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 другим (магістерським) рівнем вищої освіти
на тему
“Дослідження та програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis”

Виконав здобувач вищої освіти
II курсу, групи КІ-25М
ОПП «Комп’ютерна інженерія»
спеціальності F7 «Комп’ютерна інженерія»
_____ Дьяченко Р.В.
«____» _____ 2026 р.

Керівник проекту
доктор технічних наук, професор
_____ Коваленко О.В.
«____» _____ 2026 р.

Нормоконтроль проекту
_____ Коваленко А.С.
«____» _____ 2026 р.

Рецензент _____
_____

Підписано КЕП
Центральноукраїнський національний технічний університет
ДЬЯЧЕНКО РОМАН ВОЛОДИМИРОВИЧ
Сертифікат: 21E4B79083A82E7F0400000035F430019B411C08
Дійсний з 29.10.2026 20:22:41 по 30.10.2027 01:59:59

Центральноукраїнський національний технічний університет

Факультет *Механіко-технологічний*

Кафедра *Кібербезпеки та програмного забезпечення*

Рівень вищої освіти *магістр*

Галузь знань _F_____*"Інформаційні технології"*_____

Спеціальність F7 *"Комп'ютерна інженерія"*

Освітньо-професійна (освітньо-наукова) програма _*"Комп'ютерна інженерія"*_

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

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ДРУГИМ (МАГІСТЕРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Дьяченку Роману Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження та програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis*

2. Керівник роботи *Коваленко Олександр Володимирович, доктор технічних наук, професор*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 41-13 від 17.08.2026 року

3. Строк подання студентом роботи до захисту *2.12.2026 р.*

4. Мета та завдання випускної кваліфікаційної роботи*: Метою розробки є дослідження та програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis*

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

1. Призначення та область використання.	*5. Впровадження системи в промислову експлуатацію*
2. Перегляд аналогічних існуючих систем.	*6. Наукова новизна.*
3. Опис і обґрунтування проектних рішень.	*7. Заходи з охорони праці та техніки безпеки.*
4. Етапи програмування системи.	*8. Висновки.*

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

Наукова новизна	*1 аркуш*
Структурна схема системи	*1 аркуш*
Функціональна схема системи	*1 аркуш*
Діаграма процесів	*1 аркуш*
Блок-схема алгоритму роботи додатку	*2 аркуша*

7. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Марченко К.М., к.т.н., доцент	06.10.2026	16.11.2026

8. Дата видачі завдання « 1 » вересня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем	10.10.2026 р.	
2.	Постановка задачі, оформлення ТЗ	15.10.2026 р.	
3.	Розробка моделі компонента	20.10.2026 р.	
4.	Розробка структур даних	25.10.2026 р.	
5.	Розробка алгоритмів системи	30.10.2026 р.	
6.	Програмування алгоритмів	10.11.2026 р.	
7.	Розрахунки з охорони праці та техніки безпеки	15.11.2026 р.	
8.	Оформлення ПЗ	17.11.2026 р.	
9.	Попередній захист роботи	2.12.2026 р.	

Дата видачі завдання
« 1 » вересня 2026 р.

Підпис керівника

_____ _____
(прізвище та ініціали)

Завдання прийнято до виконання
« 1 » вересня 2026 р.

Підпис здобувача

_____ _____
(прізвище та ініціали)

АНОТАЦІЯ

Дьяченко Р.В. Дослідження та програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis. F7 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Метою розробки є дослідження та програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Об'єктом дослідження є процес мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Предметом дослідження є методи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Методи дослідження базуються на методах Інтернету речей, методах комп'ютерних мереж, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

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

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

Програму розроблено в середовищі Python.

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

ABSTRACT

Diachenko R.V. Research and software implementation of a network security system for IoT infrastructures based on open APIs and Axis technologies. F7 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

This master's-level graduation thesis involves the development of software designed for a network security system for IoT infrastructures based on open APIs and Axis technologies.

The objective of the project is to research and implement a network security system for IoT infrastructures using open APIs and Axis technologies.

The object of the study is the network security process for IoT infrastructures based on open APIs and Axis technologies.

The subject of the study comprises network security methods for IoT infrastructures based on open APIs and Axis technologies.

The research methodology incorporates approaches from the fields of the Internet of Things, computer networking, information security, mathematical statistics, and software development.

The outcome of the work is the software implementation of a network security system for IoT infrastructures based on open APIs and Axis technologies.

During the development of the software model, an analysis of existing hardware and software tools was conducted. All components of the developed software are described in detail.

A user-friendly interface has been developed, and instructions for using the software tools are provided.

The program is designed to run on PCs with Windows 10/11 operating systems.

The program was developed using the Python environment.

Keywords: computer engineering, network security, IoT, API, Axis

ВІДОМІСТЬ ПРОЕКТУ

		Текстові документи			
1	А4	Пояснювальна записка	83	–	
2	А4	Робоча програма	34	–	Додаток А
		Графічні документи			
3	А4	Наукова новизна	1	–	
4	А4	Структурна схема	1	–	
5	А4	Функціональна схема роботи системи	1	–	
6	А4	Діаграма взаємодії процесів	1	–	
7	А4	Блок-схема основної програми	1	–	
8	А4	Блок-схема роботи підпрограми	1	–	

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ 9
ВСТУП..... 10
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ 12
1.1 Призначення системи..... 12
1.2 Область застосування 12
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ 15
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти..... 15
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування 23
2.3 Розгорнута постановка завдання 25
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ 27
3.1 Опис функціонування системи 27
3.2 Розробка структурної схеми..... 36
3.3 Розробка функціональної схеми 42
3.4 Розробка діаграми процесів 44
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ 46
4.1 Розробка блок-схем та опис алгоритмів функціонування системи 46
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ..... 57
6 НАУКОВА НОВИЗНА 62

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ 63
7.1 Вступ 63
7.2 Шкідливі і небезпечні фактори при роботі з комп’ютером 65
7.3 Аналіз санітарно-гігієнічних умов праці на робочому місці програміста ... 66
7.4 Розробка заходів з умов поліпшення охорони праці 69
7.5 Розрахункова частина 70
8 ОСНОВНІ ВИСНОВКИ 74
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 76

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

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

ВСТУП

Актуальність теми. Камера Axis – це професійні IP-камери безпеки (мережеві), призначені для захоплення, обробки та передачі цифрового відео через IP-мережу. Хоча багато брендів сьогодні пропонують IP-камери, рішення Axis зазвичай позиціонуються для забезпечення безпеки корпоративного рівня, де якість зображення, надійність, довгострокова ремонтопридатність та кібербезпека є важливими вимогами. Іншими словами, камери Axis – це не просто пристрої запису; за умови правильного проектування та інтеграції вони стають інтелектуальними інструментами, які допомагають виявляти інциденти раніше, оптимізувати операції безпеки та підтримувати розслідування після подій.

Висока продуктивність IP-відео досягається завдяки поєднанню правильного розміщення камер, вибору об'єктивів, планування пропускної здатності та бітрейту, архітектури запису та інтеграції програмного забезпечення для керування відео (VMS). Такий системний інженерний підхід перетворює «камери на стіні» на безпечну, масштабовану та керовану платформу безпеки.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

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

– Огляд існуючих систем мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

– Дослідження системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

– Програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Об'єктом дослідження є процес мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Предметом дослідження є методи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Методи дослідження базуються на методах Інтернету речей, методах комп'ютерних мереж, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

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

– Удосконалено метод мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

– Розроблено вітчизняний продукт мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

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

Робота апробована на LVIII науково-технічній конференції здобувачів вищої освіти «Наука-виробництву», основні положення випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти надруковані у статті збірника праць молодих науковців ЦНТУ, випуск №17.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Камери Axis захоплюють відео за допомогою цифрових датчиків зображення, обробляють відео внутрішньо та передають його через вашу мережу на цільову платформу. Цільовим пристроєм може бути відеореєстратор, серверна система запису, хмарна платформа або рішення VMS. Основною перевагою IP-архітектури є масштабованість: у міру зростання вашого проекту ви можете додавати камери до однієї мережі та централізовано керувати користувачами, дозволами, політиками запису та екранами моніторингу.

У сучасних корпоративних середовищах від камери очікується більше, ніж просто збереження відеозапису. Віддалений доступ, централізований моніторинг, керування кількома об'єктами, запис на основі подій, робочі процеси на основі тривоги та звітність часто є частиною вимог. Системи камер Axis зазвичай вибираються для проектів, яким потрібні ці можливості для надійної роботи протягом тривалого часу.

1.2 Область застосування

Основні переваги систем камер Axis

Камери Axis відомі тим, що поєднують високу продуктивність зображення з надійною екосистемою, яка підтримує інтеграцію та довгострокове використання. Залежно від проекту, найцінніші переваги зазвичай належать до таких категорій:

– Висока чіткість зображення: краще деталізація для підтримки розслідувань та оперативної обізнаності.

– Стабільна робота за умов слабкого освітлення: стабільніше зображення за складних умов освітлення.

– Відеоаналітика: сценарії розумного аналізу, такі як виявлення вторгнень, перетин лінії та моніторинг території.

– Готовність до централізованого управління: підходить для диспетчерських пунктів безпеки та операцій на кількох об'єктах.

– Дизайн, орієнтований на кібербезпеку: створений з урахуванням міркувань безпеки підприємства.

– Масштабована архітектура: легко розширюється без переробки всієї системи.

Камери Axis проти традиційного аналогового відеоспостереження

Традиційні аналогові системи відеоспостереження зазвичай покладаються на обмежену роздільну здатність та більш жорстку архітектуру запису. IP-системи камер Axis, навпаки, використовують мережеву інфраструктуру, що забезпечує більш гнучке проектування системи. Кілька будівель, об'єктів або навіть міст можна об'єднати в один центр моніторингу, а дозволи користувачів та правила запису можна налаштувати для кожної окремої камери.

Ще однією важливою відмінністю є те, що IP-відео може підтримувати більш просунуті робочі процеси. Окрім простого зберігання відеоматеріалів, сучасні системи безпеки спрямовані на підтримку швидшого реагування та розумніших операцій. Вища якість зображення, покращене керування системою та архітектура, готова до аналітики, допомагають організаціям перейти від реактивної безпеки до проактивної.

Де використовуються камери Axis?

Камери Axis зазвичай використовуються в середовищах, де важливі надійність та безперервність роботи. Типові випадки використання включають медичні заклади, промислові об'єкти, логістичні центри, кампуси, державні установи та критично важливу інфраструктуру. У цих сценаріях метою є не лише запис подій, але й покращення видимості, вдосконалення робочих процесів контролю доступу та пришвидшення реагування на інциденти.

– Лікарні, клініки та медичні заклади

– Промислові підприємства та виробничі середовища

– Склади, логістичні центри та розподільчі центри

– Корпоративні кампуси, офісні будівлі та центри обробки даних

– Урядові будівлі та муніципальні установи

– Транспортна інфраструктура (термінали, паркувальні зони, станції тощо)

Як вибрати правильну камеру Axis

Якщо ви шукаєте «що таке камера Axis», наступним кроком зазвичай є вибір правильного рішення для ваших потреб. Професійний вибір має ґрунтуватися на меті безпеки та середовищі, а не на одній моделі продукту. Наприклад, для зон, орієнтованих на ідентифікацію, може знадобитися інша стратегія об'єктивів та роздільної здатності, ніж для загальних зон спостереження. Для зовнішнього середовища пріоритетом може бути стійкість до погодних умов та продуктивність за умов слабкого освітлення, тоді як для зон високого ризику може знадобитися вандалостійкий корпус та суворіша інтеграція контролю доступу:

– Мета безпеки: ідентифікація, розпізнавання, виявлення або загальний моніторинг.

– Навколишнє середовище: приміщення/зовнішнє середовище, умови освітлення, погода та ризик вандалізму.

– Оптика: фіксований та варіофокальний об'єктив, поле зору, висота встановлення.

– Архітектура запису: період зберігання, FPS, планування бітрейту, резервування.

– Потреби в інтеграції: сигналізація, контроль доступу, аналітичні робочі процеси, операції в диспетчерській.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

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

Security Eye

Security Eye створено спеціально для перетворення комп'ютера з Windows на практичну систему моніторингу та запису відео. Він підтримує IP-камери та веб-камери, може виявляти підтримувані мережеві камери, записує відео локально, забезпечує налаштоване виявлення та маскування руху, підтримує планування для кожної камери, може надсилати сповіщення електронною поштою/SMS та забезпечує веб-доступ для віддаленого перегляду через браузер.

Комерційна модель простіша порівняно з продуктами, що потребують багато підписки. Поточні рівні ліцензування охоплюють 2, 4, 8, 16, 32 або 64 камери. Ціни починаються від 49,95$ за 2 камери, а на сторінці покупки зазначено, що ліцензія є безстроковою та включає майбутні оновлення.

Де вирізняється Security Eye:

– Орієнтований на власний інтерфейс Windows, а не серверний стек, який має бути зібраний з кількох компонентів.

– IP-камери та звичайні USB-веб-камери можна використовувати в одній програмі моніторингу.

– Виявлення руху, маскування, розклади запису, сповіщення та віддалений перегляд через браузер покривають загальні вимоги невеликих установок.

– Ліцензування на основі кількості камер легко зрозуміти, оскільки для придбаної ліцензії не потрібна повторна підписка на програмне забезпечення.

Де інший продукт може бути кращим

Security Eye не намагається бути корпоративною системою керування відео (VMS) чи платформою для аналітики на основі штучного інтелекту. Якщо вам потрібно понад 100 камер, багатосерверне резервне копіювання, корпоративне адміністрування в стилі Active Directory/LDAP, складне розпізнавання об'єктів, розпізнавання номерних знаків або велика екосистема інтеграції, Blue Iris, Agent DVR, Xeoma, Milestone або Luxriot можуть краще підійти залежно від вимог.

Найкраще для: людей, яким потрібен звичайний відеоспостереження Windows – перегляд у реальному часі, локальний запис, сповіщення про рух, розклади та доступ до браузера – без складного розгортання в корпоративному середовищі.

Blue Iris

Blue Iris – одне з найвідоміших імен, що спеціалізуються виключно на Windows-технологіях відеозапису для самостійного використання та малого бізнесу. На поточному сайті Blue Iris 6 рекламується підтримка до 128 камер, включаючи веб-камери, мережеві IP-камери, аналогові пристрої захоплення та пристрої захоплення з робочого столу Windows. Він підтримує віддалений перегляд у режимі реального часу/запису, набори дій та різні формати запису.

Версія 6 також продовжує розширювати функціональність, пов'язану зі штучним інтелектом. Нотатки до оновлення Blue Iris 2026 року описують роботу з відстеження та аналізу об'єктів за допомогою штучного інтелекту, покращення автоматичного відстеження PTZ, функції захоплення пластин, інтеграцію H.265/GPU та інші покращення запису/відтворення. Це робить Blue Iris особливо привабливим для користувачів, які люблять детальне налаштування та хочуть ретельно налаштувати відеореєстратор Windows.

Ціни та вимоги до Blue Iris

На офіційному сайті повна ліцензія наразі вказана за ціною $99,95 для максимум 128 камер, а ліцензія LE – за $39,95 для однієї камери. Доступна безкоштовна пробна версія. Постачальник також пропонує додаткові плани

обслуговування/підтримки. Blue Iris визначає мінімальні вимоги: новіший процесор Intel, щонайменше 8 ГБ оперативної пам’яті та 64-розрядну серверну версію Windows 10 або еквівалентну; для потужніших систем рекомендується Windows 11, швидше сховище та додаткова відеокарта Nvidia.

Найкращі причини обрати Blue Iris:

– Високий ліміт камери для настільного продукту Windows.

– Глибокий запис, керування тригерами, сповіщеннями та автоматизацією.

– Активна розробка 2026 року з оновленнями версії 6.

– Чудово підходить для користувачів, які хочуть точно налаштувати спеціалізований відеореєстратор Windows.

Компроміс: глибина також може означати більше налаштувань та налаштувань. Якщо вам потрібен менший набір елементів керування відеоспостереженням та простіший робочий процес, Security Eye або ContaCam можуть бути простішими варіантами.

Agent DVR

Agent DVR – це активно розроблюваний наступник старішої програми для настільних комп’ютерів iSpy. Хоча вона працює на Windows 10+, вона не призначена лише для Windows: постачальник також підтримує macOS, Linux, Docker та Raspberry Pi. Її інтерфейс працює в браузері, а програмне забезпечення може працювати як служба.

Agent DVR підтримує IP-камери, пристрої ONVIF, потоки RTSP, USB-камери та аудіопристрої. Постачальник не публікує програмних обмежень щодо кількості камер; доступний процесор, графічний процесор, пам'ять, пропускна здатність мережі та сховище визначають практичну максимальну потужність. Він може записувати необроблені потоки камер, де це можливо, та включає виявлення руху, відстеження, розтяжки, PTZ, події/дії та інтеграцію зі штучним інтелектом. Поточний список функцій також включає опції розпізнавання об'єктів, облич, номерних знаків та звуку.

Віддалений доступ – це головна відмінність

Agent DVR пропонує розміщений віддалений доступ без переадресації портів. Це зручно для людей, які не хочуть налаштовувати VPN, DDNS або правила маршрутизатора. Компромісом є ліцензування: приватне локальне використання безкоштовне, тоді як для бізнес-використання та розміщених віддалених сервісів потрібна підписка. Офіційна сторінка з цінами на 2026 рік починається від $7,95/місяць; вищі плани розблоковують такі функції, як віддалене відтворення HD або 4K. Річна передоплата включає безстрокову локальну ліцензію на відповідні локальні функції, але розміщені сервіси все одно вимагають активної підписки.

Найкраще підходить для: користувачів, які віддають перевагу сучасному веб-інтерфейсу, потребують кросплатформного розгортання, бажають мати багато варіантів штучного інтелекту/інтеграції або цінують простий шлях віддаленого доступу через хостинг.

ContaCam

ContaCam використовує компактніший підхід. Це програма для спостереження та веб-камер у реальному часі для Windows, розроблена для економії системних ресурсів. Постачальник документує підтримку веб-камер та мережевих/IP-камер, що використовують RTSP з H.264/H.265 або MJPEG, а також запис за детекцією руху.

ContaCam також включає вбудований веб-сервер, захищений паролем, відображення подій руху у вигляді анімованих мініатюр та опцію створення щоденного відео зведення. Документація щодо підтримуваних пристроїв охоплює багато брендів камер і чітко рекомендує перевіряти підтримку RTSP від сторонніх виробників під час купівлі хмарно-орієнтованих камер.

ContaCam – це програма для пожертвування з відкритим вихідним кодом, а не звичайний комерційний продукт за підпискою. Contaware просить пожертвувати 10$ за кожне встановлення та публікує вихідний код під ліцензією GNU GPL. На поточному сайті зазначено, що підтримувані версії ContaCam 9.9.27 та Windows 7 або новіші.

Найкраще підходить для: технічно досвідчених користувачів, які хочуть

недорогий локальний запис у Windows та виявлення руху без необхідності платити за великий набір функцій VMS.

Компроміс: ContaCam навмисно спрощений. Користувачам, які шукають сучасний хостинг віддаленого доступу, складну аналітику ШІ або корпоративні дозволи, варто порівняти Agent DVR, Xeoma, Milestone або Luxriot.

Xeoma

Xeoma – це кросплатформна система відеоспостереження, побудована на основі налаштовуваних модулів. Її стандартна версія наразі включає 47 модулів, віддалений доступ без статичної IP-адреси через P2P, кілька профілів користувачів, керування PTZ, перегляд у браузері, циклічний запис на кілька дисків або NAS, подвійну потокову передачу та виявлення руху з логікою зменшення хибних тривог. Вона працює як на Windows, так і на Linux, macOS та інших підтримуваних платформах.

Xeoma особливо відрізняється від простіших програм спостереження тим, що користувачі можуть створювати ланцюжки джерел, детекторів та реакцій. Більш просунуті версії та додаткові модулі розширюють можливості системи на розпізнавання об'єктів, облич, номерних знаків та інші аналітичні можливості.

Xeoma пропонує кілька редакцій та варіантів термінів оновлення. Згідно з прайс-листом постачальника за травень 2026 року, Xeoma Lite починається від 15 доларів за одну камеру, але обмежена чотирма камерами та не включає оновлення програми. Xeoma Standard починається від 33 доларів за одну камеру з річною підпискою на оновлення; 4 камери коштують 130 доларів, а 8 камер – 259 доларів за той самий термін оновлення. Ліцензії Standard/Pro є безстроковими, також пропонуються довші періоди оновлення та підписки. Розширена аналітика може передбачати додаткові витрати на модуль кожної камери.

Найкраще підходить для: користувачів, яким подобається візуальна модульна архітектура, потрібні кросплатформні серверні/клієнтські опції або які планують додавати спеціалізовану аналітику пізніше.

Компроміс: матриця редакцій/модулів/ліцензій набагато складніша, ніж у Security Eye, Blue Iris або ContaCam. Перш ніж встановлювати ціну на систему, перевірте точні модулі, які вам потрібні.

Milestone XProtect Express+

Milestone XProtect ближче до професійної інфраструктури для керування відео, ніж до типової утиліти для домашніх камер. У поточній родині XProtect Express+ є базовим платним варіантом для невеликих підприємств з одним об'єктом. Milestone стверджує, що Express+ підтримує до 48 камер на одному об'єкті .

Платформа XProtect надає спеціалізовані клієнти для робочих станцій, веб-сайтів та мобільних пристроїв і розроблена для таких робочих процесів операторів, як перегляд у реальному часі, відтворення, сигналізація та обробка доказів. Поточні системні вимоги 2026 R1 включають Windows 10 Pro/Enterprise, Windows 11 Pro/Enterprise та підтримувані версії Windows Server для компонентів Express+.

Помітна зміна 2026 року: Essential+ більше не є поточним базовим продуктом.

У старіших статтях часто рекомендується безкоштовна версія XProtect Essential+ для восьми пристроїв. Ця порада вже застаріла. У поточній лінійці продуктів Milestone та документації для розробників перелічено Express+, Professional+, Expert та Corporate; на поточній сторінці продукту Express+ позиціонується як початковий варіант для малого бізнесу. Це одна з причин, чому порівняння 2026 року не повинно просто повторювати старі списки «найкращих безкоштовних VMS».

Найкраще підходить для: компаній, яким потрібна більш формальна архітектура VMS, клієнтів-операторів та шлях оновлення до масштабніших розгортань Milestone.

Компроміс: це більш суттєва система для розгортання та адміністрування, ніж простий додаток для спостереження за ПК, а публічні ціни не представлені так просто, як у продуктів, орієнтованих на споживача.

Luxriot EVO S

Luxriot EVO – це ще одна VMS-система, орієнтована на Windows, призначена для професійного розгортання. Luxriot документує підтримку IP-камер, аналогових пристроїв та веб-камер, з кодеками H.264/H.265/MJPEG та іншими, транспортуванням RTSP/HTTP, профілем ONVIF S, виявленням камер, PTZ, розкладами запису, записом до/після події, клієнтами для браузера/мобільних пристроїв, дозволами користувачів, робочими процесами подій/дій та розширеними інструментами відтворення/пошуку.

На поточній сторінці завантаження Luxriot EVO S 1.33.1 перелічено Windows 10, Windows 11, Windows Server 2019 та Windows Server 2022. Luxriot також пропонує інтегровану та додаткову аналітику для виявлення об'єктів, номерних знаків, розпізнавання облич та інших випадків використання, залежно від ліцензування та конфігурації.

В адміністративній документації Luxriot описано 45-денну пробну версію з одночасно увімкненими до 16 відеоканалами та доступом до функцій продукту для оцінки. Ліцензування виробництва здійснюється через запит, а не за простою таблицею цін для споживачів.

Найкраще підходить для: комерційних установок, що потребують багатокористувацького адміністрування, клієнт-серверної архітектури VMS, розширеної обробки подій та можливості розширення до більш складної аналітики або багатосерверних конструкцій.

Компроміс: для двох-восьми камер вдома Luxriot може бути більшою системою, ніж вам потрібно. Її сильні сторони стають більш актуальними зі зростанням операційних та адміністративних вимог.

Sighthound Video

Sighthound Video досі фігурує в багатьох списках «найкраще програмне забезпечення для IP-камер» та «найкраще програмне забезпечення для спостереження», оскільки історично це був помітний настільний продукт, орієнтований на виявлення людей, транспортних засобів та тварин за допомогою комп’ютерного зору. Однак на власній поточній сторінці продукту Sighthound

Video тепер називається застарілим настільним DVR/VMS, зазначається, що він більше не перебуває в стадії активної розробки функцій або регулярних оновлень програмного забезпечення, а підтримка описується як найкращі зусилля для вирішення критичних проблем. Вихідний код тепер доступний спільноті.

Для існуючих користувачів це може бути цілком прийнятним. Однак для нової інсталяції Windows 2026 року ми не будемо розміщувати неактивний застарілий продукт у основному короткому списку поруч із активно підтримуваним програмним забезпеченням. Це також приклад того, чому старі статті для порівняння потрібно перевіряти на наявність актуальної інформації про постачальника, перш ніж використовувати їх повторно.

Яке програмне забезпечення для відеоспостереження для Windows слід обрати?

Оберіть Security Eye, якщо вам потрібна простота та одноразова ліцензія. Якщо вашою метою є домашня, магазинна або невелика офісна система Windows з кількома IP-камерами або веб-камерами, а вашими пріоритетами є локальний запис, виявлення руху, розклади, сповіщення та перегляд веб-сторінок, Security Eye зберігає відносно просту архітектуру. Рівні безстрокової ліцензії від 2 до 64 камер також роблять довгострокову вартість програмного забезпечення передбачуваною.

Оберіть Blue Iris, якщо бажаєте максимального контролю над спеціалізованим відеореєстратором Windows NVR. Blue Iris краще підійде, якщо ви вмієте налаштовувати велику кількість параметрів камери, запису, запуску та штучного інтелекту, і хочете підтримувати до 128 камер в одному продукті для Windows.

Оберіть Agent DVR, якщо важливі віддалений доступ та кросплатформне розгортання. Agent DVR є переконливим варіантом, коли вам потрібен інтерфейс браузера, ви не хочете, щоб сервер був прив'язаний лише до Windows, або ви надаєте перевагу віддаленому підключенню, розміщеному на сервері постачальника, без ручного відкриття портів. Просто включіть вартість

підписки, якщо віддалені/бізнес-функції є частиною ваших вимог.

Оберіть ContaCam, якщо вашим пріоритетом є легкий та недорогий локальний запис. ContaCam надзвичайно недорога та прозора програма. Це розумна програма для перевірки того, чи ваші камери забезпечують стандартні RTSP-потоки, і чи потрібні вам переважно запис, події руху та доступ до браузера, а не корпоративна аналітика.

Оберіть Xeoma, якщо вам потрібна модульна обробка даних та опціональна аналітика. Підхід Xeoma з використанням ланцюжка модулів корисний, коли кожній камері може знадобитися різний конвеєр виявлення та дій. Він може широко масштабуватися, але ретельно порівнюйте вартість редакції та модулів.

Оберіть Milestone або Luxriot, якщо ви створюєте бізнес-систему управління відеоспостереженнями, а не просто реєстратор для ПК.

Коли дозволи користувачів, робочі процеси операторів, інтеграції, обробка подій, процеси доказів та майбутнє розширення мають більше значення, ніж швидке отримання чотирьох камер запису, професійна система управління відеоспостереженнями, така як XProtect або Luxriot EVO, стає набагато актуальнішою.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Python є високорівневою об'єктно-орієнтованою мовою програмування загального призначення з відкритим вихідним кодом. Завдяки своїй гнучкості та розвиненій екосистемі вона широко використовується для розробки серверного програмного забезпечення, інтеграції пристроїв Інтернету речей (IoT) та взаємодії із закритими чи відкритими API (зокрема обладнанням Axis).

Основні концептуальні особливості мови:

– Відкритий вихідний код: забезпечує доступність мови для модифікації, аудиту безпеки та кастомізації.

– Об’єктно-орієнтована парадигма: базується на концепції об'єктів з атрибутами й методами, що полегшує проєктування модульних архітектур безпеки.

– Високорівневість: абстрагує розробника від низькорівневих апаратних деталей, зосереджуючи увагу на бізнес-логіці та протоколах захисту.

– Загальне призначення: дозволяє створювати як хмарні сервери для агрегації телеметрії, так і скрипти автоматизованого моніторингу мережевих вузлів.

Переваги та обмеження для IoT-інфраструктур

Переваги:

– Швидкість розробки та простота синтаксису: дозволяє оперативно створювати прототипи систем безпеки та інтегрувати сторонні сервіси через відкриті API з мінімальними витратами часу.

– Динамічна типізація та інтерпретованість: спрощують написання та відлагодження скриптів для збору й аналізу пакетів у гетерогенних мережах.

– Величезна стандартна бібліотека та екосистема модулів: надає готові інструменти для роботи з мережевими протоколами (HTTP/HTTPS, MQTT, WebSockets), що критично для обміну даними з камерами та IoT-сенсорами Axis.

Обмеження:

– Обчислювальна швидкість та пам'ять: як інтерпретована мова з динамічною типізацією, Python поступається у швидкодії компільованим мовам (C/C++), що потребує обережності при роботі з інтенсивними потоками «сирих» даних на шлюзах з обмеженими ресурсами.

– Застосування на пристроях: на відміну від серверного рівня, на рівні клієнтських мікроконтролерів (Edge devices) використання Python обмежене через високе споживання пам'яті.

Сфери застосування Python у проекті:

1. Інтеграція через відкриті API та роботу з Axis-технологіями Python є оптимальним інструментом для опитування пристроїв (камер, датчиків, контролерів) через REST API, VAPIX та інші відкриті протоколи Axis. За

допомогою HTTP-запитів і бібліотек на кшталт requests реалізується управління подіями, отримання потоків відео та налаштування параметрів безпеки обладнання.

2. Моніторинг та аналіз мережевого трафіку IoT Використовується для збору метрик, аналізу логів безпеки, виявлення аномалій у поведінці пристроїв інтернету речей та автоматичного реагування на загрози.

3. Автоматизація завдань і скриптинг Скрирти на Python дозволяють автоматизувати розгортання конфігурацій безпеки на десятках IoT-вузлів, оновлення сертифікатів, перевірку цілісності з'єднань та тестування на проникнення (Penetration Testing).

4. Розробка серверної частини (Backend) та обробка подій Побудова централізованих серверів безпеки, які приймають тривожні сповіщення від систем відеоспостереження Axis, обробляють потоки даних та інтегрують їх із загальною корпоративною системою захисту.

Стек бібліотек для розробки:

– Для роботи з мережею та API: requests, urllib3, asyncio (для асинхронних запитів до великої кількості IoT-пристроїв).

– Для обробки даних та аналітики: pandas, numpy (для аналізу логів безпеки та телеметрії).

– Для візуалізації станів системи: matplotlib, seaborn (для побудови графіків навантаження мережі та інцидентів безпеки).

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускну кваліфікаційну роботу за другим (магістерським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

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

роботи:

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

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

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

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

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

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

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

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

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Камера Axis – одне з найбільш досліджених рішень для організацій, які хочуть побудувати надійну інфраструктуру відеоспостереження на основі IP. Axis Communications широко визнана піонером у сфері мережевого відео та часто розгортається у критично важливих середовищах по всьому світу. Однак для більшості осіб, які приймають рішення у сфері B2B, і шукають «камеру Axis», справжнє питання полягає не лише в бренді: чи підходить ця система для нашого об'єкта? Які типи камер нам слід вибрати? Як слід проектувати мережу та запис? Як нам керувати аналітикою та кібербезпекою? Ці фактори визначають успіх проекту Axis у реальних операціях.

Ми розглядаємо розгортання камер Axis як інженерно-орієнтовані інтеграційні проекти, а не як постачання продуктів. Високопродуктивна система Axis досягається завдяки зонуванню ризику, правильному вибору камери та оптики, надійній архітектурі мережі, оптимізованому дизайну запису та практичним робочим процесам. На цій сторінці пояснюється використання камер Axis крізь призму підприємства, охоплюючи категорії камер, стратегію обробки зображень, планування інфраструктури, інтеграції та найкращі практики реалізації проектів.

Що таке камера Axis у корпоративному контексті?

Камери Axis – це мережеві IP-камери, які захоплюють відео в цифровому вигляді, обробляють його внутрішньо та передають через мережу на систему управління відеоспостереженням (VMS), відеореєстратор (NVR) або сервер. У корпоративних системах «камера» означає більше, ніж просто пристрій: вона включає централізований моніторинг, керування записом, дозволи на основі ролей, робочі процеси обробки інцидентів та звітність. Саме тому вибір камер Axis повинен відповідати цілям безпеки, IT-стандартам та операційним

процедурам в організації.

Багато сторінок, які ранжуються за запитом «Камера Axis», зосереджені лише на специфікаціях. У корпоративних проектах продуктивність визначається багаторівневою архітектурою. Структуруємо розгортання навколо п’яти рівнів:

1. Зонування ризику та мета: виявлення / розпізнавання / ідентифікація
2. Тип камери та оптика: купольна/кулеподібна/PTZ/тепловізійна + стратегія об'єктива
3. Архітектура мережі: бюджет PoE, сегментація VLAN, пропускна здатність аплінку
4. Дизайн запису: збереження, планування бітрейту/FPS, резервування
5. Операції та інтеграція: макети VMS, робочі процеси тривог, інтеграції

Типи камер Axis: вибір правильного форм-фактора

Використання одного типу камери на корпоративному об'єкті рідко буває ефективним. Проєкти Axis часто досягають найкращих результатів завдяки гібридним конструкціям:

– Купол: входи, коридори, загальний моніторинг у приміщенні.

– Маркета: зовнішні стіни, периметральні зони, паркувальні зони.

– PTZ: широкі майданчики, логістичні зони, динамічний моніторинг диспетчерської.

– Теплові: виявлення периметра та раннє попередження за складних умов освітлення/погоди.

– 360°/Риб'яче око: широке покриття в приміщенні з однієї точки кріплення.

Стратегія візуалізації: більше, ніж просто роздільна здатність

Роздільна здатність має значення, але це не єдиний фактор. «Правильне зображення» залежить від об’єкта. На вході для ідентифікації може знадобитися правильний об’єктив, висота кріплення та план освітлення. На периметрі пріоритетом можуть бути раннє виявлення та широке охоплення. Ми визначаємо цілі візуалізації на трьох рівнях: виявлення (щось там є), розпізнавання (хто це може бути) та ідентифікація (хто це саме). Ця структура визначає рішення щодо

камери та оптики.

Продуктивність за умов слабкого освітлення та безпека вночі

Значна частина інцидентів трапляється в умовах низької освітленості. Парковки, периметральні зони, зони воріт та нічні зміни залежать від стабільного зображення в умовах низької освітленості. Проекти камер Axis повинні оцінювати роботу в нічний час за допомогою контролю шуму, збереження контрастності та читабельності рухомих об'єктів. Ці фактори визначають, наскільки дієвим буде відеозапис під час реальних інцидентів.

Відеоаналітика: від «перегляду екранів» до «керування інцидентами»

Аналітика може перетворити пасивний запис IP-відео на проактивну безпеку. Виявлення вторгнень, перетин лінії та сценарії байдикування зменшують навантаження на безперервний моніторинг та покращують час реагування. Успіх аналітики залежить від калібрування, порогових значень та робочих процесів тривоги всередині VMS. TISI керує введенням аналітики в експлуатацію за допомогою тестування на місці та критеріїв приймання, щоб забезпечити реальну цінність.

Архітектура мережі та запису: прихований фундамент

Найпоширенішою помилкою в IP-відеопроектах є нехтування мережею та записом. У розгортаннях Axis пропускна здатність, бюджет PoE, ємність комутатора, швидкість висхідного каналу, сегментація VLAN та безпечний контроль доступу повинні бути розроблені з самого початку. З боку запису, рішення щодо збереження даних, FPS, бітрейту та запису на основі руху визначають ємність сховища та стабільність системи. TISI захищає якість у зонах високого ризику, одночасно оптимізуючи ресурси в зонах низького ризику.

Кібербезпека: основна вимога для схвалення підприємства

IP-камери – це кінцеві точки мережі, тому кібербезпека не є необов’язковою. Політики паролів, дозволи на основі ролей, безпечний віддалений доступ, управління оновленнями та ведення журналу повинні відповідати корпоративним IT-стандартам. TISI проектує мережі камер Axis із

сегментацією, обмеженим доступом та документацією, готовою до аудиту, щоб зменшити площу атак та забезпечити відповідність вимогам.

Методологія для проектів Axis Camera

Структурована модель реалізації знижує технічні ризики та пришвидшує введення в експлуатацію:

1. Оцінка та вимоги: зони ризику, цілі, базова інфраструктура.
2. Дизайн: типи камер, оптика, креслення розміщення.
3. План мережі та запису: PoE, VLAN, сховище та резервування.
4. Монтаж та введення в експлуатацію: випробування, калібрування, критерії приймання.
5. Навчання та підтримка: оперативна готовність та довгострокова безперервність.

Що визначає вартість проекту з камерами Axis?

Вартість підприємства залежить не лише від моделі камери. Роздільна здатність, оптика, клас корпусу, вимоги до аналітики, політика зберігання даних, оновлення мережі та ліцензування програмного забезпечення визначають загальну вартість проекту. Найефективнішим підходом є проектування з урахуванням потреб проекту після оцінки об'єкта. TISI усуває непотрібні витрати, узгоджуючи архітектуру з реальними цілями.

Переваги камер Axis

Переваги камер Axis найкраще розуміються в корпоративних (B2B) проектах безпеки, де метою є не просто запис відео, а управління ризиками, покращення безперервності роботи та забезпечення проактивного реагування на інциденти. Хоча ринок IP-спостереження включає багато варіантів, Axis Communications широко вважається еталонним брендом у мережевому відео. Тому рішення Axis часто обираються для розгортань, які надають пріоритет надійності, якості, масштабованості та кібербезпеці, а не просто мінімізації початкових витрат. У таких середовищах, як охорона здоров'я, промислові підприємства, логістичні центри, кампуси та державні установи, довгострокова цінність системи спостереження має таке ж значення, як і початкове

встановлення.

Ми позиціонуємо переваги камер Axis через реальний операційний вплив. Функції забезпечують цінність лише за умови правильного проектування системи: правильний вибір камери, розміщення, планування мережі та сховища, інтеграція VMS та робочі процеси в разі інцидентів. Нижче ми підсумовуємо ключові переваги камер Axis та пояснюємо, чому вони важливі для операцій безпеки підприємства:

1. Зображення та детальне захоплення корпоративного рівня. У корпоративному середовищі якість зображення – це не просто «чітке відео». Вона дозволяє ідентифікувати особу, підтримує записи якості доказів та пришвидшує розслідування. Камери Axis пропонують різні варіанти роздільної здатності та опції, які можна оптимізувати для задоволення конкретних цілей безпеки. Завдяки правильному проекту, критично важливі ділянки можуть досягти рівня ідентифікації там, де це найбільше важливо.

2. Стабільність за умов слабкого освітлення та продуктивність у складних умовах. Багато зон високого ризику стають більш вразливими за умов слабкого освітлення: паркувальні майданчики, периметри, двори, енергетичні об'єкти та виробничі майданчики, що працюють у нічні зміни. Основною перевагою камер Axis є стабільне зображення за умов слабкого освітлення зі зниженим шумом та покращеною контрастністю. Це допомагає службам безпеки швидше реагувати та приймати кращі рішення під час реальних інцидентів.

3. Проактивна безпека за допомогою відеоаналітики. Сучасна безпека переходить від реактивного аналізу до проактивного виявлення. Переваги камер Axis стають сильнішими, коли аналітика розгортається правильно. Аналітика виявлення вторгнень, перетину лінії, моніторингу зони та байдикування зменшує навантаження постійного ручного моніторингу та покращує час реагування. З точки зору інтегратора, калібрування є важливим: погано налаштована аналітика може генерувати надмірну кількість хибних тривог та знижувати довіру операторів. Розглядаємо аналітику як операційний компонент: ми тестуємо сценарії на місці, точно налаштовуємо порогові значення та

розробляємо робочі процеси тривоги, щоб зробити аналітику практичною, а не відволікаючою.

4. Гнучкість інтеграції та відкрита екосистема. Системи відеоспостереження на підприємстві рідко працюють самостійно. Вони інтегруються з системами контролю доступу, сигналізації про вторгнення, розпізнавання номерних знаків, пожежної сигналізації, управління будівлями та управлінням диспетчерською. Рішення Axis підтримують архітектури на основі інтеграції, що дозволяє організаціям створювати розширені робочі процеси без прив'язки до екосистеми одного постачальника. Така гнучкість підтримує майбутнє розширення та захищає існуючі інвестиції.

5. Кібербезпека та відповідність IT-стандартам. IP-камери – це кінцеві точки, підключені до мережі, що робить кібербезпеку основною вимогою. Ключовою перевагою розгортання Axis є можливість створювати архітектури, що відповідають корпоративним практикам безпеки: управління доступом, методи автентифікації, безпечний віддалений доступ, управління оновленнями та ведення журналу. TISI зазвичай впроваджує практики сегментації (VLAN), контрольованого доступу та документування для підтримки аудитів та зменшення поверхонь атак.

6. Масштабованість: плавне розширення в міру зростання проекту. Корпоративні середовища розвиваються. З часом можуть додаватися нові будівлі, склади, виробничі лінії та майданчики. Переваги камер Axis включають масштабовану IP-архітектуру, яка підтримує розширення без перепроектування всієї системи. Завдяки правильному плануванню мережі та VMS нові пристрої, групи користувачів та станції моніторингу можна додавати безперешкодно.

7. Перспектива загальної вартості володіння (TCO). Axis може вимагати більших початкових інвестицій порівняно з альтернативами, орієнтованими на ціну, але він може забезпечити довгострокову цінність завдяки зниженню рівня збоїв, меншому навантаженню на обслуговування, безперервності роботи та стабільній підтримці програмного забезпечення. У сфері корпоративної безпеки вартість простою часто набагато перевищує ціну пристрою. Саме тому TISI

оцінює розгортання Axis крізь призму ризику та безперервності, а не лише через початкові витрати на закупівлю.

8. Оперативна керованість та централізоване управління. Зі зростанням масштабів розгортань централізоване управління стає важливим. Завдяки відповідному дизайну VMS, системи Axis підтримують дозволи на основі ролей, робочі процеси обробки інцидентів, звітність та операції на кількох сайтах. Це допомагає командам безпеки перейти від «спостереження за екранами» до «управління інцидентами» за допомогою стандартизованих процедур. TISI розробляє схеми моніторингу та робочі процеси, що відповідають операційній моделі організації.

Типи камер Axis

Типи камер Axis відносяться до професійних категорій IP-камер, вибраних відповідно до різних рівнів ризику, середовищ та цілей безпеки в корпоративних розгортаннях. Мета полягає не просто у «встановленні камер», а у досягненні необхідного рівня *виявлення*, *розпізнавання* або *ідентифікації* в ключових зонах, покращенні реагування на інциденти та стабільній роботі системи з часом. Axis Communications пропонує різні форм-фактори, оптичні опції та набори функцій, які підтримують ці цілі в реальних B2B-проектах.

Пояснимо типи камер з точки зору їхньої практичної цінності: де кожен тип працює найкраще, як його вибрати на основі параметрів конструкції та як він вписується в архітектуру безпеки підприємства. Правильний вибір типу впливає на якість зображення, експлуатаційну ефективність та довгострокову загальну вартість володіння.

Чому типи камер важливі в корпоративних проектах

Дві камери з однаковою роздільною здатністю можуть забезпечити абсолютно різні результати, якщо вони належать до різних категорій та розгортаються в різних умовах. Наприклад, PTZ-камера може бути ідеальною для динамічного моніторингу широкого відкритого подвір’я, тоді як фіксована купольна камера може бути правильним вибором для входу, де потрібен постійний зйом. Фактори навколишнього середовища (погода, пил, вандалізм),

висота монтажу, освітлення та обмеження інфраструктури (бюджет PoE, ємність мережі) визначають остаточний вибір. Найкращі результати для підприємств часто досягаються завдяки гібридній конструкції, яка стратегічно поєднує кілька типів.

1. Купольні камери (для використання всередині приміщень та вандалостійкі). Купольні камери Axis є одними з найпоширеніших типів завдяки компактному дизайну та широкому застосуванню. Їх часто встановлюють у приміщеннях офісів, лікарень, торгових приміщень, коридорів та входів. Купольні корпуси можуть забезпечити стримування, оскільки напрямок огляду менш очевидний. Вандалостійкі моделі допомагають зменшити ризик пошкодження у громадських місцях або місцях з високою прохідністю:

– Найкраще підходить для: входів, коридорів, зон рецепції, ліфтових вестибюлів.

– Переваги: естетика, довговічність, широке поле зору.

– Міркування: висота кріплення, вибір об'єктива, відбиття/освітлення.

2. Камери-кулі (зовнішній та дальній моніторинг). Кулеподібні камери Axis призначені для зовнішнього використання та зазвичай мають видовжений корпус, що підходить для охоплення периметра та зовнішньої території. Вони широко використовуються навколо складів, екстер'єрів будівель, парковок та подвір'їв. Видима орієнтація може забезпечити сильний стримуючий ефект. Для зовнішнього використання належний захист навколишнього середовища та методи встановлення є важливими для підтримки стабільної роботи:

– Найкраще підходить для: зовнішніх стін, периметральних зон, в'їздів транспортних засобів, моніторингу відкритого простору.

– Переваги: довговічність на відкритому повітрі, висока продуктивність на великі відстані.

– Міркування: відбиття ІЧ-випромінювання, кут монтажу, захист кабелю.

3. PTZ-камери (поворотні, нахилені та масштабовані для динамічного охоплення). Камери Axis PTZ забезпечують моторизоване панорамування, нахил

та оптичне масштабування, що дозволяє динамічно контролювати великі території за допомогою однієї камери. Типові випадки використання включають великі кампуси, логістичні майданчики, порти, міське відеоспостереження та критичну інфраструктуру. Цінність PTZ залежить від операційної структури: попередньо встановлені налаштування, патрульні маршрути, автоматичне відстеження за сигналізацією та навчання операторів повинні бути належним чином сплановані. В іншому випадку камера може не дивитися в потрібне місце в потрібний час:

– Найкраще підходить для: широких відкритих майданчиків, критичних зон, операцій у диспетчерській.

– Переваги: широке покриття, оптичний зум для деталізації.

– Міркування: сліпі зони, залежність від оператора, попередньо встановлений дизайн.

4. Тепловізійні камери (виявлення незалежно від видимого світла). Тепловізійні камери Axis виявляють різницю в температурі, а не покладаються на видиме світло. Це робить їх надзвичайно цінними в проектах охорони периметра та критичної інфраструктури, особливо в умовах низької освітленості, туману або складних погодних умов. Тепловізійне зображення в основному використовується для виявлення та раннього попередження, а не для ідентифікації облич. Успіх проектування залежить від правильного планування відстані виявлення та калібрування сценарію:

– Найкраще підходить для: захисту периметра, критичної інфраструктури, відкритих середовищ.

– Переваги: стабільне виявлення за умов слабкого освітлення та несприятливих погодних умов.

– Міркування: розробка сценаріїв, планування дальності виявлення.

5. Камери типу «риб’яче око» на 360° (широке покриття з однієї точки). Камери типу «риб’яче око» на 360° забезпечують широке покриття з одного місця монтажу. Вони часто використовуються в приміщеннях у вестибюлях, відкритих офісах та точках перетину складів. Найкращі результати потребують

правильної стратегії монтажу та робочих процесів виправлення спотворень VMS для перетворення зображень типу «риб'яче око» на зручні для операторів перспективи:

– Найкраще підходить для: вестибюлів, відкритих офісів, складських приміщень.

– Переваги: широке покриття, менше сліпих зон.

– Міркування: керування деформацією, висота монтажу.

6. Спеціалізовані камери Axis (LPR/ANPR, корпусні, вибухозахищені тощо). Корпоративні проекти часто потребують камер, що виходять за рамки стандартних форм-факторів. Розгортання систем розпізнавання номерних знаків (LPR/ANPR) вимагає спеціального проектування та інтеграції. Небезпечні середовища можуть вимагати вибухобезпечних рішень. Мобільні операції безпеки можуть вимагати пристроїв, що носяться на тілі. У цих проектах успіх залежить як від робочого процесу та інтеграції програмного забезпечення, так і від вибору апаратного забезпечення.

3.2 Розробка структурної схеми

Системи камер Axis

Системи камер Axis – це IP-відеоінфраструктури корпоративного рівня, які включають набагато більше, ніж просто камери. Надійне розгортання вимагає мережевої архітектури, проектування запису та зберігання даних, програмного забезпечення для керування відео (VMS), дозволів користувачів, інтеграції, робочих процесів аналітики та рівня кібербезпеки. Axis Communications широко вважається еталонним брендом у мережевому відео, який часто обирають для проектів B2B, де надійність, довгострокова ремонтопридатність та безперервність роботи є критично важливими. З цієї причини до систем Axis найкраще підходити як до інженерних проектів, а не як до закупівлі продуктів.

З яких компонентів складається система камер Axis?

Професійна система камер Axis – це екосистема компонентів, які повинні працювати разом. Потужних окремих пристроїв недостатньо; загальна архітектура повинна відповідати меті безпеки. Типове розгортання включає:

– IP-камери: купольні, кульові, PTZ, тепловізійні та інші форм-фактори.

– Мережева інфраструктура: комутатори, PoE, віртуальні локальні мережі, потужність магістралі та безпечний доступ.

– Архітектура запису: NVR/сервер, проектування сховища, резервування та політики запису.

– Програмне забезпечення для керування відео (VMS): Централізований моніторинг, управління інцидентами, дозволи користувачів.

– Аналітика та інтеграції: сигналізація, контроль доступу, робочі процеси LPR, сценарії диспетчерської.

– Кібербезпека: автентифікація, безпечний віддалений доступ, управління оновленнями, ведення журналу.

Перше питання має бути не «Скільки камер нам потрібно?», а «Якої мети безпеки ми повинні досягти?» Деякі зони потребують виявлення, інші – розпізнавання або ідентифікації . Ці цілі визначають роздільну здатність, стратегію об’єктивів, поле зору, висоту монтажу, обмеження освітлення та параметри запису.

Архітектура мережі та планування PoE

В IP-відео мережа є основою системи. Камери Axis зазвичай використовують PoE (живлення через Ethernet), передаючи живлення та дані по одному кабелю. У корпоративних розгортаннях критично важливими є бюджет PoE, розмір комутатора, пропускна здатність висхідного каналу, розділення VLAN та централізована чи розподілена топологія. Неправильне проектування мережі може призвести до падіння відео, втрати пакетів, нестабільного доступу та перерв у записі.

Архітектура запису: зберігання, резервування та збереження даних

Проектування корпоративних систем запису визначається вимогами до

дотримання нормативних вимог та операційними вимогами. Термін зберігання (скільки днів зберігати відзнятий матеріал) впливає на загальний розмір сховища, але це не єдиний фактор. FPS, бітрейт, роздільна здатність, запис на основі руху та складність сцени також впливають на сховище. Добре спроектована система Axis захищає якість у зонах високого ризику, одночасно оптимізуючи споживання ресурсів у зонах низького ризику.

Резервування не менш важливе. У критично важливих об'єктах збій сервера запису є не лише IT-проблемою, а й ризиком для безпеки.

VMS та операційне управління

Системи Axis стають справді «корпоративними» завдяки надійному шару VMS. Платформи VMS забезпечують моніторинг у реальному часі, відтворення, додавання закладок до інцидентів, дозволи на основі ролей, обробку тривог та звітність. В організаціях з кількома об’єктами централізоване управління забезпечує узгоджену роботу та стандартизовані процедури реагування.

З точки зору інтегратора, ключовим є зручність використання. Макети екранів, робочі процеси інцидентів та структури дозволів повинні відповідати операційній моделі організації . Виробничому майданчику можуть знадобитися дозволи на основі змін, тоді як лікарні можуть знадобитися різні групи доступу для різних відділів.

Аналітика, сценарії тривог та інтеграції

Сучасні розгортання Axis забезпечують більшу цінність, коли аналітика та інтеграція впроваджені ефективно. Виявлення вторгнень, перетин лінії, байдужість та спрямована аналітика підтримують проактивну безпеку. Інтеграція з контролем доступу може автоматично активувати зображення з камери, коли відбувається подія відкриття дверей, або запускати робочий процес тривоги в середовищі диспетчерської.

Критичним фактором є калібрування та управління. Занадто багато хибних тривог може знизити довіру до системи.

Кібербезпека: невід'ємний рівень у розгортанні корпоративних систем

IP-камери є кінцевими точками мережі, тому кібербезпека має бути частиною архітектури. Політики паролів, автентифікація, безпечний віддалений доступ, управління оновленнями та методи ведення журналу є важливими. За правильного проектування системи Axis можуть відповідати корпоративним вимогам безпеки.

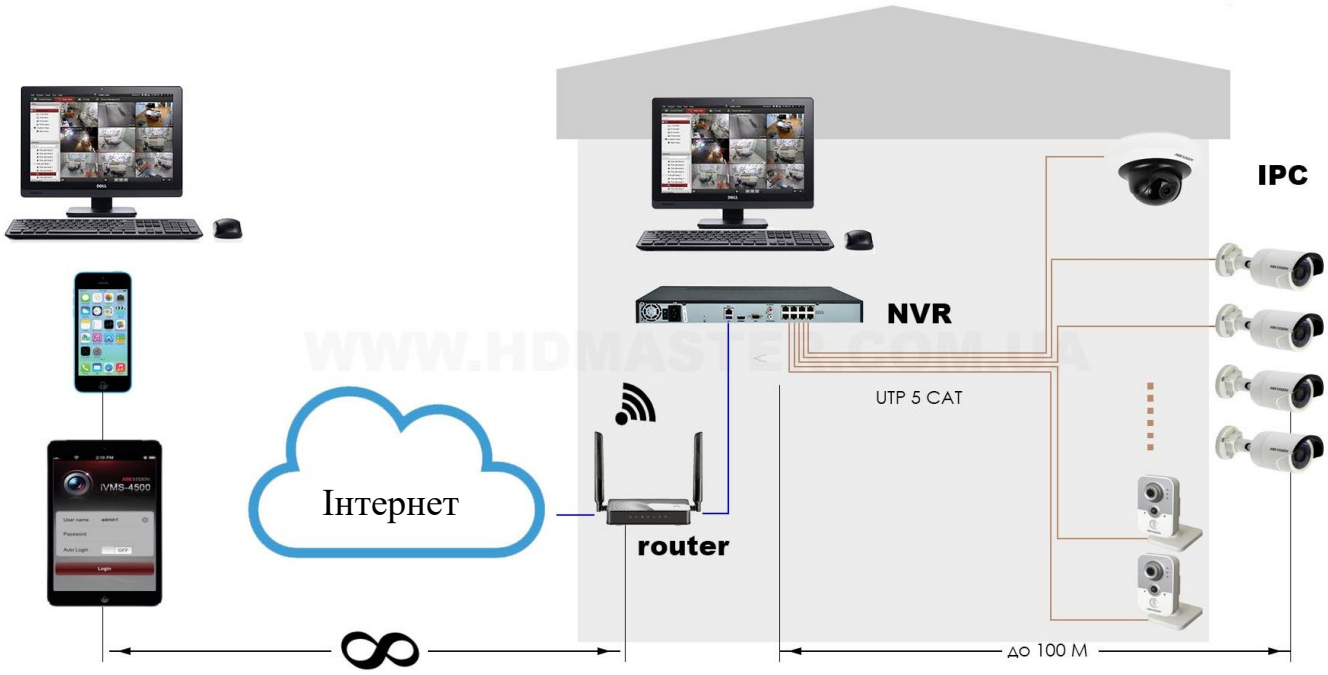


Рисунок 3.1 – Структурна схема системи

Функції камери Axis

Функції камер Axis розроблені для проектів безпеки корпоративного рівня, де вимоги виходять далеко за рамки базового запису. У середовищах B2B командам безпеки потрібні надійні зображення, масштабоване управління, робочі процеси на основі аналітики та сильна позиція в галузі кібербезпеки. Axis Communications широко визнана як еталонний бренд у сфері IP- (мережевого) відео, тому камери Axis зазвичай обираються для проектів, які надають пріоритет якості, безперервності роботи, керованості та довгостроковій

загальній вартості володіння, а не просто найнижчій початковій ціні.

Розглянемо можливості камери як частину цілісної системи. Реальна продуктивність залежить не лише від специфікації камери, але й від правильного розміщення, стратегії об'єктива, планування пропускної здатності та бітрейту, архітектури запису та інтеграції VMS. Нижче ми розглянемо найважливіші функції камер Axis та пояснимо, чому вони важливі в корпоративних розгортаннях:

1. Якість зображення та роздільна здатність. У сфері корпоративної безпеки якість зображення означає більше, ніж просто «чітке відео». Вона підтримує ідентифікацію, швидший аналіз інцидентів та кращу оперативну обізнаність. Камери Axis пропонують діапазон роздільної здатності від Full HD до 4K і вище, що дозволяє використовувати різні стратегії проектування для різних зон. Однак самої роздільної здатності недостатньо. Оптика, поле зору, висота встановлення та умови освітлення визначають, чи дійсно захоплене відео відповідатиме меті безпеки.

2. Робота в умовах низької освітленості та нічна зйомка. Багато критично важливих зон працюють у складних умовах освітлення: парковки, складські коридори, периметральні зони та виробничі зони, що працюють у нічні зміни. Ключовою особливістю камер Axis є здатність підтримувати стабільне зображення за умов слабкого освітлення, що допомагає зменшити шум, зберегти контрастність та підвищити ймовірність успішної ідентифікації під час інцидентів. Висока продуктивність за умов слабкого освітлення часто стає вирішальним фактором для критично важливих розгортань.

3. Стиснення відео, контроль бітрейту та ефективність зберігання. IP-відеопроекти повинні мати баланс між пропускною здатністю, сховищем та якістю. Камери Axis підтримують сучасні опції стиснення та механізми оптимізації бітрейту, які допомагають зменшити навантаження на мережу та витрати на сховище без шкоди для необхідного рівня деталізації. Для корпоративних проєктів метою рідко є «максимальна якість скрізь». Натомість, метою є побудова оптимізованого балансу якості та вартості на основі рівнів

ризику та операційних потреб на всьому об'єкті.

4. Відеоаналітика та інтелектуальні робочі процеси. Функції камер Axis стають значно ціннішими, коли аналітика розгортається правильно. Аналітика може запускати сповіщення для таких сценаріїв, як перетин лінії, вторгнення в зону, байдикування або аномальні моделі руху. Це зменшує навантаження на безперервний ручний моніторинг і забезпечує швидше реагування. З точки зору інтегратора, ключовим є калібрування: аналітика повинна бути налаштована на середовище, щоб уникнути надмірної кількості хибних тривог, які можуть знизити довіру до системи.

5. Кібербезпека та надійність підприємства. IP-камери – це кінцеві точки, підключені до мережі, що робить кібербезпеку основним критерієм вибору. Корпоративні розгортання часто обирають Axis завдяки її інженерному підходу, орієнтованому на безпеку. Методи контролю доступу, варіанти автентифікації, політики паролів та послідовна дисципліна оновлень підтримують відповідність корпоративним стандартам IT-безпеки. У багатьох організаціях готовність до кібербезпеки є невід'ємною вимогою для затвердження будь-якої платформи відеоспостереження.

6. Інтеграція та сумісність з відкритою платформою. У проектах B2B камери рідко працюють як ізольовані пристрої. Вони інтегровані в системи контролю доступу, сигналізації, розпізнавання номерних знаків, пожежні системи, платформи управління будівлями та процедури диспетчерської. Камери Axis розроблені для інтеграції, допомагаючи організаціям уникнути прив'язки до постачальника та забезпечуючи майбутнє розширення в міру розвитку операційних потреб.

7. Довговічність, варіанти житла та придатність для польових умов. Реальні розгортання включають реальні середовища: вплив погодних умов на відкритому повітрі, пил, перепади температур, ризик вандалізму в громадських місцях та промислові умови, такі як вібрація або вплив хімічних речовин. Правильний вибір корпусу та кріплення знижує рівень відмов та знижує довгострокові витрати на обслуговування. Вибір правильного форм-фактора для

кожної зони є практичною, але важливою рисою успішного дизайну.

8. Централізоване управління та операційна ефективність. Операційне управління є основним фактором витрат у сфері безпеки підприємства. Ручний моніторинг сотень камер неефективний. Розгортання систем Axis, якщо вони побудовані з правильною програмною архітектурою, забезпечують централізований моніторинг, дозволи на основі ролей, політики запису та робочі процеси звітності. Це допомагає командам безпеки перейти від «спостереження за екранами» до «керування інцидентами» з вимірним підвищенням ефективності.

3.3 Розробка функціональної схеми

На рисунку 3.2 наведено функціональну схему розробленої системи. Початковою ланкою в архітектурі комплексу є цільовий об'єкт або контрольований сектор, за яким здійснюється безперервний відеомоніторинг. Збір даних реалізується за допомогою мережевих відеокамер виробництва компанії Axis відповідно до структурної схеми (рисунок 3.1) із застосуванням фірмового локального обладнання. Відеопотоки та телеметрія надходять до оперативного центру (кімнати операторів), де обробляються на центральному сервері за допомогою розробленого програмного забезпечення.

Процес обробки включає первинне приймання, буферизацію та подальший аналіз інформаційних потоків. Усі зафіксовані дані архівуються у файловому сховищі у форматі .avi. Для організації впорядкованого зберігання інформація автоматично сортується за добовими каталогами відповідно до шаблону іменування ДЕНЬ_МІСЯЦЬ_РІК. Зміна конфігураційних параметрів системи, налаштування датчиків та доступ до довідкової документації здійснюються через спеціалізовані діалогові вікна інтерфейсу.

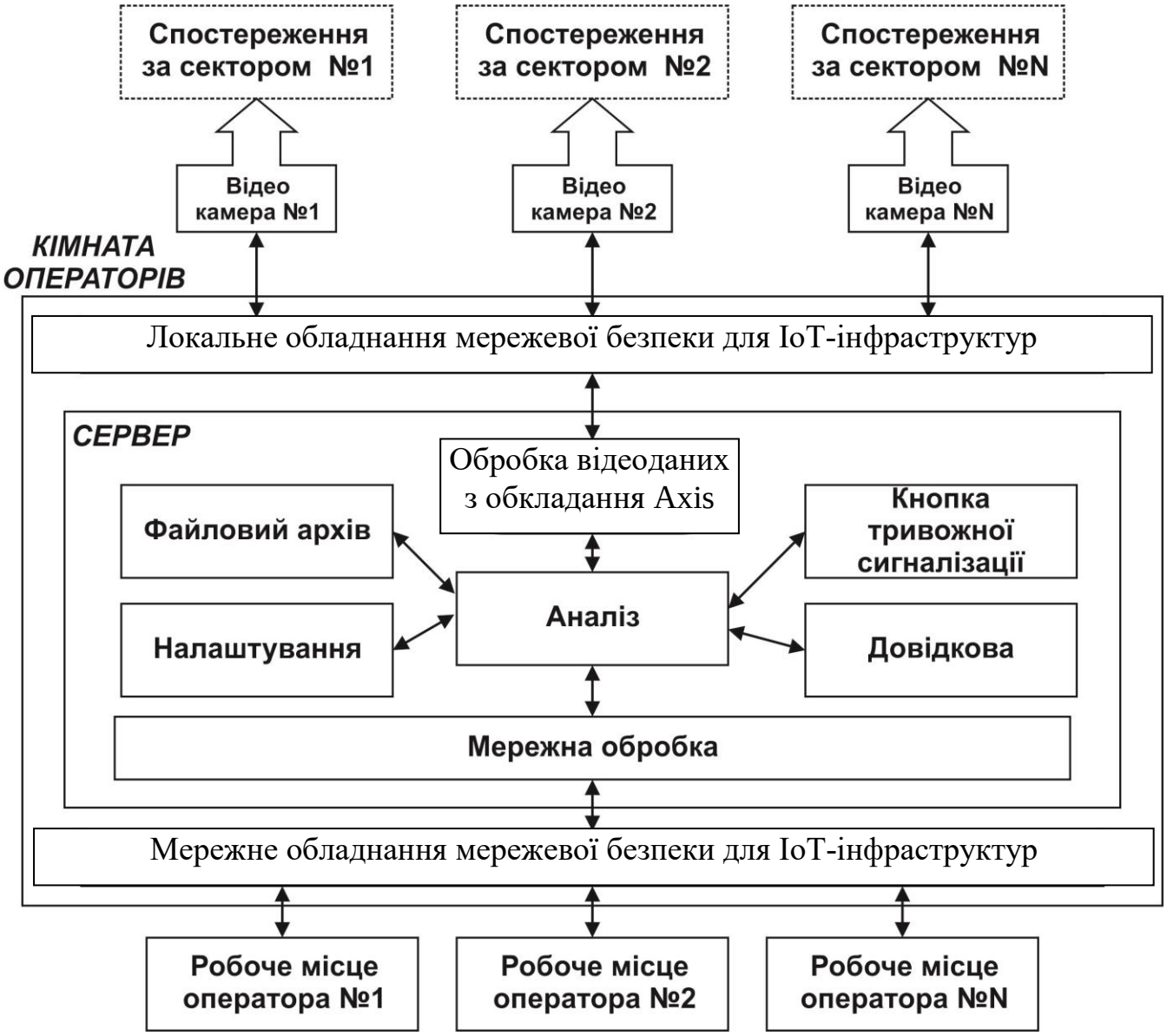


Рисунок 3.2 – Функціональна схема системи

З метою забезпечення масштабованості архітектури та контролю дій персоналу відеопотоки через мережеве обладнання Axis також ретранслюються на віддалені робочі місця керівництва. Під час проєктування апаратно-програмної частини комплексу враховувалися економічні чинники, а також специфічні кліматичні та експлуатаційні умови України. Зокрема, для розгортання в неконтрольованих або відкритих середовищах обрано відеокамери у вандалозахищеному (ударостійкому) виконанні з розширеним діапазоном робочих температур (від -40°C до +55°C) та широкими кутами огляду.

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

3.4 Розробка діаграми процесів

На рисунку 3.3 наведено діаграму процесів даних розробленої системи, детальний розгляд якої дозволяє простежити логіку взаємодії її функціональних компонентів. У процесі проєктування використовується структурний підхід та графічне представлення інформаційних потоків у системі (Data Flow Diagram, DFD), що дає змогу ефективно візуалізувати процеси обробки та передачі даних.

Згідно з інженерною методологією, розробка розпочинається з побудови контекстної діаграми (діаграми нульового рівня), яка визначає глобальні межі системи та зовнішні інтерфейси. Надалі ця модель підлягає ітераційній декомпозиції шляхом деталізації базових процесів і потоків даних з метою повного відображення архітектури розроблюваного програмно-апаратного комплексу. Завдяки застосуванню існуючих методів та інтеграції з обладнанням виробництва Axis, було створено ефективну систему мережевої безпеки для IoT-інфраструктур на базі відкритих API, яка забезпечує високий рівень захищеності контрольованих об'єктів. Мережеві камери Axis гарантують стабільно високу якість зображення у стандарті HDTV незалежно від рівня освітлення та зовнішніх умов експлуатації. Впровадження інноваційних алгоритмів стиснення дозволяє оптимізувати обсяги переданого трафіку та знизити вимоги до дискового простору для зберігання архівів, що сприяє загальній енергоефективності комплексу. Розроблене у межах цієї роботи спеціалізоване програмне забезпечення для аналізу відеоматеріалів перетворює стандартні мережеві камери на інструменти автоматизованого управління та безпеки. Комплекс забезпечує попередження операторів про нештатні ситуації, що розвиваються, сприяє прийняттю обґрунтованих управлінських рішень та оптимізації розподілу ресурсів, а також підтримує відкриту інтеграцію з іншими субсистемними елементами об'єкта.

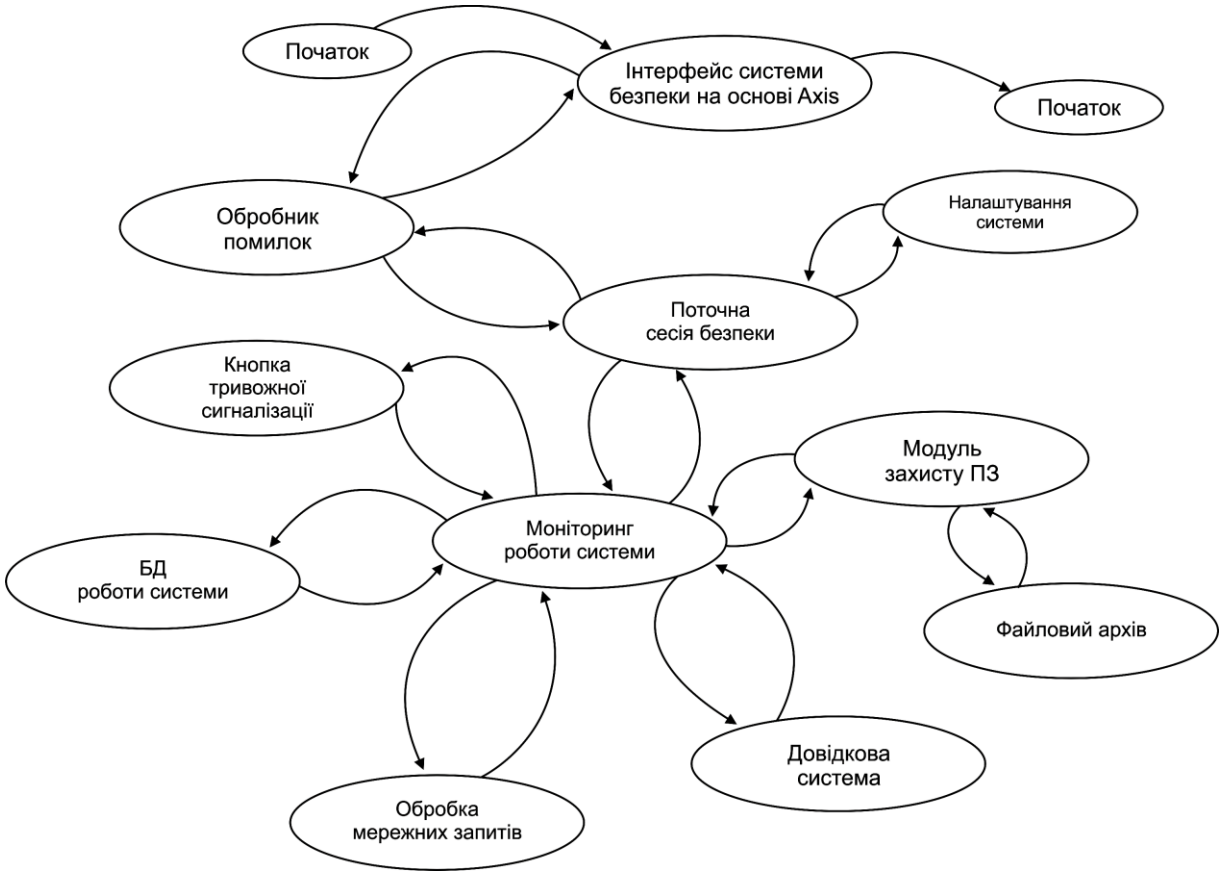


Рисунок 3.3 – Діаграма взаємодії процесів

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

Забезпечення мережевої безпеки IoT-інфраструктур потребує комплексного контролю підключених пристроїв, параметрів їхньої взаємодії та подій, які виникають під час експлуатації.

Особливістю таких інфраструктур є використання обладнання з різними апаратними можливостями, версіями системного програмного забезпечення та наборами мережевих сервісів.

Для організації централізованого захисту доцільно застосувати відкриті програмні інтерфейси, які дозволяють отримувати відомості про пристрої, контролювати їхню конфігурацію та виконувати дозволені операції керування.

Алгоритмічне забезпечення системи повинно охоплювати виявлення пристроїв, перевірку налаштувань безпеки, аналіз мережевих подій, оцінювання потенційних загроз і формування керувальних дій.

Основою запропонованого проєктного рішення є використання технологій Axis, зокрема відкритого програмного інтерфейсу VAPIX. Цей інтерфейс забезпечує можливість інтеграції мережевих пристроїв Axis із зовнішніми інформаційними системами.

Загальну блок-схему функціонування програмного комплексу передбачено на рисунку 4.1. Вона відображає послідовність отримання відомостей про IoT-обладнання, перевірки конфігурацій, аналізу подій безпеки та підготовки заходів реагування.

Застосування централізованого керування дозволяє відокремити алгоритми аналізу від конкретних способів взаємодії з обладнанням.

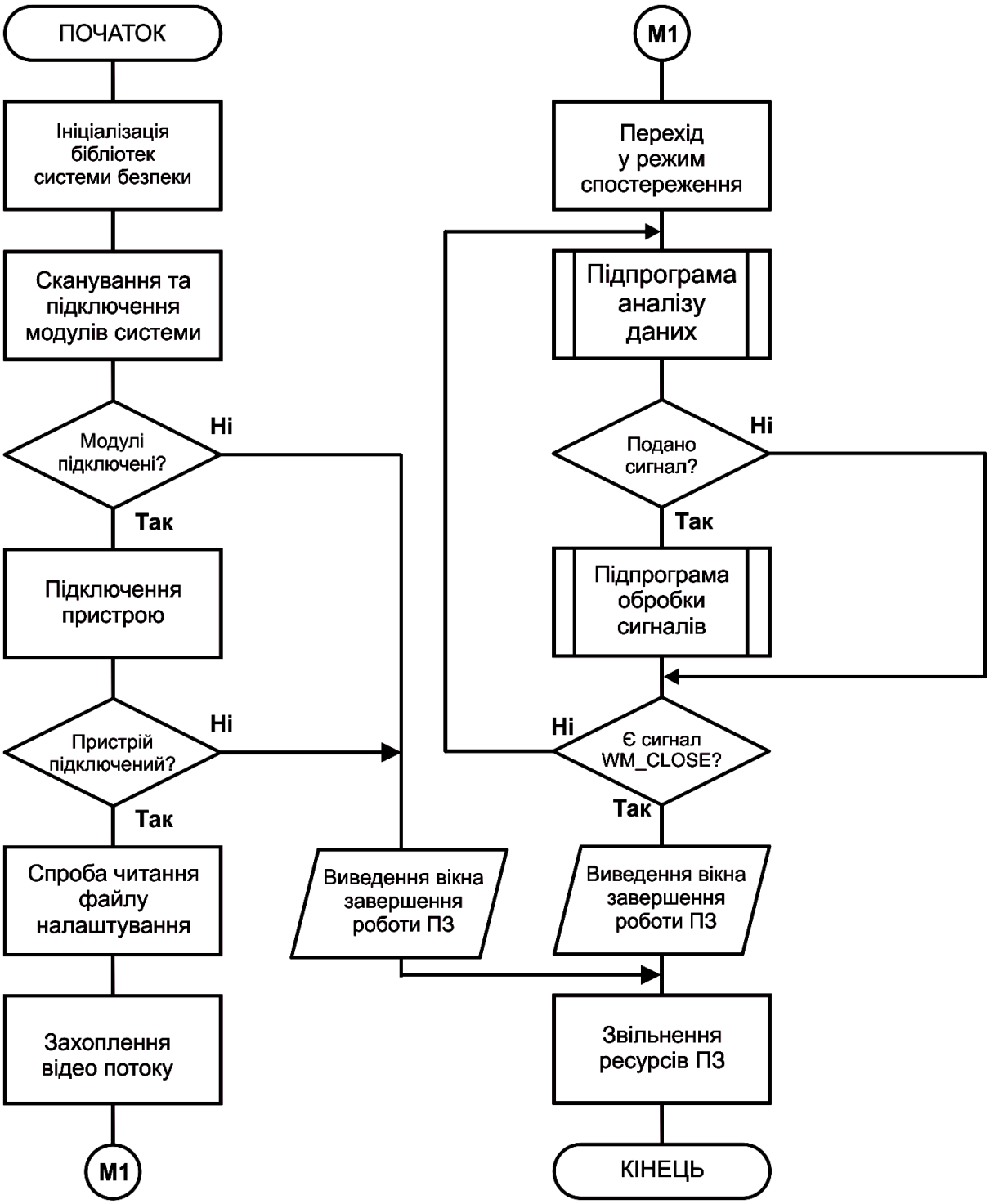


Рисунок 4.1 – Блок-схема основної програми

Вхідними даними системи є мережеві адреси пристроїв, відомості про їхні програмні інтерфейси, параметри автентифікації, характеристики активних служб, та повідомлення про події.

Додатково використовуються правила безпеки, які визначають дозволені протоколи, режими доступу та вимоги до конфігурації. Результатами роботи є актуалізована модель IoT-інфраструктури, перелік виявлених невідповідностей, оцінки ризиків і сформовані рекомендації або дозволені керувальні операції. За відсутності достатніх повноважень система повинна зберігати можливість аналізу доступних відомостей без виконання змін.

Для реалізації механізмів контролю пропонується виділити підпрограму порівняння поточних параметрів пристрою з еталонною політикою безпеки. Її алгоритмічне представлення передбачено на рисунку 4.2.

Підпрограма отримує нормалізований опис конфігурації, визначає відхилення та встановлює їхню значущість.

На підставі результатів формується рішення щодо необхідності повідомлення адміністратора або підготовки коригувальних операцій. Така організація дозволяє розглядати окремо виявлення порушень і безпосереднє застосування змін.

Побудова моделі IoT-інфраструктури та інтеграція з відкритими API Axis

Початковим етапом функціонування системи є формування актуального переліку мережевих пристроїв. До складу контрольованої IoT-інфраструктури можуть входити IP-камери, мережеві переговорні пристрої, аудіосистеми, радари, контролери доступу та інші компоненти. Необхідно враховувати, що їхня функціональність відрізняється. Окремі можливості VAPIX підтримуються лише визначеними категоріями пристроїв або версіями.

Виявлення обладнання доцільно здійснювати на основі попередньо сформованого реєстру адрес або відомостей із системи обліку мережевих ресурсів. Для кожної адреси виконується перевірка доступності керувального інтерфейсу. Після встановлення захищеного з'єднання система ініціює автентифікацію та отримує ідентифікаційні характеристики пристрою.

Масове опитування необхідно обмежувати за кількістю одночасних з'єднань, щоб запобігати додатковому навантаженню на IoT-обладнання.

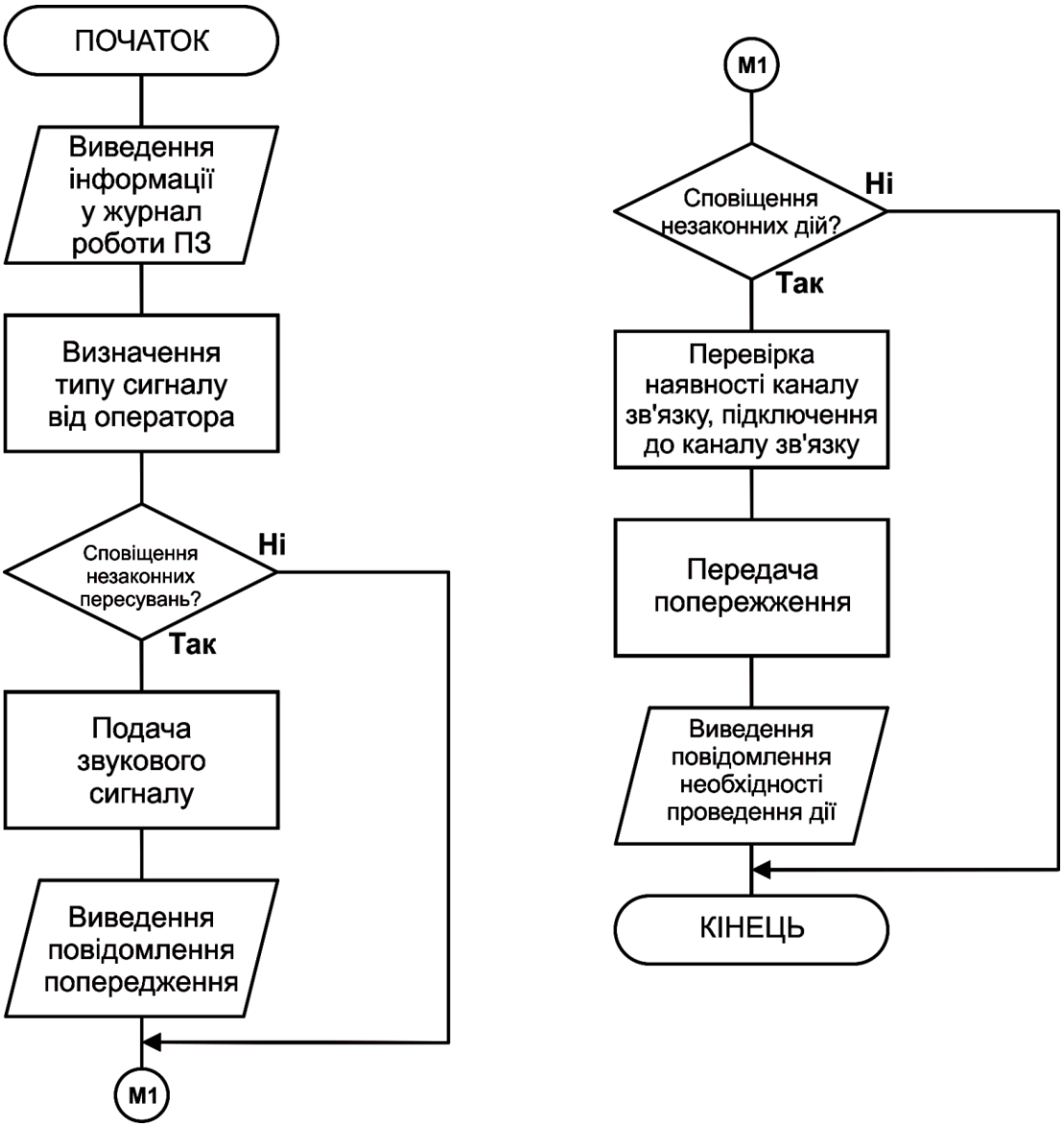


Рисунок 4.2 – Блок-схема роботи підпрограми

Для отримання відомостей про пристрій може використовуватися VAPIX Basic device information API. Він передбачає методи getProperties, getAllProperties, getAllUnrestrictedProperties і getSupportedVersions.

Отримані дані дозволяють визначати доступні характеристики обладнання та використовувати їх у внутрішній інформаційній моделі. Підтримка цього API залежить від версії програмного забезпечення конкретного пристрою.

Важливою складовою інтеграції є визначення підтримуваних програмних інтерфейсів. Для цього Axis передбачає API Discovery service, який дозволяє отримувати перелік доступних API та їхніх версій. Зокрема, використовуються

методи getApiList і getSupportedVersions. Цей механізм застосовується лише за умови його підтримки пристроєм. Для старішого обладнання необхідно передбачити окремі процедури визначення доступних функцій.

Результатом виявлення є інформаційний запис пристрою, який містить унікальний ідентифікатор, адресу керування, тип обладнання, версію системного програмного забезпечення та перелік доступних можливостей. Окремо зберігаються час останнього успішного опитування та поточний стан з'єднання. Така структура дозволяє відрізняти тимчасову недоступність обладнання від його відсутності в інфраструктурі.

Формально множину контрольованих пристроїв можна представити співвідношенням

$$D = \{d_1, d_2, \dots, d_N\},$$

де N є кількістю зареєстрованих пристроїв. Кожен елемент множини описується набором характеристик

$$d_i = (id_i, a_i, m_i, v_i, c_i, s_i, t_i),$$

де id_i є ідентифікатором пристрою, a_i визначає адресу керування, m_i характеризує модель обладнання, v_i позначає версію AXIS, c_i містить перелік підтримуваних можливостей, s_i відображає поточний стан, а t_i є часом останнього оновлення відомостей.

Для аналізу взаємодії пристроїв доцільно використовувати графову модель мережевої інфраструктури

$$G = (D, E),$$

де E є множиною зв'язків між пристроями та іншими компонентами мережі. Зв'язки можуть відображати підключення до комутатора, належність до VLAN, використання спільного сервера керування або взаємодію із зовнішньою інформаційною системою.

Необхідно враховувати, що VAPIX не є універсальним джерелом інформації про всю мережеву топологію. Відомості про фізичні підключення та мережеві сегменти доцільно отримувати від керованих комутаторів або інших

систем обліку. Програмне забезпечення повинно об'єднувати ці дані за стабільними ідентифікаторами та перевіряти їхню актуальність.

Для пристроїв Axis із підтримкою відповідних версій можна використовувати Device Configuration APIs. Ці інтерфейси надають структурований доступ до параметрів конфігурації через REST. Доступні API та їхні можливості визначаються конкретною моделлю й версією системного програмного забезпечення. Системі необхідно перевіряти підтримку відповідних операцій перед їх викликом.

У процесі інтеграції доцільно створити програмний адаптер, який забезпечує уніфіковане представлення результатів запитів. Адаптер повинен відповідати за формування HTTPS-з'єднання, автентифікацію, надсилання запиту, перевірку отриманої відповіді та перетворення даних у внутрішню структуру.

Для різних класів пристроїв можуть застосовуватися спеціалізовані адаптери. Загальний модуль обліку ресурсів повинен використовувати єдиний внутрішній інтерфейс незалежно від конкретного способу отримання характеристик. Це дозволяє доповнювати систему підтримкою нового обладнання без зміни основних алгоритмів аналізу.

Важливим обмеженням є заборона необґрунтованої зміни конфігурації під час первинного виявлення пристроїв. Початкове опитування повинно виконуватися в режимі читання. Операції, які змінюють мережеві адреси, параметри автентифікації або стан служб, необхідно відокремити від процедури інвентаризації та виконувати лише після перевірки повноважень.

Реалізація контролю конфігурацій і визначення відхилень від політики безпеки

Після формування інформаційної моделі наступним етапом є аналіз налаштувань пристроїв. Його метою є виявлення параметрів, які не відповідають прийнятій політиці мережевої безпеки. Перевірка повинна враховувати особливості обладнання, оскільки однакові правила не завжди можуть застосовуватися до камер, контролерів доступу та мережевих аудіопристроїв.

Політику безпеки доцільно представити набором правил, кожне з яких визначає характеристику конфігурації, очікуване значення та рівень важливості. До контрольованих характеристик можуть належати використання HTTPS, стан незахищених служб, доступність механізмів IEEE 802.1X, правила обмеження доступу та налаштування журналювання. Окремо необхідно контролювати чинність сертифікатів і актуальність системного програмного забезпечення.

Для побудови еталонного профілю доцільно враховувати рекомендації щодо захищеного налаштування. Зокрема, для пристроїв із відповідною підтримкою передбачаються засоби HTTPS, IEEE 802.1X, мережеві обмеження, захищене журналювання та інші механізми. Їхня наявність не означає, що всі ці функції доступні одночасно на кожній моделі.

Перевірку конфігурації необхідно виконувати після отримання актуальних значень параметрів. Якщо потрібна характеристика недоступна через API, результат не слід автоматично трактувати як порушення. Для таких ситуацій доцільно передбачити окремий стан UNKNOWN, який означає недостатність інформації для прийняття рішення.

Множину правил політики можна визначити як

$$P = \{p_1, p_2, \dots, p_M\},$$

де M є кількістю правил, що застосовуються до відповідної категорії обладнання.

Для кожного правила визначається результат перевірки

$$r_{ij} = \begin{cases} 0, & \text{вимогу виконано,} \\ 1, & \text{виявлено порушення,} \\ u, & \text{результат невизначений,} \end{cases}$$

де $r_{(ij)}$ характеризує виконання правила j для пристрою i, а u позначає неможливість достовірної оцінки.

Такий підхід дозволяє відокремлювати підтверджені порушення від ситуацій, коли пристрій тимчасово недоступний або не підтримує необхідну функцію. Для правил, які не застосовуються до відповідного типу обладнання, доцільно використовувати окремий стан NOT_APPLICABLE.

Для програмної реалізації перевірки конфігурацій можна застосувати Python із використанням структурованих об'єктів. Наведений фрагмент демонструє можливий механізм порівняння отриманих параметрів з еталонними значеннями.

```
from dataclasses import dataclass
from typing import Any


@dataclass
class SecurityRequirement:
    # Опис окремої вимоги політики безпеки
    parameter: str
    expected: Any
    severity: int

def verify_configuration(
    configuration: dict,
    requirements: list[SecurityRequirement],
    supported_parameters: set[str]
) -> list[dict]:
    # Накопичуємо результати перевірки
    results = []
    for requirement in requirements:
        name = requirement.parameter
       # Перевіряємо підтримку характеристики пристроєм
        if name not in supported_parameters:
            status = "NOT_APPLICABLE"
       # Відрізняємо відсутність даних від порушення
        elif name not in configuration:
            status = "UNKNOWN"
        # Порівнюємо фактичне та очікуване значення
        elif configuration[name] == requirement.expected:
            status = "COMPLIANT"
        else:
            status = "VIOLATION"
        results.append({
            "parameter": name,
            "status": status,
            "severity": requirement.severity
        })
    return results
```

Наведений алгоритм дозволяє класифікувати результати перевірки без безпосереднього звернення до обладнання. Значення конфігураційних параметрів повинні надходити від відповідних адаптерів Axis. Поле supported_parameters містить лише ті характеристики, підтримка яких попередньо підтверджена.

Часова складність алгоритму становить $O(M)$ за умови використання словника та множини з очікуваним сталим часом пошуку. Для інфраструктури з N пристроїв загальна кількість перевірок у найпростішому випадку

пропорційна $N \cdot M$. Фактична тривалість аналізу може визначатися переважно затримками мережевих API, а не локальними обчисленнями.

Окремо необхідно розробити механізм виявлення змін конфігурації. Для цього поточний стан порівнюється з попереднім підтвердженим знімком. Якщо параметр змінився без відповідного адміністративного запиту, система створює подію конфігураційного відхилення.

Такий механізм дозволяє виявляти не лише початково небезпечні налаштування, а й порушення, що виникли під час експлуатації. Наприклад, повторна активація незахищеної служби або зміна параметрів мережевого доступу може бути виявлена під час чергової синхронізації.

Для забезпечення правильності порівняння необхідно виключити нестабільні характеристики. До них можуть належати лічильники активності, поточне навантаження та тимчасові мережеві параметри. Включення таких показників до контрольної конфігурації призводитиме до формування великої кількості незначущих повідомлень.

Після виявлення відхилення система повинна визначити його вплив на безпеку та можливість автоматичного виправлення. Не всі порушення слід усувати без участі адміністратора. Зміна мережевих параметрів або налаштувань автентифікації може спричинити втрату доступу до обладнання. Тому для таких операцій необхідно застосовувати окрему процедуру погодження та перевірки наслідків.

Організація централізованого збирання та кореляції подій безпеки

Для реалізації цього механізму можна використати структуру deque, яка дозволяє ефективно додавати нові часові мітки та видаляти застарілі записи. Наведений фрагмент Python демонструє оброблення попередньо нормалізованих подій одного безпекового типу.

```
from collections import defaultdict, deque

class SecurityEventCorrelator:
    def __init__(self, window_seconds=60, threshold=5):
        # Тривалість вікна та поріг спрацювання
        if window_seconds <= 0 or threshold <= 0:
            raise ValueError("Некоректні параметри")
```

```
        self.window = window_seconds
        self.threshold = threshold
        # Окреме вікно для кожного пристрою
        self.events = defaultdict(deque)
    def process(self, device_id: str, timestamp: float):
        # timestamp є часом у секундах UTC
        history = self.events[device_id]
        # Додаємо нову подію у часове вікно
        history.append(timestamp)
        # Видаляємо повідомлення поза межами вікна
        cutoff = timestamp - self.window
        while history and history[0] < cutoff:
            history.popleft()
        # Перевіряємо перевищення заданого порога
        if len(history) >= self.threshold:
            return {
                "device_id": device_id,
                "event": "SECURITY_THRESHOLD_EXCEEDED",
                "count": len(history),
                "timestamp": timestamp
            }
        return None
```

Наведений алгоритм розрахований на надходження подій у неспадному часовому порядку для кожного пристрою. У разі отримання повідомлень із затримкою необхідно передбачити додаткове впорядкування та допустиме запізнення. Інакше події, які надходять не за часовою послідовністю, можуть призводити до некоректного підрахунку.

Крім того, фрагмент формує результат для кожної наступної події після досягнення порога. Для практичної системи його необхідно доповнити механізмом пригнічення повторних сповіщень. Один інцидент не повинен створювати необмежену кількість однакових повідомлень, якщо небезпечна активність триває.

Під час розроблення правил кореляції важливо уникати ототожнення аномальної активності з підтвердженим порушенням безпеки. Наприклад, значна кількість невдалих автентифікацій може бути наслідком застарілого пароля в системі керування. Тому результат алгоритму слід розглядати як підставу для подальшої перевірки. Для підвищення точності доцільно використовувати комбіновані правила. Вони можуть враховувати кількість подій, зміну конфігурації, невідповідність мережевої адреси та час останнього успішного підключення. Використання декількох незалежних характеристик дозволяє формувати більш обґрунтовані рішення щодо потенційних загроз.

Математична модель оцінювання ризику для IoT-пристроїв

Виявлені порушення можуть відрізнятися за впливом на безпеку інфраструктури. Наприклад, недоступність допоміжного сервісу не обов'язково створює такий самий ризик, як неконтрольований доступ до інтерфейсу адміністрування. Тому для визначення черговості реагування необхідно застосувати механізм кількісного оцінювання.

Для кожного пристрою пропонується формувати інтегральну оцінку, яка враховує результати перевірки конфігурації, наявність підозрілих подій, важливість пристрою та ступінь його мережевої доступності.

Узагальнену функцію ризику можна подати співвідношенням

$$R_i = \alpha C_i + \beta E_i + \gamma A_i + \delta V_i,$$

де C_i характеризує рівень конфігураційних порушень, E_i є оцінкою підозрілих подій, A_i визначає ступінь доступності пристрою з потенційно небезпечних мережевих сегментів, а V_i відображає ризик, пов'язаний із відомими вразливостями.

Коефіцієнти α, β, γ та δ задають відносну значущість компонентів. Для отримання порівнянних результатів їх можна нормувати за умовою

$$\alpha + \beta + \gamma + \delta = 1.$$

Кожен показник доцільно приводити до інтервалу від 0 до 1. У такому випадку інтегральне значення також перебуватиме в цьому інтервалі.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Програмне забезпечення системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis призначене для централізованого контролю підключених пристроїв, перевірки їхніх конфігурацій та виявлення потенційних порушень інформаційної безпеки.

Основними функціями системи є інвентаризація обладнання, отримання відомостей через програмні інтерфейси VAPIX, аналіз подій, оцінювання ризиків і формування заходів реагування.

Програма орієнтована на взаємодію з пристроями під керуванням AXIS та забезпечення єдиного середовища адміністрування. Головне вікно програми показано на рисунку 5.1.

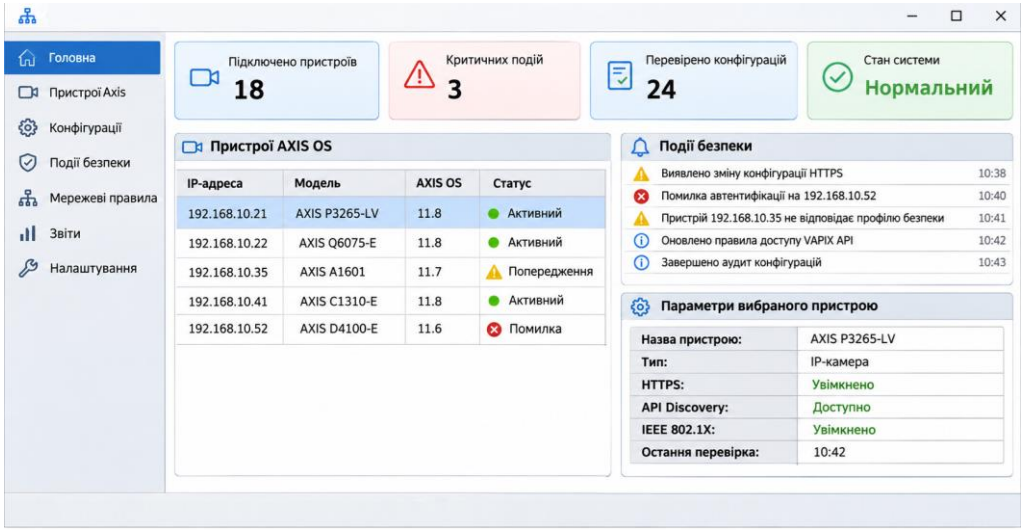


Рисунок 5.1 – Головне вікно ПЗ

Робоче середовище системи передбачає використання центрального сервера керування, мережевих пристроїв Axis і робочих станцій адміністраторів. Пристрої IoT підключаються до локальної мережі через комутатори та

взаємодіють із сервером за допомогою підтримуваних програмних інтерфейсів. Серверна частина відповідає за отримання конфігураційних параметрів, оброблення подій і виконання алгоритмів контролю безпеки. Користувацький інтерфейс забезпечує доступ до результатів аналізу та дозволених операцій керування. Для реалізації серверної частини доцільно використовувати мову Python, яка застосовується в алгоритмічній моделі системи. Вона забезпечує оброблення структурованих даних, виконання перевірок конфігурацій і формування керувальних запитів.

Як основу серверного API можна застосувати FastAPI. Взаємодія з обладнанням Axis організовується через VAPIX. Для зберігання відомостей про пристрої, політики безпеки, результати перевірок і зареєстровані події може використовуватися PostgreSQL. Зазначений склад компонентів є рекомендованим варіантом програмної реалізації.

Як серверну платформу доцільно використовувати операційну систему Linux із підтримкою необхідного середовища виконання Python. Апаратні характеристики сервера визначаються кількістю контрольованих IoT-пристроїв, частотою їх опитування та інтенсивністю надходження подій. Для клієнтського доступу може використовуватися робоча станція із сучасним веббраузером. Обов'язковою умовою функціонування є стабільне мережеве з'єднання між сервером і керувальними інтерфейсами обладнання Axis.

Підготовка середовища починається з установлення операційної системи, налаштування мережевих параметрів і перевірки доступності пристроїв. Сервер керування доцільно розміщувати в окремому адміністративному сегменті мережі. Для підключення обладнання необхідно визначити його IP-адреси та перевірити доступність HTTPS. Якщо пристрої розміщені в різних VLAN, маршрутизація між сегментами повинна забезпечувати лише необхідні керувальні з'єднання.

Доступ із недовірених мереж до адміністративних інтерфейсів обладнання потрібно обмежити.

Наступним етапом є встановлення Python і необхідних програмних бібліотек. Рекомендується створити окреме віртуальне середовище та встановити

залежності відповідно до обраної реалізації. Для HTTPS-запитів можуть застосовуватися відповідні клієнтські бібліотеки Python.

Перед запуском необхідно перевірити правильність налаштування довірених сертифікатів і доступність потрібних програмних компонентів. Версії бібліотек доцільно фіксувати для забезпечення відтворюваності розгортання.

Підготовка сховища даних передбачає створення окремої бази даних і службового облікового запису з обмеженими повноваженнями. Структура сховища повинна забезпечувати збереження ідентифікаторів пристроїв, їхніх характеристик, підтримуваних API та поточних конфігурацій. Окремо необхідно передбачити зберігання результатів перевірок політик, журналів подій і станів керувальних операцій. Перед запуском основних модулів перевіряється доступність бази даних та можливість виконання необхідних операцій.

Первинне підключення пристроїв Axis передбачає визначення параметрів автентифікації та перевірку підтримуваних програмних інтерфейсів. Для отримання характеристик обладнання може використовуватися Basic device information API. Якщо пристрій підтримує API Discovery service, система може отримувати перелік доступних API та їхніх версій. Це дозволяє визначати допустимі операції без припущень щодо функціональних можливостей конкретної моделі. Для старіших пристроїв необхідно передбачити окрему процедуру перевірки сумісності.

Особливу увагу необхідно приділити захисту службових облікових даних. Паролі та інші секрети не повинні розміщуватися безпосередньо у вихідному коді. Для інвентаризації доцільно використовувати облікові записи з мінімально необхідними повноваженнями.

Операції зміни конфігурацій повинні виконуватися лише після окремої перевірки прав доступу. Взаємодія через HTTPS має передбачати перевірку сертифікатів, а не лише встановлення зашифрованого з'єднання.

Рекомендована послідовність запуску програмного комплексу починається з перевірки працездатності бази даних і серверного застосунку. Після цього ініціалізується модуль взаємодії з пристроями Axis. Наступним кроком є запуск

інвентаризації та отримання відомостей про доступне обладнання. Після формування інформаційної моделі активуються модулі перевірки конфігурацій і збирання подій. Підсистема автоматизованого реагування повинна запускатися після перевірки правил безпеки та доступності необхідних керувальних функцій.

Початкове налаштування системи передбачає створення еталонних профілів безпеки для відповідних категорій IoT-обладнання. У профілях визначаються вимоги до використання HTTPS, параметрів автентифікації, стану мережевих служб і допустимих способів доступу. Для пристроїв, які підтримують відповідні механізми, можуть перевірятися налаштування IEEE 802.1X і локального міжмережевого екрана.

Для організації збирання подій необхідно налаштувати доступні інтерфейси повідомлень Axis та, за потреби, віддалене журналювання. Отримані події повинні приводитися до єдиного формату із зазначенням ідентифікатора пристрою, часу виникнення та типу повідомлення. Для правильного впорядкування подій необхідно забезпечити синхронізацію часу серверного обладнання та IoT-пристроїв. Після цього налаштовуються правила кореляції, порогові значення та параметри формування сповіщень.

Перевірка працездатності починається з отримання переліку підключених пристроїв та зіставлення їхніх характеристик із фактичними даними обладнання. Необхідно перевірити правильність визначення моделей. Далі виконується тестова перевірка конфігурації за попередньо визначеним профілем. Результати повинні відображати підтверджені порушення, виконані вимоги та параметри, стан яких неможливо достовірно визначити.

Наступним етапом є перевірка оброблення подій безпеки. Для цього в тестовому середовищі формуються контрольні повідомлення та перевіряється їх надходження до центрального сервера. Необхідно встановити правильність часових міток, класифікації подій і спрацювання правил кореляції. Окремо перевіряється поведінка системи за тимчасової недоступності пристрою або помилки автентифікації. Такі ситуації повинні фіксуватися без необґрунтованої зміни конфігурації обладнання.

Для ідентифікації програмного продукту та забезпечення його подальшого супроводу доцільно передбачити відображення відомостей про розробника, назву програми та її версію. Ця інформація використовується під час оновлення, технічного обслуговування й перевірки відповідності встановленого програмного забезпечення супровідній документації. Авторські дані розробленої системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis представлені на рисунку 5.2.

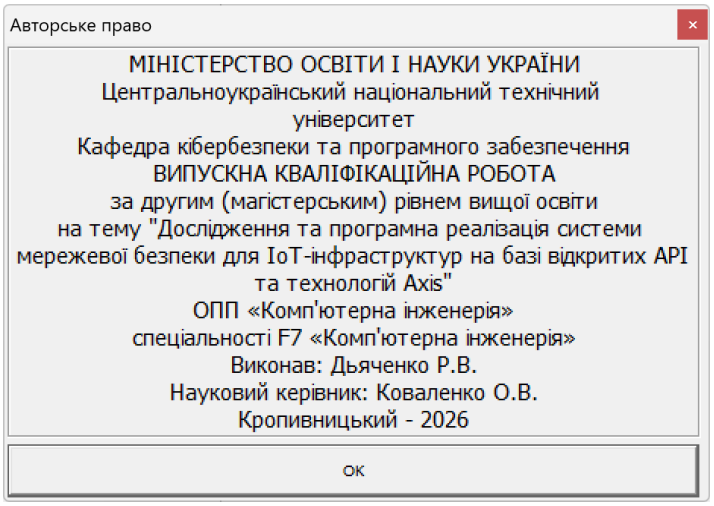


Рисунок 5.2 – Вікно авторського права

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Метою розробки є дослідження та програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Об'єктом дослідження є процес мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Предметом дослідження є методи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Методи дослідження базуються на методах Інтернету речей, методах комп'ютерних мереж, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

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

– Удосконалено метод мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

– Розроблено вітчизняний продукт мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis, який має більш широкі можливості, на відміну від існуючих аналогів.

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

7.1 Вступ

Згідно із Законом України про охорону праці, маємо визначення: "Охорона праці – це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці", тож в рамках цього визначення маємо, що техніка безпеки – це система правових, соціально-економічних, організаційно-технічних та санітарно-гігієнічних заходів та засобів, спрямованих на збереження життя та здоров'я людини під час її трудової діяльності, тобто це низка заходів по створенню безпечних умов виробництва для працівників під час виконання ними своїх трудових обов'язків, а отже, відповідно державна політика України спрямована на створення належних, безпечних і здорових умов праці, запобігання нещасним випадкам та професійним захворюванням. Основою державної політики в цьому питанні є:

– пріоритет життя і здоров'я працівників, повна відповідальність роботодавця за створення належних, безпечних і здорових умов праці;

– підвищення рівня промислової безпеки шляхом забезпечення суцільного технічного контролю за станом виробництва, технологій та продукції, а також сприяння підприємствам у створенні безпечних та нешкідливих умов праці;

– комплексне розв'язання завдань охорони праці на основі загальнодержавної, галузевих, регіональних програм з цього питання та з урахуванням інших напрямів економічної і соціальної політики, досягнень в галузі науки і техніки та охорони довкілля;

– соціальний захист працівників (повне відшкодування шкоди особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань);

– встановлення єдиних вимог з охорони праці для всіх підприємств та суб'єктів підприємницької діяльності незалежно від форм власності та видів діяльності;

– адаптація трудових процесів до можливостей працівника з урахуванням його здоров'я та психологічного стану;

– пріоритет у використанні економічних методів управління охороною праці (участі держави у фінансуванні заходів щодо охорони праці, залучення добровільних внесків та інших надходжень на ці цілі, отримання яких не суперечить законодавству);

– інформування населення та проведення навчання (постійні професійні підготовки і підвищення кваліфікації працівників) з питань охорони праці;

– забезпечення координації діяльності органів державної влади, установ, організацій, об'єднань громадян, що розв'язують проблеми охорони здоров'я, гігієни та безпеки праці,

– організація співробітництва між роботодавцями та працівниками (їх представниками); між усіма соціальними групами під час прийняття рішень з охорони праці на місцевому та державному рівнях;

– світовий досвід у організації роботи щодо поліпшення умов і підвищення безпеки праці на основі міжнародного співробітництва [40,41] .

Робочим інструментом в ІТ-сфері, що є однією з найбільш перспективних галузей економіки, є комп’ютер з наявним на ньому програмним забезпеченням. Базовими основоположними законодавчими актами по охороні праці при роботі з ПК в Україні є НПАОП 0.00-7.15-18 "Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями", ДСанПіН 3.3.2.007-98 "Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин" та ДСТУ 8604:2015 "Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги", які призначені для запобігання впливу на працівників шкідливих і небезпечних факторів. До загально правової бази, що регулюють нормативно-правові положення з техніки безпеки (й для ІТ-сфері в тому числі),

відносяться Інструкції з охорони праці при роботі з електронно-обчислювальними машинами, в яких протокольно описано поводження під час штатних робіт та в аварійних ситуаціях, основним призначенням яких є запобігання наслідків (зменшення або повне їх усунення) небезпек, що пов’язані з виробничою діяльністю.

7.2 Шкідливі і небезпечні фактори при роботі з комп’ютером

Якщо послуговуватися класифікацією небезпечних й шкідливих виробничих факторів при роботі на комп’ютері по природі їх виникнення, а отже поділивши їх на наступні групи: фізичні, хімічні, психофізіологічні, біологічні, то до фізичних можемо віднести:

– підвищену й знижену температуру повітря;

– підвищену й знижену вологість повітря;

– недостатню освітленість робочого місця;

– перевищуючі припустимі норми шуму;

– підвищений рівень іонізуючого випромінювання;

– підвищений рівень електромагнітних полів;

– підвищений рівень статичної електрики;

– небезпеку враження електричним струмом;

– блякліть екрана дисплея.

До хімічних можемо віднести:

– виникнення, у результаті іонізації повітря при роботі комп'ютера, активних часток.

До психофізіологічних можемо віднести:

– розумова напруга;

– втрата реальності;

– виникнення залежності;

– нервово-емоційні перевантаження;

– перенапруга зорового аналізатора;

До біологічних можемо віднести:

– бактеріологічну небезпеку, пов’язану з наявністю місць із сприятливим середовищем їх розмноженням (наприклад клавіатура).

7.3 Аналіз санітарно-гігієнічних умов праці на робочому місці програміста

Проаналізуємо умови праці у приміщенні, в якому працюють програмісти. Геометричні розміри приміщення наведено у таблиці 7.1.

Таблиця 7.1 – Розміри приміщення

Найменування	Значення, м
Ширина	4
Довжина	5
Висота	3

Таблиця 7.2 – Площа та обсяг приміщення, на одного працюючого*

Геометрична характеристика	Одиниця виміру	Нормативне значення*	Фактичне значення
Площа, S	м²	Не менше 6.0	6,67
Об'єм, V	м³	Не менше 20.0	20

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

У зазначеному приміщенні працюють троє людей. За даними, які наведено у табл. 7.1, та табл. 7.2, можна зробити висновок, що площа та об’єм приміщення з розрахунку на одне робоче місце програміста не відповідають нормативним вимогам ДСанПіН 3.3.2-007-98 "Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-

обчислювальних машин" [42] але відповідають нормативним вимогам Наказу Міністерства соціальної політики України № 207, від 14.02.2018 "Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями" [42] та НПАОП 0.00-7.15-18 "Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями". Таким чином, можна зробити висновок, що санітарно-гігієнічні умови праці на робочому місці програміста відповідають вимогам.

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

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

У таблиці 7.3 наведено оптимальні та фактичні значення параметрів мікроклімату як для категорії ваги робіт Іа, так і розглянутого приміщення. У приміщеннях, де встановлено ЕОМ, рекомендується застосування тільки оптимальних значень показників мікроклімату.

Таблиця 7.3 – Оптимальні і фактичні значення параметрів мікроклімату

Пора року	Оптимальні для Іа			Фактичні		
	Температура, °С	Вологість, %	Швидкість повітря, м/с	Температура, °С	Вологість, %	Швидкість повітря, м/с
Холодна	22-24	40-60	0,1	22-23	40-55	0,11
Тепла	23-25	50-70	0,1	24-25	50-65	0,17

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

В літню пору застосовується кондиціонер.

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

У приміщенні знаходяться наступні джерела шуму: принтер HP LaserJet Pro P1102, електродвигуни вентиляторів ЕОМ.

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

З 2019 року діють Державні будівельні норми України ДБН В.2.5-28:2018 "Природне і штучне освітлення" [43], у яких прописані вимоги до використання всіх освітлювальних приладів, у т.ч. світлодіодних.

Працю працівника, який постійно працює за комп’ютером, згідно ДБН В.2.5-28:2018 [43], можна віднести до роботи з малою точністю (найменший розмір об'єкта розрізнення від 1 до 5 мм) V-го розряду зорової роботи, з великою контрастністю об'єкта розрізнення (символів на екрані дисплея), з темним тлом (під розряд зорової роботи В). Приміщення можна віднести до 1-ої групи приміщень, у яких проводиться розрізнення об'єктів зорової роботи при фіксованому напрямку лінії зору того, що працює на робочу поверхню. Для такого типу приміщень і розряду зорової роботи нормоване значення коефіцієнта природної освітленості (КПО) робочої поверхні (при поєднаному,

спільному освітленні), повинен становити не більше 1,5%, освітленість при штучному висвітленні повинна становити 300 Лк. [43], Крім того, все поле зору повинне бути освітлено достатньо рівномірно – це основна гігієнічна вимога. Так, як яскраве світло на ділянці периферійного зору значно збільшує напруженість очей і, як наслідок, призводить до їх швидкої стомлюваності, ступінь освітлення приміщення і яскравість екрану комп'ютера повинні бути приблизно однаковими.

7.4 Розробка заходів з умов поліпшення охорони праці

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

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

– мікроклімат відповідає нормативному значенню;

– акустичні умови роботи не перевищують нормативних значень;

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

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

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

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

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

7.5 Розрахункова частина

Завдання: Розрахувати час для евакуації людей із виробничих приміщень.

Вхідні дані:

Виробниче приміщення, яке за вибухопожежною та пожежною небезпекою належить до категорії В, розташоване в одноповерховій будівлі зі ступенем вогнетривкості І. Один центральний поздовжній проїзд шириною 3 м та два поперечних проходів шириною 1 м поділяють приміщення на дві ділянки. З одного боку проїзду встановлено ворота з дверима для проходу людей, які в умовах вимушеної евакуації відіграють роль евакуаційного виходу. У найчисленнішій зміні працює 150 працівників.

Визначити відповідність заходів евакуації людей із виробничого приміщення встановленим нормам пожежної безпеки та розрахувати можливий час евакуації.

Початкові дані:

– кількість працівників у найчисленнішій зміни – 150;
– довжина цеху a = 50 м;
– ширина цеху b = 20 м;
– висота цеху h = 3 м.

Кількість працівників, які можуть опинитися в цеху у службових справах, становить 20% від загальної кількості працівників.

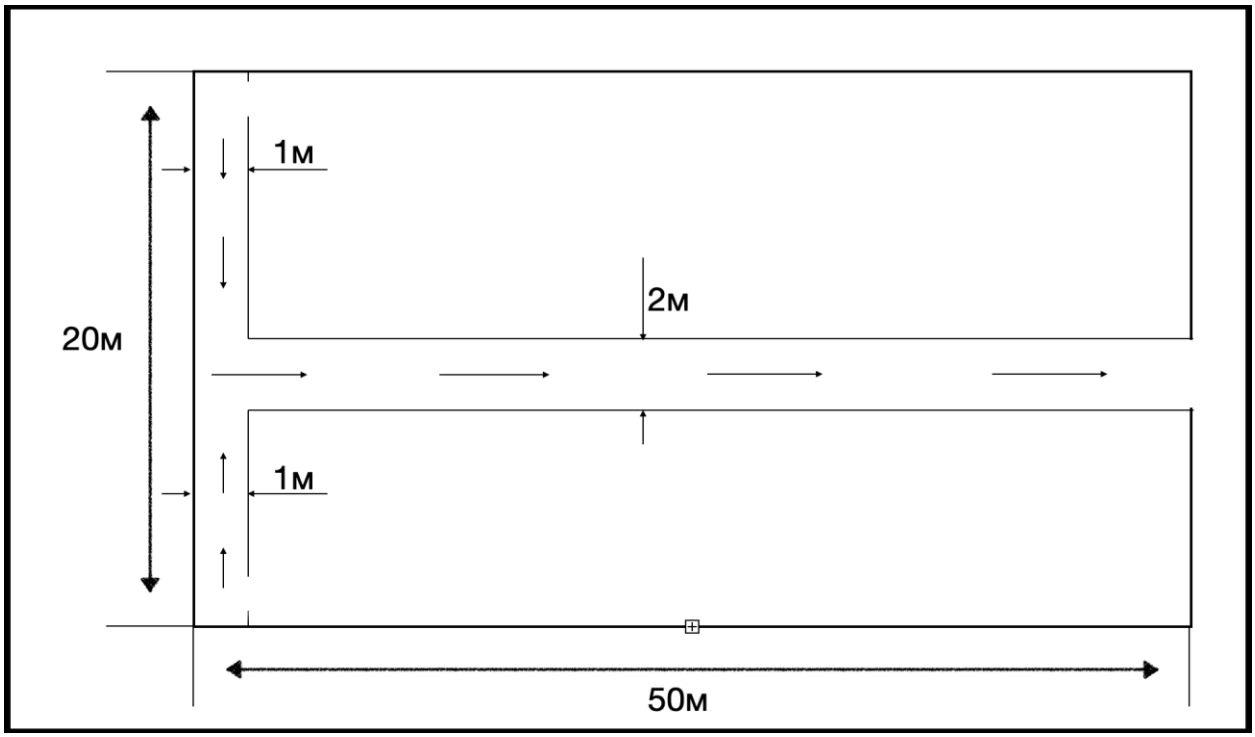


Рисунок 7.1 – Евакуаційний план

Виконаємо розрахунок.

1. Визначаємо загальну кількість працівників, які можуть перебувати в цеху:

$$150 + 0{,}2 \cdot 150 = 180.$$

2. Оскільки прохід один, то на вихід припадає 180 працівників.

3. Найвіддаленішими від евакуаційних виходів є робочі місця, відстані від яких до евакуаційних виходів однакові й становлять 60 м (10 + 50).

4. Перевіримо, чи відповідає це значення нормативним даним, регламентованим СНиП 2.09.02-85. Для цього визначимо щільність людського потоку в загальних проходах Z. Оскільки на проходи припадає 180 працівників, а їх площа від робочих місць S = 10 ·1· 2 + 50 · 2 = 120 м^2, щільність людського потоку становитиме

$$Z = \frac{N}{S} = \frac{180}{120} \approx 2{,}0 \text{ працівника/м}^2$$

Відповідно до СНиП 2.09.02-85 максимально допустима відстань від найвіддаленішого робочого місця до евакуаційного виходу з приміщення категорії В та вогнетривкості І, при такому значенні Z та об'ємі цеху 1000 м^3 становить 60 м. У даному випадку ця вимога виконується.

5. Визначимо необхідну ширину евакуаційного виходу, якщо відомо, що нормована кількість працівників на 1 м ширини такого виходу приміщення категорії В та вогнетривкості І становить 110, а на вихід припадає 180 працівників: В = 180/110 = 1,63 м; це відповідає вимозі, тому що ширина воріт, яка дорівнює ширині проїзду, становить 2 м.

6. Визначимо розрахунковий час евакуації з виробничого приміщення $t_{евак.розр}$, урахувавши, що він буде однаковий для обох ділянок. Таким чином,

$$t_{евак.\ розр} = t1 + t2$$

де t1, t2 – час евакуації працівників ділянок відповідно проходом і проїздом до виходу, хв.

7. Визначимо щільність людського потоку у проході та проїзді виробничого приміщення за формулою:

$$D1 = \frac{N1 \cdot f}{l1 \cdot \delta 1} = \frac{(180/2) \cdot 0{,}125}{10 \cdot 1} = 1{,}13 \text{ м}^2/\text{м}^2$$

$$D2 = \frac{N2 \cdot f}{l2 \cdot \delta 2} = \frac{180 \cdot 0{,}125}{50 \cdot 2} = 0{,}23 \text{ м}^2/\text{м}^2$$

За одержаними значеннями визначаємо швидкість людського потоку у проході (v1 = 15 м/хв) та проїзді цеху (v2 = 60 м/хв).

$$t1 = \frac{l1}{v1} = \frac{10}{15} = 0{,}66$$

$$t2 = \frac{l2}{v2} = \frac{50}{60} = 0{,}83$$

$$t_{евак.\ розр.} = t1 + t2 = 0{,}66 + 0{,}83 = 1{,}49 \text{ хв.}$$

Таким чином, розрахунковий час евакуації працівників із виробничого приміщення становить близько 1,5 хв.

Висновки до розділу

Дотримання всіх необхідних умов праці не лише сприяє збереженню здоров'я працівників, а також підвищує ефективність виробництва в цілому.

З цих міркувань було здійснено аналіз умов праці, призначеного для праці програмістів, проведено розгляд небезпечних та шкідливих факторів, що негативно впливають на програмістів під час роботи. Виконано розрахунок часу евакуації зі службового приміщення. Розроблено заходи з охорони праці.

8 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

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

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

– Досліджена система мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis.

Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

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

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

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

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

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

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.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дьяченко Р.В. Дослідження та програмна реалізація системи мережевої безпеки для IoT-інфраструктур на базі відкритих API та технологій Axis // Збірник праць молодих науковців ЦНТУ. – Вип. 17. – Кропивницький: ЦНТУ, 2027.

2. 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.

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

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

5. Богаченко, С., Смірнов, О., Буравченко, К., Смірнова, Т., Конопліцька-Слободенюк, О., Якименко, Н., Смірнов, С. «Обмеження ресурсів мобільних та edge-платформ при розробці програмного забезпечення для реалізації та оптимізації моделей машинного навчання». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, т. 2 № 34, С. 677-686.

6. Смірнов, О., Ткачук, Р., Козірова, Н., Константинова, Л., Конопліцька-Слободенюк, О., Якименко, Н., Смірнов, С.. «Дослідження застосування векторних баз даних у генеративному штучному інтелекті». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, Том 1 № 33, 667-682.

7. Смірнов О., Заріцкий В., Буравченко К., Конопліцька-Слободенюк О., Константинова Л., Якименко Н., Смірнов С. «Оптимізація розпізнавання облич за допомогою CUDA прискореної бібліотеки dlib». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, Том 4, № 32, С. 573-582.

8. 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.

9. 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

10. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка.* 2024. №4(24), С. 6-27.

11. 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.

12. 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.

13. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings,* Volume 3530, 2023, pp. 256-265.

14. 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.

15. 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.

16. 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,

17. 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.

18. 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

19. 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.

20. 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.

21. 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.

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

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. Zhurakovskyi, B., Tsopa, N., Batrak, Y., Odarchenko, R., Smirnova, T «Comparative analysis of modern formats of lossy audio compression». Workshop Proceedings, 2020, 2654, стр. 315-327.

32. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

41. Т.В. Смірнова, О.М. Дрєєв, О.А. Смірнов «Хмарна інформаційна система оцінювання шорсткості з використанням дискретного частотного аналізу макрофотографій». IV міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", м. Кропивницький. 15-16 квітня 2021р. – Кропивницький: ЦНТУ. – 2021. – С. 30.

42. 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.

43. 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.

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

45. 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.

46. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.

47. 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).

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

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

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

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

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

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

54. Смірнов О.А., Дрєєв О.М. Порівняння бітових щільностей при використанні різних методів кодування інформації. Збірник тез VI міжнародної науково-практичної конференції "Проблеми та перспективи розвитку ІТ-

індустрії”. м. Харків. 17-18 квітня 2014р. – Харків: ХНЄУ. – 2014. – С. 240.

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

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

57. Смірнов О.А., Доренський О.П., Дрєєв 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.

58. 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.