УДК 004

С.Якименко, магістр гр. КІ-23М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КЕРУВАННЯ МЕРЕЖНОЮ ІНФРАСТРУКТУРОЮ НА ОСНОВІ CISCO APPLICATION CENTRIC INFRASTRUCTURE

У статті розроблено програмне забезпечення, яке призначено для системи керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure. Метою розробки є дослідження та програмна реалізація системи керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure. Об'єктом дослідження є процес керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure. Предметом дослідження є методи керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure. Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. У концепції Cisco Application Centric Infrastructure (ACI) пропонується принципово новий підхід до побудови мережної інфраструктури центрів обробки даних. Чим же ця архітектура відрізняється від інших, як традиційних, так і недавно з'явилися? І як інтегрувати в неї елементи інших виробників і рішення Open Source? Архітектура ACI складається із трьох основних компонентів: моделі політик, мережної фабрики й контролера APIC, за допомогою якого прийнята політика доводить до елементів фабрики й здійснюється контроль за її функціонуванням. Нижче ми розглянемо, які ключові особливості кожного із цих компонентів і як з них формується єдине рішення. Назва Application Centric Infrastructure можна перевести як «інфраструктура, орієнтована на додатки».

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure.

– Дослідження системи керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure.

– Програмна реалізація системи керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure.

Об'єктом дослідження є процес керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure.

Предметом дослідження є методи керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure.

Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Програмне забезпечення для керування мережею – це інструмент, який допомагає вам керувати та оптимізувати вашу мережеву інфраструктуру. Він забезпечує ефективну роботу всіх пристроїв, з'єднань та потоків даних у вашій мережі. Це програмне забезпечення дає вам можливість контролювати продуктивність мережі, виявляти проблеми та захищати ваші системи від потенційних загроз. Використовуючи його, ви можете підтримувати стабільне та безпечне мережеве середовище, що є важливим для сучасного бізнесу.

Ключові функції: моніторинг, управління та захист мереж

Програмне забезпечення для керування мережею виконує три критично важливі функції: моніторинг, керування та захист вашої мережі. Моніторинг дозволяє відстежувати мережеву активність у режимі реального часу, забезпечуючи стабільну продуктивність. Функції керування дозволяють налаштовувати пристрої, розподіляти ресурси та оптимізувати потік трафіку. Функції безпеки захищають вашу мережу від кіберзагроз, забезпечуючи цілісність та конфіденційність даних.

У 2025 році компанії стикаються зі все більш складними мережевими середовищами. Кіберзагрози стають більш складними, а трафік даних продовжує зростати. Програмне забезпечення для керування мережею допомагає вам залишатися на крок попереду, надаючи інструменти для управління цими викликами. Наприклад, BP впровадила розширену сегментацію мережі, щоб обмежити переміщення загроз, посиливши безпеку своєї інфраструктури. Аналогічно, Sony впровадила Центр операцій безпеки на базі штучного інтелекту, покращивши виявлення загроз і зменшивши витрати завдяки автоматизації. Ці приклади показують, як програмне забезпечення для керування мережею може захистити ваш бізнес, одночасно підвищуючи ефективність.

Критерії вибору найкращого програмного забезпечення для керування мережею

Особливості: Що відрізняє програмне забезпечення від інших?

Вибираючи програмне забезпечення для керування мережею, слід зосередитися на функціях, які відповідають потребам вашого бізнесу. Ефективне програмне забезпечення пропонує надійні можливості моніторингу, адаптовані до розміру вашої мережі. Наприклад, воно повинно безперешкодно контролювати сервери, комутатори та електронну пошту. Підтримка поширених протоколів, таких як WMI, NetFlow та SNMP, забезпечує сумісність з різноманітними IT-середовищами. Шукайте інструменти, які надають детальні показники продуктивності у вигляді графіків та звітів. Ці аналітичні дані допоможуть вам ефективно керувати мережею та планувати майбутнє зростання. Сигналізація та сповіщення також важливі. Вони попереджають вас про проблеми в режимі реального часу, дозволяючи вам швидко реагувати. Розширені функції, такі як автоматизовані відповіді та інтегровані функції кластера, підвищують безпеку та надійність.

Зручність використання та користувацький досвід

Зручний інтерфейс суттєво впливає на ефективність керування мережею. Інтуїтивно зрозумілий дизайн підходить як для початківців, так і для досвідчених користувачів. Налаштовувані панелі інструментів дозволяють зосередитися на показниках, які є найважливішими для вашого бізнесу. Статистика показує, що хороший користувацький досвід (UX) може збільшити коефіцієнт конверсії до 400%. Інвестування в програмне забезпечення з добре розробленим інтерфейсом може заощадити час і зменшити кількість помилок. Швидкі процеси адаптації, такі як навчальні відео та посібники, також допомагають вашій команді швидше адаптуватися. Чуйна підтримка клієнтів ще більше підвищує зручність використання, оперативно вирішуючи проблеми.

Масштабованість для бізнесу різного розміру

Масштабованість гарантує, що ваше програмне забезпечення для керування мережею зростатиме разом з вашим бізнесом. Ключові показники, такі як пропускна здатність, час відгуку та використання ресурсів, вказують на те, наскільки добре програмне забезпечення

справляється зі збільшеними робочими навантаженнями. Наприклад, висока пропускна здатність та низька затримка показують, що система ефективно працює за вимогами.

Малий бізнес отримує вигоду від легких рішень, які легко розгортати. Середнім та великим підприємствам потрібні розширені функції, такі як балансування навантаження та керування кількома сайтами. Масштабоване програмне забезпечення підтримує низький рівень помилок та високу ефективність, навіть по мірі розширення вашої мережі.

Ціноутворення та співвідношення ціни та якості

Під час оцінки програмного забезпечення для керування мережею ціноутворення відіграє вирішальну роль у визначенні його загальної цінності. Вам потрібне рішення, яке збалансовує вартість і функціональність, гарантуючи максимальну віддачу від ваших інвестицій. Деякі інструменти, такі як SigNoz, пропонують до 4,7 разів більшу цінність порівняно з конкурентами. Це робить їх сильним конкурентом для компаній, які шукають економічно ефективні варіанти.

Прозорі моделі ціноутворення також допомагають вам уникнути непередбачених витрат. Наприклад, New Relic стягує 0,35 долара за ГБ, що дозволяє вам контролювати весь ваш технологічний стек, не турбуючись про приховані платежі. Такий підхід гарантує, що ви можете зосередитися на оптимізації своєї мережі, а не на управлінні непередбачуваними витратами.

Вибір програмного забезпечення, яке відповідає вашому бюджету та пропонує надійні функції, гарантує довгострокову економію. Такі інструменти, як New Relic та SigNoz, демонструють, як конкурентне ціноутворення може підвищити цінність без шкоди для продуктивності.

Відгуки та коментарі клієнтів

Відгуки клієнтів надають цінну інформацію про реальну продуктивність програмного забезпечення для керування мережею. Огляди часто висвітлюють сильні та слабкі сторони, допомагаючи вам приймати обґрунтовані рішення. Багато користувачів хвалять SigNoz за його доступність та високу цінність, відзначаючи його здатність досягати виняткових результатів за значно меншу ціну, ніж у конкурентів. Так само New Relic отримує позитивні відгуки за прозоре ціноутворення та комплексні можливості моніторингу.

Також слід враховувати користувацький досвід, читаючи відгуки. Клієнти часто згадують, як інтуїтивно зрозумілі інтерфейси та чуйні команди підтримки покращують їхню загальну задоволеність. Наприклад, компанії цінують програмне забезпечення з налаштовуваними панелями інструментів та швидким вирішенням проблем. Ці функції спрощують керування мережею та зменшують час простою.

Аналізуючи відгуки клієнтів, ви можете визначити програмне забезпечення, яке відповідає вашим конкретним потребам. Шукайте постійні похвали в таких сферах, як зручність використання, масштабованість та економічна ефективність. Такий підхід гарантує, що ви оберете інструмент, який відповідає вашим цілям та забезпечує вимірювані результати.

Найкраще програмне забезпечення для керування мережею у 2025 році

FortiManager від Fortinet

FortiManager від Fortinet виділяється як надійне рішення для керування складними мережами. Він пропонує централізоване керування, що дозволяє налаштовувати та контролювати кілька пристроїв з одного інтерфейсу. Ця функція особливо корисна для підприємств з розподіленими мережами. FortiManager також бездоганно інтегрується з Fortinet Security Fabric, забезпечуючи покращену видимість та безпеку всієї вашої інфраструктури.

Одна з його ключових переваг полягає в можливостях автоматизації. Ви можете автоматизувати повторювані завдання, такі як оновлення політик та налаштування пристроїв, заощаджуючи час і зменшуючи кількість помилок. FortiManager також підтримує розширену аналітику, допомагаючи виявляти потенційні проблеми до їх загострення. З рейтингом

задоволеності користувачів 4,2, він залишається популярним вибором серед компаній, які шукають надійне програмне забезпечення для керування мережею.

Порада: масштабованість FortiManager робить його придатним як для малого бізнесу, так і для великих підприємств. Почніть з базової конфігурації та розширюйте її в міру зростання вашої мережі.

Портал управління безпекою Quantum Spark від Check Point Software Technologies

Портал керування безпекою Quantum Spark розроблений для малого та середнього бізнесу. Він спрощує керування мережею, пропонуючи інтуїтивно зрозумілий інтерфейс та попередньо налаштовані політики безпеки. Ви можете без зусиль керувати кількома сайтами, забезпечуючи стабільну продуктивність та безпеку в усіх місцях розташування.

Ця платформа відмінно підходить для кібербезпеки. Вона включає такі функції, як запобігання загрозам, керування VPN та моніторинг у режимі реального часу. Ці інструменти допомагають захистити вашу мережу від загроз, що постійно змінюються. Quantum Spark високо цінується за простоту використання та надійні функції безпеки з рейтингом задоволеності користувачів 4,6.

OpManager Plus від ManageEngine

OpManager Plus від ManageEngine – це комплексний інструмент, який поєднує функції моніторингу мережі, керування конфігурацією та безпеки. Він надає аналітику продуктивності вашої мережі в режимі реального часу, допомагаючи вам швидко виявляти та вирішувати проблеми. Платформа підтримує широкий спектр пристроїв, що робить її універсальним вибором для бізнесу будь-якого розміру.

Однією з його видатних особливостей є налаштовувані інформаційні панелі. Ви можете налаштувати інтерфейс для відображення показників, які є найважливішими для вашого бізнесу. OpManager Plus також пропонує детальні звіти, що дозволяють відстежувати тенденції продуктивності та планувати майбутнє зростання. З рейтингом задоволеності користувачів 4,4, його хвалять за його надійність та багатофункціональний дизайн.

Аувік

Auvik – це хмарний інструмент керування мережею, розроблений для спрощення моніторингу мережі та усунення несправностей. Він забезпечує видимість вашої мережевої інфраструктури в режимі реального часу, допомагаючи вам швидко виявляти та вирішувати проблеми. За допомогою Auvik ви можете автоматизувати багато рутинних завдань, таких як виявлення пристроїв та резервне копіювання конфігурації, заощаджуючи ваш дорогоцінний час.

Основні характеристики Аувіка:

– Автоматизоване картографування мережі: Auvik автоматично створює детальні карти мережі. Ці карти оновлюються в режимі реального часу, надаючи вам точне уявлення про структуру вашої мережі.

– Аналіз трафіку: Ви можете відстежувати моделі трафіку та виявляти перевантаження пропускної здатності. Ця функція допомагає оптимізувати продуктивність вашої мережі.

– Система оповіщення: Auvik надсилає миттєві сповіщення, коли виявляє незвичайну активність. Це дозволяє вам вирішувати потенційні проблеми до їх загострення.

– Керування кількома об'єктами: Якщо ви керуєте кількома об'єктами, Auvik дозволяє вам контролювати всі об'єкти з однієї панелі керування.

Порада: Використовуйте автоматизовані функції Auvik, щоб зменшити ручну роботу та зосередитися на стратегічних завданнях.

Зручний інтерфейс Auvik спрощує навігацію та налаштування. Платформа підтримує широкий спектр пристроїв, що забезпечує сумісність з більшістю мережевих налаштувань. Її масштабованість також робить її придатною для бізнесу будь-якого розміру. Незалежно від того, чи керуєте ви невеликим офісом, чи великим підприємством, Auvik адаптується до ваших потреб.

Монітор продуктивності мережі SolarWinds

Монітор продуктивності мережі SolarWinds (NPM) – це потужний інструмент для моніторингу та управління продуктивністю вашої мережі. Він надає глибоке уявлення про стан вашої мережі, допомагаючи підтримувати оптимальну функціональність. NPM відомий своїми потужними функціями та надійністю, що робить його популярним вибором серед IT-фахівців.

Ключові характеристики SolarWinds NPM:

– Комплексний моніторинг: NPM відстежує продуктивність усієї вашої мережі, включаючи пристрої, сервери та програми.

– Налаштовувані сповіщення: Ви можете налаштувати сповіщення на основі певних порогових значень. Це гарантує, що ви отримуватимете сповіщення лише про критичні проблеми.

– Технологія NetPath™: Ця функція візуалізує шлях даних у вашій мережі. Вона допомагає вам виявляти вузькі місця та швидше усувати несправності.

– Моніторинг бездротової мережі: Якщо ви користуєтеся бездротовими мережами, NPM надає детальну інформацію про силу сигналу та покриття.

SolarWinds NPM також відрізняється масштабованістю. Він може обробляти мережі будь-якого розміру, від малого бізнесу до великих підприємств. Платформа легко інтегрується з іншими інструментами SolarWinds, що дозволяє розширювати її можливості в міру зростання ваших потреб.

Як Auvik, так і SolarWinds NPM пропонують унікальні переваги. Auvik зосереджується на автоматизації та простоті використання, тоді як SolarWinds NPM надає розширені функції для поглибленого аналізу. Ваш вибір залежатиме від ваших конкретних вимог та складності вашої мережі.

Як вибрати правильне програмне забезпечення для керування мережею

Оцінка потреб та цілей бізнесу

Вибір правильного програмного забезпечення для керування мережею починається з розуміння потреб вашого бізнесу. Почніть з визначення розміру та складності вашої мережі. Малому бізнесу часто потрібні легкі інструменти, тоді як більші підприємства отримують переваги від розширених функцій, таких як керування кількома сайтами та балансування навантаження. Враховуйте тип пристроїв та платформ, які підтримує ваша мережа. Сумісність з існуючою інфраструктурою забезпечує безперебійну інтеграцію.

Подумайте про свої цілі. Ви прагнете покращити мережеву безпеку, оптимізувати продуктивність або зменшити час простою? Надайте пріоритет програмному забезпеченню, яке відповідає цим цілям. Наприклад, якщо ви зосереджені на кібербезпеці, інструменти з надійними можливостями виявлення та запобігання загрозам будуть необхідними. Якщо масштабованість важлива, оберіть програмне забезпечення, яке розвивається разом з вашим бізнесом.

Бюджетні міркування

Бюджет відіграє вирішальну роль у процесі прийняття рішень. Почніть з аналізу своїх фінансових ресурсів та встановлення чітких лімітів. Програмне забезпечення для бюджетування може допомогти ефективно розподілити кошти, гарантуючи, що відділи залишатимуться в межах своїх можливостей. Планування сценаріїв дозволяє передбачити результати та виявити ризики, тоді як аналіз ефективності виявляє розбіжності між фактичними результатами та цілями.

Оцінюючи ціноутворення, шукайте прозорі моделі. Ціноутворення на основі використання, фіксовані тарифи або плата за кожного користувача є поширеними варіантами. Такі інструменти, як New Relic, пропонують передбачувані витрати, такі як 0,35 долара за ГБ, що спрощує планування витрат. Інтегроване програмне забезпечення для бізнес-планування узгоджує фінансову діяльність із довгостроковими цілями, гарантуючи, що ваші інвестиції підтримують вашу загальну стратегію.

– Планування сценаріїв: допомагає проаналізувати численні результати та ризики.

– Аналіз ефективності: Виявляє розбіжності для вжиття коригувальних заходів.
– Програмне забезпечення для прогнозування: прогнозує майбутню ефективність на основі історичних даних.

Примітка: Програмне забезпечення для бюджетування гарантує, що відділи працюють у межах виділених їм коштів, безпосередньо впливаючи на стратегії ціноутворення на програмне забезпечення для керування мережею.

Технічні вимоги та сумісність

Технічна сумісність гарантує безперешкодну інтеграцію вашого програмного забезпечення з вашими існуючими системами. Почніть із документування базових вимог для підтримуваних платформ. Зосередьтеся на критично важливих функціях, таких як моніторинг пристроїв та підтримка протоколів. Тестування на основі ризиків допомагає перевірити сумісність із високоризиковими комбінаціями платформ та шляхами користувачів.

Інтеграція безперервного тестування запобігає проблемам під час розробки. Автоматизовані перевірки сумісності гарантують, що програмне забезпечення працює за різних мережевих умов, включаючи обмеження пропускної здатності. Тестування на зворотну сумісність гарантує, що нове програмне забезпечення підтримує старіші версії, а пряма сумісність готує до майбутніх оновлень.

Важливість пробних/демо-версій

Пробні або демо-версії відіграють вирішальну роль під час вибору програмного забезпечення для керування мережею. Вони дозволяють вам ознайомитися з функціями програмного забезпечення та оцінити його сумісність з вашою мережею. Тестуючи програмне забезпечення безпосередньо, ви можете визначити, чи відповідає воно потребам вашого бізнесу, перш ніж здійснювати покупку.

Однією з головних переваг пробних версій є їхня здатність знижувати ризики. Ви можете виявити потенційні проблеми, такі як проблеми сумісності або відсутні функції, на ранніх етапах процесу прийняття рішень. Це гарантує, що ваші інвестиції відповідають вашим цілям, і дозволяє уникнути дорогих помилок. Пробні версії також допомагають оцінити зручність використання. Практичний досвід показує, наскільки інтуїтивно зрозумілий інтерфейс і чи відповідає він рівню кваліфікації вашої команди.

Коефіцієнти конверсії підкреслюють ефективність пропонування пробних версій. Наприклад, коефіцієнти конверсії відвідувачів у пробні версії сягають 2,5% для органічного трафіку та 2,2% для платного трафіку. Коефіцієнти конверсії з пробних версій у платні ще більш вражаючі: 48,8% для органічних користувачів та 51% для платних користувачів. Ці цифри показують, що пробні версії суттєво впливають на рішення про покупку.

Щоб максимально використати переваги пробних версій, розгляньте такі стратегії:
– Аналізуйте показники конверсії за різними сегментами клієнтів.
– Визначте фактори, що сприяють успішним конверсіям.
– Розгляньте поширені заперечення протягом випробувального періоду.

Пропонуючи пробні версії, постачальники програмного забезпечення формують довіру та демонструють цінність. Для вас це означає робити усвідомлений вибір з упевненістю. Пробні версії дають вам змогу вибрати програмне забезпечення, яке покращує продуктивність вашої мережі та відповідає вашим бізнес-цілям.

Тенденції ринку програмного забезпечення для мережевого керування у 2025 році

Інтеграція та автоматизація штучного інтелекту

Штучний інтелект (ШІ) та автоматизація трансформують способи керування мережами. Інструменти на базі ШІ аналізують величезні обсяги даних у режимі реального часу, виявляючи закономірності та прогнозуючи потенційні проблеми до їх виникнення. Такий проактивний підхід зменшує час простою та підвищує ефективність мережі. Автоматизація спрощує повторювані завдання, такі як налаштування пристроїв та оновлення політик, заощаджуючи ваш час та мінімізуючи помилки. Наприклад, рішення на базі ШІ

можуть автоматично регулювати розподіл пропускної здатності під час пікового навантаження, забезпечуючи оптимальну продуктивність.

Очікується, що ринок програмного забезпечення для керування мережами на основі штучного інтелекту значно зросте у 2025 році. Компанії впроваджують ці інструменти для роботи зі зростаючою складністю сучасних мереж. Використовуючи штучний інтелект, ви можете підвищити надійність і безпеку своєї мережі, одночасно зменшуючи експлуатаційні витрати.

Впровадження SASE (Secure Access Service Edge)

Безпечний доступ до послуг на межі (SASE) стає наріжним каменем сучасного управління мережею. SASE поєднує мережеві та безпекові функції в єдине хмарне рішення, забезпечуючи вам безперебійний та безпечний доступ до ресурсів. Такий підхід особливо цінний, оскільки віддалена робота та хмарні сервіси продовжують розширюватися.

Прогнозується, що ринок SASE зросте з 2,86 млрд доларів США у 2024 році до 17,18 млрд доларів США до 2033 року, зі сукупним річним темпом зростання (CAGR) 25,1%. Це швидке зростання свідчить про зростаючий попит на інтегровані рішення безпеки. Впроваджуючи SASE, ви можете захистити свою мережу від загроз, що постійно змінюються, зберігаючи при цьому високу продуктивність.

Розвиток технології SD-WAN (програмно-визначена глобальна мережа)

Технологія SD-WAN змінює способи підключення та управління розподіленими мережами. Вона дозволяє оптимізувати потік трафіку, покращити продуктивність програм і підвищити безпеку. Очікується, що ринок SD-WAN зросте з 5,19 млрд доларів США у 2023 році до 59,41 млрд доларів США до 2032 року зі середньорічним темпом зростання (CAGR) 31,14%.

Це зростання зумовлене зростаючою залежністю від хмарних сервісів, віддаленою роботою та потребою в гнучких мережах. SD-WAN дозволяє швидко адаптуватися до змінних потреб бізнесу, одночасно знижуючи витрати. Його здатність інтегруватися з іншим програмним забезпеченням для керування мережею робить його цінним доповненням до вашого IT-інструментарію.

Зосередьтеся на кібербезпеці та виявленні загроз

Кібербезпека стала критично важливим компонентом програмного забезпечення для керування мережею у 2025 році. Оскільки кіберзагрози стають дедалі складнішими, вам потрібні інструменти, які можуть захистити вашу мережу, забезпечуючи безперебійну роботу. Сучасне програмне забезпечення інтегрує розширені функції для ефективного виявлення, запобігання та реагування на потенційні порушення.

Однією з найважливіших можливостей є розширене виявлення загроз. Використовуючи штучний інтелект та поведінковий аналіз, програмне забезпечення для керування мережею виявляє аномалії до їх ескалації. Такий проактивний підхід допомагає запобігти атакам нульового дня, які є одними з найнебезпечніших загроз для вашої мережі. Автоматизоване стримування загроз ще більше підвищує безпеку, ізолюючи ризики одразу після їх виявлення. Функції швидкого відновлення забезпечують швидке повернення вашої мережі до нормального стану після інциденту.

Також важливим є надійний захист від шкідливого програмного забезпечення та несанкціонованого доступу. Комплексний захист від загроз пропонує виявлення в режимі реального часу, захищаючи ваші конфіденційні дані. Шифрування та надійні брандмауери захищають інформацію та підтримують цілісність даних. Ці функції особливо важливі для компаній, які обробляють конфіденційні дані клієнтів або фінансові дані.

Ось як ці функції корисні для вашої мережі:

– Покращене виявлення та реагування на загрози: швидко виявляє порушення, щоб мінімізувати збитки.

– Надійне шифрування та брандмауери: захищає конфіденційні дані від несанкціонованого доступу.

– Реагування на інциденти та відновлення: Автоматизує стримування та пришвидшує відновлення після атак.

Інвестуючи в програмне забезпечення для керування мережею з цими можливостями, ви можете бути на крок попереду загроз, що розвиваються. Правильні інструменти не лише захищають вашу мережу, але й забезпечують вам душевний спокій. Безпечна мережа гарантує безперебійну роботу вашого бізнесу, навіть за умови зростання кіберризиків.

Порада: Регулярно оновлюйте своє програмне забезпечення, щоб забезпечити його ефективність проти найновіших загроз. Кібербезпека – це безперервний процес, а не одноразове рішення.

Вибір правильного програмного забезпечення для керування мережею може змінити спосіб керування вашою мережею. Такі інструменти, як FortiManager, Quantum Spark, OpManager Plus, Auvik та SolarWinds NPM, пропонують унікальні функції для задоволення різних потреб бізнесу. Незалежно від того, чи надаєте ви пріоритет автоматизації, масштабованості чи безпеці, ці рішення надають інструменти для оптимізації вашої мережі.

Зосередьтеся на своїх цілях і тестуйте програмне забезпечення за допомогою пробних версій, щоб забезпечити сумісність. Інвестування в правильне рішення підвищує продуктивність і захищає вашу інфраструктуру. Ознайомтеся з варіантами, завантажте детальні звіти або розпочніть безкоштовну пробну версію вже сьогодні, щоб знайти найкраще рішення для вашого бізнесу.

Контролер APIC

Централізоване керування інфраструктурою ACI здійснює контролер Application Policy Infrastructure Controller (APIC). У дійсності він являє собою кластер контролерів, оскільки для цілей масштабування й забезпечення безперервності роботи APIC підтримує кластеризацію. Незважаючи на певну аналогію з контролером програмно обумовлених мереж (SDN), APIC реалізує зовсім іншу модель керування.

У традиційній моделі SDN на центральному контролері, що реалізує функції рівня керуючої логіки (control plane) для всієї мережі, консолідується вся інформація про стан всіх мережних елементів, а його завданням є повне детальне налаштування всіх таблиць комутації на всіх мережних пристроях. Таким чином, можна говорити про те, що контролер SDN реалізує імперативну модель керування, у якій центральне керування всіма елементами інфраструктури виконується шляхом точної й повної вказівки необхідних деталей налаштування. Такий підхід являє собою аналог «мікроменеджменту» як стилю організаційного керування й приводить до появи пов'язаних із цим проблем масштабованості й украй високих вимог до надійності контролера.

В архітектурі ACI функції адміністрування (management plane), тобто налаштування описаної вище мережної політики додатків, а також функцій моніторингу й діагностики, виконуються централізовано. При взаємодії з елементами мережі роль APIC полягає в тому, щоб довести до них правила, а не деталі налаштування. У цьому змісті можна говорити про те, що ACI використовує декларативну модель керування, коли мережі і її компонентів повідомляється, яке їхній стан є бажаним, а вони самостійно, без залучення ресурсів контролера, досягають його й підтримують у випадку яких-небудь змін у серверах і з'єднаннях, при міграції віртуальних машин і т.д.

Поза тим що APIC реалізує централізоване керування через графічний інтерфейс адміністратора, він також забезпечує доступ через програмний інтерфейс (API) для вищестоящих систем керування, хмарної оркестрації, моніторингу й т.д. Останній, тобто «північний» інтерфейс між вищестоящими системами й контролером, повністю відкритий для використання сторонніми розроблювачами й замовниками, але цим «відкритість» ACI не обмежується.

У галузі існує насущна потреба у використанні загальної мови декларативного опису політик інфраструктури. Разом з іншими компаніями Cisco опублікувала в IETF протокол OpFlex, де описується «південний» інтерфейс між контролером як крапкою опису правил і елементами, що реалізують ці правила, інфраструктури. Крім того, Cisco планує

опублікувати референсну реалізацію з відкритим вихідним кодом агента OpFlex для віртуального комутатора, що дозволить полегшити й прискорити впровадження даного підходу в складі систем сторонніх розроблювачів.

У майбутньому реалізація OpFlex на стороні контролера планується не тільки в складі ACI, тобто під управлінням контролера APIC, але й у рамках підтримку проекту має, що широку галузеву, контролера з відкритим вихідним кодом OpenDaylight, активним учасником якого є компанія Cisco. Таким чином, у перспективі можна буде говорити про можливість використання OpFlex як єдиного інструмента для поширення політики в інформаційних інфраструктурах.

Крім доведення політики до елементів фабрики, контролер APIC реалізує й потужні можливості по одержанню з фабрики діагностичної й телеметричної інформації. Причому й у цьому випадку використовується підхід, орієнтований на додатки, – адміністратор може побачити детальну інформацію не тільки про затримки, втрати й т.д. по кожному мережному елементі, але й про «стан здоров'я» інфраструктури з погляду конкретного додатка, що дозволяє спростити діагностику й усунення проблем, а також планування й оптимізацію продуктивності.

На закінчення відзначимо, що окремі елементи архітектури ACI доступні вже зараз, а вихід повного рішення очікується в середині 2017 року. У своєму нинішньому виді це рішення призначене для мережі ЦОД, але очевидна й потреба в розширенні моделі керування ACI як за межі ЦОД (у магістральну й кампусну мережа), так і в інші технологічні домени (обчислення й зберігання). Будемо сподіватися, що ця концепція буде розвиватися й далі.

Мікросегментація

Прикладом чутливості Cisco до вимог своїх клієнтів може служити розширення підтримки мікросегментації на віртуальні комутатори VMware (vDS або vSphere Distributed Switch) і Microsoft Hyper-V, а також на додатки, що працюють на встаткуванні bare-metal.

Мікросегментація дозволяє встановлювати гранулярні політики мережної безпеки на рівні L2 шляхом програмного «дроблення» мережі на велику кількість сегментів. Це дає можливість обмежити горизонтальне поширення погроз (шляхом реалізації так званих east-west Firewal) і поміщати в карантин скомпрометовані кінцеві крапки. Завдяки цьому досягається ізоляція зловмисника, що скомпрометировали один вузол, від інших вузлів у тім же VLAN. В ACI призначення політик можливо по декількох атрибутах віртуальної машини – ім'я, гостьова ОС, ідентифікатор VM, FQDN, IP-адреса й др.

До сьогоднішнього дня Cisco пропонувала мікросегментацію тільки на базі Cisco AVS (Application Virtual Switch). Тепер функціонал розширений і на інші віртуальні й фізичні пристрої. Мікросегментація для Hyper-V доступна вже зараз, у той час як інші розширення з'являться в першому кварталі 2016 року.

Docker-контейнери

Cisco підтримує як віртуальні, так і апаратні прикінцеві крапки (Endpoints). У новому релізі з'явиться підтримка прикінцевих крапок, що працюють у контейнерах Docker. Функціонал реалізується за допомогою інтеграції контролера Cisco APIC (Application Policy Infrastructure Controller), що є компонентом ACI, і Project Contiv – open source проекту, запущеного Cisco зовсім недавно. Метою Contiv є опис політик впровадження контейнерних додатків. Ці політики охоплюють область безпеки, інфраструктурні вимоги (дискова підсистема, виділення IP-адрес, ліміт смуги пропущення, вимоги до продуктивності, SLA), аналітикові й ін. Завдяки Project Contiv, тепер вони можуть бути поширені на додатки, що працюють в Linux-контейнерах.

Contiv включає мережний плагін до Docker, що дозволяє робити конфігурацію й підключення контейнера до фабрики ACI. Також реалізований рівень прямої взаємодії з API контролера APIC.

Зараз ми сфальцьовані на контейнерах Docker, але уважно придивляємося й до іншим рішенням, що з'являються на ринку, включаючи Kubernetes і Mesos

ACI і OpenStack

Аналітики прогнозують, що «підтримка OpenStack в ACI повинна більш ніж просто задовольнити користувачів. Цей факт може взагалі усунути причини, по яких компанії розглядають продукти конкурентів».

Функціонал реалізується за допомогою OpFlex-агента, що підключається до Open vSwitch, того самим розширюючи дію політик ACI до рівня гіпервізора. OpFlex – розроблена Cisco альтернатива протоколу OpenFlow, що у цьому випадку забезпечує інтеграцію OpenStack і APIC-контролера. У результаті, користувачі OpenStack і ACI одержують повністю розподілений мережний стек Neutron, включаючи distributed-комутатори (аналог VMware vDS), маршрутизацію й NAT. Відновлення стане доступно в 4-м кварталі 2017 року. В останньому релізі ACI також використовує OpFlex для підтримки VMware vRealize, що використовується для керування віртуалізованою інфраструктурою, побудованої на базі VMware.

Інші відновлення

Крім вищеописаного, у новий реліз увійшли наступні поліпшення (не повний список):

– Додаток в ACI Toolkit для автоматизації керування політиками в рамках декількох дата-центрів. ПЗ дозволяє синхронізувати політики між ЦОД для підвищення відкозостійкості й мобільності додатків;

– Підтримка SNMP і нового CLI для APIC, схожого з командним рядком NX-OS (підтримка запланована на 4-й квартал 2017 року).

Cisco позиціонує ACI як рішення для корпоративних клієнтів будь-якого масштабу, які шукають готове рішення від одного вендора. Компанія усвідомлює, що ACI – не для всіх, але робить ставку на те, що існуюча клієнтська база Cisco знайде її продукт більше прийнятного й зрілим, чим альтернативні SDN-рішення.

Розробка структурної схеми

Сучасні підходи до організації мережної інфраструктури центрів обробки даних у компанії Cisco одержали назву «інфраструктура, сфальцьована на додатках» (Application-Centric Infrastructure, ACI). У її основі – ACI-фабрика й керуючий контролер (Application Policy Infrastructure Controller, APIC). Концепція анонсована наприкінці минулого року й тепер стає комерційно доступною.

Ідея ACI дуже проста. Ми ставимо ідеологію інфраструктури ЦОД з голови на ноги: первинними елементами, на основі яких формуються правила безпеки, обробки трафіку й т.д., є додатки. Все інше – спосіб реалізації цих правил. Даний підхід істотно відрізняється від традиційної мережної інфраструктури, де оперують такими поняттями як VLAN, підмережі й т.д., а потреби додатків намагаються привести до цих термінів за допомогою абстрагування ресурсів».

В ACI базове поняття – мережний профіль додатка (див. Рисунок 1). У найпростішому випадку він описує правила взаємодії складовий додаток компонентів – його мережні й сервісні потреби. Міжмережні екрани, балансувальники навантаження й т.д. стають частиною опису інфраструктури додатка. Це опис повністю абстрагований від мережної й обчислювальної інфраструктури. Для нього не принципові кількість компонентів додатка і їхня природа (віртуальні вони або фізичні), IP-адресація, число серверів і т.д.

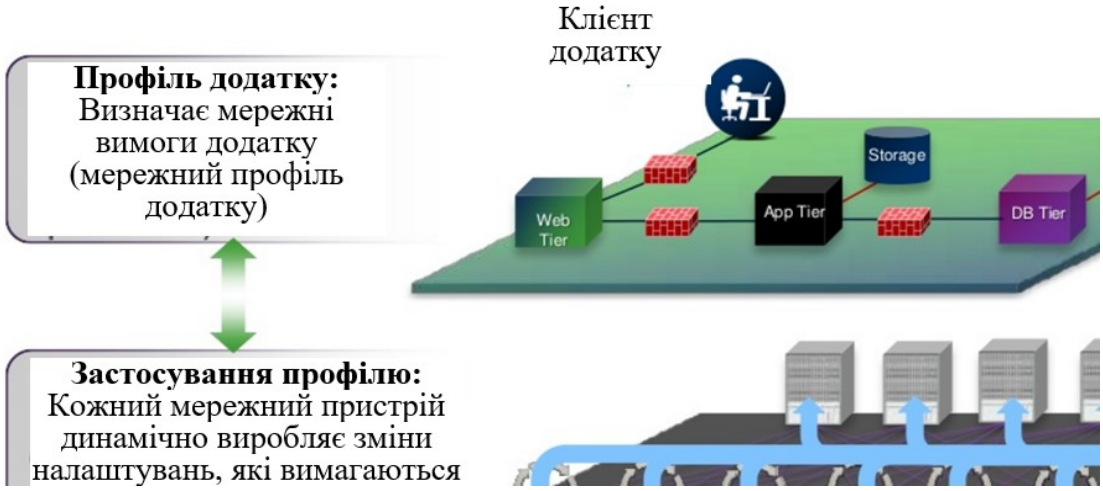

Рисунок 1 – Структурна схема системи

За допомогою профілів додатків можна управляти всією передачею даних у фабриці. Безпека й передача даних не залежать від фізичних і логічних мережних атрибутів. Адміністратор, відповідальний за додатки, формулює профіль додатка й передає такий опис контролеру APIC, керуючому всією інфраструктурою. Воно доводить до всіх елементів мережі й фабрики. Всі подальші дії й зміни, такі як міграція віртуальних машин (ВМ) спрацьовуються фабрикою автономно й не вимагають додаткових керуючих впливів контролера, на відміну від SDN, де контролер повністю управляє комутаторами.

В Cisco уважають, що таке декларативне керування значно поліпшує масштабованість ACI. Задається лише логіка керування, але не його деталі. Можна додавати й нові мережні елементи, деталі логіки керування якими контролер знати не зобов'язаний. У той же час моделі на базі протоколу OpenFlow всі можливості мережі визначаються й контролером, і комутуючими пристроями. Технічно ніщо не заважає сполучити ACI і SDN, вони не виключають один одного. Але, на відміну від SDN з високою деталізацією централізованого керування в ACI застосовується декларативний підхід.

Мережні елементи самі підбудовуються під політики. В ACI кожний мережний пристрій динамічно застосовує налаштування відповідно до вимог профілю. По суті, APIC відіграє роль репозиторію політик, зберігає й поширює їх. Це єдина крапка керування для адміністратора, систем оркестрації й автоматизації, включаючи OpenStack, Cisco UCS Director і ін. Контролер вирішує також сервісні завдання, пов'язані з виявленням фабрики, відновленням ПЗ й т.д.

Висока масштабованість досягається також за рахунок того, що контролер не бере участь у долі кожного мережного пакета й перебуває за рамками передачі даних і змін, що відбуваються в мережі. Його завдання – поширювати й обновляти політики, збирати телеметричну інформацію, але він не програмує безпосередньо деталі комутації на кожному пристрої. У результаті кластер APIC здатний підтримувати більше мільйона кінцевих хостів, понад 200 тис. порти, 64 тис. логічних організацій (tenant).

Адміністратор може формулювати потреби додатка в термінах самого додатка. Описуються рівні додатків, їхня взаємодія без таких деталей як IP-адреси, VLAN та ін. Один раз сформулювавши політику, її можна використовувати надалі без зміни, наприклад, переносити між ЦОД, фізичними й віртуальними серверами. Цей підхід працює й для повністю віртуалізованих, гібридних або не віртуалізованих середовищ.

Адміністратори додатків одержують детальну інформацію про те, що відбувається в мережі з його додатком – саме ту, котра відноситься до обслуговуючий додаток комутаторам у цей момент часу. Адміністратори безпеки мають своє бачення того, що відбувається в інфраструктурі ЦОД. Моніторинг подає інформацію про стан додатка й мережному трафіку всіх його компонентів. Для них ACI – це можливість керування правилами взаємодії

компонентів інфраструктури на зрозумілому їм рівні. ACI підтримує улюблену ними модель «білого писку»: усе, що не дозволено, заборонено за замовчуванням. Крім того, можна вбудовувати додаткові засоби безпеки (Cisco або інших вендорів), віртуальні або фізичних, передбачені засоби аудита, протоколювання дій, API для зовнішнього аналізу».

Мережним адміністраторам ACI дає можливість піти від колишньої обробки сервісних заявок і налаштувань, експлуатувати мережну інфраструктуру не як не набір пристроїв, а як комплекс із детальною телеметрією й діагностикою, ефективними механізмами перерозподілу трафіку між альтернативними маршрутами, підкреслюють в Cisco. Маршрутизація виконується в розподіленому режимі безпосередньо на границі мережі. При цьому можна розгортати середовища з довільним співвідношенням не віртуалізованих і віртуалізованих навантажень на різних платформах, впроваджувати гібридні й хмарні сервіси. Крім того, є можливість інтеграції з різними засобами оркестрації й автоматизації, включаючи OpenStack, чому Cisco приділяє особливу увагу. Опублікована модель даних і протокол OpFlex дозволяє додавати в ACI нові елементи, чому сприяє й відкритий механізм вбудовування сервісів L 4-L7.

Що стосується централізованого керування по політиках конвергентною інфраструктурою «у цілому», включаючи ПЗ віртуалізації, те дане завдання виконує Cisco UCS Director. Це один зі стратегічних продуктів Cisco, що заміняє кілька систем керування.

Як це працює? Адміністратори серверів, СЗД, мережі задають політики. Політики застосовуються для створення профілів серверів і конфігурацій LAN, SAN, СХД. Це дозволяє легко й швидко виконувати операції, що займають у реальній інфраструктурі досить багато часу. Процес максимально автоматизований.

З погляду архітектури USC Director – це одна або трохи ВМ, легко інтегрувальні з існуючим фізичним і віртуальним середовищем: в USC Director просто вписується логін/пароль для спілкування з тим або іншим пристроєм. Система може містити в собі засобу розгортання ОС і гіпервізорів, підтримує інтеграцію із зовнішніми хмарами різних вендорів і різні сценарії використання.

Адміністратор може автоматизувати різні операції й застосовувати налаштування для надання сервісів користувачам. Платформа керування UCS Director відкрита нагору й долілиць: її можна інтегрувати з різним устаткуванням через спеціальні коннектори й SDK або викликати із зовнішніх систем. Ще одна можливість – інтеграція з біллінговими системами для обліку споживаних ресурсів і виставляння рахунків.

Одна система UCS Director може управляти декількома «інтегрованими стеками», наприклад, vBlock і FlexPod, але крім конвергентних рішень Cisco підтримує серверні, мережні платформи й СЗД інших вендорів. У результаті можна вирішувати різні завдання по конфігуруванню інфраструктури, включаючи створення політик, профілів, пулів, шаблонів для Cisco UCS, створення томів і LUN, реєстрація ініціаторів та інші функції для дискових масивів EMC і NetApp, створення VLAN, налаштування конфігурації транкінгу й ін. у мережному встаткуванні, керування кластерами, віртуальними машинами й ін. у середовищах віртуалізації (VMware, Microsoft, RedHat).

Значна увага розроблювачі приділили автоматизації. Автоматизація дозволяє швидко виділяти ресурси й надавати сервіси IT на основі політик з контролем всіх операцій.

В Cisco планують і далі розвивати концепцію ACI і засобу керування. Це призначене для мережі ЦОД рішення може поширитися й за його межі – на магістральну й кампусну мережу, використовуватися в обчислювальних системах і системах зберігання).

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure.

– Досліджена система керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure.

– На основі отриманих результатів досліджень створена програмна реалізація системи керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання керування мережною інфраструктурою на основі Cisco Application Centric Infrastructure. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
2. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
3. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
4. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
5. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
6. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
7. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
8. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
9. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
10. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
11. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
12. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
13. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
14. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
15. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
16. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 .

P.517-522.
17. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
18. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
19. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
20. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
21. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
22. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
23. Smirnov A.A., Kuzne tsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
24. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.