Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“____” _____ 2025 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти
на тему
“Дослідження та програмна реалізація системи мережевого відеоспостереження на основі використання DirectX”

Виконав здобувач вищої освіти
ІІ курсу, групи КІ-24М
ОПП «Комп’ютерна інженерія»
спеціальності 123 «Комп’ютерна інженерія»
_____ Хромочкін М.В.
«____» _____ 2025 р.

Керівник проекту
доктор філософії (PhD)
_____ Дрєєва Г.М.
«____» _____ 2025 р.
Рецензент _____
_____

м. Кропивницький

АНОТАЦІЯ

Хромочкін М.В. Дослідження та програмна реалізація системи мережевого відеоспостереження на основі використання DirectX. 123 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2025.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи мережевого відеоспостереження на основі використання DirectX.

Метою розробки є дослідження та 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.

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.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ з ОС Windows 10/11.

Програму розроблено в середовищі Builder C++.

Ключові слова: комп'ютерна інженерія, відеоспостереження, DirectX

ABSTRACT

Khromochkin M.V. Research and software implementation of a network video surveillance system based on the use of DirectX. 123 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2025.

In this final qualification work for the second (master's) level of higher education, software has been developed that is intended for a network video surveillance system based on the use of DirectX.

The purpose of the development is the research and software implementation of a network video surveillance system based on the use of DirectX.

The object of the research is the process of network video surveillance based on the use of DirectX.

The subject of the research is the methods of network video surveillance based on the use of DirectX.

The research methods are based on the methods of coding theory and the theory of building computer networks, methods of mathematical statistics, and methods of software development.

The result of the work is the software implementation of a network video surveillance system based on the use of DirectX.

In the process of working on the software model, an analysis of existing hardware and software was performed. All components of the developed software are fully described.

A convenient user interface has been developed. Instructions for working with the software are provided.

The program can be used on a PC with Windows 10/11.

The program was developed in the Builder C++ environment.

Keywords: computer engineering, video surveillance, DirectX

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

БПД	–	бездротова передача даних
ПЗ	–	програмне забезпечення
СПД	–	системи передачі даних
ACK	–	повідомлення підтвердження прийому
ARQ	–	протокол повторної передачі даних
BPSK	–	Binary phase-shift keying
FFD	–	повнофункціональний пристрій
GFSK	–	Gaussian frequency-shift keying
MAC	–	шар механізму доступу
NACK	–	повідомлення непідтвердження прийому
OSI	–	мережна модель
P2P	–	однорангові мережі
PAN	–	персональна мережа
PPS	–	Portable Protocol Stack
RFD	–	пристрій з полегшеними функціями
TDMA	–	часовий поділ
Wi-Fi	–	бездротова технологія

ВСТУП

Актуальність теми. 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.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація 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.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод мережевого відеоспостереження на основі використання DirectX.

– Розроблено вітчизняний продукт мережевого відеоспостереження на основі використання DirectX, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі мережевого відеоспостереження на основі використання DirectX.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Робота апробована на LVII Науково-технічній конференції здобувачів вищої освіти LV науково-технічної конференції «Наука в ЦНТУ: основні досягнення та перспективи розвитку» (2025 р.), основні положення випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти надруковані у статті збірника праць молодих науковців ЦНТУ, випуск №15.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи мережевого відеоспостереження на основі використання DirectX, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Вибір правильної системи відеоспостереження передбачає визначення того, як ваші камери підключаються до вашого записуючого пристрою, а також як ці дані зберігаються та отримуються до них доступ. Основний вибір – це між сучасними системами на основі IP та традиційним аналоговим відеоспостереженням. Хоча аналогові технології є надійними, галузь перейшла на IP-технології через їх чудові можливості.

Ключова відмінність полягає в тому, що IP-системи є цифровими та обробляють відео, як невеликі комп'ютери, тоді як аналогові системи більше схожі на телебачення старої школи. Цей цифровий перехід дозволяє використовувати функції, які колись вважалися науковою фантастикою. Розуміння архітектури вашої системи впливає на встановлення, масштабованість та майбутні оновлення.

IP-системи є сучасним золотим стандартом у сфері відеоспостереження. Це складні пристрої, які обробляють відео внутрішньо, перш ніж надсилати цифрові сигнали через вашу мережу. Цей інтелект дозволяє створювати роздільну здатність 4K Ultra HD, здатну розпізнавати обличчя та номерні знаки, а не лише розмиті форми.

Основою системи IP-відеоспостереження є мережевий відеореєстратор (NVR), який керує камерами через мережеві з’єднання. Багато з них використовують живлення через Ethernet (PoE) – революційну технологію, яка передає живлення та дані через один кабель, спрощуючи встановлення.

IP-системи мають високу масштабованість; комерційні відеореєстратори можуть підтримувати понад 100 камер, що спрощує розширення. Багато IP-камер також мають вбудований штучний інтелект для розрізнення людей, транспортних

засобів та тварин, зменшуючи кількість хибних тривог. Ці системи добре інтегруються з контролем доступу, надсилають мобільні сповіщення та надають розширену аналітику.

1.2 Область застосування

Областю застосування є системи відеоспостереження. Головна мета функціонування системи відеоспостереження полягає в забезпеченні постійного візуального контролю об'єкту, що охороняється або території.

В залежності від способу передачі сигналу виділяють такі типи систем відеоспостереження:

– аналогові системи відеоспостереження;

– цифрові системи відеоспостереження;

– гібридні системи відеоспостереження.

У гібридних або комбінованих системах відеоспостереження встановлюються аналогові камери з пристроями для подальшої оцифровки відеоінформації.

Ефективна система відеоспостереження на вашому об'єкті замінює кількох робітників служби охорони та безпеки.

Більшість сучасних цифрових систем відеоспостереження складаються з ір-камер, які дозволяють переглядати процес спостереження через Інтернет.

Так для такої системи немає обмежень за способом перегляду запису – ви можете користуватися пультом охорони з стаціонарними комп'ютерами, домашніми ноутбуками, портативними комунікаторами, планшетами та мобільними смартфонами. Також стає можливим віддалений доступ через Інтернет до налаштувань і управління системи відеоспостереження.

Контролювати все, що відбувається на вашому об'єкті в режимі реального часу вам дозволить система відеоспостереження через інтернет.

Спроектувати бездротову систему відеоспостереження на базі IP-камер дозволяють такі технології бездротової передачі сигналу:

– Wi-Fi;

– 3G;

– GSM;

– CDMA.

В даний час не існує обмежень по кількості відеокамер для таких систем, а також установка відеоспостереження можлива як на нерухомих, так і на рухомих об'єктах.

Слід зазначити, що в сучасних комплексних системах безпеки пріоритетною складовою є система відеоспостереження. Так крім візуального контролю система дає можливість програмувати дії всієї охоронної системи в різних екстрених ситуаціях на об'єкті.

Система відеоспостереження може встановлюватися на програмному та апаратному рівнях.

Клієнти використовують сучасні охоронні системи відеоспостереження для забезпечення безпеки на самих різних об'єктах: будинки, квартири, заміської дачі, офісу, заводу або великих територій автовокзалів і аеропортів і т.д.

Також варто зазначити, що існують автономні системи відеоспостереження, які дозволяють відмовитися від трансляції сигналу на точку-приймач, а використовувати власний накопичувач відеоінформації. Така система дозволяє вирішувати проблему з відсутністю сигналу або мережі на будь-якій території або ж з непостійністю сигналу під час пересування автомобіля.

Стрімкий розвиток відеоспостереження зробив можливою появу прихованого відеоспостереження. Так система прихованого відеоспостереження складаються з мінівідеокамер. Такі мініатюрні камери найчастіше встановлюються в різних елементах інтер'єру. Розміри мікровідеокамери кілька міліметрів.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи мережевого відеоспостереження на основі використання DirectX, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти

ORIENT W802G4

Почну, з добре знайомого мені комплекту ORIENT W802G4. Це не новинка, проте, мені здається вона дуже цікавою для тих з нас, хто підбирає недороге рішення для установки у квартирі, під'їзді або дачному будиночку. Насправді, даний комплект є лише частиною системи відеоспостереження. У комплект входять чотири бездротові камери в антивандальному всепогодному корпусі, один приймач, набір з п'яти мережних джерел живлення й два композитних кабелі. У найпростішому випадку процес складання системи відеоспостереження зводиться до двох простих кроків. Ви розставляєте камери в потрібних місцях і підключаєте приймач до будь-якого телевізора. Не чи правда, просто?! При необхідності ви можете ускладнити систему відеоспостереження й інтегрувати комплект ORIENT W802G4 в існуючу систему безпеки, підключивши її до відеореєстратора.

Давайте ближче познайомимося з особливостями камер, що входять у комплект. Як було відзначено вище, кожна камера виконана в антивандальному всепогодному корпусі, установленому на спеціальному кронштейні, що дозволяє вибрати зручний ракурс зйомки. Кронштейн може кріпитися на стіні або стелі, а також може виконувати функцію підставки для установки камери на будь-якій горизонтальній поверхні.

Кожна камера обладнана кольоровою ПЗС матрицею, розміром 1/3” і розрішенням 380 горизонтальних ТВ ліній, що відповідає дозволу 628x582 у системі PAL або 510x492 в NTSC. Використовуваний об'єктив має кут огляду 45?.

Це так званий універсальний кут, що забезпечує досить гарний огляд навіть у невеликих приміщеннях.

Якість картинки дуже пристойне. Висока деталізація й відмінний фокус, як при зйомці близько розташованих об'єктів, так і віддалених, роблять ці камери вдалим вибором для рішення широкого спектра завдань по відеоспостереженню.

На фронтальній стороні камери встановлений потужний ІЧ-прожектор, що включає 30 світлодіодів. Цього досить для нормального освітлення сектора на відстані до 15 метрів, але при цьому не створюється засвітлення, що заважає нормальній зйомці близько розташованих об'єктів. Включення ІЧ-підсвічування відбувається в автоматичному режимі. Для цього використовується фотоелемент.

Ще однією особливістю камер можна назвати убудований мікрофон, що дозволяє вести запис відео зі звуком.

Для підключення камер можна використовувати як бездротове, так і провідне підключення. Кожна камера обладнана роз’єм живлення, відео й аудіо виходами.

Для бездротового підключення використовується мініатюрний чотирьохканальний приймач. На лицьовій стороні приймача розташований індикатор, що відображає номер каналу. Управляти приймачем можна як за допомогою пульта дистанційного керування, так і за допомогою кнопки на верхній стороні корпуса. Користувач може вибрати режим відображення одного із чотирьох каналів або циклічне відображення чотирьох каналів. Режим квадратора (відображення чотирьох каналів на одному екрані) дана модель приймача не підтримує.

На тильній стороні корпуса приймача розташовано: роз’єм для підключення блока живлення, антена й дві пари композитних виходів (відео+звук). Для чого необхідні два виходи? Наприклад, для одночасного підключення приймача до відеореєстратора й до телевізора.

В ORIENT W802G4 використовується аналогова бездротова технологія передачі зображення в діапазоні 2.400-2.483Ггц. Недоліком цієї технології є

залежність від розташованих рядом джерел, що працюють у тім же діапазоні. Мова йде про бездротові телефони, Wi-Fi точки доступу й інших побутових пристроїв. Всі ці прилади створюють перешкоди при прийманні інформації з камер, при цьому самі камери можуть заблокувати роботу Wi-Fi у будинку. Звертаю увагу, що перешкоди можуть створювати не тільки прилади, що працюють у вашій квартирі, але й у квартирах сусідів. У цьому змісті, бездротове підключення більш актуально для заміського будинку, де можна розраховувати на куди більший радіус дії. Відповідно до специфікації, на відкритому просторі радіус дії може досягати 100 метрів.

Якщо умови у квартирі й будинку не дозволяють нормально використовувати бездротове підключення, то завжди можна скористатися провідним підключенням. У цьому випадку, камери можна прямо підключити до окремого каналу відеореєстратора й вести незалежний запис всіх чотирьох каналів, що помітно розширює можливості системи відеоспостереження.

ORIENT W203D4 Digital

На відміну від ORIENT W802G4 в ORIENT W203D4 Digital використовується цифрова технологія передачі сигналу, що забезпечує ідеальну якість картинки на відстані до 200 метрів.

Цифрова технологія бездротового підключення не єдине, що відрізняє комплект ORIENT W203D4 Digital. Це не просто набір бездротових камер, це повноцінна 4-х канальна система відеоспостереження для комп'ютера. Причому, на відміну від звичних комп'ютерних систем відеоспостереження, що вимагають установку багатоканальної плати відеозахвата, у цьому випадку використовується маленький USB приймач, що дозволяє використовувати таке рішення не тільки з настільними комп'ютерами, але й з ноутбуками або неттопами. У комплект входять чотири камери, виконані в пластиковому корпусі. Камери відрізняються компактним розміром, що в сполученні з білим кольором корпуса, робить їх непомітними в інтер'єрі. Важливо помітити, що вага камери становить менш 60 грам. Це дозволяє кріпити її навіть на легких конструкціях.

Камери обладнані об'єктивом з фіксованою фокусною відстанню й CMOS сенсором, розміром 1/4". Сенсор має розрішення 380 ТВЛ, що дозволяє одержати картинку 628x582 пікселів у системі PAL або 510x492 пікселів у системі NTSC. ІЧ-підсвічування в даних камерах не передбачені. Кут огляду використовуваного об'єктива невеликий, і не дуже підходить для використання в маленьких квадратних приміщеннях, однак, завдяки конструкції камери, ви завжди можете замінити використовуваний об'єктив на іншій. Тут використовуються стандартні об'єктиви для мікрокамер M12. Наприклад, сюди можна без проблем установити об'єктив “риб'яче око” з кутом огляду 140?.

На тильній стороні є: роз’єм антени, кнопка CODE для прив'язки бездротової камери, світлодіодний індикатор, що відображає стан живлення камери й USB порт, використовуваний для підключення зовнішнього джерела живлення.

У підставці корпуса розташовані убудований мікрофон і кріплення для кронштейна. Використовуваний кронштейн також виконаний з білого пластику й дозволяє закріпити камеру на стіні або стелі, і вільно вибирати ракурс, з якого буде вестися зйомка.

Бездротовий приймач зовні нагадує велику флешку. Більша ширина й товщина корпуса приймача, можуть викликати проблему з підключенням USB пристроїв до сусідніх USB портів. Якщо це критично для вас, то можна скористатися USB перехідником або USB хабом.

На корпусі приймача розташовані: знімна поворотна антена й один світлодіодний індикатор. Якщо чесно, я сподівався побачити на корпусі роз’єм з аналоговими відеовиходами, що дозволило б використовувати дану бездротову систему в парі з відеореєстраторами, але нічого схожого тут ні, що ще раз підтверджує те, що ORIENT W203D4 Digital чисто комп'ютерна система відеоспостереження.

Для створення системи відеоспостереження досить розставити камери, підключити приймач до USB порту комп'ютера й установити програмне

забезпечення. Процес установки й налаштування програмного забезпечення займає лічені мінути. Софт прекрасно працює як під Windows XP, так і під Windows 7. Однією з умов нормальної роботи є підтримка Media Player версії 9 або вище. У принципі, для роботи системи відеоспостереження не потрібно робити яких-небудь налаштувань, все працює, що називається “прямо з коробки”. Проте, у деяких випадках меню налаштування параметрів дозволять зробити систему відеоспостереження більше зручною й ефективною.

Меню налаштування включає два розділи. Розділ «System» включає набір загальних параметрів, серед яких мова інтерфейсу (росіянин не підтримується), параметри поштового сервера для оповіщення про тривожну ситуацію, а так само папки для зберігання відеозаписів і фотографій. Тут же можна настроїти параметри убудованого Web сервера й MMS сервера для віддаленого доступу до системи відеоспостереження.

Другий розділ, включаючи ряд додаткових параметрів, серед яких я виділив можливість додавання штампів часу й дати, накладення водяного знака, налаштування відеопараметрів, поворот зображення, а також налаштування дозволу і якість відеозапису, області дії детектора руху й оповіщення.

Програмне забезпечення включає базовий набір функцій, властивих сучасним системам безпеки, включаючи можливість перегляду одного або чотирьох каналів на одному екрані, виявлення руху по кожному каналі окремо, запис відео, зняття фотозображення й, що мені особливо сподобалося, доступ через Інтернет, що дозволяє віддалено контролювати систему відеоспостереження, перебуваючи в будь-якій точці миру, де є Інтернет.

Вікно програми має фіксований розмір, що з однієї сторони дуже зручно, особливо, при паралельній роботі з іншими додатками. Для додаткової зручності є можливість згортання програми в компактне вікно з відображенням картинки з однієї або чотирьох камер. У компактному режимі користувач може не тільки бачити відеозображення з різних камер, але й швидко робити скриншоти зображення.

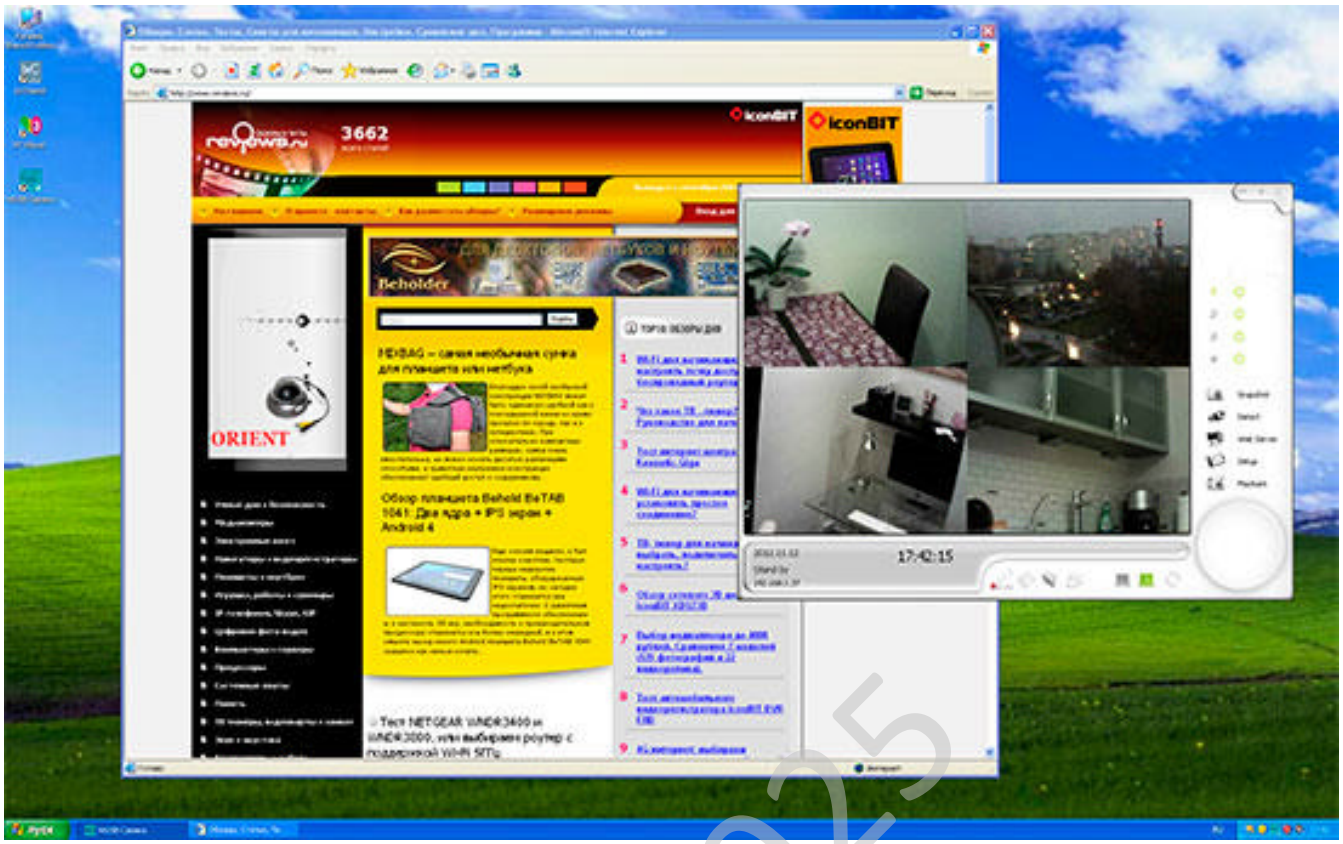

Рисунок 2.1 – Інтерфейс користувача ORIENT W203D4 Digital

Інтерфейс програми дуже схожий на інтерфейс більшості систем відеоспостереження. Більша частина екрана віддана під зображення з камер. Можна вибрати режим відображення зображення з однієї або чотирьох камер.

У правій частині вікна додатки розташовані кнопки вибору каналу, захвата зображення, включення режимі детектування (він же режим запису), включення убудованого Web-сервера для віддаленого підключення, налаштування й перегляду записів. У нижній частині вікна розташована інформація про поточний час, IP адресі, рівні сигналу й інші деякі параметри. Тут же можна включити режим перегляду одного каналу або чотирьох.

Запис ведеться у форматі WMV, що дозволяє переглянути запис, просто відкривши папку з файлами й запустивши Windows Media Player. Запис ведеться в тому же форматі, у якому зображення представлене у вікні перегляду додатка. Якщо вибрати один канал, то й результуючий файл буде містити тільки

зображення цього каналу. Якщо обрано режим відображення чотирьох каналів, то й запис буде включати зображення всіх чотирьох каналів. Можливо, це не самий звичний спосіб подання інформації, але для системи відеоспостереження даного класу, він здається більше доступним і зрозумілим.

Якщо ви хочете мати зручний механізм для пошуку записів, то рекомендую скористатися інструментом перегляду, інтегрованим у додаток відеоспостереження. Тут всі дуже зрозуміло. Користувач задає часовий інтервал, одну або кілька камер для відображення, і натискає кнопку пошуку.

Вікно перегляду включає зручний інструмент для швидкого перегляду на швидкостях до 16х, а також дозволяє швидко переміщатися по відеофайлу. При необхідності можна перейти в папку з відеофайлом або зробити скриншот.

Одне з важливих питань, можливість підключення до системи відеоспостереження через інтернет. Для цього необхідно настроїти доступ з інтернет по порту 7788. Якщо ваш комп'ютер прямо підключений до інтернет, і при цьому ваш провайдер видає вам публічний IP адреса, то для перегляду камер досить просто ввести свій IP адреса. Якщо ж доступ в інтернет здійснюється через домашній роутер, то необхідно настроїти віртуальний сервер на порт 7788. Приємно помітити, що дане рішення відмінно працює під різними браузерами, включаючи Safari під OS X. Функціонально, користувач може тільки переглядати відео в тому форматі, що обраний в основному додатку. Це звичайно не дуже добре. Було б краще, якби користувач міг вільно вибирати канал для віддаленого перегляду, примусово запускати запис і здійснювати пошук і перегляд записів на віддаленому сервері. Але якщо врахувати, що дана система ставиться до систем початкового рівня, і її головною особливістю є простота й доступність для рядового споживача, те вже те, що в ній реалізоване, здається мені більш ніж достатнім.

Безумовно, простота реалізації системи відеоспостереження на основі використання DirectX для бездротових мереж вкрай важлива, особливо коли мова йде про масового користувача, що не має спеціальних знань по налаштуванню й

експлуатації традиційних систем, проте, особисто мене більше цікавить питання, наскільки реально обіцяна висока якість картинки й наскільки сильно бездротове підключення впливає на Wi-Fi, установлений удома.

У моїх тестових умовах картинку можна назвати ідеальної. Ніяких перешкод і втрат зображення. Таке відчуття, що камери підключені по проведенню. Причому, висока якість картинки зберігається навіть при значному віддаленні камери від приймача. Що ж стосується впливу на Wi-Fi, то тут ніяких проблем не виявлено. Я запускав спеціальні тести пропускної здатності Wi-Fi каналу, і можу із упевненістю говорити, що навіть при включенні всіх чотирьох камер, швидкість і якість передачі файлів по Wi-Fi не міняються. У цьому змісті ORIENT W203D4 Digital ідеальна для використання в багатоквартирних будинках, причому, зовсім не обов'язково встановлювати камери й приймач в одній кімнаті. Приймач прекрасно приймає сигнал з камер, розташованих через несучу стіну, товщиною 20 см.

Деяких з потенційних покупців хвилює питання: наскільки безпечно таке бездротове підключення? Чи не стане моя квартира надбанням всіх сусідів, у яких може бути такий же приймач? Відповідь: все дуже безпечно. Сигнал передається в зашифрованому виді. Кожна камера прив'язана до певного приймача й не може бути видна на іншому приймачі.

Чи є недоліки в ORIENT W203D4 Digital? У цілому, явно виражених проблем я не виявив. Апаратна частина працює як годинник. Були думки, що софт може підвести, але й тут усе виявилося стабільно. Звичайно, розроблювачам програмного забезпечення ще є над чим попрацювати і як розширити функціонал комплекту, проте, уже те, що вміє ORIENT W203D4 Digital сьогодні, здається мені більш ніж достатнім для користувачів, що підбирають простий набір для швидкого розгортання системи відеоспостереження.

ORIENT W240D1 Digital

У комплекті тільки одна камера й один приймач, проте, це одне із самих універсальні рішення для відеоспостереження.

На перший погляд ORIENT W240D1 Digital, саме так називається новинка, дуже схожа на цифрову відеоняньку, але з цього не виходить, що використовувати її можна тільки для спостереження за дитиною або людьми похилого віку. На мій погляд, ORIENT W240D1 Digital може стати відмінним доповненням для вже наявної системи відеоспостереження, а також може розглядатися як єдине рішення для швидкого розгортання відеоспостереження в невеликому офісі, магазині або кафе.

Чим же так цікава ORIENT W240D1 Digital? По-перше, тут використовується цифрова технологія передачі відео й аудіо сигналу, що забезпечує бездоганну якість картинки й звуку на відстані до 200 метрів. По-друге, компактний розмір, мала вага камери й приймача, повна автономність, що дозволяє харчувати камеру й приймач від убудованого акумулятора, і, нарешті, можливість підключення до чотирьох камер, а також наявність композитного аудіо-відео виходу, що дозволяє підключити пристрій до зовнішнього ресивера для реалізації функцій запису й віддаленого доступу, дозволяють розглядати ORIENT W240D1 Digital як універсальне рішення для відеоспостереження, за допомогою якого можна вирішувати широкий спектр завдань.

Знайомство з ORIENT W240D1Digital почнемо з камери, що виконана в трохи незвичайному дизайні. З однієї сторони така незвичайна форма й сполучення кольорів нагадують дитячу іграшку, що дозволяє використовувати її в дитячій кімнаті, не побоюючись, що дитина злякається класичної камери, що стежить за нею зі стелі. З іншого боку, я не можу назвати обраний дизайн дитячим. Так що ви можете самостійно вибирати, де вам використовувати даний комплект: удома або в офісі.

Незважаючи на масивну підставку, камера відрізняється компактними розмірами, а її вага з убудованим акумулятором становить усього 130 грам. Конструкція камери дозволяє встановлювати її на будь-якій горизонтальній поверхні, а при необхідності, можна закріпити її на штативі або струбцини за допомогою кріплення, розташованого в підставці камери.

Для вибору зручного ракурсу зйомки в конструкції передбачений поворотний механізм, що дозволяє повернути камеру по горизонталі й змінити кут нахилу. Камера обладнана CMOS сенсором розміром ¼” с розрішенням 380 ТВ ліній. Це еквівалентно дозволу 628x582 пікселів у системі PAL або 510x492 в NTSC. Об'єктив камери має фіксована фокусна відстань і кут огляду близько 50º, що забезпечує гарний огляд навіть у невеликих приміщеннях. Для зйомки в темряві на лицьовій стороні камери розташовані 9 інфрачервоних світлодіодів, що дозволяють вести зйомку в повній темряві на відстані до 10 метрів. У нижній частині корпуса розташовані два світлодіода, що відображають стан камери й зарядку убудованого акумулятора. Тут же розташований мікрофон.

У тильній частині корпуса розташований убудований динамік, роз’єм для підключення антени, роз’єм для підключення зовнішнього живлення й кнопка включення. Вона використовується для прив'язки камери до приймача.

Тепер розглянемо конструктивні особливості приймача, що має досить компактні розміри й вага близько 150 грам. Компактні розміри приймача вкрай важливі для повсякденного використання. У конструкції приймача передбачена підставка, що дозволяє розташувати приймач на столі або прикроватній тумбочці, а також є “вушко” для ремінця на зап'ястя.

На лицьовій стороні приймача розташований екран, розміром 2.4” і розрішенням 480x240 пікселів. Під екраном розташовані дві кнопки, відповідальні за включення живлення приймача й включення режиму двостороннього голосового зв'язку. Тут же є чотири світлодіодних індикатори, що відображають гучність дитячого плачу. Нижче розташована панель керування, за допомогою якої користувач може управляти основними параметрами системи відеоспостереження.

На бічній грані корпуса розташовані убудований мікрофон і композитний аудіо-відео вихід, якому можна використовувати для підключення приймача до великого телевізора або відеореєстратора для запису й організації віддаленого доступу.

З іншої сторони розташовані роз’єм для підключення навушників (входять у комплект), зовнішнього джерела живлення, індикатор зарядки убудованого акумулятора й вимикач живлення, що дозволяє заощадити заряд акумулятора.

Розібравшись із конструктивними особливостями ORIENT W240D1 Digital, прийшов час ближче познайомитися з налаштуваннями й реальними можливостями приладу, при використанні як як відеонянька, так і як доповнення до домашнього або офісного відеореєстратора.

У принципі, ніяких особливих налаштувань не потрібно. Для того щоб почати використовувати ORIENT W240D1 Digital досить зарядити убудований акумулятор приймача й камери. Камера, що входить у комплект, уже прив'язана до приймача. Проте, у деяких випадках може знадобитися налаштування деяких параметрів. Для цього натискаємо кнопку меню на панелі керування приймачем.

Системне меню включає всього чотири розділи. Розділ «Volume» включає можливість роздільної установки гучності динаміків на камері й на приймачі. У розділі «Display Opt» можна змінити яскравість і кольоровість картинки, включити режим цифрового збільшення й вибрати бажаний телевізійний стандарт. У розділі «Camera» можна виконати прив'язку трьох додаткових камер, вибрати камеру, що буде відображатися за замовчуванням або включити режим послідовного перемикання камер. І, нарешті, остання функція «Default» дозволяє повернути всі параметри в стан за замовчуванням.

У процесі використання ORIENT W240D1 Digital я звернув увагу на деякі особливості. Наприклад, приймач не має убудованого детектора руху. У перший момент це виявилося дивним, але потім стало зрозуміло, що якщо камера буде реагувати на кожний рух сплячої дитини, то батьки збожеволіють. Замість цього, тут використовується детектор звуку, що відображає за допомогою чотирьох світлодіодів гучність звуку. Наприклад, якщо дитина просто закректала, то займеться всього один світлодіод, що змусить батьків просто звернути увагу. Якщо ж дитина заплаче, то всі чотири індикатори змусять батьків вжити заходів.

Важливо відзначити підтримку сплячого режиму. У цьому режимі екран приймача перебуває у виключеному стані, що дозволяє заощаджувати заряд убудованого акумулятора, і не відволікати зайвий раз батьків. Екран включається, як тільки маля заплаче.

Якість картинки досить високо й повністю відповідає якості камер цього рівня. Є невелика проблема з кольором, але для даного класу пристроїв це зовсім неважливо. Куди важливіше, наскільки якісної картинка виходить в умовах повної темряви, і тут убудована ІЧ-підсвічування виявляється як не можна до речі. Зображення виходить досить чітким, при цьому використовувані світлодіоди не дають характерного червоного світла, що може налякати дитини.

Якість бездротового каналу таке ж високе, як і в комплекті ORIENT W203D4 Digital. Я не виявив ніяких проблем з перешкодами або втратою картинки поза залежністю від того, як далеко я віддалявся від камери. Вплив на домашній Wi-Fi не виявлено. Говорячи про можливості комплекту необхідно сказати про час автономної роботи. Однієї зарядки акумулятора, убудованого в камеру, вистачає на 3 години. Час автономної роботи приймача значно вищий й залежить від яскравості екрана й підтримки сплячого режиму.

Тепер поговоримо про можливість інтеграції ORIENT W240D1 Digital в існуючу систему відеоспостереження. Навіщо це потрібно? Найчастіше це використовують для запису поводження найнятої няньки для дитини. У цьому змісті ORIENT W240D1 Digital підходить як не можна краще. Непримітний дизайн, можливість установки в зручному місці без необхідності підключення до мережі, а також можливість вибору зручного ракурсу зйомки й запис зі звуком, роблять цей комплект ідеальним вибором для рішення поставленого завдання. Як підключити ORIENT W240D1 Digital до відеореєстратора? Дуже просто. У комплект входить композитний аудіо-відео кабель, обладнаний двома парами (”тато”+”мама”) рознімань.

Налаштування запису виробляється безпосередньо на відеореєстраторі. Звичайно ви можете вибрати режим постійного запису або запису по події. Як

краще зробити, вибір за вами. Я ж відзначу, що деякі моделі відеореєстраторів підтримують можливість перегляду й запису на iOS або Android пристроях. Мені здається, можливість у будь-який момент дістати свій смартфон і подивитися, чим займається ваша дитина або чи вчасно нянька погодувала його або уклала спати, здається мені дуже важливою причиною для установки такого комплекту.

Бездротова система відеоспостереження Danrou KCM-6370DRx4

Бездротова система відеоспостереження для будинку, дачі, офісу, торговельного залу або невеликого складу:

– Комплект складається з монітора-реєстратора 7” і чотирьох бездротових камер.

– Найкраща якість картинки забезпечується, завдяки новітній бездротовій цифровій технології передачі відео.

– Відсутність проводів дозволяє легко й швидко встановити спостереження без наслідків для ремонту навіть новачкові за 15 хвилин.

– Чотири кольорові вуличні камери – 420 ТВЛ, оснащені ІЧ підсвічуванням для зйомки вночі.

– Запис відео на SD карту до 16 ГБ (7 доби по русі).

– Новітня бездротова технологія дозволяє працювати на частоті 2,4 ГГц, не створюючи перешкоди Wi-Fi, і Bluetooth мережам.

– Завдяки захищеному сигналу досягається велика відстань роботи між монітором і камерою – 300 метрів.

Danrou KCM-6370DRx4 – це бездротова система відеоспостереження, призначена для відеоспостереження в невеликих приміщеннях, офісах, приватних будинках, невеликих складах, авто-мийках, і відкритих територіях. Даний комплект складається із чотирьох бездротових відеокамер і монітора-реєстратора. Особливість системи полягає в тому, що вона швидко монтується й легко настроюється. Працює система по наступному принципі: камера передає відео по радіоканалі на приймач убудований у монітор. Приймач приймає зображення й виводить його на екран, а при необхідності записує відео на SD карту.

Бездротова технологія передачі відео:

– Завдяки бездротовій технології, Ваші приміщення не постраждають від установки, і збережуть свій зовнішній вигляд.

– Відсутність кабелів дозволяє легко й швидко встановити систему навіть новачкові за лічені мінути.

– Цифровий спосіб передачі даних забезпечує відмінна якість картинки й звуку.

– Завдяки новітній технології бездротова цифрова передача не впливає на якість Wi-Fi, і Bluetooth мереж, а так само інших мереж у частоті 2,4 Ггц.

– Дана бездротова технологія абсолютно безпечна для здоров'я.

– Зашифрований відеосигнал захищений від несанкціонованого доступу, його неможливо перехопити.

– Сигнал на 100% захищений від усіляких перешкод, картинка завжди чітка.

– Система проінформує у випадку втрати сигналу звуком, якщо ви помістите камеру за межу досяжності.

– Швидкість передачі даних становить 2 Мб/сек.

– Система працює на частоті 2,4 Ггц, загальнодоступна й не вимагає ліцензії на використання.

– Завдяки захищеному сигналу досягається велика відстань роботи між монітором і камерою – 300 метрів при прямої видимості.

Бездротова кольорова камера:

– Ергономічний і строгий дизайн камери впише в будь-який інтер'єр або екстер'єр.

– Кольорові матриці Sony розміром 1/4” і CMOS сенсором мають розрішення 420 ТВЛ.

– Конструкцією камер передбачене зовнішнє застосування, вони легко тримають високу вологість і дуже низькі температури українських зим.

– У камери убудований датчик руху, що забезпечує подвійну перевірку руху: програмну й інфрачервону від датчика.

– Камери оснащені мікрофоном і динаміком, що дозволяє не тільки спостерігати за приміщенням і прослуховувати його, але й відправляти голосові повідомлення на камери.

– Інфрачервоні світлодіоди дозволяють камерам знімати в темний час доби, забезпечуючи пристойну видимість на відстані до 4,5 метрів.

Монітор-реєстратор:

– ЖК-дисплей розміром 7 дюймів забезпечує максимальний розрішення 640?480 пікселів.

– Максимальна швидкість запису 25 кадрів у секунду.

– При записі можна вибирати більше низька якість 320x240 пікселів, якщо необхідно заощаджувати місце на носії інформації.

– Є присутнім можливість цифрового 2-х кратні наближення відео.

– Відео записується на SD карту ємністю до 16 Гб. Це 48 годин безперервного запису, і більше тижня запису по русі.

– Система підтримує до 4-х камер. Монітор покаже картинку відразу із всіх камер у режимі квадратора.

– Якщо камера, або датчик у неї убудований виявляють рух, монітор видає звукове попередження.

– Інтерфейс монітора й меню налаштувань інтуїтивно зрозумілі й у них абсолютно неможливо заплутатися, потрібні функції легко й швидко настроюються.

– Можливі режими запису по русі, за розкладом, ручний режим і циклічний запис.

– Присутні й налаштування для комфорту, наприклад картинки заставок у режимі відсутності активності, або каскадний режим відображення камер.

– Монітор попередить Вас, у випадку, якщо рівень сигналу критично низок, або загублений.

– Наявність A/V виходу дозволяє транслювати відео на телевізор, зовнішній відеореєстратор або професійний монітор.

– При підключенні до телевізора можна вибрати телевізійний стандарт PAL або SECAM.

– Пульт ДУ допоможе на відстані управляти монітором, якщо ви захочете прикріпити його на стіну, або просто розташувати у віддаленому місці.

Висновок

У цьому огляді я розглянув чотири комплекти бездротового відеоспостереження, кожний з яких має свої унікальні особливості, що дозволяють використовувати їх для рішення того або іншого завдання. Наприклад, не можу сказати, що комплект ORIENT W802G4 виявився дуже цікавим з погляду можливості бездротового підключення. У цьому змісті він програє цифровим системам. Але при цьому ніщо не заважає нам використовувати провідне підключення камер, при цьому з погляду ціни цей комплект поза конкуренцією.

Комплект ORIENT W203D4 Digital цікавий не тільки високою якістю картинки й більшим радіусом дії бездротового підключення. Не менш цікавим виявився мініатюрний дизайн використовуваних камер, можливість заміни об'єктива й, звичайно ж, USB приймач, що дозволяє за лічені мінути зібрати комп'ютерну систему відеоспостереження на базі будь-якого комп'ютера або ноутбука. Дана система відеоспостереження підтримує базовий набір функцій, достатній для рішення широкого спектра завдань. Крім цього, важливо нагадати, що ORIENT W203D4 Digital підтримує можливість віддаленого доступу до системи відеоспостереження через інтернет.

І, нарешті, комплект ORIENT W240D1 Digital. На перший погляд, звичайна цифрова відеонянька. Її функціонал досить продуманий і забезпечує зручний і ефективний спосіб для спостереження за сплячою дитиною. Однак, завдяки можливості підключення до чотирьох бездротових камер і інтеграції в існуючу систему відеоспостереження, даний комплект можна використовувати для рішення більше широкого кола завдань, причому не тільки в домашнім застосуванні, але в невеликому офісі.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Оскільки потрібно розробити просту та легку у користуванні програму, яка б виконувалась під операційною системою Windows, то для її реалізації я обрав Builder C++. Існує велике число бібліотек написаних під Builder C++ , тому це одна з важливих причин вибору мови програмування. Середовище Builder C++ досить просте в користуванні, його вихідний код значно менше по об'єму в порівнянні з Delphi чи деякими іншими програмами такого типу. Досить легко організувати взаємодію між модулями програм, об'єктно-орієнтований підхід дає можливість значно скоротити код програми, а отже і час його виконання.

На заміну старого розробленого набору елементів управління у Builder C++ інтегрована бібліотека візуальних компонентів VCL, представлених на палітрі компонентів. Після переносу на форму методом перетягування (drag-and-drop) компоненти відразу становляться діючими об'єктами вашої програми. Окрім типізованих інтерфейсних елементів Windows (кнопки, смуги прокручування, редагуємі текстові області, прості та комбіновані списки, та інше) у бібліотеку включені елементи підтримки діалогових вікон, обслуговування баз даних та багато іншого. Можливо не тільки модифікувати поведінку існуючих компонентів, але і будувати нові.

Builder C++ підтримує останні розширення стандарту мови C++ та забезпечує швидку компіляцію та складання 32-розрядних програм для Windows. Результуючі програми оптимізовані з точки зору швидкості виконання програм та затрат пам'яті. Зручний відладгоджувальник (з асемблерним вікном, можливістю крокового виконання, завдання точок зупинки, трасування та інше) повністю інтегрований у систему проектування. Дизайнер форм, редактор коду, інспектор об'єктів та інші інструменти зостаються доступними під час виконання програми, саме через це вносити зміни до коду можна прямо у процесі відлагодження.

Дизайнер форм, Інспектор об'єктів і інші засоби залишаються доступними під час роботи програми, тому вносити зміни можна в процесі відлагодження.

Builder C++ поставляється в трьох варіантах: Standard (стандартний), Professional (для професіоналів розробників, орієнтованих на мережеву архітектуру) і Client/Server Suite (для розробки систем в архітектурі клієнт/сервер). Останні два варіанти доповнюють стандартний початковими текстами візуальних компонентів, різномасштабним словником даних, новими функціями мови запитів SQL для бази даних, пакетом підтримки систем Internet, службою моніторингу програм, а також рядом інших засобів.

Builder C++ підтримує зв'язок з різними базами даних 3-х видів: dBASE і Paradox: Sybase, Oracle, InterBase і Informix; Excel, Access, FoxPro і Btrieve. Механізм BDE (Borland Database Engine) додає обслуговуванню зв'язків з базами даних дивовижну простоту і прозорість. Провідник Database Explorer дозволяє зображати зв'язки і об'єкти баз даних графічно. Використовуючи компоненти баз даних, я побудував електронний записник згідно таблиці dBASE за півгодини роботи на комп'ютері. Спадкоємство готових форм і їх "підгонка" під специфічні вимоги помітно скорочують тимчасові витрати на вирішення подібних завдань.

Довідкова служба Builder C++ надавала мені допомогу в цій і багатьох інших подібних ситуаціях. Є повний опис кожного управляємого компонента, включаючи списки властивостей і методів, а також численні приклади. Виклад матеріалу в книзі був значно покращуваний і систематизований завдяки відомостям, почерпнутим мною з довідкової служби.

Завдяки засобам управління проектами, двосторонній інтеграції додатку і синхронізації між засобами візуального і текстового редагування, а також вбудованому відладнику (з асемблерним вікном прокрутки, покрокового виконання, точок останову, трасуванням і тому подібне) – Builder C++ корпорації Borland надає собою вражаюче середовище розробки, яка, мабуть, витримає конкурентну боротьбу з такими модними продуктами як Developer Studio фірми Microsoft.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускну кваліфікаційну роботу за другим (магістерським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи мережевого відеоспостереження на основі використання DirectX.

В процесі розробки випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти необхідно виконати наступний обсяг роботи:

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику побудови системи контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран ЕОМ повідомлень про некоректні дії користувача та нестандартні ситуації в роботі технологічного обладнання;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

ж) розробити заходи по охороні праці при впровадженні та експлуатації системи, а також розробити заходи з цивільного захисту;

з) сформувати висновки про виконаний обсяг робіт та одержані результати.

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

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.

3.2 Розробка структурної схеми

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 3.1. На ній показано структуру системи відеоспостереження на основі використання DirectX для бездротових мереж.

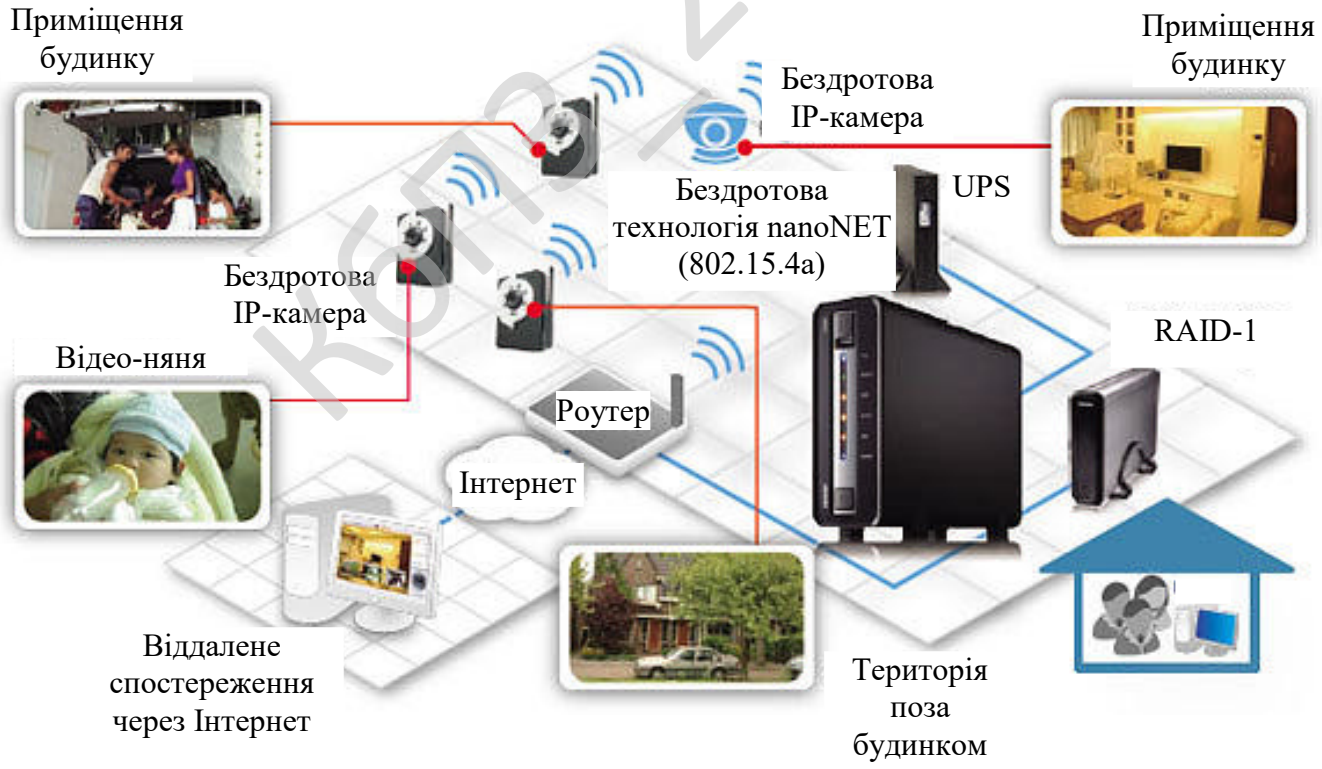

Рисунок 3.1 – Структурна схема системи

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.

3.3 Розробка функціональної схеми

Програмно-апаратний комплекс об’єкту відеоспостереження на основі використання DirectX для бездротових мереж є комплектом устаткування, що розміщується на території об’єкту відеоспостереження на основі використання DirectX для бездротових мереж та забезпечує первинний збір і обробку відеосигналу, його подальше зберігання та передачу в захищеному вигляді з використанням мережі передавання даних до центральних серверних комплексів.

Конфігурація програмно-апаратного комплексу об’єкту відеоспостереження на основі використання DirectX для бездротових мереж включає:

– дві відеокамери з роздільною здатністю не менш як 640 х 480, з можливістю передачі звукового сигналу та швидкістю відеопотоку не менш як 25 кадрів на секунду, можливістю кольорової відеозйомки, настінного/стельового кріплення, а також обов’язковою фіксацією дати та часу зйомки;

– пристрій для запису та передавання відеосигналу, який здатен забезпечити запис із роздільною здатністю не менш як 640 х 480 із швидкістю відеопотоку не менш як 25 кадрів на секунду, тривалістю не менше 120 годин з кожної камери та передавання відеосигналу до центру обробки даних з роздільною здатністю та швидкістю залежно від якості каналу передавання даних, але не менш як 320 х 240 із швидкістю відеопотоку не менш як 15 кадрів на секунду;

– система безперебійного електропостачання обладнання програмно-апаратного комплексу об’єкту відеоспостереження на основі використання DirectX для бездротових мереж протягом не менш як однієї години;

– необхідне комутаційне обладнання та з’єднувальні кабелі (довжина кабелів між камерами та пристроєм для запису і передаванням відеосигналу не повинна перевищувати 15 метрів);

– програмне забезпечення, необхідне для функціонування програмно-апаратного комплексу.

Функціональна схема розробленої системи зображена на рисунку 3.2.

З рисунку видно, що розроблена система складається з наступних частин:

– блок приймання та запису відеосигналу;

– блок обслуговування користувачів та трансляції відеосигналу (веб-сайт).

На етапі розроблення і впровадження системи відеоспостереження функціональні блоки можуть бути об’єднані в довільні логічні функціональні модулі. При такому об’єднанні кожен з модулів повинен бути функціонально незалежним від інших модулів. При цьому допускається створення територіально розподіленої системи функціональних модулів для забезпечення безвідмовності роботи системи відеоспостереження в цілому.

Для підвищення рівня безвідмовності роботи системи відеоспостереження кожен функціональний мережевий вузол центрального серверного комплексу повинен дублюватися. Застосування мережевих технологій і протоколів безвідмовного включення устаткування повинне гарантувати коректну роботу центрального серверного комплексу в разі виходу з ладу одного з двох мережевих пристроїв, з яких складається відповідний функціональний вузол.

Для захисту від мережевих загроз і атак (зокрема типу DoS та DDoS) обладнання центрального серверного комплексу повинне мати відповідне мережеве обладнання. Програмне забезпечення зазначеного обладнання повинне забезпечувати обробку мережевого трафіку на швидкості підключення до мережі передавання даних і мати у своєму складі достатню кількість мережевих інтерфейсів для підключення.

Інтерфейс користувача системи відеоспостереження на основі використання DirectX для бездротових мереж

Блок приймання та запису відеоінформації

- безперервне приймання відео- та аудіопотоків з програмно-апаратних комплексів;
- зберігання отриманих даних в архіві відеозаписів протягом не менш як 120 годин з кожної камери відеоспостереження;
- авторизація джерела відеопотоку перед отриманням даних;
- заповнення цілісності відеопотоку шляхом дозавантаження відсутніх фрагментів з архіву програмно-апаратного комплексу;
- наявність можливості перегляду відеозаписів архіву, в тому числі з використанням пошуку.

Блок обслуговування користувачів та трансляції відеосигналу

- трансляція відеопотоків для інтернет-користувачів;
- розподіл навантаження за кластером серверів;
- використання кешування для оптимізації завантаження магістральних каналів;
- доступ до веб-порталу з використанням браузерів та мобільних пристроїв (Android, iOS);
- попередня реєстрація з можливістю вибору камер відеоспостереження;
- збереження вибраних камер відеоспостереження у списках відтворення;
- швидке перемикання користувача на одну з попередньо обраних камер відеоспостереження;
- пріоритетний доступ до всіх камер відеоспостереження для групи спеціальних користувачів;
- об’єднання на головній сторінці сайту декількох навігаційних систем;
- пошук за всіма географічними назвами;
- перегляд відеоматеріалів у режимі прямої трансляції з будь-якої попередньо обраної камери відеоспостереження;
- функція додавання камер в обране;
- використання тесту CAPTCHA для забезпечення додаткового рівня захисту від великого потоку запитів;
- використання системи обмеження доступу за набором параметрів (комплексна перевірка, що передбачає обмеження кількості підключень з однієї IP-адреси за визначений період).

Рисунок 3.2 – Функціональна схема системи

Блок приймання та запису відеоінформації повинен відповідати таким функціональним вимогам:

– безперервне приймання відео- та аудіопотоків з програмно-апаратних комплексів;

– зберігання отриманих даних в архіві відеозаписів протягом не менш як 120 годин з кожної камери відеоспостереження;

– авторизація джерела відеопотоку перед отриманням даних;

– заповнення цілісності відеопотоку шляхом дозавантаження відсутніх фрагментів з архіву програмно-апаратного комплексу;

– наявність можливості перегляду відеозаписів архіву, в тому числі з використанням пошуку.

Блок обслуговування користувачів та трансляції відеосигналу (веб-сайт) повинен відповідати таким функціональним вимогам:

– трансляція відеопотоків для інтернет-користувачів;

– розподіл навантаження за кластером серверів;

– використання кешування для оптимізації завантаження магістральних каналів;

– доступ до веб-порталу з використанням браузерів (Internet 7.0 і вище, Firefox 7.0 і вище, Opera 10.0 і вище, Chrome 10.0.648 і вище) та мобільних пристроїв (Android, iOS);

– попередня реєстрація з можливістю вибору камер відеоспостереження для здійснення перегляду;

– збереження вибраних камер відеоспостереження у списках відтворення;

– швидке перемикання користувача на одну з попередньо обраних камер відеоспостереження;

– пріоритетний доступ до всіх камер відеоспостереження для групи спеціальних користувачів;

– об’єднання на головній сторінці сайту декількох навігаційних систем;

– пошук за всіма географічними назвами;

– перегляд відеоматеріалів у режимі прямої трансляції з будь-якої попередньо обраної камери відеоспостереження;

– функція додавання камер в обране;

– використання тесту CAPTCHA для забезпечення додаткового рівня захисту від великого потоку запитів;

– використання системи обмеження доступу за набором параметрів (комплексна перевірка, що передбачає обмеження кількості підключень з однієї IP-адреси за визначений період).

Функціональні вимоги до мережі передавання даних

Конфігурація каналів зв'язку мережі передавання даних включає:

– канал зв'язку об'єкту відеоспостереження на основі використання DirectX для бездротових мереж для передавання відеосигналу до центрального серверного комплексу з пропускною здатністю за напрямом передавання даних до 512 Кбіт на секунду, інтерфейс підключення на об'єкті відеоспостереження на основі використання DirectX для бездротових мереж Ethernet 10/100 Мбіт на секунду (RJ45);

– вхідний канал зв'язку центру обробки даних для отримання відеосигналу з програмно-апаратного комплексу з пропускною здатністю за напрямом отримання даних не менш як 15 Гбіт на секунду;

– вихідні канали зв'язку центру обробки даних для трансляції відеосигналу в Інтернеті із сумарною пропускною здатністю не менш як 80 Гбіт на секунду;

– канал зв'язку між центром обробки даних та центром керування системи відеоспостереження із пропускною здатністю не менш як 15 Гбіт на секунду.

Канали зв'язку повинні відповідати таким функціональним вимогам:

– організація тунельних каналів зв'язку між об'єктами відеоспостереження на основі використання DirectX для бездротових мереж, центральним серверним комплексом і ситуаційним центром системи

відеоспостереження з використанням технологій IP/MPLS, L2VPN, L3VPN та інших;

– забезпечення цілодобового обслуговування передачі даних каналами зв'язку на всіх вузлах мережі передавання даних;

– наявність централізованої диспетчерської служби, що працює в цілодобовому режимі, для обслуговування каналів передачі даних;

– мережа передавання даних у частині центрального серверного комплексу повинна мати повнопов'язану топологію архітектури побудови, яка забезпечує обмін інформацією між об'єктами відеоспостереження на основі використання DirectX для бездротових мереж та вузлами центрального серверного комплексу і ситуаційним центром системи відеоспостереження без послуги, що додатково замовляється з високим рівнем надійності;

– зона відповідальності оператора зв'язку – від інтерфейсу мережевого устаткування в центральному серверному комплексі і ситуаційному центрі системи відеоспостереження до інтерфейсу кінцевого устаткування.

Вимоги до ситуаційного центру системи відеоспостереження

Ситуаційний центр системи відеоспостереження повинен забезпечувати виконання завдань з управління процесами функціонування всіх складових частин системи відеоспостереження і нагляд за їх характеристиками, здійснення контролю за відеопотоками, що передаються з веб-камер, параметрів функціонування програмно-апаратних комплексів і складових частин центрального серверного комплексу, а також стану підключення обладнання.

У разі виявлення некоректного функціонування системи відеоспостереження ситуаційний центр повинен визначити джерело несправності.

Функціональними вимогами до ситуаційного центру системи відеоспостереження є:

– приймання діагностичної інформації про складові частини системи відеоспостереження;

– відображення діагностичної інформації на всіх пристроях системи відеоспостереження;

– здійснення нагляду за змінами заданого набору параметрів;

– забезпечення зворотного зв’язку із службою технічної підтримки для розв’язання проблем.

Моніторинг центрального серверного комплексу

Моніторинг центрального серверного комплексу здійснюється шляхом внутрішнього контролю за працездатністю серверного обладнання.

Серверний комплекс повинен мати такі параметри:

– стан використання пам’яті;

– доступність у мережі;

– кількість зайнятого місця за розділами жорстких дисків;

– кількість підключених каналів (камер).

Моніторинг програмно-апаратного комплексу

Під час проведення моніторингу програмно-апаратного комплексу встановлюється наявність таких відомостей:

1. У період здійснення відеотрансляцій для кожної об’єкту відеоспостереження на основі використання DirectX для бездротових мереж:

– номер об’єкту відеоспостереження на основі використання DirectX для бездротових мереж;

– місце її розташування;

– мережева адреса об’єкту відеоспостереження на основі використання DirectX для бездротових мереж;

– номінальна швидкість доступу до мережі передачі даних;

– фактична швидкість доступу до мережі передачі даних;

– наявність доступу програмно-апаратного комплексу до мережі передачі даних;

– тривалість періоду доступу програмно-апаратного комплексу до мережі передачі даних або його відсутності;

– час початку зйомки і збирання записів;

– час закінчення зйомки і збирання записів;

– сумарна тривалість зібраних записів (час);

– сумарний об’єм зібраних записів (Мбайт).

2. У період здійснення відеотрансляцій для повідомлень про проблеми, що виникають під час перегляду відеотрансляцій:

– кількість повідомлень про проблеми перегляду відеотрансляцій;

– кількість відеокамер, стосовно яких надійшли повідомлення про проблеми, що виникають під час перегляду відеотрансляцій;

– кількість відеокамер, стосовно яких повідомлення про проблеми перегляду відеотрансляцій були підтверджені.

3. У період здійснення відеотрансляцій для єдиного порталу:

– доступність/недоступність єдиного порталу в Інтернеті (період проведення перевірки – не більше 10 хвилин);

– тривалість періоду доступності єдиного порталу в Інтернеті або її відсутності.

4. У період зберігання зібраних записів відеотрансляцій:

– сумарна тривалість записів відеотрансляцій, зібраних у процесі роботи системи відеоспостереження (час);

– сумарний об’єм записів відеотрансляцій, зібраних у процесі роботи системи відеоспостереження (Мбайт);

– сумарна тривалість записів відеотрансляцій, що зберігаються на відповідний час;

– сумарний об’єм записів відеотрансляцій на даний час (Мбайт).

Вимоги до забезпечення цілісності інформаційних ресурсів та захисту інформації від несанкціонованого доступу

Для унеможливлення несанкціонованого доступу до системи відеоспостереження, використання інформації не за призначенням та порушення

її цілісності створюється система захисту інформації від несанкціонованого доступу.

Захист інформації в системі відеоспостереження забезпечується відповідно до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373.

Захист інформації здійснюється за такими принципами:

– безперервність процесу захисту шляхом забезпечення захисту інформації від несанкціонованого доступу протягом усього періоду функціонування системи відеоспостереження;

– керованість процесу захисту шляхом забезпечення оперативних режимів контролю за станом виконання правил доступу до системи відеоспостереження та прийняття відповідних рішень у разі порушення таких правил;

– комплексне використання засобів та методів захисту інформації від несанкціонованого доступу шляхом спільного використання технічних, програмних, організаційних засобів захисту, а також відповідних правил доступу до інформації.

Система захисту інформації від несанкціонованого доступу повинна виконувати такі функції:

– ідентифікація користувачів мережі, захист параметрів ідентифікації користувачів і параметрів;

– розмежування доступу до ресурсів і процесів у системі відеоспостереження;

– забезпечення цілісності інформаційних ресурсів;

– захист носіїв інформації від несанкціонованого доступу;

– забезпечення функцій адміністрування в системі захисту інформації від несанкціонованого доступу;

– захист від шкідливих комп’ютерних програм.

Необхідно визначити комплекс адміністративних заходів для дотримання відповідних вимог до рівня надійності приміщень, в яких розташовуються елементи системи відеоспостереження, та регламентації дій персоналу.

3.4 Розробка діаграми процесів

Діаграма взаємодії процесів розробленої системи зображена на рисунку 3.3. Процеси взаємодіють наступним чином. Спершу запускається процес виведення головного вікна програми. Цей процес взаємодіє з наступними процесами:

– Процес ведення та перегляду журналу подій.

– Процес відслідковування руху.

– Процес встановлення фільтру.

– Процес вибору пристроїв відеоспостереження.

– Процес встановлення загальних параметрів.

Процес відслідковування руху взаємодіє з процесом підняття тривоги, у випадку несанкціонованого руху на охороняє мій території, або об’єкті.

Процес встановлення фільтру взаємодіє з наступними процесами:

– Процес встановлення умови підняття тривоги.

– Процес встановлення області контролю.

– Процес встановлення області чутливості реагування системи на рухи.

Процес вибору пристроїв відеоспостереження взаємодіє з наступними процесами:

– Процес перегляду раніше записаного відео.

– Процес активізування пристрою відеоспостереження.

Останній процес взаємодіє з наступними процесами:

– Процес відображення області контролю.

– Процес відображення поточного відео.

– Процес запису відео.

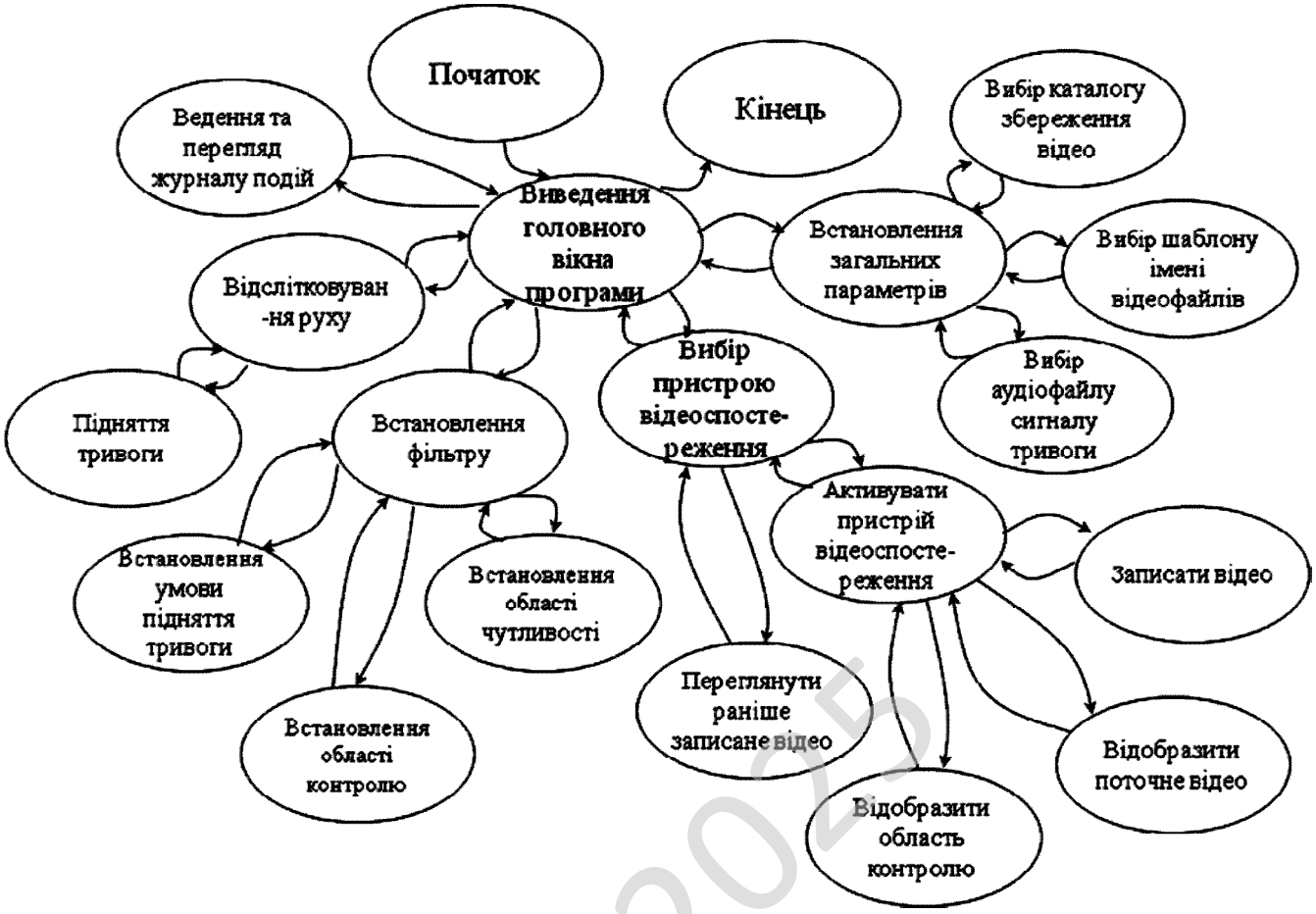

Рисунок 3.3 – Діаграма взаємодії процесів

Процес встановлення загальних параметрів взаємодіє з наступними процесами:

– Процес вибору каталогу для збереження відео.

– Процес вибору шаблону імені відеофайлів.

– Процес вибору аудіофайлу сигналу тривоги.

Таким чином, розглянувши опис системи, структурну, функціональну схеми системи, та діаграму взаємодії процесів перейдемо до опису блок-схем основної програми, та підпрограм, які використовуються, для реалізації системи.

4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Розглянемо алгоритм роботи основної програми, блок-схема якої, зображена на рисунку 4.1.

З рисунку видно, що після запуску програми спочатку відбувається виведення основного вікна програми. Потім здійснюється вибір пристрою відеоспостереження. Якщо пристрій вибрано, пропонується переглянути раніше записане відео з вибраного пристрою.

Після цього пропонується виконати активацію пристрою спостереження. Якщо активація не виконана, можливо провести операції по налаштуванню системи.

При активації пристрою спостереження відбувається виконання наступних операцій:

– Виведення відеозображення з пристрою на екран.

– За потреби відображається область контролю, відзначена у налаштуваннях фільтрації та відбувається виведення на екран цієї області.

– За потреби відбувається запис відео з пристрою на жорсткий диск.

– Якщо в процесі роботи система помічає підозрілий рух, видається сигнал тривоги.

Також програма дозволяє виконувати наступні дії:

– Встановити параметри фільтрації відео.

– Змінити загальні параметри програми.

– Переглянути журнал подій.

– Записати дію та час її виникнення у журнал подій.

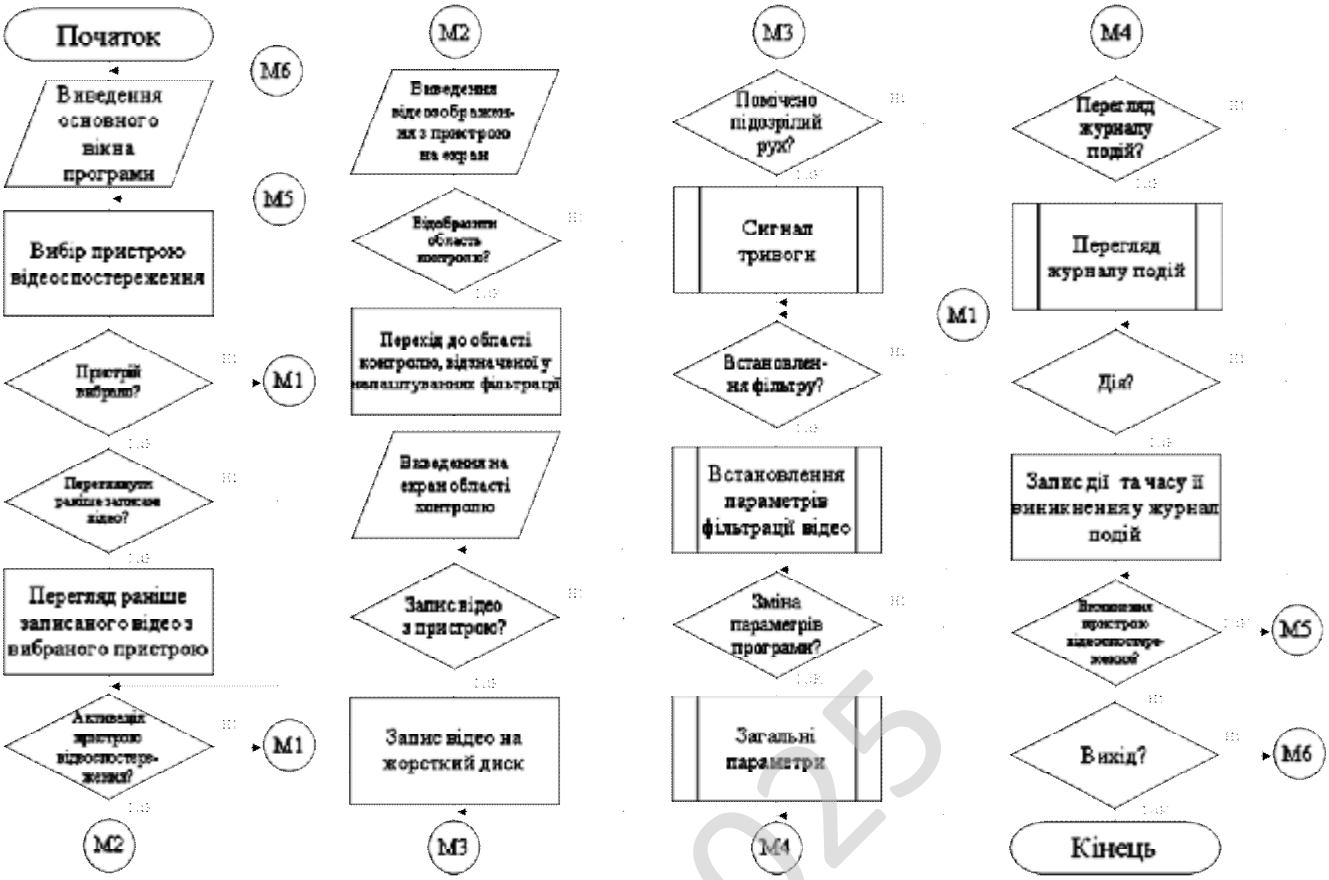

Рисунок 4.1 – Блок-схема основної програми

Наведемо частину коду підпрограми вибору пристрою для відеоспостереження:

```
TSetDeviceForm *SetDeviceForm;
//---------------------------------------------------------------------------
--
__fastcall TSetDeviceForm::TSetDeviceForm(TComponent* Owner)
        : TForm(Owner)
{
}
//---------------------------------------------------------------------------
--
void __fastcall TSetDeviceForm::FormShow(TObject *Sender)
{
  //зберегти поточні налаштування
  Sets.SaveToFile("prev.cfg");

  UpdateState();
```

```
  // перерахування пристроїв
  char szDeviceName[80];
  char szDeviceVersion[80];
  DeviceSelect->Items->Clear();
  for (int wIndex = 0; wIndex < 10; wIndex++)
  {
    if (capGetDriverDescription (wIndex, szDeviceName,
        sizeof (szDeviceName), szDeviceVersion,
        sizeof (szDeviceVersion)))
    {
        // Додати ім’я до списку встановлених драйверів захвату
        // та потім дозволити користувачеві вибрати драйвер для
використання
        DeviceSelect->Items-
>Add(AnsiString(szDeviceName)+"("+AnsiString(szDeviceVersion)+")");
        if(Sets.DevIndex == wIndex) DeviceSelect->Text =
AnsiString(szDeviceName)+"("+AnsiString(szDeviceVersion)+")";
    }
  }
}
//---------------------------------------------------------------------
--
void __fastcall TSetDeviceForm::DeviceSelectSelect(TObject *Sender)
{
   //update device index
   Sets.DevIndex = DeviceSelect->ItemIndex;
   UpdateState();
}
//---------------------------------------------------------------------
--
void __fastcall TSetDeviceForm::OkBitBtnClick(TObject *Sender)
{
  DeleteFile("prev.cfg");
  Close();
}
//---------------------------------------------------------------------
--
void __fastcall TSetDeviceForm::CancelBitBtnClick(TObject *Sender)
{
  Sets.LoadFromFile("prev.cfg");
  DeleteFile("prev.cfg");
  Close();
```

```
}
//---------------------------------------------------------------------------
--
void __fastcall TSetDeviceForm::VideoSrcBitBtnClick(TObject *Sender)
{
   capDlgVideoSource(Sets.hCaptureW);
}
//---------------------------------------------------------------------------
--
void __fastcall TSetDeviceForm::FormatBitBtnClick(TObject *Sender)
{
   capDlgVideoFormat(Sets.hCaptureW);
   capGetStatus(Sets.hCaptureW, &Sets.CapStatus, sizeof (CAPSTATUS));

   Sets.VideoFormatSize = capGetVideoFormatSize(Sets.hCaptureW);
   if(Sets.VideoFormat){
      delete[] Sets.VideoFormat;
      Sets.VideoFormat = NULL;
   }
   if(Sets.VideoFormatSize > 0){
      Sets.VideoFormat = (LPBITMAPINFO) new BYTE[Sets.VideoFormatSize];
      capGetVideoFormat(Sets.hCaptureW, Sets.VideoFormat,
Sets.VideoFormatSize);
   }
}
//---------------------------------------------------------------------------
--
void __fastcall TSetDeviceForm::DisplayBitBtnClick(TObject *Sender)
{
   capDlgVideoDisplay(Sets.hCaptureW);
}
//---------------------------------------------------------------------------
--
void TSetDeviceForm::UpdateState()
{
   //під'єднати новий пристрій
   capDriverDisconnect (Sets.hCaptureW);
   bool fOK = capDriverConnect(Sets.hCaptureW, Sets.DevIndex);
   if(fOK){
      //отримати заголовки драйверу
      capDriverGetCaps(Sets.hCaptureW, &Sets.CapDrvCaps, sizeof
(CAPDRIVERCAPS));
```

```
            //отримати заголовки вікна
            capGetStatus(Sets.hCaptureW, &Sets.CapStatus, sizeof (CAPSTATUS));
            //отримати доступні діалоги для драйверу
            // діалогове вікно для джерела відеосигналу
            VideoSrcBitBtn->Visible = false;
            if (Sets.CapDrvCaps.fHasDlgVideoSource)
               VideoSrcBitBtn->Visible = true;
            // діалогове вікно для формату відео
            FormatBitBtn->Visible = false;
            if (Sets.CapDrvCaps.fHasDlgVideoFormat)
               FormatBitBtn->Visible = true;
            // діалогове вікно для відеозображення
            DisplayBitBtn->Visible = false;
            if (Sets.CapDrvCaps.fHasDlgVideoDisplay)
               DisplayBitBtn->Visible = true;
         }
      }
```

Окремо розглянемо роботу підпрограми встановлення параметрів фільтрації відео. Її блок-схема наведена на рисунку 4.2.

Після виведення в основній програмі вікна параметрів фільтрації можна провести наступні налаштування:

– Вибрати область контролю після виведення на екран зображення з камери.

– Вибрати область чутливості.

– Вибрати умови збереження зображення та подання сигналу тривоги.

Крім області чутливості також вибираються значення чутливості у процентах та квадрати чутливості.

Для вибору умов збереження зображення та подання сигналу тривоги визначаються такі параметри, як період захвату, поріг руху, час руху, період збереження зображення.

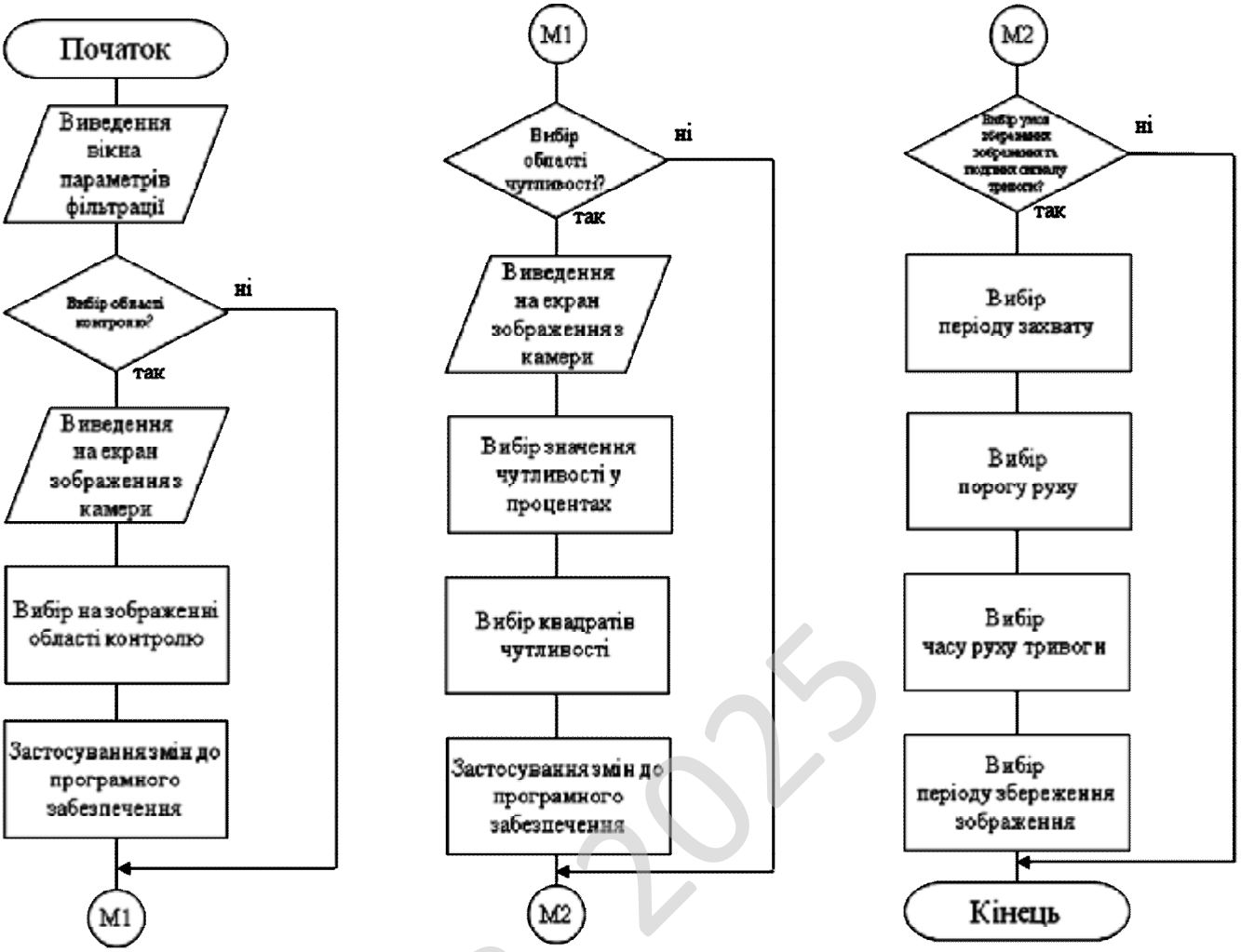

Рисунок 4.2 – Блок-схема підпрограми встановлення параметрів фільтрації відео

Наведемо частину коду підпрограми для фільтрації відеозображення:

```
TSetFilterForm *SetFilterForm;
int SRX1, SRX2, SRY1, SRY2;
int CurSens = -1;
//---------------------------------------------------------------------------
--
__fastcall TSetFilterForm::TSetFilterForm(TComponent* Owner)
        : TForm(Owner)
{
}
//---------------------------------------------------------------------------
--
```

```
void __fastcall TSetFilterForm::OkBitBtnClick(TObject *Sender)
{
   DeleteFile("prev.cfg");
   Close();
}
//---------------------------------------------------------------------------
--
void __fastcall TSetFilterForm::CancelBitBtnClick(TObject *Sender)
{
   Sets.LoadFromFile("prev.cfg");
   DeleteFile("prev.cfg");
   Close();
}
//---------------------------------------------------------------------------
--
void __fastcall TSetFilterForm::SRPBPaint(TObject *Sender)
{
   DrawSR();
}
//---------------------------------------------------------------------------
--
void __fastcall TSetFilterForm::SRPBMouseMove(TObject *Sender,
      TShiftState Shift, int X, int Y)
{
  if(DrawRectButton->Down){
     SRPB->Cursor = crCross;
     if(Shift.Contains(ssLeft)){//натиснута ліва клавіша миші
        SRX2 = X;
        SRY2 = Y;
        DrawSR();
     }
  }
  else{
     SRPB->Cursor = crDefault;
  }
}
//---------------------------------------------------------------------------
--
void __fastcall TSetFilterForm::SRPBMouseDown(TObject *Sender,
      TMouseButton Button, TShiftState Shift, int X, int Y)
{
   if(Button == mbLeft && DrawRectButton->Down){
```

```
      SRX1 = SRX2 = X;
      SRY1 = SRY2 = Y;
   }
}
//---------------------------------------------------------------------------
--
void TSetFilterForm::DrawSR()
{
    TPicture *tPic = new TPicture;
    tPic->Bitmap->Width = SRPB->Width;
    tPic->Bitmap->Height =  SRPB->Height;
    tPic->Bitmap->Canvas->Brush->Color = (TColor)RGB(100,100,100);
    tPic->Bitmap->Canvas->FillRect(tPic->Bitmap->Canvas->ClipRect);
    tPic->Bitmap->Canvas->Brush->Color = clWhite;
    tPic->Bitmap->Canvas->FillRect(Rect(SRX1, SRY1, SRX2, SRY2));
    tPic->Bitmap->Canvas->CopyMode = cmSrcAnd;
    tPic->Bitmap->Canvas->StretchDraw(tPic->Bitmap->Canvas->ClipRect,
Sets.FramePic->Bitmap);
    SRPB->Canvas->Draw(0, 0, tPic->Bitmap);
    delete tPic;
}
void __fastcall TSetFilterForm::FormShow(TObject *Sender)
{
   //зберегти поточні налаштування
   Sets.SaveToFile("prev.cfg");
   SRPB->Width = Sets.pW;
   SRPB->Height = Sets.pH;
   SensPB->Width = Sets.pW;
   SensPB->Height = Sets.pH;
   if(Sets.ClipRect.bottom > 0){
      SRX1 = Sets.ClipRect.left;
      SRX2 = Sets.ClipRect.right;
      SRY1 = Sets.ClipRect.top;
      SRY2 = Sets.ClipRect.bottom;
   }else{
      SRX1 = SRY1 = 0;
      SRX2 = Sets.pW;
      SRY2 = Sets.pH;
   }
   ActivePointsEdit->Text = IntToStr(Sets.MaxActivePoints);
   AlarmTimeEdit->Text = IntToStr(Sets.AlarmMotionTime);
   CycleTimeEdit->Text = IntToStr(Sets.CycleTime);
```

```
    ForceSaveEdit->Text = IntToStr(Sets.ForceSaveTime);
}
//---------------------------------------------------------------------------
--
void __fastcall TSetFilterForm::RectSaveButtonClick(TObject *Sender)
{
    int t;
    if(SRX1 > SRX2){
        t = SRX1; SRX1 = SRX2; SRX2 = t;
    }
    if(SRY1 > SRY2){
        t = SRY1; SRY1 = SRY2; SRY2 = t;
    }
    Sets.ClipRect.left = SRX1;
    Sets.ClipRect.right = SRX2;
    Sets.ClipRect.top = SRY1;
    Sets.ClipRect.bottom = SRY2;
    if(Sets.bConnected) capGrabFrame(Sets.hCaptureW);
}
//---------------------------------------------------------------------------
--
void __fastcall TSetFilterForm::SensPBPaint(TObject *Sender)
{
    DrawSensRegions();
}
//---------------------------------------------------------------------------
--
void TSetFilterForm::DrawSensRegions()
{
    int i;
    SensRegion *sR;
    TPicture *tPic = new TPicture;
    tPic->Bitmap->Width = SensPB->Width;
    tPic->Bitmap->Height =  SensPB->Height;
    for(i = 0; i < Sets.SensList->Count; i++){
        sR = (SensRegion*)Sets.SensList->Items[i];
        int cl = sR->sens * 255.0 / 100.0;
        tPic->Bitmap->Canvas->Brush->Color = (TColor)RGB(cl, cl, cl);
        tPic->Bitmap->Canvas->FillRect(*sR);
    }
    tPic->Bitmap->Canvas->CopyMode = cmSrcAnd;
    tPic->Bitmap->Canvas->Draw(0, 0, Sets.GrayPic->Bitmap);
```

```
   tPic->Bitmap->Canvas->Font->Color = clRed;
   tPic->Bitmap->Canvas->Pen->Width = 1;
   for(i = 0; i < Sets.SensList->Count; i++){
      sR = (SensRegion*)Sets.SensList->Items[i];
      tPic->Bitmap->Canvas->Brush->Style = bsSolid;
      tPic->Bitmap->Canvas->Brush->Color = clRed;
      tPic->Bitmap->Canvas->FrameRect(*sR);
      tPic->Bitmap->Canvas->Brush->Style = bsClear;
      tPic->Bitmap->Canvas->TextOut((sR->left+sR->right)*0.5-10, (sR-
>top+sR->bottom)*0.5-10, IntToStr(sR->sens));
   }
   SensPB->Canvas->Draw(0, 0, tPic->Bitmap);
   delete tPic;
  // SensPB->Canvas->Draw(0, 0, Sets.GrayPic->Bitmap);
}
void __fastcall TSetFilterForm::SensSpeedButtonClick(TObject *Sender)
{
   if(!((TSpeedButton*)Sender)->Down){
      CurSens = -1;
   }else{
      CurSens = StrToInt(((TSpeedButton*)Sender)->Caption);
   }
}
//---------------------------------------------------------------------------
--
void __fastcall TSetFilterForm::SensPBMouseUp(TObject *Sender,
      TMouseButton Button, TShiftState Shift, int X, int Y)
{
   int i;
   SensRegion *sR;
   if(CurSens != -1 && Button == mbLeft){
      for(i = 0; i < Sets.SensList->Count; i++){
         sR = (SensRegion*)Sets.SensList->Items[i];
         if(sR->left < X && sR->right > X && sR->top < Y && sR->bottom >
Y){
            sR->sens = CurSens;
         }
      }
      DrawSensRegions();
   }
}
```

```
//---------------------------------------------------------------------------
--
void __fastcall TSetFilterForm::SensPBMouseMove(TObject *Sender,
      TShiftState Shift, int X, int Y)
{
   if(CurSens != -1){
      SensPB->Cursor = crHandPoint;
   }else{
      SensPB->Cursor = crDefault;
   }
}
//---------------------------------------------------------------------------
--
void __fastcall TSetFilterForm::SensClearButtonClick(TObject *Sender)
{
   int i;
   SensRegion *sR;
   for(i = 0; i < Sets.SensList->Count; i++){
      sR = (SensRegion*)Sets.SensList->Items[i];
      sR->sens = 90;
   }
   DrawSensRegions();
}
//---------------------------------------------------------------------------
--
void __fastcall TSetFilterForm::AlarmApplyBitBtnClick(TObject *Sender)
{
   try{
      Sets.MaxActivePoints = StrToInt(ActivePointsEdit->Text.Trim());
      Sets.AlarmMotionTime = StrToInt(AlarmTimeEdit->Text.Trim());
      Sets.CycleTime = StrToInt(CycleTimeEdit->Text.Trim());
      Sets.ForceSaveTime = StrToInt(ForceSaveEdit->Text.Trim());
   }catch(...){
      ShowMessage("Введене число не входить в допустимий діапазон
значень!");
   }
}
```

4.2 Захист розробленого програмного забезпечення

Для захисту розробленого програмного забезпечення запропоновано використовувати алгоритм RC5, який являє собою блоковий шифр із безліччю параметрів: розміром блоку, розміром ключа й числом раундів. В алгоритмі RC5 передбачені три операції: XOR, додавання й циклічні зрушення. На більшості процесорів операції циклічного зрушення виконуються за постійний час, змінні циклічні зрушення являють собою нелінійну функцію. Циклічні зрушення залежать як від ключа, так і від даних.

В RC5 використовується блок змінної довжини, але в приводиться прикладі, що буде розглянутий, 64-бітовий блок даних. Шифрування використовує $2r+2$ залежних від ключа 32-бітових слів – S_0, S_1, S_2,... S_{2r+1} – де r – число раундів. Для шифрування спочатку потрібно розділити блок відкритого тексту на два 32-бітових слова: A и B. (При впакуванні байтів у слова в алгоритмі RC5 дотримується угода про прямий порядок (little-endian) байтів: перший байт займає молодші біти регістра A й т. ін.) Потім:

$$A=A + S_0$$

$$B = B + S_0$$

Для і від 1 до r:

$$A = ((A\oplus \quad B) <<< B) + S_{2i}$$

$$B = ((B\oplus \quad A) <<< A) + S_{2i+1}$$

Вихід перебуває в регістрах A и B.

Розшифрування теж нескладно. Потрібно розбити блок відкритого тексту на два слова, A й B, а потім:

Для i від r до 1 із кроком -1:

$$B = ((B - S_{2i+1}) >>> A) \oplus A$$

$$A = ((A - S_{2i}) >>> B) \oplus B$$

$$B = B - S_i$$

$$A = A - S_0$$

Символом «>>>» позначене циклічне зрушення вправо**.** Звичайно ж**,** всі додавання й вирахування виконуються по модулю 2^{32}.

Створення масиву ключів складніше, але теж прямолінійно. Спочатку байти ключа копіюються в масив L із 32-бітових слів, доповнюючи при необхідності заключне слово нулями. Потім масив S ініціалізується за допомогою лінійного конгруентного генератора по модулю 2^{32}:

$$S_0 = P$$

Для i від 1 до $2(r + 1) – 1$:

$$S_i = (S_{i-1} + Q) \bmod 2^{32}$$

де P = 0xb7e15163 і Q = 0x9e3779b9.

Нарешті, потрібно підставити L в S:

$$i = j = 0$$

$$A = B = 0$$

Виконати $3n$ раз (де n – максимум від $2(r + 1)$ і c):

$$A = S_i = (S_i + A + B) <<< 3$$

$$B = L_i = (L_i + A + B) <<< (A + B)$$

$$i = (i + 1) \bmod 2(r +1)$$

$$i = (j +1) \bmod c$$

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Розроблене програмне забезпечення призначене для ведення відеоспостереження на основі використання DirectX для бездротових мереж.

Дане програмне забезпечення володіє наступними функціональними можливостями:

– Виконує захват зображень із будь-якого пристрою відеозахвату, підтримуваного Windows XP/Vista/7.

– Виділяє вказану контрольну область із оригінального зображення.

– Робить автоматичний баланс рівнів контрольної області, що забезпечує незалежність роботи алгоритму виявлення від освітленості й рівня посилення відеосигналу.

– Обробляє контрольну область з налаштовуваною чутливістю до руху за 64 підобластями.

– Візуально представляє кожний етап обробки.

– Дозволяє встановити граничні умови для захвату зображення й виклику тривоги.

– При виконанні умов тривоги запускає зазначену програму, командний файл, документ або програє звуковий сигнал.

– При перевищенні порогу виявлення руху зберігає зображення у форматі JPEG.

– Примусово зберігає зображення через зазначені проміжки часу або при натисканні на кнопку **Зняти!**

– Має винятково простий і функціональний інтерфейс без непотрібних для такого роду програм графічних надмірностей.

– Абсолютно повне й досить тонке налаштування всіх параметрів користувачем.

– Не вимагає для роботи ніяких додаткових файлів і бібліотек, крім стандартних бібліотек Windows, не вносить ніякі свої записи до реєстру або файлів налаштувань ОС.

Інтерфейс головного вікна програми зображений на рисунку 5.1

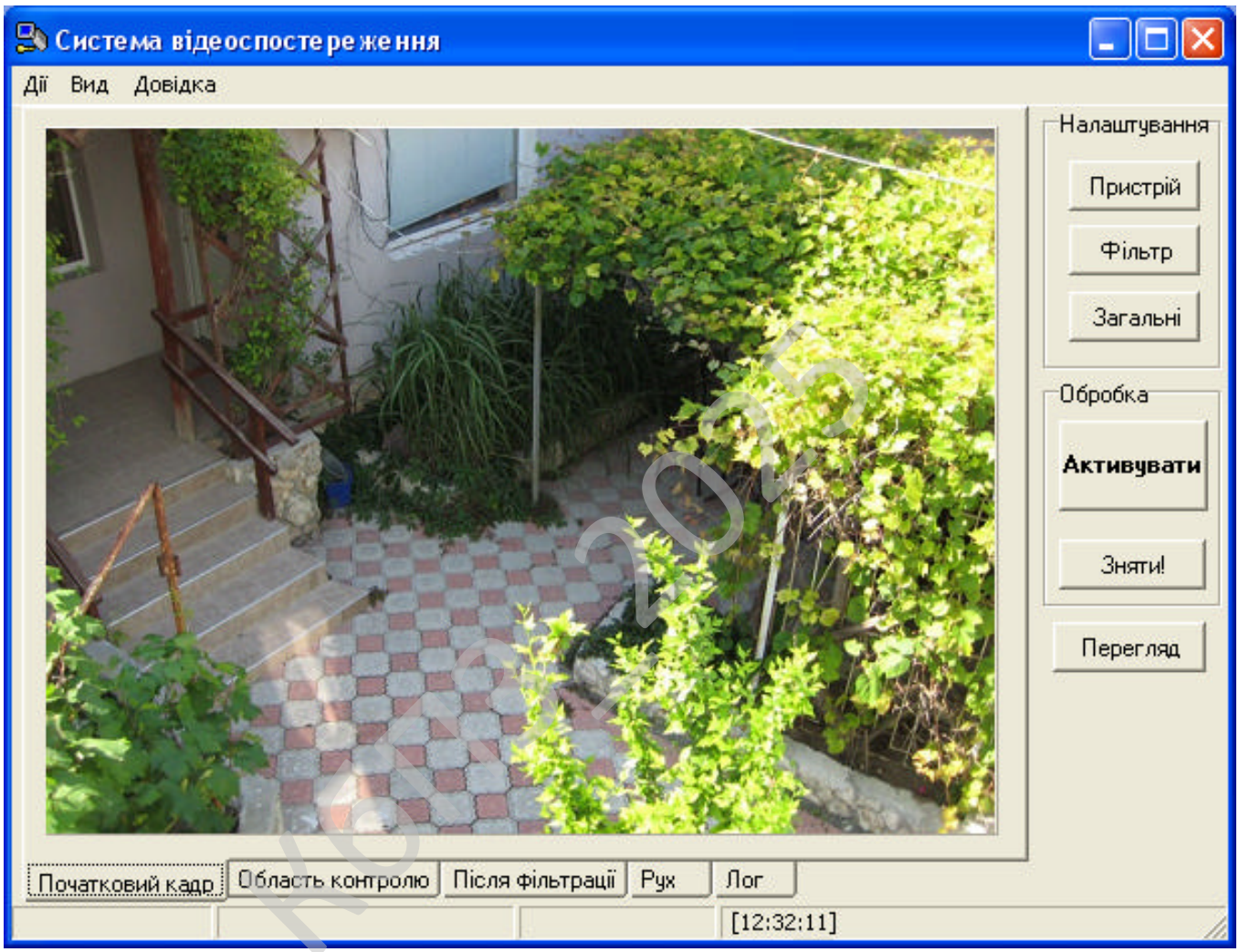

Рисунок 5.1 – Головне вікно програми, закладка **Початковий кадр**, що відображає кадр, безпосередньо отриманий із пристрою відеозахвату

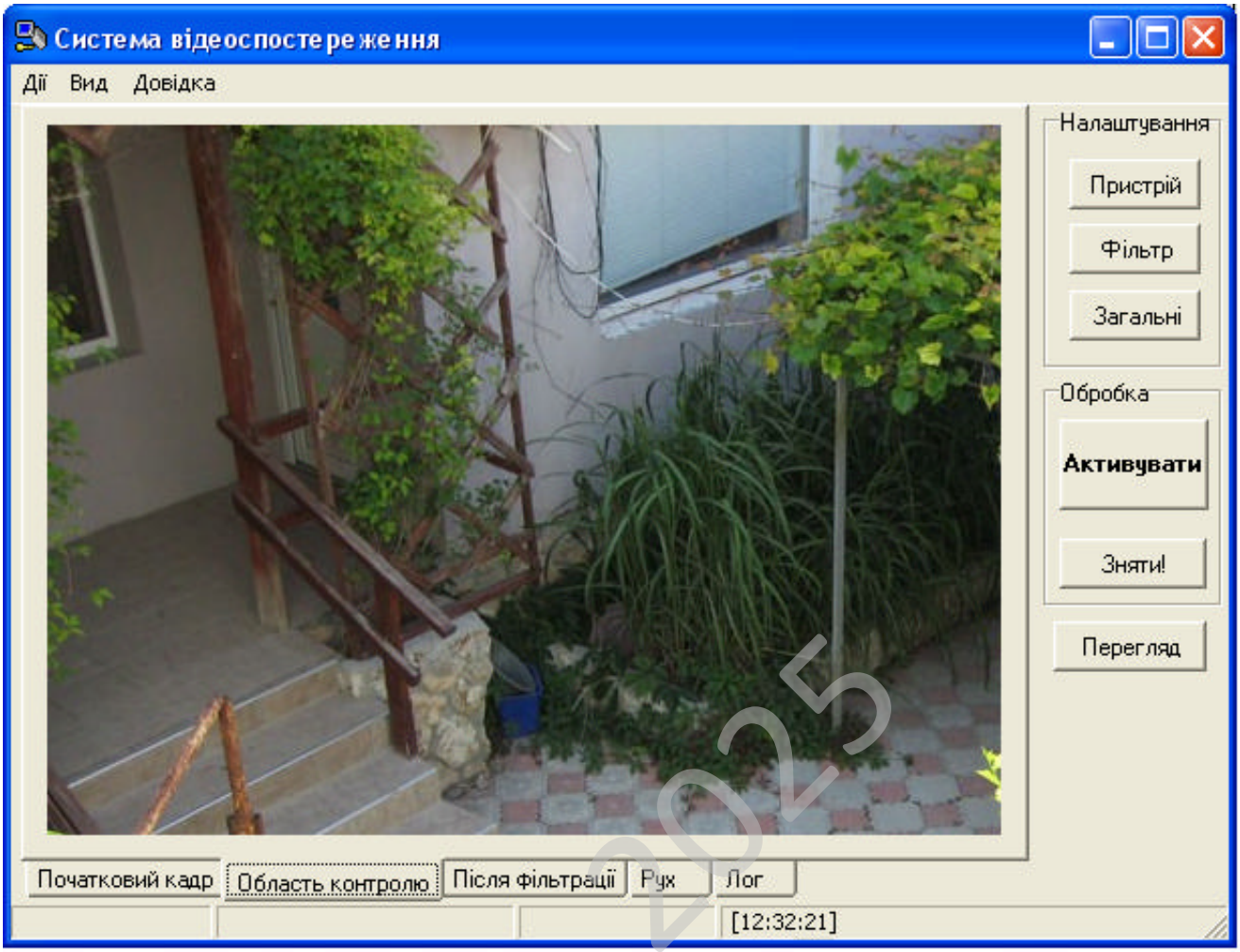

Рисунок 5.2 – Головне вікно програми, закладка **Область контролю**, що відображає зображення контрольованої області після виконання процедури автобалансування

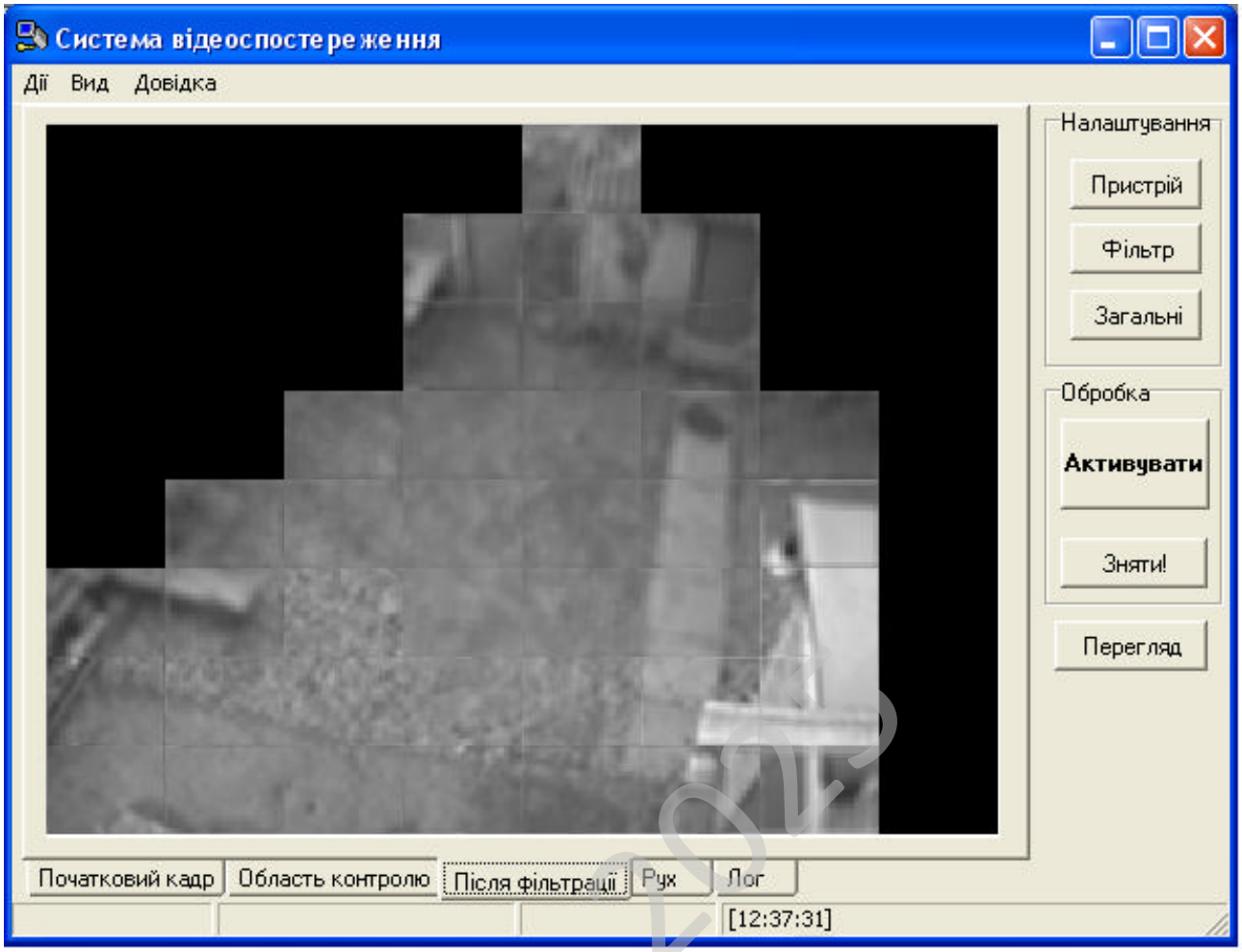

Рисунок 5.3 – Головне вікно програми, Закладка **Після фільтрації**, що відображає повністю оброблене зображення відповідно до установок користувацького фільтра руху

Закладка **Рух** відображає області, де в поточний момент спостерігається рух. Закладка **Лог** відображає інформацію про статус, помилки драйвера відеозахвату й виконаних програмою дій.

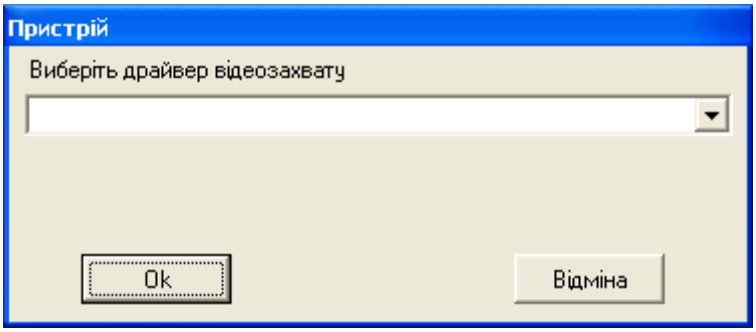

Рисунок 5.4 – Діалогове вікно **Пристрій**, в якому обирається пристрій відеоспостереження

Натиснувши на кнопку **Фільтр**, відкриваємо вікно з найважливішими для даної програми налаштуваннями.

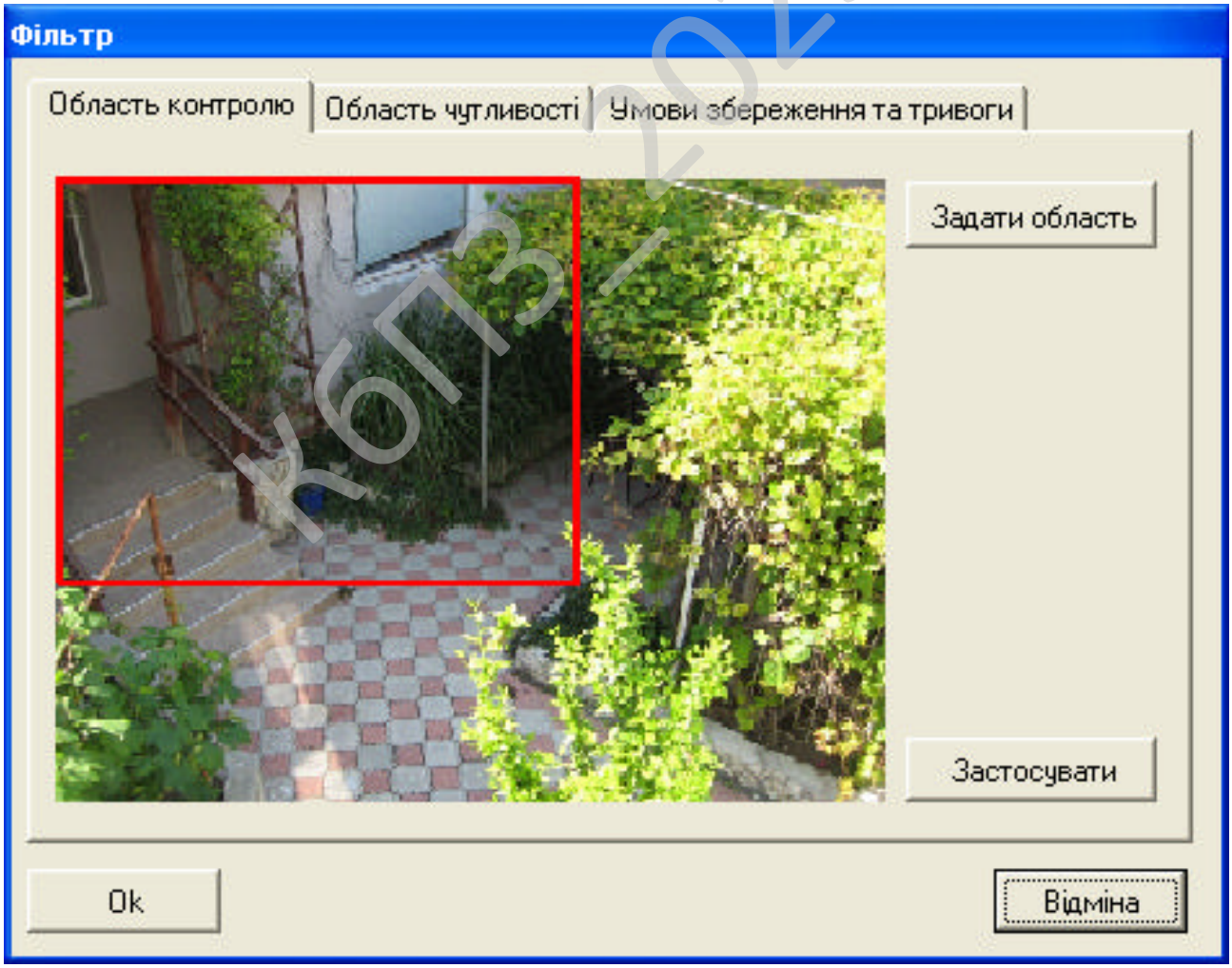

Рисунок 5.5 – Вікно **Фільтр**, закладка **Область контролю**

Для виділення області контролю слід тиснути кнопку **Задати область** і «намалювати» мишкою прямокутник на зображенні. Все, що всередині прямокутника потрапляє в область контролю. Щоб зміни вступили в дію – треба натиснути кнопку **Застосувати**.

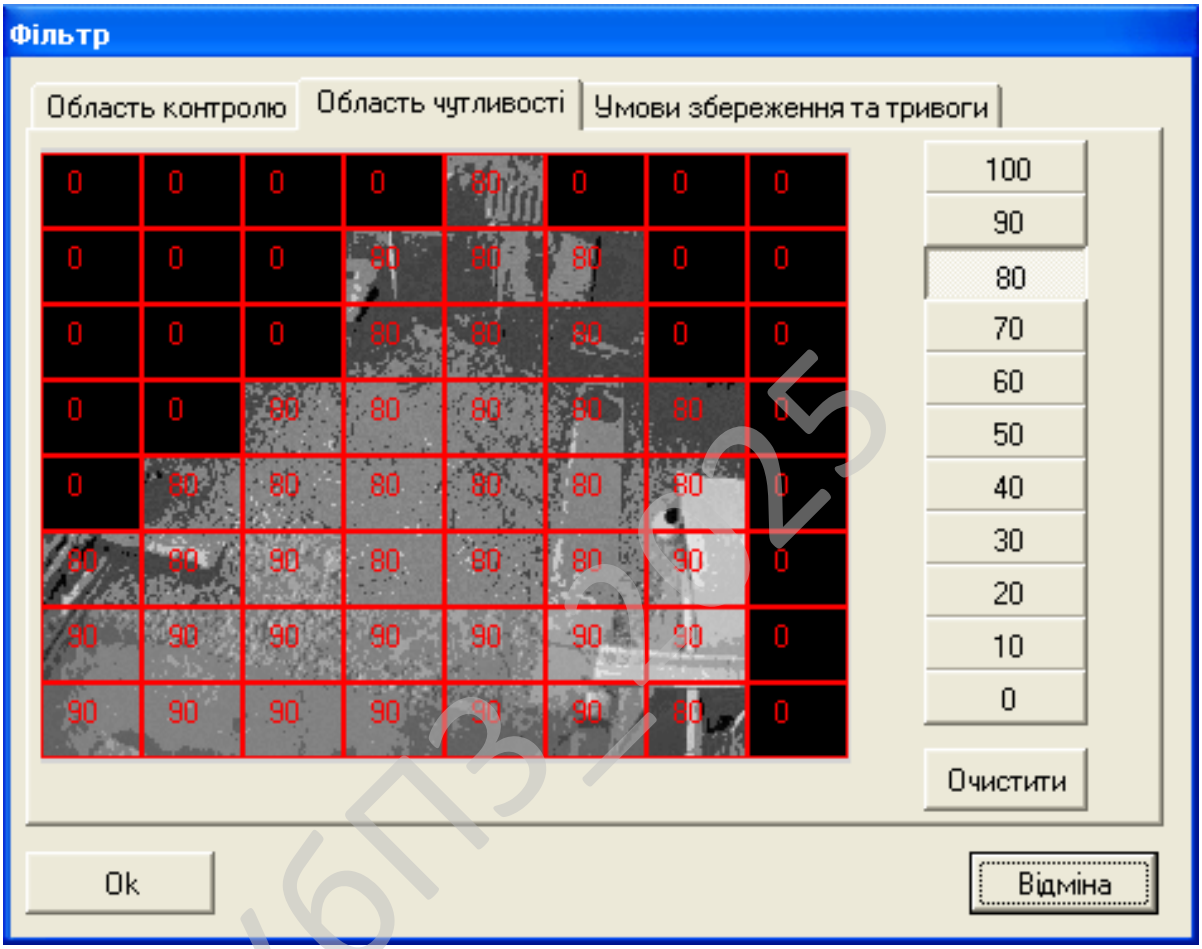

Рисунок 5.6 – Вікно **Фільтр**, закладка **Область чутливості**

На цій закладці встановлюється чутливість до руху окремих областей контрольованого зображення. Для завдання чутливості слід натиснути на кнопку праворуч із потрібним значенням чутливості, а потім клацнути лівою кнопкою миші усередині червоних прямокутників на зображенні. Непотрібні для контролю області необхідно позначити чутливістю 0 (крім усього іншого, це прискорює роботу фільтра).

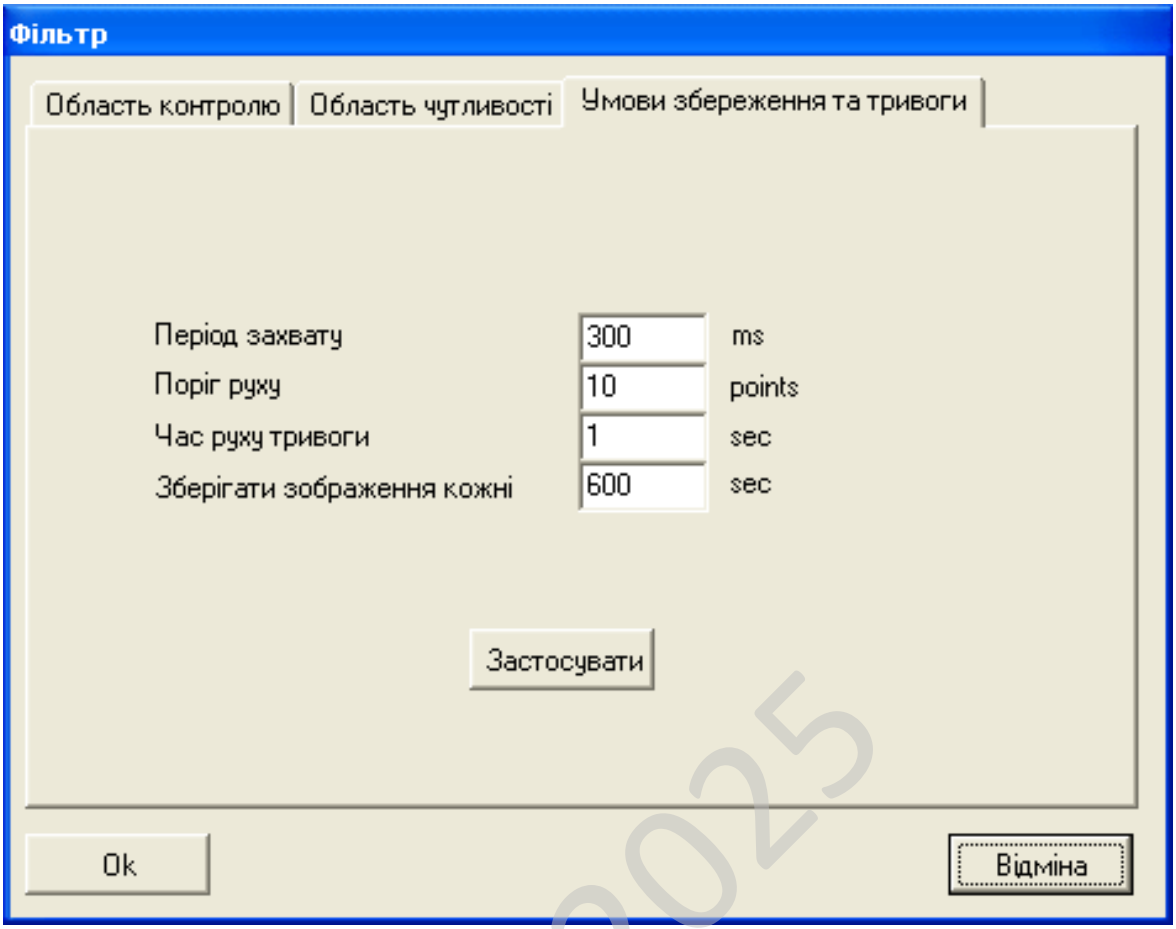

Рисунок 5.6 – Вікно **Фільтр**, закладка **Умови збереження та тривога**

Дана закладка містить налаштування порогів. Значення параметрів наступні:

Період захвату – час між захватами зображення з відеокамери. Встановлюється в мілісекундах. Оптимальне значення – 300. Якщо, наприклад, встановити 2, то програма не зможе виконати таких умов, і буде обробляти зображення з максимально можливою для вашого комп'ютера швидкістю. Впливає на мінімальну швидкість руху об'єкта в кадрі, що виявляється програмою. Чим менше час циклу, тим вище мінімальна швидкість руху для досягнення порога виявлення.

Поріг руху – мінімальна кількість точок, у яких програма засікла рух і повинна виконати збереження картинки на диск. Від цього параметра залежить мінімальний розмір об'єкта, що рухається, що буде помічений (наприклад, щоб

виявити курку досить 20 точок, а пропустити курку, але помітити людину – приблизно 100 точок). Конкретні значення залежать від масштабів зображення.

Час руху тривоги – мінімальний час, протягом якого безупинно засікається рух вище порога, заданого попереднім параметром, через який треба виконувати процедуру тривоги. Вказується в секундах, ефективно фільтрує випадкові захвати через рух гілок дерев при сильних поривах вітру або повільних пересувань домашніх тварин, наприклад, собаки.

Зберігати зображення кожні… – час у секундах, через який зображення буде зберігатися на диску в «примусовому» порядку.

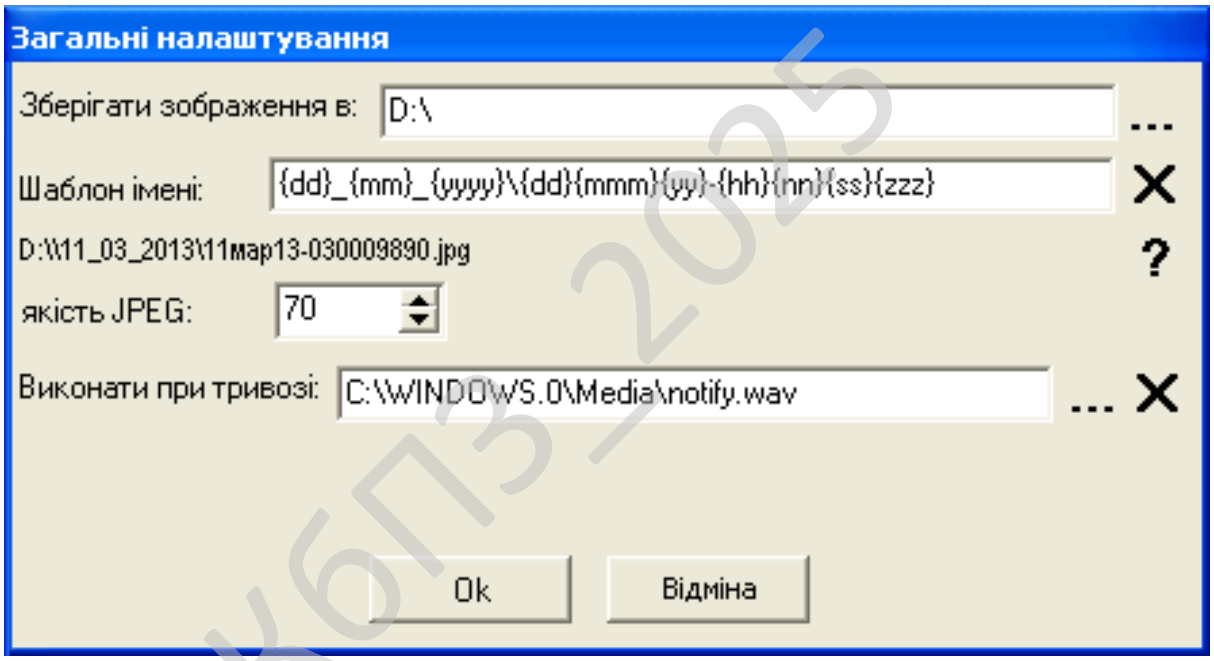

Рисунок 5.7 – Вікно **Загальні налаштування**

Дане вікно з'являється при натисканні на кнопку **Загальні**. У ньому потрібно вказати папку, у яку буде здійснюватися збереження зображень, якість збережених зображень (від 5 до 100, 100 – максимальна якість, але й максимальний розмір файлів).

Кнопки з трикрапками відкривають діалоги вибору папки для збереження картинок і програми обробки ситуації тривоги.

Виконати при тривозі… – обрання дії, яку програма буде виконувати при настанні умов тривоги. Якщо вибрати аудіофайл – програма програє записану у ньому мелодію, у всіх інших випадках спробує виконати вибраний файл.

Для початку роботи з програмою необхідно:

1. Переконатися в тому, що у вас є правильно встановлений пристрій та встановлені драйвера до нього для захвату зображень у системі. Такими пристроями є: вебкамери, ТВ-тюнери, відеокарти з відеовходом, цифрові фотоапарати в режимі вебкамери.

2. Підключити до відеовходу пристрою захвату джерело сигналу (аналогову відеокамеру). Вебкамер і цифрових фотоапаратів це не стосується.

3. Запустити програму. Задати налаштування пристрою, фільтра, збереження зображень і дій при тривозі.

4. Натиснути на кнопку **Активувати**. Програма почне захват й обробку зображень.

5. Якщо виникне помилка, переглянути журнал системних подій, що перебуває на закладці **Лог**. Спробувати змінити налаштування. Налаштування застосовуються «на льоту», тобто перезапуску програми не вимагають. Програма сама виконує всі необхідні дії для переініціалізації. Налаштування зберігаються автоматично, при виході із програми (це не стосується специфічних налаштувань пристроїв відеозахвату).

6. Переглянути безпосередній результат роботи програми можна, натиснувши кнопку **Перегляд –** відкриється вікно провідника для папки, у яку зберігаються зображення.

На рисунку 5.8 зображене вікно «Про програму…» з короткою довідкою про розроблене програмне забезпечення.

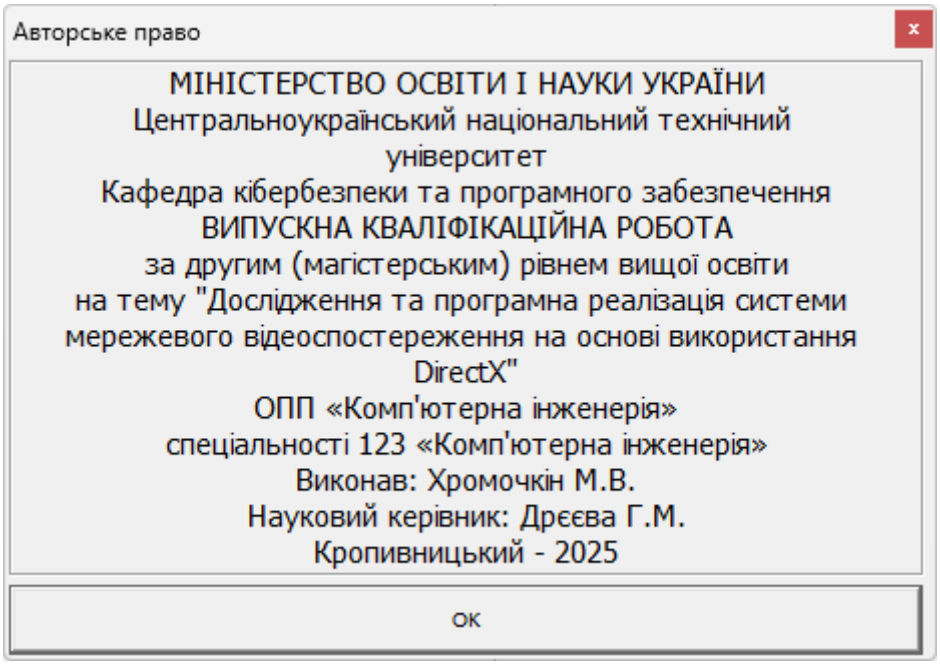

Рисунок 5.8 – Вікно «Про програму…»

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи мережевого відеоспостереження на основі використання DirectX.

Метою розробки є дослідження та 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.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод мережевого відеоспостереження на основі використання DirectX.

– Розроблено вітчизняний продукт мережевого відеоспостереження на основі використання DirectX, який має більш широкі можливості, на відміну від існуючих аналогів.

7 МАРКЕТИНГОВЕ ТА ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ІТ-ПРОЄКТУ

7.1 Визначення цільової аудиторії кінцевого готового продукту

Результати дослідження та реалізації системи мережевого відеоспостереження на базі DirectX можуть зацікавити дуже широке коло користувачів, насамперед підприємства, для яких безпека об’єктів є пріоритетом. Це можуть бути як промислові компанії, так і торговельні мережі, державні установи, заклади освіти чи охорони здоров’я. Усі вони стикаються з потребою мати стабільну систему спостереження, здатну не лише записувати відео, але й забезпечувати якісну обробку даних у реальному часі. Саме технологія DirectX дає можливість суттєво підвищити ефективність обробки графічних потоків без перевантаження процесора.

Особливо ця система може бути корисною для компаній, які мають розподілену інфраструктуру – наприклад, склади чи торгові точки в різних містах. Впровадження DirectX дозволяє забезпечити високу швидкість передачі даних та мінімізувати затримки при перегляді відео онлайн, що критично для служб безпеки.

Не менш важливим є інтерес освітніх установ технічного профілю, які можуть використовувати розробку як навчальний приклад для вивчення технологій обробки мультимедіа, комп’ютерної графіки та оптимізації програмних систем. Також дослідження може бути цікавим для розробників програмного забезпечення, які прагнуть впроваджувати сучасні рішення в галузі штучного інтелекту та комп’ютерного зору на основі високопродуктивних графічних інтерфейсів.

7.2 Оцінка привабливості шляхом застосування методів експертних оцінок

Для оцінки привабливості системи мережевого відеоспостереження, створеної на базі DirectX, можна залучити групу експертів із галузей інформаційної безпеки, комп'ютерної графіки та промислової автоматизації. Кожен експерт оцінює систему за рядом критеріїв, таких як продуктивність, надійність, масштабованість, вартість впровадження, зручність користування та сумісність із наявними мережевими рішеннями. Після цього результати узагальнюються, а середнє значення кожного параметра дозволяє визначити загальну привабливість системи.

Як приклад, можна уявити, що група з 10 експертів оцінює систему за шкалою від 1 до 10. Якщо середній бал за параметрами продуктивності складає 9,2, за надійністю – 8,8, за масштабованістю – 9,0, а за вартістю впровадження – 7,5, то загальний рівень привабливості можна оцінити як високий. Це свідчить про те, що технологія DirectX справді забезпечує переваги у швидкості обробки графічних даних і якості відеопотоку, що є вирішальним фактором для ефективної роботи сучасних систем спостереження.

Такий метод експертного оцінювання дає змогу не лише виявити сильні сторони проєкту, але й побачити напрямки його вдосконалення. Наприклад, якщо експерти звертають увагу на відносно високу вартість апаратного забезпечення, це може стати сигналом для розробників оптимізувати апаратно-програмну частину системи.

7.3 Вибір методу оцінки вартості ПЗ

Для визначення вартості проєкту впровадження системи відеоспостереження на базі DirectX доцільно застосувати комбінований підхід, що об'єднує метод повної вартості володіння (ТСО) та метод порівняльного

аналізу (Benchmarking). Метод TCO дозволяє врахувати не лише початкові витрати на придбання камер, серверів, програмного забезпечення, але й витрати на обслуговування, енергоспоживання, оновлення програмного забезпечення та навчання персоналу. Такий підхід дає реалістичне уявлення про фінансові наслідки проєкту протягом усього життєвого циклу системи.

Метод Benchmarking, у свою чергу, дозволяє порівняти вартість впровадження системи DirectX із іншими рішеннями, наприклад, на базі OpenGL або традиційних відеосерверів без GPU-прискорення. Це допоможе виявити, наскільки інноваційне рішення є конкурентним і які додаткові вигоди воно надає за схожої ціни.

Такий комбінований підхід є найоптимальнішим, оскільки дозволяє одночасно оцінити як короткострокові витрати, так і довгострокову вигоду від експлуатації системи. Розрахунки показують, що впровадження DirectX знижує навантаження на сервери, а отже, зменшує потребу в додатковому обладнанні та електроенергії, що має прямий економічний ефект у майбутньому.

7.4 Розрахунок економічної ефективності від впровадження реалізованого ПЗ як фактору його привабливості

Підприємство має 6 виробничих цехів і складські приміщення, де використовується застаріла система аналогового відеоспостереження. Передача сигналу здійснюється по коаксіальному кабелю, зображення має низьку якість, а архів зберігається на локальних DVR-записувачах без можливості віддаленого доступу. У рамках модернізації IT-інфраструктури заплановано впровадження мережевої системи відеоспостереження з використанням DirectX, що забезпечує апаратно-прискорене відтворення та обробку відеопотоків у реальному часі. Це дозволить отримувати зображення високої якості (Full HD, 4K), прискорити рендеринг на клієнтських пристроях, знизити навантаження на центральні процесори й оптимізувати використання серверних ресурсів.

Метою проєкту є не лише підвищення рівня безпеки, а й економія на експлуатаційних витратах, пов’язаних із технічним обслуговуванням старої системи, а також зниження втрат від крадіжок і простоїв виробництва. Вхідні дані зафіксовано в таблиці 7.1.

Таблиця 7.1 – Вихідні дані для розрахунку

Показник	**До впровадження**	**Після впровадження**	**Економічний ефект**
Кількість камер	60 (аналогові)	80 (IP-камери)	+20
Середня якість відео	SD (480p)	Full HD (1080p)	—
Витрати на обслуговування (грн/рік)	450 000	200 000	–250 000
Витрати на електроенергію (грн/рік)	180 000	100 000	–80 000
Втрати від інцидентів (крадіжки, псування)	600 000	150 000	–450 000
Початкові інвестиції (сервери, ПЗ, IP-камери)	—	1 500 000	—
Щорічні витрати на підтримку	—	100 000	—

Розрахунок економічного ефекту демонструє наступне: економія на технічному обслуговуванні – 250 000 грн/рік, економія на електроенергії завдяки

використанню енергоефективних IP-камер і GPU-обробки DirectX – 80 000 грн/рік, зниження втрат від інцидентів (крадіжки, псування обладнання) – 450 000 грн/рік, сукупний річний економічний ефект – 780 000 грн/рік, чистий економічний ефект – 680 000 грн/рік, термін окупності ≈ 2,2 роки, рентабельність інвестицій – 45,3 %.

Додаткові нефінансові вигоди: підвищення рівня безпеки підприємства: нові камери дозволяють оперативно виявляти інциденти й запобігати крадіжкам або псуванню матеріалів, віддалений моніторинг: завдяки DirectX і IP-технологіям відеопотоки можна переглядати з будь-якого пристрою – смартфона чи ноутбука, зниження навантаження на сервери: використання GPU-прискорення (DirectX) дозволяє обробляти більше потоків одночасно без додаткового обладнання, якісний відеоархів: висока роздільна здатність забезпечує детальність кадрів для аналізу подій і доказової бази, готовність до інтеграції з аналітичними модулями (AI/ML): можливість подальшого підключення систем розпізнавання облич або реєстраційних номерів.

Таким чином, проєкт можна вважати економічно ефективним і технологічно перспективним, оскільки він поєднує оптимізацію витрат із підвищенням безпеки підприємства та підготовкою до впровадження аналітичних систем відеоаналізу майбутнього покоління.

7.5 Пропозиція алгоритму просування проєкту розробки ПЗ

Просування проєкту системи відеоспостереження на основі DirectX має базуватись на демонстрації її технічних переваг і реальних економічних вигод. На першому етапі необхідно створити демонстраційний стенд, який дозволить потенційним клієнтам побачити роботу системи в дії – швидкість відтворення відео, якість зображення, гнучкість налаштувань. Це важливо для формування першого враження та довіри до технології.

Наступним кроком є інформаційна кампанія, орієнтована на керівників IT-відділів, служб безпеки та власників бізнесу. Матеріали мають пояснювати, як DirectX забезпечує більш ефективну обробку відеопотоків порівняно з традиційними технологіями. Паралельно варто налагоджувати партнерські відносини з інтеграторами та дистриб'юторами мережевого обладнання, які можуть включати систему в свій портфель пропозицій.

На заключному етапі доцільно представити кейси успішних впроваджень і відгуки користувачів, що стане вагомим аргументом для нових клієнтів. У перспективі можна розвивати модель SaaS (Software as a Service), надаючи систему в оренду або за підпискою, що зробить її доступною для малого та середнього бізнесу.

7.6 Оптимізація каналів збуту та шляхів реалізації ПЗ

Для підвищення ефективності збуту доцільно поєднати прямі продажі з партнерськими каналами. Важливо розвивати співпрацю з компаніями, що спеціалізуються на системах безпеки, адже вони вже мають клієнтську базу, зацікавлену у модернізації. Через таких партнерів можна швидше охопити цільовий ринок і зменшити витрати на просування.

Додатково слід зробити акцент на навчальних семінарах для потенційних клієнтів та інтеграторів, де буде продемонстровано можливості DirectX і наведено конкретні приклади зниження витрат. Це дозволяє створити додаткову цінність продукту, що є важливим у B2B-сегменті.

Варто також розглянути використання онлайн-каналів – створення демо-платформи з можливістю тестового підключення камер і перегляду відеопотоку. Це дає змогу потенційному клієнту самостійно переконатися в перевагах системи, не витрачаючи ресурси на фізичну установку.

7.7 Визначення ключових факторів успіху конкретного проєкту

Ключовими факторами успіху цього проєкту є поєднання технологічної ефективності, надійності та економічної доцільності. Висока якість зображення та швидкість обробки відео, яку забезпечує DirectX, створюють безпосередню конкурентну перевагу, що дозволяє системі задовольнити потреби навіть найвимогливіших користувачів.

Важливою умовою успіху є стабільність роботи та простота інтеграції з існуючими IT-інфраструктурами підприємств. Якщо система легко адаптується під різні типи камер і мережевого обладнання, її впровадження не потребує великих додаткових витрат, що робить її більш привабливою для клієнтів.

Не менш значущим фактором є якісна технічна підтримка, навчання персоналу та своєчасне оновлення програмного забезпечення. Це дозволяє забезпечити довгострокову стабільність і довіру користувачів до продукту.

І, звичайно, успіх визначається позитивним економічним ефектом. Якщо система не лише покращує безпеку, але й допомагає реально знизити витрати підприємства, це стає головним аргументом для масштабного впровадження та сталого розвитку проєкту в майбутньому.

8 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

8.1 Вступ

Персональні електронно-обчислювальні машини (ПЕОМ) відіграють важливу роль у житті сучасної людини. Кожного дня мільйони людей використовують ПЕОМ для пошуку необхідної інформації, спілкуванні у соціальних мережах, перегляду новин, роботи тощо. Багато людей користуються ПЕОМ у професійних цілях, оскільки завдяки ПЕОМ з'явилося багато нових професій.

В даному розділі магістерської роботи проведемо аналіз основних чинників при роботі програміста.

Основою охорони праці є науковий аналіз умов праці, технологічних процесів, виробничого обладнання, робочих місць, трудових операцій, організації виробництва з метою виявлення шкідливих і небезпечних виробничих факторів, їх властивостей, особливостей виливу на організм людини. На підставі такого аналізу розробляються заходи та засоби, спрямовані на мінімізацію несприятливого впливу виробничих факторів, створення безпечних та нешкідливих умов праці.

Для того, щоб об’єктивно проаналізувати відповідність умов праці діючим нормативно-правовим актам, необхідно здійснити санітарно-гігієнічну характеристику умов праці відділу, в якому працює програміст.

У зв’язку з цим необхідно сконцентрувати увагу на небезпечних і шкідливих чинниках пов’язаних з постійною роботою за комп’ютером.

8.2 Шкідливі і небезпечні фактори при роботі з комп'ютером

ПЕОМ та інше обладнання є джерелами небезпеки ураження електричним струмом. Оскільки робота програміста характеризується істотним зоровим навантаженням, то вимагає належного освітлення. У приміщенні, в якому працюють програмісти, необхідно створити належний мікроклімат, параметри якого регламентуються, Державними санітарними правилами і нормами, зокрема ДСанПіН 3.3.2.007-98.

При роботі з використанням ПЕОМ відзначають наступні небезпечні та шкідливі фактори:

– ризик виникнення надзвичайних ситуацій природного або штучного характеру на об'єкті або території;

– ризик виникнення пожежі;

– негативний вплив на органи зору людини;

– ризики ураження електричним струмом;

– недостатня, або надмірна освітленість робочого місця;

– електромагнітні (у тому числі високочастотні) випромінювання (коливання);

– несприятливі мікрокліматичні умови;

– нервово-емоційна напруженість праці;

– інтелектуальні навантаження;

– монотонність праці;

– невідповідність ергономічних показників робочого місця діючим вимогам;

– шум;

– статичні навантаження на кістково-м'язовий апарат.

8.3 Аналіз умов праці програміста

Умови праці в приміщенні, в якому знаходиться робоче місце програміста є сприятливими. Приміщення обладнане автономною системою газового опалення, основною перевагою якого є програмування режиму роботи в залежності від погодних умов, оскільки клімат є нестійким. Використовується система природної та штучної вентиляції, що забезпечує ефективну циркуляцію повітря. В кабінеті знаходиться кондиціонер AKAI AK-AC7010-OF.

Засоби копіювальної техніки знаходяться на достатньо далекій відстані від робочих місць, оскільки приміщення складає 20 м^2, а у відділі налічується два працівники, тобто концентрація озону та оксиду азоту в повітрі є невисокою. Таким чином, на кожного програміста приходиться 10,0 м^2 що відповідає нормам Державним санітарним правилам і нормам ДСанПіН 3.3.2.007-98 [1]. Висота стелі приміщення складає 2,9 метри, що також не порушує нормативні вимоги.

Прибиральники підтримують порядок в службових приміщеннях, дотримуються санітарно-гігієнічних норм по прибиранню приміщень, витирають пил, підмітають підлогу наприкінці кожного робочого дня.

В цілому потрібно відмітати застарілість офісної техніки та відсутність клавіатур з ергономічною розкладкою та рідкокристалічних моніторів, які здійснюють менш негативний вплив на стан здоров’я працівників відділу.

Оформлення інтер’єру приміщення є відповідає вимогам з ергономіки та стимулює працівників до підвищення працездатності та зниження втоми. Стеля білого кольору створює оптичний ефект збільшення висоти приміщення, підлога пофарбована коричневим кольором, а стіни – у жовтий. Перевагами даного кольору є створення відчуття теплоти, здатність привертати увагу без додаткової втоми.

Висота столу складає 71,5 см, до того ж його можна регулювати відповідно до власних потреб. Стіл має достатній внутрішній об’єм, завдяки ширині у 73 см та висоті простору під столом – у 63 см, є достатньо важким для

забезпечення стійкості. Крісла забезпечують фізіологічно раціональну позу, мають підлокітники, здатні обертатися та регулятор висоти, кута нахилу спинки й відстані спинки від краю сидіння.

В кабінеті створено оптимальні умови праці відносно температури, вологості приміщення та вентиляції.

Наприкінці аналізу небезпечних факторів праці побудуємо підсумкову таблицю 8.1.

Таблиця 8.1 – Підсумкова таблиця значень параметрів небезпечних факторів праці

Найменування параметра	Значення параметра		Нормативний документ
	Фактичне	Нормоване	
Освітленість штучна, лк	300	300	ДБН.В 2.5-28:2018 [2]
Значення КПО,%	1,0	1,1	ДБН.В 2.5-28:2018 [2]
Повітрообмін,м /год взимку влітку	 76 36	 80 80	 ДСН 3.3.6.042-99[3] ДСН 3.3.6.042-99 [3]
Температура повітря. °С взимку влітку	 22 24	 21-25 27-28	 ДСанПіН 3.3.2-007-98 ДСанПіН 3.3.2-007-98
Відносна вологість,% взимку влітку	 60 55	 <75 <60	 ДСанПіН 3.3.2-007-98 ДСанПіН 3.3.2-007-98
Швидкість переміщення повітря, м/с взимку влітку	 0,16 0,10	 <0,2 <0,2	 ДСанПіН 3.3.2-007-98 ДСанПіН 3.3.2-007-98

Щодо вимог електробезпеки, то приміщення за небезпекою ураження електричним струмом можна віднести до 1 класу, тобто це приміщення без підвищеної небезпеки (сухе, без пилу, з нормальною температурою повітря, ізольованими підлогами і малим числом заземлених приладів).

Для запобігання поразки електричним струмом в приміщенні відділу використовується ряд організаційно-технічних заходів: розташування проводів живлення поза зоною пересування людей; допуск до роботи електроприладів тільки тих робітників, що знайомі із технікою безпеки; використання мережних подовжувачів з вбудованими запобіжниками на 0,1 А; при ремонті обладнання персонал попереджується.

Устаткування, що працює в приміщенні, живиться від мережі 220В та частотою 50Гц. Споживачами цієї напруги є також джерела штучного освітлення. Вони розташовуються на висоті 3 м, що задовольняє нормі, відповідно до якого джерела освітлення повинні розташовуватися на висоті 2,5 м від підлоги.

Проводка схована. У якості розеток для підключення устаткування застосовуються розетки з заземленим кожухом, захищеного від випадкового доторку до струмоведучих частин. Електроустаткування, що знаходиться в приміщенні відділу відноситься до установок напругою до 1000В.

На робочому місці програміста з всього устаткування металевим є лише корпус системного блоку комп’ютера, але тут використовуються системні блоки, що відповідають стандартові фірми IBM, у яких крім робочої ізоляції передбачений елемент для заземлення і провід з жилою, що заземлює, для приєднання до джерела живлення.

Основні причини ураження людини електричним струмом на робочому місці:

– дотик до металевих неструмоведучих частин (корпусу, периферії комп'ютера), що можуть виявитися під напругою в результаті ушкодження ізоляції:

– нерегламентоване використання електричних приладів:

– відсутність інструктажу співробітників з правил електробезпеки.

На протязі роботи на корпусі комп'ютера накопичується статична електрика. На відстані 5-10 см від екрана напруженість електростатичного поля складає 60-280 кВ/м, тобто в 10 разів перевищує норму 20 кВ/м.

Отже, за результатами проведеного аналізу можна зробити висновки, що всі показники знаходяться у межах запропонованих значень.

8.4 Розробка заходів з умов поліпшення охорони праці

Згідно аналізу умов праці в розглянутому приміщенні, ми отримали наступні результати:

– розмірі приміщення, у розрахунку на одному працюючого, відповідають нормативам;

– мікроклімат відповідає нормативному значенню;

– акустичні умови роботи не перевищують нормативних значень;

Таким чином можна припустити, що основною причиною можливого зниження працездатності програміста є психофізіологічний фактор, тому основна пропозиція буде така: дотримання позитивної психологічної атмосфери в колективі та регламентованого режиму праці та відпочинку, організація робочого місця з урахуванням ергономічних вимог.

Рекомендовані заходи: регулярні періодичні наочні огляди персоналом шляхів для евакуації людей із приміщення, відповідно до плану евакуації (який повинен розташовуватись на видному місці у приміщенні), включення до колективного договору мінімально можливого вмісту аптечок з обов’язковою наявністю масок-клапанів, або іншого спорядження для штучного дихання. Регулярна періодична перевірка параметрів заземлення та занулення (вимірювання опору ланцюга).

Регулярна наочне знайомство персоналу із шляхами для евакуації людей із приміщення відповідно до плану евакуації, забезпечення розподільних щитів

спеціальними розетками з заземлюючими контактами; організація заземлення всіх приладів і пристроїв, які працюють при напрузі вище 36 В.

Так як при ураженні електричним струмом у людини може статися фібриляція шлуночків серця, в організації бажано мати дефібрилятор і підготовлений персонал для роботи з ним.

8.5 Розрахункова частина

Для захисного штучного заземлення будемо застосовувати вертикальні електроди з сталевого прокату круглого перерізу діаметром 35 мм., довжиною L=1,5 м., та горизонтальний електрод-металева полоса з перетином 35·4 мм. Напруга – 220/380 В. Розрахункова схема розташування заземлюючих електродів – по контуру (прямокутником) (рис. 8.1).

Розрахунок проводиться за допустимим опором розтіканню струму заземлювача.

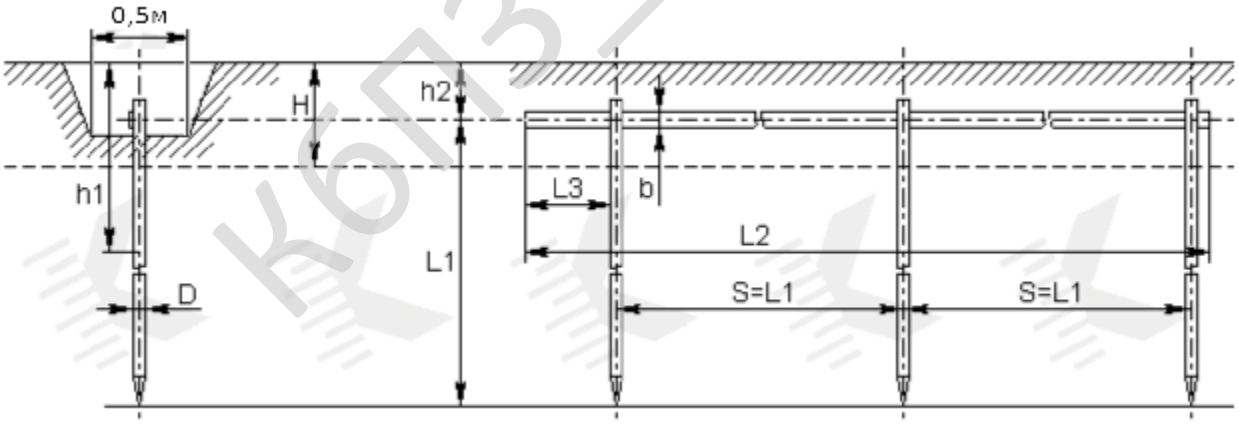

Рисунок 8.1 – Схема штучного заземлення

Початкові дані для розрахунку захисного заземлення: тип верхнього шару ґрунту – чорнозем, нижнього шару ґрунту – глина (питомий опір ρ_2 = 40 Ом·м). Умовна товщина верхнього шару ґрунту: H=0,5 м. Відстань між вертикальними

заземлювачами (електродами) А=2 м. Глибина закладення горизонтального контура заземлення t=0,7 м. Опір заземлювача, який нормується: $R_{ЗН}$ = 4 Ом. Необхідно визначити необхідну кількість вертикальних заземлювачів та довжину полоси (горизонтального заземлювача).

Виконаємо розрахунок.

Відстань від центра вертикального заземлювача до поверхні землі:

$$T= t + L/2 = 0,7 +1,5/2 =1,45 \text{ м.}$$

Розрахунковий питомий опір ґрунту (з врахуванням того, що фактично вся конструкція заземлювача розташовується у нижньому шарі ґрунту):

$$\rho = \psi \rho =1,36\cdot40=54,5 \text{ Ом·м.}$$

де

ψ = 1,36 – табличне значення коефіцієнта сезонності для відповідної кліматичної зони у багатошаровому ґрунті [11];

ρ_2= 40 Ом·м. – табличне значення питомого опору нижнього шару ґрунту (глина) [11].

Діаметр вертикального електрода (задано) Dв= 35 мм = 0,035 м.

Відношення A/L=2/1,5=1,33.

Опір розтіканню електричного струму одного електрода вертикального заземлювача з урахуванням заглиблення заземлювача [11]:

$$R_O= 0,366\cdot(\rho/L)\cdot[\lg(2L/Dв)+(1/2)\cdot\lg((4T+L)/(4T-L))]=$$

$$= 0,366\cdot(54,5/1,5)[(\lg(2\cdot1,5/0,035)+(1/2)\cdot\lg((4\cdot1,45+1,5)/(4\cdot1,45-1,5))]=27,2 \text{ Ом.}$$

Визначаємо коефіцієнт екранування вертикальних електродів Кев=0,53 при орієнтовній кількості вертикальних електродів, яке дорівнює 5 [11].

Визначаємо необхідну кількість вертикальних електродів заземлювача (без врахування горизонтального заземлювача), при $R_{ЗН}$ = 4 Ом :

$$N=R_O /(Кев\ R_{ЗН})= 27,2 / (0,53\cdot4)=12,8 \approx 13 \text{ шт.}$$

Визначаємо довжину з’єднуючої полоси:

$$L_П =1,05\cdot A\cdot N= 1,05\cdot2\cdot13=26,9 \approx 30 \text{ м.}$$

Опір розтіканню електричного струму з'єднуючої полоси з урахуванням кліматичного коефіцієнта питомого опору ґрунту $K_П$ [11]:

$$R_П = 0{,}366 \cdot (\rho \cdot K_П / L_П) \cdot \lg(2(L_П \cdot L_П)/(B \cdot t)) =$$

$$= 0{,}366 \cdot (40 \cdot 5/30) \cdot \lg((2 \cdot 30^2)/(0{,}035 \cdot 0{,}7)) = 20{,}6 \text{ Ом}.$$

де $K_П$=5 – табличне значення кліматичного коефіцієнта питомого опору ґрунту для відповідної кліматичної зони для з'єднуючої полоси [11]:

B = 35 мм = 0,035 м.- ширина з'єднуючої полоси (задана).

Загальний опір розтіканню електричного струму заземлювача [11]:

$$R = (R_O \cdot R_П)/(R_O \cdot \eta_П + N \cdot R_П \cdot Кев) =$$

$$= (27{,}2 \cdot 20{,}6)/(27{,}2 \cdot 0{,}55 + 7 \cdot 20{,}6 \cdot 0{,}53) = 3{,}38 \text{ Ом}.$$

де $\eta_П$ = 0,55 – табличне значення коефіцієнта екранування з'єднуючої полоси [11].

Умова $R \leq R_{ЗН}$ виконується ($3{,}38 \leq 4$).

Оскільки R суттєво більше $R_{ЗН}$, зменшимо кількість вертикальних електродів до 11 і виконаємо перерахунок. У результаті остаточно отримали: кількість вертикальних електродів дорівнює 11 при R =3,9 Ом.

Висновки до розділу

Дотримання всіх необхідних умов праці не лише сприяє збереженню здоров'я працівників, а також підвищує ефективність виробництва в цілому. З цих міркувань було здійснено аналіз приміщення, призначеного для праці програмістів, проведено розгляд небезпечних та шкідливих факторів, що негативно впливають на програмістів під час роботи. Можна зробити наступний висновок, що шкідливі та небезпечні виробничі фактори існують практично на будь якому робочому місці. Тільки повна усвідомленість працівника про можливі небезпеки, що можуть підстерігати його на робочому місці та дотримання вимог нормативних актів о питань охорони праці та відповідних рекомендацій фахівців, дозволять значною мірою знизити негативний вплив шкідливих та небезпечних факторів при роботі з комп'ютером на організм людини. Виконано розрахунок захисного штучного заземлення, як одного з ключових факторів безпеки програміста.

9 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи мережевого відеоспостереження на основі використання DirectX.

В межах України в недостатній мірі представлені вітчизняні розробки в цій області.

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти 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 під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти 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.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створені програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Програма реалізована на мові високого рівня Builder C++. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10/11.

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

Для підвищення рівня безпеки запропоновано застосовувати алгоритм RC5.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Проведено маркетингове та економічне обґрунтування ІТ-проєкту, що дозволило визначити ключові фактори успіху даного проекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Хромочкін М.В. Дослідження та програмна реалізація системи мережевого відеоспостереження на основі використання DirectX // Збірник праць молодих науковців ЦНТУ. – Вип. 15. – Кропивницький: ЦНТУ, 2025.

2. Alasdair McAndrew. A Computational Introduction to Digital Image Processing. Chapman & Hall. 2021. 560 p.

3. Peter Shirley, Steve Marschner. Fundamentals of Computer Graphics. 2009

4. Михайло Пічугін, Іван Канкін, Володимир Воротніков Комп'ютерна графіка. Навчальний посібник / Центр навчальної літератури 346 с. 2019р.

5. Маценко В.Г. Комп’ютерна графіка: Навчальний посібник. – Чернівці: Рута, 2009 – 343 с.

6. Інженерна комп’ютерна графіка: підручник / В.В. Проців [та ін.] / М-во освіти і науки України, Нац. гірн. унт-т. – Дніпро: НГУ, 2017. – 247 с.

7. Проців В.В. Прикладна комп'ютерна графіка [Текст]: Навч. посібник / В.В. Проців, К.А. Зіборов, К.М. Бас, Г.К. Ванжа; М-во освіти і наук, Нац. гірн. ун-т. – Д.: НГУ, 2016. – 187 с.

8. Kopf, Johannes and Lischinski, Dani. Depixelizing Pixel Art (англ.) // ACM Trans. Graph. – 2011. – Vol. 30, no. 4. – P. 99:1--99:8.

9. Giachetti, Andrea and Asuni, Nicola. Real-Time Artifact-Free Image Upscaling (англ.) // Trans. Img. Proc.. – 2011. – Vol. 20, no. 10. – P. 2760—2768.

10. 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.

11. 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

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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,

19. 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.

20. 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

21. 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.

22. 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.

23. 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.

24. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

41. 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.

42. 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.

43. 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.

44. 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.

45. 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.

46. 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.

47. 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.

48. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних

систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.

49. Smirnov, O., Kuznetsov, A., Kuznetsova., K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).

50. Смірнов О.А., Дрєєва Г.М. Метод генерування фрактального трафіку за допомогою моделі генератора на графі. Монографія: Інформаційна безпека та інформаційні технології : монографія / за заг. ред. В. С. Пономаренка. – Х. : Вид. Рожко С.Г. 2019. С. 123-139

51. Дрєєва Г.М., Смірнов О.А., Дрєєв О.М. Метод генерування фрактальноподібної числової послідовності на основі скінченного автомату для моделювання трафіку у мережі. Центральноукраїнський науковий вісник. Технічні науки. № 1(32). с. 173-183, 2019.

52. Смірнов О.А., Кавун С.В., Коваленко О.В., Дрєєв О.М. Мережні інформаційні технології. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 159 с.