Розроблена модель та метод на основі *DecisionTreeClassifier* демонструють виняткову надійність, досягаючи 100% точності виявлення DHCP – спуфінгу, що має вирішальне значення для підтримки швидкості реагування мережі.

Запропонований класифікатор *DecisionTreeClassifier* було обрано для побудови моделі через його здатність інтерпретувати складні логічні залежності між ознаками без необхідності масштабування даних. У контексті виявлення DHCP spoofing-атак, цей алгоритм виявився особливо ефективним завдяки своїй здатності автоматично будувати гілки прийняття рішень на основі чітких ознак, таких як кількість унікальних IP-адрес, відповідність MAC-адреси першого OFFER тощо. Саме детермінована структура дерева дозволила моделі точно і швидко розрізняти нормальні та аномальні сесії, зберігаючи високу точність і простоту подальшої інтерпретації результатів, що є важливим фактором для практичного впровадження в системах безпеки.

Висновки. Проблема захисту протоколу DHCP від атак типу spoofing залишається актуальною через відсутність вбудованих механізмів аутентифікації в його базовій реалізації. Як показано в роботі, зловмисник може надсилати клієнтам підроблені DHCP Offer, видаючи себе за легітимний сервер. Це призводить до можливості перехоплення або перенаправлення трафіку, порушення конфігурації мережі або навіть відмови в обслуговуванні. Традиційні підходи, зокрема технологія DHCP Snooping, передбачають ручне налаштування списку дозволених портів або IP-адрес, що створює обмеження для масштабованості й адаптивності до складних атак.

Запропонований у дослідженні підхід ґрунтується на розробці методу машинного навчання для автоматизованого виявлення аномалій у поведінці DHCP-серверів. Проведено моделювання комбінованого датасету, який охоплює як типові атаки з підміною IP-адреси, так і витончені сценарії маскування, де зловмисник використовує справжні IP-адреси легітимних DHCP серверів, але з фальшивою MAC-адресою. Створено набір ознак, який дозволяє моделі ML розпізнавати ключові аномалії: кількість відповідей DHCP Offer, перший MAC-відповідач, кількість унікальних IP/MAC-адрес у межах сесії та наявність співвідношень «одна IP – кілька MAC».

Побудована модель класифікації на основі дерева рішень *DecisionTreeClassifier* продемонструвала високу ефективність у виявленні обох типів атак. Розроблена модель та метод демонструють виняткову надійність, досягаючи 100% точності виявлення DHCP – спуфінгу, що має вирішальне значення для підтримки швидкості реагування мережі. Особливо важливо, що модель виявляє навіть ті атаки, які залишаються невидимими для стандартного DHCP Snooping – зокрема, ситуації з підміною MAC-адреси при справжньому IP. При цьому підхід не потребує фіксованого списку дозволених IP або портів, а виявлення базується на поведінковому аналізі DHCP-сесій, що значно підвищує гнучкість і масштабованість системи.

У порівнянні з класичними методами, які здебільшого статичні та орієнтовані лише на IP-контроль, машинно-навчальний підхід виявився значно точнішим і більш адаптивним до нових типів атак. Це дозволяє рекомендувати інтеграцію такого підходу в системи виявлення вторгнень (IDS) як додатковий або навіть основний механізм контролю DHCP-трафіку. З урахуванням динамічного характеру сучасних мереж, запропоноване рішення демонструє потенціал для впровадження у практичні системи кіберзахисту на рівні підприємств, навчальних закладів або операторів зв'язку.

Список використаних джерел:

1. Блозва А. І., Матус Ю. В., Смолій В. В. та ін. Комп’ютерні мережі: [навчальний посібник]. Київ: Компрінт, 2017. 821 с.
2. Lilaram H., Talpur S., Murtaza A., Syed S., Khuhawar F. Detection Of Server-Side DHCP DoS And Spoofing Attack Using Machine Learning Techniques. *Conference: 3rd International Conference on Computational Sciences and Technologies (INCCST'22).* ISBN 978-969-23372-2-9.
3. Osama S., Younes. A Secure DHCP Protocol to Mitigate LAN Attacks. *Journal of Computer and Communications.* 2016. Vol. 4 № 1. DOI: 10.4236/jcc.2016.41005.
4. Khaled E. Controlling Attacks of Rogue Dynamic Host Configuration Protocol (DHCP) to Improve Pedagogical Activities in Mobile Collaborative Learning (MCL) Environment. *Journal of Communications and Computer Engineering*. 2013. Vol. 3. № 1. P. 15-29. URL: https://doi.org/10.20454/JCCE.2013.426.
5. Talukder M. A., Islam M. M., Uddin M. A. et al. Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. *J Big Data*. 2024. Vol. 33. URL: https://doi.org/10.1186/s40537-024-00886-w.
6. Schmitt M. Securing the digital world: protecting smart infrastructures and digital industries with artificial intelligence (ai)-enabled malware and intrusion detection. *J Ind Inf Integr.* 2023. Vol. 36 (100):520.
7. Xu Y., Sun H., Xiang F., Sun Z. Efficient ddos detection based on K-FKNN in software defined networks IEEE Access. 2019. Vol. 7. P. 160536-160545, DOI: 10.1109/ACCESS.2019.2950945.

8. Ye J., Cheng X., Zhu J., Feng L., Song L. A DDoS attack detection method based on SVM in software defined network. *Secur. Commun. Netw*. 2018. Vol. 2018. Art. № 9804061. URL: https://doi.org/10.1155/2018/9804061
9. Dong S., Sarem M. DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks. *IEEE Access.* 2020. Vol. 8. P. 5039-5048. DOI: 10.1109/ACCESS.2019.2963077.
10. AbdulGhaffar A., Paul S. K., Matrawy A. An Analysis of DHCP Vulnerabilities. *Attacks, and Countermeasures, 2023 Biennial Symposium on Communications (BSC).* Montreal, QC, Canada, 2023. P. 119-124. DOI: 10.1109/BSC57238.2023.10201458.
11. Палагін В. В., Палагіна О. А., Івченко О. В., Панаско О. М., Пташкін Р. Л. Застосування методу штучного інтелекту для аналізу шкідливого мережевого трафіку на канальному рівні (ARP-атаки). *Інформатика та математичні методи в моделюванні, Національний університет «Одеська політехніка».* 2024. Вип. 14. № 1-2. P. 70-84. DOI: https://doi.org/10.15276/imms.v14.no1-2.70
12. Dynamic Host Configuration Protocol. URL: https://datatracker.ietf.org/-doc/html/rfc2131.
13. Learn Wireshark: A definitive guide to expertly analyzing protocols and troubleshooting networks using Wireshark, 2nd Edition Paperback. 5 Aug. 2022
14. The Ultimate Guide to DHCP Spoofing and Starvation Attacks. URL: https://info.pivitglobal.com/resources/dhcp-spoofing-and-starvation-attacks.
15. Active Directory-Integrated DNS Zones. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/active-directory-integrated-dns-zones.

MACHINE LEARNING METHOD FOR MALICIOUS NETWORK TRAFFIC ANALYSIS AT THE APPLICATION LEVEL (DHCP SPOOF)

DHCP (Dynamic Host Configuration Protocol) is a critically important component of network infrastructure that provides automatic assignment of IP addresses and configuration parameters to clients. However, due to the lack of authentication mechanisms in the basic protocol, it is vulnerable to DHCP spoofing attacks, in which an attacker impersonates a legitimate server and delivers malicious configuration settings to clients. This paper proposes a machine learning–based approach for detecting such attacks, capable of identifying both standard spoofing scenarios involving fake IP addresses and more sophisticated ones involving MAC address spoofing under a legitimate IP address.

As part of the study, a tool was developed to generate DHCP traffic simulating a variety of behaviors, including normal sessions, attacks from rogue IP addresses, and impersonation of legitimate servers. The application of machine learning (ML) methods is proposed for traffic analysis based on real-time data capture using the Wireshark platform. Based on the captured PCAP files, the dataset generation process was automated, producing a compact yet informative set of features (e.g., the number of unique IP/MAC addresses, the MAC address of the first responder, and IP-to-MAC consistency). The classification model built using a decision tree demonstrated high accuracy and the ability to detect both types of attacks.

The proposed method offers significant advantages over classical approaches, such as DHCP Snooping, which require manual configuration and are ineffective against attacks involving MAC spoofing. The developed model and methodology demonstrate exceptional reliability, achieving 100% detection accuracy for DHCP spoofing attacks, which is critical for maintaining real-time network responsiveness. The results confirm the effectiveness of behavioral analysis of DHCP sessions combined with machine learning techniques for anomaly detection, opening up new possibilities for integration into practical traffic monitoring and network security systems.

Key words: cyber threats, infrastructure attacks, artificial intelligence, network security, DHCP spoofing, IDS, machine learning.

Отримано: 14.06.2025

УДК 004.421.2
DOI: 10.32626/2308-5916.2025-27.121-127

Т. М. Пилипюк, канд. фіз.-мат. наук,
В. С. Щирба, канд. фіз.-мат. наук

Кам'янець-Подільський національний університет
імені Івана Огієнка, м. Кам'янець-Подільський

СПЕЦИФІКА БАГАТОПОТОКОВОГО МЕТОДУ РЕАЛІЗАЦІЇ МУРАШИНОГО АЛГОРИТМУ

Дана робота присвячена дослідженню специфіки та перспектив використання принципів розгалужених систем та паралельного програмування при обробці мережевих графових моделей. Предметом експериментального вивчення характеристичних особливостей слугує поліноміальний біоінспірований мурашиний алгоритм, що базується на метаевристичному підході моделювання поведінки мурах. Метою дослідження є одержання адекватних результатів побудови прогнозованих траєкторій руху, що задовольняють умовам оптимізації.

Мотивацією розгляду поставленої задачі та досягнення мети роботи послужило широке коло прикладних задач, що виникають як на регіональному рівні в рамках програми економічного та соціального розвитку міської громади, так і перспективних напрямків наукового дослідження від планування робіт економічного та соціального розвитку, оптимізації транспортних перевезень до дослідження телекомунікаційних мереж та систем штучного інтелекту. Результати дослідження можуть використовуватися для планування військових операцій при груповому застосуванні різного роду підрозділів збройних сил, особливо, коли передбачається ураження групових цілей.

Використання евристичного мурашиного алгоритму для дослідження задач, що подаються у вигляді графових моделей