

УДК 004

А.Мороз, магістр гр. КІ-23Мз

*Центральноукраїнський національний технічний університет*

## ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВІРТУАЛІЗОВАНОГО ВІДЕОСПОСТЕРЕЖЕННЯ

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

**Постановка проблеми.** Віртуалізація є важливою частиною ІТ-індустрії вже майже 20 років. Дивно, але багато хто в галузі не знайомі з технологією, її призначенням або тим, як вона пов'язана з постійно зростаючим ринком ІР-відеоспостереження. Перш ніж ми глибше зануримося у віртуалізацію та її роль у індустрії безпеки/ІР-відео, нам спочатку потрібно зрозуміти, що це таке, а потім ми зможемо переглянути, як це працює.

Простіше кажучи, віртуалізація – це обчислювальна технологія, яка створює віртуальне обладнання для функціонального запуску системних служб на основі програмного забезпечення, таких як програми, сервери обміну файлами, сховища, мережі та багато іншого. Створення віртуальних екземплярів цих служб і операційних систем дає змогу максимально використати ваші апаратні ресурси в повній мірі.

Віртуальні машини створюються та встановлюються на програмне забезпечення, яке називається гіпервізорами. Можливо, ви вже чули про деякі з найбільш популярних гіпервізорів у галузі, таких як VMware ESXi, Microsoft Hyper-V або Citrix XenServer. Є два основних типи гіпервізорів: голі або розміщені. Обидва дозволяють створювати кілька віртуальних машин в одній фізичній системі, яка також відома як хост. Якщо у вас є кілька хостів в одному середовищі, це називається кластером, і це надає можливість групувати всі комп'ютерні ресурси хоста в один гігантський пул, який можна ефективно та ефективно розподіляти. Після встановлення гіпервізор розподіляє ресурси цим віртуальним машинам, щоб вони могли працювати з максимальною ефективністю. Ці параметри також можна налаштувати вручну для кожного екземпляра віртуальної машини, що можна виконати, не виводячи пристрої в автономний режим. Наявність такого типу еластичного розподілу ресурсів, а також можливість запускати кілька систем на одній фізичній машині робить ІТ-операції набагато ефективнішими та знижує витрати на капітальні та операційні витрати, звільняючи простір у стійці та зменшуючи споживання електроенергії та нагрівання. і витрати на охолодження.

Оскільки вимоги до пропускної здатності камер високої роздільної здатності постійно зростають, завжди буде попит на можливість швидкого та ефективного додавання додаткових ресурсів до системи. Завдяки універсальності та гнучкості «на льоту», які досягаються завдяки використанню та розгортанню віртуальних машин, ринок відеоспостереження відчуває більший попит на такі типи розгортань. Розробка рішення системи відеоспостереження з віртуалізованим середовищем ще більше покращує

масштабованість і можливості для архітектури високої доступності, яка інакше була б неможлива з попередньо встановленою системою фізичного сервера.

**Аналіз останніх досліджень і публікацій.** При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи віртуалізованого відеоспостереження.

**Мета й завдання дослідження.** Метою роботи є дослідження та програмна реалізація системи віртуалізованого відеоспостереження.

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

- Огляд існуючих систем віртуалізованого відеоспостереження.
- Дослідження системи віртуалізованого відеоспостереження.
- Програмна реалізація системи віртуалізованого відеоспостереження.

*Об'єктом дослідження* є процес віртуалізованого відеоспостереження.

*Предметом дослідження* є методи віртуалізованого відеоспостереження.

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

**Виклад основного матеріалу.** В даний час віртуальні машини масово використовуються окремими особами та компаніями по всьому світу з різних причин і в різних сценаріях, включаючи, але не обмежуючись установками відеоспостереження. Якщо ви ще не чули про віртуальні машини, наступний розділ допоможе вам зрозуміти, що таке віртуальна машина, і чому мільйони користувачів і компаній уже користуються перевагами технології.

Віртуальна машина (яка також скорочено називається віртуальною машиною) – це емуляція (або віртуалізація) комп'ютерної системи, яка існує на фізичній машині, використовує її ресурси та апаратне забезпечення та забезпечує функціональність справжнього комп'ютера. На одній фізичній машині може бути кілька таких «дублікатів», які працюють від одного чи кількох програм гіпервізора, ізольованих і працюючих незалежно один від одного. Ви коли-небудь орендували хмарний сервер? Швидше за все, це віртуальна машина всередині фізичної машини, яка знаходиться десь у центрі обробки даних.

Технологія виникла на основі принципу *розподілу часу*, введеного в 1960-х роках, який дозволяв кільком користувачам використовувати комп'ютер одночасно, що пояснює одну з цілей використання віртуальної машини – *спільне використання ресурсів* для виконання різних завдань всередині однієї машини. Ця мета зазвичай є основною, коли віртуальна машина використовується в корпоративних системах.

Приватні особи, як правило, використовують віртуальні машини переважно з міркувань безпеки, завдяки *ізольованій роботі* віртуальних машин.

Існує третя причина використання віртуальних машин, яка зараз може представляти великий інтерес як для приватного, так і для бізнес-сектору – віртуальні машини дозволяють емулювати чужі операційні системи всередині іншої. Наприклад, коли деякі основні галузеві комп'ютерні програми працюють лише в ОС Windows, а робочими машинами є комп'ютери Mac.

Docker – це тип реалізації віртуальної машини на рівні операційної системи, що дозволяє працювати декільком ізольованим і безпечним віртуалізованим серверам на одному фізичному сервері. Docker використовує програмне забезпечення, що постачається в *контейнерах* – ізольовані комплекти програмного забезпечення, конфігураційних файлів і необхідних бібліотек – які обмінюються даними один з одним через певні визначені канали. Зазвичай докери використовують менше системних ресурсів, ніж звичайні віртуальні машини.

Якщо віртуальні машини настільки ефективні, ізольовані та безпечні речі, то чому не всі ними користуються?

Як ми встановили вище, віртуальні машини та докери не є *реальними* машинами, вони є емуляцією одного, середовища. Це збиває з пантелику багато програм, яким потрібно

отримати інформацію про машину, на якій вони працюють, або використовувати системні ресурси, до яких вони не мають доступу. Наприклад, якщо програму розроблено для роботи із зображеннями веб-камери, вона може не робити того, що повинна робити у віртуальній машині, яка не має прав доступу до USB-пристроїв.

Крім того, на деяких слабших комп'ютерах запуск віртуальних машин може інтенсивно навантажувати ЦП, тому, мабуть, не буде чудовою ідеєю створювати віртуальну машину для запуску топових відеоредакторів, сумно відомих своїми голодними вимогами.

Що стосується докерів, то не кожна програма підтримує роботу в одній, оскільки її структурно може знадобитися доступ до ресурсів, бібліотек, файлів, які не входять до їх власного контейнера. У такому випадку він може чудово працювати на реальному комп'ютері та не працювати належним чином у контейнері – і не кожен виробник витрачає дорожочіні ресурси та час на розробку обхідного шляху для Dockers, якщо це не те, що становить суттєву частку їх ринку.

Саме тому у даній роботі розробляється система для відеоспостереження, яка можуть працювати як у віртуальному середовищі, так і на фізичних машинах.

### **Розробка структурної схеми**

Система віртуалізованого відеоспостереження – віртуальний сервер відеоспостереження. Його можна встановити на комп'ютері з Windows, Mac або Linux на всіх стандартних платформах віртуалізації, таких як VMware, Hyper-V, KVM або Virtualbox, і працювати постійно. Одна або кілька віртуальних машин системи віртуалізованого відеоспостереження встановлено на одному або кількох серверах віртуалізації:

Система віртуалізованого відеоспостереження легко масштабується завдяки технології віртуалізації.

Усі переваги віртуалізації можна використати за допомогою системи віртуалізованого відеоспостереження, яка розробляється в даній роботі. До них належать:

- Безкоштовний розподіл ядер ЦП за потреби.
- Збільшити дисковий простір.
- Збільште обсяг оперативної пам'яті.
- Просте використання VLAN (віртуальних локальних мереж) для відділення мережевого трафіку від відеоспостереження.
- Продовження ліцензій або додавання ліцензій на камеру.
- Побудова інфраструктури до 90 камер з кількома віртуальними машинами системи віртуалізованого відеоспостереження, яка розробляється в даній роботі.
- Встановлення в існуючих середовищах віртуалізації, тому не потрібно купувати обладнання
- Переміщення віртуальної машини системи віртуалізованого відеоспостереження на інші фізичні сервери віртуалізації, також для балансування навантаження

Встановіть систему віртуалізованого відеоспостереження на існуючу ІТ-інфраструктуру, платформу віртуалізації VMware, Hyper-V або KVM. Тому системі віртуалізованого відеоспостереження не потрібно купувати новий сервер. У великій платформі системи віртуалізованого відеоспостереження просто встановлюється. Для цього можна розгорнути попередньо налаштовані образи для VMware або Hyper-V або встановити систему віртуалізованого відеоспостереження за допомогою образу ISO. Монтаж системи відеоспостереження системи віртуалізованого відеоспостереження виконується в найкоротші терміни.

Система віртуалізованого відеоспостереження підтримує засоби керування інтерфейсом віртуалізації. Наприклад, системою віртуалізованого відеоспостереження можна керувати за допомогою інструментів VMware у VMware vCenter для завантаження або автоматичного вимкнення та перезапуску у вікні обслуговування vCenter. Підтримка

адміністративних інструментів також працює в Hyper-V і KVM або VirtualBox. Також підтримуються менші середовища віртуалізації

Система віртуалізованого відеоспостереження встановлюється не лише у великих середовищах IT-інфраструктури, таких як кластери VMware, Hyper-V або KVM. Систему віртуалізованого відеоспостереження також можна легко встановити на окремих ПК або Mac. Систему віртуалізованого відеоспостереження можна встановити на ПК з Windows 10 під керуванням Hyper-V або на Mac із VirtualBox. Подібним чином ПК з ОС Linux можна використовувати для встановлення системи віртуалізованого відеоспостереження під VirtualBox або KVM і керування ним. Завдяки попередньо створеним інсталяційним образам інсталяція у VirtualBox на ПК або Mac завершується всього за кілька хвилин. Просто двічі клацніть файл OVA, який можна безкоштовно завантажити, щоб зручно, легко та швидко встановити у VirtualBox.

Систему віртуалізованого відеоспостереження оптимізовано для браузера Firefox, але також може використовуватися з іншими браузерами. Браузер Safari на iPhone і Chrome на Android також використовуються на мобільних пристроях.

Клієнти системи віртуалізованого відеоспостереження користуються багатьма перевагами віртуалізації. Система віртуалізованого відеоспостереження є масштабованою. Потужність процесора, простір на жорсткому диску та оперативну пам'ять можна розподілити за потреби. Систему віртуалізованого відеоспостереження можна перемістити на інший апаратний сервер або навіть працювати в надлишковому кластері. Систему віртуалізованого відеоспостереження також можна легко захистити через Veeam. І: Ви можете розширити камери за потреби та почати свій відеопроєкт з малого.

Система віртуалізованого відеоспостереження повністю управляється через Інтернет. Окрім великого веб-сайту для настільних комп'ютерів і планшетів, мобільні пристрої, такі як iPhone або телефони Android, можуть використовувати зрозумілі мобільні сторінки. Тривога, електронні листи з відео тривоги, альтернативно SMS-тривога, є однією зі стандартних функцій відеоспостереження. Тут розробники надають великого значення тому, що відео можна відтворювати без встановлення додаткового програмного забезпечення на звичайних пристроях, таких як Windows, Mac, Linux, iPhone, Android.

Система віртуалізованого відеоспостереження робить знімки на основі виявлення руху на зображенні. У веб-інтерфейсі можна встановити багато параметрів, які викликають тривогу залежно від налаштувань. За допомогою масок зображень можна оптимізувати виявлення руху. Порогові значення, які також встановлюються через веб-інтерфейс, зрештою запускають відеозаписи та відповідні електронні листи тривоги. Крім того, можна інтегрувати зовнішні детектори руху, щоб відеосигнали спрацьовували не через зміни пікселів у відеозображенні, а, наприклад, через світлові бар'єри або ультразвукові детектори руху, які вбудовані в деякі моделі камер. Будильники також можна налаштувати за допомогою часових таблиць. Тож ви отримуєте відеосигнали лише в тому випадку, якщо це актуально для вас! Також можна вільно визначати свята або свята, щоб надати їм власний профіль часу для відеозаписів і відеосигналів. На додаток до сповіщень електронною поштою з вкладеним відео, SMS-повідомлення можна надсилати на мобільний телефон одночасно, щоб ви отримували сповіщення про виявлення руху та спрацьовування сповіщення.

У системі віртуалізованого відеоспостереження ви можете надати кожному користувачу права на камери, записи та параметри налаштувань. Це робить можливим, наприклад, що користувач, який отримує лише повільніше представлення прямого ефіру через мобільний телефонний зв'язок, все ще може отримати значущий доступ до системи віртуалізованого відеоспостереження, не зупиняючи відео. Система віртуалізованого відеоспостереження пропонує прямі трансляції за допомогою технології, яка працює у веб-браузерах на комп'ютерах, а також на iPhone та смартфонах Android.

Залежно від програми, система віртуалізованого відеоспостереження може включати потоки MJPEG з високою якістю, але високою пропускну здатністю, або відео MPEG4 з

меншою пропускнуою здатністю та нижчою якістю. Користувач сам вирішує, яку потокову технологію використовувати в залежності від своїх вимог і моделі камери.

У системі віртуалізованого відеоспостереження база даних камер керується через відомі моделі камер, які можна вибрати та інтегрувати. База даних постійно поповнюється. Крім того, користувачі системи віртуалізованого відеоспостереження мають можливість інтегрувати вільно визначені камери. Немає жодних перешкод для інтеграції камер, якщо ви використовуєте загальні стандарти.

Важливою особливістю при використанні системи віртуалізованого відеоспостереження є підключення систем сигналізації. Систему віртуалізованого відеоспостереження можна підключити до систем сигналізації. У цьому випадку сигналізація системи віртуалізованого відеоспостереження викликає створення запису, який надсилається сигналізацією. Таким чином, користувач має швидке уявлення про те, що відбувається, і може швидко визначити, важливий чи неважливий сигнал тривоги.

Окрім функцій тривоги, система віртуалізованого відеоспостереження також може створювати покадрові записи протягом тривалих періодів часу. У цій сфері системи віртуалізованого відеоспостереження часто використовуються для будівельної документації великих будівель. Дуже гарні сповільнені записи можна створити майже самостійно. Погодні знімки створюють чудові ефекти.

Система віртуалізованого відеоспостереження гнучко налаштовується щодо кількості підключених камер. Моделі системи віртуалізованого відеоспостереження класифікуються відповідно до кількості ліцензій на камери. Система віртуалізованого відеоспостереження пропонує рішення від 1 до 90 камер. Тут базова версія безкоштовна з безкоштовною камерою та безкоштовна для завантаження та встановлення. Базові моделі варіюються від 3, 6, 9, 12 і 15 моделей камер. Їх можна об'єднати в рішення з 90 камерами за допомогою модуля стекування максимум до 6 систем віртуалізованого відеоспостереження. Ліцензії камери можна гнучко встановити в будь-який час. Можна додавати ліцензії на одну камеру, але через інтерфейс sch рекомендує ліцензувати ліцензії блоками по три. Модуль Stacking з'єднує як фізичні, так і віртуальні сервери відеоспостереження системи віртуалізованого відеоспостереження. Насправді модуль стекування призначений для штабелювання моделей Система віртуалізованого відеоспостереження 15, але через розподіл навантаження він може бути корисним і ефективним для штабелювання менших моделей. Тут також може зіграти роль розподіл живих зображень усіх камер на кількох моніторах. Приклади включають рішення з 24 камерами з двома системами віртуалізованого відеоспостереження 12VM або рішення з 36 камерами з чотирма системами віртуалізованого відеоспостереження 9VM, кожна з яких має розширення через модуль стекування.



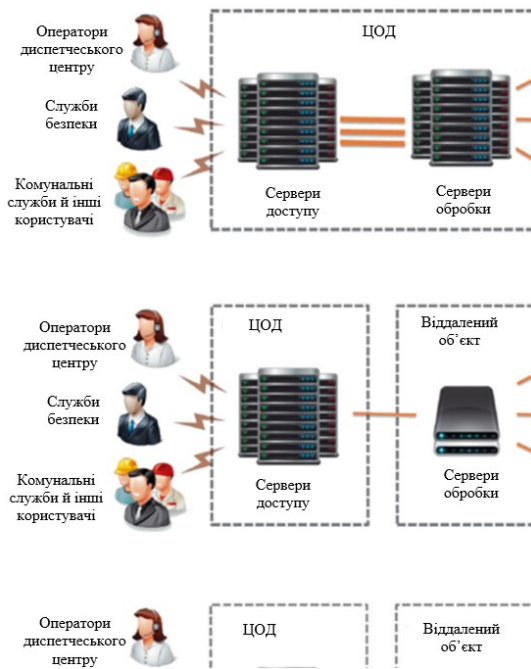


Рисунок 1 – Структурна схема системи

**Висновки.** У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів віртуалізованого відеоспостереження.

Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем віртуалізованого відеоспостереження.
- Досліджена система віртуалізованого відеоспостереження.
- На основі отриманих результатів досліджень створена програмна реалізація системи віртуалізованого відеоспостереження.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання віртуалізованого відеоспостереження. 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. 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.
2. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchov, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
3. 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.
4. Smirnov, O., Neskrodieva, T., Fedorov, E., Rudakov, K., Neskrodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
5. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022.
6. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>
7. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418.
8. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide

- Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) – 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
9. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
  10. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
  11. 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.
  12. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.
  13. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudorandom sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
  14. 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.
  15. 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.
  16. 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.
  17. 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.
  18. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.
  19. Zhurakovskiy, B., Tsopa, N., Batrak, Y., Odarchenko, R., Smirnova, T «Comparative analysis of modern formats of lossy audio compression». Workshop Proceedings, 2020, 2654, стр. 315-327.
  20. Smirnov O. Kuznetsov A., Zaichenko 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.
  21. 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.
  22. 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.
  23. 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.
  24. 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.
  25. 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.
  26. 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.