УДК 004.7

Л.А. Савицька[1], Т.І. Коробейнікова[2], І. В. Леонтьєв[1], С. В. Богомолов[1]

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ РЕСУРСІВ В КОМП'ЮТЕРНІЙ SDN-МЕРЕЖІ

[1]Вінницький національний технічний університет, Вінниця

[2]Національний університет «Львівська політехніка»

Анотація. Робота присвячена аналізу та вдосконаленню методів та засобів побудови архітектури програмно-керованих мереж. Важливим аспектом є порівняння відмінностей між керуванням мережі за допомогою традиційних методів та з використання SDN контролера. Основна увага приділяється розробці моделей безпеки на базі програмно-керованих мереж.

Дослідження ґрунтуються на аналізі конкретних випадків використання таких мереж, включаючи збір думок та експертних оцінок від професіоналів у галузі та використовують загальнодоступну інформацію про методи та засоби безпеки архітектури програмно-керованих мереж. Технологія SDN надає більше гнучкості та швидкості впровадження заходів безпеки, що дозволяє реагувати на загрози в реальному часі. У сучасних умовах, коли кіберзагрози стають складнішими та виразнішими, SDN-мережі дозволяють виявляти атаки, блокувати шкідливі дії та застосовувати політики безпеки в реальному часі. Проте, зростаюча складність кіберзагроз та постійні зміни технологій вимагають подальшого розвитку і вдосконалення інформаційної безпеки ресурсів SDN-мережі компанії. Існує необхідність у подальшому аналізі та вдосконаленні методів та засобів захисту інформаційних та інших ресурсів в комп'ютерних SDN-мережах. Потреба у подальшому аналізі та вдосконаленні методів та засобів захисту інформаційних та інших ресурсів в комп'ютерних SDN-мережах стала фундаментом для проведення цього дослідження. У результаті досягнуто підвищення рівня інформаційної безпеки ресурсів SDN-мережі шляхом: 1) скорочення часу втручання у мережу; 2) застосування вдосконаленого методу оброблення трафіку на основі мережевої безпеки потоку пакетів, що дозволяє бажаним мережевим додаткам ефективно керувати пересиланням.

Ключові слова: SDN-мережа, Семантична модель SDN, модель взаємодії мережевої операційної системи та SDN, модель мережі із гнучкими ресурсами.

Abstract. The work is dedicated to the analysis and improvement of methods and tools for building the architecture of software-defined networks (SDNs). A crucial aspect involves comparing the differences between network management using traditional methods and utilizing an SDN controller. Primary attention is given to the development of security models based on software-defined networks.

The research is grounded in the analysis of specific cases involving the use of such networks, including gathering opinions and expert assessments from professionals in the field. It leverages publicly available information on methods and tools for securing the architecture of software-defined networks. SDN technology provides greater flexibility and speed in implementing security measures, allowing real-time responses to threats. In contemporary conditions, where cyber threats are becoming more complex and pronounced, SDN networks enable the detection of attacks, blocking malicious actions, and applying security policies in real-time. However, the increasing complexity of cyber threats and constant technological changes necessitate further development and enhancement of the information security of SDN network resources for companies. There is a need for further analysis and improvement of methods and tools for protecting information and other resources in computer-based SDN networks. The necessity for further analysis and improvement of methods and tools for protecting information and other resources in computer-based SDN networks serves as the foundation for this research. As a result, an enhancement in the level of information security for SDN network resources has been achieved by: 1) reducing the intervention time in the network; 2) applying an improved method of traffic processing based on network security of packet flows, allowing desired network applications to efficiently manage forwarding.

Key words: SDN network, SDN Semantic Model, network operating system interaction model and SDN, network model with flexible resources.

DOI: https://doi.org/10.31649/1999-9941-2023-58-3-41-52.

Вступ

Кожна компанія, незалежно від свого розміру або галузі, має важливі ресурси, такі як конфіденційні дані клієнтів, комерційна інформація, інтелектуальна власність, фінансові дані тощо. Збереження цих ресурсів від несанкціонованого доступу, витоку інформації та зловживань є критично важливим завданням для забезпечення успіху компанії і захисту її репутації. Основними викликами, з якими може зіткнутися мережа компанії, може бути мережеві атаки на активи та ресурси (real time) внаслідок недосконалості або навіть відсутності політик доступу, складністю їх налаштувань, підтримки та оновлення; недостатній рівень керування мережевим трафіком; відсутність адекватного контролю, що призводить до зменшення гнучкості мережі; відсутність автоматизації базових мережевих функцій тощо [1-4].

Комп'ютерні SDN-мережі надають нові можливості для забезпечення безпеки мережевих ресурсів. Ця технологія дозволяє централізовано керувати мережевими пристроями і програмно налаштовувати правила безпеки [5-6].

Актуальність

Технологія SDN забезпечує більшу гнучкість та швидкість впровадження заходів безпеки,

дозволяючи реагувати на загрози в реальному часі [8-10]. На сьогоднішній день, коли кіберзагрози стають все більш складними і виразними, SDN-мережі дозволяють виявляти атаки, блокувати шкідливі дії та застосовувати політики безпеки в реальному часі. Проте, зростаюча складність кіберзагроз та постійні зміни технологій вимагають подальшого розвитку і вдосконалення інформаційної безпеки ресурсів SDN-мережі компанії [7-10]. Тому тема дослідження є актуальною. Таким чином, існує потреба у аналізі та вдосконаленні методів та засобів захисту інформаційних та інших ресурсів в комп'ютерній SDN- мережі.

Мета

Метою дослідження є підвищення рівня інформаційної безпеки ресурсів SDN-мережі за рахунок застосування вдосконаленої безпекової моделі SDN-мережі.

Задачі

1. Виконати аналіз архітектур SD-WAN та SD-LAN на предмет організації у порівнянні із класичними архітектурними підходами;
2. Запропонувати семантичну модель SDN та схему розподілу потоків трафіку в SDN;
3. Запропонувати спосіб розрахунку надійності мережі;
4. Запропонувати модель взаємодії мережевої операційної системи із комп'ютерною SDN-мережею та спосіб оброблення трафіку;
5. Запропонувати безпекову модель та описати прототип комп'ютерної SDN-мережі.

Аналіз архітектур SD-WAN та SD-LAN на предмет організації у порівнянні із класичними архітектурними підходами

Комп'ютерна SDN-мережа (ПКМ, англ. Software-defined Networking, SDN) – це архітектура, яка розділяє функції управління мережею та пересилання даних, що дозволяє безпосередньо програмувати управління мережею, а базову інфраструктуру абстрагувати для програм і мережевих служб.

Ресурси SDN включають можливість більш ефективно та динамічно керувати мережевим трафіком, забезпечуючи підвищений рівень контролю та гнучкості в мережі. SDN дозволяє створювати кілька логічних мереж на основі однієї фізичної інфраструктури, що дозволяє віртуалізувати мережу. Крім того, SDN допомагає автоматизувати багато мережевих функцій, що може зменшити фізичне використання пристроїв та дозволити швидше розгортання та ефективне використання ресурсів мережі. Окрім цього, SDN надає централізований огляд всієї мережі, що забезпечує кращий рівень видимості та контролю.

Популярна архітектура комп'ютерної SDN-мережі складається з трьох рівнів (див. рис. 1, а):

1) Рівень інфраструктури містить набір мережевого обладнання.

2) Рівень керування містить мережеву операційну систему (МОС). МОС надає мережеві сервіси та програмний інтерфейс для управління мережевими пристроями.

3) Рівень мережевих додатків, який надає можливість гнучкого та ефективного керування мережею через різноманітні застосунки. Сюди входять програмні рішення щодо забезпечення безпеки, балансування навантаження (load balancing), виявлення вторгнень (IDS), адміністрування (IPS), а також функції управління потоками даних, мобільністю та доступом, які сприяють ефективній роботі мережі та багатьом іншим функціям.

Для налаштування комп'ютерної SDN-мережі достатньо просто додати програмний контролер, замість того, щоб редагувати великі обсяги коду в численних мережевих пристроях. Поведінкою комп'ютерної SDN-мережі можна керувати в реальному часі, а нові рішення можна впроваджувати значно швидше, ніж у традиційній архітектурі. Централізація стану мережі в єдиній точці керування дозволяє конфігурувати SDN-мережі за допомогою програмних інструментів. Мережеві контролери також включають набір програмних інтерфейсів, які реалізують стандартні завдання у сфері маршрутизації, такі як багатоканальність, безпека, контроль доступу, управління пропускною здатністю, забезпечення якості обслуговування, при цьому вони можуть бути спеціалізовані та налаштовані під конкретні потреби користувача.

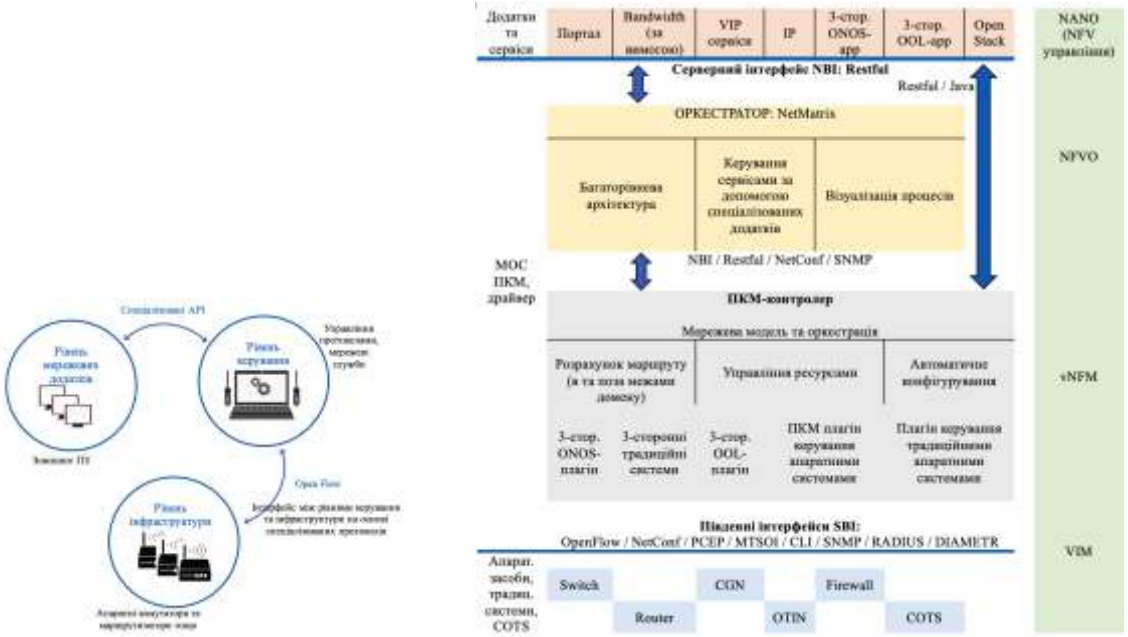
Розширена схема архітектури комп'ютерної SDN-мережі забезпечує повну гнучкість у керуванні потоками передавання, що проявляється в простому балансуванні потоку без необхідності залучення окремого пристрою. (рис. 1, б).

Архітектура SD-LAN та традиційний підхід до організації локальної мережі

Локальна мережа (Local Area Network, LAN) є сукупністю комп'ютерів, які з'єднані між собою за допомогою провідного або безпровідного зв'язку, користуються спільним мережевим обладнанням та програмним забезпеченням, і підпорядковані єдиному адміністративному контролю. LAN забезпечують можливість спільної оброблення даних користувачами, підключеними до мережі комп'ютерами, обміну інформацією між користувачами та спільного використання програм та обладнання [11-14].

Важливо відзначити, що багато офісів дозволяють користувачам підключати свої власні пристрої до локальної мережі, що відомо як «BYOD» (Bring your own device, принеси свій власний пристрій). Це створює питання щодо безпеки, які системні адміністратори повинні враховувати.

Для забезпечення ефективної роботи LAN часто використовують один або кілька комп’ютерів у ролі серверів. На серверах зберігаються програми та бази даних (БД), які можуть бути використані спільно. Комп’ютери, які підключені до мережі, і які використовуються для роботи з цими ресурсами, називаються робочими станціями. У деяких випадках на робочих станціях, які працюють із даними на сервері (наприклад, використовують БД), можуть не встановлювати жорстких дисків з метою економії або з міркувань безпеки.



а) б)

Рисунок 1 – Базова схема (а) та розширена (б) архітектури комп’ютерної SDN-мережі

Архітектура SD-LAN ґрунтується на принципах SDN і SD-WAN, що дозволяє мережевим адміністраторам керувати та налаштовувати мережу через програмне забезпечення, використовуючи централізований підхід та розділяючи мережу на потоки, щоб керувати розподілом ресурсів. Це забезпечує особливі переваги, такі як адаптивність, гнучкість, економічність та можливість масштабування для дротових та бездротових мереж доступу.

Адаптивність в мережі – це її здатність автоматично адаптуватися, налаштовуючи параметри, щоб забезпечити оптимальну роботу підключених пристроїв. В SD-LAN ця адаптивність досягається завдяки таким технологіям, як автоматична діагностика пристроїв, системи прикладних протоколів для налаштування хмарної мережі, автоматизація мережевих завдань та віртуалізація. Ці технології дозволяють мережі SD-LAN налаштовуватися автоматично відповідно до потреб підключених пристроїв, забезпечуючи оптимальну продуктивність і правильну роботу.

Гнучкість мережі – це її здатність змінювати параметри, щоб задовольняти потреби користувачів. Ця гнучкість досягається за допомогою маршрутизації, віртуалізації, контролю доступу та забезпечення безпеки. Це дозволяє мережі автоматично адаптуватися до змін у потребах користувачів.

Економічність – це принцип досягнення максимальної ефективності при найменших витратах. У SD-LAN ця економічність досягається завдяки технологіям, таким як розподіл обчислювальної потужності, використання програмно-апаратних архітектур, протоколи масштабного управління та мережеві інструменти для управління ресурсами. Це дозволяє використовувати бюджетні і легко адмініструвані програмно-апаратні рішення, що сприяють зниженню витрат на розвиток і експлуатацію мережі.

Розширення масштабу дротових і бездротових мереж доступу в SD-LAN включає в себе збільшення кількості користувачів, які можуть отримати доступ до мережі через одну точку входу, а також збільшення масштабу мережі, що дозволяє передавати дані від користувача до користувача безпосередньо.

Для досягнення розширення масштабу таких мереж використовуються наступні технології, підходи і протоколи:

- Технології віртуалізації: вони включають віртуалізацію мережі, віртуальні локальні мережі (VLAN) та віртуальні приватні мережі (VPN).
- Quality of Service (QoS): цей механізм дозволяє управляти пропускною здатністю мережі.
- Безпека мережі: забезпечення безпеки мережі за допомогою захисту мережі, такого як фільтрація пакетів, шифрування даних і ідентифікація користувачів.
- Протоколи: включають Ipv4, Ipv6, TCP/IP, UDP, які дозволяють мережі обмінюватися даними.
- Бездротові технології: такі як Wi-Fi, Bluetooth та інші бездротові технології, які надають користувачам можливість отримувати доступ до мережі.

Все це реалізується з урахуванням важливої безперервності бізнесу на рівні доступу до мережі.

Для розуміння вкладення цієї концепції: SD-LAN представляє собою систему, яка контролюється програмами та правилами, і вона відрізняє апаратний та програмний рівні, створюючи мережі, які автоматично організовуються та централізовано управляються. Ці мережі прості у використанні, інтеграції та масштабуванні [11].

Використання SD-LAN надає більший контроль над комп’ютерною SDN-мережі аж до рівня застосунків та дозволяє отримати глибше розуміння продуктивності та використання мережі.

Завдяки архітектурі SD-LAN можна значно легше налаштувати комутатори для керування локальними мережами, впровадити віртуалізацію локальної мережі та застосовувати політику безпеки. Ця автоматизована функція спрощує операції, зменшує витрати та використовує мережу WAN і LAN для забезпечення безпечного підключення.

Архітектура SD-WAN та традиційний підхід до організації міжмережевої взаємодії

Зазвичай, під глобальною мережею (Wide Area Network, WAN) розуміють телекомунікаційну структуру, яка з’єднує різні локальні комп’ютерні мережі. Ця структура використовує загальний протокол зв’язку і методи обміну даними [15].

На відміну від локальних мереж, глобальні мережі мають більш складну топологію та структуру. Основою для передавання даних у WAN є комутаційні вузли, які сполучені між собою каналами передавального середовища. Місце та кількість таких вузлів обирається так, щоб забезпечити необхідну пропускну здатність для передавання даних з мінімальними витратами. Канали передавання даних призначені для передавання дискретної інформації у вигляді даних. Для надійної передавання інформації ставляться високі вимоги до якості передавання даних.

У WAN всю роботу виконує комунікаційний сервер, і зазвичай використовується декілька таких виділених серверів. У великих мережах може бути кілька файл-серверів, які виступають як сховище для даних, оскільки у таких мережах потрібно зберігати великі обсяги інформації та забезпечувати ефективний доступ до неї з боку робочих станцій. У WAN зазвичай підключено велику кількість робочих станцій. Для цього часто використовуються спеціальні сервери доступу, які дозволяють ефективно підключати багато робочих станцій до комп’ютерної мережі. Важливо також забезпечити потрібну пропускну спроможність для передавання даних в мережі, при цьому заощаджуючи ресурси. Таким чином, кількість і розташування вузлів комутації обираються так, щоб відповідати цим вимогам [14].

Для підключення віддалених комп’ютерів до WAN використовуються різні засоби зв’язку, такі як оптичні волоконні кабелі, телефонні лінії, супутниковий та радіозв’язок. Спосіб приєднання конкретного комп’ютера до WAN впливає на швидкість та безпеку передавання даних до цього комп’ютера в глобальній мережі.

У WAN можуть бути об’єднані локальні мережі, які працюють за різними протоколами. Для забезпечення взаємодії протоколів у таких випадках використовують спеціальні засоби, які називаються шлюзами. Шлюзи можуть бути апаратними або програмними.

Існують кілька основних способів підключення до WAN:

1) Комутоване з’єднання: використовуємо телефонні лінії для передавання даних. Для організації зв’язку необхідно мати модем, який перетворює цифровий комп’ютерний сигнал на формат, придатний для передавання через телефонну лінію і навпаки. Підключення до глобальної мережі за допомогою комутованого з’єднання є епізодичним, тобто користувач приєднується до мережі лише тоді, коли це необхідно. Нині цей спосіб комутації застосовується досить рідко.

2) Безперервне з’єднання: використовуємо окремий кабель або виділену лінію для зв’язку з провайдером. Цей метод зазвичай є безпечним і швидким, але він може бути вартісним, особливо якщо провайдер розташований на великій відстані від користувача.

3) З’єднання за допомогою супутникового та радіо-зв’язку: використання супутникового або радіо-зв’язку для підключення до глобальної мережі. Він може бути дуже швидким, але є дорогим і вимагає спеціального обладнання, наприклад, супутникової антени. Крім того, він може бути вразливим до атмосферних і природних впливів.

Ці різні способи підключення мають свої переваги і недоліки, і вибір залежить від конкретних

потреб та умов користувача.

SDN-мережірована глобальна мережа (SD-WAN) забезпечує контроль за фізичними та віртуальними компонентами глобальної мережі. Важливо відзначити, що багато з технологій, що складають SD-WAN, не є новими, але представляють собою комбінацію методів агрегації, централізованого управління та динамічного розподілу пропускної здатності мережі між точками підключення.

За словами аналітика Gartner Ендрю Лернера, який вивчає ринок SD-WAN, привабливими перевагами цієї технології є простота впровадження, централізована керованість та економія витрат. За його оцінками, впровадження SD-WAN може коштувати приблизно в два з половиною рази менше, ніж традиційна архітектура глобальної мережі [16].

З іншого боку, SD-LAN використовує складні технології, такі як мережевий аналіз, маршрутизація, кількісний аналіз, аутентифікація та захист від зовнішнього втручання, для вирішення складних завдань. Однак це надає IT-відділам можливість працювати швидше та більш прогресивно.

SD-WAN також надає можливість гнучко керувати мережею, одночасно зберігаючи централізовані заздалегідь визначені корпоративні політики, які контролюють маршрутизацію додатків. Це дає можливість визначати, які програми працюють через WAN, і встановлювати політики щодо їх пріоритету та використання.

Крім того, SD-WAN використовує динамічний вибір WAN для оптимальної маршрутизації цих додатків через шляхи з найвищою продуктивністю. Також, за допомогою SD-WAN можна використовувати кілька доступних каналів у конфігурації «active/active» для балансування навантаження та автоматичного відновлення після невеликого або повного відмови. Весь трафік між різними місцями проходить через динамічні, повністю зашифровані тунелі та може бути сегментованим, що забезпечує високий рівень безпеки.

Семантична модель SDN та схему розподілу потоків трафіку в SDN

Комп’ютерній SDN-мережі нині є надважливим інструментом управління великих обсягів даних із централізованим управлінням. Технологія SDN дозволяє ефективно керувати значним трафіком в мережах, що відповідають стандартам.

Завдяки ПЗ, яке можна використовувати на рівні застосунків SDN-мереж, вирішується багато задач та проблем. Воно надає можливість управляти та автоматизувати процеси та інтегрувати додаткові моделі та функції, що можуть сприяти зниженню витрат та покращенню характеристик мережі SDN.

Такий підхід має свої обмеження, включаючи недостатню надійність та високу ціну, що випливає з архітектури «клієнт-сервер» або її централізованого характеру. Деякі мережі є гетерогенними, і SDN може допомогти покращити керування цими мережами та прискорити впровадження обладнання різних виробників. Однак це може ускладнювати роботу персоналу та робити обслуговування мережі складним та дорогим завданням.

Архітектура SDN-мереж базується на ієрархічній системі передавання трафіку, де процеси управління контролером SDN керують комутаторами Open vSwitch (OvS) та таблицею переадресації. В даній архітектурі виникає залежність рівнів одного від одного, що може призводити до нестабільності в з’єднанні між цими рівнями. Однак варто зауважити, що така архітектура демонструє покращену ефективність, і головне завдання полягає в забезпеченні надійності та розробці моделі для резервування та розподілу слабких частин системи.

У мобільній мережі зі структурою, побудованою на класичній IP-адресації, кожен елемент функціонує самостійно, що призводить до децентралізованої структури і, більшої надійності. Однак IP-мережа має свої обмеження, такі як менша ефективність та менш динамічна система управління, що робить її менш підходящою для майбутніх мереж 5G.

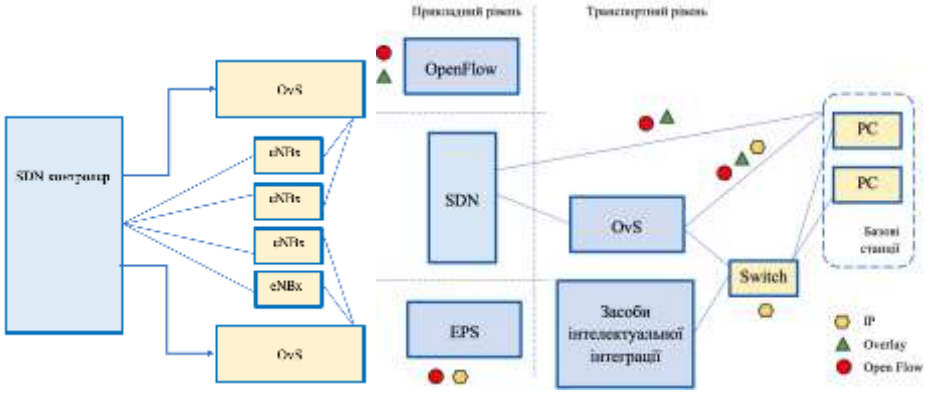
Слід зауважити, що розробка SDN-мережі «з нуля» може бути дорогою і непрактичною, оскільки зупинка роботи існуючої інфраструктури надто складна. У такому контексті мережа OpenFlow набула популярності, оскільки можна розгорнути її поверх вже існуючої інфраструктури та розвивати її як окремий «налаштований шар» (Overlay).

На моделі SDN (рис. 2) можна побачити, що взаємодія структурована таким чином, що контролер, з’єднаний з кожним блоком, може керувати кожним блоком окремо та безпосередньо отримувати показники напряму.

Інформаційні процеси інфраструктури сучасної SDN мережі

Процеси передавання даних в централізованих мережах відрізняються від процесів передавання трафіку в децентралізованих мережах, а саме основна взаємодія централізованих процесів проходить за допомогою сервера або групи серверів, відповідаючи кожен за свої задачі. В централізованій мережі або, якщо мова йде про мережу SDN, взаємодія керується сервером. Простий приклад даної системи – клієнт-серверна архітектура мережі. На рисунку 2, б зображена схема розподілу потоків трафіку в комп’ютерній мережі.

Треба зауважити, що SDN відокремлює сервісний трафік від трафіку користувачів, тому обчислювальної потужності треба набагато менше ніж для роботи з величезними масивами, в яких капсульовано користувацький і сервісний трафік. Варто також додати, що смуга передавання для кожного користувача в системі SDN на одного клієнта рівна тому, скільки цьому користувачеві потрібно, що цим самим робить роботу мережі більш оптимальною.

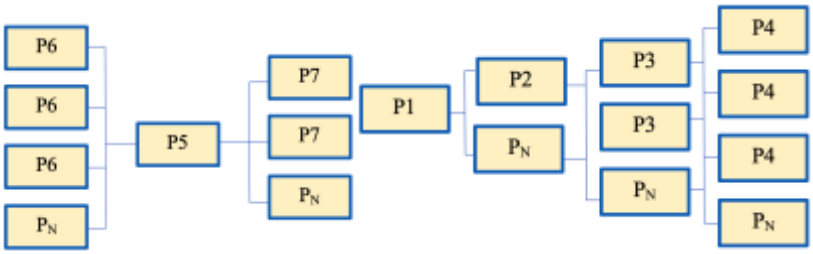


а) б)

Рисунок 2 – Семантична модель SDN (а) та схема розподілу потоків трафіку (б)

Запропонувати спосіб розрахунку надійності мережі

Для розрахунку показників надійності спочатку треба абстрагувати архітектуру до блочного рівня, як показано на рисунку 3, де а) це децентралізована мережа (класична IP-мережа), б) це централізована мережа (схема SDN), P – довільний показник надійності.



а) б)

Рисунок 3 – Блоки архітектури під час розрахунку надійності мережі, де а) – централізована мережа SDN, б – децентралізована мережа IP

Ідея способу розрахунку надійності – можливість прорахувати вразливості аналітичними виразами та застосувати відомі підходи для підвищення потрібних показників (наприклад, методику резервування або дублювання) даної системи (1).

$$P\{\sum_{i=1}^{n} A_i\} = 1 - P\{\prod_{i=1}^{n} \bar{A}_i\} \quad (1)$$

Ймовірність події A – P{A} визначається частотою її появи в серії випробувань і описується (2):

$$F_A = \frac{n_A}{N} \underset{N\to\infty}{\longrightarrow} P\{A\}, \quad (2)$$

де: À – деяка подія; N – загальне число дослідів; n_A – число появи події À; P {A} – ймовірність події À.

Ймовірність достовірної події: $P\{A_\partial\} = \frac{n_a}{N} = \frac{N}{N} = 1$. Ймовірність неможливої події: $P\{A_i\} = \frac{\ddot{I}_i}{N} = \frac{0}{N} = 0$. Ймовірність випадкової події може змінюватись в межах $0 \le P\{A\} \le 1$, але ніколи $P\{A\} > 1$. Для повної групи подій: $P\{A\} + P\{\bar{A}\} = 1$. Ймовірність складної події може бути представлена через суму і добуток простих подій. Добутком подій $A_1 \cdot A_2 \cdot A_3 \cdot \ldots \cdot A_n$ називається складна подія, яка складається з того, що відбувається і подія $A_1, A_2, A_3, \ldots, A_n$n, тобто відбуваються всі події. Така подія позначається так (3-4):

$$A_1 \cdot A_2 \cdot A_3 \cdot \ldots \cdot A_n = \prod_{i=1}^{n} A_i; \quad (3)$$

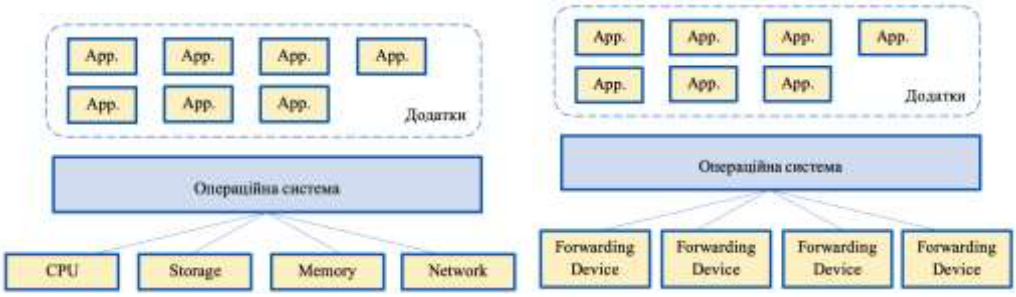
$$P\{\prod_{i=1}^{n} A_i\} = \prod_{i=1}^{n} P\{A_i\} \quad (4)$$

Сумою подій $A_1 + A_2 + A_3 + \cdots + A_n$ називається складна подія, яка має на увазі те, що відбудеться, або подія $A_1, A_2, A_3, \ldots, A_n$n, тобто виконується хоча б одна з подій. Сума подій позначається $A_1 + A_2 + A_3 + \cdots + A_n = \sum_{i=1}^{n} A_i$ таким виразом.

Модель взаємодії мережевої ОС із комп'ютерною SDN-мережею та спосіб оброблення трафіку

Модель взаємодії мережевої операційної системи та SDN. На прикладному рівні можна розглядати операційні системи (ОС) хостів (комп'ютерів) на трьох рівнях (див. рис. 3, а). Перший рівень – це сама ОС, яка є посередником, контролюючи доступ додатків до базового апаратного забезпечення (АЗ). ОС також надає основні служби, які сприяють цьому процесу і відповідає за низькорівневе управління АЗ [17].

Модель SDN-мереж має схожість з моделлю операційної системи (див. рис. 3, б). Основна відмінність полягає в тому, що на середньому рівні розташована мережева операційна система (МОС), іншими словами, SDN-контролер. МОС зазвичай надає базові служби, які допомагають у взаємодії з хосьами мережі та забезпечують програмований інтерфейс для мережевих додатків [16-17]. Мережеві пристрої тут розташовані замість АЗ і виконують оброблення мережевого трафіку. Ці пристрої отримують пакети та виконують різні операції, такі як відкидання пакету, зміна заголовків, відправка пакетів через один чи декілька інтерфейсів та оновлення лічильників.



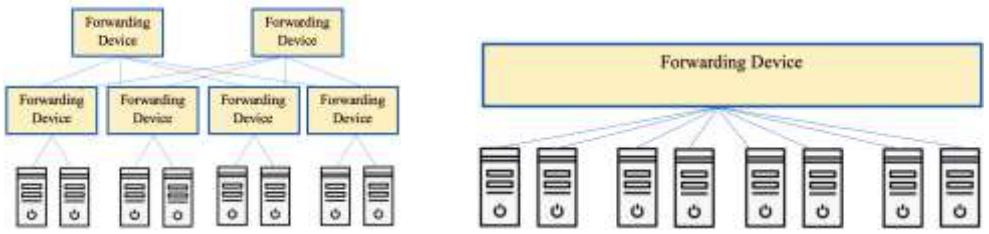
а) б)

Рисунок 3 – Модель операційної системи з та без взаємодії з SDN

Інструкції для оброблення пакетів надходять від SDN-контролера. На вищому рівні розташовані мережеві додатки, які спеціалізуються на мережевій функціональності та виконують різноманітні завдання для оптимізації мережі. Мережеві додатки грають ключову роль у реалізації SDN та можуть виконувати різні функції для покращення продуктивності та управління мережею. Застосування переваг такої комбінації моделей, дозволяє відстежувати рух трафіку в мережах і значно полегшує перехід від традиційної архітектури до SDN.

Спосіб оброблення трафіку в SDN

Безпека потоків пакетів у SDN-мережі. Аналіз заголовків пакетів визначає подальші дії для оброблення пакетів при їх надходженні на мережевий пристрій, що під контролем SDN. Мережевий пристрій може відразу мати дані про етапи та спосіб оброблення пакета, або, у випадку необхідності, звернутися до SDN-контролера для отримання таких інструкцій. Мережеві додатки на SDN-контролері будуть інструктувати, які дії слід виконувати з конкретним пакетом і передають цю інформацію з інструкціями мережевим пристроям пересилання (див. рис. 4, а).



а) б)

Рисунок 4 – Оброблення трафіку на рівні абстрактної мережі (а) на рівні додатків (б)

Пристрої пересилання, в свою чергу, діють відповідно до отриманих вказівок. Важливою є можливість кешування інструкцій пристроєм пересилання, що дозволяє зменшити навантаження на

SDN-контролер і прискорити оброблення мережевого трафіку.Аналогічний процес розгортається по маршруту від одного мережевого пристрою до іншого, доки пакет не досягне свого пункту призначення. Надалі, новосформовані пакети можуть проходити через мережу без звернення до SDN-контролера. Контролер SDN здатний створити абстрактну або спрощену модель мережі для мережевих додатків, які використовують цю інформацію для прийняття важливих рішень щодо впровадження мережевих політик.

Безпека мережевих додатків. Мережевий додаток може бути осторонь деталей щодо різних маршрутів, які пакети подолали б у мережі. SDN-контролер може створити абстракцію всієї мережі, розглядаючи її як великий комутатор (рис. 4, б). Ідеальною абстракцією пересилання була б така, яка дозволяла б мережевим додаткам (керуючим програмам) визначати бажану поведінку пересилання, не вдаючись до деталей, пов’язаних з конкретним обладнанням. Один із шляхів до реалізації цієї ідеї – це OpenFlow, який можна порівняти з «драйвером пристрою» у мережевій операційній системі.

Безпекова модель та прототип комп’ютерної SDN-мережі.

Компоненти безпекової моделі SDN. Безпекові складові в моделі SDN) можна уявити як композицію різних рівнів, кожен з яких виконує свої специфічні функції. Більшість з цих складових завжди присутні в будь-якій реалізації SDN, включно з: мережевими додатками; інтерфейсами додатків, таких як Java API і NorthBound (REST Conf); SDN-контролером, який містить служби топології, інвентаризації, статистики та хост-трекери; SouthBound інтерфейсами, які можуть містити протоколи, такі як OpenFlow, OVSDB, NETCONF і SNMP; комутаційними пристроями.

Модель мережі із гнучкими ресурсами. Гнучкий підхід до створення мережі фокусується на швидких та адаптивних змінах. Ці невеликі та регулярні зміни сприяють підвищенню продуктивності додатків, збільшенню безпеки даних і сприяють швидкому розгортанню додатків та сервісів.

Мережа SDN дозволяє ефективно розділяти мережу для різних видів робочих завдань (див. рис. 3.6). Цей розподіл може бути реалізований на різних рівнях. Наприклад, на рівні SouthBound інтерфейсу трафік може бути спрямований до повністю окремих SDN-контролерів.

На рівні NorthBound інтерфейсу різні види трафіку можуть бути оброблені різними мережевими додатками або різними способами цими ж додатками. Це можливість розглядати мережу як ресурс, що використовується різними клієнтами або завданнями і дозволяє кожному клієнту або завданню використовувати мережу відповідно потребам.

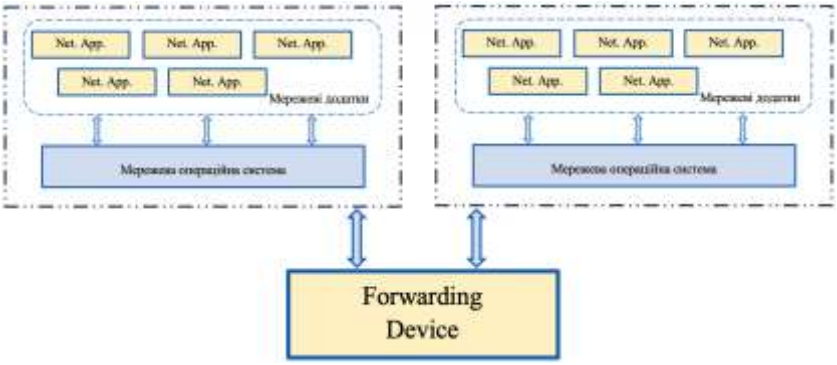


Рисунок 5 – Розподіл мережі для різних робочих навантажень

Модель відмовостійкості мережі. Висока надійність SDN-мережі досягається завдяки швидкому виявленню і усуненню відмов, причому це відбувається протягом короткого періоду. Є два основних підходи до забезпечення надійності в SDN-мережаж: 1) захисне перемикання (резервування) та 2) відновлення (ремаршрутизація).

Зазвичай SDN-контролери вважаються централізованими. У реальних мережах користувачі не повинні залежати від конкретного фізичного контролера SDN, що створює єдину точку відмови для всієї мережі. Крім того, існують питання масштабування. Існують різні методи забезпечення високої доступності та масштабованості в SDN-мережаж.

Один з таких методів – це кластеризація або групування (див. рис. 6). Цей підхід добре відомий в області серверів баз даних. Основна ідея полягає в тому, щоб мати кластер систем, які можуть розподіляти обчислювальні завдання балансовано, замість єдиної системи. Це забезпечує високу доступність, оскільки можуть бути відмови в окремих системах, але інші все ще можуть виконувати завдання. Крім того, цей метод забезпечує масштабованість, оскільки декілька систем можуть обробляти запити.

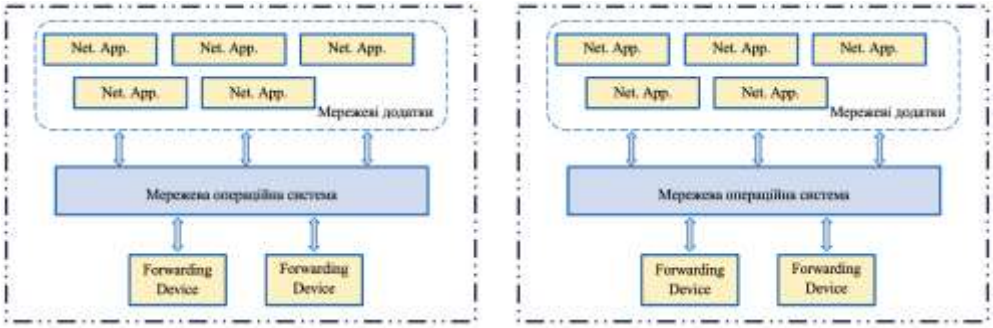


Рисунок 6 – Кластеризація мережі

Додатковою є можливість поділити якусь спеціалізовану частину мережі можна на різні регіони, де кожен регіон управляється власним контролером SDN (див. рис. 7). Різні регіони можуть взаємодіяти між собою, обмінюючи інформацію за потреби через протокол East-West.

Рисунок 7 – Ієрархічна кластеризація мережі

Отож, контролери SDN можуть бути організовані в ієрархічній структурі. Таким чином, з’являються контролери вищого рівня із спрощеною абстракцією мережі та контролери нижчого рівня, що розташовані ближче до мережевих пристроїв пересилання.

В розробленій мережі (рис. 8) для 9 пристроїв мережі, поділених на групи, виконані часові заміри (рис. 9,а) і середнє значення зменшення часу налаштування зменшилося приблизно у 10 разів (рис. 9,б).

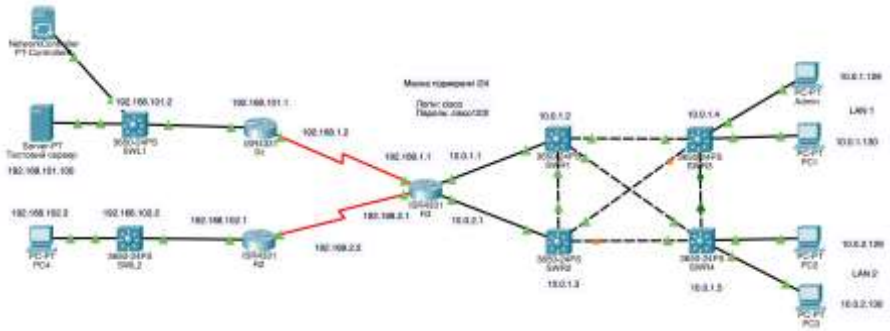


Рисунок 8 – Мережева конфігурація

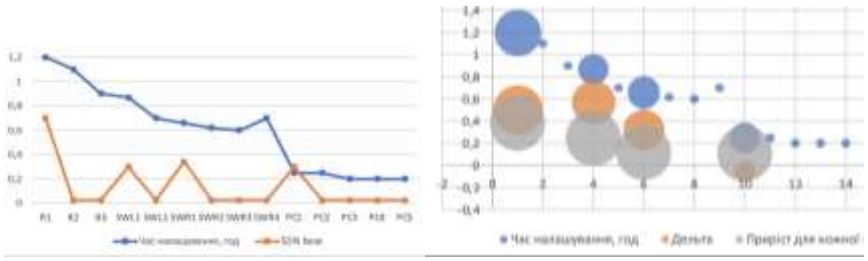


Рисунок 9 – Значення часу налаштування пристроїв у кожній з груп без (а) та з SND (б)

Очевидно, що застосування контролерів для програмного керування мережами є доцільним та прогресивним в умовах постійного розширення мережі, зміни кількості мережевих пристроїв чи хостів.

Висновки

Потреба у аналізі та вдосконаленні методів та засобів захисту інформаційних та інших ресурсів в комп'ютерній SDN- мережі стала основою для даного дослідження. У роботі досягнуто підвищення рівня інформаційної безпеки ресурсів SDN-мережі за рахунок: 1) зменшення часу втручання у мережу; 2) та із одночасним застосування вдосконаленого способу оброблення трафіку на основі мережевої безпеки потоку пакетів, що дозволяє бажану мережевим додатком поведінку пересилання.

Загалом результати полягають у такому:

- Вдосконалено модель взаємодії мережевої операційної системи та програмно-керованої мережі, що дає можливість відстежувати процеси, що відбуваються в мережах з ресурсами компанії, та забезпечує ефективний контроль і безпеку цих ресурсів;
- Вдосконалено спосіб передавання трафіку на основі мережевої безпеки потоку пакетів, що дозволяє бажану мережевим додатком поведінку пересилання;
- Вдосконалено модель відмовостійкості мережі за рахунок висхідного представлення компонентів безпеки моделі SDN.

Список літератури

[1] Todd M. S., Rahman S. M. Complete Network Security Protection for Sme's Within Limited Resources. International Journal of Network Security & Its Applications (IJNSA). 2013. Vol. 5, no. 6.

[2] Alqahtani H. S. Latest Trends and Future Directions of Cyber Security Information Systems. Journal of Information Engineering and Applications. 2016. Vol. 6, no. 11.

[3] Троян С. О. Захист інформаційних ресурсів. Умань, 2012. 120 с.

[4] Медяник А. Інформаційна безпека та методи захисту інформації. 2020.

[5] Simmons A. Software-Defined Networking (SDN) Explained. Dgtl Infra. URL: https://dgtlinfra.com/software-defined-networking-sdn/.

[6] Ot A. The Software-Defined Networking (SDN) Market in 2022 | Enterprise Storage Forum. Enterprise Storage Forum. URL: https://www.enterprisestorageforum.com/networking/software-defined-networking-market/.

[7] Software-Defined Networking: Challenges and research opportunities for Future Internet / A. Hakiri et al. Computer Networks. 2014. Vol. 75. P. 453–471. URL: https://doi.org/10.1016/j.comnet.2014.10.015.

[8] Ashton, Metzler. The Business Case for Deploying SDN in Enterprise Networks. Leverage technology & talent for success.

[9] Gray K., Nadeau T. D. SDN: Software Defined Networks. Sebastopol : O'Reilly Media, Inc, 2013.

[10] Brief About What does The Future hold for Software Defined Networking (SDN). YourTechDiet. URL: https://yourtechdiet.com/blogs/sdn-future/.

[11] SD-LAN vs LAN – What Are The Key Differences?. Extreme Marketing Team. URL: https://www.extremenetworks.com/extreme-networks-blog/sd-lan-vs-lan-what-are-the-key-differences/.

[12] Селюков О. В. Забезпечення стандартизації параметрів управління для SDN архітектури при надійній передавання інформації / О. В. Селюков, Ю. В. Хмельницький, В.М. Лоза, Р.В. Бойко // Збірник наукових праць Військового інституту Київського національного університету імені Тараса. – 2018. – С. 134–145.

[13] Управління телекомунікаціями із застосуванням новітніх технологій / Кривуца, Стеклов, Беркман та ін.]., 2007. – 384 с. – (Підручник для ВНЗ).

[14] Комп'ютерні мережі: навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2022. – 228 с.

[15] Комп'ютерні мережі:[навчальний посібник] / А. Г.Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. – Львів: Магнолія 2006, 2013. – 256 с.

[16] Коробейнікова Т.І. Розгляд архітектури програмно-керованих мереж / Коробейнікова Т.І., Калько Т.С., Лужецька Н. М. // International scientific journal «Grail of Science» – 2023. – № 23 (May, 2023). – С. 228–237. ISSN: 2710–3056. ISBN 979-8-88955-791-3. https://doi.org/10.36074/grail-of-science.09.06.2023.36

[17] Кононенко А. В. Концепція software-defined-networking та основні принципи openflow / А. В. Кононенко, І. М. Кучма, М. В. Перетятько, В. О. Кацалап, Д. О. Размислов // Наукові записки Українського науково-дослідного інституту зв'язку. – 2018. - № 3. – С. 51-58.

[18] Савицька Л.А., Коробейнікова Т.І. Удосконалений метод розробки API підвищеної швидкодії Інформаційні технології та комп`ютерна інженерія 2021: - №1 (50). – С. 31–35

[19] Савицька Л. А. Програмний модуль попереднього діагностування пацієнтів на основі нейронної мережі Кохонена [Текст] / Л. А. Савицька, Н. В. Добровольська, В. О. Кондратюк // Інформаційні технології та комп`ютерна інженерія. – 2023. – № 1. – С. 66-74.

References

[1] Todd M. S., Rahman S. M. Complete Network Security Protection for Sme's Within Limited Resources. International Journal of Network Security & Its Applications (IJNSA). 2013. Vol. 5, no. 6.

[2] Alqahtani H. S. Latest Trends and Future Directions of Cyber Security Information Systems. Journal of Information Engineering and Applications. 2016. Vol. 6, no. 11.

[3] Troyan S. O. Zakhyst informatsiynykh resursiv. Uman', 2012. 120 s.

[4] Medyanyk A. Informatsiyna bezpeka ta metody zakhystu informatsiyi. 2020.

[5] Simmons A. Software-Defined Networking (SDN) Explained. Dgtl Infra. URL: https://dgtlinfra.com/software-defined-networking-sdn/.

[6] Ot A. The Software-Defined Networking (SDN) Market in 2022 | Enterprise Storage Forum. Enterprise Storage Forum. URL: https://www.enterprisestorageforum.com/networking/software-defined-networking-market/.

[7] Software-Defined Networking: Challenges and research opportunities for Future Internet / A. Hakiri et al. Computer Networks. 2014. Vol. 75. P. 453–471. URL: https://doi.org/10.1016/j.comnet.2014.10.015.

[8] Ashton, Metzler. The Business Case for Deploying SDN in Enterprise Networks. Leverage technology & talent for success.

[9] Gray K., Nadeau T. D. SDN: Software Defined Networks. Sebastopol : O"Reilly Media, Inc, 2013.

[10] Brief About What does The Future hold for Software Defined Networking (SDN). YourTechDiet. URL: https://yourtechdiet.com/blogs/sdn-future/.

[11] SD-LAN vs LAN – What Are The Key Differences?. Extreme Marketing Team. URL: https://www.extremenetworks.com/extreme-networks-blog/sd-lan-vs-lan-what-are-the-key-differences/.

[12] Selyukov O. V. Zabezpechennya standartyzatsiyi parametriv upravlinnya dlya SDN arkhitektury pry nadiyniy peredavannya informatsiyi / O. V. Selyukov, YU. V. Khmel'nyts'kyy, V.M. Loza, R.V. Boyko // Zbirnyk naukovykh prats' Viys'kovoho instytutu Kyyivs'koho natsional'noho universytetu imeni Tarasa. – 2018. – S. 134–145.

[13] Upravlinnya telekomunikatsiyamy iz zastosuvannyam novitnikh tekhnolohiy / Kryvutsa, Steklov, Berkman ta in.]., 2007. – 384 s. – (Pidruchnyk dlya VNZ).

[14] Komp'yuterni merezhi: navch. posibnyk / T. I. Korobeĭnikova, S. M. Zakharchenko. – L'viv: Vydavnytstvo L'vivs'koï politekhniky, 2022. – 228 s.

[15] Komp"yuterni merezhi:[navchal'nyy posibnyk] / A. H.Mykytyshyn, M. M. Mytnyk, P. D. Stukhlyak, V. V. Pasichnyk. – L'viv: Mahnoliya 2006, 2013. – 256 s.

[16] Korobeynikova T.I. Roz·hlyad arkhitektury prohramno-kerovanykh merezh / Korobeynikova T.I., Kal'ko T.S., Luzhets'ka N. M. // International scientific journal «Grail of Science» – 2023. – № 23 (May, 2023). – S. 228–237. ISSN: 2710–3056. ISBN 979-8-88955-791-3. https://doi.org/10.36074/grail-of-science.09.06.2023.36

[17] Kononenko A. V. Kontseptsiya software-defined-networking ta osnovni pryntsypy openflow / A. V. Kononenko, I. M. Kuchma, M. V. Peretyat'ko, V. O. Katsalap, D. O. Razmyslov // Naukovi zapysky Ukrayins'koho naukovo-doslidnoho instytutu zv"yazku. - 2018. - № 3. - S. 51-58.

[18] Savyts'ka L.A., Korobeynikova T.I. Udoskonalenyy metod rozrobky ARI pidvyshchenoyi shvydkodiyi Informatsiyni tekhnolohiyi ta komp`yuterna inzheneriya 2021: - №1 (50). - S. 31–35

[19] Savyts'ka L. A. Prohramnyy modul' poperedn'oho diahnostuvannya patsiyentiv na osnovi neyronnoyi merezhi Kokhonena [Tekst] / L. A. Savyts'ka, N. V. Dobrovol's'ka, V. O. Kondratyuk // Informatsiyni tekhnolohiyi ta komp`yuterna inzheneriya. – 2023. – № 1. – S. 66-74.

Стаття надійшла: 20.11.2023 р.

Відомості про авторів

Савицька Людмила Анатоліївна – к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, Вінниця

Savytska Liudmyla – PhD, associate professor of computing engineering department, Vinnytsya national technical university, Vinnytsya

Коробейнікова Тетяна Іванівна – к.т.н., доцент кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка», кафедра безпеки інформаційних технологій

Korobeinikova Tetiana – PhD, associate professor of information technology security department, National university “Lvivska Politechnika”

Леонтьєв Ігор Віталійович – магістр кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, Вінниця

Leontiev Ihor Vitaliyovych – magister of computing engineering department, Vinnytsya national technical university, department of the computer engineering, Vinnytsy

Богомолов Сергій Віталійович – к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, Вінниця

Bohomolov Serhii – PhD, associate professor of computing engineering department, Vinnytsya national technical university, Vinnytsya

L. Savytska, T. Korobeinikova, I. Leontiev, S. Bohomolov

METHODS AND MEANS OF PROTECTING RESOURCES IN COMPUTER SDN NETWORK

Vinnytsya national technical university, Vinnytsya