УДК 004

Д.Ковальов, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ РЕАЛІЗАЦІЇ СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМСТВА

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

мережеве відеоспостереження

Постановка проблеми. Нещодавнє дослідження показало, що інтеграція передової відеоаналітики в системи спостереження може підвищити точність виявлення інцидентів до 30%? Цей значний крок уперед підкреслює вирішальну проблему, з якою стикаються технологічні лідери в різних галузях: інтеграція складних технологій спостереження для посилення безпеки та операційної ефективності без шкоди для конфіденційності чи відповідності вимогам.

Еволюція відеоспостереження від простого заходу безпеки до багатогранного операційного інструменту пропонує численні переваги, але також створює складні виклики. Керівники повинні діяти обережно, балансуючи між впровадженням передових технологій спостереження та етичними міркуваннями та правовими обмеженнями. У цьому блозі буде досліджено нюанси ролі відеоспостереження у підвищенні безпеки, моніторингу продуктивності, забезпеченні відповідності вимогам, покращенні обслуговування клієнтів, управлінні кризами та запобіганні фінансовим втратам. Крім того, ми заглибимося в міркування, необхідні під час вибору обладнання, важливість комплексної стратегії спостереження, необхідність забезпечення конфіденційності даних та життєво важливу роль навчання персоналу служби безпеки.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

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

– Огляд існуючих систем мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

– Дослідження системи мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

– Програмна реалізація системи мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

Об'єктом дослідження є процес мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

Предметом дослідження є методи мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

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

Виклад основного матеріалу. Важливість відеоспостереження в бізнес-середовищі неможливо переоцінити, оскільки воно відіграє вирішальну роль у забезпеченні безпеки, захисту та операційної ефективності організації. Ця технологія еволюціонувала від базових заходів безпеки до складного інструменту, який пропонує безліч переваг у різних аспектах бізнес-операцій. Ось ключові області, які підкреслюють важливість відеоспостереження в бізнес-контексті:

– Підвищення безпеки та захисту – відеоспостереження діє як превентивний захід проти потенційних зловмисників, злодіїв та інших зловмисних осіб, значно знижуючи ризик несанкціонованого доступу та крадіжки. Воно дозволяє здійснювати моніторинг приміщень у режимі реального часу, гарантуючи, що будь-яку підозрілу діяльність можна буде виявити та оперативно усунути. Більше того, у разі невдалого скоєння злочинної діяльності відеозаписи можуть слугувати важливим доказом для допомоги у розслідуваннях та судових процесах.

– Моніторинг та підвищення продуктивності праці – наявність камер спостереження також може позитивно впливати на поведінку працівників, заохочуючи дотримання політик та процедур на робочому місці. Менеджери можуть використовувати відеозаписи для моніторингу робочого процесу, оцінки ефективності персоналу та визначення областей, де можна підвищити ефективність. Такий моніторинг допомагає оптимізувати ресурси та забезпечити ефективний внесок працівників у досягнення цілей організації.

– Забезпечення відповідності вимогам та запобігання відповідальності – Деякі галузі промисловості підпадають під суворі вимоги щодо дотримання нормативних актів, які передбачають моніторинг та запис операцій. Відеоспостереження допомагає забезпечити дотримання підприємствами цих правил, тим самим уникаючи потенційних штрафів та юридичних проблем. Крім того, воно може захистити організацію від неправдивих претензій щодо відповідальності, надаючи незаперечні докази інцидентів, що відбуваються на її території.

– Покращення клієнтського досвіду -Відеоспостереження – це не лише питання безпеки, це також інструмент для покращення обслуговування клієнтів. Аналізуючи відеозаписи, компанії можуть отримати уявлення про поведінку, вподобання та моделі поведінки клієнтів. Цю інформацію можна використовувати для оптимізації планування магазинів, покращення розміщення товарів та покращення загального досвіду клієнтів, що призводить до підвищення задоволеності та лояльності.

– Управління кризовими ситуаціями та реагування на надзвичайні ситуації – у надзвичайних ситуаціях, таких як стихійні лиха, пожежі чи інші кризи, системи відеоспостереження відіграють ключову роль в управлінні кризовими ситуаціями. Вони надають дані в режимі реального часу, які можуть допомогти в оцінці ситуації, координації зусиль з реагування на надзвичайні ситуації та мінімізації збитків. Аналіз відеозаписів після події також може сприяти кращій підготовці до майбутніх інцидентів.

– Економія коштів та запобігання втратам – впровадження комплексної системи відеоспостереження може призвести до значної економії коштів, запобігаючи крадіжкам, зменшуючи страхові внески та мінімізуючи потребу у фізичних заходах безпеки. Вона також

відіграє вирішальну роль у запобіганні втратам, як з точки зору активів, так і інтелектуальної власності, тим самим захищаючи фінансове здоров'я бізнесу.

Впровадження системи відеоспостереження на підприємстві дозволяє здійснювати моніторинг у режимі реального часу, що дає змогу співробітникам служби безпеки оперативно реагувати на будь-які підозрілі дії. Це забезпечує відчуття безпеки та спокою співробітникам, відвідувачам та клієнтам, сприяючи створенню позитивної робочої атмосфери.

Вибір правильного обладнання та технологій для ваших потреб безпеки

Вибір відповідного обладнання та технологій є важливим для успіху системи відеоспостереження на підприємстві. Важливо враховувати такі фактори, як розмір приміщення, необхідний рівень безпеки та конкретні потреби організації.

Оцінка організаційних потреб та цілей безпеки

Першим кроком у виборі правильного обладнання та технологій є визначення конкретних потреб організації. Це включає розуміння основних цілей безпеки, таких як стримування, спостереження в режимі реального часу, розслідування інцидентів або контроль доступу. Кожна ціль може вимагати різних типів технологій та обладнання. Наприклад, стримування може бути досягнуто за допомогою помітно розміщених камер високої роздільної здатності, тоді як розслідування інцидентів може бути корисним для камер, оснащених криміналістичною деталізацією та можливостями масштабування.

Розуміння фізичного середовища

Планування та розмір приміщення відіграють вирішальну роль у визначенні типу та кількості необхідних камер, а також необхідності використання певних функцій, таких як ширококутні об'єктиви або можливості панорамування, нахилу та масштабування (PTZ). Умови низької освітленості можуть вимагати камер з покращеними можливостями нічного бачення, тоді як великі відкриті простори можуть виграти від камер з більшою дальністю дії.

Вибір функцій камери, таких як ширококутні об'єктиви або можливості панорамування, нахилу та масштабування (PTZ), може суттєво вплинути на ефективність системи спостереження. Ширококутні об'єктиви забезпечують ширше поле зору, що полегшує моніторинг великих площ або кількох точок входу. PTZ-камери, з іншого боку, пропонують гнучкість у налаштуванні положення камери та наближенні певних деталей, що покращує здатність системи відстежувати та фіксувати інциденти в режимі реального часу.

Оцінка варіантів технологій та обладнання

Камери – камери високої роздільної здатності необхідні для отримання чітких та детальних зображень, що забезпечують цінні докази у разі інцидентів безпеки. Вибираючи між IP- та аналоговими камерами, організації повинні враховувати такі фактори, як сумісність з мережею, масштабованість та якість зображення. IP-камери пропонують перевагу цифрового підключення, що дозволяє здійснювати віддалений доступ та легко інтегруватися з іншими системами безпеки. З іншого боку, аналогові камери можуть бути більш економічно ефективними для невеликих установок або районів з обмеженою мережевою інфраструктурою.

Окрім роздільної здатності та типу камери, використання розширених функцій, таких як тепловізор, може підвищити ефективність системи спостереження. Тепловізори можуть виявляти теплові сигнатури, забезпечуючи видимість у складних умовах освітлення або в середовищі з димом чи туманом. Завдяки впровадженню технології тепловізійного зображення організації можуть покращити можливості виявлення та забезпечити комплексне охоплення спостереженням, особливо на відкритому повітрі або в зонах високого ризику.

Зрештою, вибір між камерами високої роздільної здатності, IP або аналоговими, та додатковими функціями, такими як тепловізор, має бути адаптований до конкретних вимог безпеки та умов навколишнього середовища організації. Вибравши правильне поєднання обладнання та технологій, підприємства можуть оптимізувати продуктивність своєї системи відеоспостереження та покращити загальні заходи безпеки.

Нічне бачення та виявлення руху: Камери, оснащені технологією нічного бачення, є важливими для зйомки високоякісного відео в умовах слабкого освітлення, гарантуючи, що критичні деталі не будуть пропущені навіть у найтемніших умовах. Ця функція особливо цінна для систем спостереження, яким потрібно підтримувати видимість у нічний час або в місцях з обмеженим освітленням. Крім того, можливості виявлення руху ще більше підвищують ефективність системи, заощаджуючи місце для зберігання. Записуючи лише тоді, коли виявлена активність, мінімізується непотрібний відеоматеріал, що полегшує співробітникам служби безпеки перегляд та аналіз відповідних подій.

Відеоаналітика: Інтеграція програмного забезпечення для відеоаналітики в систему спостереження виходить за рамки пасивного моніторингу, перетворюючи її на активний та інтелектуальний інструмент безпеки. Ця передова технологія може автоматично ідентифікувати та попереджати персонал служби безпеки про підозрілу поведінку, таку як байдикування, несанкціонований доступ або незвичайні рухи, значно підвищуючи загальну ефективність безпеки. Використовуючи можливості штучного інтелекту та машинного навчання, відеоаналітика може надавати аналітику та сповіщення в режимі реального часу, що дозволяє проактивно реагувати на потенційні загрози та інциденти. Ця трансформаційна функція не лише підвищує ефективність зусиль спостереження, але й допомагає оптимізувати розподіл ресурсів та час реагування для більш комплексної стратегії безпеки.

Рішення для зберігання даних

Вибираючи ідеальне рішення для зберігання даних для системи відеоспостереження підприємства, організації повинні ретельно враховувати свої конкретні вимоги до доступності, контролю та безпеки. Вибір між хмарним сховищем та локальними серверами може суттєво вплинути на загальну ефективність та результативність системи спостереження.

Хмарне сховище пропонує неперевершену гнучкість та зручність, дозволяючи співробітникам служби безпеки отримувати доступ до відеоматеріалів з будь-якого місця з підключенням до Інтернету. Така доступність особливо корисна для організацій з кількома об'єктами або для віддалених служб безпеки, яким потрібен доступ до даних спостереження в режимі реального часу. Крім того, хмарні рішення для зберігання даних часто мають вбудовані функції резервування та резервного копіювання, що гарантує безпеку критично важливих відеоматеріалів. З іншого боку, **локальні сервери** надають організаціям підвищений контроль над своїми даними та можуть запропонувати розширені заходи безпеки. Зберігаючи відеозаписи на місці, організації можуть гарантувати, що конфіденційна інформація залишається в їхніх фізичних приміщеннях, зменшуючи ризик несанкціонованого доступу або витоку даних. Хоча локальні сервери можуть вимагати більших початкових інвестицій та постійного обслуговування, вони забезпечують рівень контролю та безпеки, який є важливим для певних галузей та організацій із суворими вимогами до дотримання нормативних вимог. Вибір між хмарним сховищем та локальними серверами має ґрунтуватися на комплексній оцінці потреб організації, бюджетних обмежень та пріоритетів безпеки. Вибравши найбільш підходяще рішення для зберігання даних, організації можуть оптимізувати продуктивність своєї системи відеоспостереження та ефективно захистити свої активи, співробітників та клієнтів.

Підтримка та масштабованість

Забезпечення ефективності системи спостереження з часом вимагає регулярного технічного обслуговування та оновлень. Це включає не лише фізичне очищення та перевірку камер і обладнання, але й оновлення програмного забезпечення для підтримки функцій безпеки в актуальному стані.

Масштабованість має бути ключовим фактором з самого початку. У міру зростання організації система спостереження повинна мати можливість безперешкодно розширюватися. Це може включати додавання більшої кількості камер, модернізацію існуючих або інтеграцію передового аналітичного програмного забезпечення без капітального ремонту всієї системи.

Також важливо вибрати надійні та масштабовані рішення для зберігання відеоматеріалів. Хмарні сховища забезпечують гнучкість та доступність, а локальні сервери пропонують підвищений контроль та безпеку. Регулярне обслуговування та оновлення обладнання й технологій необхідні для забезпечення оптимальної продуктивності та надійності.

Створення успішної системи відеоспостереження для підприємства починається з розробки комплексної стратегії спостереження. Це більше, ніж просто розміщення камер у певних місцях; це вимагає стратегічного підходу до визначення зон та активів, які потребують моніторингу для посилення заходів безпеки. Ретельно оцінюючи приміщення, включаючи виявлення сліпих зон та вразливостей, організації можуть забезпечити надійність та ефективність своєї системи спостереження.

Окрім фізичного розміщення камер, встановлення чітких політик та процедур має вирішальне значення для безперебійної роботи системи спостереження. Це включає визначення ролей та обов'язків, встановлення інструкцій щодо доступу та управління відеоматеріалами, а також розробку протоколів реагування на інциденти безпеки. Наявність цих політик гарантує, що стратегія спостереження буде не тільки ефективною, але й відповідатиме правовим та нормативним вимогам.

По суті, добре розроблена стратегія спостереження служить проактивним заходом для захисту активів, співробітників та клієнтів організації. Вона формує міцну основу для моніторингу та реагування на загрози безпеці, підвищуючи загальну безпеку та душевний спокій. Інтегруючи технології спостереження з комплексною стратегією, організації можуть максимізувати переваги своєї системи відеоспостереження та створити безпечне середовище для всіх зацікавлених сторін.

Забезпечення конфіденційності даних та відповідності вимогам

Конфіденційність даних та дотримання вимог є вирішальними міркуваннями під час впровадження системи відеоспостереження на підприємстві. Оскільки організації використовують можливості технологій спостереження для посилення заходів безпеки, вони також повинні пріоритезувати захист прав осіб на конфіденційність та забезпечувати дотримання правових та нормативних актів.

Асоціація індустрії безпеки наголошує на важливості проведення оцінки впливу на конфіденційність (ОВК) на етапі проектування та планування систем спостереження. ОВК може виявити потенційні проблеми конфіденційності на ранній стадії, такі як зони спостереження з камер та використання аналітичного програмного забезпечення. Також важливо встановити налаштування конфіденційності за замовчуванням, безпечні конфігурації мережі та визначити ролі та обов'язки щодо конфіденційності та кібербезпеки.

Під час розгортання системи відеоспостереження організації повинні ретельно орієнтуватися в динамічному середовищі законів і норм щодо конфіденційності даних. Це включає дотримання правил, що регулюють збір, зберігання та використання відеоматеріалів, а також повагу до прав осіб на конфіденційність та захист даних. Дотримуючись цих стандартів, організації можуть побудувати довіру зі співробітниками, клієнтами та іншими зацікавленими сторонами, одночасно зменшуючи ризики потенційних юридичних наслідків.

Крім того, для організацій важливо запровадити надійні та комплексні практики управління даними для захисту цілісності та конфіденційності відеозаписів. Це включає впровадження безпечних рішень для зберігання даних, протоколів шифрування, засобів контролю доступу та політик зберігання даних для запобігання несанкціонованому доступу або зловживанню конфіденційною інформацією. Завдяки проактивному вирішенню проблем конфіденційності даних, таких як Загальний регламент про захист даних (GDPR) або галузеві рекомендації, організації можуть дотримуватися етичних стандартів та захищати права осіб, записаних камерами спостереження.

Навчання та моніторинг персоналу служби безпеки з використання систем відеоспостереження

Навчання та моніторинг персоналу служби безпеки є важливими практиками для забезпечення ефективної роботи системи відеоспостереження підприємства. Важливість комплексного навчання персоналу служби безпеки неможливо переоцінити, оскільки це не лише підвищує їхню кваліфікацію та авторитет, але й відіграє значну роль у мінімізації відповідальності та підвищенні загальної безпеки організації. Належним чином навчений персонал служби безпеки краще оснащений для вирішення різних ситуацій, що позитивно відображається на його професіоналізмі та відданості організації питанням безпеки. Такі програми, як ті, що пропонуються Міжнародним фондом співробітників служби безпеки (IFPO), охоплюють широкий спектр тем, важливих для співробітників служби безпеки, включаючи фізичну безпеку, процедури дій у надзвичайних ситуаціях, правові аспекти тощо, гарантуючи, що співробітники добре підготовлені до виконання своїх обов'язків.

Більше того, Бюро статистики праці США підкреслює різноманітні ролі та обов'язки охоронців та співробітників служби спостереження за азартними іграми, наголошуючи на необхідності ретельного навчання та набуття спеціальних навичок для ефективного виконання своїх обов'язків. Навчальні заняття повинні бути зосереджені на ознайомленні персоналу служби безпеки з різними функціями та можливостями системи спостереження, включаючи те, як керувати камерами, отримувати доступ до записів та реагувати на інциденти безпеки. Крім того, персонал слід навчити найкращим практикам обслуговування системи, таким як регулярні перевірки несправностей камер та забезпечення безпеки даних.

Надаючи пріоритет навчанню та моніторингу персоналу служби безпеки, організації можуть забезпечити ефективне та відповідальне використання своїх систем спостереження, сприяючи безпеці своїх приміщень, а також дотримуючись правил конфіденційності та відповідності.

Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

– Досліджена система мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. Розроблені алгоритми дозволяють успішно вирішувати завдання мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. 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., 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.
2. 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.
3. 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.
4. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, 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 pseudo-random 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. Zhurakovskyi, 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., 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.
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.
27. 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.
28. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New Technique for Hiding Data in Cover Images Using Adaptively Generated Pseudorandom Sequences». CEUR Workshop Proceedings Volume 2732, 2020, Pages 214-227.
29. Т.В. Смірнова, О.М. Дрєєв, О.А. Смірнов «Хмарна інформаційна система оцінювання шорсткості з використанням дискретного частотного аналізу макрофотографій». IV міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології”, м. Кропивницький. 15-16 квітня 2021р. – Кропивницький: ЦНТУ. – 2021. – С. 30.
30. 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.
31. 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.
32. Смірнов О.А., Дрєєва Г.М., Дрєєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральноукраїнський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.
33. О. Смірнов, Є. Деменко, О. Онікійчук, А. Арищенко, Л. Горбачова, «Формування псевдовипадкових послідовностей для приховування даних в зображеннях» Комп’ютерні науки та кібербезпека. № 4. С. 30-37. 2019.