

УДК 004

О.Дібрівний, магістр гр. КН-22М-2

Центральноукраїнський національний технічний університет

## ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ДИНАМІЧНОГО ПЕРЕРОЗПОДІЛУ ТРАФІКУ ВУЗЛІВ МЕРЕЖІ У ХМАРІ

У статті розроблено програмне забезпечення, яке призначено для системи динамічного перерозподілу трафіку вузлів мережі у хмарі. Метою розробки є дослідження та програмна реалізація системи динамічного перерозподілу трафіку вузлів мережі у хмарі. Об'єктом дослідження є процес динамічного перерозподілу трафіку вузлів мережі у хмарі. Предметом дослідження є методи динамічного перерозподілу трафіку вузлів мережі у хмарі. Методи дослідження базуються на методах хмарних технологій, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи динамічного перерозподілу трафіку вузлів мережі у хмарі. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

**Постановка проблеми.** Для певної топології з найкращими положеннями контролера та перемикача SDN у хмарі час від часу демонструє низьку продуктивність, що призводить до затримок, що викликають роздратування, і незадоволених користувачів. Збільшений обсяг трафіку може призвести до заторів, що збільшує навантаження на певні комутатори та контролери та подовжує затримку передачі даних. Крім того, збій певних вузлів або з'єднань може призвести до аномального зростання навантаження трафіку на певні комутатори та контролери. Традиційних методів переміщення комутаторів і контролю перевантаження може бути недостатньо для забезпечення найкращої пропускної здатності та пропускної здатності для частих і непередбачуваних коливань мережевого трафіку. Крім того, певні комутатори/контролери можуть зазнавати великого трафіку порівняно з іншими комутаторами/контролерами. У таких несприятливих ситуаціях продуктивність мережі стає надзвичайно низькою.

**Аналіз останніх досліджень і публікацій.** При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи динамічного перерозподілу трафіку вузлів мережі у хмарі.

**Мета й завдання дослідження.** Метою роботи є дослідження та програмна реалізація системи динамічного перерозподілу трафіку вузлів мережі у хмарі.

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

- Огляд існуючих систем динамічного перерозподілу трафіку вузлів мережі у хмарі.
- Дослідження системи динамічного перерозподілу трафіку вузлів мережі у хмарі.
- Програмна реалізація системи динамічного перерозподілу трафіку вузлів мережі у хмарі.

*Об'єктом дослідження* є процес динамічного перерозподілу трафіку вузлів мережі у хмарі.

*Предметом дослідження* є методи динамічного перерозподілу трафіку вузлів мережі у хмарі.

*Методи дослідження* базуються на методах хмарних технологій, методах математичної статистики, методах розробки програмного забезпечення.

**Виклад основного матеріалу.** Програмно визначена мережа (SDN) є багатообіцяючою технологією в сучасних мережах і комунікаційних технологіях. Архітектура SDN складається з площини додатків, площини керування та площини даних, де відповідно розміщуються програма SDN, контролери SDN і комутатори SDN.

Протокол OpenFlow є основним протоколом зв'язку, який використовується в SDN. Південний інтерфейс SDN підтримує зв'язок між площиною керування та площиною даних, тоді як північний інтерфейс підтримує зв'язок між площиною керування та площиною додатків. Контролер є ключовим компонентом SDN, який керує загальним сценарієм мережі. Кілька контролерів існують для керування розподіленими комутаторами, які діють як об'єкти пересилання пакетів.

Комутатори консультуються з контролером для отримання правил пересилання з таблиць пошуку в контролерах. Однією з проблем SDN є проблема розміщення контролера (CPP) [1].

Правильне розташування контролерів має великий вплив на продуктивність, балансування навантаження, доступність або комбінацію кількох факторів у мережі зв'язку. Вибух мобільних телефонів, віртуалізація серверів і підходи до хмарного адміністрування є одними з прикладів, що спонукають індустрію фреймворків переоцінити скориговані моделі системних фреймворків. Edgenet запровадив екосистему Programmable Flow SDN, яка створює гіперконвергентне сховище/конвергентне сховище за допомогою контролера Openflow.

Після придбання Nicira в 2012 році VMware розробила платформу мережевої віртуалізації та безпеки VMware SDN, відому як VMware NSX. Щоб надавати прибуткові мережеві послуги на вимогу, платформа мережевих послуг Nokia (NSP) об'єднує автоматизацію обслуговування, оптимізацію мережі та динамічну гарантію. Це дає операторам більш ефективні засоби для автоматизації, оптимізації та гарантування мережевих послуг на численних мережевих рівнях, фізичній/віртуальній інфраструктурі та обладнанні від різних виробників. Nuage Networks (підприємство Nokia) надає Virtualized Services Framework (VSP) як платформу, нейтральну щодо постачальника, для побудови хмар, від невеликих приватних хмар до великих корпоративних хмар. Це інструмент SDN, який об'єднує обчислювальні ресурси в міру їх створення та віртуалізує мережеву інфраструктуру центру обробки даних. Були запропоновані різні статичні та динамічні рішення розміщення з урахуванням різних параметрів, таких як затримка зв'язку, навантаження контролера, використання контролера, накладні витрати на контрольний трафік, споживання ресурсів, час налаштування потоку, QoS тощо.

У більшості рішень CPP вирішується шляхом кластеризації, або шляхом перетворення його на задачу багатоцільової оптимізації, яка була розв'язана за допомогою евристичного або цілочисельного програмування. Розглядаючи динамічне навантаження трафіку разом із затримкою, різні дослідники, такі як Huque та ін. [2], Bhowmik і Gayen [3] та інші представили підходи до розміщення динамічного контролера. Але, для заданої топології, навіть з оптимальними положеннями контролера та перемикача,

Іноді виявлено, що SDN показує низьку продуктивність, що спричиняє затримки, що призводить до роздратування та незадоволення користувачів. Однією з причин такої низької продуктивності може бути збільшення трафіку. Збільшення трафіку через збільшення певного типу зв'язку між хостами може спричинити перевантаження, що може призвести до збільшення затримки зв'язку. Це може проявлятися у вигляді збільшення навантаження на комутатори та контролери.

Збій певних вузлів або з'єднань може спричинити ненормальне збільшення навантаження на трафік (надмірне збільшення кількості пакетів даних, що відхиляється від нормального або звичайного, як правило, у небажаний або тривожний спосіб) на певних комутаторах і контролерах, що призводить до збільшення в латентності (затримці). Існуючі методи міграції комутатора та контролю перевантажень можуть бути недостатніми для

досягнення найкращої пропускної здатності та пропускної здатності через часті та несподівані зміни мережевого трафіку.

Крім того, порівняно з іншими комутаторами та контролерами, деякі з них можуть мати високе навантаження трафіком. За таких несприятливих ситуацій продуктивність мережі стає надзвичайно низькою, що призводить до дратівливих затримок (затримок, що викликають незадоволення чи роздратування) і незадоволення користувачів мережі. Існуючі методи розподілу навантаження не завжди виявляються ефективними, оскільки вони або використовують методи міграції комутаторів, зосереджуються на балансуванні навантаження в площині даних за допомогою традиційного підходу найкоротшого шляху, або зосереджуються на балансуванні навантаження в площині керування SDN.

Враховуючи ці аспекти, було запропоновано ефективний підхід із використанням штучного інтелектуального розподілу навантаження в площині даних з урахуванням трафіку шляхом ефективного перенаправлення потоків пакетів (якщо виникає така несприятлива ситуація), щоб можна було досягти прийнятної продуктивності мережі. підтримується наявними ресурсами. продуктивність мережі стає надзвичайно низькою, що призводить до дратівливих затримок (затримок, що викликають незадоволення або роздратування) і незадоволення серед користувачів мережі. Існуючі методи розподілу навантаження не завжди виявляються ефективними, оскільки вони або використовують методи міграції комутаторів, зосереджуються на балансуванні навантаження в площині даних за допомогою традиційного підходу найкоротшого шляху, або зосереджуються на балансуванні навантаження в площині керування SDN.

У цій статті представлено підхід, що використовує штучний інтелектуальний динамічний розподіл навантаження з урахуванням трафіку в площині даних SDN шляхом перенаправлення потоків пакетів (при виникненні несприятливої ситуації) ефективним способом, щоб прийнятну продуктивність мережі можна підтримувати за допомогою наявних ресурсів. Запропонований підхід було застосовано до мережі NSF і проведено прикладне дослідження. Запропонований підхід було оцінено та визнано досить ефективним у зменшенні ненормальних навантажень на комутатори/зв'язки, оскільки виявлено, що можна зменшити середнє навантаження на 396 одиниць за рахунок збільшення середньої затримки лише на 1,29 мс.. Крім того, представлено регресійний аналіз із використанням значень дисперсії навантаження, щоб підтвердити, що запропонований підхід є більш ефективним у забезпеченні меншої дисперсії навантаження порівняно з традиційним алгоритмом найкоротшого шляху (SP).

Щоб оцінити трафік у реальному часі для запитів, які додаються до мережі в пасивному режимі, Таһаеі et al. [4] запропонували механізм, за якого підвищені накладні витрати, пов'язані з обчисленнями контролера та витратами на зв'язок, були мінімізовані при збереженні точності. Щоб покращити продуктивність мережі, Chien et al. [5] запропонував структуру балансування навантаження для сервісно-орієнтованого SDN-SFC, де класифікація запиту ґрунтувалася на типі, а кожній службі було призначено пріоритет і далі.

#### **Динамічний розподіл навантаження з урахуванням трафіку**

З наявними значеннями навантаження комутаторів головний контролер обчислює ефективні шляхи потоку від усіх джерел до місць призначення для переміщення пакетів даних через фіксований проміжок часу (за рішенням адміністратора мережі). Коли виникає несприятлива ситуація, головний контролер оновлює записи таблиці потоків у комутаторах через підлеглий контролер на основі шляхів потоку, обчислених головним контролером.

#### **Розробка структурної схеми**

Структурна схема розробленої системи зображена на рисунку 1. Не дуже давно постачальники налагодили випуск систем динамічного перерозподілу трафіку мережі – програмних продуктів, які вирівнюють навантаження, розподіляючи її по декількох серверах. Крім того, вони підвищують відказостійкість WEB-серверів: у випадку відмови однієї машини направляють пакети даних на інший сервер або сайт. Таким чином, час очікування скорочується, а число неопрацьованих запитів зводиться до мінімуму. Системи динамічного

перерозподілу трафіку мережі можна використовувати як при наявності лише одного WEB-сайту, так і при роботі із цілим рядом вузлів. Одержавши подання про те, що таке системи динамічного перерозподілу трафіку мережі і як вони працюють, можна визначити найбільш важливі їхні характеристики, які варто враховувати при виборі засобу вирівнювання навантаження.

Система динамічного перерозподілу трафіку мережі WEB-серверів – це інструментальний засіб, призначений для переадресації клієнтських запитів на найменш завантажений або найбільш підходящий WEB-сервер із групи машин, на яких зберігаються дзеркальні копії інформаційного ресурсу. Клієнт не підозрює про те, що звертається до цілої групи серверів: всі вони представляються йому у вигляді якогось єдиного віртуального сервера. Припустимо що ми обслуговуємо один WEB-сайт і маємо при цьому два WEB-сервери. Представляючи наш сайт користувачам Internet, система динамічного перерозподілу трафіку мережі використовує ім'я віртуального комп'ютера, а також віртуальна IP-адреса (VIP-адресу – скажемо). Щоб зв'язати ім'я віртуальної системи й відповідна VIP-адреса із двома нашими WEB-серверами, ми повинні опублікувати ім'я системи і її VIP-адресу на сервері DNS. Система динамічного перерозподілу трафіку мережі постійно контролює навантаження й ступінь готовності кожного з WEB-серверів. Коли на вузол заглядає відвідувач, його запит надходить не на один з WEB-серверів, а в систему динамічний перерозподіл трафіку мережі. Ця система й ухвалює рішення щодо того, на який сервер направити запит. При цьому вона керується такими критеріями, як завантаження кожного підопічного сервера, а також дотримує умов і правила, сформульовані адміністратором. Потім система динамічного перерозподілу трафіку мережі направляє запит клієнта відповідному серверу (як правило, воно ж направляє відповідь сервера клієнтові, але це залежить від конкретної реалізації).

Поряд з тестуванням стеків протоколів, кращі засоби динамічного перерозподілу трафіку мережі можуть забезпечувати моніторинг часу відгуку й готовності як самого WEB-сервера, так і встановлених на ньому додатків ще одним способом: на сервер направляється запит за протоколом HTTP на одержання інформаційних матеріалів або адреси URL. Час відгуку визначається системою динамічного перерозподілу трафіку мережі як час із моменту відправлення запиту на надання інформації до моменту одержання коду повернення.

### **Вибір сервера**

При організації стійкого з'єднання основне завдання системи полягає в тому, щоб ідентифікувати клієнта й зв'язати відповідний ідентифікатор із сервером-одержувачем запиту. Як правило, системи динамічного перерозподілу трафіку мережі використовують як ідентифікатор клієнта, застосовувану їм IP-адресу відправника. Але вся справа в тому, що адреса відправника не обов'язково збігається з реальною IP-адресою клієнта. Багато компаній і провайдери, намагаючись удержати WEB-трафік під контролем і сховати від сторонніх очей IP-адреси своїх користувачів, установлюють сервери-посередники. На щастя, цю проблему можна вирішити, якщо скористатися системою динамічного перерозподілу трафіку мережі, оснащеної засобами ідентифікації IP-адрес відправників і номерів портів TCP. Подібні системи здатні пізнавати клієнтів навіть у тому випадку, коли останні виходять в Internet через той самий проху-сервер. Така ідентифікація можлива тому, що кожне TCP-з'єднання має унікальна IP-адресу відправника й номер порту TCP. Ще один спосіб ідентифікації клієнта, що проводить захищений сеанс зв'язку за протоколом HTTP, полягає в тому, щоб зафіксувати ідентифікаційний номер сеансу зв'язку користувача за протоколом Secure Sockets Layer (SSL). Протокол SSL призначає кожному встановленому сеансу зв'язку спеціальний ідентифікатор, а прикладні програми для віртуальних магазинів часто користуються цим протоколом. Найсучасніший засіб підтримки стійких з'єднань – це розповсюджені по мережі WEB cookie-файли. Нагадаю, що ці файли містять як відомості про клієнта, так і інші дані (наприклад, про те, з яким сервером клієнт зв'язувався востаннє). Аналіз умісту cookie-файлів допомагає системі динамічного перерозподілу трафіку мережі ідентифікувати клієнтів і підбирати для них найбільш підходящий сервер. У число



постачальників систем динамічний перерозподіл трафіку мережі, оснащених засобами роботи з cookie-файлами, входять такі компанії, як Alteon WEBSystems, ArrowPoint Communications, F5 Networks і Resonate.

### **Переадресація трафіку**

Системи динамічного перерозподілу трафіку мережі можуть перенаправляти трафік клієнтів на вибраний сервер декількома способами: по методу трансляції адрес із керуванням доступом до середовища передачі (media access control (MAC) address translation, MAT), по методу трансляції мережних адрес (Network Address Translation, NAT), або – при використанні відкладеного зв'язування – за допомогою механізму шлюзу TCP (TCP gateway). Розглянемо, як реалізується кожний із цих методів перенапряму трафіка засобами вирівнювання навантаження.

**MAT.** Цей метод може бути реалізований системою динамічного перерозподілу трафіку мережі при тій умові, що кожний WEB-сервер поряд зі своїм фізичним IP-адресою використовує в якості інтерфейсного адресу зворотного зв'язка (loopback interface address) VIP-адреси системи балансування. Однак у якості IP-адреси відправника сервер указує VIP-адресу системи динамічного перерозподілу трафіку мережі, як якби трафік надходив клієнтові саме від її. Таким чином, що впливає пакет від клієнта направляється не тому, що відповів, серверу, а системі динамічного перерозподілу трафіку мережі.

### **Вибір сайту й керування трафіком на глобальному рівні**

У тих випадках, коли інформаційні ресурси розміщуються на декількох дзеркальних вузлах, системи динамічного перерозподілу трафіку мережі (іменовані також глобальними системами динамічного перерозподілу трафіку мережі) визначають підходящий для клієнта вузол за допомогою вже описаних механізмів вибору сервера. Крім того, як критерій вибору сайту глобальна система балансування може використовувати такий показник, як відстань між сайтом і клієнтом (виражене в кількості транзитних ділянок і в тривалості мережної затримки). При визначенні найбільш підходящого сайту система балансування часто направляє трафік клієнта на відповідний вузол за допомогою інтелектуальної функції DNS.

Крім методу динамічного призначення клієнтові того або іншого вузла системи динамічного перерозподілу трафіку мережі можуть використовувати для зв'язування конкретних клієнтів з конкретними сайтами метод статичного призначення (static mapping method).

### **Архітектура служби динамічного перерозподілу трафіку мережі мережі**

Для досягнення максимальної пропускну здатності й відказостійкості служба ДПТМ використовує повністю розподілену програмну архітектуру. На всіх вузлах кластера паралельно виконуються однакові драйвери служби ДПТМ. Ці драйвери поєднують всі вузли в єдину мережу для обробки вхідного потоку даних, що надходять на основну IP-адресу кластера (і на додаткові IP-адреси багатомережних вузлів). Для кожного окремого вузла драйвер виконує функції фільтра між драйвером мережного адаптера й стеком протоколів TCP/IP, дозволяючи розподіляти потік даних, одержуваних вузлом. Таким чином, що надходять запити розділяються й розподіляються між вузлами кластера.

Служба ДПТМ функціонує як мережний драйвер, розташований у мережній моделі нижче високорівневих протоколів додатків, таких як HTTP і FTP.

Така архітектура дозволяє домогтися максимальної пропускну здатності за рахунок використання широкомовної підмережі для доставки даних, що надходять, на всі вузли кластера, що дозволяє обійтися без маршрутизації вхідних пакетів. Оскільки фільтрація непотрібних пакетів працює швидше, ніж маршрутизація (при якій необхідно одержати, перевірити, перезаписати й повторно відправити кожний пакет), при використанні служби ДПТМ досягається більше висока пропуску здатність мережі в порівнянні з рішеннями на основі диспетчеризації. При рості швидкості роботи сервера й мережі пропорційно росте й продуктивність; у такий спосіб усувається залежність від продуктивності апаратних рішень для розподілу навантаження на основі маршрутизації. Наприклад, у гігабітних мережах служба ДПТМ демонструє пропуску здатність до 250 Мб/с.

Іншою ключовою перевагою повністю розподіленої архітектури служби ДПТМ є чудові показники відказостійкості (N-1) для кластера з N вузлами. Навпроти, у рішеннях на основі диспетчеризації обов'язково є центральний елемент, що є «вузьким місцем» системи, для усунення якого необхідно використовувати резервний диспетчер, забезпечуючи лише односпрямоване переміщення навантаження при збої. Такий захист від збою менш ефективний у порівнянні з повністю розподіленою архітектурою.

В архітектурі служби ДПТМ для одночасної доставки даних, що надходять, на кожний вузол кластера використовується концентратор і/або комутатор підмережі. Проте, такий підхід веде до збільшення навантаження на комутатори й вимагає додаткових ресурсів пропускної здатності портів. Звичайно це не впливає на більшість широко використовуваних додатків (наприклад, WEB-служби й мультимедіа-мовлення), оскільки вхідні дані становлять дуже невелику частку загального потоку даних у мережі. Проте, якщо пропускна здатність лінії зв'язку до комутатора з боку клієнта значно вище пропускної здатності каналу з боку сервера, що входять дані можуть становити досить значну частину загального потоку даних. Та ж проблема виникає й при підключенні декількох кластерів до одного комутатора, коли для окремих кластерів не настроєні віртуальні локальні мережі LAN.

Повністю конвеєрний механізм служби ДПТМ при надходженні пакетів одночасно передає їх у стек протоколів TCP/IP і одержує пакети від драйвера мережного адаптера. Це знижує загальний час обробки потоку даних і затримку, оскільки стек TCP/IP може обробляти пакет одночасно з одержанням драйвером NDIS наступного пакета. Крім того, потрібно менше ресурсів для координації операцій стека TCP/IP і драйвера, а також, у більшості випадків, у пам'яті не створюються додаткові копії пакетів даних. При відправленні пакетів служба ДПТМ також забезпечує підвищену пропускну здатність, малий час затримки й відсутність накладних витрат продуктивності за рахунок збільшення числа пакетів TCP/IP, які можуть бути відправлені за один виклик NDIS. Для досягнення настільки високої продуктивності служба ДПТМ використовує пул буферів і дескрипторів пакетів, використовуваний для конвеєрних операцій зі стеком TCP/IP і драйвером NDIS.

На структурній схемі, яка зображена на рисунку 1, показано, що система, структурно, складається з наступних блоків:

- Блок динамічного перерозподілу трафіку мережі.
- Блок формування звітів.
- Блок формування сигналів керування перерозподілу трафіку мережі.
- Блок збирання статистичного навантаження на вузли мережі.
- Блок аналізу статистичного навантаження.

Для рішення завдання вибору числа й розміщення вузлів мережі, представленої у вигляді інформаційно-обчислювального комплексу, запропоновано використовувати евристичні алгоритми, засновані на методах локальної оптимізації й теорії масового обслуговування. Альтернативний підхід до рішення завдання дискретного математичного програмування, заснований на теорії графів, неприйнятний через високу обчислювальну складність при великій кількості вузлів у мережі. Наприклад, у мережі з 10 вузлів існує  $2^{45}$  варіантів розташування ліній зв'язку, включаючи безліч тривіальних випадків. Якщо припустити, що аналіз кожного варіанта становить 1 секунду, то на дослідження буде потрібно більш ніж  $9 \cdot 10^8$  років.

На змістовному рівні завдання побудови оптимальної мережі формується в такий спосіб. Виходячи із заданих значень інтенсивності запитів абонентів з урахуванням вводимих допусків і обмежень визначити оптимальні за критерієм мінімуму наведених витрат структурні параметри мережі: число й розміщення програмно-апаратних модулів вузлів мережі у пунктах мережі, співвіднести групи абонентів з обслуговуваними їх вузлом мережі, ємністю вузла мережі і каналів зв'язку. При цьому повинні дотримуватися обмеження на якість обслуговування: середній час обробки повідомлення й імовірність своєчасного обслуговування не повинні перевищувати граничних значень.



Рисунок 1 – Структурна схема системи

Як критерій оптимізації обрані наведені витрати на канал зв'язку й вузол мережі.

Як модель, що інтерпретує інформаційний потік у мережі з УЦ, розглядається дві мережі масового обслуговування (СеМО):

- багатофазна СеМО з відмовами й повторними викликами;
- багатофазна СеМО комбінованою комутацією.

Завдання пошуку оптимальної структури мережі успішно вирішуються з використанням евристичних алгоритмів, заснованих на методах локальної оптимізації зі спрямованим перебором варіантів структури мережі.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів динамічного перерозподілу трафіку вузлів мережі у хмарі. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем динамічного перерозподілу трафіку вузлів мережі у хмарі; Досліджена система динамічного перерозподілу трафіку вузлів мережі у хмарі; На основі отриманих результатів досліджень створена програмна реалізація системи динамічного перерозподілу трафіку вузлів мережі у хмарі. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання динамічного перерозподілу трафіку вузлів мережі у хмарі. 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. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyzy, 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. Smirnov A.A., Kuznetsov 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.
8. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
9. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
10. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
11. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
12. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
13. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
14. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95
15. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» Вісник Черкаського державного технологічного університету. Технічні науки. №4. С. 103-110. 2020.
16. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.
17. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.
18. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.
19. Смірнов О.А., Дреєва Г.М., Дреєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральнотраїнський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.
20. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.