

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
“___” _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за першим (бакалаврським) рівнем вищої освіти
на тему
“Програмне забезпечення системи кібербезпеки для
відеонагляду мережі кафе з використанням камер Axis”

Виконав здобувач вищої освіти
IV курсу, групи КБ-23МБ
ОПП «Кібербезпека»
спеціальності 125 «Кібербезпека»
_____ Німенко Д.О.
«___» _____ 2026 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Смірнов С.А.
«___» _____ 2026 р.
Рецензент _____

Центральноукраїнський національний технічний університет
Факультет Механіко-технологічний
Кафедра Кібербезпеки та програмного забезпечення
Освітній ступінь бакалавр
Галузь знань 12 "Інформаційні технології"
Спеціальність 125 "Кібербезпека"
Освітньо-професійна (освітньо-наукова) програма "Кібербезпека"

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.т.н., проф.
_____ Олексій СМІРНОВ
« 27 » лютого 2026 року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ПЕРШИМ (БАКАЛАВРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Німенку Дмитру Олеговичу

(прізвище, ім'я, по батькові)

1. Тема роботи *Програмне забезпечення системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis*

2. Керівник роботи *Смірнов Сергій Анатолійович, канд. техн. наук, доцент*

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 127-02 від 27.02.2026 року

3. Строк подання студентом роботи до захисту *23.05.2026 р.*

4. Мета та завдання випускної кваліфікаційної роботи: *Метою роботи є розробка програмного забезпечення системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis*

5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Призначення та область використання.

2. Перегляд аналогічних існуючих систем.

3. Опис і обґрунтування проектних рішень.

4. Етапи програмування системи.

5. Впровадження системи кібербезпеки в промислову експлуатацію.

6. Висновки

6. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Структурна схема системи кібербезпеки *1 аркуш*

Функціональна схема системи кібербезпеки *1 аркуш*

Діаграма процесів *1 аркуш*

Блок-схема алгоритму роботи додатку *2 аркуша*

7. Дата видачі завдання « 27 » лютого 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем	10.03.2026 р.	
2.	Постановка задачі, оформлення ТЗ	15.03.2026 р.	
3.	Розробка моделі компонента	20.03.2026 р.	
4.	Розробка структур даних	25.03.2026 р.	
5.	Розробка алгоритмів зв'язку та відображення	30.03.2026 р.	
6.	Програмування алгоритмів	10.04.2026 р.	
7.	Оформлення ПЗ	17.04.2026 р.	
8.	Попередній захист роботи	23.05.2026 р.	

Дата видачі завдання
« 27 » лютого 2026 р.

Підпис керівника

Смірнов С.А.
(прізвище та ініціали)

Завдання прийнято до виконання
« 27 » лютого 2026 р.

Підпис здобувача

Німенко Д.О.
(прізвище та ініціали)

АНОТАЦІЯ

Німенко Д.О. Програмне забезпечення системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis. 125 Кібербезпека. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis.

Метою розробки є програмне забезпечення системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis.

Результат роботи – програмна реалізація системи кібербезпеки для відеонагляду мережі кафе з використанням камер 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: кібербезпека, відеонагляд

ABSTRACT

Nimenko D.O. Software for a cybersecurity system for video surveillance of a cafe network using Axis cameras. 125 Cybersecurity. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

In this final qualification work for the first (bachelor's) level of higher education, software has been developed that is intended for a cybersecurity system for video surveillance of a cafe network using Axis cameras.

The purpose of the development is to develop software for a cybersecurity system for video surveillance of a cafe network using Axis cameras.

The result of the work is a software implementation of a cybersecurity system for video surveillance of a cafe network using Axis cameras.

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

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

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

The program is developed in the Python environment.

Keywords: cybersecurity, video surveillance

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ	2
ВСТУП.....	3
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ	5
1.1 Призначення системи.....	5
1.2 Область застосування.....	6
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ	8
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти.....	8
2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування.....	21
2.3 Розгорнута постановка завдання	23
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	25
3.1 Опис функціонування системи	25
3.2 Розробка структурної схеми.....	27
3.3 Розробка функціональної схеми	34
3.4 Розробка діаграми процесів.....	36
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ.....	38
4.1 Розробка блок-схем та опис алгоритмів функціонування системи.....	
4.2 Захист розробленого програмного забезпечення.....	56
5 ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	60
6 ОСНОВНІ ВИСНОВКИ.....	66
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	68

					ВКРБ-125.26.0036.00.00.ПЗ			
Вим	Арк.	№ докум.	Підп.	Дата	Програмне забезпечення системи кібербезпеки для відеонагляду мереж кафе з використанням камер Axis	Літ.	Аркуш	Аркушів
Розроб.		Німенко Д.О.				Б		
Перев.		Смірнов С.А.					1	75
Н.контр.		Коваленко А.С.				ЦНТУ КБ-23МБ		
Затв.		Смірнов О.А.						

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
ІР	—	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. Підприємства малого й середнього бізнесу досить консервативні при виборі рішень для непрофільних завдань бізнесу. Головне для них – не технічні характеристики, а споживчі властивості, практична корисність. Ставлячи завдання з організації віддаленого контролю за роботою своїх кафе, власники умовної мережі «Кухня Ганнусі» особливе значення надавали якості зображення. Для відеоспостереження були обрані камери Axis.

Компанія «Кухня Ганнусі» спеціалізується на підборі програми збалансованого живлення й доставці готових блюд. Проект був заснований лікарем-дієтологом, щоб допомогти пацієнтам її клініки естетичної медицини в реалізації індивідуальних програм живлення. У цей час компанія має у своєму розпорядженні фабрику-кухню, а також мережею авторських кафе.

У міру росту бізнесу усе більше актуальним ставало завдання ефективного контролю за всіма підприємствами, що перебувають під управлінням компанії. На деяких об'єктах уже була аналогова система відеоспостереження, однак, на думку керівництва, її якість і функціонування не відповідали пропонованим вимогам.

Тому при оснащенні трьох кафе, де відеоспостереження було відсутнє («Улюблене кафе» і два фітнес-кафе fit appetit), було вирішено розглянути альтернативні рішення.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis.

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

– Огляд існуючих систем для відеонагляду мережі кафе з використанням камер Axis.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

- Дослідження системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis.
- Програмна реалізація системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі для відеонагляду мережі кафе з використанням камер Axis.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

КБПЗ – 2026

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		4

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Як правило, замовники із сегменту малого й середнього бізнесу, до яких можна віднести й «Кухня Ганнусі», досить консервативні при виборі рішень для непрофільних завдань: якщо їх все влаштовує, то спробувати щось інше вони, як правило, не хочуть і будь-які доводи беруть під сумнів. У штаті найчастіше немає технічних фахівців, що добре вивчили відповідний ринок і здатних компетентно оцінити переваги пропонованих рішень. Головне для них – не технічні характеристики, а споживчі властивості, практична корисність.

Три вимоги замовника

Камери відеоспостереження дотепер установлюються переважно для рішення завдань безпеки. Однак у даному проекті це не було головною метою, оскільки всі три кафе розташовані на території партнерів, де є своя система безпеки. (Правда, згодом наявність власної системи придалася при розслідуванні випадків дрібних крадіжок.)

У першу чергу керівництво компанії хотіло одержати можливість віддаленого контролю за роботою кафе: треба було бачити, чим зайняті співробітники, що робиться на кухні, яке наповнення залу в пікові години й т.д. Тому до рішення пред'являлися наступні основні вимоги:

- чітке зображення;
- можливість віддаленого перегляду;
- безперебійний запис і зберігання як можна більшого обсягу даних.

А основним контрольованим об'єктом, як неважко догадатися, у кожному кафе була каса, щоб у випадку сумнівної операції можна було провести перевірку за відеозаписом. Забігаючи вперед, скажемо, що розташування й розв'язний дозвіл камер дозволяють відслідковувати номінал використовуваних купюр. У

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

принципі, запис із камер може бути синхронізована з подіями, що відбуваються на касі (формування чека, відкриття грошового ящика, уведення коду товару й т.п.), але замовник поражував цю функціональність зайвої.

1.2 Область застосування

Вибір рішення

Вибір камер визначався умовами на конкретному об'єкті. Над касою встановлювалися камери з вузьким кутом огляду, а для одержання загального виду залу – пристрою із широким сектором огляду. Усього використовувалося п'ять різних моделей компактних купольних камер серії AXIS M30: Axis M 3024-LVE, Axis M 3005-V, Axis M 3006-V, Axis M 3215-V; Axis P 3224-LV. У кафе, що перебуває біля басейну, була встановлена модульна камера Axis F34 з виносними блоками (чотири блоки підключені до однієї бази для моніторингу різних зон). Спостереження за складом, у тому числі в темний час доби, здійснювалося за допомогою камери Axis M 1145-L з убудованим світлодіодним ІЧ-підсвічуванням.

У всіх перерахованих моделях підтримуються сучасні технологічні можливості: розширений динамічний діапазон (WDR Forensic Capture), точне керування діафрагмою (P-Iris), ІЧ-підсвічування (Optimized IR) і стиск відео Axis Zipstream. Стиск дозволяє майже у два рази скоротити обсяг трафіку й збережених даних (у порівнянні з камерами стандарту H.264). Всі перераховані функції вже включені за замовчуванням для одержання найкращого зображення, тому в налаштування камер зміни вносити не потрібно.

Як сховище використовувався NAS компанії Qnap, одного з технологічних партнерів Axis. Його ємність вибиралася з таким розрахунком, щоб відповідно до вимог замовника можна було зберігати архів записів із всіх камер не менш місяця. Завдяки застосуванню технології Zipstream потік даних від камер знижується вдвічі без втрати важливих деталей зображення. Крім цього, запис

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

дублювалася на встановлені в камерах карти пам'яті, чим забезпечувалося резервування архіву.

Запис налаштований за детектуванням руху. Уночі камера більшу частину часу неактивна, так що архів записів за місяць може поміститися на картці ємністю 64 Гбайт. Для скорочення обсягу даних був обраний мінімальний розв'язний дозвіл, придатне для розпізнавання особи людини й інших важливих деталей. З метою економії засобів замовник взагалі вирішив не створювати сховище для відеозаписів на одному з об'єктів. Установлені картки SanDisk досить надійні, при збої губиться запис тільки з однієї камери.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		7

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

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

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

Ці камери відрізняються чудовою якістю зображення з розв'язним дозволом 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.

Фіксовані корпусні відеокамери

Для запобігання протиправних дій у будь-якому середовищі.

Мережні камери серії AXIS M10

Компактні сучасні камери для малого бізнесу:

- Практичний і інтелектуальний дизайн.
- Легка установка, різні варіанти монтажу.
- Бездротове підключення.
- Оповіщення при несанкціонованих діях.
- Убудований мікрофон і гучномовець.
- Запис на карту пам'яті.

Практичний і інтелектуальний дизайн

Серія відеокамер AXIS M10 представлена компактними сучасними моделями, які ідеально підходять для охоронного відеоспостереження на невеликих об'єктах, наприклад у малому бізнесі, магазинах, ресторанах, готелях і

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		8

приватних будинках. Ці камери забезпечують краще у своєму класі якості зображення й професійних функцій моніторингу.

Висока ефективність стиску й передачі відеопотоку

У мережних камерах AXIS M10 передбачений убудований мікрофон для запису звуку, гучномовець для відтворення заздалегідь записаних повідомлень і пасивний ІЧ-датчик руху, здатний виявляти рух навіть у темряві. Камери цієї моделі підтримує передачу декількох відеопотоків, що набудовуються незалежно, у форматах H.264 і Motion JPEG. Камери працюють із повною частотою кадрів при всіх дозволах і з усіма алгоритмами стиску. Алгоритм стиску H.264 значно знижує бітрейт, дозволяючи скоротити обсяг трафіку й вимоги до дискового простору.

Мережні камери серії AXIS M11 Network Camera Series

Недорогі й прості в застосуванні камери:

- Компактна й універсальна конструкція.
- Передача декількох відеопотоків у форматі H.264.
- Технологія Power over Ethernet.
- Моделі для зовнішнього відеоспостереження.

Недорога, але ефективна камера для охоронного відеоспостереження

Професійні недорогі фіксовані камери серії AXIS M11 Network Camera Series підходять для рішення широкого спектра завдань охоронного відеоспостереження в таких місцях як підприємства роздрібної торгівлі, банки, готелі й інші офісні будинки.

Простота установки як усередині приміщень, так і на вулиці

Ці камери передбачають швидку й просту установку як усередині приміщень, так і на вулиці. Вони ідеально підходять для забезпечення безпеки в магазинах, школах і громадських місцях. Камера одержує живлення через локальну мережу за технологією Power over Ethernet (IEEE 802.3af), тому відпадає необхідність в окремих кабелях живлення й знижується вартість монтажу.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

Мережні камери серії AXIS P13 Network Camera Series

Чудова якість відео в будь-яких умовах:

- Чудова якість відеозображення з розв'язним дозволом від 1 Мп до 4К.
- Неперевершена світлочутливість.
- Технологія Lightfinder і режим Forensic WDR.
- Моделі для зовнішнього відеоспостереження.
- Байонет CS дозволяє використовувати різні об'єктиви.

Міцність і висока світлочутливість

У серію мережних камер AXIS P13 Network Camera Series входять моделі з високою світлочутливістю й розв'язним дозволом до 4К. Серед цих камер є моделі, призначені як для внутрішньої, так і для зовнішньої установки, які підходять для рішення широкого спектра завдань охоронного відеоспостереження в таких місцях, як урядові й виробничі будинки, магазини, приміщення банків, аеропорти, вокзали й школи.

Мережні камери серії AXIS Q16 Network Camera Series

Найвища якість зображення при несприятливих умовах:

- Неперевершена світлочутливість.
- Міцні моделі із захистом від непогоди.
- Технології Lightfinder і Forensic WDR.
- Об'єктиви зі змінною фокусною відстанню й байонетом CS або об'єктиви з байонетом Canon і EF/ EF-S.
- Електронна стабілізація зображення.
- Підтримка PoE і SFP-слот.
- Сумісність із різними системами керування відео.

Неперевершена якість відео при несприятливих умовах освітлення

Фіксовані мережні камери серії AXIS Q16 Network Camera Series, призначені для установки в приміщеннях і на відкритому повітрі, забезпечують найвищу якість зображення в складних умовах відеоспостереження, наприклад, при наявності різних джерел світла, задньому підсвічуванню або слабкій

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		10

освітленості. У цю серію входять навіть моделі з підтримкою технології OptimizedIR для роботи в повній темряві.

У це сімейство входять моделі, призначені для використання усередині приміщень і на вулиці для рішення широкого спектра завдань, включаючи відеоспостереження за дорожнім рухом, в аеропортах, на стадіонах, вокзалах і в школах, а також в урядових і виробничих будинках. Крім того, ці камери підтримують відеоспостереження з реагуванням, що попереджає, завдяки інтелектуальним додаткам відеоаналітики.

Модульні камери

Гнучка установка для винятково малопомітного відеоспостереження в будь-якому місці

Вам потрібно помістити камеру у вкрай обмежений простір? Наприклад, установити її в банкомату, на виході із супермаркету або на борті транспортного засобу? Або просто ходите встановити кілька камер поруч один з одним, не витрачаючи зайвих засобів? У кожному із цих випадків модульні камери Axis буду відмінним рішенням!

Принципи роботи

Модульна камера складається із двох окремих елементів: невеликого оптичного блоку (що складається з об'єктива й матриці) і основного модуля, що відповідає за обробку зображення й передачу даних по мережі. Обидві частини з'єднані кабелем, що дозволяє встановлювати з окремо друг від друга. Ви можете здобувати як комплектні модульні камери, так і оптичні блоки й основні модулі окремо. Ми пропонуємо одно- і чотирьохканальні основні модулі.

Поміститься скрізь

Оптичний блок модульної камери дуже малий, і розмістити його можна навіть у вкрай обмеженому просторі. Основний модуль при цьому можна встановити в іншому місці – там, де є більше вільного простору. У результаті ви одержуєте винятково малопомітну камеру, яку можна змонтувати практично де завгодно.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

Серія AXIS F

Універсальні модульні камери для практично будь-якого середовища:

- Гнучка, надійна, малопомітна конструкція.
- Одноканальні й чотирьохканальні основні блоки.
- Різні оптичні блоки на вибір: для установки в приміщеннях, для установки на вулиці, а також оптичні блоки з різними типами об'єтивів, включаючи стандартний, зі змінною фокусною відстанню, із точковим отвором, «риб'яче око», або з об'єктивом для купольного форми-фактора.
- Wide Dynamic Range і технологія Axis Zipstream.
- Двостороння передача звуку й порти вводу-виводу.
- Локальний запис даних, PoE, 8-28 В пост. струму.

Малопомітні камери для широкого застосування в багатьох місцях

Серія AXIS F містить у собі високопродуктивні камери із гнучкими кабелями й розв'язним дозволом HDTV, які виявляються досить малопомітними як при установці в стаціонарних системах відеоспостереження (у приміщеннях і на вулиці), так і на транспортних засобах. Ці камери ідеально підходять для установки біля банкоматів, у відділеннях банків, магазинах, готелях і для застосування в суворих експлуатаційних умовах, наприклад, на борті автомобілів аварійно-рятувальних служб, автобусів, трамваїв, вантажних автомобілів.

Модульна концепція

Конструкція моделей серії AXIS F заснована на концепції розділеної мережної камери, відповідно до якої камера складається із двох частин (модулів): оптичного блоку, що містить у собі об'єтив і датчик зображень із кабелем, і основного блоку, що, властиво, і є камерою. Така модульна конструкція забезпечує гнучкість у виборі апаратних компонентів і способів установки системи. Компактні оптичні блоки можна малопомітно розміщати навіть в обмеженому просторі, а базовий блок, що підключається довгим кабелем, можна розташовувати у вільному місці там, де це зручно зробити. Після первісної

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		12

установки оптичний або основний блок легко перемістити в інше місце або замінити, що ще більше підвищує гнучкість конфігурації системи.

Серія AXIS FA

Високопродуктивні модульні камери для гнучкого застосування:

- Недороге відеоспостереження із багатопоточним переглядом.
- Гнучка й у край малопомітна система для роботи в приміщеннях.
- 4-канальний основний модуль.
- Можливість вибору оптичних блоків зі стандартним об'єктивом, точковим об'єктивом і об'єктивом зі змінною фокусною відстанню.
- Передача відеопотоків з повною частотою кадрів і розв'язним дозволом 1080p із чотирьох оптичних блоків.
- Технологія Forensic WDR.
- Технологія Axis Zipstream.

Недороге відеоспостереження із багатопоточним переглядом

AXIS FA – це серія пропонованих за привабливими цінами високопродуктивних модульних камер для багатоканального відеоспостереження, за допомогою яких можна практично непомітно спостерігати за чотирма близько розташованими друг від друга приміщеннями, використовуючи один IP-адресу. Моделі цієї серії ідеально підходять для використання в магазинах, банках, офісах і аеропортах.

У моделях цієї серії використовується один чотирьохканальний основний блок (AXIS FA54) і три оптичних блоки (AXIS FA1105 зі стандартним об'єктивом, AXIS FA1125 із точковим об'єктивом і купольний блок AXIS FA4115, у якого об'єктив має змінну фокусну відстань). Основний модуль може підключатися до чотирьох оптичних блоків; він оснащений високопродуктивним процесором, що забезпечує потокову передачу відео з повною частотою кадрів і розв'язним дозволом HDTV 1080p одночасно із всіх чотирьох оптичних блоків.

Якщо врахувати підтримку широкого динамічного діапазону (WDR), технології Zipstream, засобів аналітики, розпізнавання HDMI, звуку, портів

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		13

уведення-виводу й локального зберігання даних, то розрахунок сукупної вартості володіння показує, що система серії AXIS FA є досить вигідним придбанням.

Малопомітна установка й гнучкість застосування

Подібно всім модульним системам камер, серія AXIS FA відрізняється особою малопомітністю й гнучкістю. Конструкція пристроїв із цієї серії заснована на концепції розділеної мережної камери, відповідно до якої камера складається із двох частин – датчика зображень із об'єктивом і основним блоком, що, властиво, і є камерою. Модулі з'єднуються кабелем, що входить у комплект поставки оптичного блоку.

Малюсінькі оптичні блоки можна практично непомітно встановлювати на рівні очей або в дуже обмеженому просторі. Довгий кабель, що йде від оптичного до основного блоку, дозволяє розміщати основний блок там, де для нього є місце.

У серії AXIS FA основні модулі й оптичні блоки продаються окремо, тому ви можете вибрати найбільш підходящі оптичні блоки для своїх умов застосування. Зверніть увагу, що основні модулі й оптичні блоки серії AXIS FA не можна використовувати в сполученні з основними модулями й оптичними блоками із серії AXIS F.

Чудова деталізація

Система серії AXIS FA забезпечує потокову передачу відео з повною частотою кадрів і розв'язним дозволом HDTV 1080p, щоб не пропустити ніяких деталей або дій. Крім того, вона при будь-яких обставинах підтримує технологію Axis Forensic WDR. Технологія Forensic WDR у пристроях серії AXIS FA установлює пріоритет для більше темних ділянок сцени з висококонтрастним джерелом світла, наприклад як у сценарії з фоновим засвітченням, коли напроти людини розташовується дуже яскраве тло. У такому сценарії звичайна камера без підтримки широкого динамічного діапазону створює темне зображення людини. Завдяки технології Forensic WDR у пристроях серії AXIS FA кольору й деталі в затемнених ділянках будуть більше помітними. Крім того, технологія Forensic WDR у пристроях серії AXIS FA оптимізована для руху, тому при влученні в

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14

кадр швидко, що переміщається об'єкта, артефакти руху відсутні. У сценах з недостатнім освітленням система серії AXIS FA забезпечує чудове кольорове відео з низьким рівнем шуму.

Збереження загальної суми витрат на низькому рівні

Система серії AXIS FA із чотирма оптичними блоками HDTV з розв'язним дозволом 1080p найчастіше обходиться дешевше, ніж чотири стандартних камери HDTV з розв'язним дозволом 1080p і аналогічними функціями. А за рахунок наявності єдиного кабелю Ethernet для чотирьох оптичних блоків можна скоротити вимоги до мережних портів і заощадити на вартості мережного комутатора. Крім іншого, при наявності одного IP-адреси може знадобитися тільки одна ліцензія на ПЗ для керування відео (VMS), що дає право переглядати відео із чотирьох оптичних блоків.

Система серії AXIS FA також забезпечує економію потреб у пропускній здатності й зберіганні. Наприклад, технологія Axis Zipstream ефективно кодує відеопотоки стандарту H.264, скорочуючи вимоги до сховища й смуги пропускання на величину до 50% і більше, при цьому важливі ділянки зображення зберігаються. Відеозапис, що при настанні події активується завдяки підтримуваним засобам аналітики (таких як відеодетектор руху, оповіщення при несанкціонованих діях і інші додатки, сумісні із платформою AXIS Camera Application Platform), також сприяє скороченню трафіку й ресурсів сховища. Перевірити сумісність додатків відеоаналітики можна на спеціальному веб-сайті.

Мережні камери серії AXIS P12

Повністю модульні, модернізовані камери для малопомітного відеоспостереження:

- Функціональна й надзвичайно малопомітна конструкція.
- Легка установка, різні варіанти монтажу.
- Розв'язний дозвіл до HDTV 1080p.
- Запис на карту пам'яті.
- Технологія Zipstream.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

– Технологія Power over Ethernet.

Винятково малопомітне відеоспостереження

Мережні камери серії AXIS P12 – це недорогі повнофункціональні пристрої з розв'язним дозволом HDTV 720p/1080p, що дозволяють звістки винятково малопомітне внутрішнє й зовнішнє відеоспостереження. Конструкція камер дозволяє їм легко вписуватися в навколишнє середовище. Вони ідеально підходять для установки в банкоматах, банках, магазинах, готелях, на архітектурних спорудженнях і в офісах.

Ці камери можуть бути встановлені на поверхні або заподлице в таких місцях як стіни й стелі, ліфти, або обмежений простір банкомату або дверного прорізу.

Модульна конструкція

До складу камери AXIS P12 входить оптичний блок (що складається з об'єктива й датчика зображень) з кабелем довжиною 8 м і основний модуль (з розніманням локальної мережі, розніманням живлення й слотом для карти пам'яті). Обидві частини з'єднані кабелем, що дозволяє встановити оптичний блок так, що він буде винятково малопомітним в обмеженому просторі, а основний модуль установити десь в іншому місці. Пристрою AXIS P12 можуть одержувати живлення за технологією PoE.

Інтелектуальні відеотехнології

У камерах AXIS P12 є можливість використання інтелектуальних відеотехнологій, включаючи детектор руху й оповіщення при несанкціонованих діях. Також передбачена підтримка платформи AXIS Camera Application Platform.

Зручне керування відео

Камери AXIS P12 оснащені убудованими слотами для карт пам'яті microSD, які служать для локального запису відео й для роботи з додатковим програмним забезпеченням, наприклад, з AXIS Companion. Все це створює зручне рішення для керування відеоспостереженням. Кодування відеопотоків здійснюється у форматах H.264 і Motion JPEG.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		16

Мережні камери серії AXIS P12

Повністю модульні, модернізовані камери для малопомітного відеоспостереження:

- Функціональна й надзвичайно малопомітна конструкція.
- Легка установка, різні варіанти монтажу.
- Розв'язний дозвіл до HDTV 1080p.
- Запис на карту пам'яті.
- Технологія Zipstream.
- Технологія Power over Ethernet.

Винятково малопомітне відеоспостереження

Мережні камери серії AXIS P12 – це недорогі повнофункціональні пристрої з розв'язним дозволом HDTV 720p/1080p, що дозволяють звістки винятково малопомітне внутрішнє й зовнішнє відеоспостереження. Конструкція камер дозволяє їм легко вписуватися в навколишнє середовище. Вони ідеально підходять для установки в банкоматах, банках, магазинах, готелях, на архітектурних спорудженнях і в офісах.

Ці камери можуть бути встановлені на поверхні або заподлице в таких місцях як стіни й стелі, ліфти, або обмежений простір банкомату або дверного прорізу.

Модульна конструкція

До складу камери AXIS P12 входить оптичний блок (що складається з об'єктива й датчика зображень) з кабелем довжиною 8 м і основний модуль (з розніманням локальної мережі, розніманням живлення й слотом для карти пам'яті). Обидві частини з'єднані кабелем, що дозволяє встановити оптичний блок так, що він буде винятково малопомітним в обмеженому просторі, а основний модуль установити десь в іншому місці. Пристрої AXIS P12 можуть одержувати живлення за технологією PoE.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

Комплект стереодатчиків AXIS P8804

Функції:

- Точний підрахунок за допомогою сумісного програмного забезпечення.
- Підвищена точність.
- Комплект стереодатчиків AXIS P8804 дозволяє одержати синхронізоване стереозображення від оптичного стереоблока AXIS F8804 і основного модуля AXIS F34.

Якщо доповнити цей комплект сумісними додатками аналітики, розробленими компанією Axis або її партнерами, то отримане рішення забезпечить більше високу точність при виконанні таких функцій як підрахунок людей, керування чергами й складання теплових карт.

Функція стереозображення дозволяє створювати тривимірне відображення, що підвищує точність аналітичних додатків, наприклад при підрахунку людей. За допомогою тривимірної карти глибин подібні додатки можуть ефективно працювати при несприятливому освітленні в місці розташування камери: при наявності тіней, яскравого сонячного світла, відблисків або інтенсивних людських потоків. Завдяки тривимірній карті аналітичне програмне забезпечення може визначати висоту підраховуваних об'єктів, не з огляду на такі предмети як візки й коляски. Крім того, немає необхідності забирати із зони підрахунку товари, стенди або полки.

Малопомітна установка

Оптичний стереоблок призначений для монтажу в приміщеннях на стелі – це може бути як малопомітна установка на навісній стелі, так і установка заподлице за допомогою прикладеного адаптера. Сумісне аналітичне програмне забезпечення буде працювати в основному блоці, якому можна встановити на відстані до 8 метрів від оптичного блоку. Електроживлення подається на основний модуль за технологією Power over Ethernet (PoE) або від низьковольтного джерела постійного струму. AXIS P8804 ідеально підходить для відеоспостереження в магазинах, у банках, на вокзалах і в аеропортах.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		18

AXIS 3D People Counter

Інтелектуальний аналіз тривимірного простору для підрахунку людей у складних умовах:

- Точний і надійний підрахунок людей у тривимірному просторі.
- Оптимально підходить для високоінтенсивних потоків.
- Найкраще рішення для середовищ із яскравим світлом і тінями.
- Оптимізація маркетингової політики.
- Підвищення ефективності розподілу персоналу й планування заходів у

магазині.

Оптимізація роботи магазину

Додаток AXIS 3D People Counter надає критично важливі дані для оптимізації роботи магазину. Воно здатно відповісти на питання про те, скільки людей приходить у ваші магазини щодня й скільки з них роблять покупки. Додаток у режимі реального часу автоматично підраховує кількість людей, що проходять під стереоскопічною камерою, з урахуванням напрямку руху.

Відомості про трафік в магазині допомагають виконувати наступні завдання:

- аналіз потоків покупців і тенденцій зміни трафіку;
- оцінка впливу реклами й промо-акцій;
- більше раціональне розміщення співробітників і визначення найкращого часу початку роботи, щоб забезпечити відмінна якість обслуговування клієнтів і оптимізувати витрати на персонал;
- оцінка впливу погоди на кількість покупців;
- виявлення й заохочення ефективно працюючих магазинів і співробітників.

При інтеграції із системою касових терміналів можна збирати коштовну й надійну інформацію про коефіцієнти конверсії, а це істотні характеристики, які необхідно враховувати при прийнятті найважливіших рішень для бізнесу.

Точність і надійність

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		19

Додаток AXIS 3D People Counter у сполученні із установлюваним на стелі комплектом стереодатчиків AXIS P8804 забезпечує особливу точність у важких ситуаціях, наприклад при наявності інтенсивного потоку людей або яскравого сонячного світла, відблисків і тіней. Крім того, немає необхідності забирати із зони підрахунку наявні товари, стенди або полки.

Рішення дозволяє встановлювати комплект стереодатчиків у проходах на висоті 2,4-4 м від землі з охоптом 1,7-2,5 м.

Інтеграція й доступ до даних

Додаток AXIS 3D People Counter записує дані безпосередньо на кожен камеру, де вони зберігаються до 90 днів. За допомогою додатка можливий тільки числовий підрахунок. Ніякі зображення або відео не зберігаються. Відкритий протокол додатка дозволяє вмонтувати результати підрахунку людей у систему касового термінала або в інші системи. Для користувачів передбачено чотири способи доступу до даних:

- За допомогою стандартного веб-браузера, що забезпечує доступ до веб-інтерфейсу камери, а значить – до живого перегляду й графічного подання статистичних параметрів. У цьому випадку немає необхідності встановлювати в магазині сервер або яке-небудь інше встаткування.

- Через відкритий інтерфейс HTTP API камери, що дозволяє одержувати статичні вихідні дані в режимі реального часу, а також дані за зазначені періоди часу, причому в різних форматах, включаючи JSON, XML і CSV.

- За допомогою веб-служби AXIS Store Reporter, що збирає статистичні дані з різних джерел – аналітичних додатків Axis для роздрібної торгівлі – і представляють ці дані й графіки в одному інтерфейсі. Це ідеальний спосіб при наявності декількох об'єктів (магазинів), де встановлено кілька камер.

- За допомогою прикладної програми AXIS Store Data Manager, що запускається локально й забезпечує просту інтеграцію даних в інтелектуальні додатки бізнес-аналітики сторонніх виробників.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		20

2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування

Як мова програмування обрана Python. Python – високорівнева мова програмування загального призначення з акцентом на продуктивність розроблювача й читаність коду. Синтаксис ядра Python мінімалістичний. У той же час стандартна бібліотека включає великий обсяг корисних функцій.

Python підтримує кілька парадигм програмування, у тому числі структурне, об'єктно-орієнтоване, функціональне, імперативне й аспектно-орієнтоване. Основні архітектурні риси – динамічна типізація, автоматичне керування пам'яттю, повна інтроспекція, механізм обробки виключень, підтримка багатопоточні обчислень і зручні високорівневі структури даних. Код у Python організовується у функції й класи, які можуть поєднуватися в модулі (які у свою чергу можуть бути об'єднані в пакети).

Еталонною реалізацією Python є інтерпретатор CPython, що підтримує більшість активно використовуваних платформ. Він поширюється вільно під дуже ліберальною ліцензією, що дозволяє використовувати його без обмежень у будь-яких застосунках, включаючи пропрієтарні. Є реалізації інтерпретаторів для JVM (з можливістю компіляції), MSIL (з можливістю компіляції), LLVM і інших. Проект PyPy пропонує реалізацію Python на самому Python, що зменшує витрати на зміни мови й постановку експериментів над новими можливостями.

Python – мова програмування, що активно розвивається, нові версії (з додаванням/зміною мовних властивостей) виходять приблизно раз у два з половиною року. Внаслідок цього й деяких інших причин на Python відсутні ANSI, ISO або інші офіційні стандарти, їхня роль виконує CPython.

Python портований і працює майже на всіх відомих платформах – від КПК до мейнфреймів. Існують порти під Microsoft Windows, практично всі варіанти UNIX (включаючи FreeBSD і Linux), Plan 9, Mac OS і Mac OS X, iPhone OS 2.0 і вище, Palm OS, OS/2, Amiga, AS/400 і навіть OS/390, Symbian і Android.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		21

При цьому, на відміну від багатьох портуємих систем, для всіх основних платформ Python має підтримку характерних для даної платформи технологій (наприклад, Microsoft COM/DCOM). Більше того, існує спеціальна версія Python для віртуальної машини Java – Jython, що дозволяє інтерпретаторові виконуватися на будь-якій системі, що підтримує Java, при цьому класи Java можуть безпосередньо використовуватися з Python й навіть бути написаними на Python. Також кілька проектів забезпечують інтеграцію із платформою Microsoft .NET, основні з яких – IronPython і Python.Net.

Python підтримує динамічну типізацію, тобто тип змінної визначається тільки під час виконання. Тому замість «присвоювання значення змінної» краще говорити про «зв'язування значення з деяким ім'ям». У Python є убудовані типи: бульові, рядки, Unicode-рядки, цілі числа довільної точності, числа із плаваючою комою, комплексні числа й деякі інші. З колекцій Python підтримує кортежі (*tuples*), списки, словники (асоціативні масиви) і, починаючи з версії 2.4, безлічі. Всі значення в Python є об'єктами, у тому числі функції, методи, модулі, класи.

Додати новий тип можна або написавши клас (*class*), або визначивши новий тип у модулі розширення (наприклад, написаному мовою C). Система класів підтримує спадкування (одиначне й множинне) і метапрограмування. Можливе спадкування від більшості убудованих типів і типів розширень.

Всі об'єкти діляться на посилальні й атомарні. До атомарного ставляться *int*, *long*, *complex* і деякі інші. При присвоюванні атомарних об'єктів копіюється їхнє значення, у той час як для посилальних копіюється тільки покажчик на об'єкт, таким чином, обидві змінні після присвоювання використовують те саме значення. Посилальні об'єкти бувають змінювані й незмінні. Наприклад, рядки й кортежі є незмінними, а списки, словники й багато інших об'єктів – змінюваними. Кортеж у Python є, по суті, незмінним списком. У багатьох випадках кортежі працюють швидше списків, тому якщо ви не плануєте змінювати послідовність, то краще використовувати саме їх.

Мова має чіткий і послідовний синтаксис, продуману модульність й масштабованість, завдяки чому вихідний код написаних на Python програм легко читаємий.

Python – стабільна й розповсюджена мова. Він використовується в багатьох проектах і в різних якостях: як основна мова програмування або для створення розширень і інтеграції застосунків. На Python реалізоване велика кількість проектів, також він активно використовується для створення прототипів майбутніх програм. Python використовується в багатьох великих компаніях.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускню кваліфікаційну роботу за першим (бакалаврським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis.

В процесі розробки випускної кваліфікаційної роботи за першим (бакалаврським) 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 кібербезпеки 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

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		23

забезпечать впровадження системи кібербезпеки 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) сформулювати висновки про виконаний обсяг робіт та одержані результати.

К6ПЗ-2026

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

У кожному із трьох кафе мережі «Кухня Ганнусі» було розміщено від 5 до 8 камер, так що при необхідності інсталяцію можна було б масштабувати.

Більша частина використовуваних моделей камер має розв'язний дозвіл 2 Мпкс, при цьому віддалений доступ до них планувався винятково з мобільних пристроїв. Відповідно, досить було інтернет-каналу із пропускною здатністю не більше 5 Мбіт/с.

Монтаж за ніч

Всі три кафе розташовані на території діючих спортивних і ділових комплексів, тому вдень будь-які гучні роботи заборонені.

Монтаж устаткування вироблявся винятково в нічний час. Два із трьох кафе перебувають на різних поверхах одного будинку, і для них передбачена загальна система зберігання. Щоб прокласти кабель між поверхами й установити встаткування, монтажникам довелося працювати дві ночі, на іншому об'єкті все було зроблено за одну ніч. Ніяких будівельних робіт, природно, не проводилося – кабель прокладався за підвісною стелею.

Наступного дня інші фахівці здійснили налаштування камер, віддаленого доступу й системи зберігання й з першої спроби виконали запуск системи. Реалізація проекту, від першого контакту до уведення в експлуатацію, зайняла менше двох місяців.

Технічні фахівці системи відеоспостереження в штаті компанії не передбачені, як і відповідні витрати в бюджеті на обслуговування за договором. Для малого бізнесу будь-які додаткові щомісячні абонентські платежі – обтяжне навантаження, тому краще один раз вкластися в придбання якісного встаткування, щоб згодом без проблем його експлуатувати.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

Треба сказати, ставка на Axis себе виправдала. Її переваги особливо добре видні в порівнянні з аналоговою системою, що компанія продовжує використовувати на фабриці-кухні й міняти, незважаючи на її недоліки, поки не збирається. Все-таки це працююча інфраструктура, а її заміна вимагає додаткових витрат, що для невеликого підприємства обтяжливо.

Ніяких збоїв у роботі камер Axis і сховищ Qnap зафіксовано не було. Устаткування продовжує надійно працювати з моменту його установки, і навіть у споконвічних налаштуваннях з тих пор так нічого й не мінялося.

Світ безпеки змінюється. Чи готова ваша поточна система до того, що буде далі?

Відеоспостереження фундаментально переходить від суто реактивного інструменту до двигуна проактивної бізнес-аналітики та безпеки.

Ця трансформація зумовлена двома невід'ємними силами:

– Хмарний штучний інтелект: вихід за рамки простого виявлення об'єктів до створення складних правил на основі природної мови, автоматизація абсолютно нових робочих процесів для безпеки та операцій.

– Переломний момент для корпоративної хмари: вартість обслуговування застарілих локальних систем зараз перевищує ефективність та передбачувані операційні витрати сучасних уніфікованих хмарних платформ.

Також дослідили критичні тенденції, такі як зростання активної готовності до реагування на інциденти, зростаючий попит на функції на основі штучного інтелекту, такі як виявлення зброї, та те, як дотримання нормативних вимог стає основною операційною реальністю.

Особи, що приймають рішення, – від бізнес-лідерів до муніципальних менеджерів – повинні знати, яка платформа є достатньо гнучкою для того, що буде далі. Це означає розпізнавання людей, транспортних засобів та об'єктів (від касок до зброї на витягнутому обличчі), щоб забезпечити швидке та належне реагування. А також бути готовим до аудиту цілий рік, маючи журнали, які витримують перевірку регуляторних органів. Однак, це більше, ніж просто

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		26

предмети чи проста передача повідомлень, а й ініціювання дій у відповідь на складні ситуації, коли проблема безпеки виявляється на камеру.

А коли виникає надзвичайна ситуація, це також означає координацію з місцевими службами екстреної допомоги, щоб забезпечити обізнаність про ситуацію, необхідну поліції та пожежникам для впевненого виконання своєї роботи.

Якщо ви вже користуєтеся хмарною системою керування відео (VMS) Eagle Eye, ви, ймовірно, знаєте, що ми вже впроваджуємо системи, які допомагають зробити ці тенденції корисними в реальному світі. Не дивно: інтеграція штучного інтелекту з відеоспостереженням була давнім пріоритетом для Eagle Eye, і ще довше ми пропонуємо клієнтам доступ до їхніх відеоданих з будь-якого місця через хмару.

Різниця полягає в тому, що штучний інтелект випередив можливості, тому вчорашні передові функції є сьогоднішніми відправними точками – або ж мали б бути. І межі відповідно змістилися: розширене виявлення об'єктів і складні автоматизовані дії тепер легкодоступні.

3.2 Розробка структурної схеми

Розглядаючи тенденції відеобезпеки на 2026 рік, одне зрозуміло: самого лише розширення зони охоплення камерами недостатньо. Роками організації зосереджувалися на видимості – додаючи більше камер, більше сховища та більше відеоматеріалів. Але саме покриття більше не визначає зрілість безпеки. Натомість керівники ставлять важливіше питання: Які результати мають усі ці години відеовиробництва?

На всьому ринку ми спостерігаємо структурний зсув від пасивного спостереження до проактивного відеомоніторингу та операцій безпеки на основі розвідувальних даних. Технологічні можливості розвиваються, регуляторні вимоги зростають, а організації перебувають під тиском щодо доведення

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		27

вимірюваних результатів. Результатом є новий стандарт того, як виглядатиме «ефективна» відеобезпека у 2026 році.

Кілька визначальних тенденцій у сфері відеобезпеки формують перспективи на 2026 рік.

1. Проактивний відеомоніторинг тепер є базовим

Однією з найважливіших тенденцій відеобезпеки у 2026 році є кінець принципу «записуй зараз, переглядай потім» як прийнятної операційної моделі.

Організації дедалі більше очікують відеомоніторингу в режимі реального часу, який дозволяє раніше втручатися, швидше перевіряти та знижувати ризики до ескалації інцидентів. Цей зсув відображає зростання інтелектуальної відеобезпеки, де системи розроблені не лише для захоплення відеоматеріалів, а й для допомоги командам у реагуванні на них.

Програми безпеки тепер оцінюватимуться за такими операційними результатами, як:

- Час до виявлення.
- Час до перевірки.
- Час відповіді.

Ці показники безпосередньо впливають на запобігання втратам, ризик відповідальності та безперервність бізнесу. Рішення, що підтримують перевірений відеовідповідь та керований відеомоніторинг, стають центральними в стратегіях безпеки підприємств, особливо для організацій, які керують кількома об'єктами або середовищами з високим рівнем ризику.

2. Штучний інтелект та відеоаналітика для операцій безпеки стають основною інфраструктурою

Штучний інтелект більше не є новинкою в запитах пропозицій на безпеку. Він швидко стає основною інфраструктурою сучасних програм безпеки, дозволяючи командам безпеки швидше виявляти ризики, зменшувати шум і приймати кращі рішення в розподілених середовищах. Ця еволюція докорінно змінила характер спостереження.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

Сучасна відеоаналітика тепер може ідентифікувати поведінку, співвідносити сигнали з кількох датчиків та виявляти потенційні загрози з рівнем швидкості та узгодженості, який був би немислимим ще кілька років тому. Виявлення, яке було основним обмеженням в операціях безпеки, більше не є обмежувальним фактором.

Натомість постало набагато важливіше питання: Щойно ІІІ щось виявляє, хто відповідає за вирішення того, що буде далі?

Штучний інтелект має розширені можливості виявлення швидше, ніж більшість організацій змогли впровадити реагування.

На практиці вузьке місце змістилося. Системи тепер здатні виявляти потенційні ризики з надзвичайною точністю. Але без чітко визначених робочих процесів, структур підзвітності та людського судження, вбудованого в процес, ці висновки застоюються. Сповіщення накопичуються. Шум зростає. А цінність штучного інтелекту зменшується.

Ось чому ІІІ більше не розглядається як окрема можливість. Він стає операційною інфраструктурою, яка ефективна лише в поєднанні з управлінням, логікою ескалації та навченими особами, що приймають рішення, які розуміють, коли і як втручатися.

Організації, які правильно це роблять, не запитують: «Скільки подій може виявити ІІІ?». Вони запитують: «Наскільки впевнено ми можемо діяти на основі того, що виявляє ІІІ?».

Цей перехід – від виявлення до прийняття рішень, визначатиме наступний етап інтелектуальної безпеки. Галузеві організації зараз описують візуальний ІІІ як такий, що забезпечує операційну цінність у різних випадках використання фізичної безпеки, переходячи від експериментального впровадження до повноцінного виробництва.

У 2026 році визначальним питанням буде не те, чи використовується штучний інтелект, а те, як він регулюється, включаючи контроль хибних тривог, нагляд за ефективністю та структуроване прийняття рішень з участю людини.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		29

3. Довіра, управління та відповідність вимогам визначатимуть інтелектуальну відеобезпеку

Керівники служб безпеки тепер несуть відповідальність не лише за те, що виявляють їхні системи, але й за те, наскільки відповідально вони їх експлуатують.

У 2026 році сходяться дві основні сили:

– Структури управління штучним інтелектом стають центральними в управлінні ризиками підприємства. Структура управління ризиками, пов'язаними зі штучним інтелектом (ШІ), розроблена NIST, широко використовується як модель управління надійністю, конфіденційністю, безпекою та захистом у системах на базі ШІ.

– Регуляторний тиск посилюється, особливо в Європі. Закон ЄС про штучний інтелект був прийнятий у 2024 році та повністю набуває чинності у серпні 2026 року, запроваджуючи поетапні вимоги до дотримання вимог, які безпосередньо впливають на технології спостереження.

В результаті покупці дедалі більше надаватимуть перевагу партнерам, які можуть продемонструвати задокументовані засоби контролю: забезпечення конфіденційності на етапі розробки, прозорі методи зберігання даних, пояснену логіку сповіщень, де це можливо, та посилену кібербезпеку.

4. VSaaS набирає обертів, завдяки відеоаналітиці для операцій безпеки, що сприяє їхньому впровадженню

В рамках ширших тенденцій відеобезпеки у 2026 році ринок відеоспостереження як послуги (VSaaS) продовжує розширюватися, оскільки організації надають пріоритет гнучким моделям споживання та керованим результатам над капіталомісткими підходами, що базуються лише на апаратному забезпеченні. Впровадження хмарних технологій у фізичній безпеці вийшло за рамки простого прагнення – тепер це часто є стандартним шляхом закупівель для підприємств з кількома об'єктами, які прагнуть пришвидшити розгортання, уніфікувати управління та створити довгострокову масштабованість платформи.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		30

Впровадження хмарних технологій у сфері фізичної безпеки більше не є чимось амбітним. Це стало стандартним способом закупівель для підприємств з кількома об'єктами, які прагнуть швидшого розгортання, централізованого управління та довгострокової масштабованості.

VSaaS дозволяє організаціям централізовано керувати камерами, аналітикою та моніторингом у розподілених місцях, зменшуючи локальну інфраструктуру, мінімізуючи накладні IT-витрати та покращуючи узгодженість між портфелями.

Водночас більшість підприємств не повністю переносять свою діяльність за межі офісу. Домінуючою архітектурою, що з'явиться у 2026 році, є гібридна хмара, що поєднує периферійну обробку даних для низької затримки реагування з хмарними платформами для аналітики, стійкості та оркестрації на рівні підприємства.

Лідери галузі постійно вказують на гібридну хмару, кібербезпеку та управління як визначальні сили, що формують сучасну відеоаналітику для операцій безпеки. Такий підхід дозволяє організаціям поступово модернізуватися, уникати руйнівних проектів копіювання та заміни та масштабуватися без створення операційних труднощів.

5. Стандарти кібербезпеки для керованого відеомоніторингу підвищуються

Відеосистеми тепер є основними мережевими активами, що робить їх частиною профілю кіберризиків організації.

У 2026 році закупівлі фізичної безпеки тісно пов'язані з управлінням IT. Прозорість постачальників, гарантії від третіх сторін та безпечне управління життєвим циклом більше не є необов'язковими.

Цей контроль також поширюється на дотримання вимог ланцюга постачання. Список обмежень FCC продовжує змінюватися, відображаючи обмеження, пов'язані з NDAA, які включають певне обладнання та послуги зв'язку та відеоспостереження.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		31

Для лідерів у сфері безпеки це означає одне: безпечне розгортання та безпечна робота тепер є фундаментальними критеріями покупки.

6. Метадані забезпечують дієвий відеоінтелект

Критичним і часто недооціненим зрушенням, що відбувається, є перехід галузі до стандартизованих метаданих аналітики. Замість потокового відео, сучасні системи все частіше обмінюються структурованими даними: об'єктами, класифікаціями, поведінкою та контекстними сигналами.

Деякі системи, наприклад, ONVIF, дозволяють налаштовувати та потоково передавати аналітичні метадані, такі як класифікація об'єктів, номерні знаки, обличчя, транспортні засоби та виявлення людського тіла.

Це має велике значення у 2026 році, оскільки метадані дозволяють програмам безпеки інтелектуально масштабуватися в різних портфелях, підтримуючи безпеку, захист та операції, не прив'язуючи клієнтів до жорстких власницьких екосистем.

Прогноз відеобезпеки на 2026 рік: програми безпеки оцінюватимуться за результатами, а не за візуальними характеристиками. Коли ці тенденції сходяться, вимальовується чітка картина. 2026 рік не про розгортання більшої кількості камер. Йдеться про побудову операційної моделі безпеки, яка поєднує інтелектуальне виявлення, проактивний відеомоніторинг, надійне управління та вимірюваний вплив на бізнес завдяки дієвій відеоаналітиці.

Ми бачимо, що організації, які досягають успіху, мають чотири спільні зобов'язання:

- Вони надають пріоритет швидшій перевірці та реагуванню, а не лише виявленню.
- Вони використовують гібридні архітектури, які масштабуються без ускладнень.
- Вони розглядають управління штучним інтелектом та конфіденційність як основні принципи дизайну.

– Вони створюються для забезпечення сумісності та зростання на основі метаданих .

У 2026 році лідерів визначатиме не кількість зібраних відео. Їх визначатиме кількість чіткості, яку вони створюють, і те, наскільки рішуче вони на її основі діють.

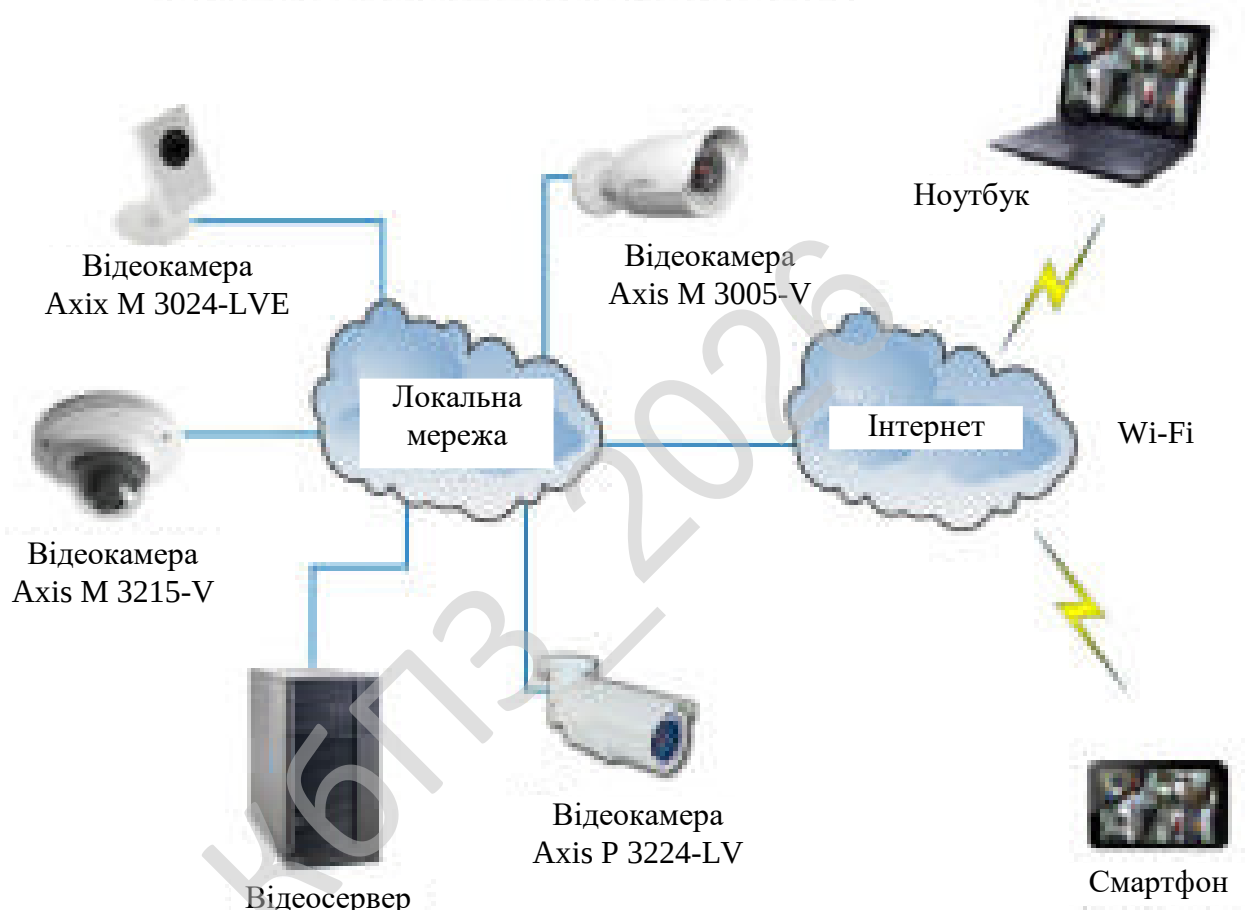


Рисунок 3.1 – Структурна схема системи

Вибір камер визначався умовами на конкретному об'єкті. Над касою встановлювалися камери з вузьким кутом огляду, а для одержання загального виду залу – пристрою із широким сектором огляду. Усього використовувалося п'ять різних моделей компактних камер серії AXIS M30:

- Axis M 3024-LVE.
- Axis M 3005-V.

- Axis M 3006-V.
- Axis M 3215-V.
- Axis P 3224-LV.

У кафе, що перебуває біля басейну, була встановлена модульна камера Axis F34 з виносними блоками (чотири блоки підключені до однієї бази для моніторингу різних зон). Спостереження за складом, у тому числі в темний час доби, здійснювалося за допомогою камери Axis M 1145-L з убудованим світлодіодним ІЧ-підсвічуванням.

У всіх перерахованих моделях підтримуються сучасні технологічні можливості:

- розширений динамічний діапазон (WDR Forensic Capture);
- точне керування діафрагмою (P-Iris);
- ІЧ-підсвічування (Optimized IR) і стиск відео Axis Zipstream.

Стиск дозволяє майже у два рази скоротити обсяг трафіку й збережених даних (у порівнянні з камерами стандарту H.264). Всі перераховані функції вже включені за замовчуванням для одержання найкращого зображення, тому в налаштування камер зміни вносити не потрібно.

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 кібербезпеки для відеонагляду мережі кафе з використанням камер Axis. Далі за допомогою відеокамер спостереження фірми Axis за розробленою схемою (рисунки 3.1) і застосуванні локального обладнання фірми Axis (KVM) сигнал надходить у кімнату операторів де обробляється на сервері за допомогою розробленого ПЗ.

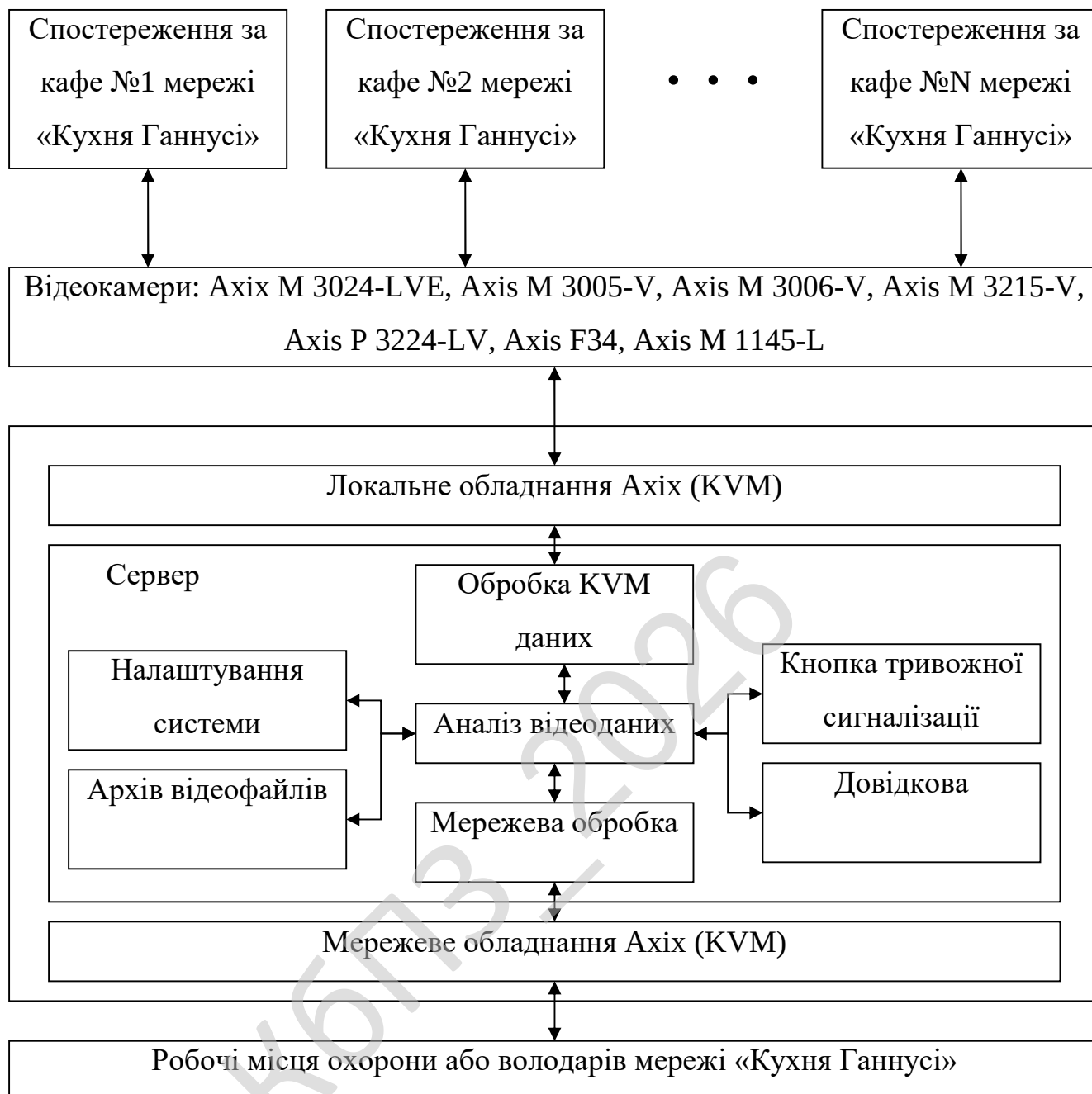


Рисунок 3.2 – Функціональна схема системи

Спочатку проходить обробка KVM даних з послідуочим 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 масштабованості системи й контролю дій над співробітниками сигнал також через мережне обладнання фірми Axis (KVM) 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.

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

3.4 Розробка діаграми процесів

Розглянемо розроблену діаграму процесів яка зображена на рисунку 3.3. Основна будова діаграми процесів полягає у графічному представленні складу сукупностей даних, що характеризуються як співвідношення різних частин кожної з сукупностей. Склад статистичної сукупності графічно може бути представлений як за допомогою абсолютних, так і відносних показників. Графічне зображення складу сукупності по абсолютними і відносними показниками сприяє проведенню більш глибокого аналізу і дозволяє проводити аналіз системи.

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.

При детальному її розгляді можна побачити як саме проходить взаємодія у розробленій системі. Використовується модель проектування, графічне представлення «потоків» даних в інформаційній системі.

Діаграми потоків даних містять чотири типи елементів:

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		36

- Зовнішні по відношенню до системи сутності.
- Потоки даних між елементами трьох попередніх типів.
- Процеси які являють собою трансформацію даних в рамках описуваної системи.
- Сховища даних (репозиторії).

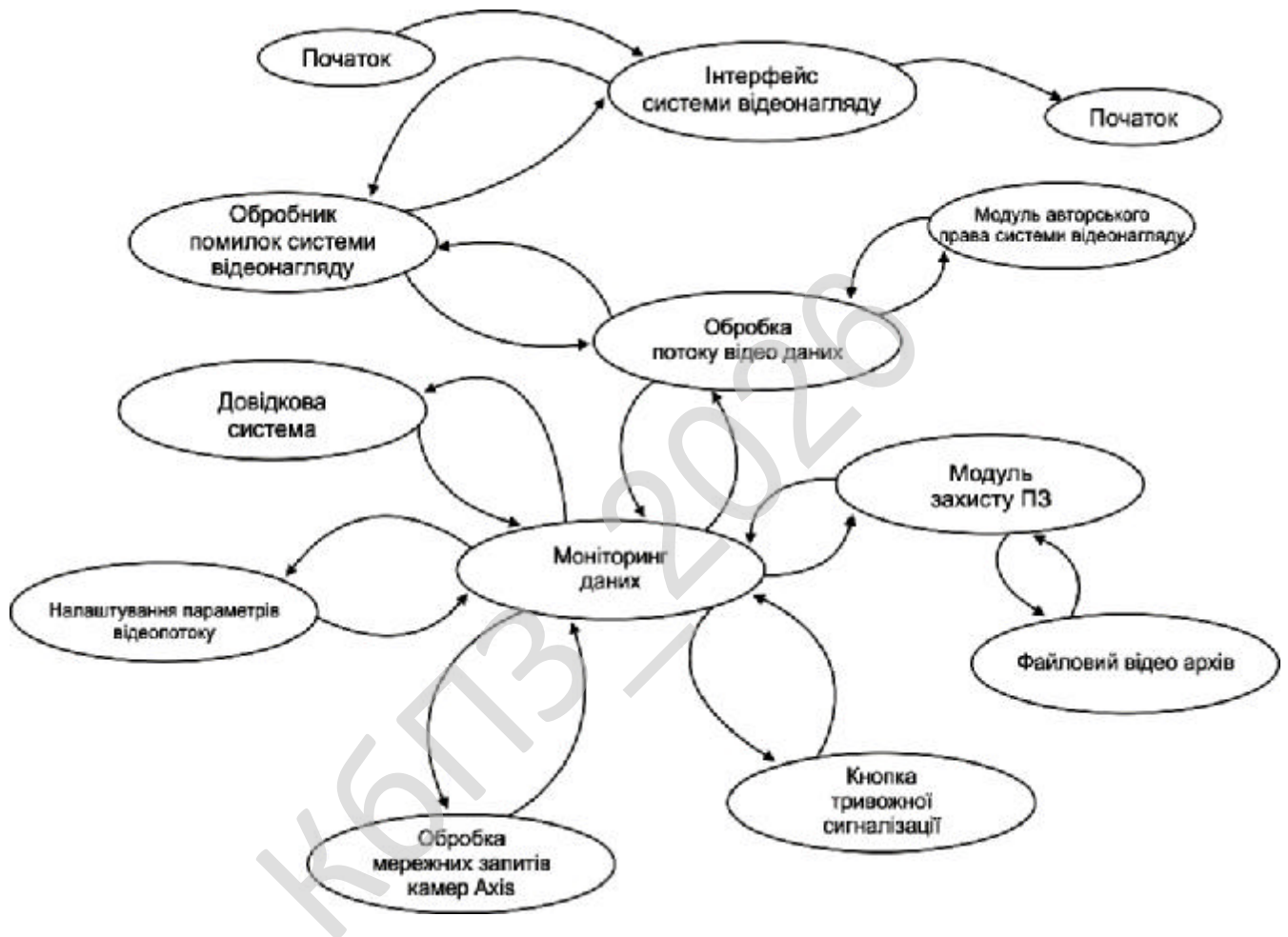


Рисунок 3.3 – Діаграма взаємодії процесів

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

Розглянемо реалізацію бакалаврської дипломної роботи. Були проведені розрахунки і підібрані набори тестових даних для перевірки правильності реалізації проектних рішень.

Було створено блок-схеми роботи системи. Перед їх розглядом необхідно провести роз'яснення який саме тип блок-схем використовується. Блок-схеми показують весь процес роботи системи з підсистемами та частково доказують правильність вибраних проектних рішень. 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 високого рівня декомпозиції задач на класи.

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 підсистеми 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.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		38

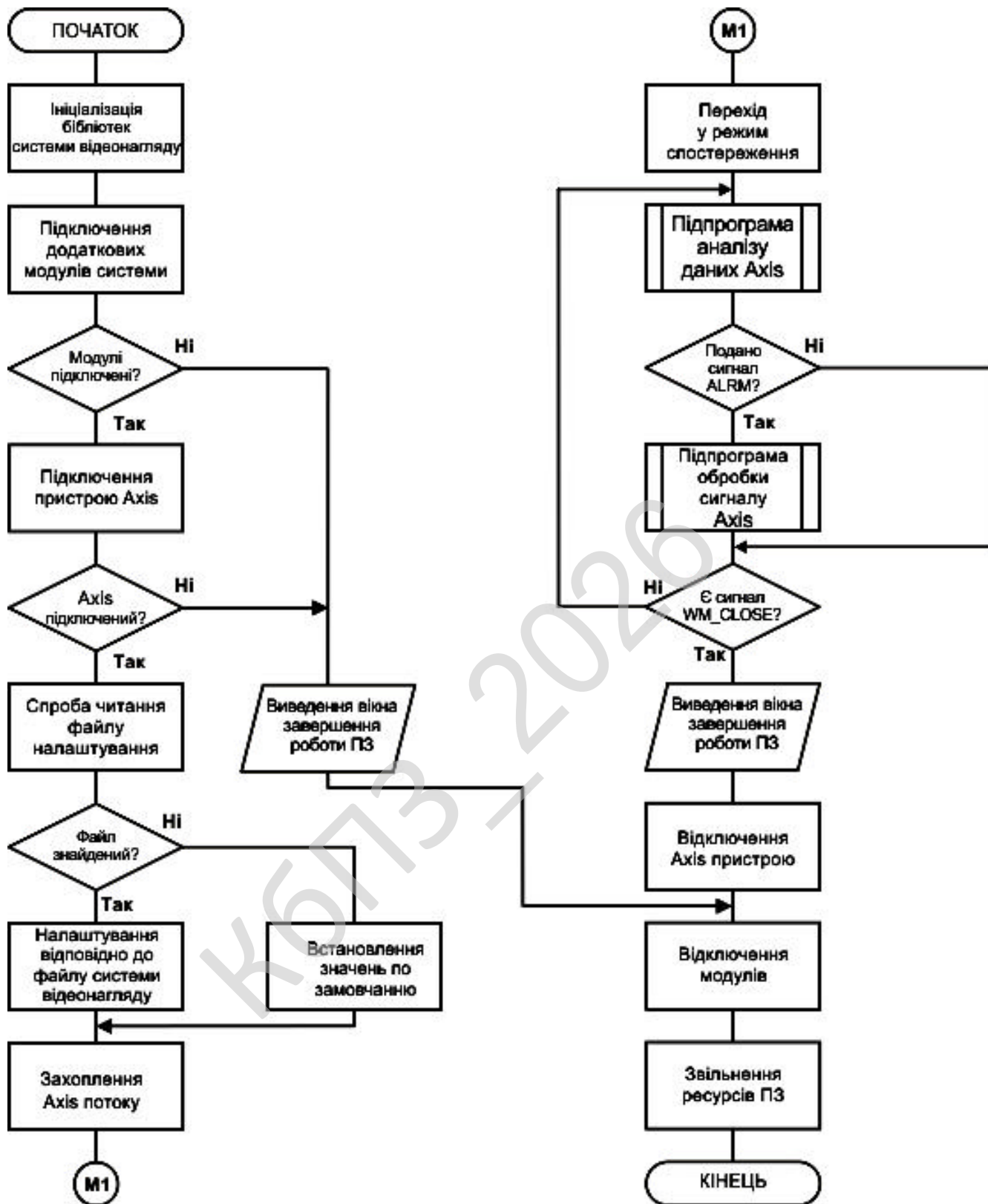


Рисунок 4.1 – Блок-схема основної програми

Архітектура клієнт-сервер є одним із архітектурних шаблонів програмного забезпечення та є домінуючою концепцією у створенні розподілених мережних програм і передбачає взаємодію та обмін даними між ними. Вона передбачає такі основні компоненти:

- набір серверів, які надають інформацію або інші послуги програмам, які звертаються до них;
- набір клієнтів, які використовують сервіси, що надаються серверами;
- мережа, яка забезпечує взаємодію між клієнтами та серверами.

Сервери є незалежними один від одного. Клієнти також функціонують паралельно і незалежно один від одного.

Немає жорсткої прив'язки клієнтів до серверів. Більш ніж типовою є ситуація, коли один сервер одночасно обробляє запити від різних клієнтів; з іншого боку, клієнт може звертатися то до одного сервера, то до іншого.

Клієнти мають знати про доступні сервери, але можуть не мати жодного уявлення про існування інших клієнтів.

Дуже важливо ясно уявляти, хто або що розглядається як «клієнт». Можна говорити про клієнтський комп'ютер, з якого відбувається звернення до інших комп'ютерів.

Можна говорити про клієнтське та серверне програмне забезпечення. Нарешті, можна говорити про людей, які бажають за допомогою відповідного програмного та апаратного забезпечення отримати доступ до тієї чи іншої інформації.

Загальноприйнятим є положення, що клієнти та сервери – це перш за все програмні модулі. Найчастіше вони знаходяться на різних комп'ютерах, але бувають ситуації, коли обидві програми – і клієнтська, і серверна, фізично розміщуються на одній машині; в такій ситуації сервер часто називається локальним.

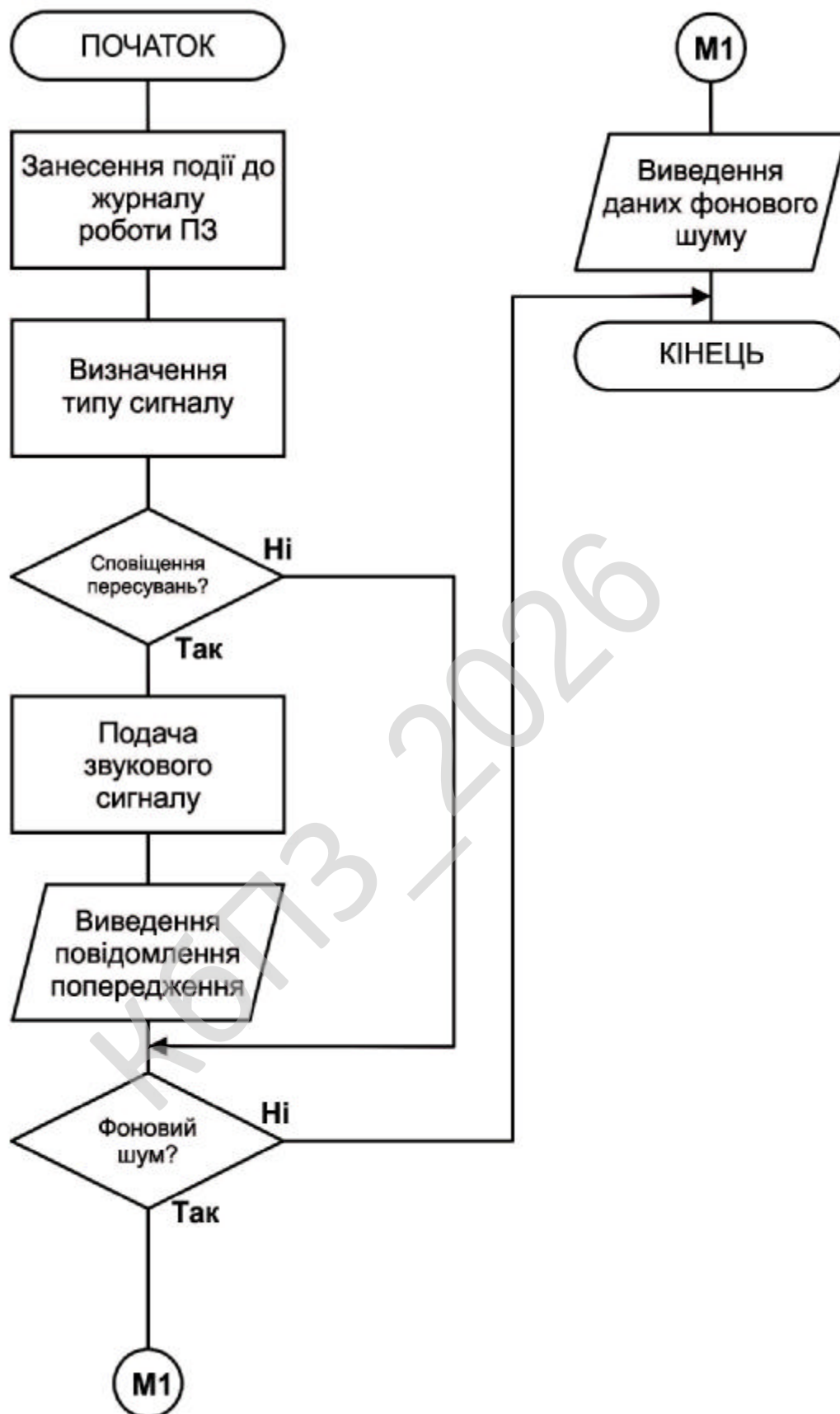


Рисунок 4.2 – Блок-схема роботи підпрограми

Модель клієнт-серверної взаємодії визначається перш за все розподілом обов'язків між клієнтом та сервером. Логічно можна відокремити три рівні операцій:

- рівень представлення даних, який по суті являє собою інтерфейс користувача і відповідає за представлення даних користувачеві і введення від нього керуючих команд;
- прикладний рівень, який реалізує основну логіку ПЗ і на якому здійснюється необхідна обробка інформації;
- рівень управління даними, який забезпечує зберігання даних та доступ до них.

Дворівнева клієнт-серверна архітектура передбачає взаємодію двох програмних модулів – клієнтського та серверного. В залежності від того, як між ними розподіляються наведені вище функції, розрізняють:

- модель тонкого клієнта, в рамках якої вся логіка ПЗ та управління даними зосереджена на сервері. Клієнтська програма забезпечує тільки функції рівня представлення;
- модель товстого клієнта, в якій сервер тільки керує даними, а обробка інформації та інтерфейс користувача зосереджені на стороні клієнта. Товстими клієнтами часто також називають пристрої з обмеженою потужністю: кишенькові комп'ютери, мобільні телефони та ін.

Типовим прикладом клієнт-серверної взаємодії є WWW. Існує величезна кількість веб-серверів, на яких розміщується та чи інша інформація. У найпростішому випадку ця інформація являє собою набір веб-сторінок, які можуть зберігатися на сервері у вигляді файлів, розмічених за допомогою мови розмітки HTML. Але ситуація, як правило, є складнішою; значна частина веб-ресурсів на сучасному етапі є динамічними, тобто вони не існують в заздалегідь підготовленому вигляді, а створюються безпосередньо в процесі обробки запиту від користувача.

Для того, щоб людина, яка працює в Інтернеті, могла переглянути ту чи іншу сторінку, на її комп'ютері повинно бути встановлено відповідне програмне забезпечення. Програми для перегляду веб-сторінок називаються браузером.

Але, крім браузерів, до серверів можуть звертатися і інші клієнти, а саме – автономні програми. Вони можуть передбачати взаємодію з людиною, а можуть працювати в цілком автоматичному режимі. Типовим класом таких програм є роботи, призначені для автоматичного перегляду веб-ресурсів. Зокрема, роботи є важливим елементом пошукових систем і використовуються ними для перегляду сторінок і збору інформації про них.

Для запиту до веб-сервера клієнтська програма повинна задати місцезнаходження комп'ютера, на якому розміщується серверна програма, назву потрібного документа і, можливо, інші дані, які специфікують запит. Мережа забезпечує знаходження сервера і передачу йому клієнтського запиту. Серверні програми обробляють цей запит, відповідь пересилається по мережі клієнтові.

Трирівнева клієнт-серверна архітектура, яка почала розвиватися з середини 90-х років, передбачає відділення прикладного рівня від управління даними. Відокремлюється окремий програмний рівень, на якому зосереджується прикладна логіка ПЗ. Програми проміжного рівня можуть функціонувати під управлінням спеціальних серверів ПЗ, але запуск таких програм може здійснюватися і під управлінням звичайного веб-сервера. Нарешті, управління даними здійснюється сервером даних.

Для роботи з системою користувач використовує стандартне програмне забезпечення – звичайний браузер. Це позбавляє його необхідності завантажувати та інсталиувати спеціальні програми (хоча інколи така необхідність все-таки виникає).

Але користувачеві слід надати в розпорядженні інтерфейс, який дозволяв би йому взаємодіяти з системою і формувати запити до неї. Форми, що визначають цей інтерфейс, розміщуються на веб-сторінках та завантажуються разом з ними.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		43

Веб-оглядач формує запит та пересилає його до сервера, який здійснює обробку. При необхідності сервер викликає серверні програмні модулі, які забезпечують обробку запиту і в разі потреби звертаються до сервера даних. Сервер даних здійснює операції з даними, що зберігаються в системі та складають її інформаційну основу. Зокрема, він може здійснити вибірку з інформаційної бази відповідно до запиту та передати її модулю проміжного рівня для подальшої обробки. Дані, з якими працює сервер даних, найчастіше організовані як реляційна база даних.

Найчастіше веб-сервер і серверні модулі проміжного рівня розміщуються на одному комп'ютері, хоч і являють собою окремі і логічно незалежні програмні модулі.

На сучасному етапі для програмування модулів проміжного рівня використовується мова серверних сценаріїв PHP, а для управління даними – СУБД MySQL. Таким чином, зв'язку PHP-MySQL слід розглядати як стандартний інструмент для створення порівняно простих інтерактивних веб-сайтів та систем електронної комерції; близько 90% комерційних систем сьогодні створюється саме на цій основі. Водночас як засоби управління даними, так і middleware-засоби можуть бути найрізноманітнішими. Так, для створення серверних програм, крім PHP, широко застосовуються Java, Perl, Python, Delphi.

Взагалі, технології створення розподілених, зокрема веб-програм, стрімко розвиваються. Слід згадати про технології EJB (Enterprise Java Beans), CORBA, а також про .NET – порівняно нову ініціативу компанії Microsoft. Для зберігання даних та їх передачі часто використовується так звана розширювана мова розмітки XML (Extensible Markup Language).

Розглянемо протокол SNMP (Simple Network Management Protocol, простий протокол керування мережею) – це протокол керування мережами зв'язку на основі архітектури TCP/IP.

На основі концепції TMN в 1980–1990 р. різними органами стандартизації був вироблений ряд протоколів керування мережами передачі даних з різним

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		44

спектром реалізації функцій TMN. До одного з типів таких протоколів керування належить Simple Network Management Protocol (SNMP).

SNMP – це технологія, покликана забезпечити керування й контроль за пристроями й програмами в мережі зв'язку шляхом обміну керуючою інформацією між агентами, що розташовуються на мережних пристроях, і менеджерами, розташованими на станціях керування. SNMP визначає мережу як сукупність мережних керуючих станцій й елементів мережі (головні машини, шлюзи й маршрутизатори, термінальні сервери), які спільно забезпечують адміністративні зв'язки між мережними керуючими станціями й мережними агентами. SNMP різних версій присвячений цілий ряд рекомендацій IETF (RFC).

Зазвичай при використанні SNMP присутні керовані та керуючі системи. До складу керованої системи входить компонент, який називається агентом, який відправляє звіти керуючій системі. По суті SNMP агенти передають управлінську інформацію на керуючі системи як змінні (такі як «вільна пам'ять», «ім'я системи», «кількість працюючих процесів» тощо).

Керуюча система може отримати достовірну інформацію через операції протоколу GET, GETNEXT і GETBULK. Агент може самостійно без запиту надсилати дані, використовуючи операцію протоколу TRAP або INFORM. Управляючі системи можуть також відправляти конфігураційні оновлення або контролюючі запити, використовуючи операцію SET для безпосереднього управління системою. Операції конфігурування та управління використовуються тільки тоді, коли потрібні зміни у мережній інфраструктурі. Операції моніторингу зазвичай виконуються на регулярній основі.

Змінні, доступні через SNMP, організовані в ієрархії. Ці ієрархії та інші метадані (такі як тип і опис змінної) описуються Базами Керуючої Інформації (Management Information Bases (MIBs)). SNMP не визначає, яку інформацію (які змінні) керована система повинна надавати. Навпаки, SNMP використовує розширювану модель, в якій доступна інформація визначається Базами Керуючої Інформації (MIB – Management Information Base).

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		45

Бази Керуючої Інформації описують структуру керуючої інформації пристроїв. Вони використовують ієрархічний адресний простір імен, що містить унікальний ідентифікатор об'єкта (object identifier (OID)).

Грубо кажучи, кожен унікальний ідентифікатор об'єкта ідентифікує змінну, яка може бути прочитана чи встановлена через SNMP. MIB'и використовують нотацію, визначену в ASN.1.

Ієрархія MIB може бути зображена як дерево з безіменним коренем, рівні якого приписані різними організаціями. На найвищому рівні MIB OID'и належать різним організаціям, що займаються стандартизацією, в той час як на нижчих рівнях OID'и виділяються асоційованими організаціями. Ця модель забезпечує управління на всіх шарах мережної моделі OSI, адже MIB'и можуть бути визначені для будь-яких типів даних і операцій.

Керований об'єкт – це одна з будь-якого числа характеристик, специфічних для керованого пристрою. Керований об'єкт включає в себе один або більше екземплярів об'єкта (що ідентифікуються за OID), які насправді є змінними.

Існує два типи керованих об'єктів: Скалярні об'єкти визначають єдиний екземпляр об'єкта; Табличні об'єкти визначають множинні, пов'язані екземпляри об'єктів які групуються в таблицях MIB.

Прикладом керованого об'єкта може бути atInput, який є скалярним об'єктом що містить єдиний екземпляр об'єкта, ціле число, яке показує загальну кількість вхідних пакетів AppleTalk на мережний інтерфейс маршрутизатора.

Ідентифікатор об'єкта (OID) унікально ідентифікує керований об'єкт в ієрархії MIB.

В телекомунікаціях і комп'ютерних мережах, ASN.1 є стандартною гнучкою нотацією для опису структур даних, що служать для кодування, передачі і декодування даних. ASN.1 являє собою набір правил для опису структури об'єктів, незалежних від специфічних для обладнання методик кодування, і формальну нотацію, яка дозволяє уникнути неоднозначностей.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		46

ASN.1 це єдиний ISO та ITU-T стандарт, спочатку визначений у 1984 році як частина стандарту CCITT X.409: 1984. Пізніше, в 1988 році, завдяки його широкому застосуванню, він був виділений в окремий стандарт X.208. Значно переглянута версія 1995 року описана в X.680.

Адаптована підмножина ASN.1 Структура Керуючої Інформації (SMI) описана в протоколі SNMP для визначення наборів пов'язаних MIB об'єктів, також званих MIB модулями.

SNMP працює на прикладному рівні TCP/IP (сьомий рівень моделі OSI). Агент SNMP отримує запити по UDP-порту 161. Менеджер може посилати запити з будь-якого доступного порту джерела на порт агента. Відповідь агента буде відправлений назад на порт джерела на менеджері. Менеджер отримує повідомлення (Traps і InformRequests) по порту 162. Агент може генерувати повідомлення з будь-якого доступного порту. При використанні TLS або DTLS запити виходять по порту 10161, а пастки відправляються на порт 10162.

У SNMPv1 зазначено п'ять основних протокольних одиниць обміну (protocol data units – PDU). Ще дві PDU, GetBulkRequest і InformRequest, були введені в SNMPv2 і перенесені в SNMPv3.

Нижче перераховані сім протокольних одиниць обміну SNMP:

1. GetRequest. Запит від менеджера до об'єкту для отримання значення змінної або списку змінних. Необхідні змінні вказуються в полі variable bindings (розділ поля values при цьому не використовується). Отримання значень зазначеної змінної повинно бути виконано агентом як Атомарна операція. Менеджеру буде повернений Response (відповідь) з поточними значеннями.

2. SetRequest. Запит від менеджера до об'єкту для зміни змінної або списку змінних. Зв'язані змінні вказуються в тілі запиту. Зміни всіх зазначених змінних повинні бути виконані агентом як атомарна операція. Менеджеру буде повернений Response з (поточними) новими значеннями змінних.

3. GetNextRequest. Запит від менеджера до об'єкту для виявлення доступних змінних і їх значень. Менеджеру буде повернений Response зі

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		47

зв'язаними змінними для змінної, яка є наступною в базі MIB в лексикографічному порядку. Обхід всієї бази MIB агента може бути проведений ітераційним використанням GetNextRequest, починаючи з OID 0. Рядки таблиці можуть бути прочитані, якщо вказати в запиті OID-и колонок в пов'язаних змінних.

4. GetBulkRequest. Покращена версія GetNextRequest. Запит від менеджера до об'єкту для численних ітерацій GetNextRequest. Менеджеру буде повернений Response з декількома пов'язаними змінними, обійденими починаючи зі пов'язаної змінної (змінних) в запиті. Специфічні для PDU поля non-repeaters і max-repetitions використовуються для контролю за поведінкою відповіді. GetBulkRequest був введений в SNMPv2.

5. Response. Повертає зв'язані змінні і значення від агента менеджеру для GetRequest, SetRequest, GetNextRequest, GetBulkRequest і InformRequest. Повідомлення про помилки забезпечуються полями статусу помилки і індексу помилки.

Ця одиниця використовується як відповідь і на Get-, і на Set-запити, в SNMPv1 називається GetResponse.

6. Trap. Асинхронне повідомлення від агента – менеджеру. Включає в себе поточне значення sysUpTime, OID, що визначає тип trap (пастки), і необов'язкові зв'язані змінні. Адресація одержувача для пасток визначається за допомогою змінних trap-конфігурації в базі MIB. Формат trap-повідомлення був змінений в SNMPv2 і PDU перейменували в SNMPv2-Trap.

7. InformRequest. Асинхронне повідомлення від менеджера менеджеру або від агента менеджеру. Повідомлення від менеджера менеджеру були можливі вже в SNMPv1 (за допомогою Trap), але SNMP зазвичай працює на протоколі UDP, в якому доставка повідомлень не гарантована, і не повідомляється про втрачені пакетах. InformRequest виправляє це зворотним відправленням підтвердження про отримання. Одержувач відповідає Response-му, що повторює всю інформацію з InformRequest. Цей PDU був введений в SNMPv2.

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.

Було використано наступні підходи UML: діаграма діяльності (діаграми поведінки типу); діаграма прецедентів (діаграми поведінки типу); Діаграма класів; Діаграма компонент; Діаграма об'єктів; Діаграма розгортання.

Діаграма класів це статичне представлення структури моделі. Відображає статичні (декларативні) елементи, такі як: класи, типи даних, їх зміст та відношення.

Діаграма класів, також, може містити позначення для пакетів та може містити позначення для вкладених пакетів. Також, діаграма класів може містити позначення деяких елементів поведінки, однак їх динаміка розкривається в інших типах діаграм.

Діаграма класів (class diagram) служить для представлення статичної структури моделі системи в термінології класів об'єктно-орієнтованого програмування. На цій діаграмі показують класи, інтерфейси, об'єкти й кооперації, а також їхні відносини.

В UML існують наступні типи зв'язків які використовуються у діаграмі класів: Асоціації; Агрегація; Композиція.

Асоціації це якщо між двома класами визначена асоціація, то можна переміщатися від об'єктів одного класу до об'єктів іншого. Цілком припустимі випадки, коли обидва кінці асоціації відносяться до одного і того ж класу. Це

означає, що з об'єктом деякого класу дозволено зв'язати інші об'єкти з того ж класу. Асоціація, що зв'язує два класи, називається бінарної. Можна, хоча це рідко буває необхідним, створювати асоціації, що зв'язують відразу кілька класів. Графічно асоціація зображується у вигляді лінії, що з'єднує клас сам з собою або з іншими класами.

Асоціації може бути присвоєно ім'я, яке описує природу відносини. Зазвичай ім'я асоціації не вказується, якщо тільки ви не хочете явно задати для неї рольові імена або у вашій моделі настільки багато асоціацій, що виникає необхідність посылатися на них і відрізняти один від одного. Ім'я буде особливо корисним, якщо між одними і тими ж класами існує кілька різних асоціацій.

Клас, що бере участь в асоціації, грає в ній деяку роль. По суті, це "обличчя", яким клас, що знаходиться на одній стороні асоціації, звернений до класу з іншого її боку. Можна явно позначити роль, яку клас грає в асоціації.

Часто при моделюванні буває важливо вказати, скільки об'єктів може бути пов'язано допомогою одного примірника асоціації. Це число називається кратністю (Multiplicity) ролі асоціації та записується або як вираз, значенням якого є діапазон значень, або в явному вигляді.

Вказуючи кратність на одному кінці асоціації, ви тим самим говорите, що на цьому кінці саме стільки об'єктів повинно відповідати кожному об'єкту на протилежному кінці. Кратність можна задати рівною одиниці (1), можна вказати діапазон: "нуль або одиниця" (0..1), "багато" (0 .. *), "одиниця або більше" (1 .. *). Дозволяється також вказувати певне число (наприклад, 3). За допомогою списку можна задати і більш складні кратності, наприклад 0. . 1, 3..4, 6 .. *, що означає "будь-яке число об'єктів, крім 2 і 5".

Агрегація це проста асоціація між двома класами відображає структурний відношення між рівноправними сутностями, коли обидва класу знаходяться на одному концептуальному рівні і ні один не є більш важливим, ніж інший. Але іноді доводиться моделювати відношення типу «частина/ціле», в якому один з класів має більш високий ранг (ціле) і складається з декількох менших за рангом

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		50

(частин). Ставлення такого типу називають агрегацією; воно зараховане до відносин типу «має» (з урахуванням того, що об'єкт-ціле має кілька об'єктів-частин). Агрегація є окремим випадком асоціації і зображується у вигляді простої асоціації з незафарбованим ромбом з боку «цілого». Графічно агрегація представляється порожнім ромбом на блоці класу, і лінією, яка від цього ромба до міститься класу.

Композиція це більш суворий варіант агрегації. Відома також як агрегація за значенням.

Композиція має жорстку залежність часу існування екземплярів класу контейнера та примірників містяться класів. Якщо контейнер буде знищений, то весь його вміст буде також знищено. Графічно представляється як і агрегація, але з зафарбовани ромбиком.

Опис системи

Програмне забезпечення системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis працює як локальний Python застосунок для контролю камер, перевірки їх доступності, фіксації подій безпеки та формування журналу інцидентів.

Система отримує дані від IP камер Axis, перевіряє стан підключення, контролює зміну кадру, зберігає інформацію про підозрілі події та показує адміністратору поточний стан відеомережі кафе. Основна мета системи полягає у своєчасному виявленні недоступності камери, втрати зображення, зміни адреси пристрою або появи критичних подій.

Система складається з модуля камер, модуля перевірки доступності, модуля аналізу кадру, модуля журналювання, модуля звітів та модуля адміністрування. Дані зберігаються у SQLite базі. Python застосунок виконує регулярний моніторинг камер і записує результати перевірок у базу.

Розглянемо основні функції у вихідному коді, а саме:

- Реєстрація камер Axis у локальній базі даних;
- Перевірка доступності камери за IP адресою;

- Отримання контрольного кадру з камери;
- Виявлення втрати відеосигналу;
- Фіксація подій безпеки;
- Формування журналу роботи системи;
- Перегляд стану всіх камер кафе.

```
import sqlite3
import hashlib
import requests
from datetime import datetime
from pathlib import Path
DB_PATH = Path("axis_cafe_security.db")
```

#Створення бази даних системи відеонагляду

```
def init_database():
    with sqlite3.connect(DB_PATH) as connection:
        cursor = connection.cursor()
        cursor.execute("""
            CREATE TABLE IF NOT EXISTS cameras (
                id INTEGER PRIMARY KEY AUTOINCREMENT,
                name TEXT NOT NULL,
                ip_address TEXT NOT NULL UNIQUE,
                location TEXT NOT NULL,
                snapshot_url TEXT NOT NULL,
                username TEXT NOT NULL,
                password TEXT NOT NULL,
                is_active INTEGER DEFAULT 1
            )
        """)
        cursor.execute("""
            CREATE TABLE IF NOT EXISTS security_events (
                id INTEGER PRIMARY KEY AUTOINCREMENT,
                camera_id INTEGER,
                event_type TEXT NOT NULL,
                event_message TEXT NOT NULL,
                created_at TEXT NOT NULL,
                FOREIGN KEY(camera_id) REFERENCES cameras(id)
            )
        """)
        cursor.execute("""
            CREATE TABLE IF NOT EXISTS camera_checks (
                id INTEGER PRIMARY KEY AUTOINCREMENT,
```

```

        camera_id INTEGER,
        status TEXT NOT NULL,
        frame_hash TEXT,
        checked_at TEXT NOT NULL,
        FOREIGN KEY(camera_id) REFERENCES cameras(id)
    )
    """
    connection.commit()

#Додавання камери Axis до системи
def add_camera(name, ip_address, location, snapshot_url, username,
password):
    with sqlite3.connect(DB_PATH) as connection:
        cursor = connection.cursor()
        try:
            cursor.execute("""
                INSERT INTO cameras
                (name, ip_address, location, snapshot_url, username, password)
                VALUES (?, ?, ?, ?, ?, ?)
            """, (name, ip_address, location, snapshot_url, username, password))
            connection.commit()
            return True
        except sqlite3.IntegrityError:
            return False

#Запис події кібербезпеки
def log_security_event(camera_id, event_type, event_message):
    with sqlite3.connect(DB_PATH) as connection:
        cursor = connection.cursor()
        cursor.execute("""
            INSERT INTO security_events
            (camera_id, event_type, event_message, created_at)
            VALUES (?, ?, ?, ?)
        """, (camera_id, event_type, event_message, datetime.now().isoformat()))
        connection.commit()

#Отримання кадру з камери Axis
def get_camera_snapshot(camera):
    try:
        response = requests.get(
            camera["snapshot_url"],
            auth=(camera["username"], camera["password"]),
            timeout=5
        )
        if response.status_code == 200 and len(response.content) > 1000:

```

```

        return response.content
    return None
except requests.RequestException:
    return None

#Обчислення цифрового відбитка кадру
def calculate_frame_hash(frame_data):
    return hashlib.sha256(frame_data).hexdigest()

#Збереження результату перевірки камери
def save_camera_check(camera_id, status, frame_hash=None):
    with sqlite3.connect(DB_PATH) as connection:
        cursor = connection.cursor()
        cursor.execute("""
            INSERT INTO camera_checks
            (camera_id, status, frame_hash, checked_at)
            VALUES (?, ?, ?, ?)
            """, (camera_id, status, frame_hash, datetime.now().isoformat()))
        connection.commit()

#Отримання списку активних камер
def get_active_cameras():
    with sqlite3.connect(DB_PATH) as connection:
        connection.row_factory = sqlite3.Row
        cursor = connection.cursor()
        cursor.execute("""
            SELECT * FROM cameras
            WHERE is_active = 1
            """)
        return [dict(row) for row in cursor.fetchall()]

#Моніторинг камер кафе
def monitor_cameras():
    cameras = get_active_cameras()
    for camera in cameras:
        frame_data = get_camera_snapshot(camera)
        if frame_data is None:
            save_camera_check(camera["id"], "Недоступна")
            log_security_event(
                camera["id"],
                "Втрата доступу",
                f"Камера {camera['name']} у зоні {camera['location']} не відповідає"
            )
            continue
        frame_hash = calculate_frame_hash(frame_data)
        save_camera_check(camera["id"], "Активна", frame_hash)

```

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		54

```

        print(
            f"Камера {camera['name']} працює. "
            f"Локація {camera['location']}. "
            f"Контрольний хеш {frame_hash[:12]}"
        )
#Формування короткого звіту про стан камер
def show_security_report():
    with sqlite3.connect(DB_PATH) as connection:
        cursor = connection.cursor()
        cursor.execute("""
            SELECT cameras.name, cameras.location, camera_checks.status,
camera_checks.checked_at
            FROM camera_checks
            JOIN cameras ON cameras.id = camera_checks.camera_id
            WHERE camera_checks.id IN (
                SELECT MAX(id)
                FROM camera_checks
                GROUP BY camera_id
            )
            ORDER BY cameras.location
        """)
        rows = cursor.fetchall()
        print("Поточний стан камер кафе")
        for row in rows:
            print(f"{row[0]} | {row[1]} | {row[2]} | {row[3]}")
#Головна логіка роботи системи
def main():
    init_database()
    add_camera(
        "Axis Entrance",
        "192.168.1.20",
        "Вхідна зона",
        "http://192.168.1.20/axis-cgi/jpg/image.cgi",
        "admin",
        "secure_password"
    )
    add_camera(
        "Axis Hall",
        "192.168.1.21",
        "Зал кафе",
        "http://192.168.1.21/axis-cgi/jpg/image.cgi",
        "admin",

```

```

        "secure_password"
    )
    monitor_cameras()
    show_security_report()
if __name__ == "__main__":
    main()

```

4.2 Захист розробленого програмного забезпечення

Дані які використовуються у даній роботі захищаються алгоритмом ДСТУ 7624:2014 («Калина»). При розробці національного стандарту ДСТУ 7624:2014 (блоковий шифр «Калина» і режими його роботи) було ухвалене рішення забезпечити прозорість проектування й використовувати консервативний підхід із застосуванням добре досліджених конструкцій, що забезпечують запас стійкості для безпечного застосування алгоритму в умовах істотного прогресу криптоаналітичних технік і засобів обробки даних.

Національний стандарт підтримує розмір блоку й довжину ключа шифрування 128, 256 і 512 біт (довжина ключа дорівнює розміру блоку або у два рази перевищує його), забезпечуючи нормальний, високий і надвисокий рівень стійкості (зараз це єдиний у світі стандарт блокового шифрування, що підтримує 512-бітові симетричні ключі). Різні варіанти забезпечують гнучкість вибору параметрів для розроблювачів систем криптографічного захисту, що дозволяє одержати як найвищий рівень швидкодії, так і найбільший запас стійкості перетворення.

Високорівнева конструкція використовує добре досліджену Square-подібну SPN-структуру, застосовувану в алгоритмах AES/Rijndael, Whirlpool, «Стрибог», «Коник» і багатьох інших. Циклове перетворення побудоване на базі таблиць підстановки (S-блоків) і множення на МДР-матрицю над кінцевим полем, забезпечуючи необхідні криптографічні властивості. Застосування саме такої конструкції дозволяє забезпечити доказову стійкість до диференціального, лінійному й ін. видам криптоаналізу, одночасно забезпечуючи ефективну

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		56

реалізацію на широкому спектрі програмних і програмно-апаратних платформ. При виборі розміру МДР-матриці був прийнятий в увагу розмір кешу L1 сучасних і перспективних процесорів, що дозволило оптимізувати швидкодія програмної реалізації шифру.

Альтернативний варіант, який розглядався при розробці циклової функції, – ARX перетворення (Addition-rotation-xor). Цей підхід реалізований у шифрі SPECK (розроблений Агентством національної безпеки США й переданий у відкритий доступ), у блокових алгоритмах, на основі яких побудовано сімейство геш-функцій SHA-0,1,2 і ін. Перевагою походу є компактність і швидкодія перетворення. Але, у той же час, є й істотний недолік, пов'язаний з відсутністю методів, що дозволяють виконати строге аналітичне обґрунтування криптографічної стійкості таких розв'язків. Навіть із наймогутнішими у світі можливостями для аналізу, США кілька раз були змушено модифікувати свої стандарти гешування через знайдені уразливості: з 1993 по 1995 рр. діяв SHA-0, з 1995 по 2001 рр. застосовувався SHA-1, з тих пор використовується SHA-2. Через питання, що піднімаються, до стійкості й цієї версії, у США з 2008 по 2012 рр. був проведений міжнародний конкурс SHA-3. До теперішнього часу розроблений проект стандарту FIPS 202, що описує нову криптографічну геш-функцію.

Таким чином, консервативний і прозорий підхід до проектування нового національного стандарту України обумовив вибір добре перевіреної конструкції на базі S-блоків і лінійного перетворення, для якої можливо забезпечити доказову стійкість до різних видів криптоаналізу. При порівнянні характеристик S-блоків і інших симетричних перетворень можна відзначити, що саме національний стандарт України забезпечує найбільшу нелінійність булевих функцій, що дає додатковий запас стійкості до лінійного криптоаналізу. Ще більше значення нелінійності для взаємо-однозначної підстановки можна забезпечити, застосовуючи, наприклад, афінно-тквівалентні статечні функції в кінцевому полі, але такі перетворення, використані в AES, Camellia і ін. алгоритмах, ставлять шифр під погрозу реалізації алгебраїчної атаки (цей метод

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		57

криптоаналізу був успішно застосований проти шифру Keeloq, використовуваного в системах автомобільної безпеки).

У якості схеми розгортання ключів була запропонована нова конструкція з наступними властивостями:

- забезпечення криптографічної стійкості до відомих методів аналізу, відсутність «слабких» ключів, які можуть погіршити властивості перетворення;
- зручність програмної й програмно-апаратної реалізації (для формування циклових ключів застосовуються тільки операції, використовувані при шифруванні);
- висока обчислювальна складність відновлення ключа шифрування по одному або декільком цикловим ключам.

Остання властивість забезпечує додатковий захист до атак на реалізацію, коли зловмисник намагається атакувати інженерні розв'язки (вимірюючи споживаний пристроєм струм, навмисне викликаючи збої в роботі через навмисний перегрів шифратора та ін.). Ця особливість є істотною перевагою для ряду додатків, зокрема, при реалізації шифрування на смарт-картах, USB-токенах та ін., коли ключ прошитий у пристрої й повинен бути захищений від зовнішнього доступу (наприклад, у модулях доступу до платних цифрових ТБ-каналів і ін.). Кількість циклів шифрування залежить від довжини ключа: 10 циклів для 128-бітового, 14 циклів для 256-бітового й 18 циклів для 512-бітового ключа шифрування. У порівнянні з іншими алгоритмами на основі Square-подібної SPN-структури, блоковий шифр «Калина» має наступні істотні конструктивні відмінності:

- початкове й кінцеве забілювання з використанням модульного додавання (264) для підвищення складності криптоаналітичних атак;
- застосування чотирьох різних S-блоків (замість одного) із властивостями для захисту від алгебраїчних атак, і при порівнянні характеристик з іншими блоковими й потоковими шифрами забезпечують найбільшу нелінійність булевих функцій (104), що дає додатковий запас стійкості перетворення;

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		58

– збільшений розмір МДР-перетворення, що поліпшує криптографічні властивості й дозволяє оптимізувати швидкодія на сучасних 64-бітових платформах;

– нову односпрямовану схему формування циклових ключів, що забезпечує захист від атак, ефективність програмної й програмно-апаратної реалізації, разом з додатковою стійкістю до методів аналізу спеціального виду.

Оцінка криптографічної стійкості до диференціального, лінійного, алгебраїчного, інтегрального й інших методам аналізу (практичний критерій) показала, що шифр є стійким при 6 циклах для 128-бітового блоку, 7 циклах для 256-бітового й 9 циклах для 512-бітового (кожний додатковий цикл забезпечує експонентний ріст складності криптоаналізу). Таким чином, шифр, що містить 10, 14 і 18 циклів для блоку 128, 256 і 512 біт відповідно, забезпечує захист від розглянутих видів аналізу й має істотний запас стійкості. Крім блокового шифру, ДСТУ 7624:2014 визначає режими роботи, що відповідають як ISO 10116:2006, так і додаткові, призначені для сучасних систем криптографічного захисту IP-трафіка, прозорого шифрування носіїв інформації й ін. У стандарті визначені обсяги повідомлень, після обробки яких потрібна обов'язкова зміна ключа. Крім того, приводяться рекомендації розроблювачам, що обертають увагу на необхідність запобігання атак з використанням особливостей реалізації засобів шифрування. Зокрема, враховані особливості, що дозволяли організацію атак BEAST і CRIME/BREACH у протоколах SSL/TLS, повторне приймання повідомлення, відновлення конфіденційних параметрів на основі залежності часу шифрування від оброблюваних даних (через промахи кешу при табличній реалізації) і ін.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку зображено розроблене у бакалаврської дипломної роботі програмне забезпечення системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи:

- Функціональних кнопок ПЗ.
- Верхнього меню: Файл; Сповіщення; Камери; Вікна; Розробник.
- Розділу виведення відеоряду – результату роботи системи.

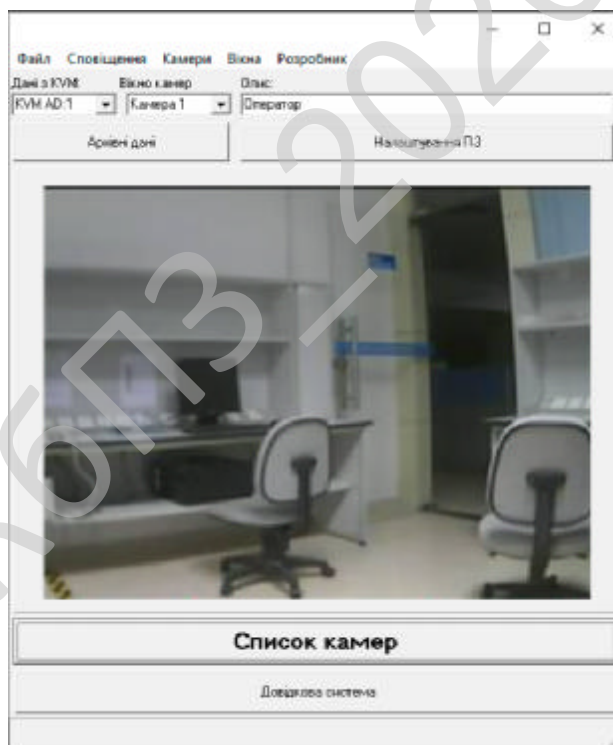


Рисунок 5.1 – Головне вікно ПЗ

Розроблена програма має дуже простий і 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.

Вибір камер визначався умовами на конкретному об'єкті. Над касою встановлювалися камери з вузьким кутом огляду, а для одержання загального виду залу – пристрою із широким сектором огляду. Усього використовувалося п'ять різних моделей компактних купольних камер серії AXIS M30: Axis M 3024-LVE, Axis M 3005-V, Axis M 3006-V, Axis M 3215-V; Axis P 3224-LV. У кафе, що перебуває біля басейну, була встановлена модульна камера Axis F34 з виносними блоками (чотири блоки підключені до однієї бази для моніторингу різних зон). Спостереження за складом, у тому числі в темний час доби, здійснювалося за допомогою камери Axis M 1145-L з убудованим світлодіодним ІЧ-підсвічуванням.

На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення.

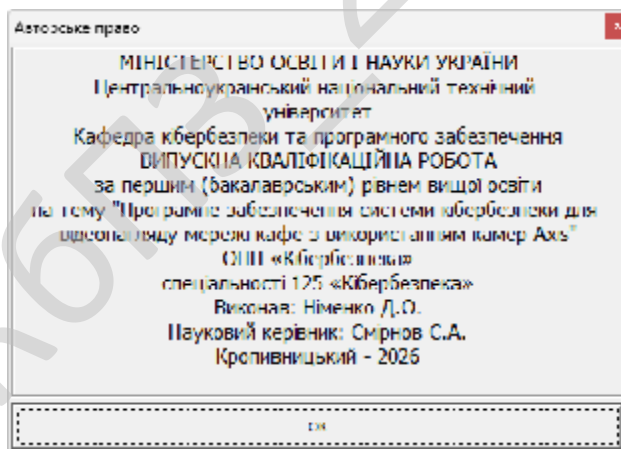


Рисунок 5.2 – Авторське право

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

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		61

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.
- Оновлення.
- 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;

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		62

– 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 форматом білої скриньки засноване на аналізі керуючої структури програми. Програма вважається повністю перевіреною, якщо проведено вичерпне тестування маршрутів (шляхів) її графа управління.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		63

У цьому випадку формуються тестові варіанти, в яких:

- Гарантується перевірка всіх незалежних маршрутів програми.
- Знаходяться гілки True, False для всіх логічних рішень.
- Виконуються всі цикли (у межах їхніх кордонів та діапазонів).
- Аналізується правильність внутрішніх структур даних.

Недоліки тестування "білої скриньки":

- Кількість незалежних маршрутів може бути дуже велика.
- Повне тестування маршрутів не гарантує відповідності програми вихідним вимогам до неї.

- У програмі можуть бути пропущені деякі маршрути.
- Не можна виявити помилки, поява яких залежить від даних.

Переваги тестування "білої скриньки" пов'язані з тим, що принцип «білої скриньки» дозволяє врахувати особливості програмних помилок:

- Кількість помилок мінімально в «центрі» і максимально на «периферії» програми.
- Попередні припущення про ймовірність потоку керування або даних у програмі часто бувають некоректними. У результаті типовим може стати маршрут, модель обчислень за яким опрацьована слабо.
- При записі алгоритму програмного забезпечення у вигляді тексту на мові програмування можливе внесення типових помилок трансляції (синтаксичних та семантичних).
- Деякі результати в програмі залежать не від вихідних даних, а від внутрішніх станів програми.

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.

К6ПЗ-2026

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		65

6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis.

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

Рішення завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем для відеонагляду мережі кафе з використанням камер Axis.
- Досліджена система для відеонагляду мережі кафе з використанням камер Axis.
- На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання для відеонагляду мережі кафе з використанням камер Axis.

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 створенні 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 призначені для системи кібербезпеки для відеонагляду мережі кафе з використанням камер Axis.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		66

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 кібербезпеки 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 ДСТУ 7624:2014.

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.

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ док.ум.	Підпис	Дата		67

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ranjan Parekh. Fundamentals of Image, Audio, and Video Processing Using MATLAB® With Applications to Pattern Recognition. CRC Press. 2021. 406 p.
2. Alasdair McAndrew. A Computational Introduction to Digital Image Processing. Chapman & Hall. 2021. 560 p.
3. Михайло Пічугін, Іван Канкін, Володимир Воротніков Комп'ютерна графіка. Навчальний посібник / Центр навчальної літератури 346 с. 2019р.
4. Маценко В.Г. Комп'ютерна графіка: Навчальний посібник. – Чернівці: Рута, 2009 – 343 с.
5. Інженерна комп'ютерна графіка: підручник / В.В. Проців [та ін.] / М-во освіти і науки України, Нац. гірн. унт-т. – Дніпро: НГУ, 2017. – 247 с.
6. Проців В.В. Прикладна комп'ютерна графіка [Текст]: Навч. посібник / В.В. Проців, К.А. Зіборов, К.М. Бас, Г.К. Ванжа; М-во освіти і наук, Нац. гірн. ун-т. - Д.: НГУ, 2016. - 187 с.
7. Kopf, Johannes and Lischinski, Dani. Depixelizing Pixel Art (англ.) // ACM Trans. Graph. – 2011. – Vol. 30, no. 4. – P. 99:1--99:8.
8. Giachetti, Andrea and Asuni, Nicola. Real-Time Artifact-Free Image Upscaling (англ.) // Trans. Img. Proc.. – 2011. – Vol. 20, no. 10. – P. 2760—2768.
9. 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.
10. 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

11. Смірнова Т.В., Коноплицька-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.
12. 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.
13. 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.
14. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchев, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.
15. 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.
16. 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.
17. 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,
18. 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.

19. 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>

20. 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.

21. 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.

22. 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.

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

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. Zhurakovskiy, 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.

33. Smirnov O. Kuznetsov A., Zaichenko 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

41. 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.

42. Т.В. Смірнова, О.М. Дреєв, 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.

43. 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.

44. 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.

45. Смірнов О.А., Дреєва Г.М., Дреєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральнотураїнський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.

46. 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.

47. Смірнов О.А., Коноплицька-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.

48. 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).

49. Смірнов О.А., Дреєва 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

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

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

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

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

54. Смірнов О.А., Дреєв 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

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

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		74

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

57. Смірнов О.А., Дреєв О.М., Дорєнський 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.

58. Смірнов О.А., Дорєнський О.П., Дреєв О.М. Аналіз процесів стиснення та відновлення зображень на основі цифрових методів. Наука і техніка Повітряних сил Збройних Сил України. – Випуск 3(12). – Х.: ХУПС. – 2013. – С.122-127.

59. Смірнов О.А., Мелешко Є.В., Семенов С.Г. Методи та засоби обробки сигналів і даних в інформаційних системах. Навчальний посібник. – Кіровоград: КНТУ 2012. – 250 с.

60. Смірнов О.А., Євсєєв С.П., Жукарев В.Ю., Король О.Г., Сорокін В.Є., Мелешко Є.В. Технології і стандарти комп'ютерних мереж. – Кіровоград: КНТУ 2012. – 454 с

					ВКРБ-125.26.0036.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		75