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 мережевої безпеки побудованої на основі рішень Axis”

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

Керівник проекту
кандидат технічних наук, доцент
_____ Смірнов С.А.
«____» _____ 2025 р.
Рецензент _____
_____

м. Кропивницький

АНОТАЦІЯ

Буханенко Л.А. Дослідження та програмна реалізація системи мережевої безпеки побудованої на основі рішень Axis. 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 мережевої безпеки побудованої на основі рішень Axis.

Метою розробки є дослідження та програмна реалізація системи мережевої безпеки побудованої на основі рішень Axis.

Об'єктом дослідження є процес мережевої безпеки побудованої на основі рішень Axis.

Предметом дослідження є методи мережевої безпеки побудованої на основі рішень Axis.

Методи дослідження базуються на методах захисту інформації у комп'ютерній мережі, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи мережевої безпеки побудованої на основі рішень Axis.

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 Python.

Ключові слова: комп'ютерна інженерія, мережева безпека, Axis

ABSTRACT

Bukhanenko L.A. Research and software implementation of a network security system based on Axis solutions. 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, which is intended for a network security system based on Axis solutions.

The purpose of the development is the research and software implementation of a network security system based on Axis solutions.

The object of the research is the process of network security based on Axis solutions.

The subject of the research is the methods of network security based on Axis solutions.

The research methods are based on methods of information protection in a computer network, methods of mathematical statistics, methods of software development.

The result of the work is the software implementation of a network security system based on Axis solutions.

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 user-friendly 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 Python environment.

Keywords: computer engineering, network security, Axis

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

АРП	–	автоматичне регулювання посилення
АТМ	–	автоматичний телевізійний моніторинг
ЕПТ	–	електронно-променева трубка
ІБ	–	інформаційна безпека
ІС	–	інформаційна система
НСД	–	несанкціонований доступ
ПЗ	–	програмне забезпечення
ПЗЗ	–	прилади із зарядовим зв'язком
СКД	–	системи контролю даних
СЦК	–	система централізованого керування
ТВЛ	–	телевізійні лінії
IP	–	Internet Protocol. Протокол міжмережної взаємодії
PIN-код	–	персональний ідентифікаційний код
TCP	–	Transmission Control Protocol. Протокол керування передачею (даних) Основний транспортний протокол у стеці протоколів TCP/IP. Встановлює зв'язок між двома ПК й організує обмін даними в дуплексному режимі
TCP/IP	–	Transmission Control Protocol/Internet Protocol. Стек протоколів, що забезпечують організацію зв'язку між комп'ютерами в мережі Інтернет

ВСТУП

Актуальність теми. Axis пропонує низку комплексних рішень для відеоспостереження, які працюватимуть для вас сьогодні та завтра, дозволяючи вам бути спокійними. Захистіть себе від зловмисників, проникнення зі зломом, вандалізму чи будь-чого іншого, що може статися, завдяки рішенню для відеоспостереження Axis. Незалежно від потреб вашого бізнесу, ваше життя стане набагато простішим завдяки кільком розумним способам.

Комплексні рішення – це комплексні системи безпеки, адаптовані та перевірені відповідно до ваших конкретних потреб. Axis може запропонувати все: від системи керування відео Axis, такої як Axis Companion або Axis Camera Station, до всіх підключених пристроїв. Кожне рішення буде індивідуальним для потреб бізнесу та може варіюватися від однієї камери на вході до сотні камер та інших пристроїв безпеки, які стежать за кожним сантиметром вашого приміщення.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи мережевої безпеки побудованої на основі рішень Axis.

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

– Огляд існуючих систем мережевої безпеки побудованої на основі рішень Axis.

– Дослідження системи мережевої безпеки побудованої на основі рішень Axis.

– Програмна реалізація системи мережевої безпеки побудованої на основі рішень Axis.

Об'єктом дослідження є процес мережевої безпеки побудованої на основі рішень Axis.

Предметом дослідження є методи мережевої безпеки побудованої на основі рішень Axis.

Методи дослідження базуються на методах захисту інформації у комп'ютерній мережі, методах математичної статистики, методах розробки програмного забезпечення.

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

– Удосконалено метод мережевої безпеки побудованої на основі рішень Axis.

– Розроблено вітчизняний продукт мережевої безпеки побудованої на основі рішень Axis, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі мережевої безпеки побудованої на основі рішень Axis.

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 мережевої безпеки побудованої на основі рішень Axis, 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

Крім розширення лінійки за рахунок випуску власних продуктів, зокрема мережних гучномовців, і організації партнерських програм для розроблювачів додатків і технологічних партнерів, Axis активно купує інших гравців, щоб прискорити реалізацію закінчених рішень. Так, в 2016 році в її состав увійшли ще три компанії:

– 2N – ведучий виробник IP-домофонів;

– Citilog – французький розроблювач рішень для транспортної аналітики;

– Cognimatics – шведський розроблювач вбудовується відеоаналітики, що, для роздрібної торгівлі.

Що б ви не шукали, у лінійці продукції Axis найдуться мережні камери, що відповідають вашим потребам – від міцних моделей для зовнішнього відеоспостереження до малопомітних пристроїв, призначених для установки там, де потрібен особливий контроль.

Камери Axis відрізняються чудовою якістю зображення з розв’язною здатністю HDTV при будь-якому рівні освітлення й умовах експлуатації. Завдяки інноваційним технологіям зменшується обсяг трафіку й знижується розмір файлів на диску, що допомагає заощаджувати електроенергію.

А застосунки для аналізу відеоматеріалів, розроблені у даній роботі, перетворюють мережні камери в інструменти керування бізнесом. Подібне ПЗ попереджає вас про ситуації, що розвиваються, і допомагає приймати обґрунтовані рішення в роботі й по розподілі ресурсів. Дані можна також інтегрувати з іншими системами об'єкта.

1.2 Область застосування

Метою установки звичайно є перегляд простору перед дверима, ліфтом і виходом на сходи, якщо це квартира, і всі входи й під'їзди до будинку, якщо це заміський будинок. Часто камери встановлюються на ділянках біля будинків, де гуляють діти. Саме головне для створення правильної системи – це точно визначити її мети й завдання, правильно підібрати встаткування й місце установки камер. Саме тому при створенні системи відеоспостереження завжди бажано технічне обстеження об'єкта й складання проекту.

У професійній сфері системи відеоспостереження прийнято підрозділяти на два види залежно від використовуваного встаткування: аналогові й цифрові.

Що таке відеоспостереження й навіщо воно потрібно?

Відповідь на це питання з кожним днем стає очевидним усе більше широкому колу людей. Останні події у світі ще раз нагадали всьому людству, що питанням безпеки потрібно приділяти набагато більше уваги, чим приділяється в цей час. Спектр охоронного встаткування, що забезпечує безпеку людей у цілому, досить широкий і містить у собі пожежну сигналізацію, системи контролю доступу й т.д. Але найбільш активним, а відповідно й важливою ланкою в комплексній системі безпеки є безпосередньо системи відеоспостереження.

Головна перевага електронних систем охорони – цілодобовий моніторинг і запис подій. У випадку виникнення НП оператор охоронних систем може прокрутити запис подій назад і одержати повну інформацію з конкретного НП. У цих випадках керівникам підприємств рекомендується поставитися до системи охоронного відео спостереження більш серйозно, тому що недостатнє вкладення коштів і економія їх приведе до того, що система буде не закінчена й мати «діри».

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи мережевої безпеки побудованої на основі рішень Axis, 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

Вибір найкращих систем безпеки NVR у 2025 році – це не просто захист вашого дому, а й отримання чіткості, контролю та впевненості. Незалежно від того, чи ви спостерігаєте за під'їзною дорогою, складом чи заднім двором, сучасні системи виходять за рамки простого запису. Вони додають інтелекту до кожного кадру.

Сучасна система відеоспостереження поєднує камери високої роздільної здатності, виявлення руху на основі штучного інтелекту, інтелектуальні сповіщення та гнучке сховище. У цьому розділі ми порівнюємо найкращі рішення на ринку – чотири системи безпеки PoE NVR та одну вдосконалену систему камер Wi-Fi NVR з локальним сховищем до 16 ТБ. Кожна з них пропонує інтелектуальні функції, керування на основі додатків та функції, адаптовані для житлових та комерційних потреб.

Ми протестували та відібрали ці системи не лише за їхні характеристики, але й за їхню продуктивність у реальному світі, функції розумного пошуку відео та екосистеми додатків, які дійсно працюють. Давайте розглянемо це.

1. Система безпеки Eufy PoE NVR S4 Max

Це найсучасніший комплект відеоспостереження PoE від eufy на сьогоднішній день. Завдяки потрійним об'єктивним камерам, інтелектуальному відстеженню та потужним фільтрам штучного інтелекту він пропонує неперевершений контроль над великими відкритими та комерційними приміщеннями. Локальна обробка зберігає конфіденційність ваших даних та забезпечує швидкий час відгуку.

Найкраще для:

– Периметри складів та зони в'їзду.

– Великі житлові об'єкти.

– Комерційні під'їзди та вітрини магазинів.

– Бізнес уникає щомісячної плати за хмарні послуги.

Продуктивність та інтелектуальні функції:

– Відстеження між камерами – система відстежує об'єкти зйомки за допомогою кількох камер у режимі реального часу.

– Розумний пошук відео – фільтрація за обличчям (знайоме/невідоме), типом руху або зоною активності.

– Штучний інтелект розпізнає людину, домашню тварину, транспортний засіб та незнайомця.

– Подвійна система оповіщення: червоний/синій прожектор + звукова сигналізація.

– Розумні сповіщення з попереднім переглядом зображень.

Технічні характеристики камери:

– 4× камери з покращеним штучним інтелектом.

– Роздільна здатність: Bullet 4K, PTZ 2K+2K.

– 8× оптичний зум.

– Обертання PTZ на 360°.

– Кольорове нічне бачення з вбудованими прожекторами.

– Корпус із захистом від атмосферних впливів IP65.

– Широкий динамічний діапазон для чіткості тіней/світлої ділянки.

Зберігання та розширення:

– 2 ТБ попередньо встановлений жорсткий диск.

– Розширюваний до 16 ТБ через SATA.

– Не потрібна щомісячна підписка.

– Розумне тегування подій для швидшого перегляду.

Додаток і віддалений доступ:

– Повна інтеграція з мобільним додатком через додаток безпеки eufy.
– Підтримує віддалене відтворення та завантаження.
– Веб-інтерфейс користувача + інтерфейс локального відеореєстратора.
– Підтримка Google Асистента та Alexa.

Налаштування та підключення:

– 100% PoE – стабільні дані + живлення через один кабель.
– Автоматичне сполучення Plug & Play з Eufy NVR.
– Оновлення прошивки камери через додаток.
– Вбудований комутатор PoE у відеореєстраторі.

Переваги:

– Відмінне відстеження об'єктів у різних зонах.
– Відсутність залежності від хмари.
– Професійна чіткість та масштабування.
– Зручний, інтуїтивно зрозумілий додаток з фільтрами.
– Чудова довгострокова цінність для використання бізнес-класу.

Недоліки:

– Вища початкова вартість (~1299 доларів США).
– Надмірне використання для невеликих будинків або квартир.
– Обмежена інтеграція сторонніх камер.

Якщо вам потрібна розумна, автономна система безпеки NVR для критичних зон, S4 Max – одна з найкращих систем NVR, доступних у 2025 році. Її продуктивність штучного інтелекту перевершує більшість конкурентів, особливо для відстеження кількох камер та судово-медичного відеопошуку. Чи то під'їзні шляхи, гаражі чи задні двори, вона розроблена для високоточного спостереження та автономного захисту.

Якщо ви шукаєте компактнішу та бюджетнішу версію, стандартна система безпеки Eufy PoE NVR S4 пропонує той самий інтелектуальний механізм штучного інтелекту та камери 4K – ідеально підходить для невеликих об'єктів.

2. Відеореєстратор Lorex 4K+ 12MP з 16 камерами (8 дротових + 8 Fusion Wi-Fi) 2 ТБ з купольними IP-камерами H30 (N4KPL2-84WD)

Ця система Lorex пропонує ідеальне поєднання надвисокої роздільної здатності (12 МП), підтримки гібридних каналів (8 PoE + 8 Wi-Fi Fusion) та розширюваної продуктивності, що робить її однією з найкращих перспективних систем відеореєстраторів вартістю до 1000 доларів. Завдяки кольоровому нічному баченню, купольним камерам із класом захисту IP67 та інтелектуальним сповіщенням, це надійний варіант для житлових та невеликих комерційних об'єктів.

Найкраще для:

Змішані середовища, де потрібна як стабільність PoE, так і гнучкість Wi-Fi – наприклад, будинки середнього розміру або магазини, яким потрібно 4–8 дротових камер та можливість бездротового розширення.

Продуктивність та інтелектуальні функції:

– Розумне виявлення руху з оповіщеннями про людей/транспортні засоби.

– Кольорове нічне бачення з активним освітленням стримування.

– Віддалений перегляд у реальному часі, відтворення та інтелектуальний пошук через додаток Lorex.

– 16 каналів загалом (8 PoE + 8 Fusion Wi-Fi).

– Push-сповіщення в режимі реального часу та фільтрація подій.

Технічні характеристики камери:

– 8× H30 12MP IP-камери купольного типу (PoE).

– Роздільна здатність: 4512 × 2512 (на 50% більше, ніж 4K).

– Поле зору 111°.

– Клас захисту IP67.

– Розумне подвійне світлодіодне відлякування + інфрачервоне нічне бачення.

Зберігання та розширення:

– 2 ТБ попередньо встановлений жорсткий диск.

– Розширюваний до 16 ТБ (2 відсіки: 1× внутрішній + 1× eSATA).

– Підтримується безперервний запис 24/7.

– Автоматичне перезаписування та планування резервного копіювання.

Додаток і віддалений доступ:

– Додаток Lorex Home для iOS/Android.

– Розумні сповіщення, зони руху та хмарний шлюз.

– Безпечне локальне керування за допомогою веб/NVR графічного інтерфейсу.

Налаштування та підключення:

– Plug-and-play PoE через CAT5e (100 футів на камеру в комплекті).

– Підтримка камер ONVIF (для розширення від сторонніх виробників).

– Fusion Wi-Fi дозволяє додавати бездротові камери Lorex.

– Відеореєстратор з подвійним виходом HDMI/VGA та резервним копіюванням через USB.

Переваги:

– Надвисока якість зображення 12 МП.

– Міцна, захищена від несанкціонованого доступу купольна конструкція.

– Гнучке розширення завдяки 16-канальному гібридному входу.

– Чисте встановлення з кабелями PoE, що входять до комплекту.

– Чудова ціна під час активної знижки.

Недоліки:

– Немає функцій PTZ, таких як автоматичне відстеження або оптичний зум.

– Бракує інтелектуальної фільтрації за обличчям або типом об'єкта (немає механізму штучного інтелекту).

– Немає інтеграції голосового помічника.

Якщо вам потрібен комплект відеоспостереження PoE, який поєднує надійність дротового з’єднання з майбутньою масштабованістю бездротового зв’язку, ця система відеореєстратора Lorex забезпечує найвищу роздільну

здатність та довговічність обладнання. Це вигідний вибір, якщо вам потрібна система відеоспостереження, яка не залежить від підписок та працює вдень і вночі.

3. Спеціальний комплект UniFi Protect: UNVR + G6 PTZ, Bullet & Turret

На відміну від багатьох готових систем відеоспостереження NVR, UniFi не продає повний комплект зі своїми останніми моделями G6. Але це не недолік. Ця збірка була налаштована на замовлення з використанням найсучасніших компонентів для досягнення максимально можливої функціональності штучного інтелекту. Ми протестували її з двома PTZ-камерами G6, однією камерою G6 Bullet, однією туреллю G6 Turret та UNVR для зберігання даних. Результат? Повністю масштабована система відеоспостереження на базі штучного інтелекту, яка може конкурувати з будь-яким комерційним рішенням.

Найкраще для:

Досвідчені користувачі та професіонали, які хочуть повного контролю над своєю інфраструктурою. Ідеально підходить для офісів, маєтків, ферм або будь-кого, хто вже інвестував в екосистему UniFi.

Продуктивність та інтелектуальні функції:

– Повний пакет штучного інтелекту, включаючи розпізнавання людей, тварин, транспортних засобів, облич та номерних знаків.

– 10-кратний гібридний зум та автоматичне відстеження на PTZ-камерах.

– HDR, розширене ІЧ-підсвічування та нічне бачення з натуральними кольорами.

– Розумне маскування, зони руху на основі площі та часові шкали з кількома камерами.

– Сповіщення в режимі реального часу через додаток або електронну пошту.

– Підтримує безперервний запис для 18 камер 4K (з відповідними накопичувачами).

Технічні характеристики камери:

– G6 PTZ: подвійний об'єктив 4K з сенсорами 1/1.8 дюйма, 10-кратний гібридний зум, відстеження повороту та нахилу.

– G6 Bullet: сенсор 4K, кут огляду 134°, захист від атмосферних впливів, інфрачервоне освітлення до 98 футів.

– Револьверна головка G6: сенсор 4K, вандалостійка, гнучке 3-осьове встановлення.

– Усі моделі: IP66, IK04, відповідають вимогам NDAA, працюють на базі штучного інтелекту з процесорами Multi-TOPS.

Зберігання та розширення:

– UNVR вміщує до чотирьох 3,5-дюймових жорстких дисків.

– Зберігайте до 30 днів відеозаписів з камер 18× 4K.

– Підтримка RAID для захисту даних.

– Додаткові відеореєстратори Protect NVR можна розгорнути для розподіленого зберігання даних..

Додаток і віддалений доступ:

– Повний контроль через UniFi Protect (з комп'ютера, мобільного пристрою, веб-сайту).

– Доступ на основі ролей для кількох користувачів.

– Очищення часової шкали, фільтри Smart Detection, експорт знімків.

– UniFi Viewport (опціонально) для виходу HDMI на монітор.

Налаштування та підключення:

– Рекомендовано використовувати комутатор PoE+ (через споживання енергії PTZ).

– Для повного доступу до хмари потрібен UniFi Gateway або сумісний маршрутизатор.

– Модульний та масштабований: додавайте камери, контроль доступу, дверні дзвінки, датчики тощо..

– Легке встановлення та оновлення через UniFi Controller.

Переваги:

– Максимальна функціональність штучного інтелекту та справжнє 4K на всіх камерах.

– Повністю налаштовувана та масштабована система.

– Найплавніший інтерфейс програми та часової шкали в галузі.

– Сильна спільнота, швидка розробка прошивки.

Недоліки:

– Не є попередньо упакованою системою: її необхідно зібрати.

– Потрібен комутатор PoE+ та сумісний маршрутизатор.

– Вища початкова вартість (~$1600+ з урахуванням сховища).

– Невелика крива навчання для нових користувачів.

Ця система розширює межі можливого в комплекті відеоспостереження для житлових приміщень або малого та середнього бізнесу. Хоча вона не продається в комплекті, її гнучкість та продуктивність не мають собі рівних. Якщо ви серйозно ставитеся до відстеження за допомогою штучного інтелекту, інтелектуальних сповіщень та довгострокової масштабованості, то це саме та система, яку варто створити.

4. RLK8-1200V4 – Розумна 12-мегапіксельна система відеоспостереження IK10 PoE з кутом огляду 145°

Reolink RLK8-1200V4 забезпечує рідкісну роздільну здатність 12 Мп з надшироким кутом огляду 145°, нічним баченням підсвічуванням та вандалозахисною купольною конструкцією IK10. Це одна з найбільш збалансованих систем PoE типу "підключи та працюй" з надійним фізичним захистом та непомітною естетикою.

Найкраще для:

Спостереження на ширшій території, де важливі як деталізація, так і захист від несанкціонованого доступу – ідеально підходить для вітрин магазинів, монтажу на низькій висоті або компактних зовнішніх приміщень.

Продуктивність та інтелектуальні функції:

Завдяки розпізнаванню людей, транспортних засобів і тварин, підсвічуванню прожектором і двосторонньому аудіо, він забезпечує чітке відео та функцію стримування в режимі реального часу. Усі функції працюють локально, без необхідності підписки.

Технічні характеристики камери:

– Роздільна здатність 12 МП (4512×2512).

– Кут зору 145° (об'єктив 2,8 мм).

– Кольорове нічне бачення з подвійними прожекторами 3000K.

– ІЧ-світлодіоди до 30 м (100 футів).

– Вбудований мікрофон і динамік.

– вандалозахисний корпус IK10.

– Захист від атмосферних впливів IP67.

Зберігання та розширення:

– 8-канальний відеореєстратор з попередньо встановленим жорстким диском на 2 ТБ.

– Можливість розширення до 16 ТБ (через eSATA).

– Цілодобовий запис або запис за рухом.

Додаток і віддалений доступ:

Додаток та клієнт Reolink підтримують перегляд у реальному часі, двосторонній розмова, інтелектуальне відтворення, зони руху та миттєві сповіщення. До 20 облікових записів користувачів.

Налаштування та підключення:

– PoE (живлення через Ethernet) – адаптери живлення на камері не потрібні.

– Налаштування «підключи та працюй».

– Сумісний з іншими камерами Reolink PoE та деякими Wi-Fi пристроями.

Переваги:

– Ультраширокий огляд 145° на кожну камеру.

– Чіткість 2 МП та повнокольорове нічне бачення.

– Вандалостійкість класу K10.

– Доступне та надійне локальне сховище (2 ТБ).

– Відмінний додаток та зручний графічний інтерфейс.

Недоліки:

– За замовчуванням включено лише 4 камери.

– Немає функцій PTZ або автоматичного відстеження.

– Купольні камери не оптимальні для монтажу на великі відстані.

– Немає фільтрації смарт-об'єктів за обличчям або поведінкою ШІ.

Для користувачів, які надають перевагу непомітному встановленню, захисту від вандалів та надзвичайно широким кутам огляду, RLK8-1200V4 є одним із найрозумніших варіантів PoE на цьому рівні роздільної здатності. Він особливо привабливий для тих, хто хоче уникнути передплати, зберігаючи при цьому високу деталізацію безпеки.

5. Aosu 4K SolarCam P1 Max з системою HomeCortex

Aosu пропонує рідкісне поєднання бездротових камер 4K на сонячній енергії з функцією виявлення об'єктів на базі штучного інтелекту та розширюваним локальним сховищем до 16 ТБ. Це робить її однією з найповніших безкоштовних систем відеоспостереження NVR для користувачів розумного дому.

Найкраще для:

Тим, хто шукає повністю бездротову систему камер на сонячній енергії, що забезпечує сповіщення від штучного інтелекту в режимі реального часу та має величезні можливості локального зберігання даних – ідеально підходить для домашнього використання без щомісячної плати.

Продуктивність та інтелектуальні функції:

– 4K UHD відео з повнокольоровим та інфрачервоним нічним баченням.

– Розпізнавання людей, транспортних засобів, тварин та незнайомих облич на основі штучного інтелекту.

– Розумний пошук за допомогою запитів на основі речень.

– Відстеження між камерами IntelliMesh.

– Розпізнавання поведінки та звіти про активність.

– Двосторонній розмова зі зміною голосу та сповіщення в режимі реального часу.

– Інтеграція з Alexa та Google Assistant.

Технічні характеристики камери:

– Роздільна здатність: 3840×2160 (4K UHD) при 15 кадрах/с.

– Поле зору: 130°.

– Зум: 6-кратний цифровий зум.

– Аудіо: 2-смуговий (мікрофон і динамік), сирена 105 дБ.

– Нічне бачення:.

o ІЧ-світлодіоди для чорно-білого зображення.

o 16 білих світлодіодів для повнокольорового підсвічування.

– Живлення: Вбудована сонячна панель + акумулятор 5000 мАг.

– Клас захисту від атмосферних впливів: IP65.

– Розміри: 5,12 × 3,94 × 2,36 дюйма.

Зберігання та розширення:

– Концентратор HomeCortex має 32 ГБ вбудованої пам'яті.

– Розширюваний до 16 ТБ за допомогою 2,5-дюймового жорсткого диска/SSD (продається окремо).

– Кожна камера підтримує microSD до 128 ГБ.

– Без обов'язкової підписки, доступний додатковий хмарний план.

Додаток і віддалений доступ:

– Перегляд у реальному часі та відтворення через мобільний додаток aosu.

– Розумні фільтри штучного інтелекту та доступ до розпізнавання обличчя.

– Сповіщення в режимі реального часу з попереднім переглядом зображень.

– Підтримує спільний доступ для членів сім'ї.

Налаштування та підключення:

– 100% бездротова, plug-and-play сонячна установка.

– Хаб HomeCortex розширює сигнал Wi-Fi.

– Синхронізація подій між камерами.

– Підключення через Wi-Fi 2,4 ГГц; HomeCortex вимагає підключення до Ethernet для маршрутизатора.

– Повне налаштування на камеру займає менше 2 хвилин.

Переваги:

– Підписка не потрібна.

– Величезний розширюваний локальний сховище об'ємом 16 ТБ.

– Розширене виявлення поведінки ШІ.

– Справжня робота від сонячної енергії з швидким налаштуванням.

– Широка інтеграція з розумним будинком.

– Кольорове нічне бачення та розумне розпізнавання людей.

Недоліки:

– Немає резервного живлення від PoE або Ethernet для камер.

– Частота кадрів обмежена 15 кадрами в секунду.

– Хаб має бути підключений до маршрутизатора.

– Немає підтримки NVR – покладається на власний HomeCortex.

Aosu 4K SolarCam P1 Max – один із найсучасніших комплектів бездротового відеоспостереження, доступних для приватних користувачів. Хоча йому бракує опцій Ethernet та сумісності з професійним відеореєстратором, його локальна обробка на базі штучного інтелекту, гнучке джерело живлення та надвисокої чіткості зображення роблять його сильним претендентом на автономні або сонячні установки. aosu також розумно надала пріоритет довгостроковій цінності, відмовившись від підписок на користь масштабованого локального сховища.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Python – динамічна інтерпретована об'єктно-орієнтована скриптова мова програмування із строгою динамічною типізацією. Офіційний сайт мови програмування Python https://www.python.org/. Python – багатоцільова мова програмування, яка дозволяє писати код, що добре читається. Відносний лаконізм мови Python дозволяє створити програму, яка буде набагато коротше свого аналога, написаного на іншій мові. Python – багатоплатформова мова програмування. Це означає, що програми на Python можна запускати в різних операційних системах без будь-яких змін.

Ще однією перевагою Python є його стандартна бібліотека, яка встановлюється разом з Python і містить готові інструменти для роботи з операційною системою, веб-сторінками, базами даних, різними форматами даних, для побудови графічного інтерфейсу програм тощо. Програми, написані на мові програмування Python, можуть бути як невеликими скриптами, так і складними системами. Python абсолютно безкоштовний.

Швидкість виконання коду Python

Один з можливих недоліків Python – швидкість виконання коду. Python не є компільованою мовою. Код на Python спочатку компілюється у внутрішній байт-код, який потім виконується інтерпретатором Python. У більшості випадків при використанні Python виходять програми повільніші в порівнянні з такими мовами, як C.

Втім, сучасні комп'ютери мають таку обчислювальну потужність, що для більшості застосунків швидкість розробки важливіша швидкості виконання, а програми на Python зазвичай пишуться набагато швидше.

Окрім того, Python легко розширюється модулями, написаними на C або C++. Такі модулі можуть використовуватися для виконання частин програми, що створюють інтенсивне навантаження на процесор.

Використання Python

Python використовується для різних цілей: для створення ігор і веб-застосунків, розробки внутрішніх інструментів для різноманітних проектів. Мова також широко застосовується в науковій області для досліджень і розв'язування прикладних завдань.

Застосування мови програмування Python:

1. BitTorrent – протокол для обміну даними.

2. Ubuntu Software Center – вільне програмне забезпечення для пошуку, установки і видалення пакунків в системі Ubuntu Linux.

3. Blender – програма для створення тривимірної комп'ютерної графіки, що включає засоби моделювання, анімації, вимальовування, пост-обробки відео, а також створення відеоігор.

4. GIMP – растровий графічний редактор, із підтримкою векторної графіки.

5. World of Tanks.

6. Вільна енциклопедія Вікіпедія.

7. Пошукова система Google.

8. DropBox – файловий хостинг, що включає персональне хмарне сховище, синхронізацію файлів і програму-клієнт.

9. YouTube – популярне відеосховище.

Версії Python

Мови програмування з часом змінюються – розробники додають в них нові можливості, а також виправляють помилки. Так з'являються різні версії мови. Наприклад, код написаний на Python 2 у більшості випадків не буде працювати у версії Python 3 без внесення додаткових змін.

Процесор є найважливішим компонентом в комп'ютері. Одна з основних функцій процесора – це обробка даних згідно комп'ютерної програми, яка є списком інструкцій, шляхом виконання арифметичних і логічних операцій над фрагментами даних.

Кожна інструкція в програмі – це команда, яка «повідомляє» процесору, яку операцію він повинен виконати. Процесор комп'ютера може розуміти лише ті інструкції, які написані на машинній мові. Машинна мова – це штучна мова, створена для передачі команд комп'ютеру. За допомогою машинної мови створюються ефективні програми, оскільки розробник отримує доступ до всіх можливостей процесора. Машинна мова – мова низького рівня.

Інструкція машинної мови існує для кожної операції, яку процесор здатний виконати – є інструкція для додавання чисел, є інструкція для віднімання чисел і т.д. Увесь набір інструкцій, який центральний процесор може виконати, відомий як набір інструкцій процесора.

Наприклад, у вас є певна програма, яка зберігається на диску вашого комп'ютера. Для виконання програми, ви здійснюєте подвійний клік на значку програми. Це змушує програму копіюватися з диска в оперативну пам'ять, після чого процесор комп'ютера виконує копію програми, яка знаходиться в оперативній пам'яті.

Коли процесор виконує інструкції програми, він бере участь у процесі, який є відомим як цикл fetch – decode – execute (отримати – декодувати – виконати). Цей цикл виконується для кожної інструкції у програмі і складається з трьох кроків:

Отримати

Програма – це послідовність інструкцій на машинній мові. Першим кроком циклу є завантаження (отримання) наступної інструкції з пам'яті в процесор.

Декодувати

Інструкція машинної мови – це двійкове число, яке представляє команду, що повідомляє процесору виконати певну операцію. На цьому кроці процесор декодує інструкцію, яку було «витягнуто» з пам'яті, для визначення того, яка операція повинна виконуватись.

Виконати

Останній крок циклу – виконати операцію.

Хоча процесор комп'ютера розуміє тільки машинну мову, людині непрактично писати програми на машинній мові. Така програма може мати тисячі або навіть мільйони бінарних інструкцій, і написання такої програми буде дуже обтяжливим процесом.

З цієї причини була створена мова асемблера як альтернатива машинній мові. Замість використання двійкових чисел для написання інструкцій, мова асемблера використовує короткі слова, відомі як мнемокоди.

Незважаючи на те, що мова асемблера не вимагає двійкових інструкцій, як у випадку машинної мови, проте вона вимагає високих знань про процесор. Використовуючи мову асемблера, навіть для найпростішої програми, необхідно написати велику кількість інструкцій.

Мова програмування високого рівня дозволяє створювати складні програми, не знаючи, як працює процесор, і не записуючи великої кількості інструкцій низького рівня. Крім того, більшість мов програмування високого рівня використовують слова, які легко зрозуміти.

Python – одна із популярних сучасних мов програмування високого рівня. Python – інтерпретована мова програмування. Python – це високорівнева інтерпретована мова програмування, на відміну від C++, яка є прикладом компільованої мови програмування. Назва Python відноситься як до мови програмування, так і до інтерпретатора – комп'ютерної програми, яка зчитує початковий код (написаний на Python) і виконує інструкції (команди).

Для перекладу мови високого рівня на машинну мову доступні два типи програм:

1. Компілятор.

2. Інтерпретатор.

Завантаження Python

Версії інтерпретатора Python для різних операційних систем доступні для безкоштовного завантаження за адресою https://www.python.org/downloads.

Середовище програмування для Python

Для написання програм використовують текстові редактори або інтегровані середовища розробки, які включають в себе різні інструменти для роботи з кодом: засіб для написання коду (текстовий редактор), інтерактивний інтерпретатор, відлагоджувач тощо.

Текстові редактори та інтегровані середовища програмування для Python:

– IDLE – стандартний редактор Python. Встановлюється разом з Python для користувачів Windows, окремим пакунком для користувачів Linux.

– Notepad++ – безкоштовний текстовий редактор початкового коду, який підтримує велику кількість мов, в тому числі і Python. Лише для користувачів Windows.

– Visual Studio Code – це легкий, але потужний редактор початкового коду, який розповсюджується безкоштовно і доступний у версіях для платформ Linux, Windows і macOS.

– PyScripter – інтегроване середовище розробки для мови програмування Python. Для користувачів Windows. Поширюється безкоштовно.

– Wing IDE 101 – вільне інтегроване середовище для Python, розроблене для навчання програмістів-початківців. Для користувачів Linux, Windows і macOS. Поширюється безкоштовно.

– Geany – вільний текстовий редактор з базовими елементами інтегрованого середовища розробки, доступний для операційних систем Linux, Windows і macOS.

– PyCharm – інтегроване середовище розробки для мови програмування Python. PyCharm є власницьким програмним забезпеченням. Наявна безкоштовна версія Community з усіченим набором можливостей. Для користувачів Linux, Windows і macOS.

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 мережевої безпеки побудованої на основі рішень Axis.

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

Axis пропонує інструмент Designer, який спростить проектування вашого комплексного рішення для відеоспостереження. Він також надасть вам корисну документацію з встановлення та можливість експортувати конфігурації, щоб уникнути помилок під час встановлення. Цей інтуїтивно зрозумілий інструмент спрощує робочий процес проектування та складання кошторисів, роблячи проєкти швидшими та простішими для створення, редагування або впровадження.

Лінійка відеореєстраторів Axis – це чудовий спосіб розпочати створення комплексного рішення. Це готові до використання рішення, які забезпечують надійне відеоспостереження високої чіткості. Попередньо завантажені всім необхідним програмним забезпеченням і ліцензіями для вашої системи, ці рішення для запису можуть задовольнити вимоги широкого кола бізнес-потреб і галузей. Якщо вам потрібне безпечне та надійне відеоспостереження, це ідеальне рішення для вас.

Axis Companion – це просте та зручне програмне забезпечення для керування відео, яке інтегрується з камерами, домофонами та аудіопродукцією Axis. Це ідеальний вибір для підприємств з невеликими об'єктами, яким потрібна проста у використанні система, наприклад, роздрібні магазини.

Axis Camera Station – це потужна та проста у використанні, повнофункціональна система керування відео, яка легко інтегрується з іншими продуктами Axis. Пропонує повну, гнучку, безпечну та надійну систему, що ідеально підходить для великих підприємств, таких як школи, роздрібна торгівля та виробництво.

Купуючи комплект для відеоспостереження, легко зосередитися на

кількості камер або роздільній здатності. Але у 2025 році розумний захист означає глибший пошук, особливо якщо вам потрібна надійність, швидкість та моніторинг без використання рук. Ось що дійсно важливо.

Роздільна здатність та якість камери

Розумна система відеоспостереження повинна забезпечувати більше, ніж просто HD. У 2025 році базовим стандартом буде 4K. Звертайте увагу на широкий динамічний діапазон, гібридний зум та кольорове нічне бачення, щоб чітко фіксувати обличчя, номерні знаки та критичні події в режимі реального часу.

Кількість каналів

Масштабованість має значення. Система відеоспостереження NVR з 8 або 16 каналами дозволяє розширити покриття пізніше – ідеально підходить для зростаючих домогосподарств або підприємств зі складними периметрами.

Місткість та можливості розширення

Найкраща система безпеки NVR повинна пропонувати щонайменше 2 ТБ локального сховища, бажано з можливістю розширення до 16 ТБ. Завдяки цілодобовому запису та відео високої роздільної здатності ємність швидко вичерпується. Локальне сховище також зменшує залежність від хмари.

Інтеграція мобільних додатків та віддалений перегляд

Кожна система з цього списку підтримує інтеграцію з мобільними додатками. Ви отримуватимете миттєві сповіщення, історію подій та прямі трансляції безпосередньо на свій телефон – з будь-якого місця. Бонусні бали за системи з графічним інтерфейсом на основі браузера та без абонентської плати.

Виявлення руху та сповіщення штучного інтелекту

Розумний штучний інтелект допомагає фільтрувати рух – не кожна тінь чи гілка повинна спрацьовувати тривога. Сучасні системи виявляють людей, домашніх тварин та транспортні засоби, а деякі пропонують сповіщення на основі облич або розпізнавання незнайомців для більшої точності.

Нічне бачення та розумне ІЧ-підсвічування

Інфрачервоне підсвічування входить до стандартної комплектації. Чудовою системою є кольорове нічне бачення, інтелектуальна адаптація ІЧ-підсвічування та система відлякування на основі прожектора. Чітке нічне відео означає, що ви не пропустите те, що відбувається після настання темряви.

Розумний пошук відео

Одним з найбільших проривів 2025 року є пошук відео на основі штучного інтелекту. Фільтрація за обличчям, об'єктом, рухом, часом або навіть певними зонами. Це скорочує час розгляду інциденту з годин до хвилин.

PoE проти бездротової інфраструктури

Системи відеоспостереження PoE NVR забезпечують швидкість та надійність завдяки одному кабелю. Бездротові комплекти пропонують гнучке розміщення, але можуть страждати від перешкод або перебоїв з'єднання. Оберіть PoE для критично важливих установок, Wi-Fi для гнучкості.

Локальне та хмарне сховище

Багато систем пропонують обидва варіанти. Деякі забезпечують гібридне сховище з кліпами подій у хмарі та повними записами локально. Ми ж віддаємо перевагу системам з локальним сховищем насамперед – для швидкості, конфіденційності та доступу офлайн.

Штучний інтелект та відстеження Cross-Cam

Високоякісні системи відеоспостереження NVR тепер включають крос-камерний штучний інтелект, що дозволяє відстежувати один об'єкт від камери до камери. Це революційно впливає на периметри бізнесу та об'єкти з широким кутом огляду.

Налаштування та екосистема програм

Простота налаштування має значення. Підключення через PoE або бездротове з’єднання за принципом «підключи та працюй», зрозумілі інтерфейси додатків, інтелектуальне керування зонами та швидке оновлення прошивки – все це додає довгострокової цінності.

Співвідношення ціни та якості

Зрештою, комплект відеокамери має окупати інвестиції. Важлива не лише початкова вартість, а й те, як довго він служить, наскільки добре захищає та наскільки ним легко користуватися.

3.2 Розробка структурної схеми

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis – це програмна платформа для керування, моніторингу та обслуговування рішень для відеоспостереження на основі мережевих камер та IP-пристроїв Axis. Зручність для системних інтеграторів та клієнтів лежить в основі програмного забезпечення мережевої безпеки побудованої на основі рішень Axis: воно проста в установці, просте у використанні та спрощує обслуговування комплексного рішення для відеоспостереження. Регулярний потік удосконалень означає, що програмне забезпечення мережевої безпеки побудованої на основі рішень Axis йде в ногу з інноваціями в технологіях, як у самому програмному забезпеченні для керування відео, так і у зв'язку зі зростанням кількості та типу пристроїв, підключених до систем спостереження.

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis забезпечує основу для створення перевіреного комплексного рішення на основі технологій Axis. Воно ідеально відповідає повному портфоліо IP-продуктів та функцій Axis, пропонуючи клієнтам повну, гнучку та надійну систему. Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis легко встановлюється, а завдяки своєму інтуїтивно зрозумілому інтерфейсу користувача вона проста у використанні.

Програмне забезпечення для керування відео на основі рішень Axis є основою комплексного рішення Axis. Комплексне рішення складається з:

– Клієнтське та серверне програмне забезпечення: обробляє весь зв'язок з камерами та допоміжними пристроями в системі, керує правами користувачів та

забезпечує взаємодію з відео в реальному часі та записаними відео, а також керування системою, функції обслуговування та журнали.

– Безпечний вхід: вбудований у програмне забезпечення Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis та забезпечує функції контролю доступу при додаванні контролерів дверей AXIS A1601

– Мережеві відеореєстратори: прості в установці та надійні рішення для запису, ідеально адаптовані до широкого спектру мережевих продуктів Axis

– Мобільний додаток для перегляду: забезпечує дистанційний перегляд відео та записів у реальному часі, а також живий зв'язок з відвідувачами та керування дверима на мобільних пристроях

– Підтримка повного портфоліо IP-підключених продуктів Axis, включаючи відеокамери, натільні камери, аудіопристрої, домофони та контролери дверей, радари

– Доступ до потужних аналітичних програм для покращення рішення для відеоспостереження, включаючи AXIS License Plate Verifier, AXIS Guard Suite, AXIS Perimeter Defender, AXIS Object Analytics та інші.

Для системних інтеграторів пакет Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis Integrator Suite – це набір інструментів, які допомагають інтеграторам проектувати, розгортати та обслуговувати рішення Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis, і включає AXIS Site Designer, AXIS Installation Verifier та Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis System Health Monitoring.

У широкому сенсі, можливості програмного забезпечення мережевої безпеки побудованої на основі рішень Axis стосуються перегляду відео в реальному часі, відтворення та пошуку відео, аудіо, контролю доступу, а також управління системами та користувачами.

Перегляд відео в реальному часі

Програмне забезпечення мережевої безпеки побудованої на основі рішень

Axis дозволяє створювати налаштований робочий простір з миттєвим доступом до зображень і камер у системі, а також інтеграцією планів поверхів і зовнішніх веб-сторінок. Ключовим фактором є максимальна гнучкість, що відповідає потребам будь-якого оператора. Підтримка кількох моніторів (наприклад, для поєднання перегляду в реальному часі та записаного зображення), визначені користувачем кнопки дій і програмовані гарячі клавіші вбудовані як стандартні функції. Також у стандартну комплектацію входять інтерактивні карти, екранні елементи керування для функцій камер, таких як керування склоочисниками PTZ-камери, і профілі відеопотоку, вибрані оператором.

Щоб забезпечити перегляд відео найвищої якості, програмне забезпечення мережевої безпеки побудованої на основі рішень Axis дозволяє одночасно синхронізувати відео в реальному часі з різних серверів та/або сайтів, а також, за наявності відповідного клієнта та дисплея, підтримує камери високої роздільної здатності UltraHD 4K для чіткої ідентифікації інцидентів.

Кілька функцій, зокрема виправлення спотворень на 360 градусів, формат коридору Axis та багатосенсорне зшивання зображень, забезпечують повний огляд без сліпих зон. Оператори можуть визначати цифрові попередньо встановлені позиції зон інтересу, гнучко налаштовувати зображення, поєднуючи карти, веб-сторінки, камери тощо, а також створювати віртуальні обходи охоронців для автоматичного огляду будь-якої ділянки.

Сигналізація та сповіщення можуть бути налаштовані таким чином, щоб негайно привертати увагу операторів до певних сцен і автоматично запускати відеозапис і аудіооголошення. Сповіщення можна надсилати в мобільний додаток Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis, що дозволяє операторам реагувати на інциденти та розслідувати їх у режимі реального часу, а також вживати необхідних заходів з будь-якого місця.

Покращене відтворення та пошук

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis також надає багатий функціонал для відтворення відео. Це включає

синхронізоване, одночасне відтворення з кількох камер та різних серверів, а також перемикання відео, швидке відтворення та покадровий перехід, що дозволяє операторам швидко та точно знаходити ділянки відео, що мають певний інтерес.

Це ще більше покращується завдяки функції Smart Search 2, яка дозволяє операторам швидко шукати у відеоматеріалах людей та транспортні засоби, що цікавлять їх. Smart Search 2 працює на основі даних про рух об'єктів з камери Axis, які можна додатково обробляти за допомогою методів машинного та глибокого навчання для швидкої класифікації об'єктів, таких як люди, автомобілі, вантажівки та велосипеди.

Окремі розділи відео, що становлять особливий інтерес, можна анотувати за допомогою закладок, коментарів і нотаток, а також експортувати для сприяння розслідуванню та побудові справ. Справи можна упакувати в захищену паролем zip-папку, а випадки спостереження можна ділитися з іншими завдяки вбудованому файловому плеєру, що полегшує одержувачу перегляд результатів.

Для захисту конфіденційності третіх осіб, знятих на відеоматеріалах, у Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis передбачено редагування відео, яке пропонує можливості маскувати людей та об’єкти на відео перед експортом.

Підтримка мережевого аудіо Axis

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis дозволяє керувати всім портфоліо IP-продуктів Axis, яке включає зростаючу кількість мережевих аудіопристроїв. Підтримуються як аудіовхід, так і аудіовихід: мікрофони, підключені до камер, дозволяють операторам прослуховувати живі сцени, а також забезпечувати аудіозаписи, тоді як живі розмови та попередньо записані повідомлення можна відтворювати або запускати через мережеві динаміки, що дозволяє оператору проактивно запобігати небажаній поведінці, а також звертатися до людей на об'єкті.

AXIS Cameras Station має інтуїтивно зрозуміле керування звуком з

можливістю регулювання гучності або вимкнення вхідного звуку. Оператори можуть прослуховувати кілька джерел звуку та керувати підключеними динаміками для забезпечення живого спілкування.

Для камер Axis із вбудованими динаміками та динаміками Axis функція «натисни і говори» дозволяє операторам отримувати аудіо та надає можливість спілкуватися в режимі реального часу. Після ввімкнення динаміка для будь-якої камери в режимі реального часу відображається кнопка голосового зв’язку.

Інтегрований контроль доступу

Функція контролю доступу вмикається в AXIS Cameras Station після додавання контролерів дверей AXIS A1601. Завдяки зручному інтерфейсу Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis оператори можуть легко налаштовувати контролери дверей та керувати власниками карток.

Об'єднання відео та контролю доступу дозволяє перевірити вхід за допомогою відео та миттєво надсилати тривоги контролю доступу співробітникам системи спостереження. Це також спрощує розслідування, дозволяючи шукати події контролю доступу за допомогою синхронізованого відео.

Налаштування автоматизованих ланцюжків дій

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis має потужний та простий у використанні механізм правил дій. Оператори можуть вибирати з різних тригерів та дій, що дозволяє налаштовувати автоматизовані дії. Автоматизовані ланцюжки дій допомагають у багатьох відношеннях, розвантажуючи оператора від виснажливої роботи перед екраном, дозволяючи йому проактивно втручатися лише за потреби.

Його також можна використовувати для покращення спостереження та загальної ефективності бізнесу. Наприклад, активація розтяжки від AXIS Fence Guard може ініціювати запис з кількох камер, перемістити PTZ-камеру в певне попередньо встановлене положення, а також потенційно ініціювати

аудіоповідомлення на динаміку, вихід для ввімкнення освітлення та сповіщення оператора.

Управління системою та користувачами

За допомогою Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis можна легко керувати камерами та підключеними IP-пристроями у великих системах та на кількох об'єктах, а також обліковими даними операторів, яким потрібно використовувати та керувати системою. Microsoft Active Directory можна використовувати для полегшення адміністрування користувачів, груп та прав доступу до пристроїв.

Клієнти можуть підключатися до кількох серверів одночасно, щоб отримати повний огляд системи, незалежно від того, чи знаходиться вона на одному чи кількох сайтах. Адміністратори можуть підключатися до кількох сайтів/серверів та налаштовувати параметри будь-якого пристрою, підключеного до системи, включаючи оновлення прошивки пристрою.

Axis Secure Remote Access спрощує доступ до віддалених систем спостереження, усуваючи необхідність ручного переадресації портів та налаштування маршрутизатора. Технологія використовує кілька рівнів автентифікації для встановлення безпечного, зашифрованого зв'язку між клієнтом та системою спостереження.

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis також підтримує покращений захист пристроїв, автоматично генеруючи безпечний випадковий пароль максимальної довжини, що підтримується вибраним(и) пристроєм(ами).

Системи можна масштабувати та підвищувати продуктивність, додаючи більше серверів для підтримки більшої кількості підключених пристроїв та збільшення вимог до сховища.

Крім того, можна використовувати кілька підходів до оптимізації сховища. До них належать керування бітрейтом за допомогою Zipstream, AXIS Average Bitrate – складний метод контролю бітрейту за допомогою стиснення

відео, адаптований для забезпечення постійного виконання вимог щодо часу зберігання, – та визначення часу зберігання відео для кожної окремої камери.

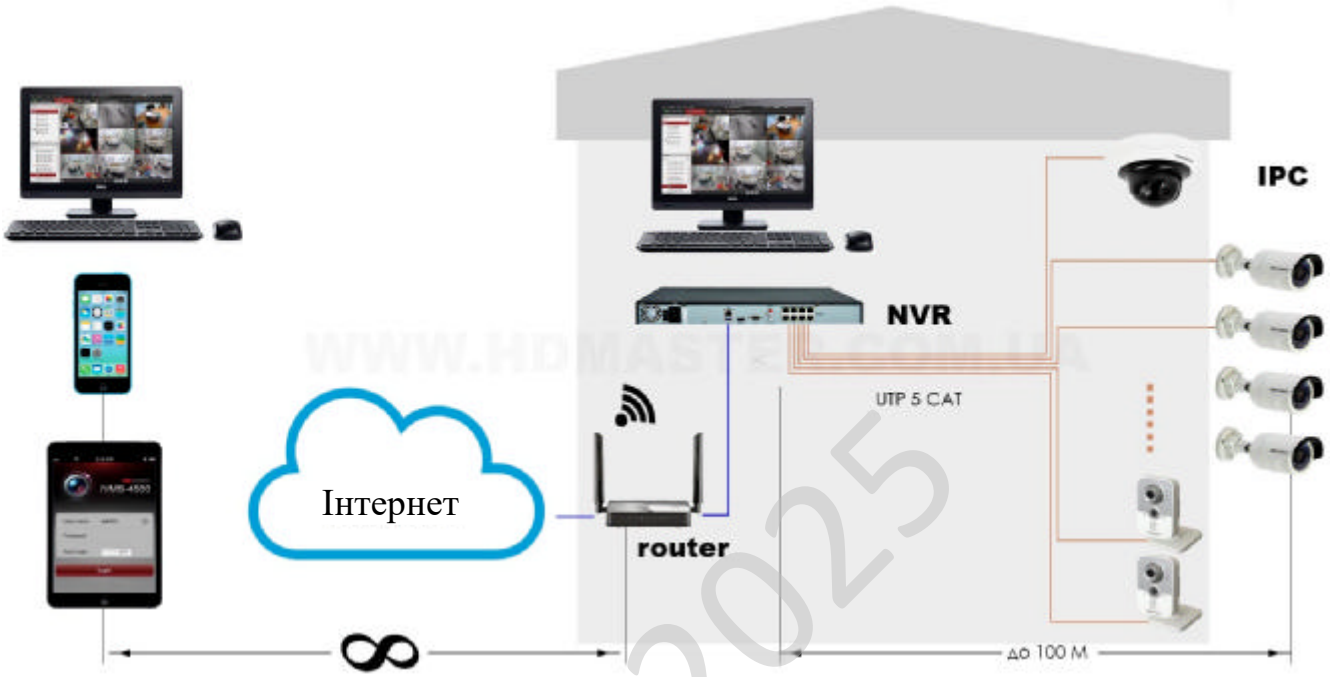

Рисунок 3.1 – Структурна схема системи

3.3 Розробка функціональної схеми

На рисунку 3.2 зображена функціональна схема системи. Найпершим блоком у схемі є кінцевий об'єкт (сектор) за яким власне і ведеться відеоспостереження. Далі за допомогою відеокамер спостереження фірми Axis за розробленою схемою (рисунок 3.1) і застосуванні локального обладнання фірми Axis сигнал надходить у кімнату операторів де обробляється на сервері за допомогою розробленого ПЗ.

Спочатку проходить обробка даних з послідуючим аналізом. Всі дані зберігаються у файловому архіві у форматі *.avi. Кожну добу інформація з камер спостереження формується у відповідну папку (шаблон папки ЧИСЛО_МІСЯЦЬ_РІК). Для зміни налаштувань чи перегляду документації

існують відповідні вікна.

Також для організації маштабуємості системи й контролю дій над співробітниками сигнал також через мережне обладнання фірми Axis надходить до керівництва. Розробляючи апаратну й програмну частину дипломного проектування враховувався ціновий фактор, а також особливості застосування камер в умовах України, а саме – застосовувався ударостійкий корпус, були обрані камери з розширеними температурними діапазонами роботи (-40 С до +55 С) і великим кутом огляду камери.

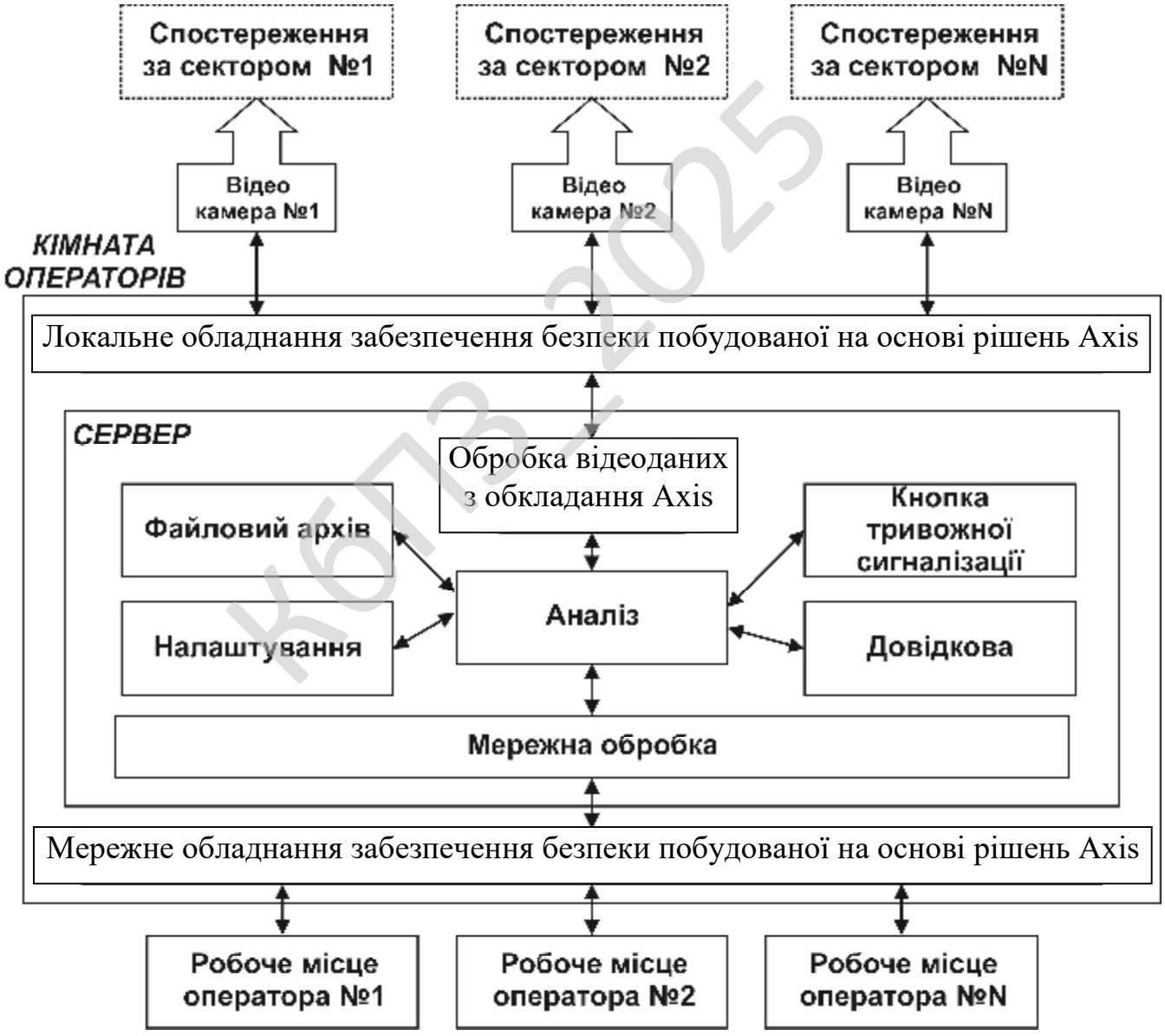

Рисунок 3.2 – Функціональна схема системи

Розглянувши всі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

3.4 Розробка діаграми процесів

Діаграма процесів розробленої системи зображена на рисунку 3.3. При детальному її розгляді можна побачити як саме проходе взаємодія у розробленій системі.

Використовується модель проектування, графічне представлення «потоків» даних в інформаційній системі.

Діаграма взаємодії процесів використовується для візуалізації процесів обробки даних (структурне проектування).

Для розробника вважається звичним спочатку креслити діаграму взаємодії процесів даних рівня контексту, завдяки чому буде показано взаємодію системи. Ця діаграма в подальшому підлягає уточненню шляхом деталізації процесів та потоків даних з метою показати систему що розробляється.

Використовуючи існуючи методи була створена системи забезпечення безпеки побудованої на основі рішень Axis, яка забезпечує безпеку об’єктів. Камери Axis відрізняються чудовою якістю зображення з розв’язною здатністю HDTV при будь-якому рівні освітлення й умовах експлуатації. Завдяки інноваційним технологіям зменшується обсяг трафіку й знижується розмір файлів на диску, що допомагає заощаджувати електроенергію.

А ПЗ для аналізу відеоматеріалів, розроблені у даній роботі, перетворюють мережні камери в інструменти керування бізнесом.

Подібне ПЗ попереджає вас про ситуації, що розвиваються, і допомагає приймати обґрунтовані рішення в роботі й по розподілі ресурсів. Дані можна також інтегрувати з іншими системами об'єкта.

Діаграми потоків даних містять чотири типи елементів:

– Процеси які являють собою трансформацію даних в рамках описуваної системи.

– Сховища даних (репозиторії).

– Зовнішні по відношенню до системи сутності.

– Потоки даних між елементами трьох попередніх типів.

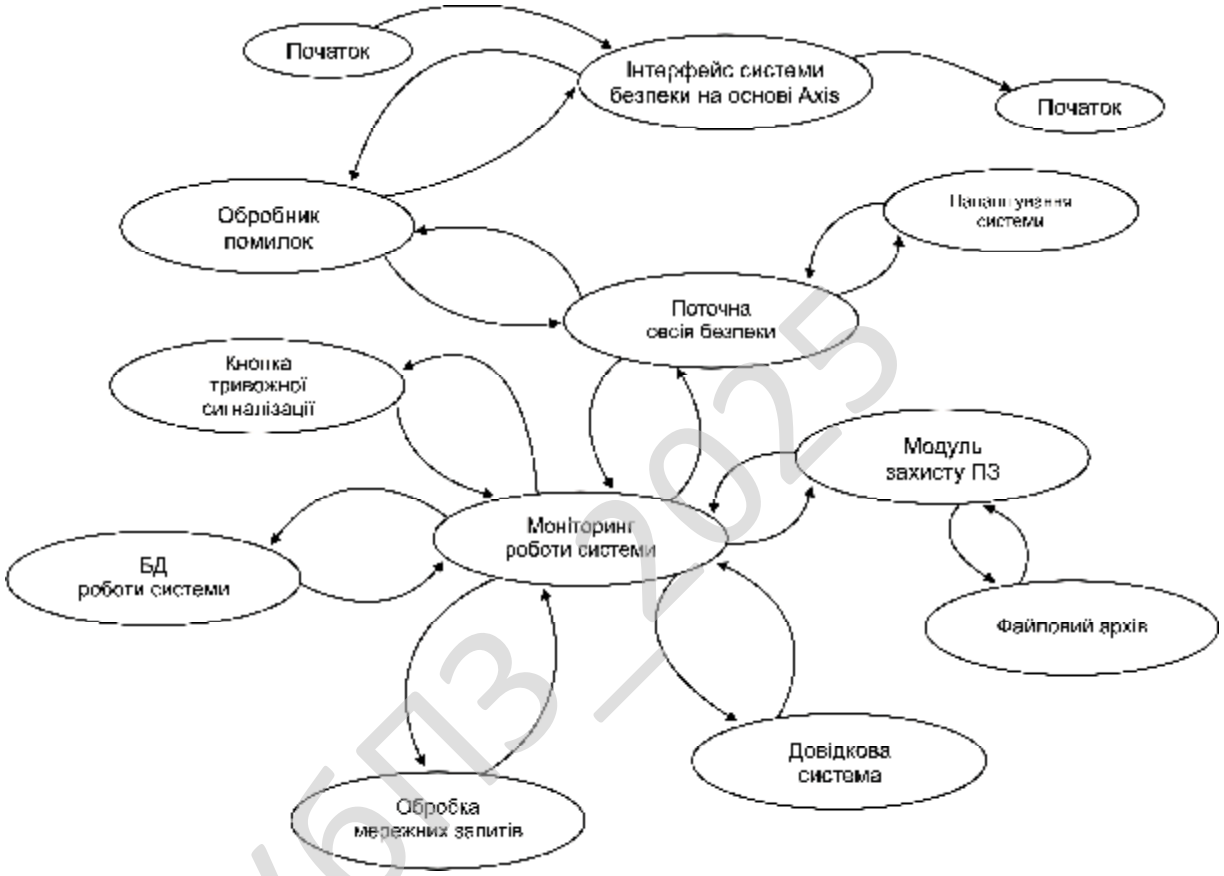

Рисунок 3.3 – Діаграма взаємодії процесів

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 ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Під час роботи над магістерською дипломною роботою було створено блок-схеми. Перед їх розглядом необхідно провести роз’яснення який саме тип блок-схем використовується.

Блок-схема це представлення задачі для її аналізу або розв'язування за допомогою спеціальних символів (геометричних образів), які позначають такі елементи, як операції, потік, дані тощо.

Блок вхідних та вихідних даних прийнято позначати паралелограмом, блок обчислень (обробки) даних – прямокутником, блок прийняття рішень – ромбом, еліпсом – початок та кінець алгоритму.

У інформаційних технологіях функціональна схема складається з функціональних блоків, які являють собою конструктивно відособлені частини (елементи або пристрої) автоматичних систем, які виконують певні функції. Функціональні блоки на схемі позначають прямокутниками, всередині яких надписують їх найменування відповідно до функцій, що виконуються. Зв'язки між функціональними блоками (внутрішні впливи) позначаються лініями зі стрілками, які вказують напрям впливів.

Функціональні схеми можуть виконуватися в укрупненому і розгорненому вигляді. У першому випадку на схемі зображають найважливіші блоки системи і зв'язки між ними.

У другому варіанті схема відображається більш детально, що полегшує її читання та ілюструє принцип роботи.

Основні елементи схем алгоритму це термінатор, процес, рішення, зумовлений процес (підпрограма), дані та з'єднувач.

Термінатор це елемент відображає вхід із зовнішнього середовища або вихід з неї (найчастіше застосування – початок і кінець програми). Всередині фігури записується відповідна дія.

Процес це виконання однієї або кількох операцій, обробка даних будь-якого виду (зміна значення даних, форми подання, розташування). Всередині фігури записують безпосередньо самі операції.

Рішення це показує рішення або функцію перемикального типу з одним входом і двома або більше альтернативними виходами, з яких тільки один може бути обраний після обчислення умов, визначених всередині цього елементу. Вхід в елемент позначається лінією, що входить зазвичай у верхню вершину елементу. Якщо виходів два чи три то зазвичай кожен вихід позначається лінією, що виходить з решти вершин (бічних і нижній). Якщо виходів більше трьох, то їх слід показувати однією лінією, що виходить з вершини (частіше нижній) елемента, яка потім розгалужується. Відповідні результати обчислень можуть записуватися поруч з лініями, що відображають ці шляхи.

Зумовлений процес (підпрограма) це символ відображає виконання процесу, що складається з однієї або кількох операцій, що визначені в іншому місці програми (у підпрограмі, модулі). Всередині символу записується назва процесу і передані в нього дані.

Дані це перетворення у форму, придатну для обробки (введення) або відображення результатів обробки (виведення). Цей символ не визначає носія даних (для вказівки типу носія даних використовуються специфічні символи).

З'єднувач це символ відображає вихід в частину схеми і вхід з іншої частини цієї схеми. Використовується для обриву лінії та продовження її в іншому місці (приклад: поділ блок-схеми, що не поміщається на листі). Відповідні сполучні символи повинні мати одне (при тому унікальне) позначення.

Блок-схеми є першоджерелами стратегії розвитку ПЗ. Тому від точності і детальної блок-схеми залежить результат всієї програми.

При виборі початкової точки відліку при побудові схем було враховано, що виходячи з вибору мови програмування і інших технічних засобів, програма буде об’єктно-орієнтована що вимагає оптимізації програми високого рівня, також те, що при розробці програми слід надати особливу увагу модулю системи забезпечення безпеки побудованої на основі рішень Axis.

На рисунку 4.1 зображена основна блок-схема програми, на рисунку 4.2 зображено роботу підпрограми.

З яких видно що робота основної програми складається з початкових етапів ініціалізації ПЗ, перевірки наявності ресурсів системи, блоку початку основного циклу з чеканням запиту від користувача в якому відбувається виклик підпрограми та останньої стадії – перевірка поточного стану з завершенням роботи розробленого ПЗ. При роботі підпрограми виконується основний функціонал системи з циклічними послідовностями, перевіркою поточного стану та поверненням в основну програму прапорів стану виконання.

Було використано підходи з використанням UML, це уніфікована мова моделювання, використовується у парадигмі об'єктно-орієнтованого програмування. Є невід'ємною частиною уніфікованого процесу розробки програмного забезпечення. UML є мовою широкого профілю, це відкритий стандарт, що використовує графічні позначення для створення абстрактної моделі системи, називаної UML-моделлю. UML був створений для визначення, візуалізації, проектування й документування в основному програмних систем. UML не є мовою програмування, але в засобах виконання UML-моделей як інтерпретованого коду можлива кодогенерація.

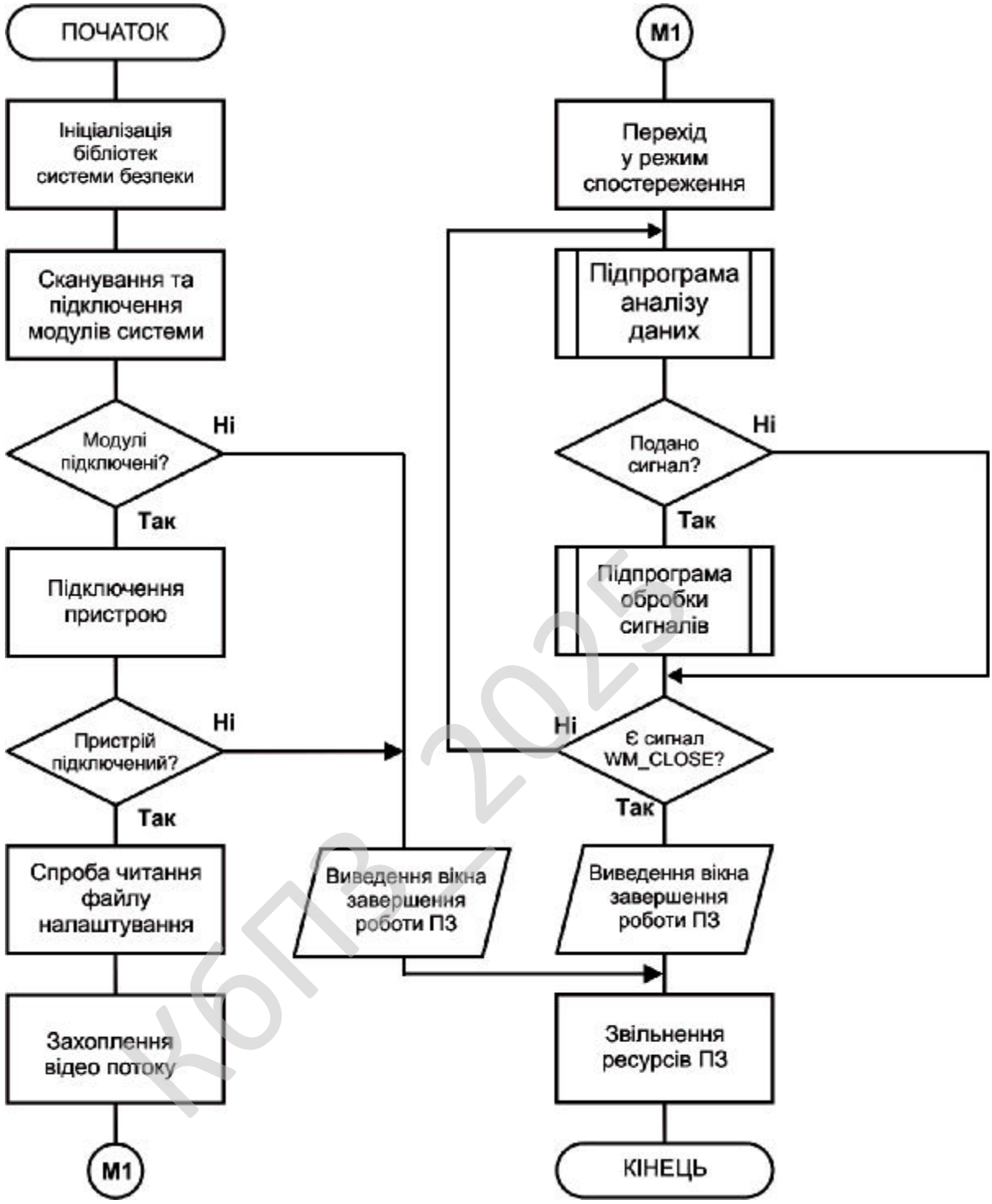

Рисунок 4.1 – Блок-схема основної програми

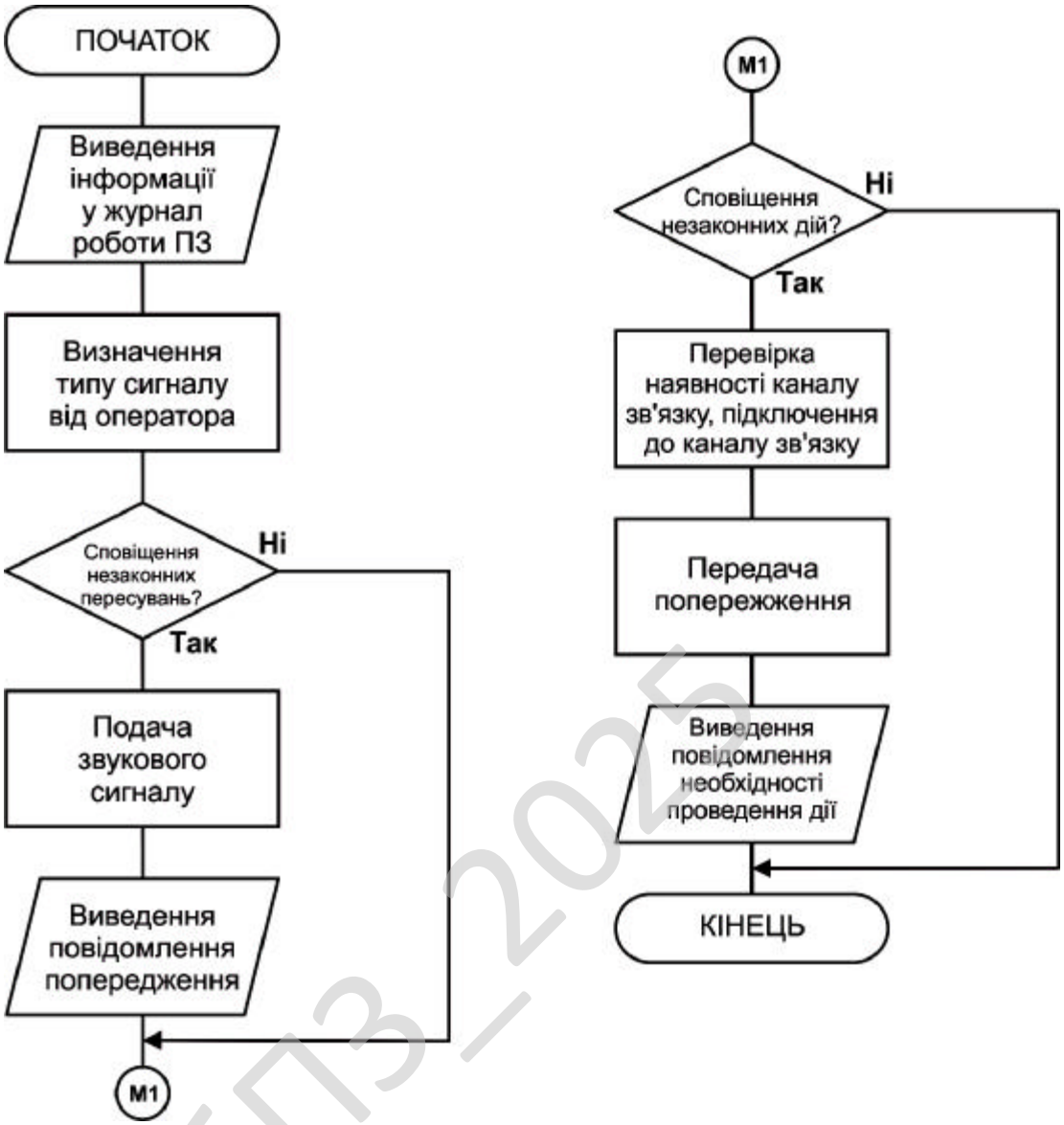

Рисунок 4.2 – Блок-схема роботи підпрограми

UML може бути застосовано на всіх етапах життєвого циклу аналізу бізнес-систем і розробки прикладних програм. Різні види діаграм які підтримуються UML, і найбагатший набір можливостей представлення певних аспектів системи робить UML універсальним засобом опису як програмних, так і ділових систем.

Діаграми дають можливість представити систему (як ділову, так і програмну) у такому вигляді, щоб її можна було легко перевести в програмний код. Основною причиною використання мови UML є спілкування розробників між собою.

Крім того, UML спеціально створювалася для оптимізації процесу розробки програмних систем, що дозволяє збільшити ефективність їх реалізації у кілька разів і помітно поліпшити якість кінцевого продукту.

UML прекрасно зарекомендувала себе в багатьох успішних програмних проектах. Засоби автоматичної генерації кодів дозволяють перетворювати моделі мовою UML у вихідний код об’єктно-орієнтованих мов програмування, що ще більш прискорює процес розробки. Практично усі CASE-засоби (програми автоматизації процесу аналізу і проектування) мають підтримку UML. Моделі розроблені в UML, дозволяють значно спростити процес кодування і направити зусилля програмістів безпосередньо на реалізацію системи.

Діаграми підвищують супроводжуваність проекту і полегшують розробку документації.

UML необхідний:

– Керівникам проектів, які керують розподілом завдань і контролем за проектом.

– Проектувальникам інформаційних систем які розробляють технічні завдання для програмістів.

– Бізнес-аналітикам, які досліджують реальну систему і здійснюють інжиніринг і реінжиніринг бізнесу компанії.

– Програмістам які реалізовують модулі інформаційної системи.

При модифікації системи об'єктний підхід дозволяє легко включати в систему нові об'єкти і виключати застарілі без істотної зміни її життєздатності. Використання побудованої моделі при модифікаціях системи дає можливість усунути небажані наслідки змін, оскільки вони не ламають структури системи, а тільки змінюють поведінку об'єктів.

Також при розробці магістерської дипломної роботи було використано наступні підходи UML: діаграма діяльності (діаграми поведінки типу); Діаграма компонент; Діаграма об'єктів; Діаграма розгортання.

Діаграма діяльності. Це візуальне представлення графу діяльностей. Граф діяльностей є різновидом графу станів скінченного автомату, вершинами якого є певні дії, а переходи відбуваються по завершенню дій. Дія є фундаментальною одиницею визначення поведінки в специфікації. Дія отримує множину вхідних сигналів, та перетворює їх на множину вихідних сигналів.

Одна із цих множин, або обидві водночас, можуть бути порожніми. Виконання дії відповідає виконанню окремої дії. Подібно до цього, виконання діяльності є виконанням окремої діяльності, буквально, включно із виконанням тих дій, що містяться в діяльності. Кожна дія в діяльності може виконуватись один, два, або більше разів під час одного виконання діяльності. Щонайменше, дії мають отримувати дані, перетворювати їх та тестувати, деякі дії можуть вимагати певної послідовності.

Специфікація діяльності (на вищих рівнях сумісності) може дозволяти виконання декількох (логічних) потоків, та існування механізмів синхронізації для гарантування виконання дій у правильному порядку.

Діаграма компонент в UML це діаграма, на якій відображаються компоненти, залежності та зв'язки між ними.

Діаграма компонент відображає залежності між компонентами програмного забезпечення, включаючи компоненти вихідних кодів, бінарні компоненти, та компоненти, що можуть виконуватись.

Модуль програмного забезпечення може бути представлено в якості компоненти. Деякі компоненти існують під час компіляції, деякі – під час компонування, а деякі під час роботи програми.

Діаграма компонент відображає лише структурні характеристики, для відображення окремих екземплярів компонент слід використовувати діаграму розгортування.

Компоненти об'єднуються разом використовуючи структурні зв'язки (assembly connector) щоб об'єднати інтерфейси двох компонент. Це ілюструє зв'язок типу «клієнт-сервер».

Структурна взаємодія – «зв'язок двох компонент, який передбачає, що один з них надає послуги, потрібні іншому компоненту».

При використанні діаграми компонент щоб показати внутрішню структуру компонента, клієнтські та серверні інтерфейси можуть утворювати пряме з'єднання з внутрішніми. Таке з'єднання називається з'єднанням делегації.

Діаграма об'єктів в UML це діаграма, що відображає об'єкти та їх зв'язки в певний момент часу. Діаграма об'єктів може розглядатись як окремий випадок діаграми класів, на якій можуть бути представлені як класи, так і екземпляри (об'єкти) класів. Схожою за змістом є діаграма взаємодії (collaboration diagram).

Діаграми об'єктів не мають власної нотації. Оскільки діаграми класів можуть відображати об'єкти, то діаграма класів, на якій відображено лише об'єкти, та не відображено класи, може вважатись діаграмою об'єктів.

Діаграма об'єктів відображає об'єкти та зв'язки в певний момент роботи програми. Об'єкти можуть містити інформацію про власні значення а не про описання. Для відображення загальних шаблонів об'єктів та зв'язків, що можуть багаторазово створюватись під час роботи програми, слід використовувати діаграму взаємодії, яка може відображати характеристики об'єктів та зв'язків. Екземпляр діаграми взаємодії створює діаграму об'єктів.

Діаграма об'єктів не відображає еволюцію системи під час роботи. Натомість, слід використовувати діаграми взаємодії з повідомленнями, або діаграми послідовності.

Діаграма розгортання (deployment diagram) це діаграма в UML, на якій відображаються обчислювальні вузли під час роботи програми, компоненти, та об'єкти, що виконуються на цих вузлах. Компоненти відповідають представленню робочих екземплярів одиниць коду. Компоненти, що не мають представлення під час роботи програми на таких діаграмах не відображаються; натомість, їх можна відобразити на діаграмах компонент. Діаграма розгортання відображає робочі екземпляри компонент, а діаграма компонент, натомість, відображає зв'язки між типами компонент.

4.2 Захист розробленого програмного забезпечення

Захист розробленого програмного забезпечення буде відбуватися за допомогою Serpent – симетричний блочний алгоритм шифрування, розроблений Россом Андерсоном, Елі Біхамом та Ларсом Кнудсеном. Алгоритм був одним з фіналістів 2-го етапу конкурсу AES. Як і інші алгоритми, які брали участь у конкурсі AES, Serpent має розмір блоку 128 біт і можливі довжини ключа 128, 192 або 256 біт. Алгоритм являє собою 32-раундовий шифр на основі SP-мережі, і працює з блоком з чотирьох 32-бітових слів. Serpent був розроблений так, що всі операції можуть бути виконані паралельно, використовуючи 32-а 1-бітних «потоків».

При розробці Serpent використовувався консервативніший підхід до безпеки, ніж у інших фіналістів AES, проектувальники шифру вважали, що 16 раундів достатньо, щоб протистояти відомим видам криптоаналізу, але збільшили число раундів до 32, щоб алгоритм міг краще протистояти ще не відомим методам криптоаналізу.

Шифр Serpent не запатентований і є громадським надбанням.

Алгоритм створювався під гаслом «криптографічний алгоритм 21 століття» для участі в конкурсі AES. При створенні нового алгоритму Serpent його автори дотримувалися консервативних поглядів на проектування, що підтверджується первісним рішенням про використання таблиць підстановки з відомого багато років раніше алгоритму шифрування DES, який протягом довгого часу вивчався провідними фахівцями в області криптографії та захисту інформації у комп'ютерній мережі і чиї властивості і особливості були добре відомі науковому світу. Одночасно з цим до нового алгоритму міг бути застосований вичерпний аналіз, вже розроблений для DES. Не використовувалися нові, неперевірені і невипробувані технології при створенні шифру, який у разі прийняття був би використаний для захисту величезних масивів фінансових транзакцій та урядової інформації. Основною вимогою до учасників конкурсу

AES було те, що алгоритм-претендент повинен бути швидшим, ніж 3DES, і надавати як мінімум такий же рівень безпеки: він повинен мати блок даних довжиною 128 біт і ключ завдовжки 256 біт. 16-раундовий Serpent був би таким же надійним, як 3DES, але в два рази швидшим. Однак, автори вирішили, що для більшої надійності варто збільшити кількість раундів до 32. Це зробило шифр таким же швидким, як DES, і набагато надійнішим, ніж 3DES.

Структура алгоритму

Алгоритм Serpent є SP-мережею, у котрій весь блок даних довжиною 128 біт на кожному раунді розбивається на 4 слова довжиною 32 біти. Всі значення, що використовуються при шифруванні є бітовими потоками. Бітові індекси змінюють значення від 0 до 31 для 32-бітових слів, від 0 до 127 – для 128-бітових блоків та від 0 до 255 для 256-бітових ключів тощо. Для внутрішніх обчислень всі біти величин представлені в прямому порядку (little-endian).

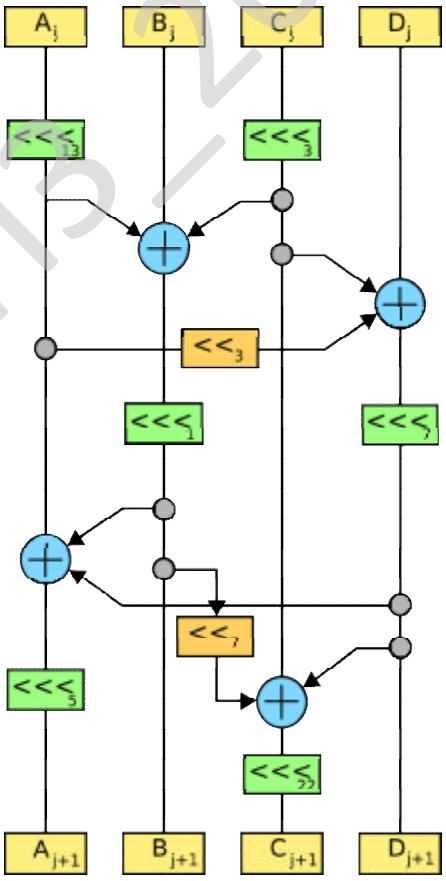

Рисунок 4.3 – Структура алгоритму Serpent

Serpent шифрує відкритий текст P довжиною 128 біт в шифротекст C довжиною таких же 128 біт за 32 раунд за допомогою 33 подключів K{0},...,K{32}, довжиною 128 біт. Довжина використовуваного ключа може приймати різні значення, але для конкретики зафіксуємо їх довжину в 128, 192 або 256 біт. Короткі ключі довжиною менше 256 біт доповнюються до повної довжини в 256 біт.

Шифрування складається з наступних основних кроків:

– Початкова перестановка.

– 32 раунд, кожен з яких складається з операції змішування з 128-бітовим ключем (побітове логічне виключаюче «або»), таблична заміна (S-box) і лінійне перетворення. В останньому раунді лінійне перетворення замінюється додатковим накладанням ключа.

– Кінцева перестановка.

Початкова і кінцева перестановки не мають будь-якої криптографічного значущості. Вони використовуються для спрощення оптимізованої реалізації алгоритму і підвищення обчислювальної ефективності.

Розширення ключа

Як і інші алгоритми, що брали участь в конкурсі AES, Serpent має можливі довжини ключа 128, 192 або 256 біт. «Неповний» ключ довжиною менше 256 біт доповнюється за наступним правилом: додається одиничний біт справа, за ним слід стільки нульових бітів, щоб довжина ключа стала дорівнює 256 бітам.

Початкова перестановка IP

Дана перестановка IP задається таблицею, де вказується позиція, на яку перейде відповідний біт (наприклад, біт 1 перейде на 32 позицію):

S-бокси (таблиці замін)

В алгоритмі Serpent таблиці замін є 4-бітовими перестановками з властивостями стійкості до диференціального криптоаналізу, до лінійного криптоаналізу і такою властивістю, що порядок вихідних біт, як функції вхідних повинен бути максимальний, тобто бути рівним 3.

Таблиця підстановки генерується з відомих і добре вивчених таблиць для алгоритму DES в ітераційному процесі, поки не будуть отримані бажані диференціальні й лінійні властивості. Таким чином, створюється 8 таблиць підстановки.

Лінійне перетворення LT

Лінійне перетворення LTзадається таблицею, де біти перераховані від 0 до 127 (наприклад, вихідний 2 біт утворений 2, 9, 15, 30, 76, 84, 126 битами, складеними за модулем 2) . В кожному рядку описується 4 вихідних біти, які разом складають вхідні дані на одну таблицю замін в наступному раунді. Варто зазначити, що даний набір являє собою таблицю IP(LT(FP(x))), де LT і є те лінійне перетворення.

Таблиця зворотного лінійного перетворення, яке використовується при розшифровці ILT.

Кінцева перестановка FP

Дана перестановка є зворотною до початкової, тобто $FP=IP^{-1}$ і задається наступною таблицею.

Ефективна реалізація алгоритму

Бажання авторів зробити алгоритм саме таким, яким він є стає зрозумілим при розгляді його ефективної низькорівневої реалізації.

Serpent був створений таким чином, щоб всі операції в процесі шифрування і розшифрування одного блоку могли бути виконані паралельно в 32 потоках. До того ж низькорівневий опис алгоритму набагато простішій, ніж стандартний опис. Ніяких початкових і кінцевих перестановок не потрібно.

Шифрування складається з 32 раундів. Відкритий текст є першими проміжними даними $B_0 = P$. Потім виконується 32 раунди, кожен і-й раунд складається з:

– Змішування з ключем. Проводиться побітове виключаюче «або» проміжних даних B_i з ключем довжиною 128 біт.

– Застосування таблиць підстановки. Вхідні дані довжиною 128 біт поділяються на 4 слова по 32 біта. Таблиця підстановки, реалізована послідовністю логічних операцій (як якщо це було б реалізовано апаратно), застосовується до цих 4 словам. В результаті виходить 4 вихідних слова. Таким чином, центральний процесор виконує підстановку по 32 копій таблиці одночасно.

– Лінійне перетворення. 32-бітові слова перетворюються заданим порядком.

Першою причиною вибору такого лінійного перетворення є максимізація лавинного ефекту. Такі таблиці підстановки мають властивість, що зміна кожного вхідного біта призведе до зміни 2 вихідних бітів. Таким чином, кожен вхідний біт відкритого тексту вже через 3 раунди впливає на всі вихідні біти. Аналогічно кожен біт ключа впливає на результат шифрування.

Друга причина полягає в простоті перетворення. Воно може бути реалізоване на будь-якому сучасному процесорі з мінімальними витратами.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Розглянемо розроблене ПЗ системи забезпечення безпеки побудованої на основі рішень Axis яке зображено на рисунку 5.1. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи:

– Навігаційне меню: Налаштування; Сповіщення; Камери; Вікна; Довідка.

– Функції представлені у графічному вигляді – вікно виведення відеопотоку.

– Розділу обрання групи камер.

– Навігаційного меню яке викликається натисканням правої клавіші маніпулятора миші.

– Функціональних кнопок ПЗ.

Розроблена програма має дуже простий і інтуїтивно зрозумілий інтерфейс з користувачем. Кожен, хто в достатньому обсязі володіє операційним середовищем Windows без особливих складностей освоїть і цю програму, оскільки її інтерфейс інтуїтивно зрозумілий.

Якщо програма не видала ніяких помилок, і працює, то можна використовувати, інакше слід слідувати інструкціям, які пропонує програма.

На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення.

Невід'ємною частиною комплексної системи безпеки стали сучасні системи відеоспостереження, оскільки вони дозволяють не тільки спостерігати й записувати відео, але й програмувати реакцію всієї системи безпеки при виникненні тривожних подій або ситуацій.

Метою установки звичайно є перегляд простору перед дверима, ліфтом і виходом на сходи, якщо це квартира, і всі входи й під'їзди до будинку, якщо це

заміський будинок. Часто камери встановлюються на ділянках біля будинків, де гуляють діти.

Саме головне для створення правильної системи – це точно визначити її мети й завдання, правильно підібрати встаткування й місце установки камер. Саме тому при створенні системи відеоспостереження завжди бажано технічне обстеження об'єкта й складання проекту.

Рисунок 5.1 – Головне вікно ПЗ

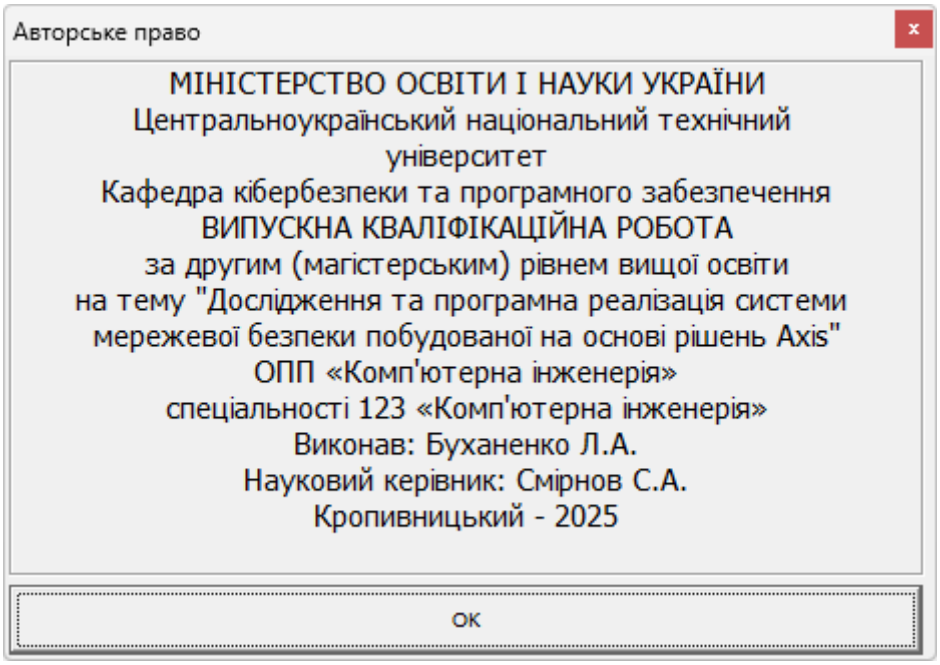

Рисунок 5.2 – Авторське право

У професійній сфері системи відеоспостереження прийнято підрозділяти на два види залежно від використовуваного встаткування: аналогові й цифрові.

Розглянемо процес впровадження програмного забезпечення, це процес налаштування програмного забезпечення під певні умови використання, а також навчання користувачів роботі з програмним продуктом. Впровадження програмного забезпечення це усі дії, що роблять розроблену програмну систему готовою до використання. Даний процес є частинною життєвого циклу програмного забезпечення.

Загалом процес розгортання складається з кількох взаємопов'язаних дій із можливими переходами між ними. Ця активність може відбуватися як з боку виробника так і з боку споживача. Оскільки кожна програмна система є унікальною, то усі процеси та процедури під час розгортання важко передбачити. Тому, "розгортання" можна трактувати як загальний процес відповідно до певних вимог та характеристик. Розгортання може здійснюватись програмістом і в процесі розробки програмного забезпечення.

До діяльностей пов'язаних із розгортанням програмного забезпечення відносять:

– Випуск.

– Встановлення та активація.

– Деактивація.

– Адаптація.

– Обновлення.

– Вмонтування.

– Відстежування версій.

– Видалення.

– Вилучення з обігу.

При впровадженні програмного забезпечення потрібно урахувати наступні дії:

– Виділення критичних, з точки зору загального результату, процедур в діяльності організації. Коли набір таких процедур визначений, необхідно в першу чергу використовувати ІТ рішення для автоматизації операцій усередині саме цих процедур. Таким чином, розроблене ІТ рішення автоматично стає життєво важливим і затребуваним для організації, а також буде забезпечена публічність процесу впровадження;

– Розширення нормативної бази організації шляхом включення до неї регламентів, що описують порядок виконання процедур автоматизованих процесів. В іншому випадку є небезпека виникнення неузгодженості між автоматизованими процедурами та іншими процесами організації.

– Виконання робіт з загальної стандартизації існуючої діяльності організації, коли виділяються кращі практики виконання процедур і включаються в ІТ рішення за принципом найбільшої корисності для більшості учасників. Відсоток таких процедур щодо загального обсягу автоматизації може бути невеликий, але це надає процесу побудови рішення вагу в організації за рахунок збільшення його необхідності.

Під час роботи над програмою було проведено тестування програмного забезпечення, тобто технічне дослідження, призначене для виявлення інформації про якість продукту відносно контексту, в якому воно має використовуватись.

Тестування включає як процес пошуку помилок або інших дефектів, так і випробування програмних складових з метою їх оцінки.

Проводилась оцінка:

– відповідності поставленим вимогам;

– правильна відповідь для усіх можливих вхідних даних;

– виконання функцій за прийнятний час;

– практичність;

– сумісність з ОС та стороннім ПЗ.

Оскільки число можливих тестів для програмних компонент практично нескінченне, тому стратегія тестування полягала в тому, щоб провести всі можливі тести з урахуванням наявного часу та ресурсів.

Як результат ПЗ тестувалось стандартним виконанням програми з метою виявлення помилок або інших дефектів.

Проводилось тестування чорної скриньки. Основне місце програми тестів «чорної скриньки» – інтерфейс ПЗ. Відомі: функції програми. Досліджується: робота кожної функції на всій області визначення.

Ці тести демонструють:

– Як виконуються функції програми.

– Як приймаються вихідні дані.

– Як виробляються результати.

– Як зберігається цілісність зовнішньої інформації.

При тестуванні «чорної скриньки» розглядаються системні характеристики програм, ігнорується їхня внутрішня логічна структура. Вичерпне тестування, як правило, неможливе.

Наприклад, якщо в програмі 10 вхідних величин і кожна приймає по 10 значень, то кількість тестових варіантів становитиме 10^10. Тестування «чорної скриньки» не реагує на багато особливостей програмних помилок.

Тестування «чорної скриньки» (функціональне тестування) дозволяє отримати комбінації вхідних даних, які забезпечують повну перевірку всіх функціональних вимог до програми.

Програмний виріб тут розглядається як «чорна скринька», чию поведінку можна визначити тільки дослідженням його входів та відповідних виходів. При такому підході бажано мати:

– Набір, утворений такими вхідними даними, які призводять до аномалій у поведінці програми (назвемо його ITc).

– Набір, утворений такими вхідними даними, які демонструють дефекти програми (назвемо його OT).

Будь-який спосіб тестування «чорної скриньки» повинен:

– Виявити такі вхідні дані, які з високою ймовірністю належать набору ITc;

– Сформулювати такі очікувані результати, які з високою імовірністю є елементами набору OT.

Принцип «чорної скриньки» не альтернативний принципу «білої скриньки». Скоріше це доповнює підхід, який виявляє інший клас помилок.

Тестування «чорної скриньки» забезпечує пошук наступних категорій помилок:

– Некоректних чи відсутніх функцій;

– Помилок інтерфейсу;

– Помилок у зовнішніх структурах даних або в доступі до зовнішньої бази даних;

– Помилок характеристик (необхідна ємність пам'яті і т.д.);

– Помилок ініціалізації та завершення.

Обрано умови розповсюдження – Freeware.

Це власницьке програмне забезпечення, котре можна Безоплатно використовувати протягом необмеженого терміну без обмежень у функціональності, і поширюване без сирцевих кодів.

Автори такого програмного забезпечення, як правило, хочуть «дати щось спільноті», але хочуть також контролювати його подальшу розробку. Іноді, коли програмісти вирішують припинити розробку, вони передають сирцевий код іншим програмістам, або ж спільності як вільне програмне забезпечення.

Дуже часто плутають поняття «безплатне програмне забезпечення» та «вільне програмне забезпечення», хоча вони суттєво відрізняються.

Безплатне програмне забезпечення можна безоплатно встановлювати та використовувати (іноді з певними обмеженнями, як, наприклад, «безплатне для домашнього або некомерційного вжитку»), в той час як вільне програмне забезпечення можна продавати за будь-яку суму, але при тому, у користувача, котрий його отримує, повинні бути права на вивчення, модифікацію та поширення сирцевих кодів одержаної програми.

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи мережевої безпеки побудованої на основі рішень Axis.

Метою розробки є дослідження та програмна реалізація системи мережевої безпеки побудованої на основі рішень Axis.

Об'єктом дослідження є процес мережевої безпеки побудованої на основі рішень Axis.

Предметом дослідження є методи мережевої безпеки побудованої на основі рішень Axis.

Методи дослідження базуються на методах захисту інформації у комп'ютерній мережі, методах математичної статистики, методах розробки програмного забезпечення.

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

– Удосконалено метод мережевої безпеки побудованої на основі рішень Axis.

– Розроблено вітчизняний продукт мережевої безпеки побудованої на основі рішень Axis, 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 програмної реалізації системи мережевої безпеки, побудованої на основі рішень Axis, можуть бути корисні багатьом категоріям зацікавлених осіб та організацій. Насамперед, ці результати будуть цікавими для керівників підприємств, які бажають забезпечити захист своєї інформаційної інфраструктури від потенційних загроз. Завдяки високій ефективності рішень Axis, вони зможуть автоматизувати процеси безпеки та мінімізувати витрати на фізичну охорону.

ІТ-фахівці та системні адміністратори також знайдуть цінність у таких розробках. Вони зможуть використовувати ці технології для інтеграції в існуючі системи безпеки, оптимізуючи процеси моніторингу, реагування на інциденти та збереження даних. Вендори та постачальники обладнання, які займаються реалізацією рішень у сфері безпеки, також будуть зацікавлені в результатах, оскільки вони допоможуть їм удосконалювати свої пропозиції для різних сегментів ринку.

Служби безпеки та охорони підприємств можуть застосувати ці системи для покращення фізичної безпеки, забезпечення моніторингу та контрольного доступу на об’єктах. Крім того, органи державної влади та інші регулятори будуть зацікавлені в цьому дослідженні для створення ефективних політик безпеки на рівні інфраструктурних об'єктів і критичних систем, таких як енергетика чи транспорт.

7.2 Оцінка привабливості шляхом застосування методів експертних оцінок

Оцінка привабливості для програмної реалізації системи мережевої безпеки, побудованої на основі рішень Axis, може бути здійснена за допомогою методів експертних оцінок. Наприклад, одним із таких методів є метод експертного оцінювання на основі парних порівнянь. У цьому випадку експертна група порівнює різні аспекти системи безпеки, такі як ефективність моніторингу, швидкість реагування на інциденти, ціна рішення та легкість інтеграції з іншими системами.

Експерти надають бали за кожен з критеріїв, після чого отримані оцінки перетворюються в індекс привабливості для підприємств. Наприклад, на основі цих оцінок можна визначити, що система Axis має вищу привабливість порівняно з конкурентами завдяки високому рівню автоматизації та інтеграції з іншими компонентами безпеки. Таке дослідження дозволяє отримати об'єктивну оцінку того, наскільки ефективно система відповідає вимогам підприємства та її потенціал на ринку.

7.3 Вибір методу оцінки вартості ПЗ

Для оцінки вартості програмної реалізації системи мережевої безпеки, побудованої на основі рішень Axis, можна використовувати метод ціноутворення на основі вартості життєвого циклу (LCC, Life Cycle Costing). Цей метод дозволяє оцінити загальні витрати на проект на всіх етапах його існування – від початкових витрат на впровадження та налаштування до витрат на обслуговування та оновлення системи.

Зокрема, для системи Axis до витрат можуть входити: первісна вартість обладнання та програмного забезпечення, вартість інтеграції з існуючими системами безпеки, витрати на навчання персоналу для роботи з новою

системою, поточні витрати на обслуговування та оновлення програмного забезпечення, витрати на технічну підтримку протягом усього періоду використання.

Цей метод дозволяє зібрати всі необхідні дані та отримати об'єктивну оцінку вартості програмної реалізації системи, що дає змогу зрозуміти, наскільки вигідним буде таке впровадження в довгостроковій перспективі.

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

Впровадження сучасної системи мережевої безпеки є критично важливим для забезпечення захисту підприємства від потенційних загроз. Одним із інструментів для вирішення цього завдання є використання рішень Axis Communications, які спеціалізуються на відеоспостереженні, контролі доступу та мережевій безпеці. Вхідні дані зафіксовано в таблиці 7.1.

Розрахунок економічного ефекту демонструє наступне: загальні витрати до впровадження систем Axis становили 1 030 000 грн на рік, після впровадження – 660 000 грн на рік. Сукупна економія – 370 000 грн щорічно. Додатковий економічний ефект забезпечує підвищення продуктивності персоналу з 70% до 90%, що еквівалентно приросту ефективності на 20% та зменшенню непрямих витрат на робочий час.

Економія на інтеграції систем становить 50 000 грн одноразово, а економія на технічному обслуговуванні – 20 000 грн/рік. Загальний чистий економічний ефект за перший рік – 420 000 грн. За умови інвестицій у впровадження на рівні 300 000 грн, термін окупності (Payback Period) становить ≈ 0,71 року (близько 8,5 місяців), а рентабельність інвестицій (ROI) – 140%.

Таблиця 7.1 – Вихідні дані для розрахунку

Показник	**До впровадження**	**Після впровадження**	**Зміна (%)**
Витрати на охорону та безпеку	500 000 грн/рік	300 000 грн/рік	–40%
Витрати на моніторинг і архівацію	100 000 грн/рік	50 000 грн/рік	–50%
Витрати на страхування майна	200 000 грн/рік	150 000 грн/рік	–25%
Продуктивність персоналу	70%	90%	+20%
Витрати на інтеграцію систем	150 000 грн	100 000 грн	–33%
Витрати на технічне обслуговування	80 000 грн/рік	60 000 грн/рік	–25%

Додаткові нефінансові переваги: зниження витрат на охорону та фізичну безпеку полягає у переході від витрат на фізичних охоронців і патрулювання до використання мережевих камер із детекцією руху та розпізнаванням облич. Це дозволяє автоматизувати контроль території та скоротити витрати на 25–40%.

Покращення ефективності моніторингу та обробки даних досягається завдяки інтелектуальним камерам і ПЗ Axis, які автоматично фільтрують та зберігають дані. Це зменшує час ручного перегляду відео та забезпечує економію 30–50%.

Мінімізація ризику втрати або крадіжки майна забезпечується інтеграцією відеоспостереження з системами контролю доступу та сповіщення, що зменшує несанкціонований доступ і скорочує втрати на 15–30%.

Покращення продуктивності персоналу відбувається завдяки автоматизації процесів спостереження: система сама фіксує критичні інциденти, а співробітники зосереджуються на основних задачах. Це підвищує продуктивність на 20-35%.

Інтеграція з іншими бізнес-системами спрощується завдяки єдиній платформі Axis, яка поєднує відеоспостереження, контроль доступу, сигналізацію та освітлення, знижуючи витрати на інтеграцію й обслуговування на 15–25%.

Зниження витрат на технічне обслуговування забезпечується надійністю обладнання Axis та його довговічністю, що дозволяє скоротити витрати на підтримку на 10–15%.

Впровадження системи мережевої безпеки на основі рішень Axis дозволяє значно знизити витрати на фізичну охорону, технічне обслуговування та моніторинг. Інтеграція різних систем у єдину мережу забезпечує ефективність управління та скорочує витрати на персонал. Високоякісне обладнання та автоматизація процесів підвищують надійність і знижують ризики втрат.

7.5 Пропозиція алгоритму просування проєкту розробки ПЗ

Алгоритм просування проєкту програмної реалізації системи мережевої безпеки на основі рішень Axis можна побудувати через кілька етапів. На першому етапі необхідно здійснити маркетингове дослідження для визначення цільової аудиторії та конкурентів на ринку. Важливо зрозуміти, яким компаніям та організаціям потрібні рішення у сфері мережевої безпеки.

Другим етапом є створення комунікаційної стратегії, що включає позиціонування рішення Axis як інноваційного та ефективного інструменту для

зниження витрат на безпеку та зменшення ризиків. На цьому етапі варто зібрати кейси успішного застосування технологій для різних секторів бізнесу.

Третім етапом є вибір каналів просування: участь у виставках, конференціях, розсилки на професійні форуми, створення тематичних вебінарів і блогів. На цьому етапі важливо активно використовувати соціальні мережі для залучення уваги до проекту.

Заключним етапом є аналіз ефективності кампанії через показники кількості зацікавлених клієнтів, зростання продажів та позитивні відгуки, які допомагають сформувати репутацію на ринку.

7.6 Оптимізація каналів збуту та шляхів реалізації ПЗ

Для оптимізації каналів збуту та шляхів реалізації проєкту програмної реалізації системи мережевої безпеки можна запропонувати кілька стратегій. По-перше, варто інвестувати в партнерські мережі. Створення альянсів з іншими постачальниками технологій безпеки дозволить збільшити охоплення та доступ до потенційних клієнтів.

По-друге, доцільно створити онлайн-платформу для демонстрації можливостей системи, де потенційні клієнти можуть ознайомитись із кейсами, переглянути вебінари та отримати консультації. Це дозволить скоротити час на підготовку персоналізованих пропозицій.

По-третє, важливо зосередитись на післяпродажній підтримці та технічному супроводі. Наявність висококласної підтримки для клієнтів збільшує довіру до бренду та спрощує довгострокові угоди.

7.7 Визначення ключових факторів успіху конкретного проєкту

Ключовими факторами успіху проєкту програмної реалізації мережевої безпеки є якість та надійність використовуваних технологій, адже система

повинна забезпечувати високу продуктивність і безперебійну роботу в будь-яких умовах. Також важливою є гнучкість і масштабованість рішень – можливість інтеграції з іншими існуючими системами та адаптація під потреби клієнтів. Третім важливим фактором є підтримка клієнтів та технічний супровід, оскільки гарантії та швидка реакція на проблеми є основою довіри до бренду. І, нарешті, для успіху важливо правильно популяризувати систему на ринку, через якісне позиціонування та маркетингові стратегії.

8 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

8.1 Вступ

Охорона праці є головною умовою безпеки та збереження здоров'я працівників. Згідно закону України “Про охорону праці” [3] кожна ІТ-компанія впроваджує заходи з охорони праці. Реалізується трудові відносини з вживанням необхідних засобів з охорони праці та розробки відповідних документів:

– Інструкцій з охорони праці по кожній професії і загальні;

– Положення про охорону праці;

– Накази з охорони праці;

– Журнали реєстрації та інструктажу.

Роботодавець створює відділ який працює відповідно до типового положення, яку затверджується центральним органом виконавчої влади і забезпечує виконання вимог державної політики у сфері охорони праці.

За недотриманням вимог, керівники ІТ компаній можуть бути притягнуті до відповідальності, яка виглядає у виді накладання штрафу. Якщо в результаті порушення умов охорони праці є постраждалі працівники то керівні особи ІТ компаній притягуються до кримінальної відповідальності.

Законом України “Про охорону праці” [3] регламентуються загальні положення державної політики в галузі охорони праці, а конкретизуються ці положення нормативно-правовими актами про охорону праці, зокрема Наказом Міністерства соціальної політики України 14.02.2018 № 207, який зареєстровано в Міністерстві юстиції України 25 квітня 2018 р. за №508/31960 «Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» [5], яким затверджено нормативно-правовий акт з охорони праці НПАОП 0.00-7.15-18, «Правила охорони праці під час експлуатації електронно-обчислювальних машин», та «Державні санітарні правила і норми

роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-98.

Програмісти у процесі роботи мають негативний вплив на органи зору, а також мають значну розумову напругою і нервово-емоційне навантаження. Руки (суглоби пальців та м'язи рук) при роботі з клавіатурою мають теж істотне навантаженням. До шкідливих факторів, які впливають на робітників галузі інформаційних технологій (ІТ) спеціалісти відносять високочастотні електромагнітні коливання (випромінювання) роботи апаратної частини ЕОМ та виділення шкідливих газів.

Ці шкідливі фактори можуть привести до професійних захворювань.

Розглянемо шкідливі чинники роботи програмістів керуючись наступними нормативно-правовими актами: «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно- обчислювальних машин» ДСанПіН 3.3.2-007-98 [5], та «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» НПАОП 0.00-7.15-18.

Умови праці програміста включають наступні фактори:

– параметри повітряного середовища в приміщенні;

– вентиляція приміщення;

– освітлення приміщення;

– параметри повітряного середовища в приміщенні, тощо.

Щоб запропонувати заходи щодо зменшення негативного впливу комп'ютера на організм людини визначимо фактори, які можуть викликати професійне захворювання і впливають на працездатність ІТ-працівників.

8.2 Шкідливі і небезпечні фактори при роботі з комп'ютером

Електронно-обчислювальна машина (ЕОМ) 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, праметри якого регламентуються нормативними документами – Державними санітарними правилами і нормами, зокрема ДСанПіН 3.3.2.007-98.

При роботі з використанням ЕОМ 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.

Працю користувачів ЕОМ відносять до психічних форм праці з високим ступенем навантаження. Ця діяльність пов'язана зі сприйняттям зображення на екрані, постійним стеженням за його динамікою, розрізненням картин, схем, читанням тексту рукописних та друкованих матеріалів, введенням інформації з клавіатури, необхідністю підтримувати активну увагу високою ціною помилки.

Будь-яка діяльність із застосуванням ЕОМ супроводжується необхідністю активації уваги та інших вищих психічних функцій, а організм людини, крім того, піддається впливу кількох десятків різноманітних факторів.

8.3 Аналіз санітарно-гігієнічних умов праці на робочому місці програміста

Розглянемо умови праці у приміщенні, в якому працюють програмісти. Геометричні розміри приміщення наведено у таблиці 8.1.

Таблиця 8.1 – Розміри приміщення

Найменування	Значення, м
Ширина	5
Довжина	6,2
Висота	3,4

Таблиця 8.2 – Площа та обсяг приміщення, на одного працюючого*

Геометрична характеристика	Одиниця виміру	Нормативне значення*	Фактичне значення
Площа, S	$м^2$	не менше 6.0	6,2
Об'єм, V	$м^3$	не менше 20.0	21,8

* Згідно ДСанПіН 3.3.2.007-98 (Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин).

У зазначеному приміщенні працюють двоє людей. За даними, які наведено у таблицях 8.1-8.2, можна зробити висновок, що площа та об’єм приміщення у розрахунку на одне робоче місце програміста не відповідають нормативним вимогам ДСанПіН 3.3.2-007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно- обчислювальних машин» [5], але відповідають нормативним вимогам Наказу Міністерства соціальної політики України № 207, від 14.02.2018 «Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» [5] та

НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин». Таким чином, можна зробити висновок, що санітарно-гігієнічні умови праці на робочому місці програміста відповідають вимогам.

Температура повітря в приміщенні визначається впливом температури зовнішнього повітря і тепловою енергією, яка виділяється всередині приміщення. Джерелами виділення теплоти в даному приміщенні є електроустаткування, освітлювальні прилади, а також люди. У світлий час доби джерелом надлишкового тепла є сонячна радіація. Згідно Постанови №42 від 01.12.1999 Головного державного санітарного лікаря України робота, виконувана в даному приміщенні, відноситься до категорії Іа. В цьому випадку людина витрачає енергії до 120 ккал у годину. Вологість повітря в приміщенні визначається впливом багатьох факторів, серед яких: вологість атмосферного повітря, виділення вологи людьми (при диханні та випарами з поверхні шкіри).

Мікроклімат повітряного середовища в приміщенні характеризується запиленістю та загазованістю повітря. Мікроклімат приміщення визначається діючим на організм людини поєднанням, вологості, температури, швидкості руху повітря та інтенсивності теплового випромінювання. Аналіз мікроклімату складається з визначення зазначених вище факторів і порівняння результатів із встановленими нормами.

У таблиці 8.3 наведено оптимальні та фактичні значення параметрів мікроклімату як для категорії важкості робіт Іа, так і для розглянутого приміщення.

Таблиця 8.3 – Оптимальні і фактичні значення параметрів мікроклімату

Пора року	Оптимальні для Іа			Фактичні		
	Температура, °С	Вологість,%	Швидкість повітря, м/с	Температура,°С	Вологість%	Швидкість повітря, м/с
Холодна	22-24	40-60	0,1	22-23	40-58	0,11
Тепла	23-25	50-70	0,1	24-25	50-65	0,2

У приміщеннях, де встановлено ЕОМ, рекомендується застосування тільки оптимальних значень показників мікроклімату.

Проведений аналіз показує, що показники мікроклімату в приміщенні відповідають установленим нормам. Штучне опалення застосовується у холодний період року.

В літню пору застосовується кондиціонер.

Для боротьби з пилом робляться регулярні провітрювання та вологі прибирання приміщенні.

У приміщенні знаходяться наступні джерела шуму: принтер Epson L132 (C11CE58403), електродвигуни вентиляторів ЕОМ.

Одним з найважливіших факторів, які впливають на ефективність трудової діяльності людини та попереджають травматизм і професійні захворювання програмістів, є освітлення на робочому місці.

З 2019 року діють Державні будівельні норми України “Природне і штучне освітлення” – ДБН В.2.5-28:2018 [1], у яких прописані вимоги до використання всіх освітлювальних приладів, у т.ч. світлодіодних.

Умови праці працівника, який постійно працює за комп’ютером, згідно ДБН В.2.5-28:2018 [1], можна віднести до роботи з малою точністю (найменший розмір об'єкта розрізнення від 1 до 5 мм) V-го розряду зорової роботи, з великою контрастністю об'єкта розрізнення (символів на екрані дисплея), з темним тлом (під розряд зорової роботи В). Приміщення можна віднести до 1-ої групи приміщень, у яких проводиться розрізнення об'єктів зорової роботи при фіксованому напрямку лінії зору того, що працює на робочу поверхню. Для такого типу приміщень і розряду зорової роботи нормоване значення коефіцієнта природної освітленості (КПО) робочої поверхні (при поєднаному, спільному освітленні), повинен становити не більше 1,5%, освітленість при штучному висвітленні повинна становити 300 Лк. [1]. Крім того, все поле зору повинно бути освітленим достатньо рівномірно – це основна гігієнічна вимога. Оскільки яскраве світло на ділянці периферійного зору значно збільшує напруженість очей і, як наслідок, призводить до їх швидкої стомлюваності, ступінь освітлення приміщення і яскравість екрану комп'ютера повинні бути приблизно однаковими.

8.4 Розробка заходів з умов поліпшення охорони праці

Згідно аналізу умов праці в розглянутому приміщенні, ми одержали 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.

Оскільки 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

Проведемо розрахунок штучного освітлення за методом коефіцієнту використання світлового потоку для приміщення ширина якого складає 5 м, довжина – 6,2 м, висота – 3,4 м.

У зазначеному приміщенні працює 5 людей.

Для того, щоб визначити потрібну кількість світильників, які повинні забезпечити нормований рівень освітленості, визначимо світловий потік, що падає на робочу поверхню за формулою:

$$F = E \cdot S \cdot K \cdot Z/n,$$

де

F – світловий потік, що розраховується, Лм;

E – нормована мінімальна освітленість, Лк; E = 300 Лк;

S – площа освітлюваного приміщення (у нашому випадку S = 5x6,2 = 31 $м^2$);

K – коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників в процесі експлуатації (його значення залежить від типу приміщення і характеру робіт, що проводяться в ньому, в нашому випадку K = 1,5);

Z – відношення середньої освітленості до мінімальної (зазвичай приймається рівним 1.1... 1.2, в нашому випадку Z = 1,1);

n – коефіцієнт використання світлового потоку, (відношення світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп, обчислюється в долях одиниці; залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі та характеризуються коефіцієнтами відбиття від стін ($\rho_{стін.}$) і стелі ($\rho_{стелі}$), значення коефіцієнтів дорівнюють $\rho_{стін}$ = 50% і $\rho_{стелі}$ = 50%.

Обчислимо індекс приміщення за формулою:

$$i = S/(h \cdot (A+B)),$$

де

S – площа приміщення, S = 31 м2;

h – розрахункова висота підвісу, h = 3 м (співпадає з висотою стелі, оскільки лампи освітлення закріплюються на стелі);

A – ширина приміщення, A = 5 м;

B – довжина приміщення, B = 6,2 м.

Підставимо всі значення у формулу та визначимо індекс приміщення: i=0,43.

Знаючи індекс приміщення, за знаходимо n = 0,23 (з табличних даних коефіцієнтів використання світлового потоку (n) світильників з відповідним типом лампам). Підставимо всі значення у формулу, визначимо світловий потік: F=66717 Лм.

Для розрахунку будемо використовувати світлодіодні панелі LED панель PL PFM 600 30W/3000K, світловий потік яких $F_л$ = 3000 Лм.

Число ламп визначається по формулі:

$$N=F/F_л$$

де

F – світловий потік,

$F_л$ – світловий потік однієї лампи.

Підставимо всі значення у формулу та визначимо потрібну кількість світильників

$$N= 66717/ 3000=22,18 \text{ шт.}$$

Приймаємо необхідну кількість світлодіодних світильників 23 шт.

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 умов праці, призначеного для праці програмістів, проведено розгляд небезпечних та шкідливих факторів, що негативно впливають на програмістів під час роботи. Виконано розрахунок штучного освітлення, як одного з ключових факторів впливу на працездатність та здоров’я програміста. Розроблено заходи з охорони праці.

9 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи мережевої безпеки побудованої на основі рішень Axis.

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 мережевої безпеки побудованої на основі рішень Axis.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем мережевої безпеки побудованої на основі рішень Axis.

– Досліджена система мережевої безпеки побудованої на основі рішень Axis.

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевої безпеки побудованої на основі рішень Axis.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання мережевої безпеки побудованої на основі рішень Axis.

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 Python. 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 Serpent.

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. Буханенко Л.А. Дослідження та програмна реалізація системи мережевої безпеки побудованої на основі рішень Axis // Збірник праць молодих науковців ЦНТУ. – Вип. 15. – Кропивницький: ЦНТУ, 2025.

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

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

3. 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.

4. 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

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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,

12. 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.

13. 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

14. 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.

15. 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.

16. 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.

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

18. 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.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

41. 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.

42. 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).

43. 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

44. 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.

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

46. Смірнов О.А., Смірнов С.А. Дідик А.К., Дрєєв О.М. Моделі системи нейромережевих експертів безпечної маршрутизації у хмарних антивірусних системах. Збірник наукових праць "Системи обробки інформації". – Випуск 3 (140). – Х.: ХУПС – 2016. – С. 36-39.

47. Смірнов О.А., Кавун С.В., Коваленко О.В., Доренський О.П., Дрєєв О.М., Вялкова В.І. Комп'ютерні мережі. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 233 с.

48. Смірнов О.А., Дрєєв О.М. Порівняння бітових щільностей при використанні різних методів кодування інформації. Збірник наукових праць "Системи обробки інформації". – Випуск 2 (118). т.2. – Х.: ХУПС – 2014. – С. 64-67

49. Смірнов О.А., Дрєєв О.М. Порівняння бітових щільностей при використанні різних методів кодування інформації. Збірник тез VI міжнародної науково-практичної конференції "Проблеми та перспективи розвитку IT-індустрії". м. Харків. 17-18 квітня 2014р. – Харків: ХНЄУ. – 2014. – С. 240.

50. Смірнов О.А., Коваленко О.В., Кожанова А.С., Левошко О.Л., Константинова Л.В. Основи системного програмування. Навчальний посібник. – Кіровоград: КНТУ 2013. – 257с.

51. Смірнов О.А., Дрєєв О.М., Доренський О.П. «Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі. Збірник наукових праць "Системи обробки інформації". – Випуск 8(115). – Х.: ХУПС – 2013. – С. 234-239.