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

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“____” _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за першим (бакалаврським) рівнем вищої освіти
на тему
“Програмне забезпечення системи мережевого комплексного засобу відеонагляду для підприємства”

Виконав здобувач вищої освіти
IV курсу, групи КІ-22-1
ОПП «Комп’ютерна інженерія»
спеціальності 123 «Комп’ютерна інженерія»
_____ Андрюшков Д.В.
«____» _____ 2026 р.

Керівник проекту
доктор філософії (PhD)
_____ Усік П.С.
«____» _____ 2026 р.
Рецензент _____
_____

м. Кропивницький

Центральноукраїнський національний технічний університет
Факультет *Механіко-технологічний*
Кафедра *Кібербезпеки та програмного забезпечення*
Освітній ступінь *бакалавр*
Галузь знань ._12 _____*“Інформаційні технології”*_____
Спеціальність 123 *“Комп’ютерна інженерія”*
Освітньо-професійна (освітньо-наукова) програма _*“Комп’ютерна інженерія”*_

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

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

Андрюшкову Дмитру Валерійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи *Програмне забезпечення системи мережевого комплексного засобу відеонагляду для підприємства*

2. Керівник роботи *Усік Павло Сергійович, доктор філософії (PhD)*
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 133-02 від 27.02.2026 року

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

4. Мета та завдання випускної кваліфікаційної роботи*: Метою роботи є розробка програмного забезпечення системи мережевого комплексного засобу відеонагляду для підприємства*

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

1. Призначення та область використання.
2.Перегляд аналогічних існуючих систем.
3. Опис і обґрунтування проектних рішень.
4. Етапи програмування системи.
5. Впровадження системи в промислову експлуатацію.
6. Висновки

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

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

7. Дата видачі завдання « 15 » січня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

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

Дата видачі завдання
« 15 » січня 2026 р.

Підпис керівника
_____ Усік П.С.
(прізвище та ініціали)

Завдання прийнято до виконання
« 15 » січня 2026 р.

Підпис здобувача
_____ Андрюшков Д.В.
(прізвище та ініціали)

АНОТАЦІЯ

Андрюшков Д.В. Програмне забезпечення системи мережевого комплексного засобу відеонагляду для підприємства. 123 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи мережевого комплексного засобу відеонагляду для підприємства.

Метою розробки є програмне забезпечення системи мережевого комплексного засобу відеонагляду для підприємства.

Результат роботи – програмна реалізація системи мережевого комплексного засобу відеонагляду для підприємства.

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, комп'ютерна мережа, відеонагляд

ABSTRACT

Andriushkov D.V. Software for a network complex video surveillance system for an enterprise. 123 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

In this final qualification work for the first (bachelor's) level of higher education, software has been developed that is intended for a network complex video surveillance system for an enterprise.

The purpose of the development is software for a network complex video surveillance system for an enterprise.

The result of the work is a software implementation of a network complex video surveillance system for an enterprise.

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

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

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

The program was developed in the Python environment.

Keywords: computer engineering, computer network, video surveillance

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

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

ВСТУП

Актуальність теми. Вибір правильної хмарної системи керування відео (VMS) є одним із найважливіших рішень для сучасних підприємств. Оскільки організації все частіше переходять до хмарної інфраструктури відеоспостереження, ринок пропонує численні варіанти, кожен з яких має унікальні переваги, моделі ціноутворення та можливості розгортання. У 2026 році ландшафт хмарних VMS значно розвинувся, і постачальники пропонують розширені функції, такі як аналітика на базі штучного інтелекту, інтеграція з периферійними пристроями та безпека корпоративного рівня.

Хмарні системи керування відео революціонізували корпоративний відеоспостереження, усунувши потребу в дорогій локальній серверній інфраструктурі. Організації тепер отримують переваги глобальної масштабованості, автоматичного оновлення програмного забезпечення, керування кількома об'єктами з однієї панелі керування та розширеного резервування даних. Хмарні платформи VMS дозволяють компаніям контролювати тисячі камер у розподілених місцях без підтримки складної IT-інфраструктури. Крім того, хмарні рішення пропонують нижчі капітальні витрати, гнучке ліцензування та швидке розгортання – критичні переваги для підприємств, які керують операціями з кількома об'єктами або проходять цифрову трансформацію.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи мережевого комплексного засобу відеонагляду для підприємства.

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

– Огляд існуючих систем мережевого комплексного засобу відеонагляду для підприємства.

– Дослідження системи мережевого комплексного засобу відеонагляду для підприємства.

– Програмна реалізація системи мережевого комплексного засобу відеонагляду для підприємства.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі мережевого комплексного засобу відеонагляду для підприємства.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи мережевого комплексного засобу відеонагляду для підприємства, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Створення й розгортання охоронної сигналізації на периметрі – одна зі найбільш складних з технічної точки зору завдань. Складні умови роботи не дозволяють повністю усунути помилкові спрацьовування. Різного роду погрози вимагають різних методів виявлення й установки відповідних датчиків. Кожний тип огородження вимагає різної тактики охорони й використовуваного устаткування. Непрості погодні умови: широкий діапазон температур, сонце, вітер, дощ, сніг, дикі й свійські тварина й птахи – все це може стати причиною помилкового спрацьовування.

Кожний фактор вимагає ретельного аналізу й найбільш оптимальних для кожного випадку технічних рішень, що відповідають датчиків, а також їхнього ретельного налаштування. Нерідко налаштування займає значний період досвідченої експлуатації.

Вибір способів виявлення проникнення й тактики захисту периметра об'єкта повинен здійснюватися професіоналами з більшим досвідом. Вибір тут украй великий.

Оптико-електронні інфрачервоні активні променеві оповіщувачі

Недорогий і ефективний спосіб виявлення проникнення. Являє собою випромінювач і приймач ІЧ випромінювання. Заснований на фіксації факту перетинання невидимого ІЧ-луча. Для захисту від помилкових спрацьовувань, перетинання лучу комахами, птахами, опадами, використовуються оповіщувачі із двома, трьома й навіть 4-мя променями. Відмінно підходить для прямих огороджень і рівного по висоті забору.

Радіохвильові датчики

Для виявлення об'єктів, що рухаються, використовують ефект Доплера. Відмінною рисою такого типу оповіщувачів є практично повна незалежність від погодних умов. Вони можуть працювати в дощ, сніг і туман однаково ефективно. Внаслідок широкого кута й обмеженого радіуса дії такі датчики використовують для локальних зон відчуження, де поява об'єкта є тривогою.

Радіолучеві сенсори

Являють собою передавач і приймач радіохвиль із частотою 1Ггц і вище. Радіохвильові датчики фіксують зміна сигналу на приймачі. За рахунок цього є можливість підбудовуватися під перешкодову обстановку, а так само працювати на нерівні й різнорівневих периметрах. У той же час радіохвильові датчики мають ширину лучу значно ширше ІЧ бар'єрів і вимагають наявність зони відчуження, де виключена поява людей, відсутні природні й штучні перешкоди, а так само немає зелених насаджень.

Вібраційні оповіщувачі

У зв'язку з великою довжиною периметра як чутливий елемент прийнятий використовувати спеціальний кабель. Датчик уловлює зміни стану, положення, геометрії чутливого кабелю, і тим самим фіксує факт проникнення по впливі на кабель при перелазі, розрізуванні забору, проламу й т.п. Ці датчики дуже ефективні на гнучких огородженнях виготовлених на основі сітки рабиці, ніздрюватого забору, профнастилу. А так само для виявлення спроби перелазу через колючий дріт закріплену зверху забору. Якість роботи вібраційних оповіщувачів сильно залежить від дотримання вимог до монтажу й кріплення на огородження, і вимагають серйозного налаштування й тривалої адаптації.

Ємнісні сенсори

Один з єдиних способів виявлення зловмисника на підході до об'єкта охорони. Принцип виявлення заснований на фіксації зміни ємності антенного поля створюваного одним або декількома провідниками протягненими уздовж огородження

Вибір типу датчиків і методів виявлення повинен здійснюватися виходячи з типу огородження, його конфігурації, тактики охорони, рівня захищеності об'єкта. Комбінуючи різні принципи виявлення можна створити надійний захист і мінімізувати помилкові спрацьовування.

1.2 Область застосування

Захист своєї території – це один з найглибших інстинктів, закладених природою й сотнями років еволюції людини. Якщо периметр території під надійною охороною ми починаємо почувати себе набагато комфортніше. Розглянемо найбільш ефективні методи забезпечення відеонагляду охоронюваної території й особливості реалізації відеоспостереження на периметрі.

Периметр території – це перший рубіж захисту будь-якого об'єкта. При проникненні на об'єкт зловмисник може легко загубитися усередині об'єкта й відстежити його місцезнаходження буде вже практично не можливо. Власник будь-якого об'єкта дуже добре розуміє, чим може загрожувати проникнення небажаних осіб на територію. У деяких випадках збиток може бути колосальним.

Представте, що відбудеться, якщо зловмисник проникне на територію насосної станції, що постачає котеджне селище питною водою, або найняті конкурентом диверсанти одержать доступ до ліній постачання електрикою вашого підприємства, або просто місцевий алкоголік викрутить вентилі на газових трубопроводах що б здати як кольоровий метал. Масштаби збитків іноді навіть складно прорахувати.

Приклади відеокамер для спостереження на периметрі

Камери для відеоспостереження на периметрі вибираються виходячи з вимог замовника й умовам експлуатації. Такими вимогами й умовами є: ступінь деталізації об'єктів у поле огляду, побажання до формфактора, наявність зовнішнього освітлення, висота установки, місце установки (стовп, стіна, навіс і

т.п.), наявність засвітлення від ліхтарів, фар автомобілів, сонячних променів і т.п. Вибір камер краще довірити професіоналам з великим досвідом.

IP-відеокамера AXIS P1365 MK II

Професійна фіксована вулична IP-камера стандартного дизайну в термокожусі, день/ніч ІЧ фільтр, розв'язну здатність 2Мп (1920x1080), стиск H.264/MJPEG, світлосильний варіофокальний об'єктив 2, 8-8 мм 109-39 град; матриця 1/2,8", прогресивне розгорнення, живлення – 8-28В і HiPOE, microSD, темп. -40...50град

IP-відеокамера AXIS P1254

Компактна IP-камера з винесеним оптичним блоком, для вулиці до -20град, розв'язну здатність 1,3 Мп, стиск H.264/MJPEG, фіксований об'єктив 2,8 мм 102 град; матриця 1/4', прогресивне розгорнення, живлення – POE або адаптер 220 В, темп. -20...50град

IP-відеокамера LTV CNE-620 58

Бюджетна вулична IP-відеокамера Bullet 3в1, день/ніч ІЧ фільтр, 1/3", розв'язну здатність 1,3 Мріх (1280x960), H264/MJPEG, варіофокальний об'єктив 3-10,5мм, кут огляду 79-28 град, убудована ІЧ підсвічування до 20м, схована проводка, температура -40...+50град, живлення 12 В або POE

Відеоспостереження – ефективний інструмент захисту периметра

Класична система охорони периметра має на увазі установку датчиків охоронної сигналізація, які призначені для фіксації й передачі повідомлень про спробу проникнення на охоронювану територію. Залежно від типу огородження периметра об'єкта, вимог по деталізації місця проникнення й необхідної захищеності, використовують сенсори, засновані на різним принципах виявлення: вібраційні, променеві, радіохвильові, акустичні, електростатичні й т.п.

Будь-які, навіть самі зроблені засоби виявлення, подають інформацію лише про факт спрацьовування оповіщувача. Це може бути упала вітка дерева, домашня або дика тварина, хлопчиська хулігани, до зубів збройна банда, а може бути й просто помилкове спрацьовування. Зовсім ясно, що реакція охорони

повинна бути різної. Нам адже не хочеться, що б мобільна група вийшла віч-на-віч до збройного злочинця, або ж їздила за кілька кілометрів на ділянку периметра, де було помилкове спрацьовування. Надати черговому охорони достовірну й повну інформацію про факт проникнення здатна лише система відеоспостереження.

У той же час усе більше популярна точка зору, що говорить, що для захисту периметра досить установити тільки лише систему відеоспостереження. Це переконання підживлюється рекламними проспектами й розповідями виробників про досконаліть технологій відеоаналізу. Нас запевняють, що спеціальні алгоритми можуть визначити факт проникнення аналізуючи зображення з камери. При цьому немає достовірної інформації про ймовірності помилок 1 і 2 роди в різних умовах використання: нічний час, сніг, дощ і т.п. Ми вважаємо, що система охорони периметра, що покликана запобігти проникненню на об'єкт і уникнути збитку від дій зловмисника, повинна будуватися на інтегрованій системі, у якій одночасно працюють і охоронна сигналізація, і відеоспостереження.

Використовувати на периметрі систему відеоспостереження без охоронної сигналізація має сенс лише в тих випадках, коли потрібно тільки лише довідатися звідки прийшов зловмисник і які дії вживав. Це можуть бути приватні котеджі, невеликі відособлені господарства, малі підприємства, і інші об'єкти, де немає можливості або не доцільно розміщати стаціонарний пост охорони. Запис у цьому випадку служить тільки лише для того, щоб в органів правопорядку була повна картина події й дій злочинців.

Особливості організації відеоспостереження на периметрі

Організувати відеоспостереження на периметрі, ефективно виконуюче покладені функції, це складний процес при якому необхідно врахувати велику кількість різноманітних завдань, факторів, вимог. По-різному організується відеоспостереження на периметрі об'єкта усередині густонаселеного пункту, і у

відкритій місцевості. Яку розв’язну здатність вибрати й потрібно чи додаткове підсвічування? Немаловажну роль мають організаційні заходи.

Розв’язну здатність камер для спостереження за периметром

Ступінь деталізації зображення на екрані визначає – яка кількість інформації й на якій відстані ми можемо довідатися про об'єкт спостереження. Чим вище розв’язну здатність, тим далі ми можемо виявити об'єкт. Для більшості завдань спостереження на периметрі достатнє виконання завдання виявлення – виявити об'єкт на заданій відстані й визначити його тип: машина, людина, свійська тварина й т.д. Це дозволяє встановлювати камери на дуже великому видаленні друг від друга. У деяких випадках буває достатнім установити камери на видаленні до 100 метрів.

Розвиток технологій зробило доступним камери надвисокого дозволу 2,3,5 і навіть 8 Мріх. Доступність мегапіксельного відеоспостереження зробило вкрай привабливим використання багатоомегапіксельних камер на периметрі. У той же час при збільшенні кількості мегапікселів різко падає чутливість камери в умовах недостатнього освітлення. Цей фактор на стільки значний, що в деяких випадках камери більше низького дозволу бачать далі.

Одержати максимальну дальність виявлення можливо при сполученні балансу дозволу камери і її чутливості з урахуванням освітлення в темний час доби на конкретній ділянці периметра. Чітких рекомендацій на цей рахунок не існує й тут можливий один з варіантів:

– проектувати свідомо більшу кількість камер, ніж це визначають граничні показання чутливості, при цьому витрати будуть істотно вище

– провести експеримент із різними камерами з різним розв’язною здатністю на конкретній ділянці периметра власними силами, або силами майбутнього підрядника

– покласти відповідальність на досвідченого підрядника, що можливо вже провів необхідне тестування

Тактика використання ІЧ підсвічування

Без світла не буде зображення. Чим більше світла, тим якісніше зображення й більше відстань, на якому буде виявлений порушник. Ця аксіома є визначальною при побудові відеоспостереження й рішення завдань спостереження в темний час доби.

Сучасним відеокамерам, крім видимого для людини світлового діапазону, доступний нижній спектр частот – інфрачервоне (теплове) випромінювання. Здатність камери бачити ІЧ випромінювання значно збільшує можливість для ведення спостереження в нічний час, при цьому зображення стає чорно-білим. Цією особливістю відеокамер користуються для створення додаткового підсвічування для спостереження при відсутності стандартного освітлення (ліхтарів, прожекторів, світильників і т.п.).

ІЧ підсвічування дуже ефективне, коли потрібно зробити відеоспостереження непомітним для порушника. Тобто тоді, коли Вам необхідно піймати лиходія. Порушник не підозрюючи, що його бачать, буде спокійно перелазити забір, у той час як за огорожею його чекає група негайного реагування.

Використання камер з ІЧ підсвічуванням стало дуже популярним. Польщі половини моделей вуличних камер виробляється вже з убудованими ІЧ випромінювачами. Інфрачервоне підсвічування стали застосовувати повсюдно. Навіть там, де це не потрібно або навіть шкідливо. Уявимо собі периметр мирного підприємства або котеджного селища. Навряд чи так гостро необхідно когось піймати. Швидше за все потрібно запобігти, уникнути або не допустити проникнення. У цьому випадку вірніше буде встановити стовпи освітлення, змонтувати економічні світильники й показати потенційному порушникові, що об'єкт перебуває під контролем. 99% порушників, якими є дрібні злодюжки, хулігани й вандали, навіть не захочуть намагатися перелізти забір під спостереженням камер при світлі ліхтарів.

Набагато симпатичніше переглядається добре освітлений гарний забір і кольорове зображення на камерах, ніж кромішня тьма й неприродна ч/б картинка в ІЧ спектрі. Витрата електрики економічного світлодіодного ліхтаря не набагато більше, ніж у потужної ІЧ підсвічування.

Використання поворотних камер

Сучасні поворотні камери мають вражаючі швидкісні параметри й оптичне збільшення. Одна поворотна камера, установлена на великій висоті здатна обдивлятися територію в сотні метрів, а іноді й кілька кілометрів, навколо себе. Виникає велика спокуса встановити одну камеру й замінити нею кілька десятків стаціонарних.

Необхідно пам'ятати, що поворотна камера має більшу зону контролю, а не огляду. Тобто вона здатна наблизити й деталізувати подія на великій території. Але в один момент часу вона може бачити тільки одну ділянку. Інші залишаються повністю неконтрольовані.

Найбільш удале застосування поворотні камери з оптичним зумом одержали у випадку оснащення периметра системами сигналізації. Якщо інтегрувати охоронну сигналізація з поворотною камерою можливо автоматичне позиціонуванні камери на ділянку, що спрацювала, периметра. Далі оператор може деталізувати подію й вести ціль у ручному режимі з пульта керування поворотною камерою.

Найбільш ефективне рішення – комбінація стаціонарних і поворотних камер. Коли стаціонарні оглядові камери детектують ціль, а поворотні дозволяють у ручному режимі її вести, і робити розпізнавання або навіть ідентифікацію об'єкта.

Тактика спостереження. Робоче місце оператора

Створити систему, що у будь-яких умовах експлуатації дозволить виявити й розібратися в тому, що відбувається на периметрі це необхідне, але не достатня умова побудови ефективної системи охорони периметра. Немаловажне значення мають організаційні заходи: обслуговування системи, періодичні навчання,

організація роботи постів охорони, розташування й графік патрулювання мобільних груп, оснащення охорони сучасними засобами зв'язку, пересування й затримки.

Компактна, підготовлена й добре оснащена служба охорони має потребу в якісному оперативному керуванні й координації. І тут немаловажну роль грає оператор системи відеоспостереження. Від того, як організоване його робоче місце, як надається інформація, як організований моніторинг залежить швидкість реакції.

У черговому режимі співробітник охорони не здатний контролювати більше 16-ти камер на більш ніж 2-х моніторах. Тоді як на протяжних периметрах можуть працювати десятки й навіть сотня камер. Для того, щоб можна було щось розглянути на камерах у режимі мультикартинки, часто встановлюють велику кількість моніторів і виводять всі камери одночасно не замислюючись – чи здатний оператор щось побачити на цих екранах. У підсумку, у силу фізіологічних особливостей людини, вона не бачить нічого й оперативність його роботи практично нульова. Разом із цим знижується й ефективність всієї служби охорони. Значні засоби на систему захисту периметра знову витрачені зрячи.

Вивід камер на монітори, кількість камер на одному моніторі, кількість моніторів, режим спостереження й навіть час знаходження оператора на пості повинні визначати можливостями людського організму. Існують досить серйозні дослідження на цей рахунок і в рамках статті про усім розповісти не можливо. Відзначити як тільки наступні прості правила:

– в оператора повинна бути можливість відлучитися від екранів на якийсь час. Мінімум на 15 мінут кожні друга година не беручи в облік перерва на прийом їжі й сон;

– виводити операторові на головні 1-2 монітори не більше 9-ти найважливіших камер: в'їзди/виїзди, оглядові камери, критично важливі зони життєзабезпечення об'єкта й т.п.

– якщо периметр оснащений датчиками охоронної сигналізація, то має сенс в автоматичному режимі виводити операторові інформацію з найближчих до місця події камер. Це дозволить звернути його увагу на подію для швидкого ухвалення рішення

– якщо на периметрі встановлена тільки система відеоспостереження, без датчиків охоронної сигналізація, то правильним рішенням буде тонке відбудування програмних детекторів руху, заснованих на відеоаналізі й звертати увагу оператора на камери, де відбувається спрацьовування цих детекторів

Якщо уважно підійти до організації робочого місця оператора й проробити тактикові охорони, то в багатьох випадках можна обійтися одним постом спостереження з одним оператором, що здатний швидко розібратися в події й прийняти правильне рішення.

Резюме

Кожний об'єкт унікальний і виробити універсальні рішення, або дати загальні рекомендації, неможливо. Особливо це стосується систем захисту периметра об'єкта. Занадто багато різних факторів впливає на вихідний результат. А ціна помилки вкрай висока. Капіталовкладення для таких систем одні із самих значних. У цих умовах дуже важливо вибрати грамотного підрядника з великим досвідом і контролювати роботу на всіх стадіях підготовки й реалізації проекту.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи мережевого комплексного засобу відеонагляду для підприємства, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

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

Відеоспостереження вже давно використовується для рішення різних завдань. В 60-х роках це були аналогові закриті системи відеоспостереження, назва CCTV (closed circuit television – замкнута телевізійна система) розкриває зміст поняття.

Розвиток не стояв на місці й в 90-х роках, а саме в 1996 була розроблена перша у світі цифрова IP відеокамера компанією Axis Communication. Технічні характеристики камери не здавалися настільки грандіозними, і, у порівнянні з аналоговими, камери виглядали блідо. Незважаючи на це, перших IP камер було продано порядку 10000 штук.

Вихід IP камер на ринок послужив відправною точкою для розвитку систем відеоспостереження, поява камери вимагало появи програмного забезпечення для роботи с їй.

Згодом з'являлися нові IP камери відеоспостереження, разом ними й програмне забезпечення. Розвиток пішов двома шляхами: частина компаній зайнялося розробкою софту для роботи з будь-якими IP камерами, друга частина – виробництвом власних камер і софту для роботи винятково зі своїми камерами.

Такий підхід у розвитку розділив системи відеоспостереження на «відкриті» і «закриті». Відкриті, Open Platform системи розвуються убік багатовендорності – підтримці камер незалежно від виробника, і закриті – одновендорні системи, що підтримують роботу тільки з устаткуванням власного виробництва.

Однак зараз проглядається тенденція до того, що закриті системи починають дивитися убік підтримки устаткування сторонніх виробників, але їм усе ще далеко до того, щоб називатися відкритими платформами.

Додатково варто згадати про відеоаналітику. На сьогоднішній день це невід'ємна частина СВС, що стрімко розвивається, здатна полегшити й допомогти операторам не втратитися у величезному потоці відеоінформації. А також вирішувати бізнес-завдання й у цілому перетворювати відео в дані, якими можна з легкістю оперувати. Тому сучасна й комплексна система відеоспостереження повинна підтримувати роботу з аналітикою, підтримувати інтеграцію із системою контролю доступу, керування будинком.

Відкритих платформ відеоспостереження на ринку представлено досить. Щоб небагато розібратися в них, проведемо невеликий огляд деяких СВС, а більше детальну інформацію з характеристик можна побачити в таблиці порівняння VMS.

MileStone Systems. XProtect

(www.milestonesys.com)

Компанія Milestone займається розробкою ПЗ для IP систем відеоспостереження з кінця 90-х років. Через джерела своєї діяльності тісно співробітничає з компанією Axis Communication, лідером в області виробництва пристроїв відеоспостереження.

Протягом 10 років компанія Milestone є лідером на ринку СВС за результатами IHS Markit, а також засновником поняття відкритої платформи у відеоспостереженні.

Продуктова лінійка представлена групою програмного забезпечення XProtect, сім версій і лінійкою мережних реєстраторів Husky.

Продуктова лінійка покриває різні потреби до систем відеоспостереження: від простих і невеликих систем, до складних, географічно розподіленим без обмеження за кількістю камер на сервер або систему в цілому.

Для ознайомлення із програмним продуктом є можливість скачати ознайомлювальну версію будь-якої версії або ж використовувати зовсім безкоштовно молодшу версію продукту Essential+ на 8 пристроїв, без обмеження з дозволу камер, що підключаються користувачам, періоду зберігання й не тільки.

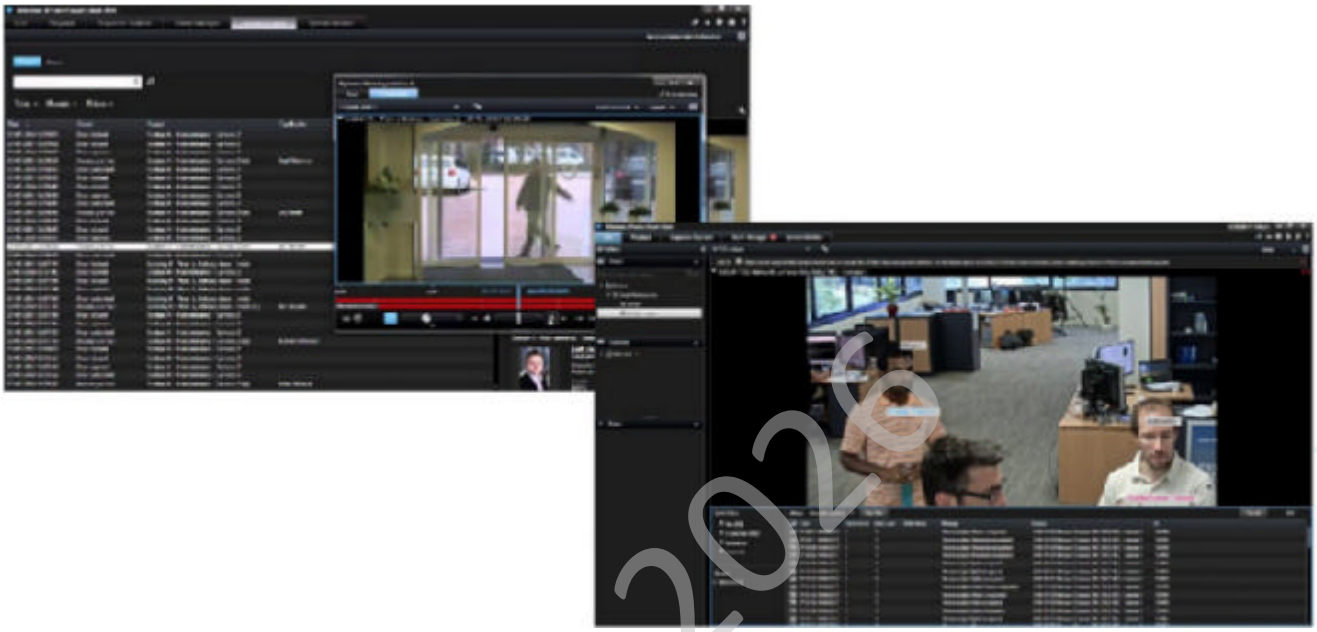

Рисунок 2.1 – Інтерфейс користувача Milestone

Milestone підтримує найбільша кількість IP пристроїв на рівні драйвера й зараз це більше 7000 перевірених моделей різних виробників і кількість готових інтеграцій – відеоаналітика (захист периметра, розпізнавання осіб, розпізнавання номерних знаків, рішень для паркінгу, бізнес аналітика, аналітика звуку), системи контролю доступу, системи керування будинками й т.д.

Для кастомізації функціонала є можливість використовувати безкоштовний SDK у всіх версіях і/або конфігураційний API у старшій версії.

Milestone має дуже просту систему ліцензування. Ліцензування складається з однієї базової ліцензії на ПЗ, без прив'язки до заліза сервера й ліцензії на пристрій. Ліцензування пристрою не обмежує його функціонал і дозволяє використовувати, «вичавлювати» із пристрою максимум: кількість

потоків (каналів), порти I/O, підтримка звуку, робота з картою пам'яті, убудована аналітика. Базова ліцензія на софт не обмежується однією інсталяцією й може бути встановлена на різні локації, сайти без обмеження. Повторне підключення пристрою в межах однієї базової ліцензії не вимагає додаткового ліцензування, що дає можливість здійснювати подвійний запис, наприклад. Підключення реєстраторів в Milestone XProtect у більшості випадків вимагає однієї ліцензії, у такий спосіб можна підключити NVR до 64-х каналів. Єдиним недоліком у роботі з реєстраторами є відсутність прямого доступу до архіву на реєстраторі.

В Milestone XProtect відсутнє обмеження на кількість користувачів і одночасних підключень (одна лише версія обмежується п'ятьома клієнтськими підключеннями). Підтримує три типи користувачів: пропрієтарний, Windows і Active Directory. Для зручності й гнучкості роботи зі СВС, у наявності три абсолютно безкоштовних клієнти: товстий клієнт, mobile і web клієнт, що дозволяють працювати з живим, архівним відео, реагувати на тривоги в системі. За допомогою мобільного клієнта можна перетворити пристрій з камерою в IP камеру й транслювати відео з можливістю запису в архів.

Для конфігурації системи використовується додаткове ПЗ, є клієнт-серверним і може використовуватися де-небудь у мережній доступності до сервера.

Milestone не розробляє власної аналітики. Ідеологія компанії полягає в створенні зручного й відкритого інструмента для інтеграції, роботи з відео: перегляду, запису, забезпечення його схоронності й дійсності, а розробкою аналітики повинні займатися профільні компанії, у такий спосіб у портфелі Milestone величезна кількість технологічних партнерів і рішень по інтеграції.

Для розширення функціонала Milestone XProtect у своєму портфелі має кілька модулів, це Transact – для роботи із транзакціями (текстовою інформацією) і зіставлення їх з відео, LPR – система розпізнавання номерних знаків, Retail – модуль інтеграції з ERP системою, ACS – інтеграція із системами контролю доступу.

СВС Milestone XProtect розроблений під використання в середовищі Windows, як серверна, так і клієнтська частина (товстий клієнт). Для зберігання конфігурації й різної служебної інформації використовує MS SQL, за замовчуванням це версія Express. Milestone підтримує роботу у віртуальному середовищі.

Додаткова інформація втримується в таблиці порівняння й доступна по посиланнях із сайту виробника.

Genetec. Omnicast

(www.genetec.com)

Компанія Genetec веде свою діяльність із кінця 90-х років і є одним з лідерів ринку систем відеоспостереження.

Genetec – розроблювач уніфікованої платформи відеонагляду. Основними продуктами є Security Center і Omnicast. Останній продукт є безпосередньо системою відеоспостереження, а перший – верхньою точкою, агрегатором додаткових компонентів системи, і деякі можливості системи Onmicast розкриваються при використанні Security Center.

І так, Omnicast представлений трьома версіями, що мають різні обмеження за кількістю камер у системі, користувачів і інших функціональних можливостей.

Genetec здатний закрити різні потреби до системи відеоспостереження: від простих і невеликих систем, до складних, географічно розподіленим, без обмеження за кількістю камер на сервер або систему в цілому, але з обмеженням на потік сервера запису в 200 Мб/с, тому при інсталяціях з більшою кількістю камер, готуйтеся до великої кількості серверів запису.

Безкоштовної версії в Genetec не існує, тому єдиний варіант ознайомлення із програмним продуктом – запит демо версії.

Genetec Onmicast підтримує порядку 6000 IP пристроїв і велика кількість інтегрованих рішень по відеоаналітиці (захист периметра, розпізнавання осіб, розпізнавання номерних знаків, бізнес аналітика) системи контролю доступу, системи керування будинками й т.д. Інформацію про підтримку пристроїв і

пошук інтегрованих рішень можна знайти на сайті Genetec, через те, що підтримка, приміром, може бути можлива тільки в Security Center, а в Omnicast бути відсутньою.

Для розширення функціонала Genetec надає SDK.

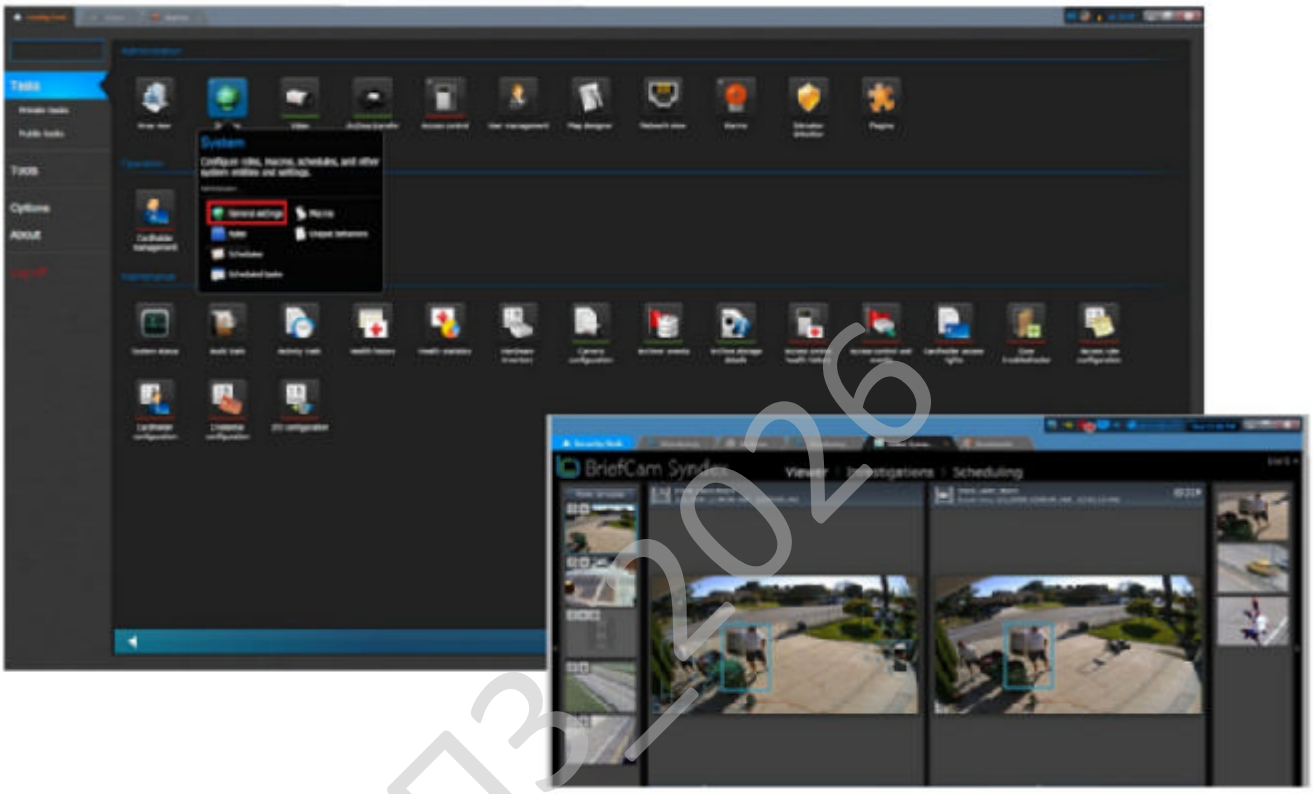

Рисунок 2.2 – Інтерфейс користувача Genetec

Ліцензується Genetec за кількістю пристроїв, із прив'язкою до базової ліцензії. Підтримуваний функціонал устаткування залежить від рівня інтеграції, це може бути підтримка багатоканальності, звуку, портів I/O, роботи з картою пам'яті, бортова аналітика. Ліцензія прив’язується до якоїсь системної інформації, тому зміна конфігурації ПК може спровокувати її ануляцію й зажадати повторної активації.

Genetec Omnicast, залежно від версії, має обмеження на кількість користувачів, що підключаються, обмеження відсутнє тільки в старшій версії.

Тип облікових записів користувачів, підтримуваний в Onmicast один – пропрієтарний, інтеграція з Active Directory можлива при використанні Security Center.

Для роботи оператора передбачений товстий клієнт, mobile – відсутній. Для підтримки мобільних пристроїв і веб доступу буде потрібно установка мобільного сервера, як компонент Security Center. Мобільний сервер – компонентів ліцензуємий. Мобільний доступ у свою чергу дасть не тільки можливість переглядати й працювати з відео з будь-якої точки миру, але й використовувати камеру пристрою мобільного як IP камеру.

Власні аналітичні модулі Genetec не розробляє, при цьому є присутнім широкий вибір партнерів по інтеграції різного роду відеоаналітики.

Функціонал Genetec може бути розширений власними модулями, це – система розпізнавання номерів AutoVu і системи контролю доступу Synergis**.** Використання даних компонентів має на увазі наявність Security Center.

Також Genetec випускає програмно-апаратні комплекси Streamvault**.**

Genetec Omnicast розроблений під Windows, як серверна, так і клієнтська частина. Для налаштування системи використовується окреме програмне забезпечення. Для зберігання різної службової інформації використовує MS SQL, підтримується робота у віртуальному середовищі.

Додаткова інформація втримується в таблиці порівняння й доступна по посиланнях із сайту виробника.

Luxriot. Evo

(www.luxriot.com)

Luxriot – американська компанія по розробці програмного забезпечення для систем відеоспостереження, крім софту пропонує сервера із передвстановленим ПЗ, плати захвата для аналогових систем відеоспостереження.

Luxriot представлений на ринку трьома версіями програмного забезпечення й закриває потреби дрібних і більших систем відеоспостереження, у

тому числі й географічно розподілених. У системи відсутні обмеження на кількість камер на сервер або систему в рамках придбаної ліцензії.

Ознайомитися із продуктами від Luxriot можна за допомогою запиту демо ліцензій або ж використовувати безкоштовну версію продукту. Безкоштовна версія має ряд обмежень, основні з яких: дев'ять підтримуваних каналів, максимальний розв’язну здатність камер до 2Мр, одне користувальницьке підключення на систему. Безкоштовна ліцензія може бути розширена до 16 каналів за потребою.

Лінійка СВС Luxriot підтримує порядку 6000 IP пристроїв і підтримує невелику кількість інтеграцій сторонніх рішень по відео аналітиці й таким рішенням, як система контролю доступу. Що стосується бортовий аналітики камер, Luxriot підтримує обмежений список виробників.

Ліцензування в Luxriot поканально й поширюється у вигляді бандлов на молодші версії й поканально в старшій версії. Тому що більшість IP камер на ринку зараз багатоканальні (профільні), поканально ліцензування в деяких випадках накладає незручності й вимагає додаткового ліцензування при використанні багатоканальних пристроїв. Ліцензія в Luxriot прив’язується до апаратної частини сервера, тому при зміні конфігурації можливо буде потрібно повторна активація.

Незважаючи на невеликий вибір рішень по інтеграції рішень сторонніх виробників, функціонал СВС може бути розширений власними модулями аналітики. Luxriot розробляє наступні модулі відеоаналітики: захисту периметра, бізнес аналітики, розпізнавання номерних знаків і осіб.

Для рішення питань по розширенню функціонала й інтеграції надається API/SDK.

Користувальницькі підключення обмежені лише в безкоштовній версії. Підтримуються два типи облікових записів: пропрієтарні й Active Directory.

Для роботи операторів доступно три типи клієнтів: товстий клієнт, mobile і web клієнт. Клієнтські додатки абсолютно безкоштовні й додатково не

ліцензуються. Використання камери пристрою мобільного клієнта дає можливість транслювати й записувати відео в систему.

Luxriot розроблений під Windows, його серверна частина, а основне ПЗ для оператора – під Windows і MacOS. Luxriot для зберігання конфігурації й системної інформації використовує пропрієтарну базу даних і підтримує роботу у віртуальному середовищі.

Додаткова інформація втримується в таблиці порівняння й доступна по посиланнях із сайту виробника.

Network Optix. NxWitness / Hanwha. Wisenet Wave

(www.networkoptix.com / www.hanwhasecurity.com)

Дана VMS розглядається у двох назвах і від різних вендорів. Причина в OEM, компанія Network Optix брендує свою СВС NxWitness для Hanwha, що на ринку відома як Wisenet Wave. Network Optix не обмежується лише співробітництвом з Hanwha у цьому плані, як наслідок, можна знайти знайомий інтерфейс від інших вендорів.

Компанія Network Optix бере свій початок з 2010-2011 років і представлена на ринку основним програмним продуктом NxWitness.

NxWitness існує в одному варіанті, без розподілу на версії. Із всіх розглянутих, СВС має самий компактний інсталятор і позиціонується розроблювачами як дуже легковагий і невимогливий до апаратних ресурсів продукт, при цьому не на шкоду функціоналові.

Дана СВС підходить для об'єктів різних розмірів, легко масштабується й застосовна навіть для географічно розподілених об'єктів. В NxWitness є присутнім обмеження в 128 пристроїв на сервер і рекомендовану кількість серверів у єдиній системі не більше 50. Теоретично й практично кількість серверів може бути більше, але до планування системи повинен залучатися розроблювач, і такі інсталяції існують.

Для знайомства з NxWitness доступна демо ліцензія на сайті виробника, а також NxWitness можна абсолютно безкоштовно використовувати для перегляду живого відео або знайти застосування як відео-проксі сервера.

NxWitness підтримує порядку 5000 IP пристроїв. Ліцензується – по пристроях, а при підключенні NVR ліцензується кожні чотири канали. Сам NxWitness добре працює з NVR, зокрема від Hanwha, і підтримує доступ до архіву на самому пристрої. Ліцензія прив'язується до апаратної частини, після зміни конфігурації сервера може знадобитися переактивація ліцензії. Ліцензія дає можливість використовувати в повному обсязі підтримуваний функціонал IP пристрою (порти I/O, звук, бортова аналітика), що стосується каналів – NxWitness підтримує тільки двоканальну схему роботи – основний і додатковий. В архітектурі NxWitness вторинний потік відіграє роль зниження навантаження на мережу або на АРМ оператора при перегляді відео. Другий потік за замовчуванням записується, але запис можна відключити.

Система має невеликий вибір уже готових рішень інтеграції відеоаналітики, але надає багатофункціональний API і SDK на безкоштовній основі. З використанням API повністю можна автоматизувати рутинну роботу із системою, аж до повного її налаштування або нестандартного моніторингу.

Типи облікових записів у системі дві: пропрієтарний і LDAP. Для роботи зі СВС існує три клієнтських ПЗ: товстий клієнт, mobile і web. Всі клієнти абсолютно безкоштовні. Програма налаштування системи сполучена із програмою роботи з відео, єдиний інтерфейс, поділ відбувається на рівні прав користувачів.

Серверна частина NxWitness підтримує роботу в середовищі Windows, Linux, клієнтська – Windows, Linux, MacOS. Відмінною рисою є підтримка ARM архітектури для північної частини програмного забезпечення. Вендором перевірена робота на одноплатних комп'ютерах Raspberry Pi і Banana Pi, хоча теоретично немає обмежень для використання на інших подібних пристроях.

NxWitness може бути розгорнуть у віртуальному середовищі, а також в Docker.

Додаткова інформація втримується в таблиці порівняння й доступна по посиланнях із сайту виробника.

Сателіт Інновація. Macroscop (Eocortex)

(macroscop.com / eocortex.com)

Сателіт Інновація – компанія, що розробляє програмні рішення для професійних систем відеоспостереження за назвою Macroscop, для європейського ринку відома за назвою Eocortex. Macroscop бере свій початок з 2008 року й розробляє програмне забезпечення, функції відеоаналітики й мережних реєстраторів.

Macroscop містить у собі три версії програмного забезпечення з різною кількістю підтримуваних камер, серверів, клієнтських підключень, підтримкою аналітики. Macroscop застосовна для дрібних об'єктів і великих об'єктів. Обмеження в старших версіях на кількість камер у системі відсутній, а от кількість камер на сервер обмежене до 479.

Для ознайомлення доступна демо версія продукту, безкоштовної версії в Macroscop немає.

Лінійка продуктів Macroscop підтримує близько 5000 IP камер і певні моделі реєстраторів. Ліцензування поканальне, більшість IP камер на ринку зараз багатоканальні (профільні), такий тип ліцензування в деяких випадках накладає незручності й вимагає додаткового ліцензування при використанні багатоканальних пристроїв. Прив'язка ліцензії здійснюється до апаратної частини сервера, тому при зміні конфігурації можливо буде потрібно переактивація. Після активації ключа він не може бути перенесений на інший комп'ютер. Як варіант, є можливість використовувати USB ключа, що не має прив'язки.

Підтримка бортовий аналітики з камер в Macroscop не спостерігається. Для цих цілей Macroscop пропонує використовувати інтелектуальні модулі, убудовані в програмне забезпечення. Система нараховує порядку п'ятнадцяти

модулів, вони ліцензуються окремо за кількістю каналів, старша версія включає частину модулів на безкоштовній основі. Забавний факт, що деварпинг – розгорнення Fisheye-камери, відноситься до інтелектуального модуля й ліцензується додатково.

Macroscop розташовує власним SDK для потреб інтеграції й розширення функціонала системи. Готових сторонніх рішень по відеоаналітиці практично немає у вільному доступі, але існують інтеграції з деякими системами контролю доступу.

У системі підтримується один, пропрієтарний тип облікових записів. Підтримка користувачів Active Directory припинена. Для роботи зі СВС існує три клієнтських ПЗ: основне, mobile і web. Всі клієнти абсолютно безкоштовні. Існує окремий конфігуратор для налаштування системи.

Серверна й клієнтська частина підтримує роботу в середовищі Windows.

Додаткова інформація втримується в таблиці порівняння й доступна по посиланнях із сайту виробника.

До вибору системи відеоспостереження потрібно підходити комплексно, ґрунтовно й з поглядом у майбутнє. Головний вибір може стояти між закритою й відкритою системою відеоспостереження, між системою з убудованою аналітикою або без, але з можливістю інтеграції; і завжди потрібно враховувати, є чи необхідність інтегрувати сторонні комплекси.

Що ж вибрати? Як по мені, то вибір очевидний – відкрита платформа, і бажано в повному обсязі цього слова.

Відкрита платформа надасть Вам гнучкість і право вибору – без прив'язки до IP устаткування, апаратним комплексам і найчастіше до аналітики. Відкритість платформи відеоспостереження дасть Вам поле для діяльності – тестуванню й вибору рішення, що дійсно буде вирішувати Ваші завдання.

Тому, вибираючи систему, важливо звертати увагу на її інноваційність і послужний список. Потрібно налаштувати себе на одержання максимальної віддачі від продукту. І не варто дивитися тільки на вартість за канал, а скоріше

більше розумним рішенням може бути оцінка співвідношення вартості каналу з його цінністю.

Тепловізійні відеокамери: найбільш ефективне рішення для охорони периметра

Одне з економічних і ефективних рішень у цій сфері забезпечення відеонагляду – системи охоронного телебачення. При цьому обов'язково використовуються тепловізори в цих системах відеоспостереження. Чому таке рішення одне з найкращих – розглянемо далі.

Охорона периметра містить у собі кілька структурних елементів:

– сам охоронюваний периметр;

– забір або інший символ (звичайно ж, в очах порушника) закритої території;

– пристрою контролю (датчики систем периметральної охорони, тепловізійні відеокамери й т.п.);

– пристрою відображення й сигналізації порушення периметра (охоронні пульти з моніторами, аудиосвітлова сигналізація);

– служби реагування (охоронці, групи швидкого реагування й т.п.);

– служба технічної підтримки або власна, або працююча за контрактом.

При досить масштабному периметрі (площі об'єкта) облаштованість звичайних систем периметрального контролю – досить дороге задоволення. Представте, скільки необхідно тільки стійок для периметра довжиною всього 4 км? Наприклад, активний інфрачервоний оповіщувач AX-350DH MKIII при вартості порядку 20 тис. грн. працює на відстані до 200 м. 4/0,2 км = 2 таких оповіщувача. Вартість устаткування, плюс вартість робіт, кабелів і ін. показники легко підрахувати. Зрозуміло, що дане високоякісне устаткування призначене для рішення певних завдань, і воно їх вирішує.

Однак можна застосувати тепловізійну камеру, наприклад, AXIS Q 1931-E13MM 8.3 FPS з кутом огляду в 28°, і контролювати границю фактично без обмеження по відстані. У її можливостях:

– розв’язну здатність 384x288 при швидкості запису 8,3 кадр/сек;

– вулична установка;

– програмний детектор руху;

– визначення перетинання заданої лінії й т.д.

Основна конкурентна перевага відеокамер з тепловізором – ефективна робота в будь-яких погодних умовах. При снігу, у пургу, у дощ, вітер, такі камери знаходять мету навіть якщо вона сховалася за густим листям дерев і т.п.

Їх легко перенаправляти на ділянка, що цікавить на даний момент, периметра, перенести на інший об'єкт і т.д.

Застосовуються тепловізори в системах відеоспостереження в нафтогазовій промисловості. Причому не тільки для боротьби з вандалами й іншими зловмисниками, але й для контролю теплових витоків, небезпечних загорянь поблизу й т.п. На магістральних трубопроводах особливо яскраво видна економічна вигода від застосування таких камер.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Python – високорівнева мова програмування, яку називають другою за популярністю в світі. Її використовують для розробки вебзастосунків, програмного забезпечення, машинного навчання. Python застосовують для вирішення робочих завдань у компаніях Google, Instagram, Facebook, IBM, NASA, Dropbox, Netflix та інших. Розробники цінують цю мову програмування за простоту у вивченні, ефективність та мультиплатформність.

Python – скриптова мова програмування з досить простим синтаксисом. Для розуміння достатньо порівняти принципи написання найпростішої програми, яка виводить на екран текстове повідомлення. Саме тому мова програмування Python більш доступна для новачків, а професіонали встигли адаптувати її для вирішення великої кількості завдань. Це мультиплатформне рішення, тому

знання Python дає можливість працювати у різних сферах: від розробки мобільних застосунків до ігрової індустрії та штучного інтелекту.

У мови програмування динамічна типізація: є можливість передавати до функцій будь-який тип даних без попереднього вказання. Інтерпретованість дозволяє знаходити помилки у коді ще до повної збірки у робочий застосунок. При цьому Python дуже чітко дає зрозуміти, де та через що виникла помилка.

Це мова об'єктноорієнтованого програмування (ООП). Програмне забезпечення на Python оформлене у вигляді моделей, які можуть бути зібраними у пакети. Тип та структуру кожного об’єкта можна запитати під час виконання програми. Для кожного з об’єктів можна отримати всю інформацію щодо його внутрішньої структури. Окрім того:

– у мови логічний синтаксис, завдяки чому вихідний код легко читати та розуміти;

– гнучкість та масштабованість Python дозволяє адаптувати високорівневу логіку та розширяти складні застосунки, як тільки виникне така необхідність;

– розробка на Python у більшості випадків проходить швидше, ніж на інших мовах програмування;

– Python – інтерпретована мова програмування. Це значить, що код можна написати у будь-якому текстовому файлі на будь-якій платформі, і потім успішно запустити;

– у Python – колосальна спільнота однодумців. Тож будь-які складнощі конкретних розробників вирішуються колективно.

Проте є декілька особливостей, які можна віднести до недоліків. Це повільність (ця мова програмування хоч і універсальна, проте повільніша за інші), велика кількість ресурсів, необхідних для роботи та «прив’язаність» до системних бібліотек.

Мова програмування Python використовується у наступних сферах:

1. Розробка програмних застосунків будь-якого напрямку.

2. Розробка серверної частини мобільних застосунків (найпопулярніший напрямок).

3. Ігри. Багато сучасних ігор для комп'ютерів (наприклад, World of Tanks) частково чи повністю написані на Python.

4. Вбудовані системи для різних пристроїв. Дуже часто Python використовують для написання внутрішніх платформ управління банкоматами.

5. Скрипти та плагіни до уже реалізованих програм для автоматизації процесів чи створення інших рішень.

6. Тестування (автоматизація цього процесу).

7. Машинне навчання. – основна мова для написання алгоритмів і аналітичних застосунків у сфері Machine Learning.

Бібліотеки Python

Різні бібліотеки Python використовують для виконання конкретних завдань. Наприклад, Matplotlib підходить для відображення даних у двовимірній та тривимірній графіці. Pandas підходить для зручної роботи з даними. NumPy дозволяє створювати масиви та керувати ними. Requests використовується для веброзробки. OpenCV-Python відкриває можливості для обробки зображень з метою оптимізації систем «машинного зору».

Найвідоміші фреймворки для мови програмування Python

Фреймворки Python допомагають створити зручне та функціональне середовище для розробки. У них міститься набір інструментів, модулів та бібліотек, корисних для виконання конкретних завдань. Це значно полегшує роботу: наприклад, дає змогу не витрачати час на розписування дій, які повторюються, а використати релевантний інструмент. Тож є можливість позбутися рутинних процесів та сконцентруватися на логіці проєкту.

Серед найпопулярніших фреймворків для Python:

– Django – найстаріший та найвідоміший. Створений для реалізації великих інтерактивних проєктів;

– Pyramid – зручний у налаштуваннях, і дає можливість реалізувати складні нестандартні ідеї;

– Web2py – підходить в першу чергу для вебзастосунків і може використовуватись на будь-яких архітектурах.

Популярні Python IDE

IDE або інтегровані середовища розробки – це програмне забезпечення, яке надає розробникам необхідні інструменти для написання, редагування, тестування та налаштування коду. Для розробки на Python найчастіше використовують IDE PyCharm, IDLE, Spyder та Atom.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускну кваліфікаційну роботу за першим (бакалаврським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи мережевого комплексного засобу відеонагляду для підприємства.

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

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

б) вибрати та обґрунтувати методику побудови системи 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

Вибір правильних камер відеонагляду для вашого бізнесу – одне з найважливіших рішень, які ви можете прийняти для захисту своїх активів, співробітників та клієнтів. Сучасні комерційні системи відеоспостереження вийшли далеко за рамки простого запису; тепер вони діють як датчики на базі штучного інтелекту та інструменти бізнес-аналітики, які допомагають вам ефективніше керувати операціями.

Незалежно від того, чи керуєте ви комерційним офісом, багатоквартирним житловим будинком, роздрібним магазином чи будівельним майданчиком, цей посібник пояснює, на що звернути увагу, вибираючи найкращі камери відеонагляду для бізнесу у 2026 році, з акцентом на перевірених професійних брендах, що підходять для нью-йоркських компаній, таких як Axis, Hanwha, Bosch, Pelco, Panasonic, Sony, Digital Watchdog та інші.

Камери відеонагляду для бізнесу тепер відіграють подвійну роль: захищають людей і майно, а також надають аналітичні дані, які допомагають приймати більш розумні рішення. Основні причини, чому кожен бізнес повинен впровадити сучасну систему камер, включають:

– Стримування та запобігання – Видимі камери запобігають крадіжкам, вандалізму та несанкціонованому доступу до того, як трапляться інциденти.

– Моніторинг у режимі реального часу – IP- та хмарні системи дозволяють безпечно переглядати прямі трансляції зі смартфона, планшета або ПК з будь-якого місця.

– Аналітика на базі штучного інтелекту – такі функції, як підрахунок людей, фільтрація руху, класифікація облич і транспортних засобів, а також аналітика присутності, допомагають вам вийти за рамки базового спостереження

та перейти до оперативної аналітики.

– Докази відповідальності та інцидентів – Записано відео може бути вирішальним для страхових претензій, інцидентів на робочому місці та юридичних спорів.

– Дотримання нормативних вимог та політик – Багато галузей промисловості та місцевих юрисдикцій, включаючи Нью-Йорк, очікують або вимагають відеоспостереження для забезпечення відеонагляду, контролю доступу та документування інцидентів.

Для бізнес-середовища фінансовий та репутаційний вплив порушення відеонагляду може бути суттєвим, що робить надійну систему камер відеоспостереження ключовою частиною вашої стратегії управління ризиками.

Коли ви обираєте камери відеонагляду для бізнесу, бренд має значення. Виробники корпоративного класу інвестують значні кошти в якість зображення, кібербезпеку, надійність та довгострокову підтримку – все це є важливим для комерційного розгортання. Нижче наведено провідні бренди, які широко використовуються в професійних бізнес-інсталяціях та підтримуються такими інтеграторами, як Vertex Security.

Hanwha Vision – відеоспостереження на основі штучного інтелекту, орієнтоване на відповідність вимогам

Hanwha Vision (раніше Samsung Techwin) стала одним із найбільш збалансованих варіантів для професійних інсталяцій, поєднуючи високу якість зображення, передову аналітику на основі штучного інтелекту та конкурентні ціни. Її Wisenet 9 SoC та камери наступного покоління серії P та X зі штучним інтелектом забезпечують високу чіткість, інтелектуальне виявлення подій та надійні функції кібервідеонагляду, розроблені для сучасних підприємств.

Камери Hanwha включають аналітичні засоби, такі як виявлення людей і транспортних засобів, розпізнавання номерних знаків, аналіз поведінки, а також інструменти бізнес-аналітики, такі як моніторинг заповненості та черг. Вони особливо добре підходять для освіти, офісів, міського відеоспостереження,

змішаних хмарних/локальних архітектур та будь-якого бізнесу, якому потрібен надійний штучний інтелект разом із сильним контролем конфіденційності та кібервідеонагляду.

Axis Communications – золотий стандарт корпоративного відео

Компанія Axis Communications широко вважається преміальним стандартом для розгортання камер відеонагляду на підприємствах та критично важливих об'єктах. Камери Axis побудовані на технології відкритої платформи, що дозволяє легко інтегруватися з провідними платформами VMS, такими як Milestone, Genetec та іншими, що зазвичай використовуються у великих комерційних та державних проектах.

Axis часто обирають для середовищ, де надійність, управління життєвим циклом та кібербезпека є головними пріоритетами, таких як корпоративні кампуси, фінансові установи та критична інфраструктура. Такі функції, як розширена обробка зображень, аналітика периферійних даних та надійне шифрування, роблять Axis найкращим варіантом для компаній, яким потрібна система камер, здатна масштабуватися відповідно до їхніх потреб.

Bosch Security – створено для суворих умов та середовищ високого ризику

Камери відеонагляду Bosch розроблені для вимогливих промислових та комерційних умов, де час безвідмовної роботи та точність аналітики мають вирішальне значення. Вони пропонують міцні корпуси, широкий діапазон робочих температур та вбудовану інтелектуальну відеоаналітику, включаючи виявлення вторгнень, підрахунок людей, виявлення щільності натовпу та виявлення бездіяльності.

Компанію Bosch часто рекомендують для високоризикованих промислових та інфраструктурних проектів, таких як енергетика, комунальні послуги, транспортні вузли та великі промислові підприємства, де потрібні тривалі життєві цикли продукції та глибока інтеграція з системами контролю доступу та будівель. Для нью-йоркських підприємств зі складними об'єктами,

такими як логістичні операції або великі об'єкти змішаного використання, Bosch може стати чудовою основою для надійного рівня відеоспостереження.

Pelco – перевірена ефективність у комерційних приміщеннях

Pelco має довгу історію на ринку комерційного відеонагляду та залишається надійним брендом у сфері надійних систем камер професійного рівня. Її портфоліо охоплює стаціонарні, купольні та PTZ-камери, призначені для цілодобової роботи в таких закладах, як готельний бізнес, охорона здоров'я, освіта та багатоквартирні комерційні комплекси.

Рішення Pelco часто використовуються в проектах, де пріоритетами є стабільна продуктивність, інтеграція з існуючими системами управління та довгострокова підтримка. Для керуючих нерухомістю та операторів об'єктів, які бажають мати надійний, добре зарекомендував себе бренд, Pelco залишається надійним вибором.

Panasonic i-PRO – розумна аналітика за середньою ціною

Лінійка i-PRO від Panasonic зосереджена на наданні потужних функцій штучного інтелекту безпосередньо на периферії, що робить розширену аналітику доступною для клієнтів середнього та державного секторів. Завдяки вбудованій обробці даних, камери i-PRO можуть виконувати виявлення, класифікацію та аналіз поведінки об’єктів без необхідності дорогої серверної інфраструктури.

Ці камери популярні в роздрібній торгівлі, освіті та муніципальних установах, де бюджети контролюються, але розумна аналітика з урахуванням конфіденційності все ще важлива. Підтримка гібридної хмари та локального розгортання також робить Panasonic i-PRO привабливим для організацій, яким потрібна гнучкість у зберіганні та управлінні відео.

Sony – Чудові сенсори зображення та продуктивність за умов слабкого освітлення

Sony використовує свою відому технологію датчиків зображення для створення камер з винятковою продуктивністю в умовах слабкого освітлення та точністю передачі кольору. Це робить Sony сильним кандидатом для місць з

обмеженим освітленням, таких як паркінги, провулки, вантажні рампи та зовнішні периметри.

Підприємства, яким потрібні чіткі, деталізовані зображення майже в умовах повної темряви – без надмірного використання видимого або інфрачервоного освітлення – отримують вигоду від широкого динамічного діапазону та продуктивності сенсора Sony. Ці переваги особливо цінні для розслідування інцидентів та ідентифікації номерних знаків або облич у реальних умовах.

Digital Watchdog – гнучкі рішення

Digital Watchdog пропонує широкий спектр IP-камер, відеореєстраторів та платформ керування відео, адаптованих для комерційного розгортання по всій Північній Америці. Її системи часто включають розширену відеоаналітику, розпізнавання номерних знаків та гнучкі варіанти інтеграції, які добре працюють у роздрібній торгівлі, готельному бізнесі та управлінні нерухомістю.

Digital Watchdog поєднує продуктивність та вартість, що робить його гарним вибором для малого та середнього бізнесу, який хоче отримати професійні функції та довгострокову підтримку, не переходячи на преміальні корпоративні тарифні плани.

Ключові характеристики, які слід шукати в камерах відеонагляду для бізнесу

Окрім бренду, важливо оцінити технічні можливості та відповідність вашому конкретному середовищу. Оцінюючи камери відеонагляду для бізнесу, пріоритетними є такі характеристики:

– Роздільна здатність та чіткість – для більшості комерційних приміщень роздільна здатність від 4 до 8 МП (до 4K) забезпечує надійний баланс між деталізацією та вимогами до пам’яті, дозволяючи чітко ідентифікувати людей та номерні знаки в типових зонах покриття.

– Продуктивність за умов слабкого освітлення та WDR – шукайте камери з високою продуктивністю за умов слабкого освітлення та широким динамічним

діапазоном, щоб вони могли знімати яскраві вітрини магазинів, підсвічені вестибюлі та тьмяні коридори без втрати деталей.

– Штучний інтелект та відеоаналітика – багато камер сучасного покоління від Hanwha, Axis, Bosch та Panasonic пропонують вбудовану аналітику, таку як класифікація людей та транспортних засобів, час перебування, перетин лінії та аналіз присутності, що покращує як безпеку, так і роботу.

– Віддалений доступ та доступ до кількох об'єктів – підключені до хмари або централізовано керовані IP-системи дозволяють переглядати кілька локацій з одного інтерфейсу, що ідеально підходить для компаній з кількома будівлями або об'єктами.

– Захист від атмосферних впливів та вандалостійкість – Зовнішні та відкриті камери повинні мати такі показники захисту, як IP66/67 та IK10, що забезпечують стійкість до пилу, води та ударів, особливо на рівні вулиці або в місцях з високою прохідністю.

– Масштабованість та інтеграція – Забезпечте можливість розвитку системи разом з вашим бізнесом та інтеграцію з контролем доступу, домофонами, сигналізацією та управлінням відвідувачами, щоб з часом ви могли створити єдину платформу відеонагляду.

– Функції кібервідеонагляду та конфіденційності – Сучасні бренди, орієнтовані на підприємства, тепер пропонують безпечне завантаження, підписану прошивку, шифрування та маскування конфіденційності для підтримки відповідності вимогам та захисту від кіберзагроз.

Навіть найкращі бренди камер відеонагляду працюватимуть неефективно, якщо їх неправильно спроектувати та встановити. Професійне проектування та розгортання гарантують, що ваші камери охоплюють потрібні зони, ваша мережа та інфраструктура запису стабільні, а ваша система відповідає місцевим нормам.

Професійний інтегратор комерційного відеонагляду зазвичай:

– Проведіть оцінку на місці, щоб виявити зони ризику, вузькі місця та прогалини в покритті.

– Розробіть власне розташування камери з відповідним вибором об'єктивів, роздільною здатністю та положеннями кріплення.

– Налаштуйте розклади запису, політики зберігання та дозволи користувачів відповідно до вимог вашого бізнесу та законодавства.

– Інтегруйте камери з системами контролю доступу, домофоном та сигналізацією, щоб створити єдину екосистему відеонагляду, керовану подіями.

– Проведіть навчання користувачів, щоб ваша команда могла ефективно переглядати відзнятий матеріал, реагувати на сповіщення та експортувати відео за потреби.

– Пропонуйте постійне технічне обслуговування, моніторинг справності та оновлення, щоб ваша система була безпечною та актуальною протягом усього її життєвого циклу.

Вибір правильної системи відеоспостереження для бізнесу

«Найкращі камери відеонагляду для бізнесу» виглядатимуть по-різному для невеликого бутика, офісної вежі з кількома орендарями та логістичного центру. Бюджет, профіль ризику, вимоги до відповідності та плани зростання впливають на те, який бренд та архітектура підійдуть саме вам. Через це найефективніший шлях – співпрацювати з комерційним партнером з відеонагляду, який пропонує портфоліо провідних брендів, таких як Hanwha, Axis, Bosch, Pelco, Panasonic, Sony та Digital Watchdog, і може порекомендувати індивідуальну комбінацію камер, відеореєстраторів та аналітичних систем для вашого середовища. Гарний інтегратор допоможе вам збалансувати вартість та покриття, спроектувати систему для майбутнього розширення та забезпечити її придатність до роботи та відповідність вимогам протягом багатьох років. Інвестуючи сьогодні в професійно розроблену систему камер відеоспостереження, що відповідає вашому бренду, ваш бізнес отримує більше, ніж просто відеодокази. Ви отримуєте постійний контроль над тим, що відбувається на ваших об'єктах, дані для покращення відеонагляду та операцій, а також душевний спокій, який виникає від усвідомлення того, що ваші люди та майно захищені цілодобово.

3.2 Розробка структурної схеми

Ви можете бути знайомі з деякими з найновіших технологій фізичного відеонагляду, оскільки вони, як правило, відіграють важливу роль у повсякденному житті. Багато офісних приміщень та комерційних будівель оснащені низкою технологій фізичного відеонагляду. IP-камери відеонагляду та системи сигналізації є одними з найпоширеніших прикладів технологій відеонагляду, але є деякі додаткові технологічні тенденції корпоративного відеонагляду, які починають впливати на сучасні технології систем фізичного відеонагляду, зокрема:

Хмарні рішення для відеоспостереження

Хмарні технології продовжують революціонізувати способи зберігання та обміну інформацією в компаніях, закладаючи міцну основу для майбутнього управління безпекою. Хмарні обчислення, як одна з провідних тенденцій відеонагляду 2026 року, сприяють оптимізованому управлінню безпекою на кількох об'єктах, інтегрованим технологічним рішенням відеонагляду та забезпечують повністю віддалені операції відеонагляду.

В результаті, компанії та служби відеонагляду можуть отримувати доступ, керувати та контролювати свої операції відеонагляду з будь-якого місця та в будь-який час. Оператори відеонагляду більше не обмежуються моніторингом подій на своїх об'єктах з-за своїх робочих столів або в диспетчерській відеоспостереження . Команди можуть виконувати свої щоденні обов'язки та контролювати діяльність на місці дистанційно за допомогою відеокамер, таких як IP-камери з куполом, а також у дорозі через браузери або мобільні пристрої.

Рішення у сфері технологій відеонагляду, що керуються через хмару, такі як хмарні системи відеоспостереження, також поширюються на завдання технічного обслуговування та забезпечення доступності систем і визначені як одна з нових тенденцій у сфері технологій відеонагляду 2026 року . Підприємства отримують сповіщення в режимі реального часу на свої мобільні пристрої у разі

несправності камери відеонагляду або збою сервера. Завдяки цьому команди відеонагляду можуть переконатися, що їхні системи працюють для забезпечення відеонагляду людей, активів та приміщень.

Хоча хмарна безпека допомогла бізнесу адаптуватися до гнучких та гібридних моделей роботи, вона також пов'язана з ризиками. Оскільки компанії все більше покладаються на хмарне сховище для своїх технологій та пристроїв відеонагляду, вони повинні посилити свої заходи відеонагляду для захисту від втрати даних та загроз хакерства. Впровадження рішень відеонагляду, таких як системи виявлення вторгнень, системи контролю доступу до дверей та розширене шифрування даних, може забезпечити безпеку та надійний захист інформації бізнесу.

Використання штучного інтелекту та машинного навчання

Можливості штучного інтелекту та машинного навчання мають вирішальне значення для забезпечення глобального відеонагляду бізнес-операцій та даних клієнтів. Технології штучного інтелекту можуть виявляти аномалії мережевого трафіку та даних, а також відстежувати поведінку користувачів на предмет будь-якої підозрілої активності як з кібер-, так і з фізичного рівня відеонагляду.

У галузі вже спостерігається значний стрибок у точності та надійності відеокамер, оснащених аналітикою на основі штучного інтелекту . Ця інтелектуальна технологія значно зменшує залежність операторів від постійного моніторингу відео в реальному часі.

Системи камер на базі штучного інтелекту можуть точно виявляти та ідентифікувати людей, класифікувати транспортні засоби та об'єкти, а також точно визначати їхнє місцезнаходження та забезпечувати швидший пошук. З точки зору бізнес-операцій, рішення для відеоаналітики на основі штучного інтелекту можуть надати ключову інформацію, яка допоможе збільшити дохід та зменшити неефективність завдяки тепловим картам, підрахунку людей/транспортних засобів та аналізу журналів активності.

Деякі з найновіших інструментів відеоаналітики на основі штучного інтелекту, що використовуються компаніями для покращення операцій відеоспостереження, включають:

– **Автоматичне розпізнавання номерних знаків (ALPR):** Завдяки поєднанню технологій оптичного розпізнавання символів (OCR) та глибокого навчання, програмне забезпечення ALPR може виявляти та зчитувати інформацію про номерні знаки транспортних засобів, що проїжджають повз, для підтримки операцій управління паркуванням та контролю доступу транспортних засобів.

– **Відстеження об'єктів:** Аналітику відстеження об'єктів можна навчити контролювати певні елементи в полі зору камери, блокуючи при цьому подразники, пов'язані зі звичайними умовами навколишнього середовища, що робить її корисною в логістиці, управлінні дорожнім рухом та безпеці транспорту.

– **Ідентифікація особи:** Новітні технології відеонагляду у відеоаналітиці на основі штучного інтелекту можуть виявляти присутність певних осіб за допомогою поєднання розпізнавання обличчя, голосу та поведінкової біометрії, щоб допомогти командам відеонагляду ідентифікувати осіб, що представляють інтерес.

– **Виявлення вогнепальної зброї:** Найновіша технологія штучного інтелекту показує, що можна виявляти наявність вогнепальної зброї як за допомогою алгоритмів ідентифікації об'єктів, так і за допомогою алгоритмів аналітики штучного інтелекту для виявлення пострілів.

– **Виявлення предметів без нагляду: відеоаналітику** на основі штучного інтелекту можна навчити ретельно спостерігати за статичними предметами у встановлених місцях, що дозволяє командам отримувати сповіщення та програмувати ширші реакції технік відеонагляду, якщо предмет переміщено або потенційно небезпечний предмет залишено у зоні високого ризику.

Машинне навчання продовжує бути важливим компонентом нових тенденцій технологій інформаційного відеонагляду 2026 року та може бути знайдено в багатьох сучасних системах розпізнавання номерних знаків та рішеннях для управління відео. Завдяки постійному моніторингу конфігурацій мережі та системи на наявність підозрілої активності та забезпеченню автоматичної реакції на будь-які виявлені загрози, команди відеонагляду можуть бути в курсі потенційних інцидентів у режимі реального часу. Серед тенденцій фізичного відеонагляду та кібервідеонагляду 2026 року саме цю варто уважно стежити, оскільки головною перевагою машинного навчання є те, що з часом технологія стає лише швидшою та точнішою.

Індустрія відеонагляду переживає різке зростання попиту на штучний інтелект (ШІ) у камерах та комплексних системах фізичного відеонагляду. Хоча камери з відеоаналітикою на основі ШІ вже використовуються в різних сферах застосування, нові досягнення в технологіях відеонагляду роблять ШІ більш цінним для підприємств, які раніше вважали, що він їм не потрібен.

Найновіша технологія відеонагляду на основі штучного інтелекту для різних типів камер може точно розпізнавати аномальну поведінку та розрізняти людей, транспортні засоби та об'єкти для генерування даних про місцезнаходження та рух, а також надсилати автоматичні сповіщення, щоб команди були краще інформовані.

Технології відеонагляду на основі штучного інтелекту також використовуються в інтелектуальних датчиках, щоб допомогти власникам нерухомості виявляти інциденти вейпінгу в школах, розбите скло та постріли, а аналітика виявлення звуку допомагає визначити, де відбувається інцидент.

Зі зростанням популярності генеративного штучного інтелекту та мовних моделей, таких як ChatGPT, штучний інтелект міцно опинився в центрі уваги громадськості. Бізнес повинен усвідомлювати ризики для кібервідеонагляду та конфіденційності, пов'язані з такими технологіями. Мережі камер є майданчиками для зловмисних хакерів, і необхідно вживати заходів для захисту

інфраструктури, включаючи шифрування, встановлення останніх оновлень програмного забезпечення та дотримання передових практик кібервідеонагляду – однієї з ключових тенденцій кібервідеонагляду та інформаційного відеонагляду 2026 року, яка, ймовірно, впливатиме на майбутнє розвитку відеонагляду протягом багатьох років.

Бізнес також не повинен надмірно залежати від штучного інтелекту та машинного навчання для управління своїми операціями відеонагляду. Людський внесок все ще має вирішальне значення для захисту цінних активів та людей, тому команди відеонагляду повинні знайти баланс між використанням технологічних рішень відеонагляду на основі штучного інтелекту та машинного навчання, не позбавляючи при цьому цінної участі навченого оператора-людини.

Об'єднання систем відеонагляду та централізованих платформ

В останні роки компанії почали інтегрувати різні рішення в галузі технологій відеонагляду з новими тенденціями контролю доступу, щоб підвищити безпеку та захист у своїх приміщеннях. Очевидним об'єднанням, про яке знає більшість підприємств, є інтеграція контролю доступу з відеоспостереженням для синхронізації записів з діяльністю доступу в точках доступу, щоб оператори могли перевіряти події.

Однак існує більше інтеграцій, які можуть ще більше покращити операції відеонагляду. Потужні зв'язки через екосистему технологій, такі як інтеграція радіо з відеоохороною та контролем доступу, можуть призвести до більш ефективної роботи, вищої продуктивності та швидшого реагування на загрози та інциденти, що розвиваються. Усуваючи ці розрізненості та об'єднуючи їх на одній платформі, команди відеонагляду можуть спростити управління та автоматизувати робочі процеси. Наприклад, замість встановлення зчитувача доступу, камери відеонагляду та домофона біля вхідних дверей, універсальні системи відеодомофона тепер поєднують усі ці функції в одному пристрої.

Все більше організацій впроваджують свої існуючі системи в централізовані платформи для більш повного огляду своєї мережі відеонагляду.

Централізовані платформи забезпечують інтегрований центр відеонагляду для активів відеонагляду організації, включаючи фізичне обладнання, програмне забезпечення, засоби зв'язку, дані та рішення кібервідеонагляду, доступ до яких здійснюється з одного місця.

Рушійною силою їх впровадження є зменшення накладних витрат, пов'язаних з управлінням безпекою, водночас надаючи командам більш оптимізований метод масштабування систем відеонагляду та ефективніший спосіб реагування на інциденти. Спрощений, але масштабований підхід дозволяє компаніям відповідати операційним вимогам, одночасно зменшуючи витрати, пов'язані зі співпрацею з кількома постачальниками рішень відеонагляду.

Ось чому вкрай важливо знаходити рішення для технологій відеонагляду, побудовані на відкритій платформі, щоб забезпечити таку інтеграцію між різними платформами відеонагляду, а також з економічної точки зору. Технологія відеонагляду на відкритій платформі безперешкодно інтегрується з вашими існуючими системами, а це означає, що компаніям не потрібно копіювати та замінювати своє поточне обладнання, що заощаджує час і гроші.

Прогнозна аналітика відеонагляду

Виходячи за рамки простого виявлення, однією з головних тенденцій технологій відеонагляду на 2026 рік є зростання прогнозної аналітики. Ця технологія використовує штучний інтелект та машинне навчання для аналізу величезних обсягів даних, включаючи журнали інцидентів, дані датчиків у режимі реального часу, поведінку користувачів і навіть зовнішні потоки інформації про загрози.

Замість того, щоб просто реагувати на сповіщення, прогнозні системи відеонагляду прагнуть передбачати потенційні загрози до того, як вони матеріалізуються. Наприклад, система може виявити модель поведінки, яка, хоча сама по собі не є шкідливою, є відомим попередником кібератаки або фізичного порушення. Це дозволяє командам відеонагляду перейти від реактивної до проактивної позиції, розподіляючи ресурси між зонами або окремими особами з

високим рівнем ризику та нейтралізуючи загрози, перш ніж вони зможуть завдати шкоди. Ця проактивна здатність являє собою значний крок вперед у майбутньому технологій відеонагляду.

Конвергенція відеонагляду кіберфізичних систем (КФС)

Роками фізична безпека, така як камери та замки, і кібербезпека розглядалися як окремі сфери. Сьогодні ці дві галузі рішуче зближуються. Основною тенденцією 2026 року є зосередження уваги на безпеці кіберфізичних систем (КФС). Сучасні технології відеонагляду, від інтелектуальних камер до датчиків Інтернету речей та систем контролю доступу, – це всі мережеві пристрої. Це робить їх кіберфізичними системами.

Ця тенденція в галузі відеонагляду визнає, що кібератака може відімкнути фізичні двері, а фізичне порушення може надати доступ до IT- мережі. З цієї причини стратегії відеонагляду повинні бути цілісними. Це включає захист пристроїв, мереж, у яких вони працюють, та фізичного середовища, яке вони контролюють. Захист цієї точки конвергенції є критичним викликом для технологій відеонагляду, оскільки зловмисники все частіше шукають найслабшу ланку, будь то цифрова чи фізична.

Впровадження архітектури нульової довіри (ZTA)

Стара модель відеонагляду« довірена» внутрішня мережа та« Ненадійна» зовнішня мережа є застарілою, особливо при віддаленій роботі та хмарних сервісах. Модель архітектури нульової довіри (ZTA) швидко стає домінуючою тенденцією в інформаційній безпеці. Її основний принцип полягає в« Ніколи не довіряй, завжди перевіряй».

У системі ZTA жоден користувач чи пристрій не є довіреним за замовчуванням, незалежно від того, чи знаходиться він у мережі, чи поза нею. Кожен запит на доступ ретельно автентифікований, авторизований та шифрується перед його наданням. Це стосується як даних, так і фізичних активів. У 2026 році ми бачимо, як принципи ZTA застосовуються не лише до IT- мереж, а й до систем фізичного відеонагляду. Це означає, що картка-ключ, мобільні

облікові дані або навіть команда з консолі відеонагляду повинні постійно перевірятися, щоб значно зменшити ризик переміщення зловмисника через мережу після одного порушення.

Аналітика поведінки користувачів

Аналітика поведінки користувачів та об'єктів (UEBA) – це тренд у корпоративній безпеці, який привертає значну увагу серед фахівців з відеонагляду, враховуючи його здатність виявляти навіть найскладніші загрози. Використовуючи алгоритми машинного навчання, UEBA може виявляти будь-яку незвичайну поведінку користувачів, програм і мереж, а також попереджати команди про потенційні невідеонагляду в режимі реального часу.

Як це впливає на технології та безпеку для бізнесу? Розуміючи, як користувачі взаємодіють із системами, компанії можуть швидко виявляти та усувати будь-які загрози, перш ніж вони завдадуть шкоди. Системи UEBA, що є прогресом у порівнянні з системами UBA, які аналізували лише поведінку користувачів, є важливою тенденцією в галузі технологій кібервідеонагляду 2026 року, пропонуючи складнішу звітність та більшу здатність виявляти аномальну поведінку на основі додаткових даних та покращеного розпізнавання шаблонів.

Аналіз відео зі штучним інтелектом

Протягом останнього року штучний інтелект став чимось на зразок мейнстріму, і ми не можемо ігнорувати його наслідки для майбутнього відеонагляду.

Індустрія відеонагляду переживає різке зростання попиту на штучний інтелект (ШІ) у камерах та комплексних системах фізичного відеонагляду. Хоча камери з відеоаналітикою на основі ШІ вже використовуються в різних сферах застосування, нові досягнення в цій технології для відеонагляду роблять ШІ більш цінним для підприємств, які раніше вважали, що він їм не потрібен. Найновіша технологія відеонагляду на основі ШІ для різних типів камер, включаючи кульові IP-камери відеонагляду, може точно розпізнавати аномальну поведінку та розрізняти людей, транспортні засоби та об'єкти, генеруючи дані

про місцезнаходження та рух, а також надсилаючи автоматичні сповіщення, щоб команди були краще інформовані.

Технології відеонагляду на основі штучного інтелекту також використовуються в інтелектуальних датчиках, щоб допомогти власникам нерухомості виявляти випадки вейпінгу в школах, розбите скло та постріли, а аналітика виявлення звуку допомагає визначити, де відбувається інцидент. Справжня перевага цієї тенденції в галузі відеонагляду 2026 року полягає в інтеграції пристроїв та систем на базі штучного інтелекту для централізованого управління всією будівлею або підприємством в рамках єдиної програмної платформи для керування відео .

Оскільки ці перспективні пристрої використовують неймовірні обсяги даних для аналізу складних та мінливих елементів свого середовища, чим довше вони активні, тим точніше вони можуть виявляти потенційні загрози безпеці. Однак, потрапляння всіх цих даних у чужі руки може виявитися серйозною проблемою. Ось чому ще однією тенденцією технологій відеонагляду у 2026 році, за якою варто стежити, є те, як команди кібервідеонагляду та фізичного відеонагляду використовують технології штучного інтелекту для проактивного моніторингу мереж, модернізації аудиту відеонагляду, оптимізації систем моніторингу та розробки стратегій запобігання загрозам.

Технологія розумних датчиків

Роль інтелектуальних датчиків стає дедалі важливішою в безпеці. Ці передові пристрої оснащені здатністю виявляти зміни навколишнього середовища та загрози безпеці, змінюючи наш підхід до відеонагляду в різних умовах.

Розумні датчики, такі як HALO Smart Sensor, ідеально підходять для боротьби зі зростаючою проблемою вживання вейпів у школах, але мають розширені функції, що виходять за рамки виявлення вейпів. Датчики також виявляють зміни навколишнього середовища, такі як коливання якості повітря,

звукові аномалії, які можуть свідчити про агресію чи знущання, та присутність хімічних речовин, таких як сигаретний дим.

Значення інтелектуальних датчиків та нових технологій відеонагляду, таких як передові детектори вейпів, полягає в їхній здатності працювати в зонах, де важлива конфіденційність, таких як ванні кімнати та роздягальні, тоді як традиційні рішення з технологій відеонагляду є або непрактичними, або нав'язливими. Ця можливість є надзвичайно важливою, особливо в освітніх середовищах, де збереження конфіденційності учнів так само важливе, як і забезпечення їхнього відеонагляду.

Інтеграція інтелектуальних датчиків у ширші системи відеонагляду пропонує додатковий рівень захисту. Постійно спостерігаючи за змінами в навколишньому середовищі, ці датчики можуть надавати сповіщення в режимі реального часу та забезпечувати швидке реагування на потенційні загрози. Це не лише підвищує загальну безпеку, але й допомагає установам випереджати нові виклики, які, ймовірно, формуватимуть майбутнє тенденцій технологій відеонагляду.

Мобільно-орієнтована технологія

І останнє, але не менш важливе: прогнозується, що технології, орієнтовані на мобільні пристрої, стануть ключовим трендом фізичного відеонагляду у 2026 році та будуть у центрі уваги компаній, які прагнуть захистити свої приміщення. У світі, де домінують мобільні технології, попит на додатки, що дозволяють дистанційний моніторинг відеонагляду, вже не є винятком, а правилом.

Підприємства з кількома об'єктами або командами відеонагляду, що постійно працюють у русі, отримають найбільшу користь від можливостей віддаленого моніторингу, оскільки вони можуть отримати доступ до відеоматеріалів у реальному часі та записаних відео з кількох об'єктів прямо з долоні та легко виконувати завдання.

Більшість мобільних систем, таких як мобільні облікові дані, керуються в хмарі, що надає операторам більшу гнучкість в управлінні безпекою. Крім того,

люди вважають мобільні системи простими в експлуатації. Технологія мобільних систем відеонагляду є зручною, швидкою та надійною, або натисканням кнопки в додатку, або за допомогою безконтактних опцій контролю доступу .

Оскільки впровадження мобільних пристроїв продовжує зростати, майбутні тенденції в технологіях включатимуть ще більше вдосконалень для мобільних систем, що зробить їх ще безпечнішими та сумісніші з іншими системами будівель.

Сталий розвиток

Рішення у сфері сталого розвитку відеонагляду стали більш помітними у 2026 році, враховуючи переваги, які вони дають для досягнення спільних цілей організації. Зростання витрат та суспільний попит на сталий розвиток спонукали осіб, які приймають рішення, розглянути можливість впровадження більш екологічних активів у свою структуру фізичного відеонагляду.

Все більше компаній переходять на екологічно чисті пристрої та протоколи сталого захисту як частину своєї загальної стратегії відеонагляду. Технології, що сприяють розробці рішень для сталого захисту, включають енергоефективне обладнання, таке як камери на сонячних батареях, матеріали, що використовуються для переробки, світлодіодне освітлення та малопотужні сигналізаційні системи.

Інтеграція рішень сталого розвитку відеонагляду не лише допомагає знизити експлуатаційні витрати, але й забезпечує більшу масштабованість та надійність з меншими ресурсами. Оскільки компанії постійно прагнуть покращити безпеку зі зростанням, екологічно чисте та зелене обладнання може споживати менше енергії та виробляти менше викидів, що зрештою знижує витрати та підвищує публічний авторитет як лідера у сфері сталого розвитку.

Біометрична автентифікація

Біометрична авторизація – це ще одна тенденція в галузі відеонагляду, яка замінює традиційні методи контролю доступу, такі як ключ-картки та брелоки. У той час як покращений захист є основною метою служб відеонагляду,

занепокоєння щодо зростаючої втрати, крадіжки або спільного використання фізичних ключів доступу призвели до розгляду більш персоналізованих рішень, які допомагають забезпечити правильні дозволи.

З розвитком технологій фізичного відеонагляду біометрична автентифікація стала ефективним методом контролю доступу для бізнесу, а ринок зросте до очікуваних 70 мільярдів доларів у 2026 році . Привабливість автентифікації полягає в тому, що вона зменшує потребу користувачів носити фізичні ключі, а системи сканування використовують розпізнавання обличчя, відбитків пальців або очей для перевірки особи.

Переваги, які ця технологія надає організаціям, стимулюють їхнє швидке впровадження біометричного контролю доступу в чутливих зонах. До переваг належать зниження ризику несанкціонованого доступу, зручність для користувачів та детальніші журнали активності, які відображають точніші дані про те, хто мав доступ до обмежених зон.

Централізовані платформи

Тенденції відеонагляду 2026 року схиляються до більш інтегрованого підходу, який об'єднує всі компоненти в системі відеонагляду. Зростаючий попит на комплексний, інтуїтивно зрозумілий ландшафт відеонагляду поступився місцем централізованим платформам для бізнесу, щоб впроваджувати та керувати компонентами більш ефективно.

Централізовані платформи забезпечують інтегрований центр відеонагляду для активів відеонагляду організації, включаючи фізичне обладнання, програмне забезпечення, засоби зв'язку, дані та рішення кібервідеонагляду, доступ до яких здійснюється з одного місця. Рушійною силою їх впровадження є сприяння зменшенню накладних витрат, пов'язаних з управлінням безпекою, водночас надаючи командам більш оптимізований метод масштабування систем відеонагляду та ефективніший спосіб реагування на інциденти.

Все більше організацій впроваджують свої існуючі системи на централізованих платформах для більш повного огляду своєї мережі

відеонагляду. Спрощений, але масштабований підхід дозволяє компаніям відповідати операційним вимогам, одночасно зменшуючи витрати, пов'язані зі співпрацею з кількома постачальниками рішень відеонагляду.

Рисунок 3.1 – Структурна схема системи

Як різні галузі використовують технології відеонагляду

Підприємства та організації в різних галузях промисловості по всьому світу впроваджують трендові рішення відеонагляду в міру розвитку загроз. Зі зростанням кількості фізичних інцидентів та інцидентів з кібербезпекою різні сектори використовують технології відеонагляду в різних цілях для зменшення проблем, пов'язаних із вторгненнями та порушеннями.

Ось як деякі з галузей використовують технології відеонагляду:

Освіта

Безпека учнів у кампусах є одним із головних завдань адміністрації шкіл у кожному окрузі. Ради впровадять систему відеонагляду школи, яка включає відеокамери, контроль доступу та інтелектуальні сенсорні пристрої навколо ключових зон, щоб допомогти захистити як викладачів, так і учнів.

Охорона здоров'я

Підприємства та організації в галузі охорони здоров'я потребують комплексної стратегії відеонагляду, особливо враховуючи цінні та конфіденційні активи та дані, які вони зберігають. Системи контролю доступу до медичних закладів захищають обмежені зони з контрольованими речовинами та стерильні операційні, а камери відеонагляду на базі штучного інтелекту постійно контролюють та аналізують поведінку в приміщеннях, щоб забезпечити швидке реагування на інциденти та захист пацієнтів.

Роздрібна торгівля

Вітрини магазинів та торгові центри мають значно більшу кількість людей порівняно з іншими галузями. У роздрібних магазинах зазвичай встановлюються камери відеонагляду та інтелектуальні сенсорні технології, щоб допомогти керувати натовпом, запобігати крадіжкам та захищати товарні запаси.

Будівництво

Будівельні майданчики становлять більше небезпек для людей, враховуючи характер галузі. Програмне забезпечення для аналітики на основі штучного інтелекту допомагає керівникам проектів та керівникам планувати стратегії відеонагляду будівництва на всьому об'єкті, де вони встановлюватимуть камери промислового класу для контролю за операціями, виявлення потенційних проблем відеонагляду та забезпечення дотримання вимог щодо здоров'я та відеонагляду працівників.

Фінанси та банківська справа

У фінансах та банківській справі технології відеонагляду мають вирішальне значення для захисту цінних активів та конфіденційних даних. Передові заходи банківського відеонагляду, такі як біометрична перевірка, хмарні рішення, виявлення руху та надійні платформи кібервідеонагляду, є важливими для захисту установ від загроз, що постійно змінюються.

Центри обробки даних

Для безперебійної роботи безпека центру обробки даних вимагає єдиної та комплексної стратегії. Це включає камери, теплові детектори, розширений контроль доступу та надійні протоколи кібервідеонагляду для запобігання будь-яким збоям, які можуть суттєво вплинути на ваш бізнес.

Комерційні офіси

Комерційні та корпоративні офіси часто містять конфіденційну інформацію, важливу для їхньої щоденної діяльності, а це означає, що будь-які фізичні чи цифрові збої можуть дорого коштувати бізнесу. Багато компаній у галузі інтегрують централізовані платформи зі спеціальними сповіщеннями в режимі реального часу, щоб комерційні команди відеонагляду могли контролювати як фізичні, так і кіберзагрози.

Уряд

Урядові установи стикаються з унікальними проблемами відеонагляду, від шпигунства до загроз з боку невдоволених громадян. Щоб забезпечити безпеку цих територій, посадовцям необхідно впровадити комплексну стратегію. Це включає відповідні урядові камери відеонагляду та вдосконалений біометричний контроль доступу для запобігання несанкціонованому проникненню та захисту від потенційних загроз.

Гостинність

Ресторани, бари та заклади громадського харчування більш схильні до публічних інцидентів, ніж багато інших галузей, потенційно приймаючи тисячі клієнтів щодня. Все більше закладів гостинності встановлюють камери на базі штучного інтелекту, щоб допомогти виявляти та аналізувати поведінку гостей, навчаючись, як забезпечити кращий досвід, а також вживати швидших і практичніших заходів у разі інциденту.

Майбутнє тенденцій у сфері технологій відеонагляду

Організації повинні бути пильними у захисті своїх даних від постійно зростаючого спектру загроз. Розуміння нових тенденцій у сфері технологій

фізичного відеонагляду, кібервідеонагляду та інформаційного відеонагляду 2026 року є важливим кроком, який будь-яка організація може зробити для захисту своїх активів. Хоча інвестування в рішення для технологій відеонагляду допомагає захистити людей, активи та приміщення, заходи кібервідеонагляду запобігають спробам зловмисного злому та витокам даних.

Бізнесу необхідно постійно бути в курсі мінливих ризиків, пов'язаних з фізичними та кіберзагрозами. Зменшення цих ризиків починається з комплексного плану конвергенції відеонагляду, щоб створити ефективний захист від низки потенційних загроз безпеці.

Використання найновіших тенденцій у сфері технологій відеонагляду може допомогти організаціям застосовувати більш проактивний підхід. Майбутні тенденції у сфері технологій відеонагляду 2026 року вказують на більш спільні, інтегровані та цілісні системи, що надають командам відеонагляду більше даних, ніж будь-коли. Саме тому інвестування в технології на базі штучного інтелекту є важливою тенденцією, якої варто дотримуватися, адже автоматизація, інтеграції та хмарні технології допомагають компаніям розуміти моделі поведінки, приймати обґрунтовані рішення та швидко реагувати на інциденти.

Такий захист може вимагати значних початкових інвестицій, але відстеження майбутніх технологічних тенденцій у сфері відеонагляду може заощадити організації час і кошти в довгостроковій перспективі. Крім того, впровадження надійних заходів відеонагляду може допомогти підвищити довіру клієнтів.

3.3 Розробка функціональної схеми

На рисунку 3.2 зображена функціональна схема системи. Нижче розглянемо її більш докладно.

Цифрова система мережевого комплексного засобу відеонагляду для підприємства, що розроблена:

– забезпечує високу якість відтвореного відеозапису;

– високу швидкість доступу до відеоархіву;

– можливість цифрового збільшення й масштабування будь-якого кадру;

– миттєвий пошук і перегляд відеозапису за камерою, датою й часом;

– можливість інтеграції з іншими комп'ютерними системами безпеки;

– легка й недорога трансляція відеоархівів по каналах зв'язку (Інтернет та ін.);

– можливість відправлення тривожних повідомлень по електронній пошті й SMS;

– можливість експорту відеоінформації на сумісні зовнішні носії.

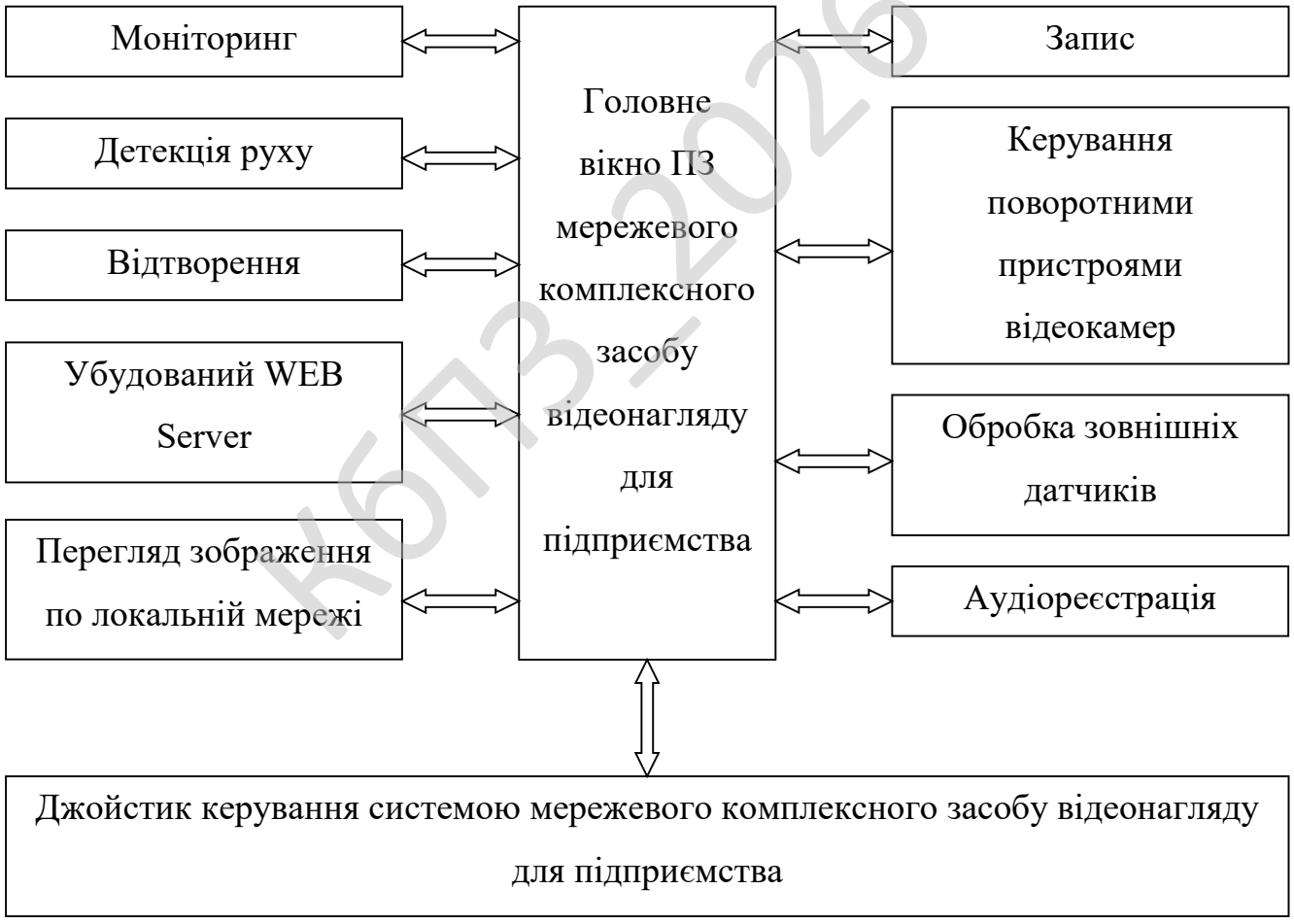

Рисунок 3.2 – Функціональна схема системи

Цифрові системи мережевого комплексного засобу відеонагляду для підприємства виконують наступні функції:

– Моніторинг. Можливе підключення до 32-х камер, відображення всіх на одному екрані. Можливість поділу камер на два монітори. Використання режиму overlay дозволяє виводити зображення на екран монітора з аналоговою якістю. Можливість цифрового збільшення в 2, 4, 8 і 16 разів. Функція голосового супроводу подій (при підключених аудіоколонках).

– Запис. Стиск зображення здійснюється за алгоритмом Motion-Wavelet (розмір кадру залежить від дозволу, кольоровості камери, ступеня стиску й деталізації зображення) дозволяє досягти значень бітрейта в межах від 2 до 80 Кб. Режими запису: по детекції руху, по команді, постійно, передзапис і дозапис по кожній камері.

– Детекція руху. Відстеження наявності об'єктів, що рухаються. Основні переваги: висока перешкодозахищеність, емпіричні настроювання за розміром й контрастністю зображення, конфігурування області детекції руху незалежно для кожної камери, візуальне виділення контурів об'єктів, що рухаються, перерозподіл ресурсів для тривожної камери.

– Відтворення. Одна камера в один момент часу, перегляд відеоархіву одночасно із записом, індексація відеоархіву при запуску системи для швидкого пошуку, пошук у відеоархіві по даті й часу, відображення щільності запису за добу, покадрове програвання вперед та назад, збільшення швидкості програвання до 25 Fps, утиліта зовнішнього декодування й перегляду відеозаписів зроблених системою, можливість збереження шматків відеоархіву в avi, що б мати можливість перегляду на будь-якому комп'ютері.

– Убудований WEB server. Надає можливість контролювати й управляти відеокамерами, переглядати відеоархів, а також здійснювати постановку й зняття з охорони з віддаленого комп'ютера через web-браузер.

– Аудіореєстрація. Дозволяє вводити в систему аналоговий сигнал із зовнішніх джерел: мікрофонів, телефонних каналів і інших. Аудіореєстрація

може вестися по незалежних каналах, а може й синхронно. У випадку настроювання аудіореєстрації разом з відеозображенням, архів від цих камер записується спільно зі звуком. Аудіореєстрація необхідна у випадках недостачі тієї інформації, що надають відеокамери. Більше твердий контроль за підлеглими й персоналом. Найбільш часті сфери й місця застосування аудіоконтроля – кімнати переговорів і нарад, місця для паління, спостереження за будинком під час відсутності хазяїна, спостереження за обслуговуючим персоналом, (покоївкою, гувернанткою й іншою прислугою), запис телефонних переговорів секретаря. Для реалізації необхідного ефекту від аудіоконтролю й поліпшення розбірливості записаного архіву рекомендується застосування якісного встаткування прослуховування.

– Перегляд зображення по локальній мережі. Інтерфейс віддаленого робочого місця нічим не відрізняється від інтерфейсу на відеосервері. Завдяки чому доступні всі функції по керуванню системою, що й на сервері, включаючи перегляд відеоархіву й звуковий супровід. Існує відмінність як зображення відео на віддаленому робочому місці від зображення на відеосервері. Так, як по лініях зв'язку передається стисле зображення, якість відображення цілком залежить від величини стиску відеосигналу, установленої по кожній камері на відеосервері. Віддалених робочих місць може бути трохи: використовується так званий мережний режим. Такий режим може бути використаний на об'єктах з декількома постами охорони, з наявністю постів начальника охорони, адміністратора системи безпеки; для забезпечення можливості спостереження за переміщенням співробітників начальницькому составу; а також для аналізу архіву відеозображення віддалено по локальній мережі не займаючи робоче місце співробітників оперативної служби.

– Керування поворотними пристроями відеокамер. Програмне забезпечення має можливість підключення поворотних пристроїв відеокамер і керування ними прямо з робочого місця.

– Обробка зовнішніх датчиків. Крім функцій мережевого комплексного засобу відеонагляду для підприємства може виконувати контролювати різні датчики (охоронної й пожежної сигналізацій), і управляти зовнішніми виконавчими пристроями (сиреною, голосовим оповіщувачем або іншим пристроєм).

– Джойстик керування системою мережевого комплексного засобу відеонагляду для підприємства. Маніпулятор для керування системою заміняє мишу й клавіатуру. При експлуатації цифрових відеосерверів нерідко виникають проблемами втручання оператора в роботу системи: зміна настроювань операційної системи, настроювань програми мережевого комплексного засобу відеонагляду для підприємства, установки ігор і сторонніх додатків. Рішенням даної проблеми є заміна стандартних пристроїв уведення (клавіатури й миші) на спеціалізований маніпулятор. Даний маніпулятор дозволяє працювати тільки із програмним забезпеченням .

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

3.4 Розробка діаграми процесів

Розглянемо розроблену діаграму процесів яка зображена на рисунку 3.3. Основна будова діаграми процесів полягає у графічному представленні складу сукупностей даних, що характеризуються як співвідношення різних частин кожної з сукупностей.

Склад статистичної сукупності графічно може бути представлений як за допомогою абсолютних, так і відносних показників.

Графічне зображення складу сукупності по абсолютними і відносними показниками сприяє проведенню більш глибокого аналізу і дозволяє проводити аналіз системи.

Діаграма взаємодії процесів використовується для візуалізації процесів обробки даних (структурне проектування). Для розробника вважається звичним спочатку креслити діаграму взаємодії процесів даних рівня контексту, завдяки чому буде показано взаємодію системи. Ця діаграма в подальшому підлягає уточненню шляхом деталізації процесів та потоків даних з метою показати систему що розробляється. При детальному її розгляді можна побачити як саме проходе взаємодія у розробленій системі. Використовується модель проектування, графічне представлення «потоків» даних в інформаційній системі.

Діаграми потоків даних містять чотири типи елементів:

– Зовнішні по відношенню до системи сутності.

– Потоки даних між елементами трьох попередніх типів.

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

– Сховища даних (репозиторії).

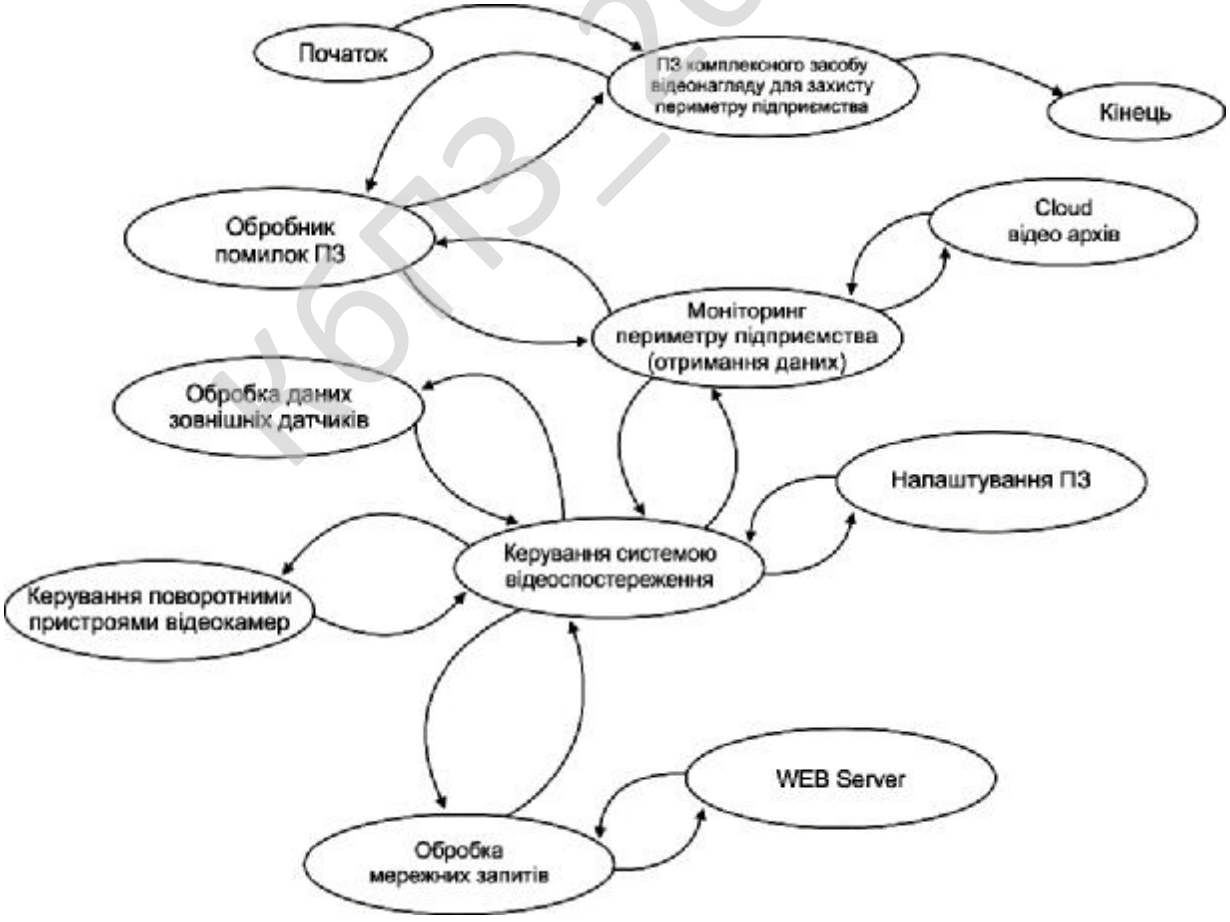

Рисунок 3.3 – Діаграма взаємодії процесів

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

4.1 Блок-схеми та опис алгоритмів функціонування системи

Розглянемо реалізацію бакалаврської дипломної роботи. Були проведені розрахунки і підібрані набори тестових даних для перевірки правильності реалізації проектних рішень. Блок-схеми показують весь процес роботи системи з підсистемами та частково доказують правильність вибраних проектних рішень. Тому від точності і детальної блок-схеми залежить результат всієї програми.

При виборі початкової точки відліку при побудові схем було враховано, що виходячи з вибору мови програмування і інших технічних засобів, програма буде об’єктно-орієнтована що вимагає високого рівня декомпозиції задач на класи.

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

З яких видно що робота основної програми складається з початкових етапів ініціалізації ПЗ, перевірки наявності ресурсів системи, блоку початку основного циклу з чеканням запиту від користувача в якому відбувається виклик підсистеми та останньої стадії – перевірка поточного стану з завершенням роботи розробленого ПЗ. При роботі підпрограми виконується основний функціонал системи з циклічними послідовностями, перевіркою поточного стану та поверненням в основну програму прапорів стану виконання. Було використано підходи з використанням UML, це уніфікована мова моделювання, використовується у парадигмі об'єктно-орієнтованого програмування. Є невід'ємною частиною уніфікованого процесу розробки програмного забезпечення. UML є мовою широкого профілю, це відкритий стандарт, що

використовує графічні позначення для створення абстрактної моделі системи, називаної UML-моделлю. UML був створений для визначення, візуалізації, проектування й документування в основному програмних систем. UML не є мовою програмування, але в засобах виконання UML-моделей як інтерпретованого коду можлива кодогенерація.

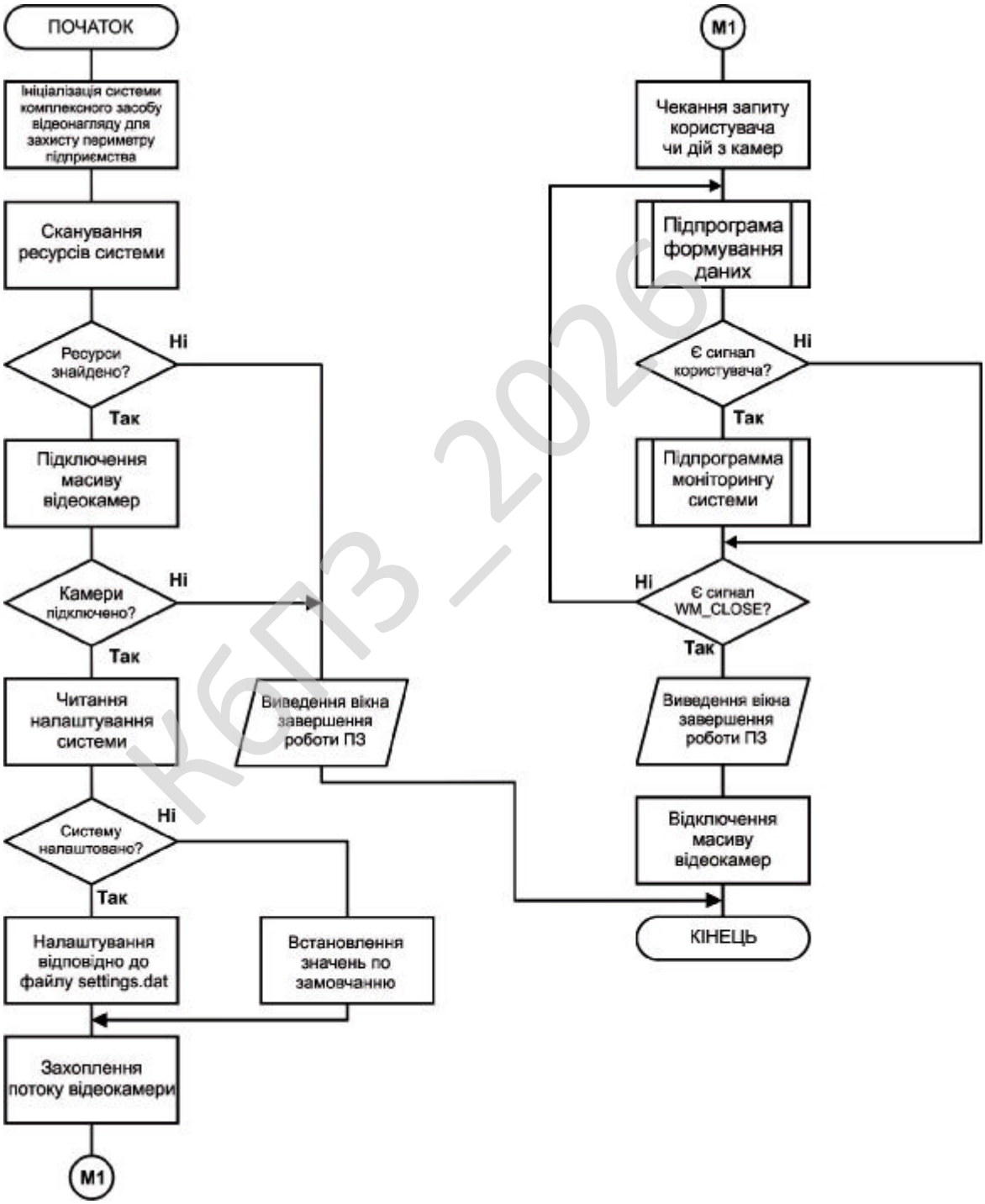

Рисунок 4.1 – Блок-схема основної програми

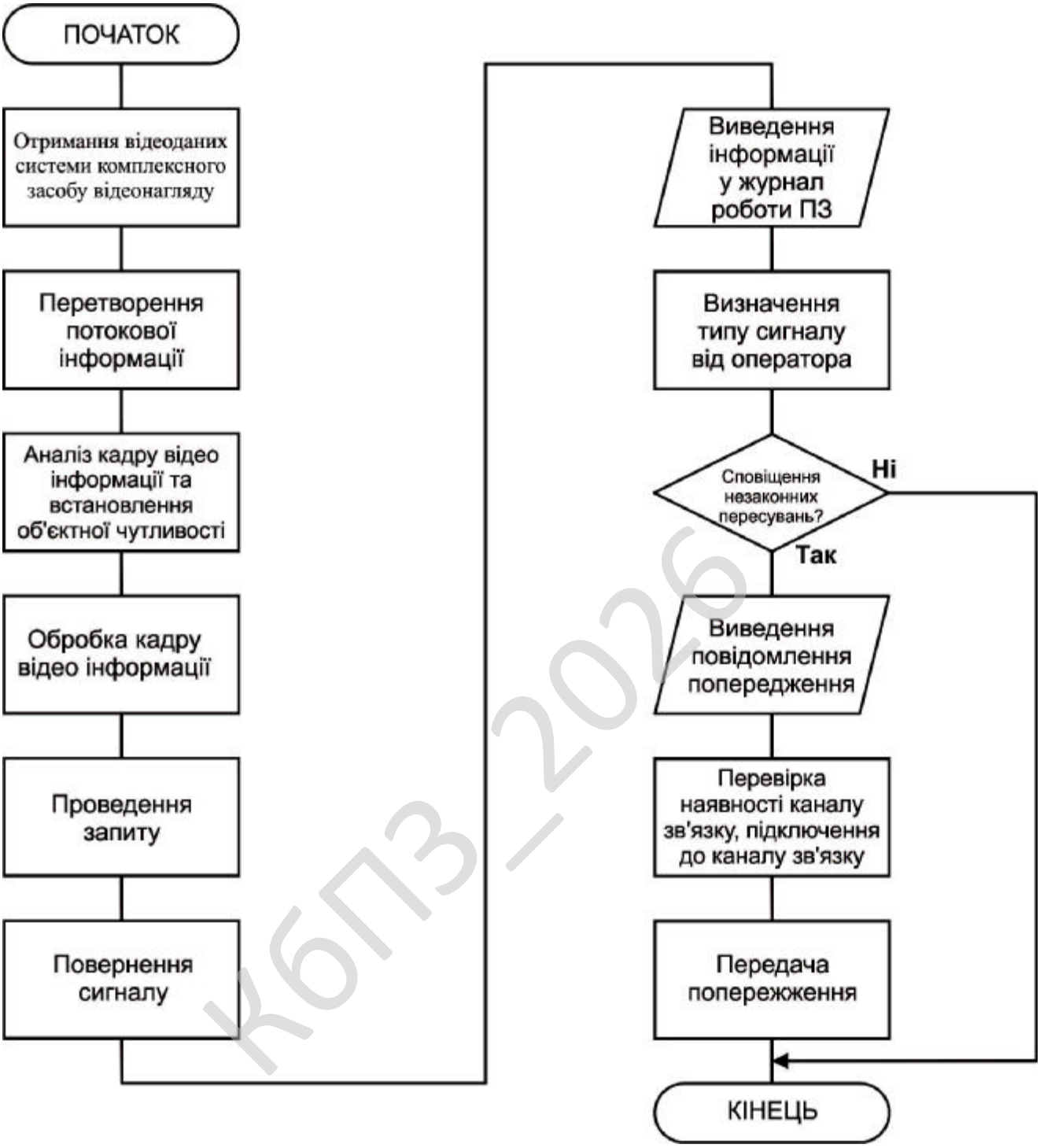

Рисунок 4.2 – Блок-схема роботи підпрограми

Використовувалась БД SQLite – полегшена реляційна система керування базами даних. Втілена у вигляді бібліотеки, де реалізовано багато зі стандарту SQL-92.

Сирцевий код SQLite поширюється як суспільне надбання (public domain), тобто може використовуватися без обмежень та безоплатно з будь-якою метою. Фінансову підтримку розробників SQLite здійснює спеціально створений консорціум, до якого входять такі компанії, як Adobe, Oracle, Mozilla, Nokia, Bentley і Bloomberg.

З 2018р SQLite, як й JSON та CSV, рекомендований Бібліотекою Конгресу США формат зберігання структурованого набору даних. У 2005 році проект отримав нагороду Google-O'Reilly Open Source Awards.

Особливістю SQLite є те, що вона не використовує парадигму клієнт-сервер, тобто рушій SQLite не є окремим процесом, з яким взаємодіє застосунок, а надає бібліотеку, з якою програма компілюється і рушій стає складовою частиною програми.

Таким чином, як протокол обміну використовуються виклики функцій (API) бібліотеки SQLite. Такий підхід зменшує накладні витрати, час відгуку і спрощує програму.

SQLite зберігає всю базу даних (включаючи визначення, таблиці, індекси і дані) в єдиному стандартному файлі на тому комп'ютері, на якому виконується застосунок.

Простота реалізації досягається за рахунок того, що перед початком виконання транзакції весь файл, що зберігає базу даних, блокується; ACID-функції досягаються зокрема за рахунок створення файлу-журналу.

Кілька процесів або потоків можуть одночасно без жодних проблем читати дані з однієї бази. Запис в базу можна здійснити тільки в тому випадку, коли жодних інших запитів у цей час не обслуговується; інакше спроба запису закінчується невдачею, і в програму повертається код помилки. Іншим варіантом розвитку подій є автоматичне повторення спроб запису протягом заданого інтервалу часу.

У комплекті постачання йде також функціональна клієнтська частина у вигляді виконуваного файлу sqlite3, за допомогою якого демонструється

реалізація функцій основної бібліотеки. Клієнтська частина працює з командного рядка, і дозволяє звертатися до файлу БД на основі типових функцій ОС.

Завдяки архітектурі рушія можливо використовувати SQlite як на вбудовуваних (embedded) системах, так і на виділених машинах з гігабайтними масивами даних.

Особливості SQLite:

1. Транзакції атомарні, послідовні, ізольовані, і міцні (ACID) навіть після збоїв системи і збоїв живлення.

2. Встановлення без конфігурації – не потребує ані установки, ані адміністрування.

3. Реалізує значну частину стандарту SQL92.

4. База даних зберігається в одному крос-платформовому файлі на диску.

5. Підтримка терабайтних розмірів баз даних і гігабайтного розміру рядків і BLOBів.

6. Малий розмір коду: менше ніж 350KB повністю налаштований, і менш 200KB з опущеними додатковими функціями.

7. Швидший за популярні рушії клієнт-серверних баз даних для найпоширеніших операцій.

8. Простий, легкий у використанні API.

9. Написана в ANSI C, включена прив'язка до TCL; доступні також прив'язки для десятків інших мов.

10. Добре прокоментований сирцевий код зі 100% тестовий покриттям гілок.

11. Доступний як єдиний файл сирцевого коду на ANSI C, який можна легко вставити в інший проект.

12. Автономність: немає зовнішніх залежностей.

13. Крос-платформовість: з коробки підтримується Unix (Linux і Mac OS X), OS/2, Windows (Win32 і WinCE). Легко переноситься на інші системи.

14. Сирці перебувають в суспільному надбанні.

15. Поставляється з автономним клієнтом інтерфейсу командного рядка, який може бути використаний для управління базами даних SQLite.

Інструменти створення та обслуговування БД

Створення та обслуговування БД можуть здійснюватись через текстову консоль SQL-командами або через спеціальні інструменти, у тому числі – з графічним інтерфейсом користувача.

Технології, що підтримують SQLite та мови програмування

Сама бібліотека SQLite написана мовою С. Проте є реалізація бібліотеки на JavaScript sql.js, яка дозволяє обробляти файли БД безпосередньо в браузері.

Для інших мов програмування розроблено механізм підключення й роботи з БД через цю бібліотеку: C++, Java, Python, Perl, PHP, Ruby, Haskell, Scheme, Smalltalk, Lua тощо. Засоби для роботи з Tcl включені в комплект постачання SQLite. Повний список наявних засобів можна знайти на сторінці проекту.

Web-інструментарії

У ряді інструментаріїв присутня можливість використання SQLite як бази даних, наприклад: Django; Java; PHP; Ruby on Rails; Trac; Symfony; Parser.

Багато програм підтримують SQLite як формат зберігання даних, зокрема:

1. Amarok – може використовувати бази даних SQLite як сховище музичної колекції.

2. Gajim – SQLite використовується для зберігання історії контактів.

3. Songbird (як застосунок, заснований на XULRunner 1.9)

4. Banshee.

5. F-Spot.

6. Платформа XUL на рушії Gecko 1.9, XULRunner 1.9 і, потенційно, всі застосунки, засновані на цій платформі, у тому числі й Firefox починаючи з версії 3.0.

7. Google Chrome.

8. Google Gears.

9. Mendeley – менеджер pdf-документів, академічний засіб для дослідження (реалізується desktop & web).

10. Zotero – менеджер інформації, бібліографічний менеджер, додаток Firefox.

Хоча я реалізовував програму сам, було використано підходи Scrum для саморозвитку та пришвидшенню розробки, розглянемо цей метод. Scrum – підхід управління проектами для гнучкої розробки програмного забезпечення. Скрам чітко робить акцент на якісному контролі процесу розробки.

Підхід вперше описали Гіротака Такеучі та Ікуджіро Нонака в статті The New New Product Development Game (Гарвардський Діловий Огляд, січ-лют 1986). Вони відзначили, що проекти, над якими працюють невеликі, крос–функціональні команди, зазвичай систематично продукують кращі результати, і пояснили це, як «підхід регбі». У 1991 році ДеҐрейс та Шталь у книжці Злі проблеми, справедливі рішення послалися на цей підхід, як на Scrum (штовханина; сутичка навколо м'яча (у регбі)), спортивний термін, згаданий в статті Такеучі і Нонака. Кен Швабер на початку 1990–х використовував підхід який привів Scrum в його компанію.

Вперше метод Scrum було представлено на загальний огляд задокументованим, чітко сформульованим та описаним спільно Сазерлендом та Швабером на OOPSLA'96 в Остіні. Швабер та Сазерленд протягом наступних років працювали разом щоб обробити та описати весь їхній досвід та найкращі практичні зразки для індустрії в одне ціле, в ту методологію, що відома сьогодні як Scrum. Швабер об'єднав зусилля з Майком Бідлом в 2001, щоб детально описати метод в книжці Agile Software Development with SCRUM. Не зважаючи на те, що для Scrum нарікли долю управління проектами з розробки ПЗ, він може також використовуватися в роботі команд обслуговувань програмного забезпечення (software maintenance teams), або як підхід управління розробкою і супроводом програм: Scrum of Scrums.

Scrum – це кістяк процесу, який включає набір методів і попередньо визначених ролей. Головні дійові особи – ScrumMaster, той хто опікується

процесами, веде їх і працює як керівник проекту, Власник Продукту, людина, що представляє інтереси кінцевих користувачів та інших зацікавлених в продукті сторін, та Команду, яка включає розробників.

Протягом кожного спринту, 15–30 денного періоду (тривалість визначається командою), працівники створюють функціональний ріст програмного забезпечення.

Набір можливостей, які імплементуються кожного спринту, приходять з етапу, що має назву product backlog (документація запитів на виконання робіт), який має найвищу пріоритетність за рівнем вимог до роботи, що повинна бути виконана.

Запити на виконання робіт (backlog items), що визначені протягом наради з планування спринту (sprint planning meeting), переміщуються в етап спринту. Протягом цієї наради Власник Продукту інформує про завдання, які він хоче, аби були виконані. Тоді Команда визначає, скільки з бажаного вони можуть зробити, щоб завершити необхідні частини протягом наступного спринту. Протягом спринту команда виконує визначений фіксований список завдань (т.з. backlog items). Впродовж цього періоду ніхто не має права змінювати перелік запитів на виконання робіт, що слід розуміти, як заморожування вимог (requirements) протягом спринту.

Product backlog – це документ, який має список вимог до функціональності, які упорядковані згідно зі ступенем важливості. Product backlog представляє список того, що повинно бути реалізовано. Елементи цього списку називається «історіями» (user story) або елементами backlog–у (backlog items). Product backlog відкритий для редагування усім учасникам Scrum–процесу.

Обов'язкові поля:

1. ID – унікальний ідентифікатор, порядковий номер, який використовується для ідентифікації історій у разі їх перейменування.

2. Назва (Name) – стислий опис історії. Він повинен бути однозначним, щоб і розробники і product owner могли зрозуміти, про що йдеться і відрізнити одну історію від іншої.

3. Важливість (Importance) – ступінь важливості даної історії на погляд product owner ’а. Зазвичай являє собою натуральне число, іноді для цієї цілі використовуються числа Фібоначчі. Чим більше значення, тим більше пріоритет.

4. Попередня оцінка (initial estimate) – початкова оцінка об'єму робіт, необхідного для реалізації історії порівняно з іншими історіями. Вимірюється у story point'ах. Приблизно відповідає числу «ідеальних людино–днів».

5. Як продемонструвати (how to demo) – стисле пояснення того, як завершена задача буде продемонстрована у кінці спринта. Дане поле може являти собою код автоматизованого приймального тесту.

Додаткові поля. Іноді, також, використовуються додаткові поля у product backlog, в основному для того, щоб допомогти product owner'у визначитися з його пріоритетами.

Категорія (track). Наприклад, «панель управління» чи «оптимізація». За допомогою цього поля product owner може легко вибрати усі пункти категорії «оптимізація» і задати їм низький пріоритет.

Компоненти (components) – указує, які компоненти (наприклад, база даних, сервер, клієнт) будуть зачеплені при реалізації історії. Дане поле складається з групи checkbox'ів, які відмічаються, якщо відповідні компоненти потребують змін.

Ініціатор запиту (requestor). Product owner може захотіти зберігати інформацію про усіх замовників, зацікавлених у даній задачі. Це потрібно для того, щоб тримати їх у курсі діла про хід виконання робіт.

ID у системі обліку помилок (bug tracking ID) – якщо ви використовуєте окрему систему обліку помилок, тоді у описі історії корисно зберігати посилання на всі дефекти, які до неї відносяться.

Sprint backlog – містить функціональність, обрану Product Owner із Product Backlog. Всі функції розбиті по задачах, кожна з яких оцінюється командою. Кожен день команда оцінює об'єм роботи, який необхідно провести для завершення задачі.

Burndown chart – показує, скільки вже виконано і скільки ще залишається зробити.

Планування спринта (Sprint Planning Meeting)

Проходить на початку нової ітерації Спринта:

– Із Product Backlog обираються задачі, зобов'язання по виконанню яких за спринт приймає на себе команда;

– На основі обраних задач створюється Sprint Backlog. Кожна задача оцінюється у ідеальних людино–годинах;

– Рішення задачі не повинно займати більше 12 годин або одного дня. При необхідності задача розбивається на підзадачі;

– Обговорюється та визначається, яким чином буде реалізовано цей об'єм робіт;

– Тривалість наради обмежена зверху 4–8 годинами в залежності від тривалості ітерації, досвіду команди тощо;

– (перша частина наради) Беруть участь Product Owner + Команда: обирають задачі із Product Backlog;

– (друга частина наради) Бере участь лише команда: обговорюють технічні деталі реалізації, наповнюють Sprint Backlog.

Щоденна нарада (Daily Scrum Meeting)

Відбувається кожен день протягом спринта. Є «пульсом» ходу спринта. Нараді властиві наступні обмеження:

– починається точно вчасно;

– всі можуть спостерігати, але говорять тільки обрані;

– триває не більш ніж 15 хвилин;

– проводиться в одному і тому ж місці протягом одного спринта.

Протягом наради кожен член команди відповідає на 3 запитання:

– Що зроблено з моменту попередньої щоденної наради?

– Що буде зроблено з моменту поточної наради до наступної?

– Які проблеми заважають досягненню цілей спринта? (Над рішенням цих проблем працює ScrumMaster. Зазвичай це рішення проходить за рамками щоденної наради і у складі осіб, що безпосередньо займаються даною перешкодою.)

Демонстрація (Sprint Review Meeting):

– Проходить у кінці ітерації (спринта).

– Команда демонструє внесок функціональності до продукту всім зацікавленим особам.

– Залучається максимальна кількість глядачів.

– Усі члени команди беруть участь у демонстрації (одна людина на демонстрацію або кожен показує, що зробив за спринт).

– Обмежена 4–ма годинами в залежності від тривалості ітерації і змін у продукті.

Ретроспектива (Sprint Retrospective):

– Члени команди висловлюють свою думку про минулий спринт.

– Відповідають на два основних запитання: Що було зроблено добре у минулому спринті? Що потрібно покращити в наступному?.

– Виконують покращення процесу розробки (вирішують питання та фіксують вдалі рішення).

– Обмежена 1–3ма годинами.

Подійно-орієнтована архітектура (Event-driven architecture, надалі EDA) – шаблон архітектури програмного забезпечення, який призначений для створення подій, їх виявлення, споживання і реагування на них.

Подія може бути визначена як значна зміна стану. Наприклад, коли споживач купує автомобіль, стан автомобіля змінюється з "на продаж" до "продано". Архітектура системи дилера автомобілів може трактувати цю зміну

стану як подію, поява якої може стати відомою іншим програмам даної архітектури.

З формальної точки зору, те, що виробляється, публікується, поширюється, виявляється і споживається (як правило, асинхронно) є повідомленням, яке називають сповіщенням про подію (або нотифікацією), а не самою подією, яка є зміною стану, що викликає появу повідомлення.

Події не подорожують, вони просто відбуваються. Проте термін подія часто використовується метонімічно для позначення самого нотифікаційного повідомлення, що може призвести до певної плутанини.

Цей архітектурний шаблон може застосовуватися при проектуванні і реалізації ПЗ і систем, які передають події між слабкозв'язаними компонентами програмного забезпечення і сервісами (службами).

Подійно-орієнтована система як правило складається з емітерів подій (або агентів) і споживачів подій (або стоків).

Стоки несуть відповідальність за здійснення реагування на появу події. Реакція не завжди може бути повністю забезпечена самим стоком. Наприклад, стік, може бути відповідальним лише за фільтрацію, трансформацію і відправку події до іншого компонента або він може забезпечити повністю самостійну реакцію на таку подію.

Перша категорія стоків може бути заснована на традиційних компонентах, таких як проміжне програмне забезпечення, орієнтоване на обробку повідомлень (message oriented middleware, MOM), в той час, як друга категорія стоків (самостійна реакція в режимі он-лайн) може вимагати більш придатної платформи (фреймворку) для виконання транзакцій.

Розробка ПЗ і систем в подійно-орієнтованій архітектурі дозволяє їм бути сконструйованими способом, який більш відповідає вимогам до їх створення, оскільки такі системи в більшій мірі пристосовуються до непередбачуваних і асинхронних середовищ.

Подійно-орієнтована архітектура (EDA) може доповнювати сервісно-орієнтовану архітектуру (SOA), оскільки сервіси (служби) можуть бути активовані тригерами, які ініціюються при настанні подій.

Ця парадигма особливо корисна, коли стік не забезпечує власного виконання будь-яких дій.

Подійно-орієнтована SOA (SOA-2) розвиває архітектури SOA і EDA для забезпечення більш глибокого і надійного рівня сервісів за рахунок використання раніше невідомих причинно-наслідкових зв'язків, щоб сформувати новий шаблон подій. Цей новий шаблон бізнес-аналітики дає поштовх до небаченого раніше зростання рівня автоматизації підприємства за рахунок привнесення додаткової цінної інформації в описану раніше модель діяльності.

Обчислювальна техніка та сенсорні пристрої (сенсори, датчики, контролери) можуть виявляти зміни стану об'єктів або умов і створювати події, які потім можуть бути оброблені сервісом (службою) або системою.

Подія може складатися з двох частин: заголовка події та тіла події. Заголовок події може включати в себе інформацію таку як, наприклад, назва події, часова мітка події і тип події. Тіло події – це частина, яка описує факт, що стався в дійсності. Тіло події не слід плутати з шаблоном або логікою, яка може бути застосована як реакція на саму події.

Архітектура, керована подіями, складається з чотирьох логічних рівнів (шарів). Вона починається з виявлення факту, його технічного подання у формі події і закінчується непустою множиною реакцій на цю подію.

Генератор подій.

Першим логічним шаром є генератор подій, який виявляє факт і представляє цей факт подією. Оскільки фактом може бути практично все, що може бути сприйнято, то ним може бути і генератор подій. Наприклад, генератором може бути клієнт електронної пошти, система електронної комерції або певний тип датчика.

Перетворення різних даних, отриманих від датчиків, в єдину стандартизовану форму даних, які можуть бути оцінені, є основною проблемою при розробці та реалізації цього шару. Однак, враховуючи, що подія є строго декларативною, можна легко застосовувати будь-які операції трансформації, тим самим усуваючи необхідність забезпечення високого рівня стандартизації.

Канал подій.

Канал подій - це механізм, через який інформація від генератора подій передається до обробника подій (event engine) або стоку.

Це може бути з'єднання TCP/IP або вхідний файл будь-якого типу (простий текст, формат XML, e-mail тощо). В один і той же час може бути відкрито кілька каналів подій.

Як правило, оскільки обробник подій повинен працювати в режимі, наближеному до реального часу, канали подій зчитуються асинхронно. Події зберігаються в черзі, очікуючи наступної обробки механізмом обробки подій.

Механізм обробки подій.

Механізм обробки подій (event processing engine) є місцем, де подія ідентифікується і вибирається відповідна реакція на нього, яка потім виконується. Це також може призвести до породження ряду тверджень. Якщо подія, яка надійшла до механізму обробки подій, є наприклад такою «Запаси продукту ID досягли нижнього допустимого рівня», це може ініціювати, наприклад, такі реакції як «Замовити продукт ID» і «Сповістити персонал».

Наступна подійно-орієнтована дія (післядія).

Щодо того, як можуть проявлятися наслідки події, слід відмітити, що вони можуть проявитись багатьма різними способами і у різноманітних формах (наприклад, повідомлення електронної пошти, надіслане комусь, або ПЗ, що виводить деяке попередження на екран).

Залежно від рівня автоматизації, який забезпечується стоком (механізмом обробки подій), ці дії можуть виявитись зайвими.

Є три основні стилі обробки подій: простий, потоковий і складний. Часто ці три стилі використовуються спільно у розвинутій подійно-орієнтованій архітектурі.

Проста обробка подій.

Проста обробка подій стосується подій, які безпосередньо належать до специфічних вимірних змін умов. У випадку простої обробки подій, мають справу з появою відомих подій, що ініціюють післядію (післядії). Проста обробка подій зазвичай використовується для управління потоком робіт в реальному часі, скорочуючи тим самим час затримки і вартість робіт.

Наприклад, прості події можуть створюватись (породжуватись) датчиком, що виявляє зміну тиску в шині або температуру навколишнього середовища.

Обробка потоку подій.

При обробці потоку подій (event stream processing, далі ESP) відбуваються як звичайні, так і відомі події. Звичайні події (заявки, передачі RFID) перевіряються на те, чи є вони відомими, і передаються інформаційним передплатникам. Обробка потоку подій зазвичай використовується для управління потоком інформації в реальному часі і на рівні підприємства, що дозволяє своєчасно приймати рішення.

Обробка складних подій.

Обробка складних подій (Complex event processing (CEP)) дозволяє за шаблонами простих і звичайних подій проводити аналіз того, чи наступила складна подія. Обробка складних подій полягає в оцінюванні взаємного впливу подій і в наступному виконанні дій. При цьому, типи подій (відомих або звичайних) можуть перетинатись, а події можуть виникати протягом тривалого періоду часу.

– Кореляція подій може бути причинною, тимчасовою або просторовою. CEP вимагає використання складних інтерпретаторів подій, визначення і підбору шаблонів подій, а також відповідних кореляційних методів. Обробка складних подій зазвичай використовується для виявлення і реагування на аномальну поведінку, загрози і можливості у бізнесі.

4.2 Захист розробленого програмного забезпечення

Розроблене програмне забезпечення захистимо за допомогою національного стандарту захисту інформації на основі алгоритму шифрування/дешифрування ДСТУ 4145-2002 з використанням еліптичних кривих над двійковим розширеним полем Галуа. У системі шифрування/дешифрування як параметри розглядається еліптична крива E_p (a,b) і точка G на ній. Учасник В вибирає закритий ключ n і обчислює відкритий ключ $P_B = n \times G$. Щоб зашифрувати повідомлення P_m використовується відкритий ключ одержувача В P_B. Учасник А вибирає випадкове ціле позитивне число k і обчислює зашифроване повідомлення C_m, що є точкою на еліптичній кривій.

$$C_m = \{k \times G,\ P_m + k \times P_B\}. \quad (4.1)$$

Щоб дешифрувати повідомлення, учасник В множить першу координату точки на свій закритий ключ і віднімає результат від другої координати:

$$P_m + k \times P_B - n_B \times (k \times G) = P_m + k \times (n_B \times G) - n_B \times (k \times G) = P_m. \quad (4.2)$$

Учасник А зашифрував повідомлення P_m додаванням до нього $k \times P_B$. Ніхто не знає значення k, тому, хоча P_B і є відкритим ключем, ніхто не знає $k \times P_B$. Супротивнику для відновлення повідомлення доведеться обчислити k. Зробити це буде нелегко. Одержувач також не знає k, але йому як підказку посилається $k \times G$. Помноживши $k \times G$ на свій закритий ключ, одержувач одержить значення, що було додано відправником до незашифрованого повідомлення. Тим самим одержувач, не знаючи k, але маючи свій закритий ключ, може відновити незашифроване повідомлення.

Нехай задано просте число $p > 4$. Тоді еліптичною кривою E, визначеною над розширеним двійковим полем полем F_{2^m}, називається безліч пар чисел (x, y), $x, y \in F$, що задовольняють тотожності:

$$y^2 \equiv x^3 + a \cdot x + b (\mathrm{mod}\, 2^m), \quad (4.3)$$

де $4 \cdot a^3 + 27 \cdot b^2$ не рівно з нулю по модулю 2^m.

Інваріантом еліптичної кривої називається величина $J(E)$, що задовольняє

тотожності:

$$J(E) \equiv 1728 \frac{4a^3}{4a^3 + 27b^2} (\mathrm{mod}\, 2^m). \quad (4.4)$$

Коефіцієнти a, b еліптичної кривої E, по відомому інваріанту $J(E)$, визначаються таким чином:

$$\begin{cases} a \equiv 3k (\mathrm{mod}\, 2^m) \\ b \equiv 2k (\mathrm{mod}\, 2^m) \end{cases} \text{де } k \equiv \frac{J(E)}{1728 - J(E)} (\mathrm{mod}\, 2^m), J(E) \neq 0 \text{ або } 1728. \quad (4.5)$$

Пари (x,y), що задовольняють тотожності (4.1), називаються точками еліптичної кривої E, x та y – відповідно x– та y-координатами точки.

Точки еліптичної кривої позначатимемо $Q(x,y)$ або просто Q. Дві точки еліптичної кривої рівні, якщо рівні їх відповідні x– і y-координати.

На безлічі всіх точок еліптичною кривою Е введемо операцію додавання, яку позначатимемо знаком "+". Для двох довільних точок $Q_1(x_1, y_1)$ та $Q_2(x_2, y_2)$ еліптичної кривої Е, розглянемо декілька варіантів.

Нехай координати точок Q_1 та Q_2 задовольняють умові $x_1 \neq x_2$. В цьому випадку їх сумою називатимемо точку $Q_3(x_3, y_3)$ координати якої визначаються порівняннями:

$$\begin{cases} x_3 \equiv \lambda^2 - x_1 - x_2 (\mathrm{mod}\, 2^m), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\, 2^m), \end{cases} \text{де } \lambda \equiv \frac{y_2 - y_1}{x_2 - x_1} (\mathrm{mod}\, 2^m). \quad (4.6)$$

Якщо виконана рівність $x_1 = x_2$ та $y_1 = y_2 \neq 0$, то визначимо координати точки Q_3 таким чином:

$$\begin{cases} x_3 \equiv \lambda^2 - 2x_1 (\mathrm{mod}\, 2^m), \\ y_3 \equiv \lambda(x_1 - x_3) - y_1 (\mathrm{mod}\, 2^m), \end{cases} \text{де } \lambda \equiv \frac{3x_1^2 + a}{2y_1} (\mathrm{mod}\, 2^m). \quad (4.7)$$

У разі, коли виконана умова $x_1 = x_2$ та $y_1 = -y_2 (\mathrm{mod}\, p)$, суму точок Q_1та Q_2 називатимемо нульовою точкою О, не визначаючи її х– і у-координати. В цьому випадку, точка Q_2 називається запереченням точки Q_1. Для нульової точки О виконана рівність:

$$Q + 0 = 0 + Q = Q, \quad (4.8)$$

де Q – довільна точка еліптичної кривої E.

Щодо введеної операції складання безліч всіх точок еліптичною кривою E, разом з нульовою точкою, утворюють кінцеву абельову (комутативну) групу порядку т, для якого виконана нерівність:

$$p+1-2\sqrt{p} \le m \le p+1+2\sqrt{p} \tag{4.9}$$

Точка Q називається точкою кратності k, або просто – кратною точкою еліптичної кривої E, якщо для деякої точки P виконана рівність:

$$Q = P + ... + P = kP \tag{4.10}$$

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку зображено розроблене у бакалаврської дипломної роботі ПЗ системи мережевого комплексного засобу відеонагляду для підприємства. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи:

– Навігаційного меню яке викликається натисканням правої клавіші маніпулятора миші.

– Верхнього меню: Файл; Вид; камера; Налаштування; Вікно; Довідка.

– Розділу обрання групи.

– Розділу виведення результату роботи системи.

– Функції представлені у графічному вигляді.

Рисунок 5.1 – Головне вікно ПЗ

Створення й розгортання охоронної сигналізації на периметрі – одна зі найбільш складних з технічної точки зору завдань. Складні умови роботи не дозволяють повністю усунути помилкові спрацьовування. Різного роду погрози вимагають різних методів виявлення й установки відповідних датчиків. Кожний тип огородження вимагає різної тактики охорони й використовуваного устаткування. Непрості погодні умови: широкий діапазон температур, сонце, вітер, дощ, сніг, дикі й свійські тварина й птахи – все це може стати причиною помилкового спрацьовування.

Кожний фактор вимагає ретельного аналізу й найбільш оптимальних для кожного випадку технічних рішень, що відповідають датчиків, а також їхнього ретельного налаштування. Нерідко налаштування займає значний період досвідченої експлуатації.

На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення.

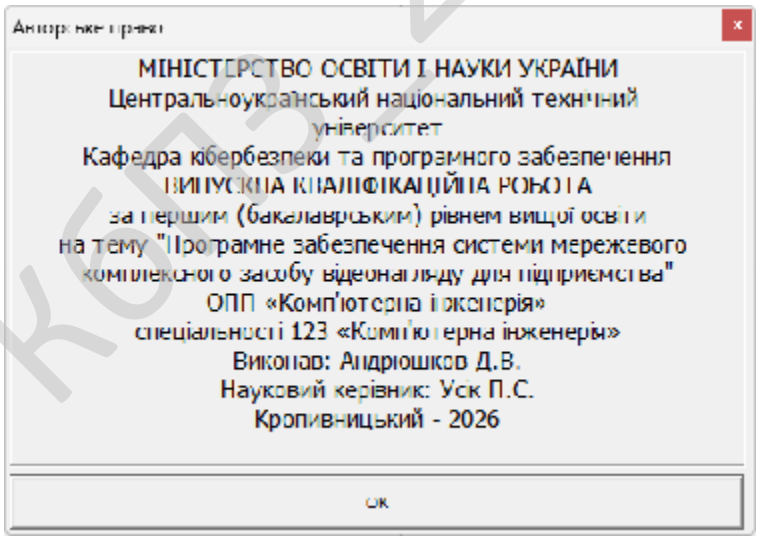

Рисунок 5.2 – Авторське право

Вибір способів виявлення проникнення й тактики захисту периметра об'єкта повинен здійснюватися професіоналами з більшим досвідом. Вибір тут украй великий.

Розроблена програма має дуже простий і зрозумілий інтерфейс з користувачем. Кожен, хто в достатньому обсязі володіє операційним середовищем Windows без особливих складностей освоїть і цю програму, оскільки її інтерфейс інтуїтивно зрозумілий. Якщо програма не видала ніяких помилок, і працює, то можна використовувати, інакше слід слідувати інструкціям, які пропонує програма.

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

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

До діяльностей пов'язаних із розгортанням програмного забезпечення відносять:

– Випуск.

– Встановлення та активація.

– Деактивація.

– Адаптація.

– Обновлення.

– Вмонтування.

– Відстежування версій.

– Видалення.

– Вилучення з обігу.

При впровадженні програмного забезпечення потрібно урахувати наступні дії:

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

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

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

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

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

Проводилась оцінка:

– відповідності поставленим вимогам;

– правильна відповідь для усіх можливих вхідних даних;

– виконання функцій за прийнятний час;

– практичність;

– сумісність з ОС та стороннім ПЗ.

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

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

Проводилось тестування чорної скриньки.

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

Ці тести демонструють:

– Як виконуються функції програми.

– Як приймаються вихідні дані.

– Як виробляються результати.

– Як зберігається цілісність зовнішньої інформації.

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

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

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

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

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

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

Будь-який спосіб тестування «чорної скриньки» повинен:

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

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

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

Тестування «чорної скриньки» забезпечує пошук наступних категорій помилок:

– Некоректних чи відсутніх функцій.

– Помилок інтерфейсу.

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

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

– Помилок ініціалізації та завершення.

Обрано умови розповсюдження – Freeware.

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

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

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

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

6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи мережевого комплексного засобу відеонагляду для підприємства.

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

Рішення завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем мережевого комплексного засобу відеонагляду для підприємства.

– Досліджена система мережевого комплексного засобу відеонагляду для підприємства.

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевого комплексного засобу відеонагляду для підприємства.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання мережевого комплексного засобу відеонагляду для підприємства.

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 призначені для системи мережевого комплексного засобу відеонагляду для підприємства. Це

дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

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

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

Для підвищення рівня безпеки запропоновано застосовувати алгоритм ДСТУ 4145-2002.

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

2. 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.

3. 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

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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,

11. 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.

12. 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

13. 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.

14. 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.

15. 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.

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

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

41. 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).

42. 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

43. 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.

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

45. 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.

46. 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.

47. 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

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

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

50. 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.

51. 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.

52. 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.

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