DOI: https://doi.org/10.36910/6775-2524-0560-2023-53-14
УДК 004.72
Багнюк Наталія Володимирівна[1], к.т.н., доцент
https://orcid.org/0000-0002-7120-5455
Луцький національний технічний університет, м.Луцьк, Україна
Мельник Василь Михайлович[2], к.ф-м.н., доцент
https://orcid.org/0000-0001-8282-6639
Булатецький Віталій Вікторович[3], к.ф.-м.н., доцент
https://orcid.org/0000-0002-9883-4550
Сичов Денис Ігорович[1], магістр
Карпович Володимир Олегович[1], магістр
[1] Луцький національний технічний університет, м.Луцьк, Україна,
[2] Волинський фаховий коледж Національного університету харчових технологій, м.Луцьк, Україна,
[3] Волинський національний університет імені Лесі Українки, м.Луцьк, Україна

АЛГОРИТМІЧНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АНАЛІЗУ СТАНУ ТА ФУНКЦІОНУВАННЯ РОЗПОДІЛЕНОЇ ГЕТЕРОГЕННОЇ МЕРЕЖІ

Багнюк Н. В., Мельник В.М., Булатецький В.В., Сичов Д.І., Карпович В.О. Алгоритмічне програмне забезпечення стану та функціонування розподіленої гетерогенної мережі. Представлено програмне забезпечення для аналізу, моніторингу та керування розподілених гетерогенних мереж. Проведено порівняння з іншими безкоштовними та умовно-безкоштовними засобами контролю та керування мережами.
Ключові слова: ЗККМ, мережа, SNMP, MAC-адреса, IP-адреса, моніторинг.

Bagniuk N., Melnyk V., Bulatetskyi V., Sychov D., Karpovych V. Algorithmic software for analyzing the state and operation of a distributed heterogeneous network. The presented software is designed for analysis, monitoring, and management of distributed heterogeneous networks. A comparison with other free and conditionally-free network control and management tools has been conducted.
Keywords: NMS, network, SNMP, MAC-address, IP-address, monitoring.

Постановка наукової проблеми. Сучасні розподілені гетерогенні мережі, такі як IoT-екосистеми, обчислювальні хмари та мобільні мережі, активно інтегруються в різні сфери нашого життя. Вони знаходять застосування в медицині, промисловості, транспорті та багатьох інших галузях. Наприклад, у смарт-містах такі мережі допомагають оптимізувати рух транспорту, контролювати енергоспоживання та надавати громадянам різноманітні сервіси. У медицині вони дозволяють збирати дані про стан пацієнта в реальному часі, аналізувати їх та надавати рекомендації лікарям. Ці мережі включають в себе різноманітні пристрої та системи, які мають різні характеристики та можливості. Проте, з ростом складності таких мереж, з'являється потреба в алгоритмічному програмному забезпеченні, яке б дозволяє аналізувати стан та функціонування цих систем. Відсутність ефективних інструментів для аналізу може призвести до зниження продуктивності, збоїв у роботі мережі, а також до проблем з безпекою та конфіденційністю даних. Як забезпечити стабільність роботи мережі, коли в ній тисячі пристроїв різних типів? Як вчасно виявляти і усувати збої? Як аналізувати великі обсяги даних, що надходять з різних джерел? Всі ці питання вимагають розробки нового алгоритмічного програмного забезпечення. Розробка ефективних алгоритмів та програмного забезпечення для аналізу розподілених гетерогенних мереж є важливим кроком на шляху до створення надійних, безпечних та ефективних систем, які будуть відповідати вимогам сучасного світу.

Аналіз останніх досліджень і публікацій. За останні роки було опубліковано численні дослідження, присвячені проблемам аналізу та моніторингу розподілених гетерогенних мереж. Інженери активно працюють над розробкою нових методів та інструментів для ефективного управління такими системами. Однією з ключових робіт у цій області є стаття [2], де автори пропонують різні засоби контролю та керування мережами розподілених систем. У висновку автори рекомендують використовувати безагентову модель, яка знімає проблеми доступності активів мережі.

Виділення невирішених раніше частин загальної проблеми. Попри численні дослідження в області розподілених гетерогенних мереж, деякі аспекти цієї проблеми залишаються недостатньо дослідженими. Основні з них включають:

– Динамічна адаптація мережі до змінних умов. Більшість існуючих рішень передбачає статичну конфігурацію мережі, що може бути неефективною при динамічних змінах навантаження або умов роботи.

– Інтеграція з новітніми технологіями. З появою нових типів пристроїв та технологій, таких як квантові комп'ютери або нейронні мережі нового покоління, виникає потреба в їх інтеграції в розподілені гетерогенні мережі.

– Безпека та конфіденційність. Незважаючи на численні дослідження в області безпеки мереж, захист від нових видів загроз та атак залишається актуальною проблемою.

– Тому ці невирішені питання стали предметом дослідження та розробки нових методів та підходи для їх вирішення в контексті розподілених гетерогенних мереж.

Мета дослідження: розробка алгоритмічного програмного забезпечення, яке дозволить ефективно аналізувати стан та функціонування розподіленої гетерогенної мережі. Результатом є створений інструментарій, який допоможе інженерам та адміністраторам мережі виявляти потенційні проблеми, оптимізувати роботу мережі та гарантувати її стабільність та безпеку. Завдання дослідження:

– Розробка алгоритмів для динамічного моніторингу стану пристроїв у мережі.

– Створення методик аналізу великих обсягів гетерогенних даних, які надходять від різних пристроїв.

– Розробка механізмів для виявлення та відстеження аномалій та потенційних збоїв у роботі мережі.

– Створення інтерфейсу для взаємодії користувача з програмним забезпеченням, який буде інтуїтивно зрозумілим та зручним для використання.

Успішна реалізація цих завдань дозволить значно підвищити ефективність управління розподіленими гетерогенними мережами та забезпечити їх надійність та безпеку.

Основна частина дослідження. Архітектура системи складається з кількох ключових компонентів, які взаємодіють між собою для забезпечення високої продуктивності та надійності в гетерогенному мережевому середовищі. В основі архітектури лежить модульна структура, що дозволяє гнучко налаштовувати систему відповідно до потреб користувачів та мережевих вимог. Основні компоненти архітектури включають серверну частину, клієнтську частину, базу даних та мережевий інтерфейс. Серверна частина відповідає за обробку даних, отриманих від мережевих пристроїв, та їх аналіз. Клієнтська частина надає інтерфейс для взаємодії користувачів з системою та відображення отриманих даних. База даних забезпечує зберігання та управління даними, а мережевий інтерфейс забезпечує взаємодію між серверною та клієнтською частиною та мережевими пристроїв.

Для забезпечення високої продуктивності та надійності, архітектура системи передбачає використання віртуалізації ресурсів, кластеризації серверів та балансування навантаження між ними. Також передбачено можливість горизонтального масштабування системи шляхом додавання додаткових сервісів або вузлів в кластер.

Архітектура системи також враховує вимоги безпеки та конфіденційності даних. Всі дані, які передаються та обробляються системою, захищені за допомогою сучасних криптографічних протоколів та технологій. Безпека даних забезпечується на рівні серверів, баз даних та мережевих з'єднань.

Крім того, архітектура системи передбачає інтеграцію з існуючою мережевою інфраструктурою та можливість взаємодії з іншими системами та платформами через API. Це дозволяє розширювати функціональність системи та адаптувати її до змінних вимог та умов експлуатації.

Отже, архітектура розробленої системи є гнучкою, масштабованою та надійною, що дозволяє ефективно використовувати її для моніторингу та аналізу гетерогенних мережевих середовищ.

Програмне забезпечення для аналізу стану та функціонування мережі є критично важливим у контексті постійного розширення корпоративних мереж. Це розширення відбувається завдяки збільшенню кількості пристроїв, процесів, служб та локацій, що призводить до зростання проблем, пов'язаних із розподіленим моніторингом. Гетерогенні мережі, що функціонують у розподіленому

режимі, породжують виклики, такі як безпека, конфіденційність, доступність та затримки, ускладнюючи процес моніторингу та обробки великих даних [3].

Вибір конкретних засобів контролю та керування мережами (ЗККМ) для специфічних потреб використання є складним завданням через велику кількість доступних варіантів. Кожна організація має унікальні вимоги до ЗККМ, що вимагає ретельного підходу до їх вибору. Існує безліч рекомендацій та характеристик, що допомагають здійснити обґрунтований вибір ЗККМ, враховуючи вагові коефіцієнти для різних груп характеристик. З практичної точки зору, серед численних ЗККМ, рекомендується вибирати ті, що регулярно оновлюються та доступні безкоштовно. Після відсіювання за допомогою цих критеріїв, для порівняння варто розглядати такі ЗККМ як Zabbix, NetXMS, OpenNMS, Cacti та Nagios [1].

Організації мають здійснювати детальний попередній аналіз для визначення своїх специфічних потреб у сфері управління мережевою інфраструктурою. Вибір конкретного засобу керування та моніторингу мережі визначається п'ятьма ключовими функціональними характеристиками, які сприяють ефективності використання засобу.

Крім того, вибір ЗККМ може залежати від таких факторів, як архітектура системи, мови програмування, технології зберігання та обробки даних, які використовуються. Системна архітектура, заснована на розширеннях за допомогою плагінів, дозволяє більш точно налаштовувати ЗККМ для вирішення специфічних задач моніторингу. Однак, це вимагає наявності більш висококваліфікованих фахівців. Модель, яка працює без агентів, вирішує проблеми, пов'язані з доступністю контрольованих мережевих активів.

У даному випадку, розглянувши різні ЗККМ, було вирішено написати власне програмне забезпечення для управління, моніторингу, аналізу звичайних та гетерогенних мереж. ПЗ написано на мові програмування Perl. Вона відома своєю потужністю та гнучкістю, а також володіє великою кількість вбудованих функцій та колекцій модулів, які містять готові рішення для різних задач. Для прикладу, використали наступні модулі:

– Discovery.pm – модуль для виявлення мережевих пристроїв. Він використовує SNMP для отримання інформації про пристрої в мережі.

– Arpnip.pm – модуль для отримання ARP-таблиць з мережевих пристроїв.

– Macsuck.pm – модуль для отримання таблиць MAC-адрес з мережевих пристроїв.

– Nbtstat.pm – модуль для отримання NetBios імен з пристроїв в мережі.

– Expire.pm – модуль для очищення старих даних з бази даних.

– Worker.pm – основний модуль, який керує виконанням інших модулів та задач.

В основному ПЗ використовує такі протоколи як SNMP (Simple Network Management Protocol), CDP (Cisco Discovery Protocol), LLDP (Link Layer Discovery Protocol), FDP (Foundry Discovery Protocol) та SONMP (SynOptics Network Management Protocol). Окремо використовується CLI (Command-Line Interface) та API (Application Programming Interface). CDP – пропрієтарний протокол Cisco для виявлення пристроїв. Він дозволяє пристроям розпізнавати один одного та обмінюватись базовою інформацією про конфігурацію. LLDP – стандартний протокол для виявлення пристроїв на рівні посилань (Data Link Layer). Він використовується для виявлення сусідніх пристроїв та їх характеристик. FDP та SONMP – це інші пропрієтарні протоколи виявлення пристроїв, які використовуються деякими виробниками мережевого обладнання.

Деякі функції ПЗ, такі як збір конфігурацій, можуть використовувати CLI та API пристроїв для отримання даних, які не доступні через вищеперелічені протоколи.

Застосунок працює у веб-інтерфейсі, використовуючи бекенд у вигляді фреймворку Dancer2 мови програмування Perl. Було обрано його тому, що він є легким та гнучким у використанні, використовує DSL (Domain-Specific Language) для спрощення синтаксису та розробки веб-застосунків, що робить код коротшим та зрозумілішим, а також спрощує взаємодію з базою даних PostgreSQL, виконання SQL-запитів та отримання даних для відображення.

Для фронтенд розробки обрано також Perl та JavaScript. Саме за допомогою JavaScript стало можливим динамічно оновлювати інформацію на веб-сторінках без необхідності перезавантаження сторінки, а також використано бібліотеки D3.js для створення графіків, діаграм та інтерактивної та інформативної візуалізації.

Як основне сховище даних для програмного забезпечення використовується відкрита система управління реляційними базами даних (СУБД) PostgreSQL. В базі даних зберігаються вся

інформація, яку ПЗ збирає з мережевих пристроїв, включаючи конфігурації, статуси портів, MAC-адреси, ARP-таблиці, серійні номера, час роботи та версія ОС.

Розроблене програмне забезпечення для аналізу та моніторингу мережі має наступний функціонал:

– Пошук пристрою в мережі за MAC-адресою або IP-адресою.
– Керування портами коммутатора або зміна стану VLAN чи PoE порту.
– Інвентаризація мережевих пристроїв за моделями, виробниками та програмним забезпеченням.
– Зберігання старих даних про IP-адреси та місцезнаходження системи.
– Пошук та отримання даних через API.
– Перегляд інтерактивної карти мережі.
– Підключення до пристроїв по SSH, Telnet та Web.

Структурна схема системи розроблена таким чином, щоб забезпечити високу продуктивність, надійність та безпеку при роботі в гетерогенних мережевих середовищах (рис. 1).

Рис. 1. Структурна схема програмної системи

Як було описано вище, розроблене програмний продукт дозволяє надавати повну інформацію про пристрої, які є в мережі. Це стосується як комутаторів, Wi-Fi-точок, серверів так і кінцевих клієнтів, зокрема, користувацькі ПК, одноплатних комп'ютерів, смартфонів тощо. Результат опитування включає в себе інформацію про загальний час роботи, MAC-адрес, ARP-таблицю та інші характеристики пристрою (рис. 2).

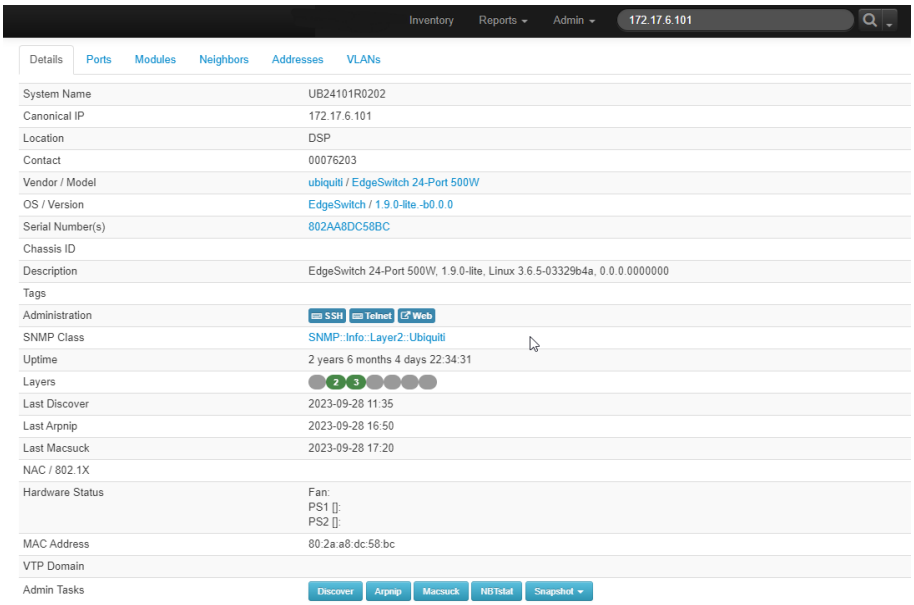

Рис. 2. Вікно інвентаризації комутатора Ubiquiti EdgeSwitch 24-Port

Таким чином, процес інвентаризації можна проводити як вручну так і налаштувавши цей процес автоматично. Також в ПЗ ведеться статистика опитування всього обладнання на увесь час, де можна побачити кількість пристроїв, вузлів, з'єднань та IP-адрес (рис. 3).

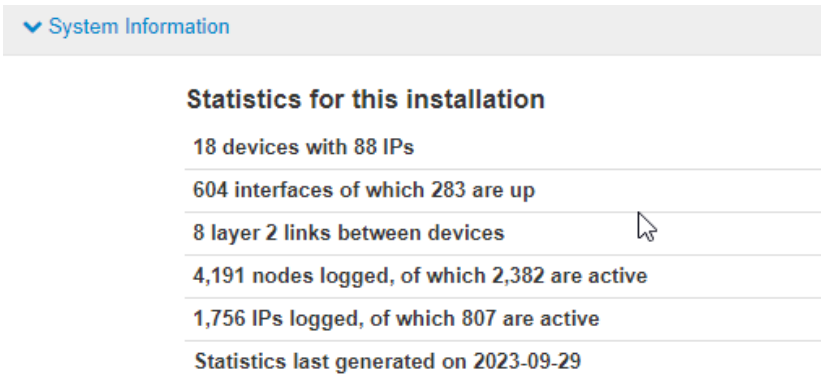

Рис. 3. Системна інформація ПЗ про статистику опитування мережі

Через аналіз трафіку можна зрозуміти, як дані передаються мережею, і виявити потенційні проблемні області, що вимагають уваги. Розуміння типів трафіку, які проходять через мережу, допомагає в управлінні пріоритетами та забезпечує, щоб критичні для бізнесу застосунки отримали необхідну пропускну здатність (рис. 4).

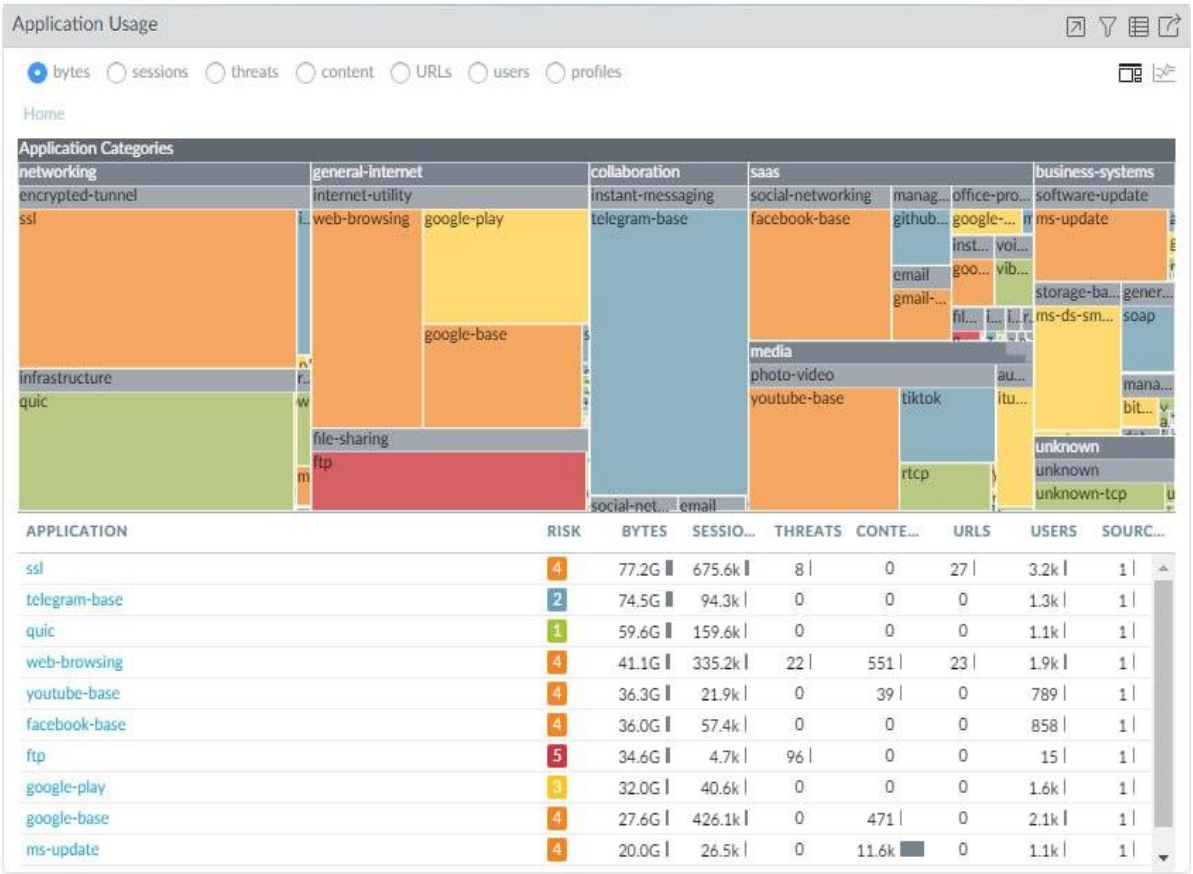

Рис. 4. Тип трафіку та обсяги використання у робочий час

Як вже зазначалось, ПЗ може будувати інтерактивну карту мережі з пристроїв, які раніше було додано до бази даних. На карті можна переглядати локацію вказаних пристроїв, переміщати їх так як зручно, переглядати коротку інформацію, видаляти та будувати інші зв'язки, а також переходити на сам пристрій, щоб можна було переглянути всю інформацію про нього та керувати ним, якщо раніше було надано такі дозволи та чи є потреба в цьому (рис. 5).

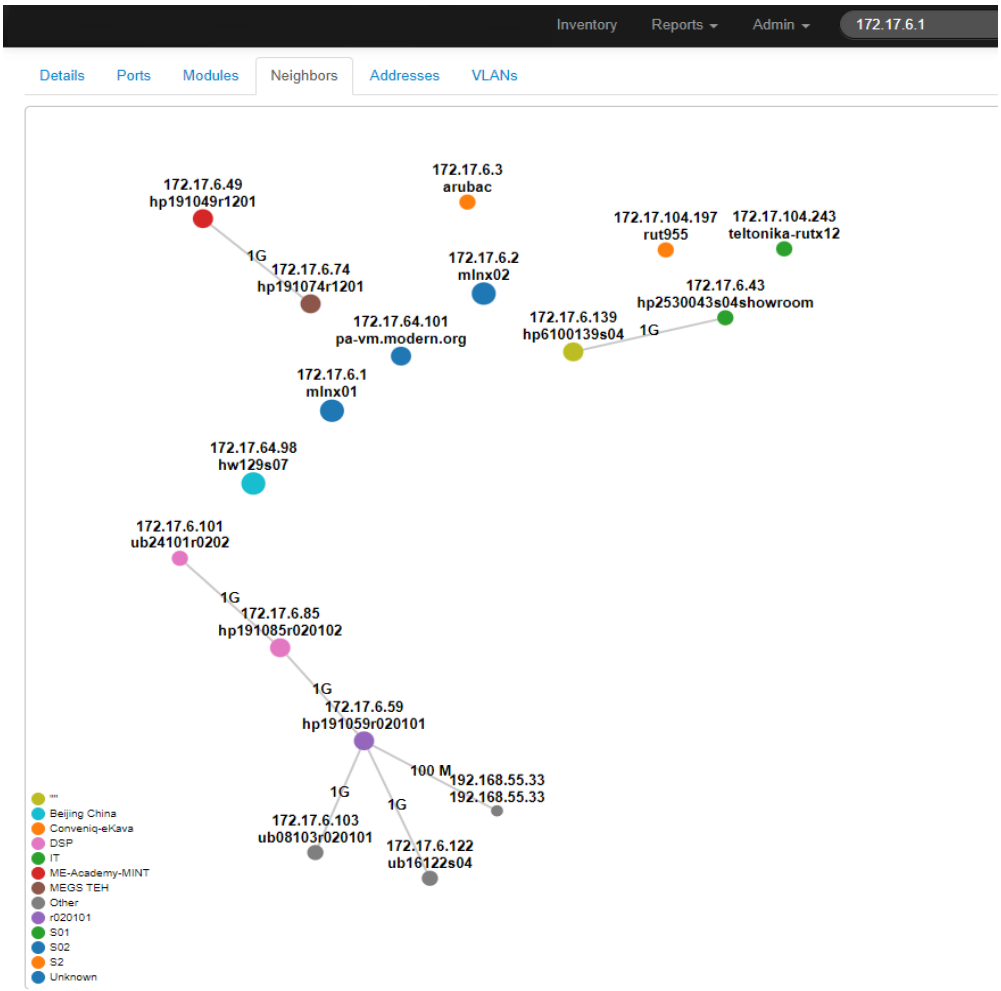

Рис. 5. Побудова інтерактивної карти відокремленої частини мережі

Висновки та перспективи подальшого дослідження. Розподілені гетерогенні мережі є досить динамічні та залишаються недостатньо дослідженими. Розроблене програмне забезпечення для аналізу стану, функціонування та моніторингу такого типу мереж є перспективним напрямком дослідження та прекрасним інструментом для мережевих та системних адміністраторів. За допомогою цього ПЗ можливо вирішувати базові та більш комплексні задачі, а також легко інтегрувати його в мережу підприємства, незалежно від її масштабності. В подальшому планується інтеграція з іншими сервісами та доповнення функціоналу ПЗ.

Список бібліографічного опису

1. Holubnychyi D., Kotsyuba V. Applying technologies of monitoring and condition analysis of IP-networks based on the use of the SNMP protocol. Bulletin of Kharkov National Automobile and Highway University. 2022. No. 96. P. 14. URL: http://surl.li/njysl
2. Kovalenko O. Y., Kuzniuk K. V. Computer network monitoring systems. Mathematical machines and systems. 2023. Vol. 1. P. 50–59. URL: https://doi.org/10.34121/1028-9763-2023-1-50-59 (date of access: 30.09.2023).
3. Калініченко Д. Система виявлення вторгнення в комп'ютерну мережу на основі аналізу трафік : автореф. Кваліфікаційна робота "Бакалавр". Київ, 2023. 76 с.
4. Heterogeneous networks: basics & examples. study.com. URL: http://surl.li/npfkn

References

1. Holubnychyi D., Kotsyuba V. Applying technologies of monitoring and condition analysis of IP-networks based on the use of the SNMP protocol. Bulletin of Kharkov National Automobile and Highway University. 2022. No. 96. P. 14. URL: http://surl.li/njysl
2. Kovalenko O. Y., Kuzniuk K. V. Computer network monitoring systems. Mathematical machines and systems. 2023. Vol. 1. P. 50–59. URL: https://doi.org/10.34121/1028-9763-2023-1-50-59
3. Kalinichenko D. System for detecting intrusion into a computer network based on traffic analysis: an abstract. Qualification work "Bachelor". Kyiv., 2023. P 76.
4. Heterogeneous networks: basics & examples. study.com. URL: http://surl.li/npfkn