РАДІОТЕХНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

УДК 004.738.5
DOI https://doi.org/10.32782/2663-5941/2024.3.2/01

Алєксєєв М.О.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Сінько В.В.
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Могилевич В.Д.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

ОЦІНКА ВПЛИВУ АТАК В ПРОГРАМНО-КЕРОВАНИХ МЕРЕЖАХ

Зростаюча складність кіберзагроз та постійні зміни технологій вимагають подальшого розвитку і вдосконалення інформаційної безпеки програмно-керованої мережі. Тому актуальним є аналіз впливу атак та вдосконалення методів і засобів захисту програмно-керованої мережі.

Стаття присвячена аналізу впливу атак на площину даних програмно-керованої мережі. Визначено та проведено оцінку загроз програмно-керованої мережі, доведено, що безпека цієї мережі значною мірою залежить від захисту площини управління мережі.

Дослідження охоплює широкий спектр сценаріїв атак, ґрунтуючись на розташуванні клієнт-серверів (веб-хостів) та зловмисників. Це дозволило детально проаналізувати різні типи атак та їх потенційні наслідки.

На основі аналізу результатів дослідження виявлено, що наслідки атак суттєво залежать від місця розташування веб-хостів та зловмисників. Зокрема, показано, що при розташуванні веб-хостів і зловмисників в різних мережах, причому, у випадку підключення клієнтів до одного комутатора, і серверів до іншого, а зловмисники мають доступ до обох комутаторів, наслідки атаки є найсерйознішими. Така атака може спричинити перевантаження контролера, переповнення буфера пам'яті та таблиць потоків комутаторів, а також блокування всіх каналів зв'язку, що призведе до повної відмови програмно-керованої мережі.

Результати оцінки впливу атак на площину даних дозволять в подальшому визначити оптимальні стратегії виявлення і захисту програмно-керованої мережі, та підвищити її стійкість до різноманітних атак.

Ключові слова: *програмно-керована мережа, площина даних, середня затримка, втрати, зловмисник.*

Постановка проблеми. Програмно-керовані мережі (SDN) стають все більш поширеними в сучасних IT-інфраструктурах. Архітектура SDN складається з площини управління, площини контролю та площини даних [1]. Фундаментальна ідея розділення площини управління та площини даних в програмно-керованих мережах є перспективною для зручного управління мережею.

Архітектура SDN пропонує новий підхід до побудови мережевої інфраструктури, але при цьому може мати потенційні вразливості з точки зору інформаційної безпеки. Необхідність розділення доступу до мережевих застосунків під час взаємодії з контролером, а також питання автентифікації та авторизації при роботі з застосунками на контролері, є лише кількома аспектами безпеки, які слід враховувати при проектуванні та експлуатації SDN. Контролер управління, як ключовий компонент інфраструктури SDN, є найбільш вразливим елементом, оскільки атака на нього може мати критичні наслідки для всієї інфраструктури [2].

Важливою частиною управління програмно-керованими мережами є розуміння потенційних ризиків та своєчасна реакція на атаки шляхом вдосконалення захисних механізмів і використання сучасних технологій кібербезпеки.

Ідентифікація та дослідження атак в програмно-керованих мережах є актуальним та

важливим напрямком у галузі кібербезпеки і вимагає подальших досліджень для розробки нових методів захисту та забезпечення стабільності цих мереж.

Аналіз останніх досліджень і публікацій. Аналіз науково-технічної літератури [3–8] показав, що безпеці самої SDN не приділяється достатня увага в порівнянні з іншими дослідницькими роботами в цій області. У деяких літературних джерелах обговорюються різні вектори загроз, а також способи їх зменшення в обмеженій області. У [9; 10] проведено класифікація загроз безпеки на різних рівнях SDN. У [11] досліджено модель маршрутизації з балансуванням навантаження в мережі на основі SD-WAN. Завдання маршрутизації представлено у вигляді оптимізаційної задачі з квадратичним критерієм оптимальності.

Постановка завдання. Метою роботи є оцінка впливу атак на площину даних програмно-керованої мережі.

Виклад основного матеріалу. Виклики безпеки в мережах, керованих SDN, є більш загрозливими порівняно з традиційними мережами. Зазвичай, у традиційній комп'ютерній мережі декілька серверів, які є частиною цієї мережі, стають об'єктами атак. На відміну від цього, якщо зловмисники скомпрометують площину управління SDN, під загрозою опиниться вся керована мережа. Проведений аналіз робіт [12–14] дозволив виділити такі вразливості та загрози:

1. *Загрози управління SDN*

Управління SDN спрямоване на вирішення різноманітних завдань, що стосуються ефективного та гнучкого керування мережевими ресурсами. Однією з основних переваг SDN є централізоване управління мережевими ресурсами. Замість розподіленого управління на окремих мережевих пристроях, SDN дозволяє централізовано керувати всією мережею через центральний контролер.

Скомпрометувати SDN через управління досить складно оскільки необхідна автентифікація та авторизація, але якщо вона буде скомпрометована, то вплив на мережу буде серйозним. Помилкове адміністрування мережі (н-д, неправильно налаштований контролер) може створити ризик відключення мережі [15].

Мережеві додатки, які працюють поверх контролера, можуть походити зі сторонніх джерел. Ці програми разом із контролером успадковують привілеї для управління мережевою поведінкою і можуть бути шкідливими або мати помилки безпеки. Додаток з помилками безпеки може бути використаний для мережевих або хост-орієнтованих атак і може призвести до розкриття інформації або довільного виконання коду з привілеями адміністратора [16]. Шкідливий SDN-додаток може виконувати різні системні команди і в найгіршому випадку може завершити роботу контролера командою виходу з системи, а також може використовувати доступні системні ресурси, такі як процесор та пам'ять, обмежуючи доступ до них іншим програмам.

Зловмисник використовуючи привілеї адміністратора може маніпулювати системними змінними та впливати на роботу мережі в цілому. Наприклад, зміна системного часу може відключити комутатори від контролера, якщо для автентифікації використовується цифровий сертифікат [17; 18]. Комутатори, що знаходяться під впливом зловмисника можуть перешкодити SDN виконувати заплановані завдання, визначені мережевою політикою.

2. *Загрози площини управління*

Площина управління включає в себе політики мережевих додатків, а також обмін трафіком між комутаторами і контролером для адміністрування керованої мережі. Політика одного мережевого додатку може суперечити іншим. Мережа може функціонувати неочікувано через відсутність пріоритетів у політиках. Наприклад, задана дія змінює правила маршрутизації всередині таблиць потоків (використовуються для переадресації трафіку на основі певних правил, що визначаються програмним забезпеченням SDN-контролера. Ці правила можуть включати в себе MAC-адреси, IP-адреси, порти, протоколи та інші атрибути пакетів). Мережева програма може використати цю дію для модифікації заголовків пакетів, щоб обійти політики брандмауера, що застосовуються іншими програмами. У найгіршому випадку шкідлива мережева програма з високим пріоритетом може видалити правила з таблиць потоків.

Згідно зі специфікацією OpenFlow (OF), канал зв'язку між контролером і комутаторами може бути реалізований за допомогою шифрування TLS/SSL або звичайного TCP. Аналіз показав, що багато виробників комутаторів і контролерів використовують протокол TCP, щоб уникнути складності, пов'язаної з зашифрованим каналом [19]. Це допустимо при функціонуванні в безпечній інфраструктурі. Однак, якщо трафік сигналізації здійснюється через незахищену мережу, атаки типу «людина посередині» або підслуховування

можуть бути успішно реалізовані. Це може статися в програмно-визначених мобільних мережах, мережах Wi-Fi або якщо сигнальний трафік проходить через мережу, що знаходиться під керуванням зловмисника. Зловмисники можуть виявляти сигнальний трафік з каналу, щоб визначити топологію мережі, а також модифікувати його, щоб змусити мережу працювати непередбачувано. Крім того, вони можуть перевантажувати таблиці потоків, встановлюючи велику кількість правил, як тільки отримують доступ до каналу [20].

Крім того, комутатор під керуванням зловмисника, з підробленою ідентичністю справжнього комутатора може відключити останній від мережі, що в подальшому призведе до відключення всіх кінцевих хостів, пов'язаних зі справжнім комутатором, і може призвести до порушення мережевого трафіку [21]. Комутатор під керуванням зловмисника може перевантажити контролер занадто великою кількістю фальшивих запитів PACKET IN і обмежити його доступність для обробки справжніх запитів потоку. Також, комутатор і контролер обмінюються ехо-запитами та повідомленнями-відповідями, щоб перевірити наявність та справність з'єднання між ними. Комутатор під управлінням зловмисника також може використовувати ці керуючі повідомлення для перевантаження контролера.

3. *Загрози на рівні даних*

Площина даних складається з комутаторів та інших мережевих пристроїв і головним чином відповідає за обробку даних, їх пересилання, відкидання, а також збір статистики. Функціонування площини даних відбувається на основі правил потоків, що надаються контролером мережі. Якщо для пакета відбувається подія flow tablemiss, пакет пересилається на контролер для встановлення правила в комутаторі або дій, які необхідно виконати для пакета. Тому час відгуку для першого пакета в потоці, як правило, довший, ніж час відгуку наступних пакетів того ж потоку. Ця особливість SDN допомагає зловмисникам відслідковувати SDN з площини даних [22]. Зловмисник може виявити потоки, для яких контролер не встановлює правила в таблицях потоків; замість цього він надсилає повідомлення PACKET OUT для їх обробки у відповідь на повідомлення PACKET IN, що надсилаються комутаторами, які відповідають потоку. Зловмисники можуть надсилати такі потоки, при обробці яких відбувається перевантаження контролера. Пакети в цих потоках займають буфер пам'яті комутатора до тих пір, поки не отримають відповіді від контролера, що призводить до погіршення продуктивності мережі. Кількість пакетів, які комутатор може зберігати в своєму буфері під час події PACKET IN обмежена і визначається під час з'єднання комутатора з контролером. Коли комутатор має достатньо пам'яті для буферизації пакетів, він надсилає повідомлення PACKET IN з невеликою частиною заголовка пакета разом з ідентифікатором буфера. У відповідь на повідомлення PACKET IN контролер надсилає повідомлення FLOW MOD або PACKET OUT, використовуючи ідентифікатор буфера в отриманому повідомленні PACKET IN. Як тільки комутатор отримує повідомлення від контролера, він видаляє пакет з буфера, ідентифікатор буфера якого збігається з ідентифікатором, зазначеним у повідомленні. Таким чином, канал управління несе менший обсяг трафіку для повідомлення PACKET IN і його повідомлень-відповідей. Однак, коли комутатори вичерпують свій буфер пам'яті через велику кількість фальшивих запитів PACKET IN від зловмисників, вони починають надсилати повний пакет в повідомленні PACKET IN, а також отримувати весь пакет з повідомленням-відповіддю від контролера. Таким чином, канал перевантажується великим обсягом трафіку порівняно з попереднім випадком [23].

В дослідженні проведено реалізацію та аналіз тих атак, для яких зловмисники не вимагають жодної автентифікації для доступу до системи SDN. У цьому контексті обрано атаку на площину даних.

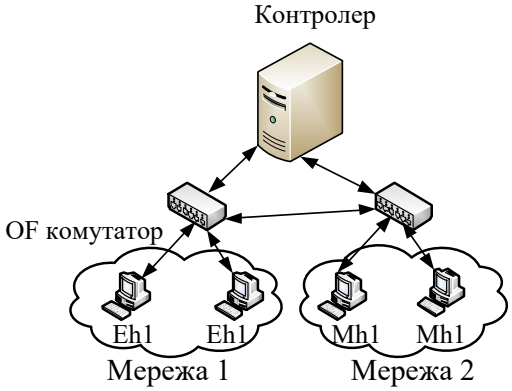

Рис. 1. Варіант структури мережі для дослідження атаки на площину даних:
Eh1, Eh2 – веб-хости користувачів,
Mh1, Mh2 – зловмисники

При атаки на площину даних зловмисники надсилають фальшиві запити, щоб завантажити контролер і комутатори для їх обробки, що призводить до затримок і втрат у налаштуванні правил потоку для легального трафіку. Проведена

оцінка впливу цієї атаки на затримку встановлення з'єднання та втрату клієнтських запитів до веб-серверів. Зі зростанням електронної комерції, мережеві оператори повинні відповідати Service Level Agreement (SLA) для своїх веб-клієнтів. Доступність веб-сервісів і час відгуку є двома важливими показниками в будь-якому SLA. Розрахунок цих показників проводився на основі вимірювання втрат клієнтських запитів і затримки встановлення з'єднання.

На основі контролера POX (контролер з відкритим вихідним кодом на основі Python, який забезпечує платформу для швидкої розробки SDN-додатків) та програмного емулятора SDN – Mininet (емулює мережеві хости, комутатори та зв'язки між ними) проведено дослідження атаки на площину даних. Комутатори на основі OF реалізовані за допомогою Open vSwitch. Комутатори підключаються до контролера який працює на тому ж хості або на віддаленому хості. Проведена модифікація наявного компоненту в POX для Ethernet-комутатора. Модифікований компонент встановлює правила потоку тільки для веб-трафіку, використовуючи повідомлення FLOW MOD. Для будь-якого іншого трафіку він генерує подію PACKET OUT для перенаправлення пакетів з певних портів комутаторів без встановлення правил. Тайм-аут простою для правила потоку встановлений на 15 секунд. Встановлене правило буде видалено з таблиць потоків, якщо комутатор не отримає жодного пакета, який відповідає правилу протягом цього періоду очікування. Веб-клієнт надсилає запит на веб-сервер через певний проміжок часу, що вважається легітимним трафіком. Вплив атаки оцінюються у двох випадках. У першому випадку інтервал між кожним запитом встановлюється меншим, ніж тайм-аут встановленого правила. У другому випадку інтервал встановлюється більшим, ніж тайм-аут встановленого правила.

Для автоматизації клієнтських запитів була використана утиліта curl (утиліта з відкритим вихідним кодом командного рядка, який підтримує різні протоколи, що використовуються для передачі даних мережею). Використовуючи цю утиліту можна встановити максимальний часовий ліміт, тобто тайм-аут з'єднання, до якого він намагатиметься з'єднатися з сервером. З'єднання вважається втраченим після закінчення тайм-ауту (у дослідженні тайм-аут – 60 сек.).

Віртуальні хости були з'єднані з двома комутаторами, які в свою чергу були підключені до контролера. Швидкість і затримка з'єднання між контролером і комутатором, комутатором і комутатором, та хостом-комутатором наведено в табл. 1.

Таблиця 1

Лінійна швидкість та затримка різних видів з'єднань

Тип з'єднання	Швидкість	Затримка
Контролер-комутатор	10 Мбіт/с	1 мс
Комутатор-комутатор	10 Мбіт/с	1 мс
Хост-комутатор	10 Мбіт/с	1 мс

Для достовірної оцінки впливу атак з'єднано 10 веб-клієнт серверних пар з комутаторами. Клієнти надсилають 20 запитів до відповідних серверів через фіксований інтервал часу за допомогою curl. Ping розглядався як ворожа атака. Хости зловмисника розглядалися як частина керованої мережі, які розташовані розподілено, щоб імітувати ботнети. Хост-зловмисник надсилає ping-пакети на свій одноранговий хост у мережі. Під час експериментів варіювалась частота надходження ping-пакетів і проводилось дослідження їхнього впливу на веб-сервіси. Розглянуто такі сценарії атаки залежно від місця розташування клієнт-серверів (веб-хостів) та зловмисників: веб-хости і зловмисники знаходяться в одній мережі; веб-хости знаходяться в одній мережі, а зловмисники – в іншій мережі; веб-хости знаходяться в одній мережі, а супротивники розподілені в різних мережах; веб-хости та зловмисники розподілені в різних мережах.

Аналіз результатів експерименту показав, що у випадку знаходження веб-хостів клієнтів та зловмисників в одній мережі затримка встановлення з'єднання досить висока, коли клієнтські запити надсилаються після закінчення періоду тайм-ауту правил потоку, порівняно з тим, коли вони надсилаються до закінчення тайм-ауту (рис. 2).

У першому випадку затримка встановлення з'єднання зросла до 22 секунд, коли частота атак досягла 14Kps (тисяч на секунду), тоді як у другому випадку – до 3 сек. Частка втрачених запитів зростає зі зростанням частоти атак в обох випадках, як показано на рис. 3.

Однак, вона є вищою в першому випадку, ніж у другому, і досягає 98 %. Причина високого рівня втрат, навіть коли запити генеруються до закінчення терміну дії правил потоку, пов'язана з великою кількістю пакетів ping-флуду від зловмисників, які призводять до вичерпання буфера пам'яті в комутаторі для черги вхідних пакетів для легітимного трафіку.

Якщо веб-хости знаходяться в одній мережі, а зловмисники – в іншій мережі (у цій експери-

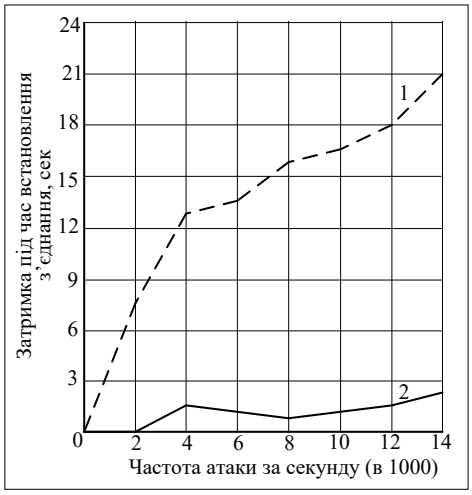

Рис. 2. Середня затримка встановлення підключення при знаходженні всіх веб-хостів та зловмисників в одній мережі:
1 – кількість надісланих запитів до закінчення дії правил потоку, 2 – кількість надісланих запитів після закінчення дії правил потоку

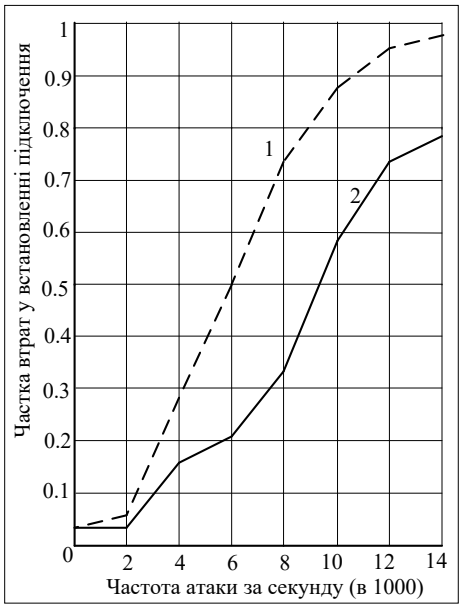

Рис. 3. Середня частка втрат при знаходженні всіх веб-хостів та зловмисників в одній мережі:
1 – кількість надісланих запитів до закінчення дії правил потоку, 2 – кількість надісланих запитів після закінчення дії правил потоку

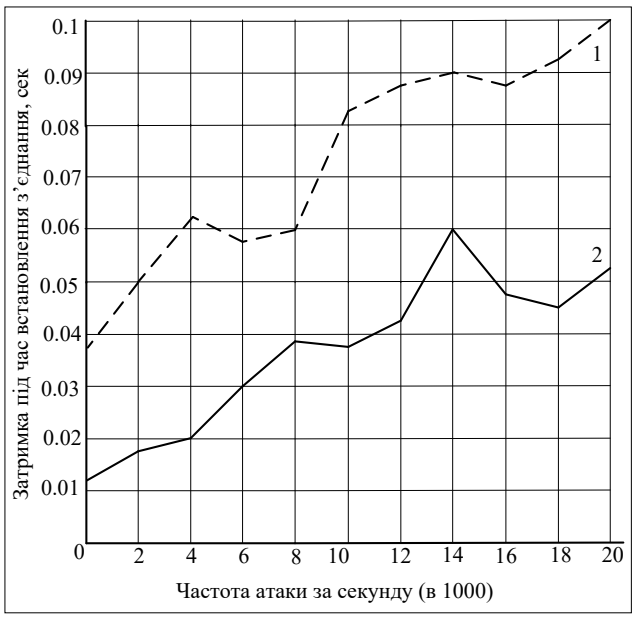

Рис. 4. Середня затримка встановлення підключення при знаходженні веб-хостів в одній мережі, а зловмисників в іншій мережі:
1 – кількість надісланих запитів до закінчення дії правил потоку, 2 – кількість надісланих запитів після закінчення дії правил потоку

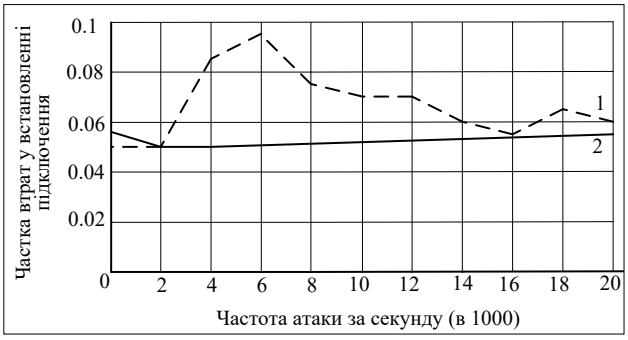

Рис. 5. Середня частка втрат при знаходженні веб-хостів в одній мережі, а зловмисників – в мержі веб-хостів та в іншій мережі:
1 – кількість надісланих запитів до закінчення дії правил потоку, 2 – кількість надісланих запитів після закінчення дії правил потоку

ментальній топології веб-вузли користувачів підключено до одного комутатора, а хости зловмисника до іншого комутатора, відповідно), то вплив атаки є дуже незначним (рис. 4 та рис. 5).

Затримка зросла до 0,11 с і 0,06 с для запитів, що були згенеровані після та до закінчення терміну дії правил потоку, відповідно.

Втрати залишаються близько 5 % протягом більшої частини часу, навіть якщо частота атак зростає в обох випадках (рис. 5). Причиною меншого впливу можна пояснити тим, що піддається атаці лише канал зв'язку між контролером та комутатором. Таблиці потоків та пам'ять буферів для постановки в чергу вхідних пакетів у комутаторі, пов'язаному з веб-вузлами, а також канал зв'язку від цього ж комутатора до контролера не були перевантажені небажаними PACKET IN запитами ping-флуду.

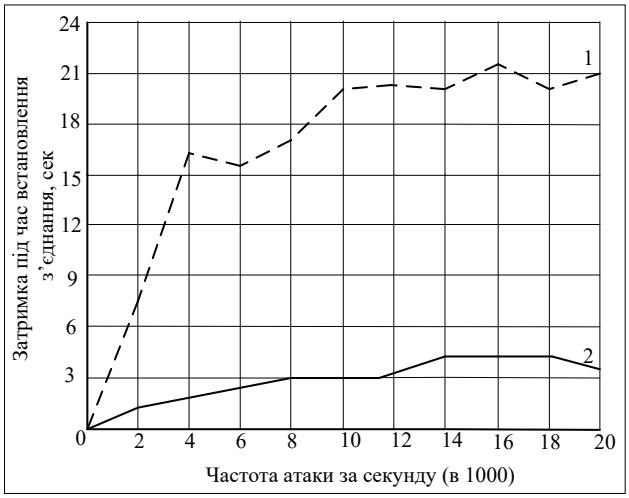

Рис. 6. Середня затримка встановлення підключення коли веб-хости знаходяться в одній мережі, а зловмисники – в мережі веб-хостів та в іншій мережі:
1 – кількість надісланих запитів до закінчення дії правил потоку, 2 – кількість надісланих запитів після закінчення дії правил потоку

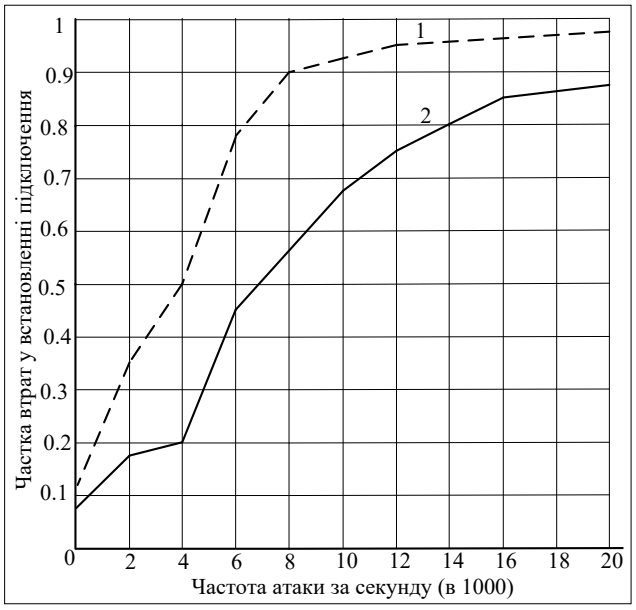

Рис. 7. Середня частка втрат коли веб-хости знаходяться в одній мережі, а зловмисники – в мержі веб-хостів та в іншій мережі:
1 – кількість надісланих запитів до закінчення дії правил потоку, 2 – кількість надісланих запитів після закінчення дії правил потоку

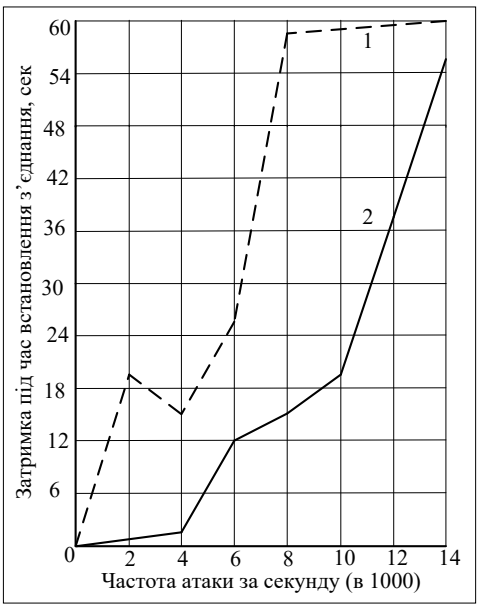

Рис. 8. Середня затримка встановлення підключення коли веб-хости та зловмисники розподілені по різним мережам:
1 – кількість надісланих запитів до закінчення дії правил потоку, 2 – кількість надісланих запитів після закінчення дії правил потоку

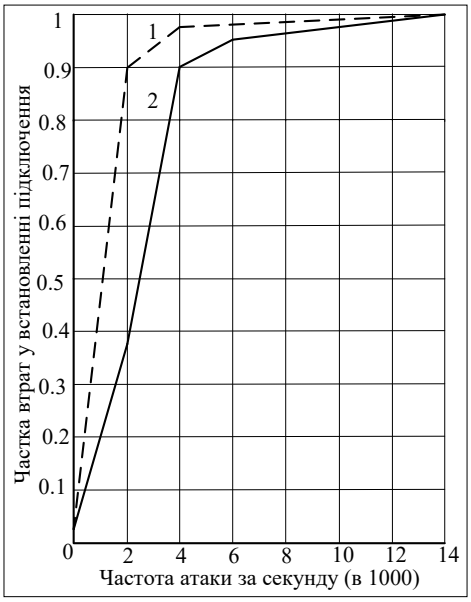

Рис. 9. Середня частка втрат коли веб-хости знаходяться в одній мережі, а зловмисники – в мержі веб-хостів та в іншій мережі:
1 – кількість надісланих запитів до закінчення дії правил потоку, 2 – кількість надісланих запитів після закінчення дії правил потоку

При знаходженні веб-вузлів клієнтів в одній мережі, а зловмисники розподілені за різними мережами (веб-вузли клієнтів пов'язані з одним комутатором, в той час як зловмисники пов'язані з обома комутаторами) спостерігається, що результати (рис. 6 та рис. 7) подібні до першого, хоча в цьому сценарії зловмисники розподілені.

У випадку коли веб-хости і зловмисники розподілені в різних мережах (клієнти пов'язані з одним комутатором, а сервери були пов'язані з іншим комутатором. Зловмисники були

пов'язані з обома комутаторами) наслідки атаки є найсерйознішими з усіх. Ця атака споживає ресурси контролера, переповнює буфер пам'яті та таблиці потоків комутаторів, а також переповнює всі канали зв'язку.

Затримка встановлення з'єднання збільшилася до 52 секунд, навіть коли запити відправлені до закінчення терміну дії правил потоку, що дає уявлення про падіння реального трафіку на комутаторах через велику кількість пакетів зловмисника (рис. 8).

Частка втрат з'єднань досягала майже 100 %, коли швидкість атаки досягала 6 Кбіт/с у випадку, коли запити надсилаються після закінчення терміну дії правил потоку (рис. 9).

Висновки. Архітектура SDN суттєво змінює структуру мережі, що призводить до появи нових загроз безпеці, спричинених вразливостями окремих компонентів інфраструктури.

Проведена оцінка впливу атак зловмисників на продуктивність мережевих сервісів, що працюють через SDN. Оцінка впливу різних атак дає уявлення про аналіз їх ризиків і дозволяє розрахувати загальну систему оцінки вразливостей, що відповідає цим атакам. Визначено, що продуктивність веб-сервісів, враховуючи час відгуку та доступність, значно погіршується за наявності атак. Негативний вплив атак на час відгуку та доступність створює загрози для забезпечення операторами нормованого SLA для своїх клієнтів.

Список літератури:

1. Гніденко М.П., Вишнівський В.В., Ільїн О.О. Побудова SDN мереж : навч. посіб. Київ : ДУТ, 2019. 190 с.

1. 2. Bai J. C. Sun Q. Software-Defined Wide Area Network Architectures and Technologies: training manual. CRC Press, 2013, 460 p.

2. Sabella A., Irons-Mclean R., Yannuzzi M. Orchestrating and automating security for the internet of things: Delivering advanced security capabilities from edge to cloud for IoT: book. Cisco Press, 2018. 1008 p.

3. Liu Y., Zhao B., Zhao P., Fan P., Liu H. A survey: Typical security issues of software-defined networking. *China Communications*. 2019. № 16 (7). P. 13 – 31. DOI: https://doi.org/10.23919/JCC.2019.07.002.

4. Mousa M., Bahaa-Eldin A.M., Sobh M. Software Defined Networking concepts and challenges. *2016 11th International Conference on Computer Engineering & Systems (ICCES)*, 2016. P. 79–90. DOI: 10.1109/ICCES.2016. 7821979.

5. Ahnaf A., Erkki H., Ylianttila M. Ahmad I. Evaluation of Machine Learning Techniques for Security in SDN. *2020 IEEE Globecom Workshops.* DOI: 10.1109/GCWkshps50303.2020.9367477.

6. Software-Defined Networks. A Systems Approach: training manual. *Systems Approach LLC*. 2020. 194 p.

7. Siham A., Meghrouni I., Sabri Y., Hilmani A., Maizate A. Security of software defined networks: evolution and challenges. *International Journal of Reconfigurable and Embedded Systems*. 2023. № 12 (3). 384 p. DOI: 10.11591/ ijres.v12.i3.pp384-391.

8. Rahouti M., Xiong K., Xin Y., Jagatheesaperumal S.K., Ayyash M., Shaheed M. SDN Security Review: Threat Taxonomy, Implications, and Open Challenges. *IEEE Access.* 2022. P. 45820–45854. DOI: 10.1109/ACCESS.2022.3168972.

9. Iftekhar A., Zulfikar A., Maher Z., Wu L. A Comprehensive Survey of Software Defined Networking and its Security Threats. *2024 IEEE 1st Karachi Section Humanitarian Technology Conference.* 2024. DOI: 10.1109/KHI-HTC60760.2024.10482096

10. Kujur P., Biswal S., Patel S. Security Challenges and Analysis for SDN-Based Networks. *Software Defined Networks: Architecture and Applications. Wiley.* 821 p. DOI: 10.1002/9781119857921.ch10.

11. Yeremenko O., Persikov M., Lemeshko V., Altaki B. Research and development of the secure routing flow-based model with load balancing. *Проблеми телекомунікацій*. 2021. № 2 (29). С. 3–14. URL: https://pt.nure.ua/wp-content/uploads/2021/12/212_yeremenko_secure.pdf. (дата звернення: 17.03.24).

12. Abdulsamad A.A., Salih, T.A. IoT security improvement based on SDN Controller. *Eurasian Journal of Engineering and Technology*. 2023. № 14, P. 49–56. URL: https://geniusjournals.org/index.php/ejet/article/view/3199 (дата звернення: 27.02.2024).

13. Pradhan A., Mathew R. Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN). *Procedia Computer Science.* 2020. Vol. 171, P. 2581–2589. DOI:10.1016/j.procs.2020.04.280.

14. Nadim A., Dutta N. Analysis of Security Attacks in SDN Network: A Comprehensive Survey. *Contemporary Issues in Communication, Cloud and Big Data Analytics*. 2022. P. 27–37. DOI:10.1007/978-981-16-4244-9_3.

15. Karthika P., Karmel Dr. A. Analysis of Different Attacks on Software Defined Network and Approaches to Mitigate using Intelligent Techniques. *International Journal of Advanced Computer Science and Applications.* 2021. № 12 (9). DOI: 10.14569/IJACSA.2021.0120938.

16. Anmol M., Abhinav B. Attacks in Software-Defined Networking: A Review. *Proceedings of the International Conference on Innovative Computing & Communications.* 2020. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id =3564048 (дата звернення: 01.04.2024).

17. Anh T., Bo Li, Faheem U., Tanvir U., Ranesh N., Muhammad A., Hung N. Defending SDN against packet injection attacks using deep learning. *Computer Networks.* 2023. Vol. 234. P. 144–158. https://doi.org/10.1016/j.comnet.2023. 109935.

18. Wang J, Wang L. SDN-Defend: A Lightweight Online Attack Detection and Mitigation System for DDoS Attacks in SDN. *Sensors*. 2022. Vol. 22 (21). P. 8287. DOI: https://doi.org/10.3390/s22218287.

19. Farooq MS, Riaz S, Alvi A. Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review. *Electronics*. 2023. № 12 (14). DOI: https://doi.org/10.3390/electronics12143077.

20. Singh J., Behal S. Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions, *Computer Science Review.* 2020. Vol. 37. DOI: https://doi.org/10.1016/j.cosrev.2020.100279.

21. Alsaghier H. Attack on sdn infrastructure and security measures. *Journal of Engineering and Applied Sciences.* 2019. P. 1–17. DOI: https://doi.org/ 10.5455 /jeas.2019090101.

22. Maleh Y., Qasmaoui Y., Gholami K., Sadqi Y., Mounir S. A comprehensive survey on SDN security: threats, mitigations,and future directions. *Journal of Reliable Intelligent Environments.* 2022. DOI: 10.1007/s40860-022-00171-8.

23. Juan Camilo Correa Chica, Jenny Cuatindioy Imbachi, Juan Felipe Botero Vega. Security in SDN: A comprehensive survey. *Journal of Network and Computer Applications.* 2020. Vol. 159. DOI: https://doi.org/10.1016/j.jnca.2020. 102595.

Alieksieiev M.O., Sinko V.V., Mohylevych V.D. ASSESSING THE IMPACT OF ATTACKS IN SOFTWARE-DEFINED NETWORKS

The growing complexity of cyber threats and constant changes in technology require further development and improvement of the information security of a software-defined network. Therefore, it is important to analyze the impact of attacks and improve the methods and means of protecting a software-defined network.

The article is devoted to analyzing the impact of attacks on the data plane of a software-defined network. The threats to a software-controlled network are identified and assessed, and it is proved that the security of this network largely depends on the protection of the network control plane.

The study covers a wide range of attack scenarios based on the location of client servers (web hosts) and attackers. This allowed us to analyze in detail different types of attacks and their potential consequences.

Based on the analysis of the study results, it was found that the consequences of attacks significantly depend on the location of web hosts and attackers. In particular, it is shown that when web hosts and attackers are located in different networks, and when clients are connected to one switch and servers to another, and attackers have access to both switches, the consequences of the attack are the most serious. Such an attack can cause controller overload, overflow of the memory buffer and switch flow tables, and blocking of all communication channels, leading to a complete failure of the software-controlled network.

The results of assessing the impact of attacks on the data plane will allow us to further determine the optimal strategies for detecting and protecting a software-defined network and increase its resistance to various attacks.

Key words: *software-defined network, data plane, average delay, losses, attacker.*