

<https://doi.org/10.31891/2307-5732-2025-355-1>

УДК 654:681.5:004.3:004.7/.8:007.5

БАНАР АНАТОЛІЙ

Чернівецький національний університет імені Юрія Федьковича

<https://orcid.org/0009-0006-7817-2058>e-mail: banar.anatolii@chnu.edu.ua**ВОРОБЕЦЬ ГЕОРГІЙ**

Чернівецький національний університет імені Юрія Федьковича

<https://orcid.org/0000-0001-8125-2047>e-mail: g.vorobets@chnu.edu.ua

ПЕРСПЕКТИВНІ НАПРЯМИ РОЗВИТКУ, УДОСКОНАЛЕННЯ І ЗАСТОСУВАНЬ МЕРЕЖІ SDN НА ОСНОВІ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ

Розглянуто сучасні підходи і методи вдосконалення та розвитку програмно-визначених мереж (SDN) з використанням методів штучного інтелекту (ШІ). Зокрема, проаналізовано підходи до оптимізації мережевої архітектури шляхом інтеграції машинного навчання та алгоритмів глибокого навчання для адаптивного управління мережею та балансування трафіку. Досліджено вплив використання інтелектуальних методів для підвищення продуктивності SDN, зокрема динамічного перерозподілу ресурсів, автоматичного налаштування параметрів мережі та забезпечення її безпеки.

Окрему увагу приділено можливостям застосування SDN у сучасних телекомунікаційних та інформаційних системах, зокрема в інфраструктурі Інтернету речей (IoT), промислових мережах та транспортних системах «розумного міста» (Smart City). Розглянуто роль SDN у забезпеченні якості обслуговування (QoS) та покращенні якості користувацького досвіду (QoE), що є критично важливим для оцінки роботи розподілених цифрових сервісів.

Результати дослідження демонструють, що застосування алгоритмів ШІ в SDN сприяє автоматизації процесів прийняття рішень, забезпечує ефективне управління потоками трафіку та дозволяє адаптивно реагувати на зміни мережевого середовища. Це відкриває перспективи використання SDN у таких сферах, як розумне місто, системи захисту інформаційної інфраструктури та управління критично важливими сервісами в режимі реального часу. Також, інтеграція методів ШІ в SDN може покращити показники QoS та QoE.

Ключові слова: програмно-визначені мережі, штучний інтелект, машинне навчання, балансування трафіку, оптимізація мережевих ресурсів.

BANAR ANATOLII, HEORHII VOROBETS

Yuriy Fedkovych Chernivtsi National University

PROMISING DIRECTIONS FOR DEVELOPING, IMPROVING AND APPLICATION SDN NETWORKS BASED ON ARTIFICIAL INTELLIGENCE METHODS

This article explores promising directions for developing and enhancing Software-Defined Networking (SDN) using artificial intelligence (AI) methods. Software-Defined Networking (SDN) represents a modern networking approach that decouples control functions from data forwarding mechanisms, thereby enabling centralized oversight and flexible reconfiguration of network components. However, in conditions of limited resources, such as computing power, memory, or bandwidth, traditional SDN approaches face significant challenges in maintaining performance, security, and adaptability.

The study emphasizes the integration of machine learning (ML) algorithms for solving tasks related to access control, intelligent traffic distribution, detection of anomalies, and efficient allocation of cloud and edge resources. Particular attention is given to lightweight AI models that can operate on conventional hardware without requiring specialized equipment. Several practical cases are considered, including the use of clustering and classification algorithms to support decision-making in resource-constrained SDN nodes.

The paper also analyses the benefits of AI for improving the resilience and scalability of SDN controllers, including support for distributed intelligence and partial decentralization of control logic. This is especially relevant for hybrid infrastructures where centralized cloud services coexist with edge computing devices. Additionally, the article discusses the potential of AI in reducing energy consumption, enhancing quality of service (QoS), and enabling predictive analytics in dynamic network environments.

The results of this research highlight the relevance of AI-driven SDN for future communication systems, particularly in scenarios where access to computing and network resources is limited. The proposed approaches contribute to the vision of building smarter, more adaptive, and resource-efficient software-defined infrastructures.

Keywords: Software-Defined Networks, Artificial Intelligence, Machine Learning, Traffic Balancing, network resource optimization.

Стаття надійшла до редакції / Received 23.04.2025

Прийнята до друку / Accepted 26.05.2025

Вступ

Мережеві технології все частіше використовують в сучасному світі як для персональних потреб, так і для вирішення професійних задач. Збільшення кількості користувачів у сегменті WEB-сервісів потребує нарощування мережевої інфраструктури. Відповідно, виникає необхідність більш гнучкого і адаптивного управління мережами, зокрема застосування інтелектуальних (Smart) методів конфігурування мережевих комунікацій, балансування трафіку [1] і навантаження транзитних і кінцевих (Host) комп'ютерів, прогнозування потреб і потужностей апаратних ресурсів. Реалізація таких методів перспективна на основі застосування алгоритмів штучного інтелекту [2, 3].

SDN є одним з сучасних підходів в інформаційних технологіях, спрямованих на подолання вказаних викликів. Основною перевагою SDN порівняно з традиційними мережами є гнучкість управління. SDN

дозволяє динамічно змінювати налаштування мережі через програмний інтерфейс, що забезпечує можливість адаптовувати в реальному часі мережу відповідно до нових вимог і оптимізовувати доступ до обмежених ресурсів. ШІ, включаючи машинне навчання (ML) та глибоке навчання (DL), вважається перспективним інструментом для реалізації більш ефективних та автономних систем управління. Це досягається застосуванням прогностичних моделей адаптивного управління мережевими структурами, в тому числі шляхом їх реконфігурування. Незважаючи на численні переваги, що приносить SDN, питання оптимізації та безпеки, трансляції даних, телекомунікаційного трафіку, технологічної і сервісної інформації для засобів інтернету речей промислових систем, завжди залишаються актуальними.

Аналіз літературних джерел

Основною ідеєю SDN є розділення площини даних від площини управління, що вперше застосовано в телефонних мережах загального користування [4], ще задовго до спроб застосувати її для мереж передачі даних. Робоча група з питань інженерії інтернету (IETF) в 2004 році працювала над дослідженням методів розділення операцій управління і передачі даних, деякі із запропонованих ідей на той час не отримали належного визнання. Одною з причин була думка, що відокремлення управління від даних є небезпечною ініціативою, через можливість збою у площині управління. Іншою причиною стали побоювання виробників, що створення спільного прикладного програмного інтерфейсу (API) може призвести до збільшення конкурентного тиску на їх продукти. Дослідження факультету комп'ютерної інженерії Стенфордського університету створили прецедент використання відкритого програмного забезпечення у проєктах з розділеними площинами управління та даних. Як результат – з'явився OpenFlow протокол, завдяки дизайну комутаторів (Рис. 1), які дозволяли мережевим контролерам визначати шлях мережових пакетів.

Зважаючи на відносну новизну даного типу мереж, і той факт що в першу чергу SDN-підхід дозволяє реалізувати програмоване управління ресурсами, тим самим підтримуючи більшу гнучкість і маневреність з точки зору конфігурації, моніторингу та продуктивності – безпека в SDN є важливою та складною проблемою [5], яка потребує уваги від усіх зацікавлених сторін. SDN створює нові можливості для атак на різні рівні архітектури, які можуть мати серйозні наслідки для функціонування та надійності. У цьому випадку гарантування безпеки є безперервним процесом навчання та адаптації.

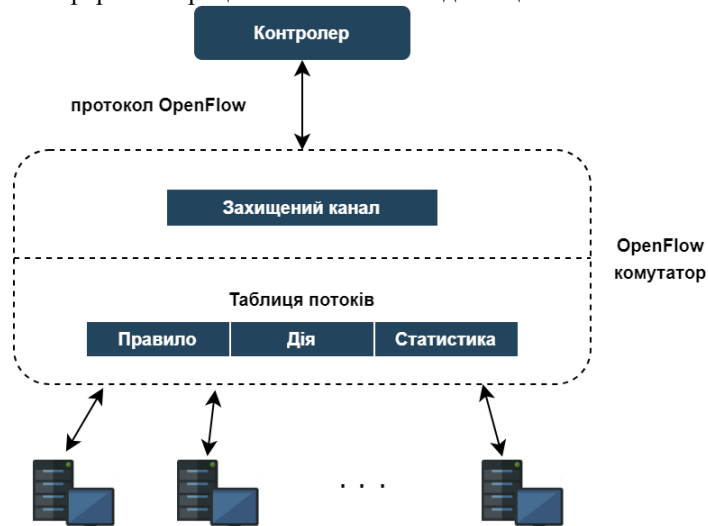


Рис. 1. Архітектура комутатора OpenFlow

Програмно визначені мережі змінюють підходи до безпеки, пропонуючи централізоване управління та програмованість, які підвищують гнучкість у виявленні та реагуванні на загрози [6]. Використання SDN також уможливорює нові типи атак, зокрема, спрямованих на контролери та комунікаційні протоколи між площинами даних та керування. Рішення для захисту SDN включають розширені системи запобігання вторгненням (IPS) та системи виявлення вторгнень (IDS), інтегровані з централізованим управлінням такого типу мереж. Розробка нових методів захисту, які враховують унікальну архітектуру SDN, є актуальною задачею [7], через необхідність протидіяти атакам на контролери та інші компоненти системи. Також, важливо розробляти нові стратегії для протидії DDoS-атакам, спуфінгу, атак на рівні даних і програм, а також безпеці комунікацій між рівнями SDN архітектури та забезпечення цілісності даних. Ефективний розвиток таких мереж потребує постійного аналізу можливих загроз і впровадження комплексних підходів до безпеки, які поєднують технічні та організаційні заходи.

Сучасний розвиток ШІ дає можливість інтеграції його в різні технологічні сфери, особливо у сферах автоматизації та оптимізації процесів. Перспектива застосування ШІ в SDN відкриває можливості для підвищення адаптивності мереж у відповідності до умов роботи, що динамічно змінюються, забезпечуючи глибший аналіз та прогнозування мережевого трафіку. До прикладу, ШІ в мережах 6G [8, 9] є ключовим фактором для підвищення ефективності, надійності та адаптивності мережових сервісів та ресурсів, який дозволяє автоматизувати процеси управління, оптимізації та захисту мереж, а також покращити якість обслуговування та якість досвіду використання користувачів.

Критерії оцінки QoS. Якість обслуговування користувачів охоплює параметри мережі, які впливають на передачу даних, що включає:

Пропускна здатність – доступний обсяг даних, який може бути переданий мережею за певний час.

Затримка – час, необхідний для передачі пакету даних від відправника до отримувача.

Стійкість до помилок – здатність мережі виявляти та виправляти помилки передачі даних.

Коливання затримок (джиттер) – коливання часу між доставкою послідовних пакетів даних.

Критерій QoE визначає якість послуги з точки зору кінцевих користувачів, враховує їх суб'єктивне сприйняття і залежить від QoS [10]. Ці параметри є основою для забезпечення ефективності роботи мереж і значною мірою впливають на сприйняття користувачами якості сервісів.

У забезпеченні якості обслуговування в мережах SDN [11] акцентується увага на необхідності гнучкого та масштабованого рішення для налаштування мережевого трафіку. Автори вказують на проблеми класичних мереж, де зростаюча кількість протоколів ускладнює забезпечення QoS і пропонують використання SDN для розділення рівня управління і передачі даних, що дозволяє централізовано керувати трафіком через контролер SDN. Описано переваги SDN у контексті оптимізації мережевих конфігурацій, а саме - зменшення кількості обладнання, підвищення ефективності розгортання мережевої інфраструктури, можливість керування без потреби у використанні додаткового обладнання. Тому, забезпечення якості обслуговування, особливо у світлі посилення різноманітності мережевого трафіку (зростання числа мобільних з'єднань, швидкості передачі даних, збільшення кількості «розумних пристроїв» IoT) є однією з найактуальніших проблем в телекомунікаційних мережах [12]. Основну увагу слід акцентувати на розробці та вдосконаленні SDN мереж, які мають потенціал вирішити ці виклики в телекомунікаційній сфері. Для вирішення завдання попередження перенавантажень, може бути використаний варіант застосування класичної технології маршрутизації в поєднанні з SDN (використання самої технології SDN вирішує проблему, але може бути дороговартісним, якщо потрібно вирішити лише одне завдання). Використання запропонованої автором [13] математичної моделі розподілу трафіку в гібридних системах (із використання звичайних маршрутизаторів та SDN вузлів) може виявитись ефективним з точки зору підвищення продуктивності мережі та зниження витрат на її обслуговування.

Виклад основного матеріалу

Архітектура SDN мережі. Підхід SDN до мережевої архітектури (Рис. 2,а), дозволяє централізовано керувати мережевими ресурсами та конфігурувати їх за допомогою програмного забезпечення [14, 15] і при цьому - відокремити площину управління мережі від площини передачі даних. SDN технологія більше нагадує хмарні рішення [4], що зосереджує системний інтелект у єдиному місці, на відміну від класичного управління мережею. SDN контролер, або мережева операційна система (network operating system, NOS) надає абстрактну схему елементів перенаправлення (маршрутизаторів, комутаторів) для додатків мережі вищого рівня [16, 17].

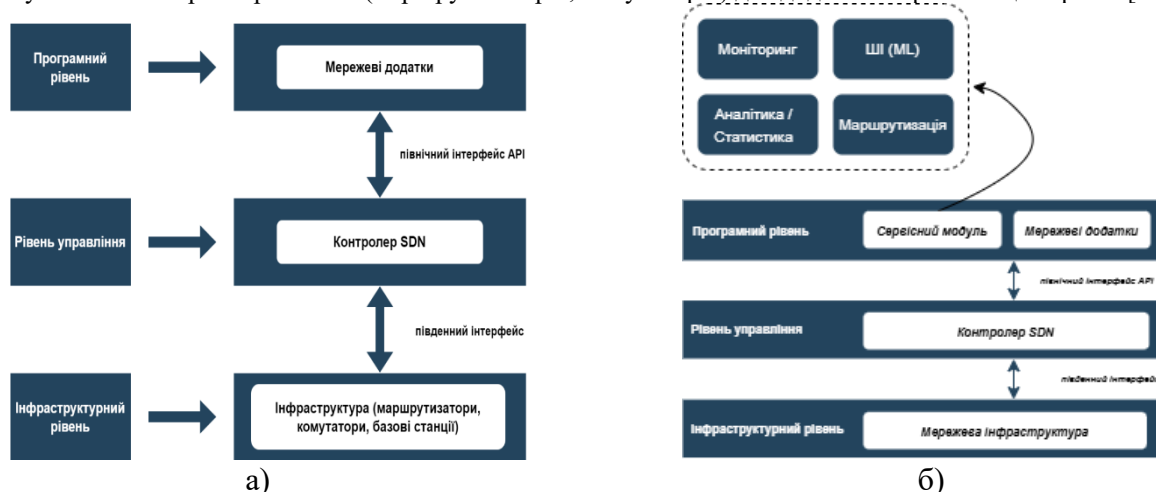


Рис. 2. Архітектура мережі SDN: а) типова, б) із сервісними додатками

Програмний рівень знаходиться на вершині архітектури SDN, де реалізовані такі мережеві функції та служби, як маршрутизація, інженерія трафіку, балансування та інші. Наступним йде рівень управління, на якому реалізовано контролер SDN та мережеву операційну систему. Цей рівень приховує розподілену фізичну структуру мережі та надає граф мережі для послуг верхнього рівня.

Рівень управління. Відповідальність за налаштування комутаторів лежить на контролері SDN, який встановлює правила маршрутизації через південний інтерфейс. У порівнянні з класичною архітектурою комп'ютерних мереж, в нашому випадку комутатори на інфраструктурному рівні забезпечують лише передачу даних згідно з правилами, встановленими на рівні управління. Тим часом контролер SDN на цьому рівні діє як мережевий оператор, намагаючись керувати кожним комутатором за допомогою конкретних управлінських стандартів. Основним стандартом для цієї взаємодії є OpenFlow [18] протокол.

Інфраструктурний рівень містить набір з'єднаних елементів переадресації (комутаторів SDN), що забезпечують маршрутизацію пакетів і представляють собою площину даних.

Враховуючи централізовану концепцію архітектури SDN, а також ієрархічну, багатoshарову систему передачі трафіку, яка використовує механізми керування SDN контролером – можна зробити висновок, що головний недолік цієї структури це залежність ефективності кожного шару від попереднього, через що з'єднання можуть бути нестабільними, також необхідно гарантувати безпеку самих з'єднань.

Використання підходів штучного інтелекту пропонує вдосконалені методи для моніторингу та автоматизації [19]. Це може сприяти розумному управлінню мережею на різних рівнях. ШІ також може підсилити здатність контролера SDN до гнучкого та розумного керування мережею, здійснювати маршрутизацію, включаючи автоматизоване прийняття рішень, діагностику, переналаштування та ін.

В даному аспекті використання, ШІ в SDN має виконувати прогностичну роль у керуванні мережею та оптимізації трафіку. Мережі на базі ШІ менше залежать від людського досвіду. Завдяки цьому, можна керувати та налаштовувати мережу на основі детального аналізу даних і алгоритмів що постійно вдосконалюються, що сприяє ефективному використанню мережевих ресурсів [20]. Контролер SDN надає ШІ докладну інформацію про мережу, зокрема статистику трафіку, стан пристроїв і каналів, політики управління трафіком, топологію мережі та історичні дані, що дозволяє алгоритмам аналізувати закономірності і прогнозувати майбутнє навантаження для адаптивного налаштування мережі [21]. Після цього алгоритми ШІ можуть адаптивно коригувати трафік з урахуванням поточного стану мережі.

Використання методів ML, і зокрема DL, в SDN мережах, дозволяє ефективно ідентифікувати та протидіяти загрозам, пов'язаними з розвідкою (наприклад, сканування портів) та прихованим спостереженням за мережею. Гібридна модель [22] (поєднання двох різних моделей глибокого навчання — Convolutional Neural Network (CNN) та Long Short-Term Memory (LSTM)) підвищує точність визначення атак, оптимізуючи швидкість та продуктивність системи [23]. Перспективи для подальших досліджень глибокого навчання в SDN включають розробку і впровадження більш складних і точних моделей для виявлення і протидії загрозам. Дослідження [24] показало, що машинне навчання та системи на основі нечіткої логіки є найпопулярнішими методами ШІ в SDN. Взагалі кажучи, методи ШІ виявилися ефективними для використання разом з SDN (Таблиця 1), проте потрібно приділити більше уваги дослідженню стабільності методів ШІ в конкурентних умовах.

Таблиця 1

Порівняння підходів штучного інтелекту в SDN

Підхід ШІ	Переваги	Недоліки	Застосування в SDN	Показники продуктивності
Нейронні мережі	Швидка обробка даних, здатність до навчання	Висока складність моделей, потребує багато даних та обчислювальної потужності	Управління трафіком та його класифікація	Точність, час навчання
Машинне навчання	Адаптивність до нових умов, адаптивні у навчанні	Потреба в великих обсягах даних, висока обчислювальна вартість	Оптимізація мережі (прогнозування трафіку, виявлення аномалій)	Точність, зниження затримок
Глибоке навчання	Навчання на неструктурованих даних, висока точність розпізнавання	Потреба у великих обчислювальних ресурсах	Безпека (виявлення вторгнень), аналіз продуктивності	Обчислювальна ефективність, швидкість виявлення загроз

Практичне застосування та апробація

Охорона здоров'я є важливою сферою для апробації SDN є, що виступає однією з ключових сфер суспільства, де інформаційні технології відіграють надважливу роль у підвищенні ефективності та якості надання медичних послуг. З ростом кількості IoT (інтернет речей) пристроїв у медичному середовищі, таких як портативні медичні датчики, автономні маніпулятори, телемедичне обладнання та інші інтелектуальні системи, з'являється необхідність в ефективному управлінні та координації цих пристроїв. Контролер програмно-визначеної мережі в такому випадку може забезпечувати інтелектуальне управління даними та ресурсами, враховуючи потреби охорони здоров'я. У таких системах, IoT пристрої повинні проходити автентифікацію перед передачею даних, після чого дані обробляються на централізованому чи локальному сервері. У запропонованому в [25] захищеному фреймворку для SDN в системах охорони здоров'я з підтримкою IoT, пристрої IoT автентифікуються за допомогою полегшеної схеми автентифікації. Граничні сервери співпрацюють для балансування навантаження і мають налаштований SDN-контролер для прийняття рішень та управління безпекою обміну даних.

Розумне місто. У розрізі практичного використання в межах «розумного міста» використовують технології інтернету речей (IoT) та гібридних мереж для забезпечення масштабованої, надійної зв'язності, для покращення якості надання послуг та ефективного управління інфраструктурою в міських районах [26]. Розумні міста інтегрують різноманітні пристрої, такі як сенсори, валідатори, транспорт [27], засоби для збору даних. Впровадження SDN у концепцію «розумного міста» [28] допомагає вирішити наступні виклики: здатність обробляти великі об'єми даних, стандартизація інтерфейсів і протоколів, масштабованість

управління мережею, забезпечення безпеки і конфіденційності, а також зменшення споживання електроенергії. Результати дослідження [29] показують, що SDN дозволяє легко програмувати та адаптувати мережу до змінних вимог, що робить її ідеальною для динамічного та різноманітного середовища розумних міст.

Інтелектуальні транспортні системи. Використання машинного навчання дає можливість прогнозування та оптимізації маршрутів в реальному часі, що є критично важливим для застосунків, чутливих до затримок. Цей підхід зменшує затримку на доставку пакетів у мережі, забезпечує ефективне використання ресурсів мережі в години пік. Також, надає системі можливість автономно освоювати нові знання та вдосконалювати свої алгоритми, виходячи з аналізу доступних транспортних даних, що є надзвичайно важливим в умовах, які постійно змінюються на дорозі а отже, і в мережі. Такий підхід у застосуванні та побудові SDN є перспективним до подальшого розвитку та оптимізації комунікаційних систем [26], дозволяючи їм ефективно реагувати на змінні вимоги та обставини.

Певної мірою оглянуті підходи та ідеї апробовані в дослідженні [30], де зроблено акцент на покращенні якості сприйняття послуг в інфокомунікаційних системах через розробку нових методів моніторингу та управління, можливість адаптації до мінливих вимог користувачів і обмеженості ресурсів. Пропонуються мережі гібридного типу, де в рамках підходу SDN застосовуватимуться як традиційні компоненти мереж, так і компоненти, орієнтовані на вирішення певної проблеми, зокрема покращення досвіду користування споживачів. Для забезпечення високої точності прогнозування та мінімізації вимог до обчислювальних ресурсів обрано алгоритм машинного навчання Random Forest [30].

Застосований алгоритм ML для сервісного модуля (Рис. 2,б), який інтегрується в SDN, дозволив до 30% зменшити обсяг сигнального трафіку. Отже, використання глибокого навчання та нейромереж для аналізу даних підвищує точність прогнозування і розпізнавання патернів у мережевому трафіку. Розробка специфічних модулів для інтеграції з різними типами SDN контролерів покращує ефективність управління мережею. Також, впровадження алгоритмів, які працюють в реальному часі, потенційно дозволить реагувати на зміни в мережі та приймати управлінські рішення не потребуючи залученості адміністратора мережі, тому буде доцільним в подальшій роботі акцентувати увагу на дизайні таких компонентів SDN.

Висновки

Програмно-визначені мережі відповідають сучасним викликам управління мережами, особливо у контексті зростання трафіку та інтеграції IoT пристроїв. Інтеграція штучного інтелекту в SDN не лише підсилює ефективність та безпеку мережі, але й дозволяє адаптуватися до динамічно змінюваних умов, передбачаючи мережевий трафік. Потенційно актуальним цей підхід є у сфері охорони здоров'я та у випадку «розумного міста», де комбінація SDN, IoT та ШІ може покращити управління обладнанням та підвищити якість наданих послуг. Також даний підхід може бути корисним і в інших сферах (логістика, аграрна сфера, соціальні проекти).

Література

1. Щур В., Кулаков Ю. Аналіз сучасних методів балансування навантаження в SDN мережах // Herald of Khmelnytskyi National University. Technical Sciences. – 2023. – Т. 323, №4. – С. 352-357. DOI: <https://doi.org/10.31891/2307-5732-2023-323-4-352-357>
2. Панченко О.М. Адаптивне управління ресурсами та якістю обслуговування у програмно-конфігурованих сервісноорієнтованих телекомунікаційних мережах: дис. ... д-ра філософії: 172 – Телекомунікації та радіотехніка / Панченко Олексій Михайлович. – Львів, 2021. – 200 с.
3. Андрущак В.С. Моделі управління потоками інфокомунікаційних мереж з використанням методів штучного інтелекту і машинного навчання: дис. ... д-ра філософії: 172 – Телекомунікації та радіотехніка / Андрущак Володимир Степанович. – Львів, 2021. – 189 с.
4. Fabio Caccioli Capra. Definition and Applications of SDN, NFV, Edge Computing and AI/ML Techniques // Journal of Machine and Computing. – 2022. – Vol. 2, №3. – P. 103-113. DOI: <https://doi.org/10.53759/7669/jmc202202015>
5. 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. – Vol. 10. – P. 45820-45854. DOI: <https://doi.org/10.1109/ACCESS.2022.3168972>
6. Hnidenko M.P., Prokopov S.V., Hnidenko M.M. Enhancing the security of Software-Defined Networks (SDNs) // State University of Information and Communication Technologies, F SNSUT. – 2023. – Vol. 4, №2. DOI: <https://doi.org/10.31673/2518-7678.2023.020707>
7. Abdulqadder I.H., Zou D., Aziz I.T., Yuan B., Li W. SecSDN-Cloud: Defeating Vulnerable Attacks Through Secure Software-Defined Networks // IEEE Access. – 2018. – Vol. 6. – P. 8292-8301. DOI: <https://doi.org/10.1109/ACCESS.2018.2797214>
8. Васильківський М., Варгатюк Г., Болдирева О. Дослідження архітектури штучного інтелекту для інфокомунікаційних мереж 6G // Measuring and Computing Devices in Technological Processes. – 2022. – №4. – С. 62–70. DOI: <https://doi.org/10.31891/2219-9365-2022-72-4-7>
9. Yang H., Alphones A., Xiong Z., Niyato D., Zhao J., Wu K. Artificial-Intelligence-Enabled Intelligent 6G

Networks // IEEE Network. – 2020. – Vol. 34, №6. – P. 272-280. DOI: <https://doi.org/10.1109/MNET.011.2000195>

10. Пелех П. Оцінка QoE на основі вимірювання QoS для відео реального часу у безпроводних мережах // Herald of Khmelnytskyi National University. Technical Sciences. – 2024. – Т. 337, №3(2). – С. 237-245. DOI: <https://doi.org/10.31891/2307-5732-2024-337-3-35>

11. Ряба Н.М., Правило В.В. Забезпечення виконання заданих показників якості обслуговування в мережах SDN // Збірник матеріалів Міжнародної науково-технічної конференції «Перспективи телекомунікацій», Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна. – 2018. – Режим доступу: <https://conference-journal.its.kpi.ua/article/view/131516/127598> (дата звернення: 14.11.2024). — Назва з екрана.

12. Єфанова К.А., Пономаренко З.М., Масесов М.О. Актуальність впровадження та використання мережі SDN // Сучасні інформаційні технології у сфері безпеки та оборони. – 2018. – Т. 32, №2. – С. 147-150. DOI: <https://doi.org/10.33099/2311-7249/2018-32-2-147-150>

13. Бовда Е.М. Метод управління перерозподілом навантаження в SDN мережах // Збірник наукових праць Військового інституту телекомунікацій та інформатизації. – 2017. – Вип. 2. – С. 6-15. – Режим доступу: http://nbuv.gov.ua/UJRN/Znpviti_2017_2_3 (дата звернення: 10.12.2024). — Назва з екрана.

14. Даков С.Ю. Метод підвищення ефективності SDN мережі за допомогою керуючого програмного забезпечення // Вісник Хмельницького національного університету. Технічні науки. – 2018. – №6(2). – С. 216-223. DOI: [https://doi.org/10.31891/2307-5732-2018-267-6\(2\)-216-223](https://doi.org/10.31891/2307-5732-2018-267-6(2)-216-223)

15. Akyildiz I.F., Lee A., Wang P., Luo M., Chou W. A roadmap for traffic engineering in SDN-OpenFlow networks // Computer Networks. – 2014. – Vol. 71. – P. 1-30. DOI: <https://doi.org/10.1016/j.comnet.2014.06.002>

16. Al-Najjar A., Khan F.H., Portmann M. Network traffic control for multi-homed end-hosts via SDN // IET Communications. – 2020. – Vol. 14. – P. 3312-3323. DOI: <https://doi.org/10.1049/iet-com.2020.0335>

17. Prabakaran P., Isravel D.P., Silas S. A Review of SDN-Based Next Generation Smart Networks // 2019 3rd International Conference on Computing and Communications Technologies (ICCT). – 2019. – P. 80-85. DOI: <https://doi.org/10.1109/ICCT2.2019.8824871>

18. Open Flow Standard. [Електронний ресурс]. Режим доступу: <https://opennetworking.org/software-defined-standards/specifications> (дата звернення: 12.12.2024). — Назва з екрана.

19. Jiang J., Lin C., Han G., Abu-Mahfouz A.M., Shah S.B.H., Martínez-García M. How AI-enabled SDN technologies improve the security and functionality of industrial IoT networks // Digital Communications and Networks. – 2022. – DOI: <https://doi.org/10.1016/j.dcan.2022.07.001>

20. Wu Y.-J., Hwang P.-C., Hwang W.-S., Cheng M.-H. Artificial Intelligence Enabled Routing in Software Defined Networking // Applied Sciences. – 2020. – Vol. 10. – P. 6564. DOI: <https://doi.org/10.3390/app10186564>

21. Guo A., Yuan C. Network Intelligent Control and Traffic Optimization Based on SDN and Artificial Intelligence // Electronics. – 2021. – Vol. 10. – P. 700. DOI: <https://doi.org/10.3390/electronics10060700>

22. Malik J., Akhuzada A., Bibi I., Imran M., Musaddiq A., Kim S.W. Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN // IEEE Access. – 2020. – Vol. 8. – P. 134695-134706. DOI: <https://doi.org/10.1109/ACCESS.2020.3009849>

23. Swami R., Dave M., Ranga V. Software-defined Networking-based DDoS Defense Mechanisms // ACM Computing Surveys. – 2019. – Vol. 52, №2. DOI: <https://doi.org/10.1145/3301614>

24. Latah M., Toker L. Artificial intelligence enabled software-defined networking: a comprehensive overview // IET Networks. – 2019. – Vol. 8. – P. 79-99. DOI: <https://doi.org/10.1049/iet-net.2018.5082>

25. Li J., et al. A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System // IEEE Access. – 2020. – Vol. 8. – P. 135479-135490. DOI: <https://doi.org/10.1109/ACCESS.2020.3011503>

26. Дуда О., Станько А. Архітектура мережевої платформи моніторингу об'єктів у кіберфізичних системах «Розумних міст» // Herald of Khmelnytskyi National University. Technical Sciences. – 2023. – Т. 323, №4. – С. 123-130. DOI: <https://doi.org/10.31891/2307-5732-2023-323-4-123-130>

27. Singh P.K., Sharma S., Nandi S.K., Nandi S. Multipath TCP for V2I communication in SDN controlled small cell deployment of smart city // Vehicular Communications. – 2019. – Vol. 15. – P. 1-15. DOI: <https://doi.org/10.1016/j.vehcom.2018.11.002>

28. Митник О.М. Застосування технології SDN для вирішення проблем впровадження концепції «Розумне місто» // Матеріали VII Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій», 28–29 листопада 2018 р., Тернопіль, Україна / Тернопільський національний технічний університет ім. Івана Пулюя. – Тернопіль, 2018. – С. 126-127. Режим доступу: https://elartu.tntu.edu.ua/bitstream/lib/27137/2/VII_MNTK_2018v2_Mytnyk_O_M-Application_of_SDN_technology_126-127.pdf (дата звернення: 12.01.2025). — Назва з екрана.

29. EL-Garoui L., Pierre S., Chamberland S. A New SDN-Based Routing Protocol for Improving Delay in Smart City Environments // Smart Cities. – 2020. – Vol. 3. – P. 1004-1021. DOI: <https://doi.org/10.3390/smartcities3030050>

30. Прислупський А.І. Підвищення показників якості сприйняття інфокомунікаційних послуг в інтелектуальних мережах нового покоління: дис. ... д-ра філософії: 172 – Телекомунікації та радіотехніка / Прислупський Андрій Іванович. – Львів, 2022. – 277 с.

References

1. Shchur V., Kulakov Yu. Analiz suchasnykh metodiv balansuvannya navantazhennia v SDN merezhakh // Herald of Khmelnytskyi National University. Technical Sciences. – 2023. – T. 323, №4. – S. 352-357. DOI: <https://doi.org/10.31891/2307-5732-2023-323-4-352-357>
2. Panchenko O.M. Adaptivne upravlinnia resursamy ta yakistiu obsluhovuvannya u prohramno-konfigurovanykh servisnoorientovanykh telekomunikatsiinykh merezhakh: dys. ... d-ra filosofii: 172 – Telekomunikatsii ta radiotekhnika / Panchenko Oleksii Mykhailovych. – Lviv, 2021. – 200 s.
3. Andrushchak V.S. Modeli upravlinnia potokamy infokomunikatsiinykh merezh z vykorystanniam metodiv shtuchnoho intelektu i mashynnoho navchannia: dys. ... d-ra filosofii: 172 – Telekomunikatsii ta radiotekhnika / Andrushchak Volodymyr Stepanovych. – Lviv, 2021. – 189 s.
4. Fabio Caccioli Capra. Definition and Applications of SDN, NFV, Edge Computing and AI/ML Techniques // Journal of Machine and Computing. – 2022. – Vol. 2, №3. – P. 103-113. DOI: <https://doi.org/10.53759/7669/jmc202202015>
5. 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. – Vol. 10. – P. 45820-45854. DOI: <https://doi.org/10.1109/ACCESS.2022.3168972>
6. Hnidenko M.P., Prokopov S.V., Hnidenko M.M. Enhancing the security of Software-Defined Networks (SDNs) // State University of Information and Communication Technologies, F SNSUT. – 2023. – Vol. 4, №2. DOI: <https://doi.org/10.31673/2518-7678.2023.020707>
7. Abdulqadder I.H., Zou D., Aziz I.T., Yuan B., Li W. SecSDN-Cloud: Defeating Vulnerable Attacks Through Secure Software-Defined Networks // IEEE Access. – 2018. – Vol. 6. – P. 8292-8301. DOI: <https://doi.org/10.1109/ACCESS.2018.2797214>
8. Vasylyukivskiy M., Varhatiuk H., Boldyreva O. Doslidzhennia arkhitektury shtuchnoho intelektu dlia infokomunikatsiinykh merezh 6G // Measuring and Computing Devices in Technological Processes. – 2022. – №4. – S. 62–70. DOI: <https://doi.org/10.31891/2219-9365-2022-72-4-7>
9. Yang H., Alphones A., Xiong Z., Niyato D., Zhao J., Wu K. Artificial-Intelligence-Enabled Intelligent 6G Networks // IEEE Network. – 2020. – Vol. 34, №6. – P. 272-280. DOI: <https://doi.org/10.1109/MNET.011.2000195>
10. Pelekh P. Otsinka QoE na osnovi vymiruvannya QoS dlia video realnoho chasu u bezprovidnykh merezhakh // Herald of Khmelnytskyi National University. Technical Sciences. – 2024. – T. 337, №3(2). – S. 237-245. DOI: <https://doi.org/10.31891/2307-5732-2024-337-3-35>
11. Riaba N.M., Pravylo V.V. Zabezpechennia vykonannia zadanykh pokaznykiv yakosti obsluhovuvannya v merezhakh SDN // Zbirnyk materialiv Mizhnarodnoi nauko-tekhnichnoi konferentsii «Perspektyvy telekomunikatsii», Instytut telekomunikatsiinykh system KPI im. Ihoria Sikorskoho, Ukraina. – 2018. – Rezhym dostupu: <https://conference-journal.iits.kpi.ua/article/view/131516/127598>
12. Yefanova K.A., Ponomarenko Z.M., Masesov M.O. Aktualnist vprovadzhennia ta vykorystannia merezhi SDN // Suchasni informatsiini tekhnologii u sferi bezpeky ta oborony. – 2018. – T. 32, №2. – S. 147-150. DOI: <https://doi.org/10.33099/2311-7249/2018-32-2-147-150>
13. Bovda E.M. Metod upravlinnia pererozpodilom navantazhennia v SDN merezhakh // Zbirnyk naukovykh prats Viiskovoho instytutu telekomunikatsii ta informatyzatsii. – 2017. – Vyp. 2. – S. 6-15. – Rezhym dostupu: http://nbuv.gov.ua/UJRN/Znpviti_2017_2_3 (data zvernennia: 10.12.2024). — Nazva z ekrana.
14. Dakov S.Iu. Metod pidvyshchennia efektyvnosti SDN merezhi za dopomohoiu keruiuchoho prohramnoho zabezpechennia // Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – 2018. – №6(2). – S. 216-223. DOI: [https://doi.org/10.31891/2307-5732-2018-267-6\(2\)-216-223](https://doi.org/10.31891/2307-5732-2018-267-6(2)-216-223)
15. Akyildiz I.F., Lee A., Wang P., Luo M., Chou W. A roadmap for traffic engineering in SDN-OpenFlow networks // Computer Networks. – 2014. – Vol. 71. – P. 1-30. DOI: <https://doi.org/10.1016/j.comnet.2014.06.002>
16. Al-Najjar A., Khan F.H., Portmann M. Network traffic control for multi-homed end-hosts via SDN // IET Communications. – 2020. – Vol. 14. – P. 3312-3323. DOI: <https://doi.org/10.1049/iet-com.2020.0335>
17. Prabakaran P., Isravel D.P., Silas S. A Review of SDN-Based Next Generation Smart Networks // 2019 3rd International Conference on Computing and Communications Technologies (ICCTT). – 2019. – P. 80-85. DOI: <https://doi.org/10.1109/ICCTT2.2019.8824871>
18. Open Flow Standard. [Elektronnyi resurs]. Rezhym dostupu: <https://opennetworking.org/software-defined-standards/specifications> (data zvernennia: 12.12.2024). — Nazva z ekrana.
19. Jiang J., Lin C., Han G., Abu-Mahfouz A.M., Shah S.B.H., Martinez-Garcia M. How AI-enabled SDN technologies improve the security and functionality of industrial IoT networks // Digital Communications and Networks. – 2022. – DOI: <https://doi.org/10.1016/j.dcan.2022.07.001>
20. Wu Y.-J., Hwang P.-C., Hwang W.-S., Cheng M.-H. Artificial Intelligence Enabled Routing in Software Defined Networking // Applied Sciences. – 2020. – Vol. 10. – P. 6564. DOI: <https://doi.org/10.3390/app10186564>
21. Guo A., Yuan C. Network Intelligent Control and Traffic Optimization Based on SDN and Artificial Intelligence // Electronics. – 2021. – Vol. 10. – P. 700. DOI: <https://doi.org/10.3390/electronics10060700>
22. Malik J., Akhunzada A., Bibi I., Imran M., Musaddiq A., Kim S.W. Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN // IEEE Access. – 2020. – Vol. 8. – P. 134695-134706. DOI: <https://doi.org/10.1109/ACCESS.2020.3009849>
23. Swami R., Dave M., Ranga V. Software-defined Networking-based DDoS Defense Mechanisms // ACM Computing Surveys. – 2019. – Vol. 52, №2. DOI: <https://doi.org/10.1145/3301614>
24. Latah M., Toker L. Artificial intelligence enabled software-defined networking: a comprehensive overview // IET Networks. – 2019. – Vol. 8. – P. 79-99. DOI: <https://doi.org/10.1049/iet-net.2018.5082>
25. Li J., et al. A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System // IEEE Access. – 2020. – Vol. 8. – P. 135479-135490. DOI: <https://doi.org/10.1109/ACCESS.2020.3011503>
26. Duda O., Stanko A. Arkhitektura merezhevoi platformy monitorynu obektiv u kiberfizychnykh systemakh «Rozumnykh mist» // Herald of Khmelnytskyi National University. Technical Sciences. – 2023. – T. 323, №4. – S. 123-130. DOI: <https://doi.org/10.31891/2307-5732-2023-323-4-123-130>
27. Singh P.K., Sharma S., Nandi S.K., Nandi S. Multipath TCP for V2I communication in SDN controlled small cell deployment of smart city // Vehicular Communications. – 2019. – Vol. 15. – P. 1-15. DOI: <https://doi.org/10.1016/j.vehcom.2018.11.002>
28. Mytnyk O.M. Zastosuvannya tekhnologii SDN dlia vyrisnennia problem vprovadzhennia kontseptsii «Rozumne misto» // Materialy VII Mizhnarodnoi nauko-tekhnichnoi konferentsii molodykh uchenykh ta studentiv «Aktualni zadachi suchasnykh tekhnologii», 28–29 lystopada 2018 r., Ternopil, Ukraina / Ternopilskyi natsionalnyi tekhnichnyi universytet im. Ivana Puliua. – Ternopil, 2018. – S. 126-127. Rezhym dostupu: https://elartu.tntu.edu.ua/bitstream/lib/27137/2/VII_MNTK_2018v2_Mytnyk_O_M-Application_of_SDN_technology_126-127.pdf (data zvernennia: 12.01.2025). — Nazva z ekrana.
29. EL-Garoui L., Pierre S., Chamberland S. A New SDN-Based Routing Protocol for Improving Delay in Smart City Environments // Smart Cities. – 2020. – Vol. 3. – P. 1004-1021. DOI: <https://doi.org/10.3390/smartsities3030050>
30. Pryslupskiy A.I. Pidvyshchennia pokaznykiv yakosti spryiniattia infokomunikatsiinykh posluh v intelektualnykh merezhakh novoho pokolinnia: dys. ... d-ra filosofii: 172 – Telekomunikatsii ta radiotekhnika / Pryslupskiy Andrii Ivanovych. – Lviv, 2022. – 277 s.