УДК 004

С.Олексієнко, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КОМПЛЕКСНИХ ІНТЕЛЕКТУАЛЬНИХ РІШЕНЬ ДЛЯ ВІДЕОНАГЛЯДУ

У статті розроблено програмне забезпечення, яке призначено для системи комплексних інтелектуальних рішень для відеонагляду. Метою розробки є дослідження та принципи побудови системи комплексних інтелектуальних рішень для відеонагляду. Об’єктом дослідження є процес комплексних інтелектуальних рішень для відеонагляду. Предметом дослідження є методи комплексних інтелектуальних рішень для відеонагляду. Методи дослідження базуються на методах розпізнавання образів, методах великих даних, методах комп’ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи комплексних інтелектуальних рішень для відеонагляду. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

інтелектуальне рішення, відеонагляд

Постановка проблеми. У кожній галузі платформи відеоспостереження стали важливими інструментами для забезпечення безпеки, моніторингу активів та підвищення операційної ефективності. Нещодавні технологічні досягнення збільшили попит на інтелектуальні, масштабовані та хмарні рішення для спостереження. Багато організацій зараз переходять на платформи на базі штучного інтелекту, які пропонують розширені можливості, такі як розпізнавання облич, виявлення об'єктів та складна аналітика даних. Новіші системи покращують виявлення загроз, прискорюють час реагування та мінімізують людські помилки завдяки автоматизації. Вибір нової платформи відеоспостереження являє собою значну інвестицію, яка має наслідки для організаційної безпеки та бізнес-аналітики. Індустрія відеоспостереження постійно розвивається, а штучний інтелект та хмарні обчислення відіграють вирішальну роль у сучасних рішеннях безпеки. Незалежно від того, чи шукаєте ви повністю хмарну систему на базі штучного інтелекту, чи простіше локальне рішення, варіанти відеонагляду задовольнять будь-які потреби безпеки. Вибір правильної платформи залежить від ваших конкретних вимог, бюджету та рівня інтеграції, який ви шукаєте для своєї інфраструктури спостереження.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи комплексних інтелектуальних рішень для відеонагляду.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи комплексних інтелектуальних рішень для відеонагляду.

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

– Огляд існуючих систем комплексних інтелектуальних рішень для відеонагляду.

– Дослідження системи комплексних інтелектуальних рішень для відеонагляду.

– Програмна реалізація системи комплексних інтелектуальних рішень для відеонагляду.

Об’єктом дослідження є процес комплексних інтелектуальних рішень для відеонагляду.

Предметом дослідження є методи комплексних інтелектуальних рішень для відеонагляду.

Методи дослідження базуються на методах розпізнавання образів, методах великих даних, методах комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Більшість систем безпеки містять камери відеоспостереження, які допомагають службам безпеки виявляти потенційні загрози. Однак, чим більшою та складнішою стає установка, тим складніше може бути забезпечити належне спостереження за всіма активними камерами та потоками спостереження.

З появою інтелектуальних технологій, таких як штучний інтелект та машинне навчання, сучасні системи спостереження можна запрограмувати на автоматичне виявлення аномальних подій та сигналів безпеки, що допомагає командам зосередити свої зусилля на подіях, що розгортаються, та питаннях негайної важливості.

Це основна передумова відеоаналітики. Ця передова технологія може самостійно аналізувати відеоконтент та отримувати з нього корисну інформацію для покращення прийняття рішень та підвищення ефективності реагування систем безпеки. Щоб дізнатися більше про практичні можливості аналітики відеоспостереження, нижче наведено повний посібник із застосування, можливостей та варіантів використання відеоаналітики.

Відеоаналітика – це передова технологія, яка автоматично аналізує контент, записаний відеокамерами. Інтелектуальні алгоритми обробляють відеодані в режимі реального часу, щоб генерувати інформацію про те, що відбувається, у серії зображень. Відеоаналітика для безпеки зазвичай використовується для виявлення та отримання інформації про рух об'єктів, людей та транспортних засобів на записах відеоспостереження .

Системи відеоаналітики спостереження пропонують більш практичний та ефективний спосіб перегляду та спостереження за записами з камер спостереження. Контент, знятий кількома камерами протягом кількох днів, може бути автоматично сортований за інтересами, допомагаючи співробітникам служби безпеки виявляти підозрілу активність та належним чином реагувати на неї в режимі реального часу та під час розслідувань.

Системи відеоаналітики обробляють відеопотоки за допомогою алгоритмів, розроблених для виявлення певних подразників. Захоплені зображення послідовно переглядаються спеціалізованими програмними інструментами, запрограмованими на перевірку певних подій або об'єктів, які можуть становити загрозу безпеці.

У простому сенсі, відеоаналітика шукає аномальні відмінності в послідовності зображень, а потім генерує дані про ці події за допомогою алгоритмів на основі правил. Наприклад, якщо відеокамера фіксує об'єкт, що рухається в її полі зору, відеоаналітика ставитиме запитання, щоб допомогти визначити об'єкт і вирішити, чи заслуговує його присутність на подальші дії.

Під поняттям відеоаналітики слід розуміти два основні типи систем:

– Традиційна відеоаналітика: Базові системи використовують алгоритми на основі правил для аналізу відеоконтенту. Якщо щось у серії зображень змінюється, програмне забезпечення задасть низку запитань типу «*якщо/тоді*», щоб звузити коло можливої зміни. Однак традиційні системи аналітики не можуть зберігати інформацію або навчатися на основі раніше зареєстрованих інцидентів.

– Відеоаналітика на основі штучного інтелекту: Відеоаналітика на основі штучного інтелекту також використовує процес на основі правил для отримання інформації про зображення. Однак їхні алгоритми використовують інструменти штучного інтелекту та машинного навчання, щоб навчатися на основі ширших даних. Простіше кажучи, глибоке навчання у відеоаналітиці дозволяє системам вивчати закономірності з історичних подій для підвищення точності виявлення.

Поширені типи відеоаналітики в системах відеоспостереження

Відеоаналітика в режимі реального часу дозволяє службам безпеки виявляти закономірності, аномальні події та підозрілу активність, які в іншому випадку могли б залишитися непоміченими. Камери відеоаналітики забезпечують постійне спостереження за

ключовими зонами, а різні алгоритми відеоаналітики спеціально розроблені для пошуку певних подразників. Нижче наведено деякі поширені типи аналітики.

Автоматичне розпізнавання номерних знаків (ALPR)

Камери ALPR використовують спеціальний тип відеоаналітики, який називається оптичним розпізнаванням символів (OCR), для зчитування інформації про номерні знаки транспортних засобів, що проїжджають повз. Технологію ALPR можна використовувати для підтримки операцій управління паркуванням та контролю доступу транспортних засобів, а також для спостереження за під'їзними дорогами та паркувальними зонами, щоб виявити наявність підозрілих транспортних засобів.

Виявлення натовпу

Алгоритми відеоаналітики, що використовуються для виявлення натовпу, запрограмовані на ідентифікацію людей та вимірювання щільності натовпу в полі зору камери. Аналітика виявлення натовпу використовується для підвищення безпеки на живих заходах, попередження команд про потенційні вузькі місця та порушення, які можуть потребувати додаткової уваги, а також для відстеження рівня заповненості та виявлення незвичайної активності.

Розпізнавання обличчя

Розпізнавання облич використовується для ідентифікації присутності людських облич у відеоконтенті, а також для порівняння облич з тими, що зберігаються в базах даних. Цей тип відеоаналітики може контролювати доступ до безпечних місць та покращувати безпеку периметра, попереджаючи команди про присутність відомих правопорушників та сторонніх осіб, які перебувають навколо приватних володінь.

Підрахунок людей

Системи відстеження людей аналізують різні типи біометричних показників, щоб краще зрозуміти дії людей у цільових зонах. Завдяки розпізнаванню облич, виявленню руху та поведінкових характеристик ці системи можуть ідентифікувати осіб та стежити за ними в приміщеннях, щоб покращити методи виявлення вторгнень та управління зайнятістю.

Відстеження об'єктів

Відеоаналітика для відстеження об'єктів контролює наявність та рух певних предметів у полі зору камери. Алгоритми можна налаштувати відповідно до різних випадків використання відеоаналітики. Наприклад, камери можуть бути запрограмовані для моніторингу посилок під час їхнього переміщення через пункти доставки та виконання замовлень або використовуватися для відстеження автомобілів для підтримки операцій з контролю дорожнього руху.

Виявлення руху

Алгоритми відеоаналітики, оптимізовані для виявлення руху, запрограмовані на безперервний пошук ознак руху в заданій області. Для цієї мети зазвичай використовується аналітика відеоспостереження з машинним навчанням. Системи можна навчити розуміти, як простори використовуються за нормальних умов, тому вони попереджають охоронців лише про рухи, які можуть становити проблему.

Виявлення предметів без нагляду

Системи відеоаналітики можна запрограмувати на моніторинг появи та руху статичних об'єктів у визначеному місці. Ці рішення добре впроваджуються в громадських місцях, таких як торгові центри, розважальні заклади та транспортні вузли, щоб допомогти співробітникам служби безпеки виявляти потенційні бомби та забезпечувати вільні аварійні виходи від перешкод.

Моніторинг зайнятості

Інструменти моніторингу заповнюваності підраховують кількість людей, які проходять через заздалегідь визначену зону протягом встановленого періоду часу. Цю технологію можна використовувати для забезпечення підтримки безпечного рівня заповнюваності та для збору даних про те, як використовуються приміщення. Наприклад, у

роздрібній торгівлі її можна використовувати для визначення того, коли послуги є найбільш популярними, та для вимірювання ефективності організаційних планів.

Переваги технології відеоаналітики

Вибір розробки та впровадження індивідуальних рішень для відеоаналітики може надати бізнесу та фахівцям з безпеки кілька суттєвих переваг. Завдяки інтелектуальному програмному забезпеченню, яке використовується для ефективного управління та отримання аналітичних даних з величезних обсягів, команди людей можуть покращити виконання ключових завдань, автоматично виділяючи високоякісну та релевантну аналітику.

1. Підвищена ефективність

Типова система безпеки містить багато IP-камер та моніторів, розташованих для охоплення ключових зон. Навіть найменша зміна в сигналі безпеки може свідчити про загрозу, що розгортається, але командам може бути важко ефективно спостерігати за всіма камерами безперервно.

Системи відеоаналітики безпеки можна навчити автоматично виявляти аномальні події та попереджати операторів про них, надсилаючи інформацію персоналу диспетчерської відеоспостереження та персоналу на місці через SMS або електронну пошту. Це допомагає забезпечити доведення до відома відповідного персоналу всіх підозрілих дій, а високоякісні записи подій миттєво генеруються для покращення розслідувань.

2. Покращене прийняття рішень

Поряд з виявленням аномальних подій, які можуть вимагати подальшого розслідування, системи відеоаналітики можуть розпізнати тип інциденту, який може розгорнутися. Завдяки ключовим типам відеоаналітики, таким як інструменти відстеження об'єктів та розпізнавання облич, персонал може бути попереджений про наявність вогнепальної зброї, сторонніх осіб або скупчення людей, що сприятиме обґрунтованому реагуванню на інциденти.

3. Зменшення кількості хибних тривог

Хоча традиційні системи безпеки можуть бути ефективними засобами стримування злочинів, оператори або центральні станції моніторингу повинні проводити додатковий аналіз, щоб зрозуміти причини активації. За оцінками, від 95% до 98% спрацьованих сигналів тривоги про крадіжку, паніку та пограбування є хибнопозитивними, що потенційно призводить до втрати часу та ресурсів, що може зробити організації вразливими до ширших ризиків.

Оскільки системи відеоаналітики безпеки розроблені для ідентифікації та розуміння конкретних подразників в унікальних умовах їхнього конкретного середовища, ризик хибних тривог можна суттєво зменшити. Це дозволяє персоналу швидко реагувати на ризики та скорочує час, витрачений на аналіз даних фізичної безпеки, щоб персонал міг зосередитися на важливих завданнях.

4. Потенційна економія коштів

Хоча початкові витрати на розробку систем відеоаналітики можуть бути високими, компанії, які впроваджують ці інструменти, можуть отримати довгострокову економію коштів. Перш за все, підвищена точність систем безпеки відеоаналітики може допомогти обмежити фінансовий вплив таких подій, як крадіжка та пошкодження майна, а додаткові переваги можна знайти в організаційних покращеннях.

Для аналізу, організації та реагування на дані безпеки знадобиться менше часу та ресурсів, що дозволить організаціям підвищити ефективність моніторингу відеоспостереження та процесів розслідування. Рішення для відеоаналітики також можуть бути впроваджені для спостереження за тим, як співробітники та гості взаємодіють з фізичними активами та інфраструктурою, допомагаючи підприємствам покращувати послуги та відповідати очікуванням клієнтів.

5. Постійні вдосконалення

Дані, зібрані та проаналізовані інструментами відеоаналітики, можна використовувати для постійного вдосконалення ширших аспектів діяльності бізнесу. Наприклад,

відеоаналітика в поєднанні з камерами зі штучним інтелектом може допомогти фахівцям зрозуміти типи загроз, до яких їхні організації найбільш вразливі, впливаючи на майбутні рішення щодо вдосконалення систем безпеки та внутрішніх політик.

Подібні принципи можна застосовувати до інших застосувань відеоаналітики. Системи, розгорнуті для спостереження за виробничими завданнями, можуть надавати інформацію щодо покращення виробництва. Аналітика ALPR може допомогти командам покращити операції з управління паркуванням, а поведінкова аналітика може сприяти покращенню обслуговування клієнтів у роздрібній торгівлі та готельному бізнесі.

Міркування щодо впровадження систем відеоаналітики

Системи безпеки відеоаналітики та управління бізнесом можуть забезпечити вимірні переваги лише за умови адаптації до унікальних потреб організації. Розробляючи індивідуальні рішення для відеоаналітики, власники бізнесу повинні враховувати такі фактори:

– Обробка: Аналітичне програмне забезпечення може обробляти дані на центральному сервері або на найближчому пристрої. Старіші камери зазвичай потребують серверних систем, які часто страждають від затримки під час обробки аналітики. Для порівняння, новіші IP- камери можуть використовувати периферійну аналітику для обробки даних та отримання аналітики про сам пристрій у режимі реального часу.

– Точність виявлення: Відеоаналітика з використанням машинного навчання та функцій штучного інтелекту може бути використана для розробки високоточних систем. Програмне забезпечення можна навчити розуміти нормальні умови роботи цільових зон та попереджати персонал про аномальні події.

– Масштабованість: Потреби в безпеці можуть змінюватися з часом, тому вкрай важливо вибрати рішення, яке можна масштабувати за потреби. Подумайте, наскільки легко та економічно ефективно може бути додавання нового обладнання та програмних функцій відеоаналітики до запропонованих інсталяцій.

– Можливості інтеграції: Аналітичні дані, отримані за допомогою інструментів відеоаналітики, можна використовувати для оптимізації роботи ширших систем безпеки. Перевірте, чи підтримують потрібні рішення конфігурації відкритого API та чи сумісні вони з існуючими пристроями безпеки для бізнесу.

Майбутні тенденції у відеоаналітиці

Зростаючий інтерес до технологій на основі штучного інтелекту призвів до збільшення впровадження штучного інтелекту в різних бізнес-секторах, причому з 2022 року цілих 72 % організацій впроваджують штучний інтелект для виконання принаймні однієї бізнес-функції. Оскільки штучний інтелект та алгоритми глибокого навчання стають дедалі більш досконалими, все більше галузей готові отримати вигоду від інтелектуальних систем відеоаналітики.

Відеоаналітика на основі штучного інтелекту зараз є звичайним явищем у сучасних розумних містах та технологіях розумних будівель, а інструменти використовуються не лише для покращення безпеки, але й для підвищення енергоефективності, моніторингу навколишнього середовища та забезпечення належного обслуговування інфраструктури. Відеоаналітика, пов'язана з промисловим Інтернетом речей (IIoT), допомагає фахівцям виконувати ці завдання, дозволяючи автономно коригувати фізичну інфраструктуру у відповідь на високоякісні дані.

Інтерес до нових технологій штучного інтелекту, таких як відеоаналітика, поширюється також на малий бізнес та додатки, а дослідження, опубліковане у 2024 році, показало, що 98% малих підприємств зараз використовують інструменти на базі штучного інтелекту. Оскільки програмне забезпечення для відеоаналітики стає більш доступним та зручним у використанні, його впровадження в усіх галузях промисловості та середовищах, ймовірно, продовжуватиме зростати.

Відеоаналітика в режимі реального часу надає численні суттєві переваги підприємствам у більшості основних секторів, дозволяючи фахівцям отримувати практичну інформацію про важливі процеси безпеки, інфраструктури та організації. Використовуючи унікальні системи відеоаналітики, команди можуть покращити реагування на безпеку, отримати інформацію про бізнес-операції та допомогти працівникам-людям виконувати завдання безпечно та ефективно, що може бути корисним для сучасних підприємств будь-якого розміру.

Мережевий відеореєстратор (NVR) – це спеціалізований комп'ютер, який записує відео з камер безпеки в цифровому форматі на жорсткий диск. Оскільки NVR не має можливості відеозахоплення, відео зазвичай обробляється та кодується з IP-камери спостереження або камери CCTV і передається на NVR для зберігання через мережу Ethernet або Wi-Fi. NVR зазвичай використовуються в системах IP-відеоспостереження.

Мережеві відеореєстратори замінили застарілі цифрові відеореєстратори (DVR). Переваги включають:

- Запис відео та аудіо.
- Краща якість зображення.
- Гнучкість системи.
- Краще покриття огляду.
- Дротове або бездротове.
- Потрібен 1 кабель для відео, аудіо та живлення.
- Розпізнавання облич, номерних знаків тощо завдяки кращій якості зображення.

Функції мережевого відеореєстратора (NVR)

Функції NVR можуть включати:

- Відеоаналітику.
- Параметри режиму запису.
- Мережеві комутатори з живленням через Ethernet (PoE).
- Керування PTZ-камерою.
- Дистанційне налаштування.
- Тригери запису.
- Схеми стиснення відео.

Порівняння цифрових відеореєстраторів та мережевих відеореєстраторів

Цифровий відеореєстратор (DVR) записує відеозаписи з камер спостереження на локальні пристрої зберігання даних, найчастіше на жорсткий диск. DVR може записувати відео з аналогових джерел на місці або захоплювати відео з цифрового джерела. DVR можна підключити до аналогових камер за допомогою коаксіальних кабелів, що дозволяє отримати до них віддалений доступ. DVR пропонують розширені функції, такі як можливість пошуку записів за подіями або сортування за часом і датою. DVR можна налаштувати на автоматичну заміну старих записів після заповнення сховища.

Кожній камері безпеки потрібен центральний відеореєстратор для передачі та архівування записаного матеріалу. Відеомагнітофони еволюціонували в моделі DVR, які потім були замінені технологією NVR, що дозволяє контролювати необмежену кількість камер, як в одному місці, так і по всьому світу.

Результати порівняння між відеореєстраторами та мережевими відеореєстраторами:

– Роздільна здатність записів. Відеореєстратори можуть записувати лише з роздільною здатністю 720p. З іншого боку, відеореєстратори пропонують можливості запису високої чіткості 1080p та неймовірну чіткість зображення. D1 – це стандартна якість відео, що використовується системами відеоспостереження замкнутого контуру, тоді як HD пропонує набагато чіткіше зображення з роздільною здатністю 1920×1080 пікселів деталізації.

– Підключення камери. Підключення аналогових систем відеоспостереження є досить складним, оскільки вони вимагають BNC-роз'ємів для кожної камери, підключеної до одного

пристрою, що означає прокладання великої кількості проводів між пристроями (або використання PoE). Це також обмежує кількість камер, які ви можете мати одночасно, перш ніж знадобиться ще один пристрій.

Відеореєстратори (NVR) – це сучасний погляд на цифровий відеореєстратор (DVR), який вирішує багато його проблем. NVR усуває ці проблеми, оскільки він підключений безпосередньо до однієї мережі, тоді як IP-камери передають свої кадри через інше з'єднання. Це робить масштабування NVR набагато доступнішим, ніж у випадку з системою DVR, яка вимагає складніших оновлень обладнання та процесів встановлення, щоб нові системи належним чином працювали разом.

Відеонаглядові відеореєстратори (NVR) – це найпоширеніший спосіб зберігання та доступу до відео з IP-камер. Моделі з підтримкою Wi-Fi можуть передавати відео бездротовим способом без обмежень щодо близькості, якщо вони знаходяться в одній мережі. Однак, перед покупкою обладнання важливо знати про проблеми сумісності.

Гібридні відеореєстратори

Гібридні відеореєстратори (HVR) – це новітня технологія відеоспостереження. Вони можуть працювати як з аналоговими камерами, так і з IP-камерами, що дає їм перевагу над традиційними системами. Ця універсальність заощадить ваші кошти, коли справа доходить до купівлі нового обладнання.

Результати порівняння між відеореєстраторами та мережевими відеореєстраторами:

Підключення камери:

– Відеонаглядові відеореєстратори (NVR) – це найпоширеніший спосіб зберігання та доступу до відеозаписів з IP-камер.

– NVR набагато масштабованіші, ніж DVR.

Роздільна здатність записів:

– Відеореєстратори можуть записувати лише з роздільною здатністю 720p. З іншого боку, відеореєстратори пропонують можливості запису високої чіткості 1080p та неймовірну чіткість зображення.

Гібридні відеореєстратори

– Може працювати як з аналоговими камерами, так і з IP-камерами.

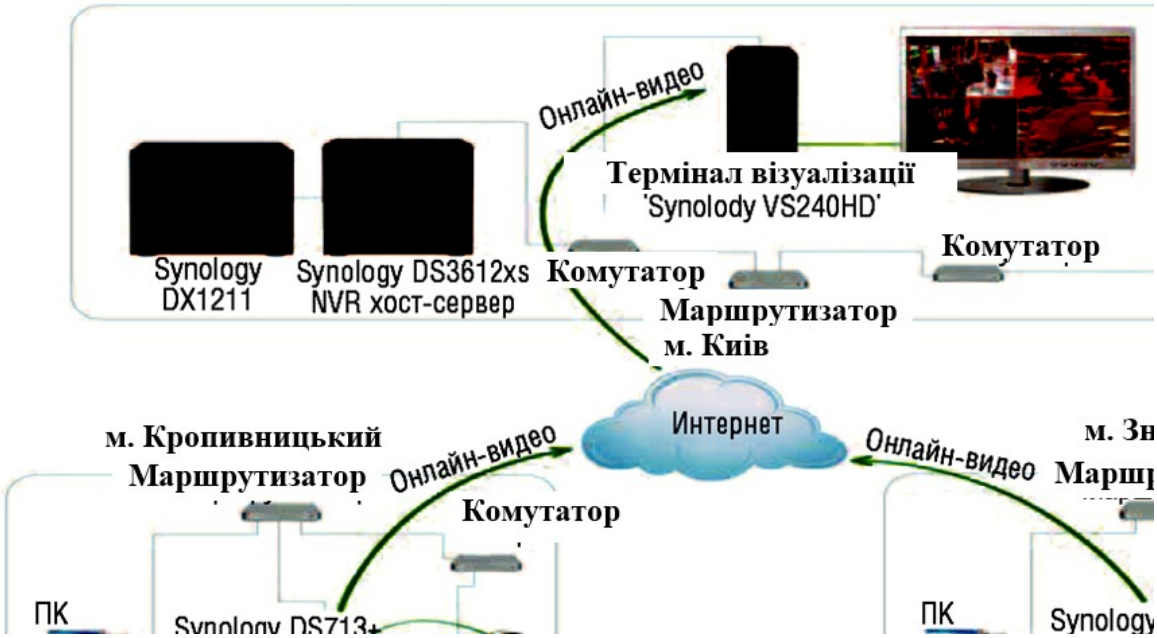

Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів комплексних інтелектуальних рішень для відеонагляду. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем комплексних інтелектуальних рішень для відеонагляду.

– Досліджена система комплексних інтелектуальних рішень для відеонагляду.

– На основі отриманих результатів досліджень створена програмна реалізація системи комплексних інтелектуальних рішень для відеонагляду.

Розроблені алгоритми дозволяють успішно вирішувати завдання комплексних інтелектуальних рішень для відеонагляду. 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., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
2. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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,
10. 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.
11. 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
12. 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.
13. 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.
14. 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.
15. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.