УДК 004

С.Гречушкін, магістр гр. КН-23М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ОПТИМІЗАЦІЇ ПРОДУКТИВНОСТІ ТА НАДІЙНОСТІ МЕРЕЖНИХ СИСТЕМ ЗБЕРІГАННЯ BIG DATA

У статті розроблено програмне забезпечення, яке призначено для системи оптимізації продуктивності та надійності мережних систем зберігання Big Data. Метою розробки є дослідження та програмна реалізація системи оптимізації продуктивності та надійності мережних систем зберігання Big Data. Об'єктом дослідження є процес оптимізації продуктивності та надійності мережних систем зберігання Big Data. Предметом дослідження є методи оптимізації продуктивності та надійності мережних систем зберігання Big Data. Методи дослідження базуються на методах Big Data та теорії надійності, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи оптимізації продуктивності та надійності мережних систем зберігання Big Data. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Централізоване зберігання даних для систем зберігання Big Data на підключені до мережі ресурсах має безліч переваг – як для малого бізнесу, так і для корпоративних ЦОД. У той же час при централізованому зберіганні можливі проблеми продуктивності – у випадку інтенсивного доступу до тих або інших ресурсів або при виконанні ресурсномістких додатків. Як же забезпечити достатню продуктивність при виборі мережної інфраструктури для зберігання даних і при налаштуванні її конфігурації з урахуванням потреб організації?

Незалежно від того, чи використовуєте ви мережа зберігання даних SAN або пристрій NAS, швидше за все, ті або інші критичні корпоративні дані зберігаються в якійсь мережній файловій системі або, у всякому разі, повинні в ній зберігатися. Їхнє спільне використання означає більше ефективний розподіл ємності зберігання, простий доступ до корпоративної інформації й захищеність за допомогою таких засобів, як RAID. Централізоване зберігання означає також більше просте керування ресурсами зберігання, а заплановане створення резервних копій простіше виконувати у випадку мережних систем зберігання, чим при використанні DAS.

У той же час при централізованому зберіганні можливі проблеми продуктивності – у випадку інтенсивного доступу до тих або інших ресурсів або при виконанні ресурсномістких додатків. Як же забезпечити достатню продуктивність при виборі мережної інфраструктури для зберігання даних і налаштуванні її конфігурації для потреб організації?

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи оптимізації продуктивності та надійності мережних систем зберігання Big Data.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи оптимізації продуктивності та надійності мережних систем зберігання Big Data.

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

– Огляд існуючих систем оптимізації продуктивності та надійності мережних систем зберігання Big Data.

– Дослідження системи оптимізації продуктивності та надійності мережних систем зберігання Big Data.

– Програмна реалізація системи оптимізації продуктивності та надійності мережних систем зберігання Big Data.

Об'єктом дослідження є процес оптимізації продуктивності та надійності мережних систем зберігання Big Data.

Предметом дослідження є методи оптимізації продуктивності та надійності мережних систем зберігання Big Data.

Методи дослідження базуються на методах Big Data та теорії надійності, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Включення у свій час програмного забезпечення ініціатора iSCSI в Windows 7 і Windows Server 2008 вплинуло на корпоративні системи зберігання, дозволивши без додаткових зусиль реалізувати блоковий доступ до мережних СЗД не тільки на серверах, але й на звичайних настільних ПК і робочих станціях. Однак простота використання iSCSI виявилася ціпком про два кінці. Хоча сумісність програмного забезпечення iSCSI – зручна властивість сучасних операційних систем, програмна обробка команд зберігання даних iSCSI і пакетів TCP/IP вимагає ресурсів процесора хосту, що знижує його продуктивність.

Рішення складається у використанні апаратних засобів для «розвантаження» iSCSI і TCP/IP (offloading). При виділенні процесорного ядра для обробки даних iSCSI і TCP/IP, апаратні засоби, такі як Qsan QiSOE, можуть при мінімальних початкових інвестиціях знизити непродуктивні витрати на протокол, що виливається в значне поліпшення продуктивності як при послідовних читанні й записі, так і при довільному доступі до даних.

Накладні витрати на комунікаційний протокол позначаються як на хості, так і на пристрої зберігання. Апаратні карти розширення на стороні хосту – так звані конвергентні мережні адаптери (Converged Network Adapter, CNA) – поєднують функціональність традиційної мережної карти й адаптера шини хосту (Host Bus Adapter, HBA), переносячи обробку протоколів TCP/IP і iSCSI в устаткування. Виключення обробки протоколу зберігання даних із програмного навантаження виявляється корисним і в інших випадках. Протокол Fibre Channel, найбільш популярний у мережах зберігання SAN, теж може одержати значний виграш по продуктивності за рахунок переносу на апаратний рівень непродуктивних витрат при обробці протоколу зберігання даних.

Апаратний RAID

Забезпечуючи надмірність даних, контроль парності й навіть чудову продуктивність, RAID є однієї з основних технологій систем зберігання даних корпоративного рівня, про яку проте нерідко забувають і не враховують того, що програмний RAID позначається на продуктивності. Будучи убудованим у кожну сучасну операційну систему, він не завжди ідеально відповідає потребам корпоративних ЦОД.

Відділення реалізації RAID від операційної системи може дати ряд переваг. При простої реалізації, такий як RAID0 або RAID1, впливом програмного забезпечення RAID на продуктивність системи можна зневажити, але цей режим рідко застосовується в корпоративних системах. Якщо враховувати операції перевірки парності й велика кількість дисків, то апаратний RAID буде помітно відрізнятися від програмного в характеристиках IOPS.

Апаратний RAID більше надійний для корпоративного застосування. На випадок проблем з електроживленням передбачена можливість використання батареї (Battery Backup Unit, BBU), що дозволяє зберігати всі важливі дані в енергонезалежній пам'яті й зчитувати їх звідти після подачі електроенергії. Оскільки керування RAID відділене від операційної системи, цілісності даних ніщо не загрожує навіть при аварійному завершенні роботи ОС. Крім того, апаратний RAID здатний захищати дані в процесі завантаження операційної системи, у той час як програмний «виходить на сцену» лише по його завершенні.

Хочемо ми того чи ні, виходять із ладу навіть диски корпоративного класу. У такому випадку RAID повинен перешикувати масив, використовуючи диск гарячого резерву й дані парності зі справних дисків. Якщо ємність виміряється в гігабайтах, час перебудування дискового масиву виявиться цілком прийнятним, але при терабайтної ємності, що зараз уже не рідкість, інтервал перебудування може становити кілька годин, і все це час корпоративна інформація буде уразливою. У сучасних ЦОД, де ємності зберігання, звичайно, виміряються терабайтами й петабайтами, функція швидкого перебудування (fast rebuild), убудована в мережні СЗД, є вкрай необхідною.

У корпоративних ЦОД широко застосовується віртуалізація. У мережних СЗД віртуалізуються ресурси зберігання, що дозволяє управляти ними централізовано. Крім того, завдяки віртуалізації можна консолідувати обчислювальні потужності, централізовано управляти робочими станціями, відновленнями й т.д. Всі ці переваги цілком реальні, але найбільші вигоди приносить використання мережних систем зберігання даних, сертифікованих для віртуалізованих середовищ.

Тим часом віртуалізація пред'являє до систем зберігання унікальні вимоги, і СЗД нерідко стають вузьким місцем при спробі збільшити продуктивність середовища VDI. Так, VMware, беручи до уваги унікальні вимоги, які віртуалізація пред'являє до СЗД, пропонує спеціальні протоколи, наприклад VMware vSphere Storage API – Array Integration (VAAI). Аналогічно тому, як операції iSCSI і RAID можна перенести на рівень спеціальних апаратних засобів, тим самим розвантаживши процесор, VAAI дозволяє відокремити операції зберігання даних від сервера віртуалізації. У результаті кожний компонент ЦОД одержує можливість робити те, на що він найбільше здатний. Устаткування зберігання даних, сертифіковане й сумісне з VAAI, не тільки підвищує продуктивність середовища віртуалізації, але й забезпечує ефективне виконання найважливіших функцій віртуалізованих СЗД – зокрема, клонування, обнуління й знімки даних.

Ключовими метриками будь-якого корпоративного ЦОД є продуктивність і надійність мережних СЗД, але диявол криється в деталях. Кешування на SSD у багаторівневому середовищі зберігання (tiered storage) і динамічний розподіл ємності (thin provisioning), перенос функцій iSCSI і RAID на апаратний рівень (offloading), вибір систем зберігання даних з функцією швидкого перебудування (fast rebuild), сумісність із VMware дозволять компаніям одержати максимальну віддачу від своїх інвестицій в устаткування.

Розробка структурної схеми

Мережна система зберігання даних (NAS) – це пристрій зберігання із загальним доступом, що надає консолідовану файлову систему й послуги зі зберігання серверам відкритих систем. Додатки й користувачі одержують доступ до даних через загальну IP-мережу. У кожного NAS-пристрою є власна унікальна IP-адреса.

Як працює NAS

NAS – це відкрита комп'ютерна система з ємністю для зберігання, приєднаної до мережі, що надає послуги зі зберігання даних на файловій основі іншим пристроям у мережі. NAS використовує стандартну файлову систему CIFS і мережну файлову систему NFS, що дозволить клієнтам Microsoft Windows, Linux і UNIX одержати доступ до файлів, файловим системам і базам даних в IP-мережі.

Переваги NAS

Коли в наявності є більші обсяги, різні типи й рівні системи зберігання даних, приєднаної безпосередньо до сервера (DAS) або внутрішньої СЗД, може бути складно й дорого управляти даними й підтримувати їх у зв'язку з дуже низькими коефіцієнтом використання. NAS надає економію засобів і простоту в консолідованому зберіганні при використанні існуючої IP-мережі, при цьому усуває витрати й складності, зв'язані з будівництвом і підтримкою вторинної мережі, як з мережею зберігання даних (SAN).

Можна виділити три способи рішення завдання побудови каскаду схоронності даних.

1. Мережне резервування на інші сервера й NAS. Мережне резервування має масу переваг, тому що дозволяє резервувати масив даних незалежно від дистанції до мети

зберігання резервної копії. Мережний сервер зберігання резервних копій може одночасно використовуватися й для резервування інших типів дані компанії. При мережному резервуванні процес передачі потоку даних може відбуватися по протоколах: FTP, sFTP, HTTP/HTTPs, а також rsync, що найбільше часто зустрічається для міжсерверного обміну.

Якщо як базове встаткування відеореєстрації й зберігання використовуються NAS-сервери, то між джерелом і метою резервування можна створити не просто систему автоматичного резервування за розкладом, але й автосинхронізацію. Тобто в режимі реального часу безперервним потоком буде відбуватися дзеркалювання даних, створюючи дублюючий образ масиву на іншому NAS, установленому в межах вашої локальної мережі або десь у вилученому офісі. На сьогодні мережне резервування є самим вірним рішенням для організації постійного процесу резервування даних. Мінусом такого рішення можна назвати вартість, оскільки вартість резервного сервера або NAS може наближатися до вартості провідного сервера. Серед провідних виробників спеціалізованих мережних систем зберігання й резервування можна відзначити наступних найбільш помітних гравців:

– середній рівень і початок верхнього – Netgear, Synology, QNAP;
– масштабовані системи вищої категорії (причому й у плані ціни) – Netapp, EMC2, HP.

2. Локальне резервування на NAS. Одержавши у своє розпорядження 8 – 10 дискових накопичувачів, ви неминуче зштовхнетеся з такою проблемою: куди можна зарезервувати настільки великий обсяг даних. Якщо з якихось причин немає можливості використовувати аналогічне по ємності мережне сховище, то відповіддю є NAS (Direct Attached Storage) – зовнішні сховища прямого підключення.

NAS являє собою апаратний RAID-масив без якої-небудь убудованої ОС. Управляється й конфігурується зовнішніми засобами Це автономний продукт ємністю звичайно від 4 до 8 дисків і більше, створений для безпосереднього підключення до сервера, NAS або NVR як зовнішня ємність розширення або зовнішнього масиву, на який здійснюється локальне резервування даних із провідного сервера або NAS.

Перевагою NAS є ціна, що звичайно в 1,5 рази нижче NAS з ідентичною кількістю дисків. NAS можуть підключатися до сервера або NVR по інтерфейсах eSATA, USB 2.0/3.0 або SAS і підтримують рівні зберігання JBOD, RAID5, 50, 0 і касетний режим. Якщо ми підключимо NAS до будь-якому NAS (навіть початкового рівня) або серверу й пропишемо відповідні права доступу до цієї зовнішньої ємності, то одержимо для цілей резервування справжнє мережне сховище високої ємності, причому за дуже розумні гроші.

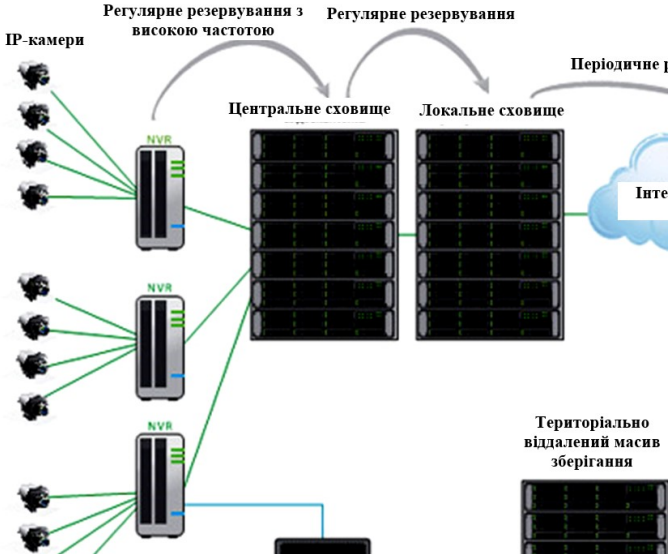

Рисунок 1 – Структурна схема системи

Серед виробників NAS-накопичувачів можна відзначити CFI Group, RAIDON, Promise Technology. У виробника мережних систем зберігання Synology є фірмове рішення – модулі

розширення DX/RX. По суті, це теж NAS-продукти, але розраховані винятково для підключення до мережних накопичувачів і NVR Synology Особливість даного рішення – можливість об'єднання даних у єдиний масив зберігання з головним NAS.

3. Резервування в комерційні ЦОД. Як варіант реалізації територіально розподіленого резервування в додатку до завдання схоронності особливо коштовного відеоконтенту можна розглядати систему резервування в комерційні ЦОД. Безумовно, сьогодні це недешево, і як і раніше можуть виникати проблеми з каналами передачі даних, але, як правило, завдання організації постійного каналу між вашим власним центром агрегації відеоконтенту й зовнішнім ЦОД вирішити можливо. Особливо якщо жорстко ставити завдання виключення більшості ризиків, пов'язаних з локалізацією даних у межах власних мереж зберігання.

Для зв'язку із ЦОД може бути використана й фізична лінія, і передача даних через Інтернет за умови організації VPN-підключення до ЦОД. VPN забезпечує захищеність каналу й дає можливість мережним накопичувачам і серверам звертатися до ємностей ЦОД як до локальних ресурсів своєї мережі. Це забезпечує можливості застосування стандартних політик резервування. Сучасні NVR, наприклад Synology, мають убудований VPN-клієнт і можуть самостійно створювати тунель резервування в дата-центр.

Яку би модель по забезпеченню схоронності даних не вибрала ваша компанія, вона повинна бути попередньо ретельно осмислена й розрахована математично як з погляду необхідних ємностей, так і з погляду циклу відновлення масиву. Сучасні технології інкрементального резервування й зберігання снапшотів (не самого репліканта масиву, а його моментальних знімків на точку часу) можуть істотно знизити потреба в обсязі зберігання й, отже, зберегти ваші гроші.

Резервування – дуже важливий і непростий процес як з погляду правильної технічної реалізації, так і з погляду організаційній складовій. Рекомендується обов'язково мати чітко формалізовану схему політики резервування й розписати по ролях всі зони персональної відповідальності фахівців з екстреного відновлення даних з резервних ємностей і введенню системи в роботу у випадку збоїти

Аудит мережної інфраструктури

Будь-які мережні пристрої відеореєстрації будуть працювати в межах конкретної локальної мережі з усіма її проблемами й недоліками. Задайте собі питання, чи може поточна мережна інфраструктура стати причиною збоїти й розриву зв'язку між камерами й NVR? На жаль, часто відповідь може бути позитивним. Не заглиблюючись у тему причин і недоліків, опишемо, що потрібно мати на увазі для зниження ризиків.

1. Мережа відеоспостереження повинна бути відділена від мережі загального користування. При використанні безлічі камер високого дозволу пропускна здатність мережі може досягати граничних значень, тому не виключається негативний взаємний вплив офісного трафіку й відеопотоків з камер, особливо у великих організаціях. Крім того, якщо з вини IT-адміністратора трапляється тимчасовий колапс у мережі, можуть бути зроблені перезавантаження мережного встаткування й зв'язаних серверів без попередження адміністрації мережі відеоспостереження. В ідеалі в IT-устаткування й устаткування мережі відеоспостереження повинні бути різні відповідальні особи з поділом прав доступу й навіть різна локалізація

2. При підключенні до активного мережного встаткування NVR урахуйте їхню особливість: сучасні NVR мають кілька мережних портів (звичайно 2 – 4). Включайте NVR різними портами в різні комутатори (світчі), тоді навіть вихід з ладу одного з комутаторів не паралізує відеореєстрацію повністю Ніколи не включайте всі камери одного сегмента відеоспостереження в один свитч або хаб.

3. Зареєструйте камери, установлені в критично важливих зонах відеоспостереження, на декількох NVR, що мають підключення до різного мережного встаткування. Більшість професійних IP-камер мають функцію генерації декількох потоків одночасно. Збережете таблицю крос-реєстрації камер на різних NVR.

Аудит системи енергопостачання й резервного живлення

Велика історія СЗД і систем відеореєстрації знала масу прикладів, коли, вклавши масу грошей в устаткування й ПЗ, люди відкладали "на потім" яку-небудь на перший погляд несуттєву деталь – систему кондиціювання або резервного живлення. І те й інше найчастіше приводило до застрашливої тиші в серверному й організаційно-кадровому виводам керівництва. І якщо кондиціювання – річ досить дорога, її хочеться мати, але аргументувати її закупівлю керівництву не завжди вдається, то за безперебійне живлення у випадку СЗД і систем збору відеоконтенту потрібно просто битися

Необхідно взяти за правило, що в системах СЗД і відеореєстрації кожний вузол повинен мати хоча б примітивне джерело резервного живлення – хоча б побутовий ДБЖ. Джерела безперебійного живлення (ДБЖ) повинні бути забезпечені кожному NVR, на який відбувається збір хоч скільки-небудь коштовної інформації. ДБЖ повинні живити світчі й варті перед ними маршрутизатори. Втрата живлення на камері може відключити відеоканал на якийсь час, а різкий кидок напруги або провал по живленню можуть віднести із собою в "кращий світ" десятки терабайт важливого відеоархіву разом з NVR, який вийшов з ладу.

Необхідно згадати ще про одну особливість: багато джерел безперебійного живлення прекрасно працюють при тимчасових відключеннях живлення, але найчастіше самі виявляються жертвами у випадку різкого стрибка напруги, тому що тільки деякі моделі ДБЖ мають убудовані стабілізатори напруги. Тому, якщо ви знаєте, що у вас може "гуляти" напруга, необхідно затурбуватися захистом ланцюга живлення потужним стабілізатором напруги.

Треба пам'ятати, що все, що пов'язане із системами безпеки, повинне мати багаторазове дублювання.

Треба визнати, що вибір джерел резервного живлення невеликий як для традиційних серверів, так і для NVR. На мій погляд, найбільш вірним вибором буде ДБЖ від APC, тому що вони мають підтримку зворотного зв'язка з NVR. Як пристрої для захисту мережного встаткування підійде й APC, і Powercom, і в принципі будь-який іншої. Для енергозахисту великих систем підійдуть продукти Emerson, але отут, звичайно, питання бюджету.

Те ж саме й для Windows-серверів: найбільш удалі програмні пакети по керуванню живленням сервера й екстреним відключенням і перезапуском при поновленні живлення створені саме для продуктів APC.

У ряду сучасних серверів доступне налаштування широкомовного оповіщення "побратимів" про надходження сигналу тривоги з ДБЖ. У результаті може бути активований ланцюговий механізм безпечного гасіння NAS-серверів.

Незважаючи на наявність всіх функцій керування живленням і в NVR/NAS, і в традиційних серверах, не варто зневажати такою простою функцією, як налаштування політик засипання й відключення у випадку одержання сигналу тривоги. Якщо ви не визначите їх, то встаткування саме "не догадається".

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів оптимізації продуктивності та надійності мережних систем зберігання Big Data.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем оптимізації продуктивності та надійності мережних систем зберігання Big Data.

– Досліджена система оптимізації продуктивності та надійності мережних систем зберігання Big Data.

– На основі отриманих результатів досліджень створена програмна реалізація системи оптимізації продуктивності та надійності мережних систем зберігання Big Data.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання оптимізації продуктивності та надійності мережних систем зберігання Big Data. 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.
25. 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.