DOI: 10.20998/2079-0023.2023.01.02
УДК 004.056.5

А. І. ЛЕВТЕРОВ, кандидат технічних наук, професор, Харківський національний автомобільно-дорожній університет, завідувач кафедри інформатики та прикладної математики; м. Харків, Україна, e-mail: lai@khadi.kharkov.ua, ORCID: https://orcid.org/0000-0001-6586-1061
Г. А. ПЛЄХОВА, кандидат технічних наук, доцент, Харківський національний автомобільно-дорожній університет, доцент кафедри інформатики та прикладної математики; м. Харків, Україна, e-mail: plehovaanna11@gmail.com, ORCID: https://orcid.org/0000-0002-6912-6520
М. В. КОСТІКОВА, кандидат технічних наук, доцент, Харківський національний автомобільно-дорожній університет, доцент кафедри інформатики та прикладної математики; м. Харків, Україна, e-mail: kmv_topaz@ukr.net, ORCID: https://orcid.org/0000-0001-5197-7389
Н. Г. БЕРЕЖНА, кандидат технічних наук, доцент, Державний біотехнологічний університет, доцент кафедри транспортних технологій і логістики; м. Харків, Україна, e-mail: bereg_nat@ukr.net, ORCID: https://orcid.org/0000-0001-8740-3387
А. О. ОКУНЬ, кандидат технічних наук, доцент, Національний технічний університет «Харківський політехнічний інститут», доцент кафедри комп'ютерного моделювання та інтегрованих технологій обробки тиском; м. Харків, Україна, e-mail: okunanton@gmail.com, ORCID: https://orcid.org/0000-0002-6467-4229

ДОСЛІДЖЕННЯ МЕТОДІВ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ У ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ

У сучасному світі безпека мережі є ключовим питанням інформаційної безпеки. Віртуальні мережі стали невід'ємною частиною сучасної IT-інфраструктури, що ставить перед нами виклики у сфері безпеки. Одним з рішень цієї проблеми є використання програмно-визначеної мережі (SDN), яка надає засоби контролю та керування мережевим трафіком. Однак, як і будь-яка технологія, SDN має свої вразливості, які необхідно враховувати під час її розгортання. Одним із інструментів, який допомагає врахувати вразливості мережевої інфраструктури, є стандарт Common Vulnerability Scoring System (CVSS). Це дозволяє кількісно визначити рівень уразливості інфраструктури, що забезпечує ефективний захист мережі. Аналіз стандарту CVSS є важливим етапом у розробці стратегії безпеки мережі. У цій статті аналізуються стандарти для побудови програмно-конфігурованих мереж. Зазначається, що SDN – це сучасний підхід до проектування, побудови та експлуатації інформаційних комунікаційних мереж. Використання SDN дає можливість безпосередньо програмувати та динамічно керувати мережею, а також абстрагувати функціональні можливості рівня інфраструктури. Однак зростання інтересу до SDN виявило недоліки їх застосування в боротьбі із загрозами кібербезпеці. Сама архітектура SDN, зовнішні шкідливі атаки, недостатній контроль доступу та засоби шифрування були визнані основними проблемами безпеки. Запропоновано використання інструментів безпечної маршрутизації на основі показників уразливості для підвищення рівня безпеки мережі площини даних SDN. Відповідно до проведеного аналізу вразливостей площини даних SDN та функціональності інструментів маршрутизації, автори рекомендують використовувати стандарт CVSS для кількісної оцінки рівня вразливості інфраструктури під час розробки та дослідження перспективних підходів до безпечної маршрутизації в площині даних програмно налаштованих мереж.

Ключові слова: SDN, CVSS, вразливість, NFV, площина даних, NVD, програмно-визначена мережа.

Вступ. Розгортання таких мережних архітектур, як програмно-конфігуровані мережі (Software-Defined Networking, SDN), стикається з новими загрозами кібербезпеці, які вимагають розробку та дослідження нових спеціалізованих рішень щодо підвищення рівня мережної безпеки. Незважаючи на високу відкритість і можливості програмованості, архітектура SDN замінює традиційну мережу, проте збільшує кількість потенційних мережних атак, що призводить до нових проблем безпеки.

Саме тому у статті проведений аналіз стандартів побудови програмно-конфігурованих мереж. Крім того, представлено аналіз вразливостей архітектур SDN.

Частина роботи присвячена аналізу вразливостей площини даних SDN і функціональних можливостей засобів маршрутизації щодо протидії можливим атакам. Приділено увагу специфіці еволюції площини даних архітектури SDN, а також існуючим технологіям і підходам захисту площини даних SDN. Показано перспективність використання засобів безпечної маршрутизації на основі базових метрик критичності вразливостей для підвищення рівня мережної безпеки площини даних SDN.

Також проведений аналіз стандарту CVSS щодо кількісного розрахунку рівня вразливості мережного обладнання. Було розглянуто категорії вразливостей, використання національної бази даних вразливостей та загальної системи оцінки вразливостей, метрики загальної системи оцінки вразливостей.

Аналіз публікацій. *Основні стандарти побудови програмно-конфігурованих мереж.* Програмно-конфігуровані мережі є підходом до проектування, побудови та експлуатації інфокомунікаційних мереж шляхом розділення площин управління (control plane) та передавання даних (data plane). Такий розподіл надає мережі безпосередньої програмованості та динамічності, а також дозволяє абстрагувати функціональні можливості рівня інфраструктури.

Сам термін виник ще у середині 1990-х років. Однак лише у 2011 році була заснована Open Networking Foundation для просування SDN, що почала використовувати OpenFlow як ключовий протокол для опису того, як керувати мережею та вносити відповідні

зміни стандартизованим способом. Наразі OpenFlow – лише один з прикладів із множини протоколів взаємодії SDN контролерів і пристроїв площини даних, і для надання можливостей SDN можна використовувати інші механізми зв'язку [1].

Існують різні архітектури, що відокремлюють логіку управління від ресурсів поза пристроєм, але всі підходи до побудови SDN включають контролер SDN і відповідні прикладні програмні інтерфейси – Southbound API та Northbound API (рис. 1).

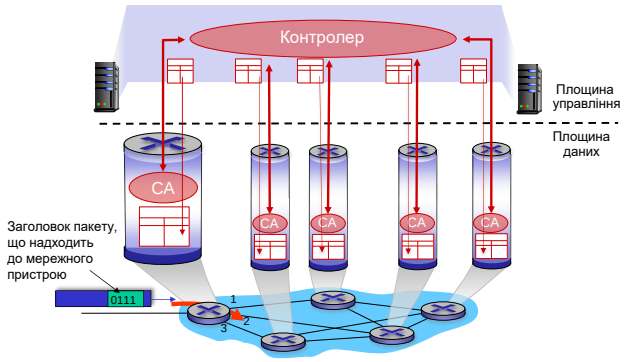


Рис. 1. Базова архітектура програмно-конфігурованої мережі [2]

Рис. 2. Концепція віртуалізації мережних функцій [1]

Зі свого боку віртуалізація мережних функцій (Network Functions Virtualization, NFV) є стандартизованим способом розробки, впровадження та керування мережними службами. Дана концепція передбачає заміну спеціальних пристроїв для мережної інфраструктури, таких як маршрутизатори та брандмауери, стандартними серверами, комутаторами, сховищем, хмарою або навіть туманною обчислювальною інфраструктурою [1]. NFV відокремлює такі функції мережі, як маршрутизація, комутація та безпека, від пропрієтарних або виділених апаратних пристроїв, щоб дозволити їм працювати в межах програмного забезпечення.

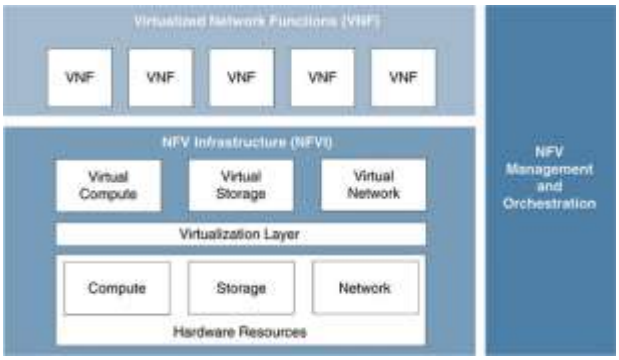
Головна мета використання NFV полягає в тому, щоб використовувати стандартні технології віртуалізації для консолідації апаратного забезпечення та віртуалізації мережних функцій у блоки, які можна об'єднувати для створення наскрізних комунікаційних послуг. Це може бути реалізовано для будь-якої функції площини управління або площини даних у середовищі як проводових, так і безпроводових мереж.

NFV з'явився в 2012 році, коли сім провідних глобальних постачальників мережних послуг об'єдналися під Групою галузевих специфікацій (Industry Specification Group, ISG) ETSI для NFV [1]. Це основна група для розробки вимог та архітектури для віртуалізації різних функцій в інфокомунікаційних мережах і для архітектурних стандартів NFV, зокрема NFV MANO (Management and Orchestration), який став стандартом де-факто для NFV.

Отже, NFV складається з трьох основних компонентів [1]:

- Віртуалізовані мережні функції (Virtualized Network Functions, VNF) – мережні функції, які реалізовані в програмному забезпеченні та можуть бути розгорнуті в інфраструктурі віртуалізації мережних функцій (Network Functions Virtualization Infrastructure, NFVI).
- NFVI – загальні апаратні та програмні компоненти, де розгортаються VNF.
- Середовище керування та оркестровки NFV (Management and Orchestration, MANO) – архітектурний фреймворк, що містить функціональні блоки, сховища даних, що використовуються цими блоками, та інтерфейси, через які функціональні блоки обмінюються інформацією з метою управління та оркестрації NFVI та VNF.

З концепцією віртуалізації мережних функцій можна ознайомитися на рис. 2.



Нижче наведено добірку ключових груп розробників стандартів тісно пов'язаних передових технологічних областей NFV і SDN:

- Фокус група SDN і NFV Alliance for Telecommunications Industry Solutions (ATIS) було створено в січні 2014 року з метою об'єднання сервісів апаратного забезпечення/пристроїв NFV за допомогою концепції SDN, а також розробки API для інтерфейсів та OAM для зв'язування служб OpenStack та OpenDaylight [3].
- Broadband Forum (BBF) працює як з SDN, так і з NFV, зосереджуючись на наданні хмарного широкосмугового з'єднання та NFV. У 2017 році BBF уклав меморандум про взаєморозуміння (MoU) з SDN/NFV Industry Alliance [4].
- ETSI є головним глобальним рушієм стандартизації NFV [5].
- Інститут інженерів з електротехніки та електроніки (Institute of Electrical and Electronics Engineers, IEEE) займається стандартизацією SDN у межах дослідницьких груп, що вивчають можливості стандартизації в програмно-конфігурованих мережах, віртуалізації мережних функцій і суміжних областях [6].
- Міжнародна рада з великих електричних систем (International Council on Large Electrical Systems, CIGRE) має робочу групу, діяльність якої зосереджена на розробці стандарту IEEE P1915.1, що визначає структуру безпеки, моделей, аналітики та вимог для SDN/NFV [7]. CIGRE розглядає моделі безпеки, термінологію та аналітику (основні компоненти середовищ

SDN і NFV), щоб забезпечити конфіденційність, цілісність і доступність.

- Сектор стандартизації телекомунікацій Міжнародного союзу електрозв'язку (International Telecommunication Union Telecommunication Standardization Sector, ITU-T) зосередився на SDN з листопада 2012 року. ITU-T прийняв резолюцію 77, щоб просувати стандартизацію в SDN, а також виконує роботу, орієнтовану на SDN, у групі WTSA-12 [8].
- Internet Engineering Taskforce (IETF) працює як над SDN (через RFC 7426 SDN), так і над новою групою стандартів IETF SDN (I2RS), зосередившись на протоколах програмування Southbound, NFV і мережних послуг [9].
- Internet Research Task Force (IRTF) має групу SDN, метою якої є надання переваг усім типам мереж, включаючи безпроводові, мобільні, домашні, корпоративні, центри обробки даних і глобальні мережі [10]. Дослідницька група програмно-визначених мереж (Software-Defined Networking Research Group, SDNRG) прагне визначити підходи, які можна розгорнути та використати найближчим часом, а також завдання майбутніх досліджень. Основні сфери інтересів включають масштабованість рішень, абстракції, мови програмування та парадигми, які особливо корисні в контексті SDN.
- Internet Society (ISOC) має групи IRTF і IETF, які зосереджуються на NFV і SDN і забезпечують архітектурний нагляд за Internet Architecture Board (IAB) [11].
- Metro Ethernet Forum (MEF), заснований у 2001 році, сприяє створенню нейтральних для промисловості середовищ для оркестровки послуг (OpenLSO) і служб підключення L2–L7 (OpenCS) на основі SDN і NFV [12].
- Альянс відкритих центрів даних (Open Data Centre Alliance, ODCA) був створений у жовтні 2010 року. ODCA керує об'єднаною хмарною архітектурою зі спільними стандартами як для апаратного, так і для програмного забезпечення [13].
- OpenDaylight Foundation була заснована в 2013 році і просуває платформу SDN з відкритим кодом для створення програмованих і гнучких мереж [14].
- Open Networking Foundation (ONF) – некомерційна організація, орієнтована на користувачів, яка прагне прискорити впровадження SDN і NFV. ONF дійсно стимулював рух SDN у 2011 році, а у 2017 році ONF оголосив Open Innovation Pipeline, щоб спрямувати галузь до наступного покоління SDN і NFV [15].
- Відкрита платформа для NFV (Open Platform for NFV, OPNFV), сформована в 2014 році фондом Linux, сприяє розробці та еволюції компонентів NFV для екосистем з відкритим кодом [16].
- Optical Internetworking Forum (OIF) має робочу групу з архітектури та сигналізації, яка визначає інтерфейси для SDN [17].

Специфіка еволюції площини даних архітектури SDN. 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 інше. У межах роботи проаналізовано типові проблеми безпеки та об'єкти атак у межах площини даних – мережних пристроїв, що керуються контролером SDN. Результати аналізу наведено в табл. 1. Очевидно, що об'єктами атаки можуть бути пристрої різних рівнів мережі, і відповідно до чіткої багаторівневої архітектури SDN можна класифікувати загрози безпеці на різних рівнях з урахуванням підвищення.

Отже, площина даних складається з комутаторів та інших мережних 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. Типові проблеми безпеки у площині даних розглядаються відповідно до наступного [18]:

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

Таблиця 1 – Загальна класифікація метрик CVSS [23]

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

Правомірність правил потоків стосується зловмисного або невірного впровадження правил потоків. Зі свого боку узгодженість правил потоків в основному включає три аспекти [18]. 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.

- 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 [18]. 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.
- Атака сторонніми каналами. SDN весь час переносить приватну та конфіденційну інформацію [18]. 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, основними причинами проблем безпеки є власне архітектура SDN, зовнішні шкідливі атаки, недостатність контролю доступу та засобів шифрування.

Мета та постановка задачі. Об'єктом дослідження є процес забезпечення мережної безпеки у програмно-конфігурованих мережах засобами маршрутизації.

Предмет дослідження – це стандарти побудови програмно-конфігурованих мереж (SDN), стандарт Common Vulnerability Scoring System (CVSS) щодо кількісного розрахунку рівня вразливості мережного обладнання, функціональні можливості протоколів IP-маршрутизації.

Мета роботи – аналіз стандартів побудови програмно-конфігурованих мереж, стандарту CVSS, функціональних можливостей протоколів IP-маршрутизації.

В роботі використані наступні методи досліджень: формалізація, порівняння.

Дана робота присвячена аналізу загроз, об'єктів атак і потенційних рішень щодо підвищення рівня мережної безпеки у площині даних SDN мереж засобами маршрутизації.

Аналіз вразливостей архітектур SDN. Завдяки зростаючому інтересу до SDN та широкому розгортанню програмно-конфігурованих мереж поступово виявляються їхні недоліки у боротьбі із загрозами кібербезпеці. Відповідно питання щодо безпеки тісно пов'язані з характеристиками SDN. Згідно з дослідженнями [18, 19], наступні аспекти роблять програмно-конфігуровані мережі вразливими до атак:

- SDN контролер, що відповідає за централізований контроль мережею, має недостатні механізми захисту, через що стає ціллю зовнішніх зловмисних атак.
- У процесі складної взаємодії пов'язаних між собою різноманітних прикладних програм і мережних застосунків між ними часто виникають конфлікти у правилах передавання потоків у межах площини даних.
- Відсутність належних механізмів авторизації та автентифікації прикладних програм робить їх вразливими для атак з використанням зловмисного програмного забезпечення.
- Існує певна недостатність засобів безпеки та шифрування в процесі комунікації між площиною управління та площиною даних. Отже, правила передавання потоків (flow rules) вразливі щодо зловмисного втручання під час їхньої публікації.

У межах архітектури SDN реалізуються окремі рівні щодо площини управління та площини даних на відміну від традиційних мереж, де ці площини функціонують в єдиному пристрої. Площина управління формулює правила потоків, а площина даних зі свого боку відповідає лише за пересилання пакетів даних відповідно до правил потоків. У той же час контролер мережі може отримати статус кожного пристрою через південний інтерфейс (Southbound Interface, SBI), щоб мати глобальне уявлення про стан мережі. Таке функціональне розділення в архітектурах SDN значно підвищує гнучкість мереж, але також створює нові загрози безпеці, які переважно відображаються в наступних двох аспектах [18]:

- Вибірковий дозвіл пристроїв захисту. SDN – це мережа, що керується правилами потоків, де фізичний пристрій захисту не має права прийняття рішень. Саме правила потоків визначають, чи будуть пакети даних передаватися через пристрій захисту та коли саме. Таким чином, в SDN зловмисник може обійти пристрої захисту, що призведе до збою заходів безпеки перед розгортанням мережі.
- Автоматичне отримання глобального уявлення про стан мережі. В SDN контролер, як командний і контрольний центр усієї мережі, може створити глобальне уявлення про мережу. Він може отримувати різноманітну інформацію про стан мережі в режимі реального часу. Таким чином, інформацію щодо стану безпеки мережі можна легко отримати від контролера. Отже, зловмисники можуть дістати глобальне уявлен-

ня про мережу безпосередньо від контролера, очікуючи найкращої нагоди для масштабної атаки.

Технології та підходи захисту площини даних SDN. 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.

- Виявлення помилок у мережі може бути реалізовано за допомогою алгоритмів виявлення. Так, наприклад, NICE [18] 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.
- 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.
- 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 [18].
- Модуль автентифікації й авторизації може використовувати сервер RADIUS для автентифікації ідентифікатора хоста. Крім того, можливе застосування квантової криптографії для розробки надлегкої верифікації цілісності [18]. Зазначається, що квантові паролі є більш безпечними, ніж традиційні, проте їхнє впровадження може бути дорожчим.
- Захист від DoS/DDoS-атак у площині даних може бути трансформована в задачу оптимізації таблиці потоків.

Засоби безпечної маршрутизації для підвищення рівня мережної безпеки площини даних SDN. На сьогоднішній день важливе місце у комплексі засобів підвищення мережної безпеки, у тому числі мереж SDN, відводиться протоколам маршрутизації, які потребують системної та скоординованої взаємодії одночасно множини мережних елементів – SDN-комутаторів, і контролерів мережі під час формування (розрахунку) шляхів і правил потоків, вздовж яких має забезпечуватися необхідний рівень безпеки за обраними показниками або критеріями.

Отже, у напрямку безпечної маршрутизації проведено значну кількість теоретичних досліджень, починаючи від найпростіших емпіричних варіантів рішень до системних оптимізаційних підходів.

Так, у роботі [20] 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 з балансуванням навантаження з адитивною метрикою враховує продуктивність і безпеку мережі, дозволяє ефективніше використовувати наявні мережні ресурси, але також враховує ймовірність компрометації каналів зв'язку під час прийняття маршрутних рішень.

Тоді як у роботах [21, 22] пропонуються потокові моделі маршрутизації з врахуванням 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. У моделі [21] для розрахунку маршрутних метрик використовуються вирази, які характеризують ризик інформаційної безпеки в каналах зв'язку мережі та відповідно до рекомендацій NIST враховують збитки від порушення конфіденційності та цілісності інформації, доступності мережного ресурсу у випадку використання наявних вразливостей; показники складності використання вразливостей на вузлах мережі та отримання доступу до мережних елементів та мережі загалом внаслідок використання зазначених вразливостей. Запропонований авторами підхід до формування маршрутних метрик може бути використаний під час комплексного врахування в процесі розв'язання задач маршрутизації як показників мережної безпеки, так і показників якості обслуговування.

Аналіз стандарту CVSS щодо кількісного розрахунку рівня вразливості мережного обладнання. 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

Таблиця 2 – Існуючі технології безпеки у площині даних SDN [18]

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

системи, проектуванні, реалізації або внутрішніх засобах контролю, які можуть бути випадково активовані або навмисно використані під час виявлення загрози. Отже, далі розглянуто категорії вразливостей та проаналізовано підходи до ідентифікації та документування вразливостей, а також обговорено використання національної бази даних вразливостей – National Vulnerability Database (NVD).

Категорії вразливостей. Узагальнена класифікація вразливостей може бути представлена наступним чином [23]:

- 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.
- Вразливості, спричинені діяльністю людини: залежність від певних осіб, прогалини в обізнаності та навчанні, прогалини в дисципліні та неправомірне обмеження доступу.
- Фізичні вразливості та вразливості середовища: недостатній контроль (фізичного) доступу, невдале розміщення обладнання, невідповідний контроль температури/вологості та неналежне кондиціювання у приміщеннях, де знаходиться обладнання.
- 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.
- 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.

Національна база даних вразливостей та загальна система оцінки вразливостей. 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 [21–25]. 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 [21, 22].

Кожен запис NVD містить наступну інформацію [20]:

- 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 [23]. У табл. 3 перелічені окремі показники та показані 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 віддаленіша атака, тим більше джерел атаки можливе, а отже, тим серйозніша вразливість. Ця інформація є безцінною, оскільки дозволяє користувачам зрозуміти характеристики вразливості.

Як показано в табл. 3, кожен рівень метрики має описову назву [23]. 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.

Таблиця 3 – Загальна класифікація метрик CVSS [23]

Група базових метрик		Група часових метрик	Група базових метрик
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			

Базова група метрик представляє внутрішні характеристики вразливості, які є незмінними протягом часу та серед користувачів. Він складається з трьох наборів показників [23]:

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 вразливого 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 ураженого IT-активу для

організації користувача, виміряного з точки зору конфіденційності, цілісності та доступності.

Висновки. Таким чином, у даній роботі було проаналізовано стандарти побудови програмно-конфігурованих мереж. Зазначено, що SDN є сучасним підходом до проектування, побудови та експлуатації інфокомунікаційних мереж шляхом розділення площин управління та передавання даних. Завдяки такому розподілу мережі набувають безпосередньої програмованості та динамічності, а також абстрагування функціональних можливостей рівня інфраструктури. Крім того, віртуалізація мережних функцій стала стандартизованим способом розробки, впровадження та керування мережними службами. Дана концепція передбачає заміну спеціальних пристроїв мережної інфраструктури, таких як маршрутизатори та брандмауери, стандартними серверами, комутаторами, сховищем, хмарою.

Проте, зростаючий інтерес до SDN та їхнього розгортання дозволили виявити їхні недоліки у боротьбі із загрозами кібербезпеці. На сучасному етапі розвитку архітектур SDN доведено, що типові проблеми безпеки у програмно-конфігурованих мережах перш за все проявляються в таких аспектах, як шкідливе програмне забезпечення, вразливість контролера, легітимність та узгодженість правил потоків, проблема стандартизації північного інтерфейсу, безпека комунікації в процесі використання південного інтерфейсу. Таким чином, основними причинами проблем безпеки є власне архітектура SDN, зовнішні шкідливі атаки, недостатність контролю доступу та засобів шифрування. Базуючись на дослідженнях типових проблем безпеки, стає очевидним, що централізоване керування та функції програмованості SDN надають зловмисникам потужні та зручні канали атак.

Проведений аналіз вразливостей площини даних SDN і функціональних можливостей засобів маршрутизації щодо протидії можливим атакам показав перспективність використання засобів безпечної маршрутизації на основі базових метрик критичності вразливостей для підвищення рівня мережної безпеки площини даних SDN.

Аналіз стандарту CVSS щодо кількісного розрахунку рівня вразливості мережного обладнання довів доцільність його використання під час розробки та дослідження перспективних підходів до безпечної маршрутизації у площині даних програмно-конфігурованих мереж.

Список використаної літератури

1. 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*. Cisco Press, 2018. 1008 p.
2. Kurose J. F., Ross K. *Computer networking*. 8th Edition. Pearson, 2020 775 p.
3. *The Alliance for Telecommunications Industry Solutions (ATIS)*. URL: http://www.atis.org/ (дата звернення: 03.05.2023).
4. *The Broadband Forum Member (BBF)*. URL: https://www.broadband-forum.org/ (дата звернення: 03.05.2023).
5. *The European Telecommunications Standards Institute (ETSI)*. URL: http://www.etsi.org/technologies-clusters/technologies/nfv (дата звернення: 03.05.2023).
6. *The Institute of Electrical and Electronics Engineers (IEEE)*. URL: https://sdn.ieee.org/ (дата звернення: 03.05.2023).
7. *The International Council on Large Electrical Systems (CIGRE)*. URL: http://www.cigre.org/ (дата звернення: 03.05.2023).
8. *The International Telecommunication Union Telecommunication Standardization Sector (ITU-T)*. URL: http://www.itu.int/en/ITU-T/sdn/Pages/default.aspx (дата звернення: 03.05.2023).
9. *The Internet Engineering Taskforce (IETF)*. URL: https://ietf.org (дата звернення: 03.05.2023).
10. *The Internet Research Task Force (IRTF)*. URL: https://irtf.org/concluded/sdnrg (дата звернення: 03.05.2023).
11. *The Internet Society (ISOC)*. URL: https://www.internetsociety.org/ (дата звернення: 03.05.2023).
12. *The Metro Ethernet Forum (MEF)*. URL: https://mef.net/ (дата звернення: 03.05.2023).
13. *The Open Data Centre Alliance (ODCA)*. URL: https://opendatacenteralliance.org/ (дата звернення: 03.05.2023).
14. *OpenDaylight*. URL: https://www.opendaylight.org/ (дата звернення: 03.05.2023).
15. *The Open Networking Foundation (ONF)*. URL: https://www.opennetworking.org/ (дата звернення: 03.05.2023).
16. *The Open Platform for NFV (OPNFV)*. URL: https://www.opnfv.org (дата звернення: 03.05.2023).
17. *The Optical Internetworking Forum (OIF)*. URL: http://www.oiforum.com/ (дата звернення: 03.05.2023).
18. Liu Y., Zhao B., Zhao P., Fan P., Liu H. A survey: Typical security issues of software-defined networking. *China Communications.* 2019. Vol. 16(7). P. 13–31.
19. Sagare A. A., Khondoker R. Security analysis of SDN routing applications. *SDN and NFV Security. Lecture Notes in Networks and Systems*. Springer, Cham, 2018. Vol. 30. P. 1–17.
20. 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.
21. 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.
22. 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. P. 207-217.
23. Stallings W. *Effective Cybersecurity: Understanding and Using Standards and Best Practices*. Addison-Wesley, 2019. 800 p.
24. Common Vulnerability Scoring System v3.0: Examples, Forum of Incident Response and Security Teams. URL: https://www.first.org/cvss/examples (дата звернення: 03.05.2023).
25. NIST National Vulnerability Database, URL: https://nvd.nist.gov (дата звернення: 03.05.2023).

References (transliterated)

1. 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*. Cisco Press, 2018, 1008 p.
2. Kurose J. F., Ross K. *Computer networking.* 8th Edition. Pearson, 2020. 775 p.
3. *The Alliance for Telecommunications Industry Solutions (ATIS)*. URL: http://www.atis.org/ (accessed 03.05.2023).
4. *The Broadband Forum Member (BBF)*. URL: https://www.broadband-forum.org/ (accessed 03.05.2023).
5. *The European Telecommunications Standards Institute (ETSI)*. URL: http://www.etsi.org/technologies-clusters/technologies/nfv (accessed 03.05.2023).
6. *The Institute of Electrical and Electronics Engineers (IEEE)*. URL: https://sdn.ieee.org (accessed 03.05.2023).
7. *The International Council on Large Electrical Systems (CIGRE)*. URL: http://www.cigre.org/ (accessed 03.05.2023).
8. *The International Telecommunication Union Telecommunication Standardization Sector (ITU-T)*. URL: http://www.itu.int/en/ITU-T/sdn/Pages/default.aspx (accessed 03.05.2023).
9. *The Internet Engineering Taskforce (IETF)*. URL: https://ietf.org.

10. *The Internet Research Task Force (IRTF)*. URL: https://irtf.org/concluded/sdnrg (accessed 03.05.2023).
11. *The Internet Society (ISOC)*. URL: https://www.internetsociety.org/ (accessed 03.05.2023).
12. *The Metro Ethernet Forum (MEF)*. URL: https://mef.net/ (accessed 03.05.2023).
13. *The Open Data Centre Alliance (ODCA)*. URL: https://opendatacenteralliance.org/ (accessed 03.05.2023).
14. *OpenDaylight*. URL: https://www.opendaylight.org/ (accessed 03.05.2023).
15. *The Open Networking Foundation (ONF)*. URL: https://www.opennetworking.org/ (accessed 03.05.2023).
16. *The Open Platform for NFV (OPNFV)*. URL: https://www.opnfv.org.
17. The Optical Internetworking Forum (OIF). URL: http://www.oiforum.com/ (accessed 03.05.2023).
18. Liu Y., Zhao B., Zhao P., Fan P., Liu H. A survey: Typical security issues of software-defined networking. *China Communications*. 2019, vol. 16(7), pp. 13–31.
19. Sagare A. A., Khondoker R. Security analysis of SDN routing applications. *SDN and NFV Security. Lecture Notes in Networks and Systems*. Springer, Cham, 2018, vol. 30, pp. 1–17.
20. Yeremenko O., Persikov M., Lemeshko V., Altaki B. Research and development of the secure routing flow-based model with load balancing. Problemy telekomunikatsii [Telecommunication Problems]. 2021, no. 2(29), pp. 3–14.
21. Yevdokymenko M., Shapovalova A., Shapoval M. Potokova model marshrutyzatsii iz vrakhuvanniam ryzykiv informatsiinoi bezpeky za dopomohoiu bazovykh metryk krytychnosti vrazlyvostei [Flow model of routing taking into account information security risks using basic vulnerability criticality metrics]. Problemy telekomunikatsii [Telecommunication Problems]. 2020, no. 1(26), pp. 48–62.
22. 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.
23. Stallings W. *Effective Cybersecurity: Understanding and using standards and best practices*. Addison-Wesley, 2019. 800 p.
24. Common Vulnerability Scoring System v3.0: Examples, Forum of Incident Response and Security Teams. URL: https://www.first.org/cvss/examples (accessed 03.05.2023).
25. NIST National Vulnerability Database, URL: https://nvd.nist.gov (accessed 03.05.2023).

Надійшла (received) 10.05.2023

UDC 004.056.5

A. I. LEVTEROV, Candidate of Technical Sciences, Professor, Kharkiv National Automobile and Highway University, Head of the Department of Informatics and Applied Mathematics, Kharkiv, Ukraine, e-mail: lai@khadi.kharkov.ua, ORCID: https://orcid.org/0000-0001-6586-1061
H. A. PLIEKHOVA, Candidate of Technical Sciences, Docent, Kharkiv National Automobile and Highway University, Associate Professor at the Department of Informatics and Applied Mathematics, Kharkiv, Ukraine, e mail: plehovaanna11@gmail.com, ORCID: https://orcid.org/0000-0002-6912-6520
M. V. KOSTIKOVA, Candidate of Technical Sciences, Docent, Kharkiv National Automobile and Highway University, Associate Professor at the Department of Informatics and Applied Mathematics, Kharkiv, Ukraine, e mail: kmv_topaz@ukr.net, ORCID: https://orcid.org/0000-0001-5197-7389
N. G. BEREZHNA, Candidate of Technical Sciences, Docent, State Biotechnological University, Associate Professor at the Department of Transport Technologies and Logistics, Kharkiv, Ukraine, e mail: bereg_nat@ukr.net, ORCID: https://orcid.org/0000-0001-8740-3387
A. O. OKUN, Candidate of Technical Sciences, Docent, National Technical University "Kharkiv Polytechnic Institute", Associate Professor at the Department of Computer Modeling and Integrated Forming Technologies, Kharkiv, Ukraine, e mail: okunanton@gmail.com, ORCID: https://orcid.org/0000-0002-6467-4229

ENHANCING SECURITY IN SOFTWARE-DEFINED NETWORKING THROUGH ROUTING TECHNIQUES EXPLORATION

In today's world, network security is a key issue of information security. Virtual Networks have become an integral part of modern IT infrastructure, which presents us with challenges in the field of security. One solution to this problem is the use of software-defined networking (SDN), which provides a means to control and manage network traffic. However, as with any technology, SDN has its vulnerabilities that must be considered when deploying it. One of the tools that helps to take into account the vulnerabilities of network infrastructure is the Common Vulnerability Scoring System (CVSS) standard. It allows you to quantify the level of vulnerability of the infrastructure, which enables effective network protection. Analysis of the CVSS standard is an important stage in the development of a network security strategy. This paper analyzes the standards for building software-configured networks. It is noted that SDN is a modern approach to the design, construction, and operation of information communication networks. Using SDN makes it possible to directly program and dynamically manage the network, as well as to abstract the functionality of the infrastructure layer. However, the growing interest in SDN has revealed the shortcomings of their application in the fight against cybersecurity threats. The SDN architecture itself, external malicious attacks, and insufficient access control and encryption tools were found to be the main security challenges. The use of secure routing tools based on vulnerability metrics is proposed to increase the level of SDN data plane network security. According to the conducted analysis of SDN data plane vulnerabilities and the functionality of routing tools, the authors recommend using the CVSS standard to quantify the level of infrastructure vulnerability during the development and research of promising approaches to secure routing in the data plane of software-configured networks.

Keywords: SDN, CVSS, vulnerability, NFV, data plane, NVD, Software-Defined Networking.

Повні імена авторів / Author's full names

Автор 1 / Author 1: Левтеров Андрій Іванович, Levterov Andrii Ivanovych
Автор 2 / Author 2: Плєхова Ганна Анатоліївна, Pliekhova Hanna Anatoliivna
Автор 3 / Author 3: Костікова Марина Володимирівна, Kostikova Maryna Volodymyrivna
Автор 4 / Author 4: Бережна Наталія Георгіївна, Berezhna Nataliia Heorhiivna
Автор 5 / Author 5: Окунь Антон Олександрович, Okun Anton Oleksandrovych