УДК 004.056 **doi: 10.26906/SUNZ.2022.3.123**

А. І. Левтеров, Г. А. Плєхова, М. В. Костікова, С. В. Очеретенко

Харківський національний автомобільно-дорожній університет, Харків,Україна

АНАЛІЗ ВРАЗЛИВОСТЕЙ ПЛОЩИНИ ДАНИХ SDN І ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ ЗАСОБІВ МАРШРУТИЗАЦІЇ ЩОДО ПРОТИДІЇ МОЖЛИВИМ АТАКАМ

Анотація. Проведений аналіз вразливостей площини даних SDN і функціональних можливостей засобів безпечної маршрутизації щодо протидії можливим атакам. Розглянуті у межах площини даних основні типові проблеми безпеки, вказані їх причини та можливі об'єкти атак. Описані існуючі технології захисту площини даних SDN. Надана узагальнена класифікація вразливостей та їх характеристики.

Ключові слова: SDN, метрика, безпека, вразливість, CVSS.

Вступ

В сьогоденні все більш використовують такі мережні архітектури, як програмно-конфігуровані мережі *(Software-Defined Networking, SDN*). У сучасному світі розгортаються нові загрози кібербезпеки для таких мереж, що вимагає розробку та дослідження нових спеціалізованих рішень щодо підвищення рівня мережної безпеки. В роботі проводиться дослідження функціонування архітектур *SDN* з урахуванням збільшення кількість потенційних мережних атак які приводять до нових проблем безпеки.

Аналіз публікацій. На сучасному етапі розвитку архітектур *SDN*, вітчизняні та іноземні дослідники вважають, що типові проблеми безпеки у програмно-конфігурованих мережах перш за все проявляються в таких аспектах: шкідливе програмне забезпечення, вразливість контролера, легітимність та узгодженість правил потоків, проблема стандартизації північного інтерфейсу, безпека комунікації в процесі використання південного інтерфейсу та ін [1 – 4].

Мета та постановка задачі. Метою статті є необхідність проаналізувати вразливості які виникають в площини даних *SDN* використовуючи аналітичні та порівняльні методи. Провести аналіз типових проблем безпеки, вказати причини та об'єкти атак. Вказати на вразливості в функціональних засобах при безпечної маршрутизації щодо протидії можливим атакам. Постановка задачі – удосконалити безпечну маршрутизацію, за рахунок зниження типових проблем безпеки.

Виклад основного матеріалу

У роботі проаналізовано наведені у табл. 1 типові проблеми безпеки та об'єкти атак у межах площини даних - мережних пристроїв, що керуються контролером *SDN*. Очевидно, що об'єктами атаки можуть бути різні пристрої мережі. Вони можуть бути розташовані на різних рівнях мережі. Архітектура *SDN* багаторівнева, тому можна класифікувати загрози безпеці на різних рівнях. В роботі аналізуються загрози та наданий аналіз об'єктів атак і потенційних рішень щодо підвищення рівня мережної безпеки у площині даних *SDN*.

Таким чином, можна зробити висновок, що площина даних складається з комутаторів та інших мережних пристроїв. Основною функцією є те, що вона відповідає за обробку даних, їх пересилання, відкидання, а також збір статистики. Площина даних працює на основі правил потоків, які надаються контролером мережі. Розглянемо проблеми безпеки у площині даних відповідно до [1] (табл. 1):

Таблиця 1 – **Типові проблеми безпеки, об'єкти атак і причини** [1]

Проблема безпеки	Об'єкт атаки	Причина
Авторизована автентифікація	Мережне обладнання	Управління доступом
Правомірність правил потоків	Правила потоків	Управління доступом
Узгодженість правил потоків	Правила потоків	Архітектура *SDN*
DoS/*DDoS*-атаки	Таблиці потоків	Архітектура *SDN*, зловмисна атака
Атака сторонніми каналами	Конфіденційність даних	Зловмисна атака

1. Авторизована автентифікація. По суті, на рівні площини даних відсутній ефективний механізм автентифікації між мережним обладнанням і контролером. Таким чином, можуть виникнути деякі проблеми, а саме видавання особи за іншу особу та незаконний доступ. Зловмисний *SDN*-комутатор може генерувати підроблений або фальшивий потік даних у мережі, маніпулювати або перевіряти вміст пакетів даних і відхиляти дозволені пакети даних. Це може призвести до порушення цілісності даних і вплинути на доступність площини даних.

Крім того, якщо комутатор встановлює з'єднання з контролером без автентифікації, комутатором може керувати зловмисний контролер, що може призвести до фальсифікації інформації таблиці потоків, що призведе до витоку даних та інших проблем безпеки. Не відповідні керуючі інструкції можуть спричинити плутанину в таблицях потоків комутаторів та безпосередньо збільшити ризики порушення безпеки.

2. Правомірність і узгодженість правил потоків є одними з головних проблем на рівні площини

даних. Правомірність правил потоків стосується зловмисного або невірного впровадження правил потоків. Зі свого боку узгодженість правил потоків в основному включає три аспекти [1]. Під час процесу генерації функціонування значної кількості застосунків може викликати конфлікти або перевизначення правил потоків. Під час процесу випуску правил потоків затримка передавання або зловмисне втручання може також спричинити їхню неузгодженість між контролером і комутаторами. Зі свого боку процес оновлення ініціює синхронізацію правил потоків між різними комутаторами. Слід зазначити, що до оновлення правил потоків в *SDN* призводять, наприклад, відмови вузлів мережі, передача службового навантаження або технічне обслуговування мережі, через що пакети бачитимуть неузгоджені уявлення мережі щодо її поточного стану. Таким чином, якщо пакети даних передаються відповідно до нових і старих правил потоків, то можуть виникнути такі проблеми, як «чорні діри», циклічні шляхи або перевантаження мережі.

3. *DoS*/*DDoS*-атаки. Простір таблиці потоків обмежений, проте за звичайних обставин розмірність таблиці потоків комутатора відповідає вимогам пересилання пакетів даних. Однак в умовах *DoS*/*DDoS*-атак зловмисник створює низку незаконних доступів, і простір таблиці потоку переповнюється недійсними правилами трафіку [1]. У разі цього буде спожито значну кількість ресурсів таблиці потоків, а звичайні правила потоків не мають достатньо місця для обробки. Отже, *DoS*/*DDoS*-атаки можуть значно погіршити продуктивність мережі.

4. Атака сторонніми каналами. *SDN* весь час переносить приватну та конфіденційну інформацію [1]. У *SDN* атрибути процесу (наприклад, атрибут часу) кожної дії виконання різні. Використовуючи атаки сторонніми каналами, зловмисник може отримати пов’язану з мережею інформацію про стан (наприклад, інформацію таблиці потоків), перевіряючи час виконання конкретного типу пакета даних. Тому таблиця потоків може спричинити проблеми з витоком даних. Хоча атаки через сторонні канали безпосередньо не впливають на доступність, конфіденційність або цілісність даних, вони можуть викликати подальші атаки.

Таким чином, вважаємо необхідним акцентувати, що причинами проблем безпеки є власне архітектура *SDN*. Коли виникають зовнішні атаки, ми отримуємо недостатність контролю доступу та засобів шифрування.

Технології та підходи захисту площини даних *SDN* уявляють базуючись на дослідженнях типових проблем безпеки, стає очевидним, що централізоване керування та функції програмованості *SDN* надають зловмисникам потужні та зручні канали атак. Отже, поширене використання архітектур *SDN* на практиці робить питання безпеки все більш помітними. Основні існуючі технології захисту площини даних *SDN* наведені в табл. 2.

Таблиця 2 – **Існуючі технології безпеки у площині даних *SDN*** [1]

Технологія захисту	Проблема безпеки
Виявлення помилок у мережі	Помилка конфігурації
Класифікація правил потоків	Правомірність правил потоків
Формальний математичний аналіз	Правомірність правил потоків
Виявлення зв’язності	Узгодженість правил потоків
Модуль автентифікації й авторизації	Авторизована автентифікація

1. Виявлення помилок мережі може бути реалізовано за допомогою алгоритмів виявлення. Так, наприклад, *NICE* [1] надає тестову схему, засновану на символічній моделі виконання з метою перевірки, чи створює програма верхнього рівня неузгоджений стан мережі. Однак ці методи не є рішеннями в реальному часі, мають велику затримку обробки та високий рівень запитів. Такі рішення не можуть принципово усунути вплив конфігураційних конфліктів на мережу.

2. Поділ правил потоків. Розподіл дозволів додатків на основі ролі та пріоритету об’єкта є основним методом вирішення правомірності та узгодженості правил потоків. Дозвіл правил потоків поділяється за такими методами, як цифровий підпис, розподіл ролей і класифікація функцій.

3. Виявлення зв’язності може бути реалізовано різними засобами, наприклад, шляхом використання технології віртуалізованого обміну з метою розділення мережі на ізольовані фрагменти і таким чином запобігання конфлікту правил потоків у них; механізмів виявлення цілісності пакетів на основі поєднання правил потоків з номером версії тощо [1].

4. Модуль автентифікації й авторизації може використовувати сервер *RADIUS* для автентифікації ідентифікатора хоста. Крім того, можливе застосування квантової криптографії для розробки надлегкої верифікації цілісності [1]. Зазначається, що квантові паролі є більш безпечними, ніж традиційні, проте їхнє впровадження може бути дорожчим.

5. Захист від *DoS*/*DDoS*-атак у площині даних може бути трансформована в задачу оптимізації таблиці потоків.

Для підвищення мережної безпеки, що також стосується мереж *SDN*, особливе місце надається протоколам маршрутизації. Протоколи потребують системної та скоординованої взаємодії одночасно множини мережних елементів. Такими елементами є *SDN*-комутатори, а також контролери мережі під час формування (розрахунку) шляхів і правил потоків. Коли ми використовуємо поняття потоків, то маємо на увазі ті, вздовж яких має забезпечуватися необхідний рівень безпеки за обраними показниками або критеріями.

Безпечної маршрутизації приділено багато уваги в наукових виданнях. Велика кількість теоретичних досліджень та наукових робіт присвячена цьому напрямку. Для розв'язання таких задач використовувались як найпростіші емпіричні варіанти рішень так і системні оптимізаційні підходів.

Так, у роботі [2] розроблено та досліджено модель безпечної маршрутизації з балансуванням навантаження в мережах на основі *SD-WAN*. Технологічне завдання безпечної маршрутизації з балансуванням навантаження було сформульовано у формі оптимізаційної задачі з квадратичним критерієм оптимальності. Така форма критерію дозволяє збалансувати частки потоків, що передаються в мережі. Представлена модель безпечної маршрутизації збалансуванням навантаження з адитивною метрикою враховує продуктивність і безпеку мережі, дозволяє ефективніше використовувати наявні мережні ресурси, також враховує ймовірність компрометації каналів зв'язку під час прийняття маршрутних рішень.

У роботах [2, 3] пропонуються потокові моделі маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Основу моделі складають умови реалізації одно- та багатошляхової маршрутизації, збереження потоку та запобігання перевантаженню каналів зв'язку мережі, а задача безпечної маршрутизації також сформульована як оптимізаційна.

Важливим є аналіз стандарту *CVSS* щодо кількісного розрахунку рівня вразливості. Виявлення й ідентифікація вразливостей – це процес виявлення вразливостей, які можуть бути використані загрозами для заподіяння шкоди активам. Вразливість – це слабке місце або недолік у процедурах безпеки системи, проектуванні, реалізації або внутрішніх засобах контролю, які можуть бути випадково активовані або навмисно використані під час виявлення загрози. В роботі розглянуто категорії вразливостей та проаналізовано підходи до ідентифікації та документування вразливостей, а також обговорено використання національної бази даних вразливостей – *National Vulnerability Database* (*NVD*).

Узагальнена класифікація вразливостей може бути представлена наступним чином [5]:

1. Технічні вразливості: недоліки в розробці, реалізації та/або конфігурації програмного забезпечення та/або апаратних компонентів, включно з прикладним програмним забезпеченням, системним програмним забезпеченням, комунікаційним програмним забезпеченням, обчислювальним обладнанням, комунікаційним обладнанням і вбудованими пристроями.

2.Вразливості, спричинені діяльністю людини: залежність від певних осіб, прогалини в обізнаності та навчанні, прогалини в дисципліні та неправомірне обмеження доступу.

3. Фізичні вразливості та вразливості середовища: недостатній контроль (фізичного) доступу, невдале розміщення обладнання, невідповідний контроль температури/вологості та неналежне кондиціонування у приміщеннях, де знаходиться обладнання.

4. Операційні вразливості: відсутність керування змінами, неналежний розподіл обов'язків, відсутність контролю за встановленням програмного забезпечення, відсутність контролю над обробкою та зберіганням медіафайлів, відсутність контролю над системним зв'язком, неналежний контроль доступу або недоліки в процедурах контролю доступу, неналежний запис та/або перегляд записів системної діяльності, неадекватний контроль над ключами шифрування, неадекватне звітування, обробка та/або вирішення інцидентів безпеки, а також неадекватний моніторинг та оцінка ефективності засобів контролю безпеки.

5. Вразливості безперервності бізнесу та дотримання нормативних вимог: недоречні, відсутні або невідповідні процеси для належного управління бізнес-ризиками; неадекватне планування безперервності бізнесу та дій у разі виникнення надзвичайних ситуацій; а також неадекватний моніторинг та оцінка відповідності керівним політикам і нормам.

У багатьох сферах, перерахованих тут, виявлення вразливості критично залежить від ініціативи керівництва та подальших дій. Такі методи, як інтерв'ю, анкетування, перегляд попередніх оцінок ризиків та аудиторських звітів, а також контрольні списки – усі вони сприяють створенню ефективного уявлення ландшафту вразливості.

Розглянемо більш детально сферу технічних вразливостей. Видатним ресурсом є національна база даних про вразливості *NIST – National Vulnerability Database* (*NVD*), і відповідна загальна система оцінки вразливостей – *Common Vulnerability Scoring System* (*CVSS*), описана в *NISTIR* 7946, Посібник із впровадження *CVSS* [3 – 9]. *NVD* – це вичерпний список відомих технічних вразливостей систем, апаратного та програмного забезпечення. *CVSS* забезпечує відкриту структуру для передачі характеристик вразливостей. *CVSS* визначає вразливість як помилку, недолік, слабкість або відкритість програми, системного пристрою чи сервісу, що може призвести до збою конфіденційності, цілісності чи доступності.

Отже, модель *CVSS* намагається забезпечити повторювані та точні вимірювання, одночасно дозволяючи користувачам переглядати базові характеристики вразливості, які використовуються для створення числових оцінок. *CVSS* надає загальну систему вимірювання для галузей промисловості, організацій та урядів, які вимагають точних і послідовних оцінок використання вразливостей та їхнього впливу.

Розуміння *CVSS* дозволяє оцінити широкий спектр вразливостей, які впливають на системи. Крім того, систематизована схема для оцінки вразливостей у *CVSS* є корисною для розробки подібного системного підходу до інших вразливостей, таких як ті, що пов'язані з організаційними питаннями, політикою та процедурами, а також фізичною інфраструктурою. На сьогоднішній день *CVSS* широко прийнятий і використовуваний підхід. Наприклад, використання *CVSS* рекомендується для кількісного розрахунку рівня вразливості мережного обладнання [3, 4].

Кожен запис *NVD* містить такну інформацію [2]:

- унікальний словниковий ідентифікатор вразливостей і ризиків – *Common Vulnerabilities and Exposure* (*CVE*);

- опис вразливості;

- посилання на веб-сайти та інші посилання з інформацією, пов'язаною з вразливістю;

- метрики *CVSS*.

Метрики загальної системи оцінки вразливостей – *CVSS*. Існує 14 метрик *CVSS*, розділених за трьома групами [5]. У табл. 3 перелічені окремі показники та показано рівні, визначені для кожного з них. У кожному випадку рівні вказані від найвищого до найнижчого. По суті, підрахунок балів здійснюється таким чином: для кожної виявленої вразливості *NVD* надає рівень для кожного показника в базовій групі на основі характеристик вразливості. Наприклад, метрика вектора атаки вказує, чи можна атаку запустити віддалено через мережу чи через Інтернет, запускати лише через мережу, до якої підключено як джерело атаки, так і цільову систему, має бути здійснено за допомогою локального входу , або вимагає фізичного доступу до машини. Чим віддаленіш атака, тим більше джерел атаки можливе, а отже, тим серйозніша вразливість. Ця інформація є безцінною, оскільки дозволяє користувачам зрозуміти характеристики вразливості.

Таблиця 3 – **Загальна** класифікація метрик CVSS [5]

Група базових метрик		**Група часових метрик**	**Група метрик середовища**
Можливість використання	**Вплив**		
Вектор атаки: - Мережа - Прилеглий - Локальний - Фізичний *Складність атаки:* - Низька - Висока *Необхідність привілеїв:* - Немає - Низька - Висока *Взаємодія з користувачем:* - Немає - Вимагається	*Вплив на конфіденційність:* - Високий - Низький - Немає *Вплив на цілісність:* - Високий - Низький - Немає *Вплив на доступність:* - Високий - Низький - Немає	*Зрілість коду експлойту:* - Не визначений - Високий - Функціональний - Доказ концепції - Недоведений *Рівень виправлення:* - Не визначений - Обхідний шлях - Тимчасове виправлення - Офіційне виправлення *Достовірність звіту:* - Не визначена - Підтверджена - Обґрунтована - Невідома	*Вимоги конфіденційності:* - Не визначені - Високі - Середні - Низькі *Вимоги цілісності:* - Не визначені - Високі - Середні - Низькі *Вимоги доступності:* - Не визначені - Високі - Середні - Низькі
Область застосування: - Без змін - Змінена			

Як показано в табл. 3, кожен рівень метрики має описову назву [5]. Крім того, *CVSS* призначає числове значення за шкалою від 0,0 до 10,0, де 10,0 є найсерйознішою проблемою безпеки. Числові оцінки для показників у групі базових показників поміщаються в рівняння, визначене в *CVSS*, яке створює сукупний базовий показник безпеки в діапазоні від 0,0 до 10,0.

Базова група метрик представляє внутрішні характеристики вразливості, які є незмінними протягом часу та серед користувачів. Вона складається з трьох наборів показників [5]:

1. Можливість використання (*Exploitability*): ці показники відображають легкість і технічні засоби, за допомогою яких використовується вразливість. Показники:

- Вектор атаки, який вказує, наскільки віддаленим може бути зловмисник від уразливого компонента.

- Складність атаки передає рівень складності, необхідний зловмиснику для використання вразливості після ідентифікації цільового компонента. Складність оцінюється як висока, якщо зловмисник не може здійснити атаку за власним бажанням, але повинен докласти певних зусиль для підготовки або виконання.

- Необхідні привілеї характеризують доступ, потрібний зловмиснику для використання вразливості. Значення: «немає/*none*» (привілейований доступ не потрібен), «низький/*low*» (базові привілеї користувача) і «високий/*high*» (права адміністратора).

- Взаємодія з користувачем вказує, чи має брати участь інший користувач, крім зловмисника, для успішної атаки.

2. Вплив (*Impact*): ці показники вказують на ступінь впливу на основні цілі безпеки – конфіденційність, цілісність і доступність. У кожному з цих випадків оцінка відображає найгірший результат, якщо уражено більше ніж один компонент. Для кожної з трьох цілей вводяться аналогічні значення впливу: «високий/*high*» (повна втрата конфіденційності, цілісності або доступності), «низький/*low*» (певні втрати) і «немає/*none*» (відсутність впливу).

3. Сфера застосування (*Scope*): цей показник знаходиться в групі базових показників, хоча він є дещо незалежним від решти груп. Він стосується здатності вразливості в одному компоненті програмного забезпечення впливати на ресурси, що виходять за межі його можливостей, або на привілеї. Прикладом є вразливість у віртуальній машині, яка дозволяє зловмиснику видаляти файли в операційній системі хоста.

Зазвичай базові та часові метрики визначаються аналітиками бюлетенів вразливостей, постачальниками програмних засобів безпеки або програмного забезпечення, оскільки вони мають кращу інформацію щодо характеристик вразливостей, ніж користувачі. Однак показники, що стосуються середовища,

визначаються користувачами, оскільки вони найкраще можуть оцінити потенційний вплив вразливості у своєму власному середовищі.

Група часових метрик представляє характеристики вразливості, які змінюються з часом, але не в середовищі користувача. Він складається з трьох показників. У випадку, коли значення такої метрики «не визначено», цей показник слід пропустити в рівнянні оцінки.

Зрілість коду експлойту оцінює поточний стан методів експлойту або доступність коду. Загальнодоступний простий у використанні код експлойта збільшує кількість потенційних зловмисників, включаючи некваліфікованих осіб, тим самим підвищуючи серйозність вразливості. Рівні відображають ступінь доступності та придатності експлойта для використання вразливості. Рівень виправлення вимірює ступінь доступності виправлення.

Достовірність звіту вимірює ступінь впевненості в існуванні вразливості та достовірність відомих технічних деталей.

Група метрик середовища фіксує характеристики вразливості, пов’язані з *IT*-середовищем користувача. Це дає змогу аналітику налаштувати оцінку *CVSS* залежно від важливості враженого *IT*-активу для організації користувача, виміряного з точки зору конфіденційності, цілісності та доступності.

Висновки

Таким чином, в роботі проведений аналіз стандарту *CVSS* щодо кількісного розрахунку рівня вразливості мережного обладнання та доведена доцільність його використання під час розробки та дослідження перспективних підходів до безпечної маршрутизації у площині даних програмно-конфігурованих мереж.

Список літератури

1. Liu Y., Zhao B., Zhao P., Fan P., Liu H. A survey: Typical security issues of software-defined networking. China Communications. 2019. № 16 (7). pp. 13-31. DOI: https://doi.org/10.23919/JCC.2019.07.002.
2. Sagare A. A., Khondoker R. Security Analysis of SDN Routing Applications. In: Khondoker, R. (eds) SDN and NFV Security. Lecture Notes in Networks and Systems, vol. 30. Springer, Cham, 2018, pp. 1-17. DOI: https://doi.org/10.1007/978-3-319-71761-6_1.
3. 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). pp. 3-14. URL: https://pt.nure.ua/wp-content/uploads/2021/12/212_yeremenko_secure.pdf.
4. Євдокименко М. О., Шаповалова А. С., Шаповал М. М. Потокова модель маршрутизації із врахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Проблеми телекомунікацій. 2020. № 1 (26). С. 48-62. URL: http://pt.nure.ua/wp-content/uploads/2021/03/201_yevdokimenko_security.pdf.
5. Yevdokymenko M., Yeremenko O., Shapovalova A., Shapoval M., Porokhniak V., Rogovaya N. Investigation of the Secure Paths Set Calculation Approach Based on Vulnerability Assessment. Workshop Proceedings of the MoMLeT+DS 2021: 3rd International Workshop on Modern Machine Learning Technologies and Data Science, June 5, 2021, Lviv-Shatsk, Ukraine. pp. 207-217. URL: http://ceur-ws.org/Vol-2917/paper19.pdf.
6. Stallings W. Effective Cybersecurity: Understanding and Using Standards and Best Practices, Addison-Wesley, 2019. 800 p.
7. Common Vulnerability Scoring System v 3.0: Examples, Forum of Incident Response and Security Teams, URL: https://www.first.org/cvss/examples.
8. Lou W., Kwon Y. H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks. IEEE Transactions on Vehicular Technology. 2006. Vol. 55, No. 4. pp. 1320-1330. DOI: https://doi.org/10.1109/TVT.2006.877707.
9. Snihurov A., Chakrian V. Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters. Scholars Journal of Engineering and Technology. 2015. Vol. 3, No. 8. pp. 707-714.

Received (Надійшла) 26.05.2023
Accepted for publication (Прийнята до друку) 16.08.2023

Analysis of vulnerabilities of the SDN data plane and the functional capabilities of the routing tools in relation to preventing potential attacks

A. Levterov, G. Pliekhova, M. Kostikova, S. Ocheretenko

Abstract. Problem. The article is devoted to the analysis of the vulnerabilities of the SDN data plane and the functionality of secure routing tools in terms of countering possible attacks. The main typical security problems, their causes and possible targets of attacks are considered within the data plane. Existing SDN data plane protection technologies are described. A generalized classification of vulnerabilities and their characteristics is provided. **Goal.** The purpose of the article is to analyze the vulnerabilities of the SDN data plane and the functionality of secure routing tools to counter possible attacks. **Methodology**. Analytical modeling, formalization and comparison. Task statement – To improve secure routing taking into account the basic metrics of the criticality of vulnerabilities. **Results.** An analysis of the vulnerabilities of the SDN data plane and the functionality of secure routing tools against possible attacks, as well as the existing technologies and approaches to protect the SDN data plane, has been carried out. Conclusions: Thus, the paper analyzes the CVSS standard for quantitative calculation of the level of vulnerability of network equipment and proves the feasibility of its use during the development and research of promising approaches to secure routing in the data plane of software-configured networks. **Originality.** Systematized and analyzed the vulnerabilities of the SDN data plane and their functionality in terms of secure routing and countermeasures against possible attacks. **Practical value.** Computer-configured SDN networks are considered within the data plane, the main typical security problems are found, their causes and possible objects of attacks are indicated.

Keywords: SDN, metrics, security, vulnerability, CVSS.