УДК 004

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

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО ВІДЕОСПОСТЕРЕЖЕННЯ НА ОСНОВІ ВИКОРИСТАННЯ DIRECTX

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

мережеве відеоспостереження, DirectX

Постановка проблеми. Система відеоспостереження забезпечує цілодобовий моніторинг, запобігання злочинам та збір доказів. З огляду на те, що світовий ринок, за прогнозами, досягне 147,04 мільярда доларів до 2030 року, ці системи мають вирішальне значення для захисту співробітників, активів та майна.

Основні компоненти системи відеоспостереження:

- Камери: Запис відео високої чіткості.
- Пристрій запису: Зберігає відео локально (NVR/DVR) або в хмарі.
- Монітор/дисплей: Перегляд відео в реальному часі та записаного відео.
- Мережеве підключення: Забезпечує віддалений доступ.
- Рішення для зберігання даних: керує збереженням відео.

Сучасні системи пропонують розширені функції, такі як виявлення на базі штучного інтелекту, розпізнавання облич та розпізнавання номерних знаків, часто інтегруючись із системами контролю доступу для надсилання сповіщень у режимі реального часу. Технологія вийшла за рамки простого запису та використовує аналіз закономірностей та виявлення аномалій, змінюючи безпеку з реактивної на проактивну.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевого відеоспостереження на основі використання directx.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевого відеоспостереження на основі використання DirectX.

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

– Огляд існуючих систем мережевого відеоспостереження на основі використання DirectX.

– Дослідження системи мережевого відеоспостереження на основі використання DirectX.

– Програмна реалізація системи мережевого відеоспостереження на основі використання DirectX.

Об'єктом дослідження є процес мережевого відеоспостереження на основі використання DirectX.

Предметом дослідження є методи мережевого відеоспостереження на основі використання DirectX.

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

Виклад основного матеріалу. Системи відеоспостереження важливі для забезпечення безпеки в різних місцях. Вони допомагають, показуючи відео в реальному часі та покращуючи безпеку. Нові технології змінили принципи роботи цих систем, зробивши їх швидшими та розумнішими. Очікується, що ринок відеоспостереження значно зросте. До 2030 року він може коштувати 88,71 мільярда доларів. Такі круті ідеї, як інструменти штучного інтелекту, блокчейн та чітке зображення, перетворюють старі системи на розумніші.

Системи спостереження на базі штучного інтелекту та інтелектуальні технології

Краще виявлення та розпізнавання об'єктів

Швидке виявлення загроз

Системи на базі штучного інтелекту одразу перевіряють відеопотоки. Розумні програми виявляють небезпеки в міру їх виникнення. Швидкі перевірки допомагають у ризикованих місцях. Служби безпеки діють швидше під час надзвичайних ситуацій. Інструменти штучного інтелекту помічають невеликі проблеми, які люди можуть пропустити. Дослідження мереж реального часу показує, що штучний інтелект економить час у складних ситуаціях.

Спостереження за моделями поведінки

Інструменти штучного інтелекту спостерігають за тим, як люди поводяться в певних місцях. Вони вивчають звичайні дії та виявляють дивні. Це допомагає зупинити проблеми, перш ніж вони погіршаться. Журнал «Campus Safety» стверджує, що системи штучного інтелекту чудово справляються з вивченням поведінки. Спостереження за закономірностями означає меншу потребу в нагляді за людьми, що спрощує роботу.

Розумні прогнози для безпечніших місць

Менше хибних тривог

Системи штучного інтелекту зменшують кількість хибних тривог. Вони розрізняють реальні небезпеки від нешкідливих подій. Це робить роботу служби безпеки більш плавною та з меншою кількістю перерв. Дослідження Bokysee показують, що штучний інтелект значно зменшує кількість хибних тривог. Краща точність допомагає командам безпеки використовувати свій час розумно.

Раннє усунення проблем

Інструменти штучного інтелекту прогнозують ризики до того, як вони стануться. Вони вивчають старі дані, щоб побачити майбутні проблеми. Це допомагає виправити слабкі місця до того, як почнуться проблеми. Ринки та дослідження ринків показують, що штучний інтелект дає поради в режимі реального часу, щоб команди не просто реагували. Прогнозування проблем підвищує безпеку загалом.

Хмарне відеоспостереження та гібридні рішення

Переваги хмарного сховища

Легко вирощувати та економити гроші

Хмарні відеосистеми легко розширювати за потреби. Бізнес може додавати більше сховища, не купуючи нове обладнання. Вони можуть змінювати розмір сховища залежно від того, що їм потрібно на даний момент. Це допомагає заощаджувати гроші та розумно використовувати ресурси. VSaaS пропонує доступні варіанти як для малих, так і для великих компаній. Збільшення або зменшення обсягу сховища дозволяє контролювати витрати.

Дивіться та керуйте з будь-якого місця

Хмарні системи дозволяють перевіряти камери з будь-якого місця. Служби безпеки можуть переглядати відео в реальному часі або збережені відео онлайн. Керування багатьма локаціями стало простіше за допомогою однієї системи. Хмарні інструменти швидко надсилають сповіщення, допомагаючи під час надзвичайних ситуацій. Віддалене спостереження спрощує роботу та забезпечує безперебійний режим.

Збереження безпеки та конфіденційності даних

Надійний захист даних

Спеціальні інструменти захищають дані, що зберігаються в хмарі, від хакерів. Зашифровані дані запобігають доступу інших до конфіденційної інформації. Рівні захисту забезпечують безпеку відео під час надсилання або зберігання. Хмарні компанії використовують надійні засоби безпеки, щоб запобігти витоку даних. Шифрування забезпечує безпеку та конфіденційність відеоданих.

Дотримання правил у всьому світі

Хмарні системи допомагають дотримуватися глобальних правил безпеки даних. Такі правила, як GDPR та CCPA, гарантують правильне оброблення даних. Хмарні інструменти допомагають керувати тим, хто може переглядати або зберігати дані. Дотримання правил зміцнює довіру та уникає юридичних проблем. Дотримання цих стандартів робить системи безпечнішими загалом.

Інтеграція Інтернету речей та смарт-пристроїв у системи відеоспостереження

Розумні пристрої та підключення

Роль датчиків Інтернету речей

Датчики Інтернету речей збирають дані з навколишнього середовища та діляться ними. Вони перевіряють такі речі, як рух, звук і температура. Це покращує роботу систем спостереження. Камери та датчики разом швидко виявляють дивну активність. Ці датчики допомагають у небезпечних зонах, надаючи більше деталей. Системи безпеки використовують їх для швидкого реагування під час надзвичайних ситуацій.

Безшовна інтеграція з розумними містами

Розумні міста використовують інструменти Інтернету речей (IoT) для кращого управління. Камери та датчики вивчають дорожній рух, щоб покращити час сигналізації. Вони також стежать за натовпами, щоб запобігти переповненню в людних місцях. IoT підключає сигналізацію, камери та вуличні ліхтарі для забезпечення безпеки. Міські планувальники покладаються на ці системи для забезпечення безпеки територій.

Проблеми інтеграції Інтернету речей

Вразливості мережі

Пристрої Інтернету речей можуть бути атаковані через слабкі мережі. Поганий рівень безпеки дозволяє хакерам переглядати приватні відеодані. Хакери знаходять прогалини в незахищених системах Інтернету речей. Брандмауери та сповіщення допомагають блокувати ці ризики. Оновлення пристроїв часто захищає їх від нових загроз.

Проблеми сумісності

Різні бренди виготовляють пристрої Інтернету речей з унікальним дизайном. Це спричиняє проблеми під час їх підключення в одній системі. Пристрої можуть погано працювати разом через різні правила. Розробники створюють інструменти для виправлення цих проблем з’єднання. Стандартні правила спрощують підключення пристроїв для великих проектів.

Досягнення в технологіях камер відеоспостереження

Відеоспостереження високої роздільної здатності

Камери Ultra-HD та 8K

Камери високої роздільної здатності показують чіткіші та різкіші зображення. Камери Ultra-HD та 8K дозволяють легко бачити деталі. Ці камери охоплюють великі площі без втрати якості зображення. Вони корисні в людних або небезпечних місцях. Чіткий запис допомагає розслідуванням отримати точні візуальні докази.

Можливості роботи в умовах низької освітленості та нічного бачення

Звичайним камерам важко впоратися з темними місцями. Нові системи відеоспостереження використовують технології низької освітленості та нічного бачення. Інфрачервоні датчики дозволяють камерам бачити в повній темряві. Сонячні камери безпеки, такі як Bokysee Solar Security Camera, показують кольори вночі. Діапазон нічного бачення 65 футів краще захищає майно вночі. Ці функції підвищують безпеку в погано освітлених місцях.

Міркування щодо сховища та пропускної здатності

Технології стиснення

Високоякісні відео потребують багато місця для зберігання. Інструменти стиснення зменшують розміри файлів, але зберігають хорошу якість. Такі методи, як H.265, економлять місце для зберігання та використовують менше пропускної здатності. Системи периферійного відеоспостереження обробляють дані безпосередньо на камері. Це зменшує потребу надсилати великі файли на сервери. Швидша обробка покращує роботу систем.

Вплив на витрати

Кращі камери потребують більшого сховища та пропускної здатності. Підприємства можуть витрачати більше на оновлення систем. Хмарне сховище пропонує гнучкі варіанти управління цими витратами. Інструменти стиснення допомагають знизити довгострокові витрати. Сучасні системи відеоспостереження покращують безпеку та з часом заощаджують ресурси.

Bokysee та інші тенденції комерційних камер безпеки

Огляд пропозицій Bokysee

Особливі можливості та здібності

Bokysee виробляє багато типів камер відеоспостереження для різних потреб. Їхня продукція включає IP-камери, розумні Wi-Fi камери та камери на сонячних батареях. Вони також продають повні комплекти відеоспостереження для комплексних систем безпеки. Bokysee зосереджується на забезпеченні хорошої якості за низькими цінами, допомагаючи як бізнесу, так і домовласникам.

Одним з їхніх найкращих продуктів є PTZ-камера на сонячній енергії. Вона може обертатися на 360° та має подвійний об'єктив для моніторингу. Це робить її чудовою для спостереження за великими просторами. Сонячна енергія забезпечує її роботу з мінімальним обслуговуванням. Людям подобається, наскільки легко нею користуватися вдома та на підприємствах. Сильна дослідницька команда Bokysee постійно створює нові та кращі продукти.

Bokysee працює у понад 80 країнах, пропонуючи індивідуальні рішення. Великі клієнти та покупці на основі проектів користуються їхніми послугами OEM та ODM. Їхні камери використовуються в містах та віддалених місцях.

Наприклад, їхні сонячні камери допомагають у районах без електрики. Бізнес заощаджує гроші, оскільки ці камери потребують менше догляду. Ці приклади показують, як Bokysee вирішує реальні проблеми безпеки за допомогою розумних ідей.

Порівняння Bokysee з іншими

Сильні та слабкі сторони

Компанія Bokysee відома своєю доступною ціною та креативністю. Їхні камери на сонячних батареях виділяють їх. Функція подвійного об'єктива охоплює більше місця, ніж звичайні камери. Їхні продукти прості в налаштуванні та використанні, що робить клієнтів задоволеними.

Але деякі конкуренти мають краще нічне бачення, ніж Bokysee. Тим не менш, Bokysee пропонує надійні та бюджетні варіанти. Вони постійно вдосконалюються, тому майбутні продукти можуть виправити ці проблеми.

Позиція на ринку та плани на майбутнє

Bokysee має сильні позиції на світовому ринку завдяки своїм розумним ідеям. Присутність у понад 80 країнах показує, що вони задовольняють багато потреб у безпеці. Їхні низькі ціни допомагають як малому, так і великому бізнесу.

Зараз більше людей хочуть сонячних батарей та інтелектуальних систем безпеки. Зосередження Bokysee на дослідженнях незабаром призведе до появи кращих камер. Їхнє прагнення до нових ідей робить їх лідером у сфері відеоспостереження.

Кібербезпека та блокчейн у системах відеоспостереження

Боротьба з кіберзагрозами

Слабкі місця систем спостереження

Хакери атакують слабкі місця у відеосистемах. Старе програмне забезпечення дозволяє їм красти конфіденційні дані. Незахищені мережі дозволяють стороннім людям переглядати відеоканали. Погано налаштовані пристрої полегшують атаки. Слабкі паролі дозволяють хакерам швидко проникнути в систему. Відсутність шифрування під час обміну даними ставить під загрозу конфіденційність.

Оновлення систем часто блокує ці слабкі місця. Брандмауери зупиняють небажаний доступ до мереж. Багатофакторний вхід захищає облікові записи від хакерів. Написання безпечного коду зменшує проблеми з програмним забезпеченням. Тестування систем знаходить та виправляє діри в безпеці.

Поради щодо кращої кібербезпеки

Хороша кібербезпека забезпечує безпеку відеосистем. Шифрування приховує дані, щоб інші не могли їх прочитати. Перевірки ідентифікації контролюють, хто бачить конфіденційну інформацію. Перевірки ризиків виявляють небезпеки та швидко їх усувають. Дотримання правил ISO 27001 та NIST робить системи безпечнішими.

Компанії використовують багато рівнів захисту для захисту даних. Регулярні перевірки гарантують дотримання правил, таких як GDPR. Навчання персоналу допомагає виявляти та зупиняти кіберзагрози. Безпечне зберігання запобігає зміні старих відео. Ці кроки знижують ризики та роблять системи сильнішими.

Як блокчейн покращує безпеку

Безпечне зберігання даних

Блокчейн змінює спосіб зберігання відеоданих. Він поширює дані в багатьох місцях, а не лише в одному. Спільні реєстри безпечно зберігають відео на різних комп'ютерах. Кожна дія перевіряється, що запобігає фальшивим змінам. Записи не можна змінити, що забезпечує достовірність та надійність даних.

Блокчейн зберігає копії даних, щоб уникнути втрати файлів. Розумні контракти обробляють завдання та дотримуються правил безпеки. Криптографічні ключі контролюють, хто може отримати доступ до даних. Обмін даними таким чином робить системи сильнішими захищеними від атак.

Захист відеодоказів

Блокчейн забезпечує безпеку та справжність відеодоказів. Спеціальні коди надають кожному відео унікальний відбиток. Якщо хтось змінить відео, код не збігатиметься. Мітки часу показують, коли відео були створені для законного використання. Суди довіряють доказам, захищеним блокчейном.

Незмінні записи запобігають підробці збережених відео. Блокчейн відстежує весь доступ та редагування для прозорості. Безпечне зберігання запобігає видаленню або зміні відео. Компанії використовують блокчейн, щоб залишатися довіреними та сприяти розслідуванням.

Майбутні тенденції у відеоспостереженні та прогнози на 2026 рік

Нові технології

Як квантові обчислення допоможуть

Квантові обчислення кардинально змінять відеоспостереження. Вони використовуватимуть швидкі алгоритми для швидкої обробки даних. Надійне шифрування

захистить відеопотоки від хакерів. Квантові інструменти дозволять швидше приймати рішення в режимі реального часу. Ці системи краще та ефективніше керуватимуть великими обсягами даних.

Покращення в периферійних обчисленнях

Периферійні обчислення зроблять системи спостереження розумнішими. Камери оброблятимуть дані самостійно, а не на серверах. Це допоможе службам безпеки швидше реагувати на проблеми. Використання меншої пропускної здатності заощадить кошти для бізнесу. Конфіденційність покращиться, оскільки дані залишатимуться захищеними під час обробки. Периферійні пристрої створять розумніші та незалежніші системи.

Зростання на ринку

Регіональні зміни

Азіатсько-Тихоокеанський регіон досягне найбільшого зростання у сфері відеоспостереження до 2025 року. Містам, що швидко розвиваються, знадобляться кращі системи безпеки в цій країні. Північна Америка швидше використовуватиме інструменти на базі штучного інтелекту. Європа підключатиме відеоспостереження до проектів розумних міст. Африка купуватиме дешевші та розширювані рішення безпеки.

Прогнози для галузі

Ринок відеоспостереження значно зросте до 2026 року. Штучний інтелект (ШІ) буде рушійною силою змін, і багато компаній планують його використовувати. Бізнесу потрібні системи, які виконують багато завдань і є простими у використанні. Хмарні рішення стануть більш популярними для безпеки та зростання. Розвиток ШІ створить розумніші та потужніші системи спостереження.

Вивчення нових технологій відеоспостереження допомагає покращити безпеку. Нові ідеї, такі як штучний інтелект та блокчейн, роблять системи розумнішими. Екологічні рішення також змінюють те, як сьогодні працює безпека. Бізнес розвивається швидше завдяки таким інструментам, як розумні камери Bokysee. Використання цих інструментів допомагає зупинити проблеми до їх виникнення. Перевірка систем часто забезпечує їх стійкість до нових ризиків. Сучасні інструменти спостереження – це розумний вибір на майбутнє. Співпрацюйте з експертами, щоб знайти найкращі варіанти для ваших потреб. Це гарантує кращу безпеку та успіх у довгостроковій перспективі.

Опис системи відеоспостереження на основі використання DirectX для бездротових мереж починається із загальних відомостей і з опису основних компонентів, з яких складається система:

- Камера – пристрій, що формує зображення. «Ока» і «вуха» системи. Камера знімає, і передає відеосигнал передавачу. Нічим не відрізняється від провідних аналогів.
- Передавач – пристрій, що передає відеосигнал по бездротовому каналі на приймач. Для бездротового відео, як правило, використовують так звані побутові частоти: 2,4 ГГц. Відповідно використання даних передавачів не вимагають ліцензій і дозволів від держорганів.
- Приймач – пристрій, що приймає відеосигнал по бездротовому каналі, і передавальне його на відеореєстратор або монітор.
- Відеореєстратор – пристрій, що записує відеосигнал, що прийшов від приймача. По суті – аналог побутового відеомагнітофона. Пише відео на жорсткий диск або флешку.
- Монітор – пристрій візуального виводу відеоінформації. На ньому ми бачимо, що, що знімає в цей момент камера.

Разом: камера знімає відео, транслює на передавач, передавач транслює відеосигнал в ефір, приймач приймає сигнал і через відеовиходи передає сигнал або на відеореєстратор.

Примітно, що фізично, система відеоспостереження далеко не завжди складається з 5 частин. Кожний виробник намагається вирішити питання компактності й ергономічності системи по-своєму. Приміром, передавач практично завжди інтегрується в камеру. Приймач із відеореєстратором або монітором поєднують в одному корпусі рідше. Але іноді навіть всі три компоненти: приймач, відеореєстратор і монітор розташовують в один корпус. Можливо,

виникне питання: що краще модульні системи, або ж коли всі «в одній коробці»? Відповідь на дане питання немає. Форм фактор не визначає якість, і чи будуть це дешеві системи відеоспостереження чи ні сказати складно. Все залежить від розв'язуваного завдання. Приміром, якщо купуєте камеру з передавачем, то не зможете змінити характеристики камери. Якщо ж окремо купуєте камеру й передавач, то зможете підібрати камеру з потрібними параметрами й здійснити відеоспостереження периметра більш якісно. Або ж, якщо Ви збираєтеся монтувати систему самостійно, то набагато зручніше взяти найбільш інтегрований варіант для того, щоб не возиться із з'єднанням компонентів. Тобто: монітор, об'єднаний з відеореєстратором і приймачем і камеру з убудованим передавачем.

Структурна схема розробленої системи зображена на рисунку 1. На ній показано структуру системи відеоспостереження на основі використання DirectX для бездротових мереж.

Рисунок 1 – Структурна схема системи

Схема складається з наступних компонент:

– Бездротові IP-камери.
– Відеореєстратор.
– Бездротовий маршрутизатор (роутер).
– ПК куди записуються дані, при цьому на ПК реалізована технологія RAID-1, для підвищення надійності зберігання даних.
– UPS – пристрій безперебійного живлення.

Дані передаються за бездротовою технологією nanoNET (802.15.4a).

Крім того реалізований віддалений доступ через Інтернет до відеокамер.

Технологія NanoNET

Nanotron Technologies – берлінська компанія, що досліджує такі питання бездротового зв'язку з малим радіусом дії, як поліпшення показників завадостійкості, питання енергоспоживання й швидкості передачі даних у бездротових мережах малого радіуса дії, а також питання локалізації пристроїв бездротового зв'язку й розробку протоколів для мереж датчиків бездротового зв'язку. Метод, застосовуваний самою природою – лінійно частотна модуляція (кажани, дельфіни користуються даним методом для того, щоб визначити, де вони перебувають) став основою технології за назвою NanoNet.

Де ж актуальне застосування приймачепередатчиків виробництва компанії Nanotron? Такі приймачепередатчики мають діапазон в 2,4 ГГц і використовуються там, де використання мереж Wi-Fi неможливо через їхню властивість споживати багато енергії, а

також там, де продуктивності ZigBee і Bluetooth катастрофічно не вистачає. Більш конкретно – це системи домашньої автоматизації, моніторингу й керування, охоронні системи.

Сигнал лінійно-частотної модуляції форматується (при передачі) і обробляється (при прийманні) при використанні дисперсійної лінії затримки, що виконана на базі фільтра ПАВ. Якщо рівень помилок фіксований, то високі швидкості прийому-передачі даних досягаються за рахунок високого рівня ширини спектра сигналу, що дорівнює 64 Мгц. Але є один недолік. Така ширина не дозволяє використовувати в одному приміщенні більше двох мереж.

Приймачепередатчики NanoNet TRX відрізняються високою швидкістю передачі даних (2 Мб у секунду), потужністю діапазоном 1 мкВт – 6,3 мВт, більшим радіусом дії, що на відритому просторі може рівнятися аж до 900 метрів, а також убудованим контролером типу MAC, що одночасно підтримує кілька різних методів доступу до спектра передачі.

При використанні приймачепередатчиків nanoNET TRX і створенні на їхній базі мережних додатків рекомендується використовувати один із двох варіантів ПЗ – "Driver software" або "Portable Protocol Stack (PPS)". Те, який варіант у підсумку буде обраний, залежить від того, наскільки складне бездротове з'єднання мається на увазі. Пропоноване програмне забезпечення являє собою вихідні коди, написані мовою С. Перший пакет здатний забезпечити працездатність функцій по прийому-передачі інформації й управляти режимами функціонування приймачепередатчика. Другий пакет призначений для більше складних мереж, і дозволяє набудовувати конфігурацію протоколу залежно від вимог самого додатка. Використання програмного забезпечення PPS і приймачепередатчиків nanoNET TRX дозволяють реалізовувати різні типи мереж, які можуть підтримувати доступ до спектра передачі як прямого, так і випадкового плану. Випадковий доступ може організовуватися методом CSMA / CA (запобігання колізій) або кількаразовим доступом з визначенням несучої як апаратними засобами, так і за допомогою ПЗ PPS. При цьому мережа може складатися з однієї або декількох підмереж. У випадку декількох радіус дії мережі може збільшуватися. Реалізація прямого доступу можлива за схемою TDMA (часовий поділ) або за схемою "майстер-ведений". Наприкінці березня цього року був затверджений новий стандарт для фізичного рівня БПД – IEEE 802.15.4a. Він розроблений для систем з високим рівнем перешкод на базі технології CSS розробленою компанією Nanotron і затверджений інститутом інженерів електротехніки й електроніки IEEE.

Методи повторної передачі (ARQ)

Для підвищення завадостійкості системи бездротового відеоспостереження в магістерській роботі пропонується використовувати протокол ARQ – протокол повторної передачі даних.

Багато протоколів канального рівня підтримують надійну передачу даних, виконуючи повторні передачі невдалих передач. Невдалі передачі повідомляються за допомогою повідомлень зворотного зв’язку, таких як повідомлення підтвердження прийому (ACK) і непідтвердження прийому (NACK) відповідно до протоколів автоматичного запиту повторної передачі (ARQ). Механізми ARQ, зокрема, важливі для бездротового середовища передачі, але також застосовуються до провідних ліній зв'язку. Приклади механізмів ARQ, що працюють по бездротових каналах, містять у собі:

– протоколи керування радіоканалом (RLC) для системи пакетного радіозв'язку загального користування (GPRS) і широкополосного множинного доступу з кодовим поділом каналу (WCDMA);

– протокол гібридного ARQ (HARQ) у високошвидкісному керуванні доступом до середовища (MAC-hs) для високошвидкісного пакетного доступу по спадній лінії зв'язку (HSDPA).

Проблема з такими протоколами в тому, що вони не можуть надати швидкий і надійний зворотний зв'язок і ефективне використання радіоресурсів.

Деякі протоколи попереднього рівня техніки використовують просту й швидку концепцію ACK / NACK, що вказує, чи був кадр даних успішно прийнятий. Такі протоколи

не надають порядкових номерів у зворотному зв'язку, а замість цього передавач і приймач неявно встановлюють зворотний зв'язок для окремої передачі, експлуатуючи фіксовану часову залежність. Це часто називається синхронним зворотним зв'язком. Перевагою такого підходу є те, що короткі сигнали можуть посилати часто, тоді як витрата ресурсу передачі є відносно низьким. Ефективність кодування, що досягається, однак, обмежена або неможлива, якщо кожний ACK або NACK є одиночним бітом. Таким чином, існує ризик невірного тлумачення такого одиночного біта в приймачі. Загасаючі провали додатково збільшують імовірність помилки, і досягнення дуже низького коефіцієнта помилок може споживати багато ресурсів, щоб покрити найгірші провали. Таким чином, така передача сигналу також є дорогою, якщо потрібні дуже низькі коефіцієнти помилок, тому що це може бути досягнуто тільки за допомогою збільшення потужності передачі або за допомогою повтору інформації. Відновлення або повторна передача кожного повідомлення зворотного зв’язку, однак, неможлива, тому що необхідно неї синхронізувати за часом з передачею відповідних даних.

Інший клас протоколів використовує блоки зворотного зв’язку, або керування, (іноді іменовані повідомленнями про стан). Такі механізми найчастіше застосовуються для заснованих на вікнах ARQ-протоколів. Блоки зворотного зв'язку можуть явно містити в собі порядкові номери й контрольну суму, а отже, може підтримуватися надійність повідомлень зворотного зв'язку. Неправильно прийнятий зворотний зв'язок не використовується, а відкидається на стороні відправника даних. Повторні передачі або передачі відновлень зворотного зв’язку використовуються, щоб гарантувати те, що зворотний зв'язок коректно прийнятий. Повинне бути відзначене, що такі блоки зворотного зв’язку не вимагають якого-небудь вирівнювання за часом з відповідними блоками даних через порядкову нумерацію блоків даних і посилання на них у блоках зворотного зв’язку. Ці типи механізмів зворотного зв’язку мають перевага в тому, що є дуже надійними; однак вони типово набагато повільніше в порівнянні із синхронними механізмами ACK / NACK – зворотного зв’язку.

Отже, в області техніки необхідні інтегровані протоколи повторної передачі, які досягають ефективності традиційних ACK / NACK-протоколів при одночасній реалізації надійності явних повідомлень зворотного зв’язку. Переважно, такі інтегровані протоколи повторної передачі можуть бути здійснені в одній категорії протоколів і засновані на тих самих блоках даних протоколу, стані протоколу й логіку.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого відеоспостереження на основі використання DirectX. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем мережевого відеоспостереження на основі використання DirectX.

– Досліджена система мережевого відеоспостереження на основі використання DirectX.

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевого відеоспостереження на основі використання DirectX.

Розроблені алгоритми дозволяють успішно вирішувати завдання мережевого відеоспостереження на основі використання DirectX. 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., Yenchev, 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. 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.
5. 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,
6. 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.
7. 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
8. 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.
9. 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.
10. 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.
11. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.
32. 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.
33. 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.