

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

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за першим (бакалаврським) рівнем вищої освіти
на тему

“Програмне забезпечення системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II”

Виконав здобувач вищої освіти
IV курсу, групи КБ-22-2
ОПП «Кібербезпека»
спеціальності 125 «Кібербезпека»
_____ Шамшур С.О.
«___» _____ 2026 р.

Керівник проекту
доктор технічних наук, професор
_____ Смірнов О.А.
«___» _____ 2026 р.
Рецензент _____

Центральноукраїнський національний технічний університет
Факультет Механіко-технологічний
Кафедра Кібербезпеки та програмного забезпечення
Освітній ступінь бакалавр
Галузь знань ._12 _____“Інформаційні технології”
Спеціальність 125 “Кібербезпека”
Освітньо-професійна (освітньо-наукова) програма “Кібербезпека”

ЗАТВЕРДЖУЮ

Завідувач кафедри

д.т.н., проф.

_____ Олексій СМІРНОВ

« 27 » лютого 2026 року

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

Шамишуру Станіславу Олександровичу

(прізвище, ім'я, по батькові)

1. Тема роботи *Програмне забезпечення системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II*

2. Керівник роботи *Смірнов Олексій Анатолійович, доктор технічних наук, професор*

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

затверджені наказом вищого навчального закладу № 129-02 від 27.02.2026 року

3. Строк подання студентом роботи до захисту 23.05.2026 р.

4. Мета та завдання випускної кваліфікаційної роботи: *Метою роботи є розробка програмного забезпечення системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II*

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

1. Призначення та область використання.

2.Перегляд аналогічних існуючих систем.

3. Опис і обґрунтування проектних рішень.

4. Етапи програмування системи.

5. Впровадження системи кібербезпеки в промислову експлуатацію.

6. Висновки

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

Структурна схема системи кібербезпеки 1 аркуш

Функціональна схема системи кібербезпеки 1 аркуш

Діаграма процесів 1 аркуш

Блок-схема алгоритму роботи додатку 2 аркуша

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

КАЛЕНДАРНИЙ ПЛАН

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

Дата видачі завдання
« 27 » лютого 2026 р.

Підпис керівника

Смірнов О.А.
(прізвище та ініціали)

Завдання прийнято до виконання
« 27 » лютого 2026 р.

Підпис здобувача

Шамшур С.О.
(прізвище та ініціали)

АНОТАЦІЯ

Шамшур С.О. Програмне забезпечення системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II. 125 Кібербезпека. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

Метою розробки є програмне забезпечення системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

Результат роботи – програмна реалізація системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

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

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

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

Програму розроблено в середовищі Python.

Ключові слова: кібербезпека, відеонагляд

ABSTRACT

Shamshur S.O. Cybersecurity system software for secure video surveillance implemented on the basis of Axis P1364-E and Axis P1365-E Mk II. 125 Cybersecurity. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

In this final qualification work for the first (bachelor's) level of higher education, software has been developed, which is intended for a cybersecurity system for secure video surveillance implemented on the basis of Axis P1364-E and Axis P1365-E Mk II.

The purpose of the development is to develop a cybersecurity system software for secure video surveillance implemented on the basis of Axis P1364-E and Axis P1365-E Mk II.

The result of the work is a software implementation of a cybersecurity system for secure video surveillance based on Axis P1364-E and Axis P1365-E Mk II.

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

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

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

The program was developed in the Python environment.

Keywords: cybersecurity, video surveillance

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ	2
ВСТУП.....	3
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ	5
1.1 Призначення системи.....	5
1.2 Область застосування.....	6
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ	8
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти.....	8
2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування.....	21
2.3 Розгорнута постановка завдання	25
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	27
3.1 Опис функціонування системи	27
3.2 Розробка структурної схеми.....	31
3.3 Розробка функціональної схеми	36
3.4 Розробка діаграми процесів.....	39
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ.....	40
4.1 Розробка блок-схем та опис алгоритмів функціонування системи.....	40
4.2 Захист розробленого програмного забезпечення.....	58
5 ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	62
6 ОСНОВНІ ВИСНОВКИ.....	67
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	69

					ВКРБ-125.26.0046.00.00.ПЗ			
Вим.	Арк.	№ докум.	Підп.	Дата	<i>Програмне забезпечення системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II</i>	Літ.	Аркуш	Аркушів
<i>Розроб.</i>	Шамиур С.О.					Б	1	76
<i>Перев.</i>	Смірнов О.А.							
<i>Н.контр.</i>	Коваленко А.С.					ЦНТУ КБ-22-2		
<i>Затв.</i>	Смірнов О.А.							

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

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

ВСТУП

Актуальність теми. Відео набуває нової, підвищеної ролі в бізнес-операціях, оскільки все більше галузей визнають його джерелом даних та аналітики. Axis Perspectives дозволяє нам відстежувати цю еволюцію та досліджувати, як організації стратегічно ставляться до відеотехнологій. Ці технології мають потенціал для підвищення цінності, що виходить за рамки фізичної безпеки та моніторингу, і оскільки вони продовжують поширюватися в бізнес-ландшафті, вони не лише демонструють свою ефективність, але й те, як інтелектуальні відеосистеми стають конкурентною перевагою:

- Безпека залишаються найсильнішими рушійними силами: безпека все ще є основною метою відеосистем для 89% кінцевих клієнтів, тоді як 81% надають пріоритет безпеці.

- Відео тепер підвищує цінність бізнесу: використання відео для бізнес-аналітики зросло майже вдвічі за один рік, зростаючи з 20% до 38%, тоді як 42% тепер використовують відео для підтримки операційної ефективності.

- Кібербезпека зараз є головним пріоритетом: 44% кінцевих клієнтів кажуть, що кібербезпека та захист даних будуть ключовим пріоритетом протягом наступних одного-трьох років, що підкреслює необхідність розглядати підключені камери як частину ширшого планування кіберризиків.

- Клієнти хочуть простіших, об'єднаних систем: 41% кажуть, що об'єднання різних систем безпеки на одній платформі є головним пріоритетом, оскільки організації прагнуть зменшити складність та покращити прозорість на різних об'єктах.

- Впровадження хмарних технологій прискорюється: очікується, що використання хмарних технологій у сфері фізичної безпеки зросте з 27% до 44% протягом двох років.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

– Модернізація інфраструктури залишається ключовим фактором: 64% кінцевих користувачів кажуть, що модернізація інфраструктури є основною причиною інвестування у відео, оскільки організації шукають системи, якими легше керувати та які безпечніше.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

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

– Огляд існуючих систем для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

– Дослідження системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

– Програмна реалізація системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		4

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

У силу географічного положення України на багатьох об'єктах інфраструктури тяжкі умови експлуатації. Це накладає високі вимоги до якості пристроїв, їх відказостійкості пристроїв і захищеності від перепадів температури, вологи, пилу. Axis приділяє велику увагу якості камер і проводить по усьому світі випробування свого встаткування в реальних умовах відеоспостереження. У режимі реального часу виробляється збір даних про навколишнє середовище й стан камер для наступного аналізу. Отримані дані дозволяють поліпшити експлуатаційні характеристики камер.

Визначаються вимоги в тому числі й до інтелектуального відеоспостереження в частині ідентифікації фізичних осіб і виявлення тривожних ситуацій. (однак наявність таких систем не є обов'язковим – у всякому разі вимоги до необхідності їхньої установки встановлюються). Камери Axis оснащуються власним чипом Axis ARTPEC (цього року з'явилася вже шоста версія цього процесора). Він використовується для завантаження додаткових застосунків, за допомогою яких камера перетворюється в пристрій по аналітичній обробки. Так, убудована аналітика Axis Perimeter Defender убудована в камери відеоспостереження Axis дозволяє ідентифікувати факт проникнення в охоронювану зону.

Камери використовуються як для розслідування інцидентів постфактум, так і для моніторингу поточної обстановки, у тому числі виявлення залишених без догляду речей. Висока світлочутливість камер і підтримка розв'язної здатності HDTV 1080p із частотою до 60 кадрів у секунду дозволяє реалізувати відеоаналітику в умовах щільного пасажирського потоку.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

1.2 Область застосування

Застосування сучасних систем відеоспостереження не обмежується режимними об'єктами. Системи безпеки даного виду тепер широко застосовуються в самих різних сферах.

Як правило, такі системи підрозділяються на різні групи виходячи з області їхнього подальшого використання:

- Системи можуть бути як зовнішнього використання, так і внутрішнього. Природно, зовнішні камери, розташовані поза приміщеннями, повинні бути несприйнятливими до вологості, низьким і високим температурам, а також іншим агресивним факторам. Важливим в таких випадках є антивандальний захист.

- Для внутрішніх систем не висувається настільки твердих вимог. Як правило, вони використовуються в офісах, торгових центрах і місцях суспільного користування.

- У квартирах, будинках і дачах поряд із уже звичними відеодомофонами часто встановлюють зовнішні системи для відеоспостереження.

- Сховані системи призначені для неявного візуального контролю над об'єктом.

Основні завдання системи відеоспостереження

У сучасних умовах складно уявити собі систему безпеки якого-небудь об'єкта без використання відеоспостереження. Установка комплексної системи відеоспостереження на охоронюваному об'єкті дозволяє ефективно виконувати цілий ряд важливих функцій.

- Територія об'єкта й прилягаюча до неї область перебуває під постійним візуальним контролем.

- З'являється можливість оперативного контролю за всіма переміщеннями (санкціонованими й несанкціонованими) по території об'єкта, а також за робочим процесом на підприємствах.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

– Система відеоспостереження дозволяє фіксувати спроби несанкціонованого проникнення на об'єкт, а в комплексі з іншими системами й припиняти такі спроби.

– Такі системи дають можливість здійснювати не тільки оперативний візуальний контроль, але й проводити фіксацію подій для архіву.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

К6ПЗ_2026

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		7

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

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

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 крапкою для розвитку систем відеоспостереження, поява камери вимагало появи програмного забезпечення для роботи з її.

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

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

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		8

Однак зараз проглядається тенденція до того, що закриті системи починають дивитися убік підтримки встаткування 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 систем відеонагляду (СВН), 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 СВН, 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 співробітничав з компанією Axis Communication, лідером в області виробництва пристроїв відеоспостереження.

Протягом 10 років компанія Milestone є лідером на ринку СВН 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 по кількості камер на сервер або систему в цілому.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

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 розв'язної здатності камер, що підключаються користувачам, періоду зберігання й не тільки.

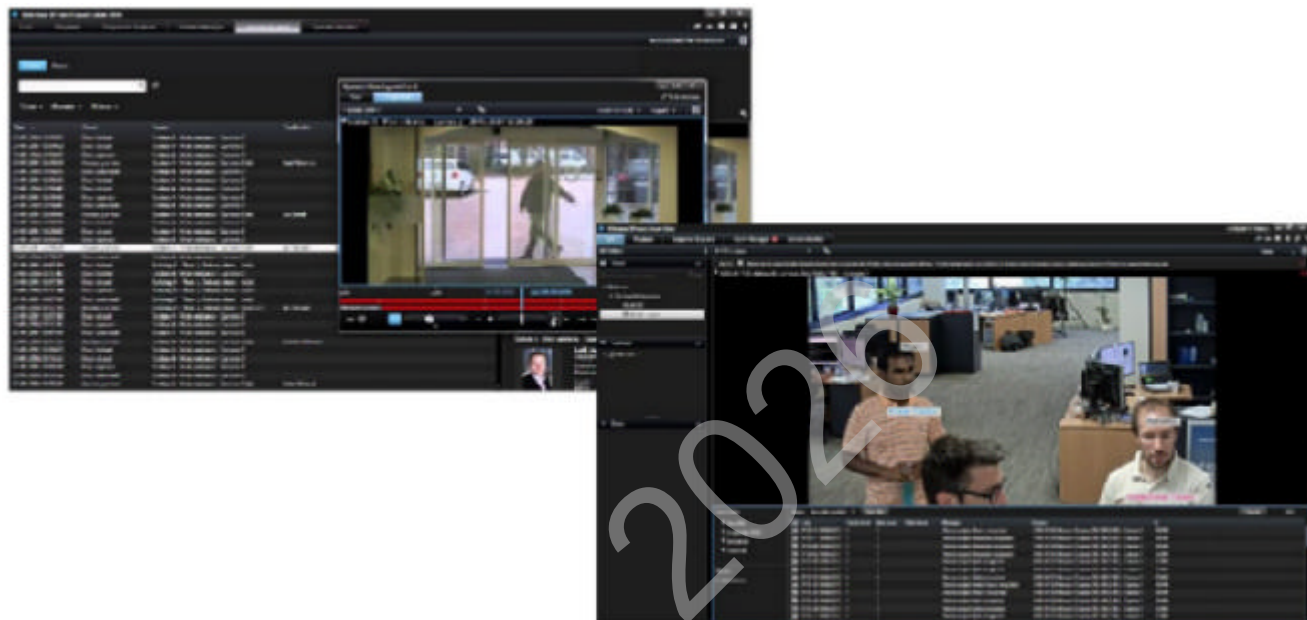


Рисунок 2.1 – Інтерфейс користувача Milestone XProtect

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

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		10

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'ятьма клієнтськими підключеннями). Підтримує три типи користувачів: пропрієтарний, Windows і Active Directory. Для зручності й гнучкості роботи зі СВН, 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.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

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

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 безпеки. Основними продуктами є Security Center і Omnicast. Останній продукт є безпосередньо системою відеоспостереження, а перший – верхньою крапкою, агрегатором додаткових компонентів системи, і деякі можливості системи Omnicast розкриваються при використанні Security Center.

І так, Omnicast представлений трьома версіями, що мають різні обмеження по кількості 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 по кількості 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 Omnicast 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 відсутня.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		12

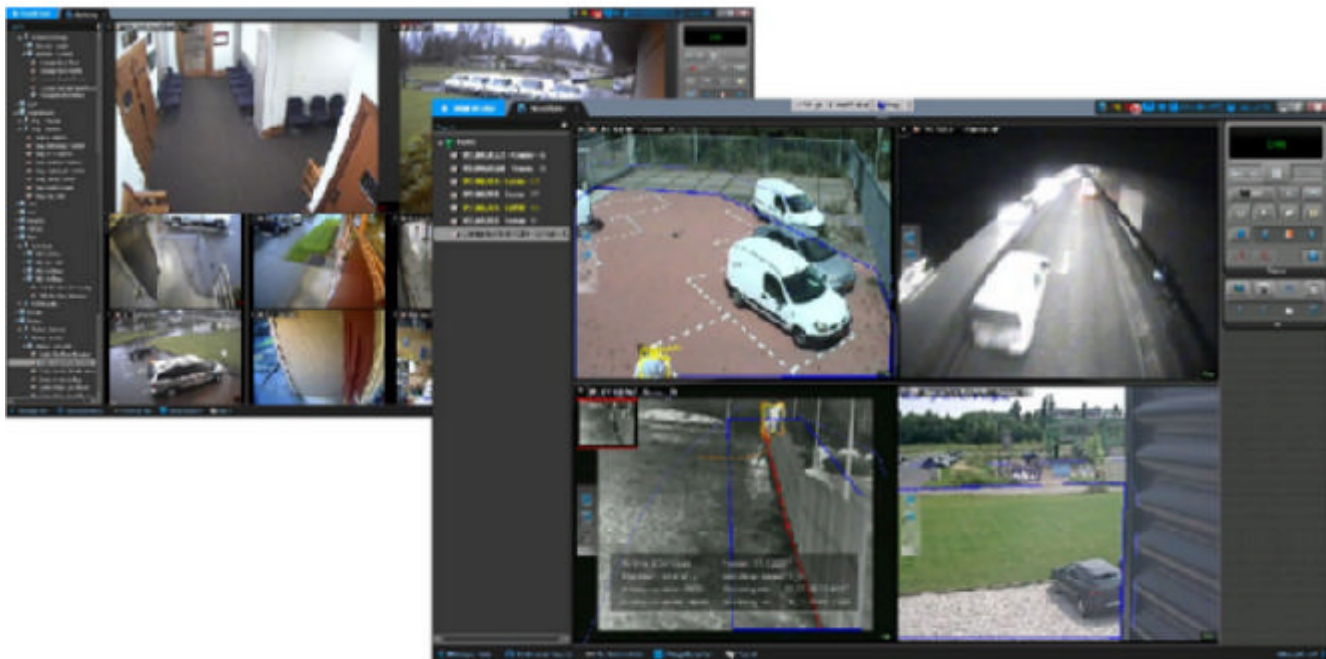


Рисунок 2.2 – Інтерфейс користувача Genetec Onmicast

Для розширення функціонала Genetec надає SDK.

Ліцензується Genetec по кількості 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 Onmicast, 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 крапки 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.

Luxriot. Evo

(www.luxriot.com)

Luxriot – американська компанія по розробці програмного забезпечення для систем відеоспостереження, крім софта 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, максимальна розв'язна здатність камер до 2Мр, одне користувальницьке підключення на систему. Безкоштовна ліцензія може бути розширена до 16 каналів за потребою.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14



Рисунок 2.3 – Інтерфейс користувача Luxgriot

Лінійка СВН Luxgriot підтримує порядку 6000 IP пристроїв і підтримує невелику кількість інтеграцій сторонніх рішень по відео аналітиці й таким рішенням, як система контролю доступу. Що стосується бортової аналітики камер, Luxgriot підтримує обмежений список виробників. Ліцензування в Luxgriot поканальне й поширюється у вигляді бандлів на молодші версії й поканально в старшій версії. Тому що більшість IP камер на ринку зараз багатоканальні (профільні), поканальне ліцензування в деяких випадках накладає незручності й вимагає додаткового ліцензування при використанні багатоканальних пристроїв. Ліцензія в Luxgriot прив'язується до апаратної частини сервера, тому при зміні конфігурації можливо буде потрібно повторна активація.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

Незважаючи на невеликий вибір рішень по інтеграції рішень сторонніх виробників, функціонал СВН 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 транслявати 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.

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 СВН 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, СВН має самий компактний інсталятор і позиціонується розроблювачами як дуже легковагий і невимогливий до апаратних ресурсів продукт, при цьому не на шкоду функціоналу.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		16



Рисунок 2.4 – Інтерфейс користувача Network Optix

Дана СВН 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

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

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 СВН 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 розгорнутий у віртуальному середовищі, а також в Docker.

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

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		18

розробляє програмне забезпечення, функції відеоаналітики й мережних реєстраторів.



Рисунок 2.5 – Інтерфейс користувача Macroscop

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 реактивація. Після

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		19

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 по кількості каналів, старша версія включає частину модулів на безкоштовній основі. Забавний факт, що деварпінг – розгорнення Fisheye-камери, ставиться 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 СВН 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.

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.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		20

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.

2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування

Python – це об'єктно-орієнтована мова програмування високого рівня загального призначення з відкритим кодом. Це визначення може бути важким для новачків, тому розглянемо кожну характеристику окремо, щоб зрозуміти, що вона означає:

- Відкритий вихідний код: це безкоштовно та доступно для подальших покращень, таких як додавання корисних функцій або виправлення помилок.
- Об'єктно-орієнтована: заснована не на функціях, але в об'єктах з певними атрибутами й методами.
- Високий рівень: зручний для людини, а не для комп'ютера.
- Загальне призначення: можна використовувати для створення будь-яких програм.

Ця мова використовується в будь-якому програмному забезпеченні, про яке ви тільки можете подумати. Ви можете використовувати його для створення веб-сайтів, штучного інтелекту, серверів, програмного забезпечення для бізнесу та багато іншого. Також застосовується в науці про дані, аналізі даних, машинному навчанні, інженерії даних, веб-розробці, розробці програмного забезпечення та інших галузях.

Переваги та недоліки Python

Переваги:

- Її легко читати, вчити та писати. Це мова програмування високого рівня з англійським синтаксисом. Це полегшує читання та розуміння коду. Її дійсно

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		21

легко зрозуміти і вивчити, тому багато людей рекомендують Python новачкам. Вам потрібно менше рядків коду для виконання того ж завдання в порівнянні з іншими основними мовами, такими як C/C++ та Java.

– Підвищує продуктивність. Це дуже продуктивна мова. Завдяки її простоті розробники можуть зосередитися на розв'язанні проблеми. Їм не потрібно витрачати багато часу на розуміння синтаксису або поведінку мови програмування. Ви пишете менше коду та виконуєте більше завдань.

– Інтерпретована мова. Python мова, що інтерпретується, а це означає, що вона безпосередньо виконує код по рядку. Якщо сталася помилка, вона зупиняє подальше виконання та повідомляє про її виникнення. Вона показує лише одну помилку, навіть якщо у програмі їх кілька. Це спрощує налагодження.

– Динамічно типізована. Python не визначає тип змінної, доки ми не запустимо код. Вона автоматично надає тип даних, коли відбувається процес виконання. Не треба турбуватися про оголошення змінних та типи даних.

– Безкоштовна та з відкритим вихідним кодом. Ця мова постачається під схваленою OSI ліцензією з відкритим вихідним кодом. Це робить його безкоштовним для використання та розповсюдження. Ви можете завантажити вихідний код, змінити його та навіть розповсюджувати свою версію. Це корисно для організацій, які хочуть використати свою версію для розробки.

– Підтримка великих бібліотек. Стандартна бібліотека Python є величезною, ви можете знайти майже всі функції, необхідні для вашого завдання. Таким чином ви не залежите від зовнішніх бібліотек.

– Портативність. У багатьох мовах, таких як C/C++, потрібно змінити свій код, щоб запустити програму на різних платформах. З Python все інакше. Ви тільки пишете один раз і запускаєте її будь-де.

Недоліки:

– Низька швидкість. Вище ми обговорювали, що це інтерпретована мова з динамічною типізацією. Порядкове виконання коду часто призводить до повільного виконання. Динамічна природа Python також є причиною її низької

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		22

швидкості, оскільки їй доводиться виконувати додаткову роботу при виконанні коду. Тому вона не підходить для цілей, де швидкість важливий аспект проєкту.

– Неєфективна для пам'яті. Ця мова програмування використовує великий обсяг пам'яті, це може бути недоліком при створенні програм, коли віддають перевагу оптимізації пам'яті.

– Слабка у мобільних обчисленнях. Python зазвичай використовується у серверному програмуванні. Ми не бачимо – її на стороні клієнта або в мобільних програмах з таких причин: вона не заощаджує пам'ять і має повільну обчислювальну потужність у порівнянні з іншими мовами.

– Доступ до бази даних. Програмувати на цій мові легко, але коли ми взаємодіємо з базою даних, її не вистачає. Рівень доступу до бази даних у Python примітивний та недостатньо розвинений у порівнянні з іншими популярними технологіями.

– Помилки виконання. Це мова з динамічною типізацією, тому тип даних змінної може змінюватись у будь-який час. Змінна, що містить ціле число, у майбутньому може містити рядок, що може призвести до помилок виконання.

Застосування Python:

– Для аналізу даних. Дані стали цінним активом у будь-якій сучасній галузі, і більшість компаній зацікавлені у збиранні, обробці та аналізі релевантних даних, щоб витягти з них цінну інформацію для бізнесу. І тут Python виходить за межі будь-якої конкуренції. Python особливо цінна тим, що крім великої стандартної бібліотеки надає величезний набір додаткових модулів, розроблених спеціально для аналітичних цілей. Найвідоміші бібліотеки Python для аналізу даних – це pandas і NumPy . Ці інструменти дозволяють робити з вашими даними майже все, наприклад, очищати і аналізувати їх, вивчати статистику або візуалізувати приховані тенденції у ваших даних.

– Для візуалізації даних. Візуалізація даних – це окрема частина аналізу даних, яка допомагає нам подавати інформацію, необроблену чи очищену, у більш змістовній формі. Тут Python знову входить у гру, пропонуючи широкий

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		23

спектр інструментів візуалізації даних. Найпопулярніші з них – matplotlib і заснований на ній seaborn. Використовуючи їх, ми можемо створювати буквально всі види візуалізації: від найпростіших до складніших.

– Для машинного навчання. Машинне навчання (ML) є основою більшості завдань науки даних. Він є областю штучного інтелекту, пов'язаною з використанням алгоритмів, що дозволяють машинам вивчати закономірності та тенденції на основі історичних даних, щоб робити прогнози на основі невідомих даних. – Використовуючи методи ML, ми можемо створювати моделі, які можуть точно передбачити швидкість відтоку клієнтів компанії, оцінити ризик виникнення у людини певного захворювання, визначити оптимальне розташування автомобілів таксі й т.д. За допомогою Python ми можемо побудувати модель ML, використовуючи лише три рядки коду.

– Для розробки програмного забезпечення. Крім свого багатостороннього застосування в галузях науки про дані, Python використовується на кожному етапі розробки програмного забезпечення, включаючи контроль складання, автоматичну безперервну компіляцію, прототипування, відстеження помилок, тестування та обслуговування програмного забезпечення. За допомогою цієї мови можемо створювати аудіо- або відеопрограми на основі методів штучного інтелекту, машинного навчання, API (інтерфейсів прикладного програмування), GUI (графічних інтерфейсів) або будь-якого іншого типу програмного забезпечення.

– Для веброзробки. У той час як для створення візуальної частини вебсайту ми переважно будемо використовувати такі мови, як HTML, CSS та JavaScript, для його невидимої частини ми часто вибираємо Python. Серед масштабних вебсайтів та програм, створених за допомогою цієї мови, варто згадати Google, Facebook, Instagram, YouTube, Dropbox та Reddit.

– Для автоматизації задач/скриптингу. Це відмінний інструмент для написання програм для автоматизації різних завдань, що повторюються. Цей процес називається скриптингом. Зокрема, можна робити скрипти для роботи з

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

файлами та папками. Наприклад, можна створювати, перейменовувати, перетворювати, розділяти, об'єднувати або видаляти файли, перевіряти їх наявність помилок. Ви також можете використовувати автоматизацію Python для пошуку та завантаження інформації з Інтернету, заповнення та надсилання онлайн-форм та надсилання регулярних повідомлень або електронних листів.

Яким фахівцям потрібно володіти Python:

- Фахівець з даних.
- Аналітик даних.
- Інженер даних.
- Інженер з машинного навчання.
- Журналіст даних.
- Архітектор даних.
- Повний стек веб-розробника.
- Backend-розробник.
- DevOps-інженер.
- Інженер-програміст.

Можемо зробити висновок, що Python ще довго буде популярною мовою, хоч і має низку недоліків. Цю мову використовують для створення вебсайтів, штучного інтелекту, серверів, програмного забезпечення для бізнесу, аналізу даних, машинного навчання, інженерії даних та для багатьох інших областей. Це перспективна і затребувана навичка, яка необхідна у всіх галузях.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускню кваліфікаційну роботу за першим (бакалаврським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

В процесі розробки випускної кваліфікаційної роботи за першим

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

(бакалаврським) рівнем вищої освіти необхідно виконати наступний обсяг роботи:

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

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

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

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

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

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

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

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

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

AXIS P 1364-E

AXIS P 1364-E RU(0739-014) – вулична HDTV 720p камера IP-відеоспостереження, призначена для роботи при дуже слабкому освітленні, що підтримує фірмові технології Axis: Lightfinder, WDR – Forensic Capture, P-iris, Zipstream і оснащена системою віддаленого фокусування. Камера P 1364-E RU(0739-014) дозволяє одержати відеозображення з розв'язною здатністю HDTV 720p при частоті кадрів 50/60 кадр/с, забезпечуючи при цьому придушення шуму й зниження размиття об'єктів, що рухаються, при недостатнім освітленні. Технологія Axis Zipstream значно знижує обсяг переданого трафіку й вимоги до обсягу пам'яті для зберігання даних. Підтримка камерою широкого динамічного діапазону WDR – Forensic Capture дозволяє одержати відеозображення, що оптимально для розпізнавання об'єктів завдяки винятковому проробленню деталей – навіть у самих несприятливих умовах освітленості. Можливість віддаленого регулювання заднього фокуса підвищує ефективність установки камери й забезпечує чіткість зображення. Модель P 1364-E RU(0739-014) відповідає стандартам IP66, IP67, NEMA 4X і IK10. У комплект поставки камери входить кронштейн для кріплення на стіну й сонцезахистний козирок. Технологія Arctic Temperature Control гарантує запуск і роботу камери при температурах від -40 до 50°C.

Axis P 1365-E Mk II

Камера AXIS P 1365-E Mk II призначена для зовнішньої установки й експлуатації в екстремальних умовах – вона може працювати навіть при температурах -40°C і 50°C. Функція Arctic Temperature Control гарантує безпечний запуск камери при температурах до -40°C навіть після аварійного

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		27

відключення живлення. Ви можете бути впевнені, що кожух камери зможе витримати як суворі погодні умови, так і дії вандалів, оскільки він має захист, що відповідає стандартам IP66, IP67, NEMA 4X і IK10. Модель AXIS P 1365-E Mk II поставляється в комплекті з настінним кронштейном і сонцезахистним козирком для захисту від пилу, дощу, снігу й сонячного світла.

Компанія Axis визначила п'ять технологічних трендів, які, на її думку, формуватимуть сектор безпеки у 2026 році, вказуючи на більшу участь ІТ-команд та зростаючий акцент на інтегрованих системах. Результати відображають зміни в тому, як організації розгортають камери, аналітику та інфраструктуру у фізичному та цифровому середовищах.

Фокус на екосистемі

Перша тенденція зосереджена на переході до того, що Axis описує як підхід, що ставить екосистему на перше місце. Рішення щодо безпеки все частіше формуються навколо вибору єдиної, цілісної платформи, а не окремих пристроїв чи програм.

Оскільки системи безпеки включають більше датчиків, аналітичних інструментів та програмних рівнів, інтеграція стала центральною проблемою. Організації надають пріоритет платформам, які можуть обробляти конфігурацію, управління та масштабування, не покладаючись на складні комбінації несумісних продуктів.

Такий підхід надає більшій ваги широті апаратного та програмного забезпечення, доступного в одній екосистемі, включаючи продукти, розроблені партнерами. Змішані платформні середовища залишаються поширеними, але їх дедалі частіше розглядають як складніші в управлінні та менш адаптивні з часом.

Гібридні архітектури

Гібридне проектування систем залишається ключовою особливістю розгортання систем безпеки. Воно поєднує локальні сервери, хмарні сервіси та обробку на периферії, зазвичай за допомогою камер або датчиків. Axis припускає, що баланс між цими компонентами зміщується.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

Периферійні та хмарні ресурси беруть на себе більшу частку робочих навантажень, оскільки з'являються нові варіанти використання. Камери з вбудованою обробкою тепер можуть обробляти завдання, які раніше залежали від центральних серверів. Водночас хмарні платформи використовуються для аналізу відеоданих для отримання операційної інформації, що виходить за рамки безпеки.

Локальна інфраструктура продовжує відігравати домінуючу роль, особливо там, де управління даними або затримка є критично важливими. Гібридна модель представлена як спосіб задоволення вимог до ефективності ІТ, водночас дотримуючись очікувань щодо операційної безпеки та безпеки даних.

Периферійні обчислення

Периферійні обчислення визнаються дедалі важливішою частиною проектування систем безпеки. Досягнення в галузі штучного інтелекту та обчислювальної потужності зменшили багато попередніх обмежень, пов'язаних із запуском аналітики безпосередньо на пристроях.

Камери та датчики тепер здатні виконувати розширеніші функції локально, включаючи виявлення об'єктів та інтелектуальний пошук відео. Це зменшує необхідність передачі великих обсягів необроблених даних через мережі.

Розширення можливостей периферійних мереж також вплинуло на розробку систем кібербезпеки. Такі функції, як безпечне завантаження та підписані операційні системи, стають стандартними, що відображає прагнення до вбудовування засобів контролю безпеки безпосередньо в пристрої, а не покладатися виключно на мережевий захист.

Мобільне спостереження

Очікується, що мобільне відеоспостереження продовжить зростати протягом 2026 року. Покращення в підключенні, віддаленому управлінні та обробці даних на периферії розширили спектр середовищ, де можна розгортати тимчасові або мобільні камери.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		29

Випадки використання включають громадську безпеку, будівельні майданчики, транспортні вузли та великі заходи. У цих умовах мобільні системи можна встановити швидше, ніж постійну інфраструктуру, і їх часто легше затвердити.

Також покращилася енергоефективність. Камери тепер споживають менше енергії без зниження якості зображення, що підтримує розгортання систем живлення від батарей або відновлюваних джерел енергії. Це дозволяє вести відеоспостереження в місцях, де немає стаціонарного джерела живлення.

Ця тенденція відображає ширший зсув у бік гнучких рішень безпеки, які можна переміщувати або масштабувати залежно від зміни потреб.

Технологічна автономія

Остання тенденція зосереджена на технологічній автономії. Організації в усьому технологічному секторі прагнуть більшого контролю над критично важливими компонентами, особливо з огляду на еволюцію ланцюгів поставок та регуляторного тиску. Компанія Axis наголошує на своєму довгостроковому підході до розробки власної технології систем на кристалі як способу контролю над функціональністю продукту. Розробка власних компонентів дозволяє тіснішу інтеграцію між апаратним та програмним забезпеченням, але також вимагає постійних інвестицій та досвіду. Компанія позиціонує автономію як вибірккову, а не всеохоплюючу. Основні технології розробляються власними силами, тоді як партнерські відносини залишаються центральними для вирішення питань, що виходять за межі її основного фокусу. Цей баланс між внутрішнім розвитком та зовнішньою співпрацею представлений як спосіб реагування на швидкі технологічні зміни, зберігаючи при цьому узгодженість між лініями продуктів.

Компанія Axis зазначає, що її дослідження вказує на постійний попит на системи, що підтримують безпеку, захист, операційну ефективність та бізнес-аналітику. Вона також виділяє співпрацю з клієнтами та партнерами як ключовий фактор адаптації до змінних вимог наближення 2026 року.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		30

3.2 Розробка структурної схеми

В останні роки розвиток та впровадження технологій штучного інтелекту прискорилися безпрецедентними темпами, впливаючи на різні галузі промисловості. Звичайно, іскра інновацій, яку забезпечує штучний інтелект, вже є характерною рисою сектора відеоспостереження. Передбачається, що штучний інтелект вийде за рамки простого впровадження та стане невід'ємною основою всієї галузі – поява так званих «автономних агентів штучного інтелекту» змінить структуру та функціонування систем відеоспостереження.

Визначено п'ять ключових тенденцій, на яких має зосередитися галузь. Ці тенденції сигналізують про майбутнє, де штучний інтелект слугуватиме основним двигуном, піднімаючи відеоспостереження далі від моніторингу до забезпечення центральних стовпів операційної ефективності та сталого розвитку.

1: Надійний штучний інтелект: якість даних та відповідальне використання

Оскільки аналіз за допомогою штучного інтелекту стає повсюдним, принцип «Сміття на вході – сміття на виході» матиме вирішальне значення у відеоспостереженні. Візуальний шум та спотворення, спричинені складними умовами, такими як низька освітленість, підсвічування або туман, є основними причинами хибних тривог, спричинених штучним інтелектом. У 2026 році створення «Довіреного середовища даних» для вирішення цих проблем стане головним пріоритетом галузі.

Зі зростанням продуктивності аналітичних систем на основі штучного інтелекту, акцент інвестицій зміщується на забезпечення високоякісних відеоданих, які штучний інтелект може інтерпретувати без помилок.

Прикладом цього є мінімізація шуму та спотворень в екстремальних умовах за допомогою високопродуктивної технології ISP (обробка сигналів зображення) на основі штучного інтелекту та використання більших датчиків. ISP на основі штучного інтелекту використовує глибоке навчання для розрізнення

об'єктів та шуму, ефективно усуваючи шум та оптимізуючи деталі об'єктів для надання даних у режимі реального часу, що найбільше сприяє аналізу за допомогою штучного інтелекту. Більші датчики зображення захоплюють більше світла, що принципово пригнічує утворення шуму відео, починаючи з умов низької освітленості.

Паралельно, оскільки етичне використання штучного інтелекту стає серйозною проблемою, наближається обов'язкове впровадження систем управління ШІ. ШІ ЄС використовує класифікацію систем ШІ, що розгортаються в громадських місцях, на основі ризиків, і накладає юридичне зобов'язання на виробників забезпечувати прозорість ШІ з етапу проектування, і це може лише прискорити прагнення галузі до створення справді надійного ШІ.

2: Партнерство ШІ-агента – від інструменту до члена команди

У міру розвитку ШІ від простого виявлення до агента, здатного аналізувати складні сцени та пропонувати початкові реакції, роль оператора докорінно зміниться. Люди делегуватимуть повторювані завдання спостереження агентам ШІ, звільняючи себе для більш критичної діяльності високого рівня.

У той час як попередні системи штучного інтелекту у відеоспостереженні лише зменшували робоче навантаження оператора, автоматизуючи повторювані завдання, такі як пошук об'єктів, відстеження та генерація тривоги, агент штучного інтелекту зможе піти далі. Він автономно проводитиме складний ситуаційний аналіз, автоматично виконуватиме початкову реакцію та рекомендувати оператору моніторингу найефективніші подальші дії. Наприклад, агент штучного інтелекту може самостійно оцінити вторгнення, ініціювати попередні кроки, такі як увімкнення тривоги, а потім запропонувати оператору остаточні варіанти рішення (наприклад, чи викликати поліцію). Одночасно він може автоматично генерувати вичерпний звіт з детальним відео в реальному часі зони вторгнення, записами доступу, журналом початкових дій штучного інтелекту та запропонованими оптимальними стратегіями реагування. Оператори стануть більше схожими на Командирів, приймаючи остаточні рішення, що вимагають

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		32

нюансованого судження, складного аналізу та врахування правових і контекстуальних наслідків. Вони також візьмуть на себе роль менеджера з управління ІІІ, прозоро відстежуючи та контролюючи всі автономні дії та процеси міркування, що виконуються Агентом ІІІ. Ця важлива функція, яка запобігає зловживанню системою, вимагає значного підвищення кваліфікації оператора моніторингу.

3: Забезпечення сталої безпеки

Вибухове зростання генеративного штучного інтелекту стимулює попит на енергію. За даними Міжнародного енергетичного агентства (МЕА), споживання енергії центрами обробки даних зросте більш ніж удвічі до 2030 року за базовим сценарієм – через попит на штучний інтелект.

Індустрія відеоспостереження більше не може безмежно пріоритизувати продуктивність, оскільки вона стикається з подвійним викликом: стрімким зростанням обсягу відеоданих високої роздільної здатності та обчислювальним навантаженням штучного інтелекту на периферії. Таким чином, «стала безпека», яка надає пріоритет довговічності експлуатації та мінімізації впливу на навколишнє середовище, має стати ключовою компетенцією для досягнення зниження загальної вартості володіння (TCO) та досягнення цілей ESG (екологічної, соціальної та корпоративної відповідальності).

Для досягнення сталого рівня безпеки галузь рухається до розробки малопотужних чіпсетів штучного інтелекту, які значно знижують споживання енергії, зберігаючи при цьому високу якість зображення та обчислювальну потужність штучного інтелекту. Вона також надає пріоритет технологіям, що забезпечують ефективність обробки даних безпосередньо на периферійному пристрої (камері).

4: Розумні простори на базі відеоінтелекту

Оскільки штучний інтелект інтегрується в камери, а хмарні технології для обробки великомасштабних даних досягають успіхів, концепція «розумного простору» – простору, який може відчувати та розуміти – стає реальністю.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

Це означає, що відеоспостереження виходить за рамки простого моніторингу та стає основним джерелом даних для технології «цифрового двійника», яка відображає фізичне середовище в режимі реального часу. Цифровий двійник — це віртуальна копія реального фізичного активу, створена у віртуальному середовищі на базі комп'ютера.

Наразі інформація (метадані) штучного інтелекту, отримана камерами зі штучним інтелектом, вже використовується для бізнес-аналітики з метою оптимізації операцій у таких секторах, як розумні міста, роздрібна торгівля та передове виробництво. У майбутньому ці метадані будуть об'єднані з різноманітною інформацією з пристроїв контролю доступу, датчиків Інтернету речей та датчиків навколишнього середовища для створення єдиного, інтелектуального середовища цифрового двійника.

Це середовище цифрового двійника революціонує процес моніторингу. Замість складних, фрагментованих екранів оператори отримують цілісне уявлення про взаємозв'язки подій на інтерфейсі на основі карти, який інтегрує VMS (систему керування відео) та системи контролю доступу. У цьому ідеально відображеному цифровому просторі відеосистема зрештою перетвориться на автономний інтелектуальний простір, який глибоко розуміє ситуації, самостійно керує проблемами та вирішує їх.

Додавання новітньої технології штучного інтелекту може надати менеджерам безпеки або операторам більший контроль над роботою системи. Наприклад, ШІ може миттєво розуміти питання природною мовою, такі як «Знайти особу, яка заходила до серверної кімнати після 22:00 минулої ночі», та автоматично аналізувати записи доступу та відео, щоб повідомити про результати. Це означає справжню ситуаційну обізнаність, яка може виходити далеко за рамки базових складних параметрів пошуку.

5: Гібридна архітектура: Розподілена енергія

Зростання вартості передачі відеоданих високої чіткості, у поєднанні з проблемами суверенітету даних та нормативними вимогами, створює проблеми

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		34

для виключно хмарних систем. Таким чином, «гібридна архітектура», яка зберігає переваги хмари, одночасно зменшуючи операційне навантаження, швидко зарекомендувала себе як оптимальне рішення для сектора відеоспостереження.

Гібридна архітектура надає користувачам максимальний контроль та гнучкість над роботою системи. Оскільки вона дозволяє розгортати системні функції в найефективнішому місці на основі бізнес-потреб організації, бюджету та правового/нормативного середовища, вона стане ключовою стратегією для максимізації загальної вартості володіння (ТСО).

З точки зору відеоспостереження, гібридна архітектура максимізує ефективність завдяки гнучкому розподілу функцій між локальним та хмарним середовищами. Локальні середовища можуть розміщувати функції моніторингу в режимі реального часу та критично важливі функції, які повинні відповідати нормам короткострокового зберігання та утримання відео. Функції, що включають локальну обробку та контроль висококонфіденційних даних, також розміщуються локально для посилення контролю безпеки даних та забезпечення можливостей негайного реагування на об'єкті.

Тим часом хмарне середовище використовується для таких функцій, як віддалене централізоване управління, аналіз великомасштабних даних, глибоке навчання для моделей штучного інтелекту та довгострокове архівування. Використання хмари таким чином забезпечує масштабованість системи та зручність експлуатації.

Окрім простого розділення інфраструктури, ця архітектура також підтримує оптимальну структуру розподілених обчислень, необхідну для успішної роботи систем відеоспостереження на основі аналізу штучного інтелекту.

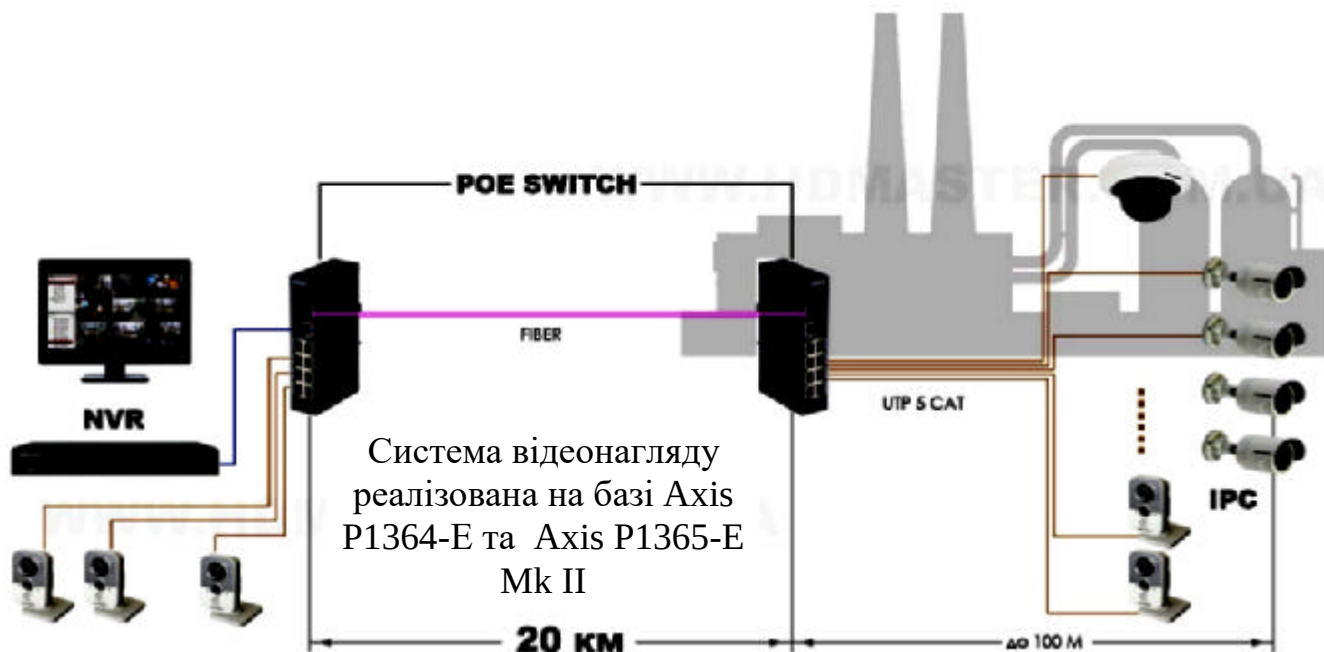


Рисунок 3.1 – Структурна схема системи

У цій структурі периферійні пристрої (камера/NVR) обробляють перший рівень обчислень, виконуючи виявлення в режимі реального часу та передаючи лише необхідні дані до хмари. Це зменшує навантаження на пропускну здатність мережі, максимізує швидкість та ефективність зберігання. Після цього хмарне середовище (центральний сервер) проводить другий рівень глибокого аналізу та великомасштабного машинного навчання на основі відфільтрованих даних з периферії, значно підвищуючи точність та складність функцій штучного інтелекту. Я вважаю, що у 2026 році штучний інтелект міцно утвердиться як новий стандарт інфраструктури безпеки.

3.3 Розробка функціональної схеми

Опишемо функції розробленої системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

Функціональна схема системи складається з наступних блоків:

– Блок функцій адміністратора.

– Блок функцій оператора.

– Блок функцій інженера.

Блок функцій адміністратора

1. Додавання нових користувачів.

Система дозволяє не тільки контролювати обстановку по відеоряду, але й відслідковувати всі зміни на двомірному плані охоронюваного простору. На плані відображаються області видимості камер і виявлені об'єкти, що полегшує сприйняття загальної обстановки.

Так, наприклад, на плані легко помітити області контрольованого простору не видимі ні однією відеокамерою.

Крім того система надає користувальницький інтерфейс для керування камерами за допомогою кліків миші на компоненті головного вікна, із зображенням плану.

Система кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II має розвинутий графічний інтерфейс і істотну обчислювальну частину.

Система має більш багату функціональність ніж існуючі комерційні розробки. Використання поворотних камер, розмаїтість можливостей по керуванню камерами й спостереженню за обстановкою дозволяє ефективніше вирішувати завдання відеонагляду, ніж при використанні традиційних систем відеонагляду з нерухливими камерами.

Таких можливостей удалося досягти завдяки використанню розроблених методів калібрування камер і виявлення областей інтересу.

Блок функцій оператора

1. Перегляд відео з камер.

2. Оцінка ситуації по плану:

– Відображення областей спостереження камер.

– Відображення доданих об'єктів.

– Відображення знайдених об'єктів.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		37



Рисунок 3.2 – Функціональна схема системи

3. Керування камерами:

- Клік по відео.
- Обертання камери.
- Клік по карті.
- Режим супроводу.

4. Зміна налаштувань системи.

Блок функцій інженера

1. Завантаження плану контролюемого простору.
2. Додавання заборонених областей на план.
3. Додавання об'єктів на план.
4. Калібрування камер.
5. Додавання та видалення камер.
6. Калібрування плану.

3.4 Розробка діаграми процесів

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

Склад статистичної сукупності графічно може бути представлений як за допомогою абсолютних, так і відносних показників. Графічне зображення складу сукупності по абсолютними і відносними показниками сприяє проведенню більш глибокого аналізу і дозволяє проводити аналіз системи.

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

Для розробника вважається звичним спочатку креслити діаграму взаємодії процесів даних рівня контексту, завдяки чому буде показано взаємодію системи.

Ця діаграма в подальшому підлягає уточненню шляхом деталізації процесів та потоків даних з метою показати систему що розробляється.

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

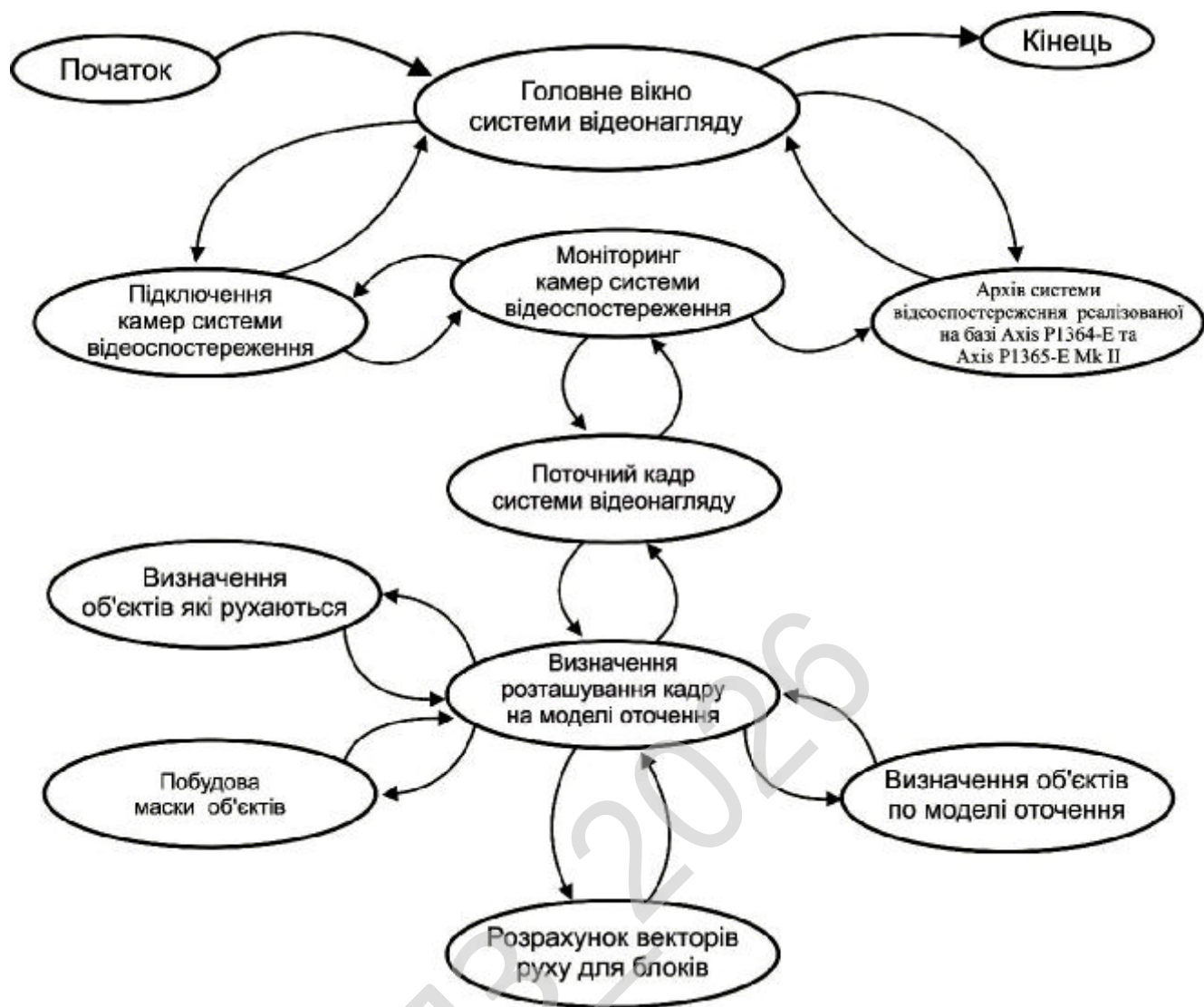


Рисунок 3.3 – Діаграма взаємодії процесів

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).

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

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

4.1 Блок-схеми та опис алгоритмів функціонування системи

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

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.

Незважаючи на те що я працював над ПЗ один в реалізації програми я використовував підходи пришвидшення розробки на основі методологій Agile.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		41

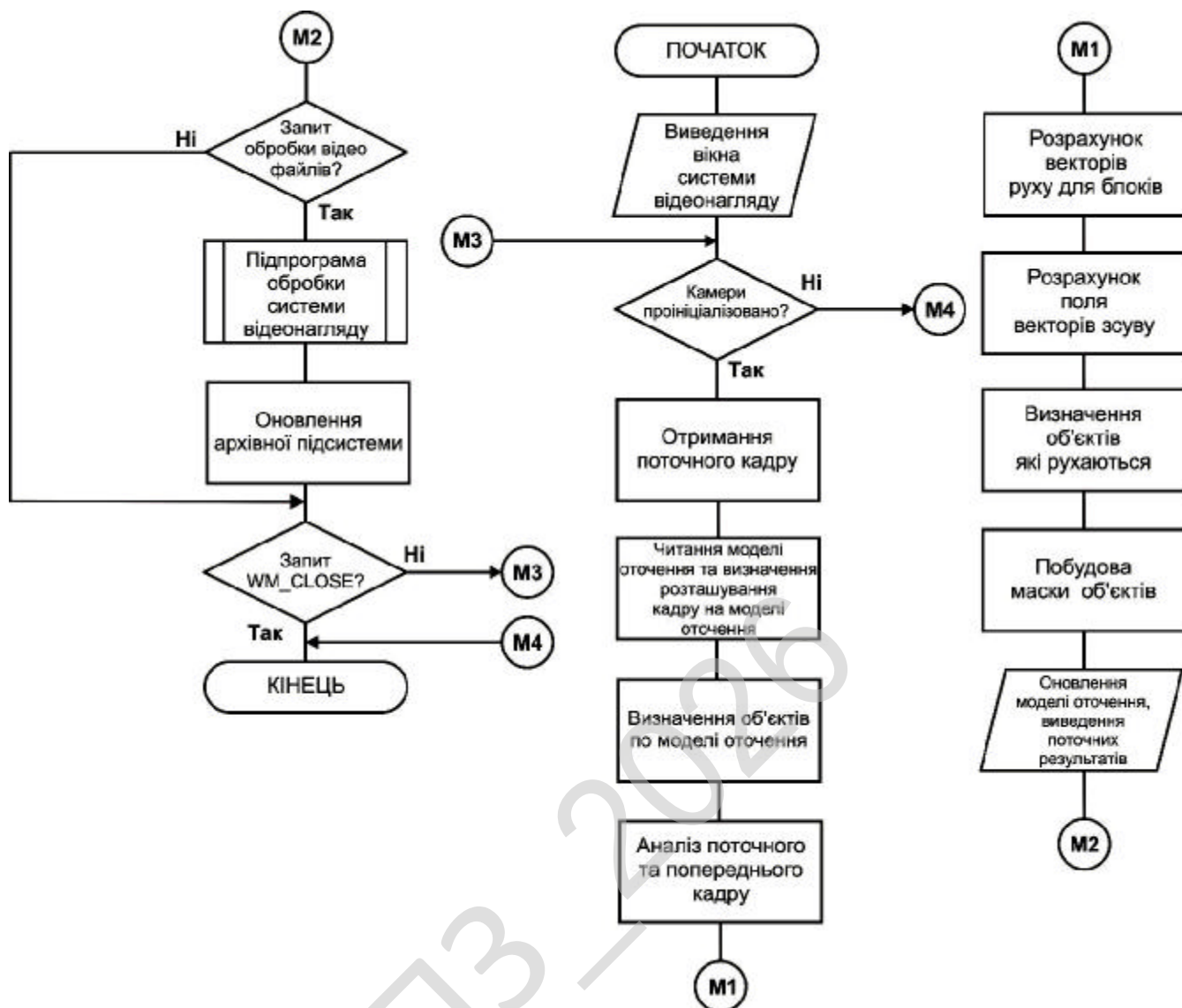


Рисунок 4.1 – Блок-схема основної програми

Гнучка́ розробка програмного забезпечення (Agile software development, agile-методи) – клас методологій розробки програмного забезпечення, що базується на ітеративній розробці, в якій вимоги та розв'язки еволюціонують через співпрацю між самоорганізовуваними багатофункціональними командами.

Гнучка розробка – найкращий засіб для підвищення продуктивності розробників програмного забезпечення.

Більшість гнучких методологій націлені на мінімізацію ризиків, шляхом зведення розробки до серії коротких циклів, що мають назву ітерацій, які зазвичай тривають один-два тижні.

Кожна ітерація сама по собі виглядає як програмний проект в мініатюрі, і включає всі завдання, необхідні для видачі мінімального приросту за функціональністю: планування, аналіз вимог, проектування, кодування, тестування і документування.

Хоча окрема ітерація, як правило, недостатня для випуску нової версії продукту, мається на увазі те, що гнучкий програмний проект готовий до випуску наприкінці кожної ітерації. Після закінчення кожної ітерації, команда виконує переоцінку пріоритетів розробки.

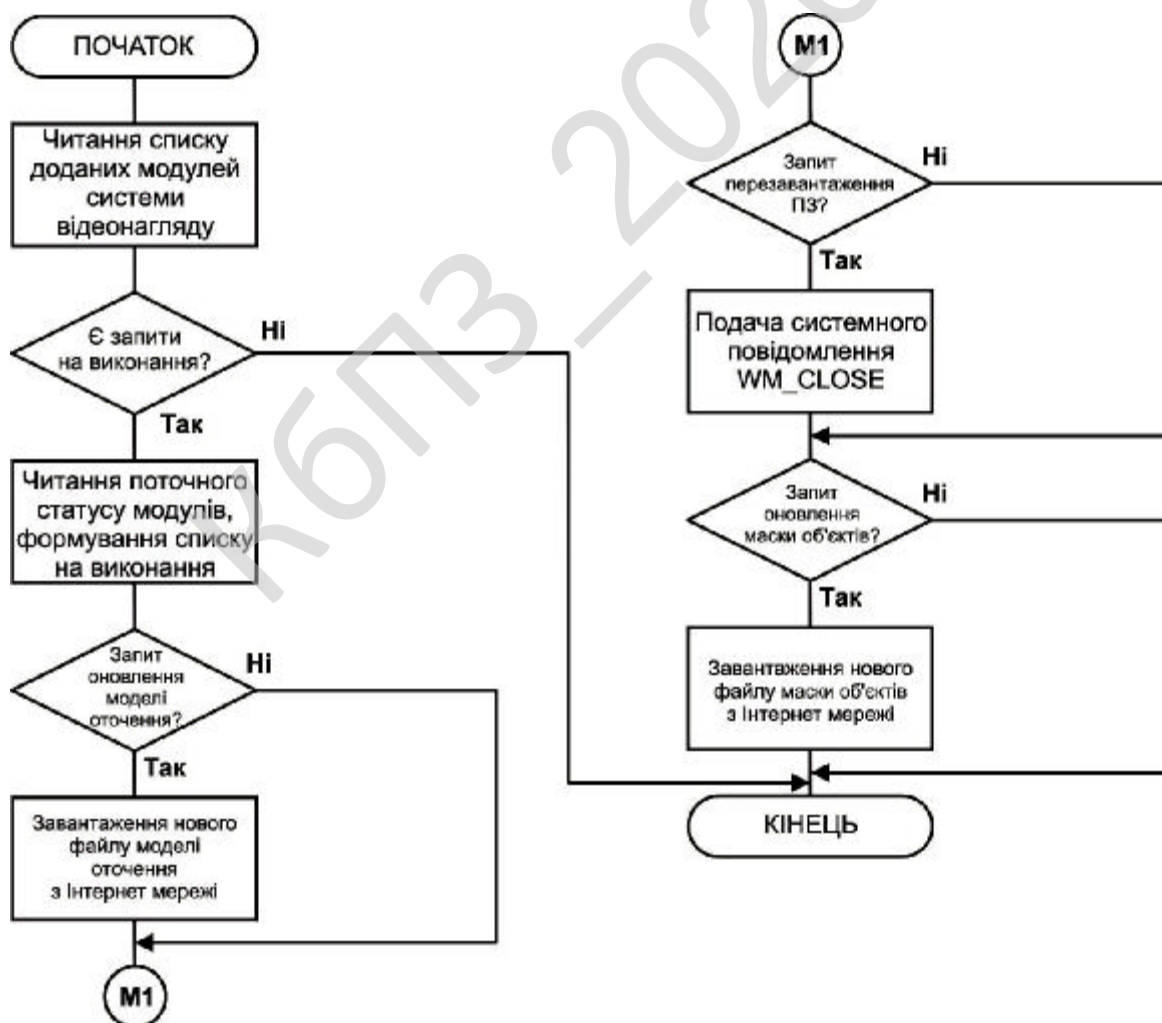


Рисунок 4.2 – Блок-схема роботи підпрограми

Agile акцентує увагу на безпосередньому спілкуванні «віч-на-віч». Більшість agile команд розташовані в одному офісі, його іноді називають bullpen. Як мінімум вона включає і «замовників» (замовники, які визначають продукт, також це можуть бути менеджери продукту, бізнес аналітики або клієнти). Офіс може також включати тестувальників, дизайнерів інтерфейсу, технічних авторів і менеджерів.

Основною метрикою agile методів є робочий продукт. Віддаючи перевагу безпосередньому спілкуванню, agile-методи зменшують обсяг письмової документації в порівнянні з іншими методами. Це привело до критики цих методів як недисциплінованих.

Agile – родина процесів розробки, а не єдиний підхід в розробці програмного забезпечення, і визначається Agile Manifesto. Agile не включає практик, а визначає цінності та принципи, якими керуються успішні команди.

Agile Manifesto розроблений і прийнятий 17 розробниками 11-13 лютого 2001 року на лижному курорті The Lodge at Snowbird в горах Юти. Маніфест підписали представники наступних методологій Extreme programming, Scrum, DSDM, Adaptive software development, Crystal Clear, Feature driven development, Pragmatic Programming. Agile Manifesto містить 4 основні ідеї та 12 принципів. Примітно, що Agile Manifesto не містить практичних порад.

Основні ідеї:

- Особистості та їхні взаємодії важливіші, ніж процеси та інструменти.
- Робоче програмне забезпечення важливіше, ніж повна документація.
- Співпраця із замовником важливіша, ніж контрактні зобов'язання.
- Реакція на зміни важливіша, ніж дотримання плану.

Принципи, які роз'яснює Agile Manifesto:

- задоволення клієнта за рахунок ранньої та безперебійної поставки коштовного програмного забезпечення;
- вітання змін вимог навіть наприкінці розробки (це може підвищити конкурентоспроможність отриманого продукту);

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		44

- часта поставка робочого програмного забезпечення (кожен місяць або тиждень або ще частіше);
- тісне, щоденне спілкування замовника з розробниками впродовж всього проекту;
- проектом займаються мотивовані особистості, які забезпечені потрібними умовами роботи, підтримкою і довірою;
- рекомендований метод передачі інформації – особиста розмова (віч-на-віч);
- робоче програмне забезпечення – найкращий вимірювач прогресу;
- спонсори, розробники та користувачі повинні мати можливість підтримувати постійний темп на невизначений термін;
- постійну увагу поліпшенню технічної майстерності та зручному дизайну;
- простота – мистецтво не робити зайвої роботи;
- найкращі технічні вимоги, дизайн та архітектура виходять у самоорганізованої команди;
- постійна адаптація до мінливих обставин.

Маніфест та Принципи гнучкої розробки містять високорівневі ідеї щодо того, як потрібно вибудовувати процес розробки програмного забезпечення, щоб успішно завершувати проекти й створювати команди, в яких приємно та цікаво працювати.

Документи визначають, що потрібно для цього зробити, але не говорять, як це зробити. По-іншому й не могло бути, оскільки Маніфест та Принципи народилися внаслідок консенсусу представників різних (хоча й споріднених) напрямів, які могли знайти спільну основу лише на рівні базових цінностей та принципів.

Критика. Багато керівників проектів, що працюють у традиційних методологіях на кшталт «водоспаду», критикують agile-методи.

Один з повторюваних пунктів критики: при agile-підході часто нехтують створенням «дорожньої карти» розвитку продукту, так само як і управлінням

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		45

вимогами, в процесі якого і формується така «карта». Гнучкий підхід до управління вимогами не має на увазі далекосяжних планів (по суті, управління вимогами просто не існує в даній методології), а має на увазі можливість замовника раптом і несподівано наприкінці кожної ітерації виставляти нові вимоги, що часто суперечать архітектурі вже створеного і поставленого продукту. Таке іноді призводить до катастрофічних «авралів» з масовим рефакторингом і переробками практично на кожній черговій ітерації.

Крім того вважається, що робота в agile мотивує розробників вирішувати всі прибулі завдання найпростішим і найшвидшим можливим способом, при цьому часто не звертаючи уваги на коректність коду з точки зору вимог базової платформи (підхід «працює, та й добре», при цьому не враховується, що може перестати працювати при найменшій зміні або ж породити важкі до відтворення дефекти після реального розгортання у клієнта). Це призводить до зниження якості продукту і накопиченню дефектів.

Методології. Існують методології, які дотримуються цінностей і принципів заявлених в Agile Manifesto, деякі з них:

1. Agile Modeling – набір понять, принципів і прийомів (практик), що дозволяють швидко і просто виконувати моделювання і документування в проектах розробки програмного забезпечення. Не включає в себе детальну інструкцію з проектування, не містить описів, як будувати діаграми на UML.

Основна мета – ефективне моделювання і документування; але не охоплює програмування та тестування, не включає питання управління проектом, розгортання і супроводу системи. Однак включає в себе перевірку моделі кодом.

2. Agile Unified Process (AUP) спрощена версія IBM Rational Unified Process (RUP), розроблена Скоттом Амблером, яка описує просте і зрозуміле наближення (модель) для створення програмного забезпечення для бізнес-додатків.

3 Agile Data Method – група ітеративних методів розробки програмного забезпечення, в яких вимоги та рішення досягаються в рамках співпраці різних крос-функціональних команд.

4. DSDM заснований на концепції швидкої розробки додатків (Rapid Application Development, RAD). Являє собою ітеративний і інкрементний підхід, який надає особливого значення тривалій участі в процесі користувача/споживача.

5. Essential Unified Process (EssUP).

6. Екстремальне програмування (Extreme programming, XP).

7. Feature driven development (FDD) – функціонально-орієнтована розробка. Використовуване в FDD поняття функції або властивості (feature) Системи досить близько до поняття прецеденту використання, використовуваному в RUP, істотна відмінність – це додаткове обмеження: «кожна функція повинна допускати реалізацію не більше, ніж за два тижні». Тобто якщо сценарій використання досить малий, його можна вважати функцією. Якщо ж великий, то його треба розбити на декілька відносно незалежних функцій.

8. Getting Real – ітераційний підхід без функціональних специфікацій, що використовується для веб-додатків. У даному методі спершу розробляється інтерфейс програми, а потім її функціональна частина.

9. OpenUP – це ітераційно-інкрементний метод розробки програмного забезпечення. Позиціюється, як легкий і гнучкий варіант RUP. OpenUP ділить життєвий цикл проекту на чотири фази: початкова фаза, фази уточнення, конструювання та передачі. Життєвий цикл проекту забезпечує надання зацікавленим особам та членам колективу точок ознайомлення і прийняття рішень впродовж усього проекту. Це дозволяє ефективно контролювати ситуацію і вчасно приймати рішення про задовільність результатів. План проекту визначає життєвий цикл, а кінцевим результатом є остаточний додаток.

10. Scrum встановлює правила керування процесом розробки та дозволяє використовувати вже існуючі практики кодування, коректуючи вимоги або

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		47

вносячи тактичні зміни. Використання цієї методології дає можливість виявляти і усувати відхилення від бажаного результату на більш ранніх етапах розробки програмного продукту.

11. Бережлива розробка програмного забезпечення (lean software development). Використовує підходи з концепції бережливого виробництва.

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 ДеГрейс та Шталь у книжці Злі проблеми, справедливі рішення посилалися 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.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		48

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.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		49

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.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		50

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.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		51

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.

NetBIOS (Network Basic Input/Output System) – протокол для роботи в локальних мережах на персональних ЕОМ типу IBM/PC, розроблений у вигляді інтерфейсу, який не залежить від фірми-виробника. Був розроблений фірмою Sytek Corporation за замовленням IBM в 1983 році. Він включає в себе інтерфейс сеансового рівня (англ. NetBIOS interface), в якості транспортних протоколів використовує TCP і UDP.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		52

Особливістю NetBIOS є можливість його роботи поверх різних протоколів, найпоширенішими/відомими з яких є NetBEUI, IPX і стек протоколів TCP/IP; причому якщо старі версії Windows орієнтувалися на більш легкі в реалізації і менш ресурсомісткі NetBEUI і IPX, то сучасні Windows орієнтуються на TCP/IP.

При використанні NetBEUI і IPX NetBIOS сам забезпечує надійність доставки даних (функціональність SPX не використовувати), а при використанні TCP/IP надійність доставки забезпечує TCP, за що удостоївся окремого імені «NBT».

Інтерфейс NetBIOS являє собою типовий інтерфейс взаємодії програм (API) для забезпечення мережових операцій введення–виведення і управління транспортним протоколом.

Програми, що використовують NetBIOS API інтерфейс, можуть працювати тільки при наявності протоколу, що допускає використання такого інтерфейсу.

NetBIOS також визначає протокол, що функціонує на сеансовому/транспортному рівнях моделі OSI. Цей протокол використовується протоколами нижчих рівнів, такими як NBFP (NetBEUI) і NetBT для виконання мережових запитів вводу–виводу і операцій, описаних в стандартному інтерфейсному наборі команд NetBIOS.

Тобто, NetBIOS сам не підтримує виконання файлових операцій. Ця функція покладається на протоколи нижчих рівнів, а сам NetBIOS забезпечує тільки зв'язок з цими протоколами і NetBIOS API–інтерфейс.

Пакет NETBIOS створений для використання групою EOM. Підтримує як режим сесій (робота через з'єднання), так і режим дейтаграм (без встановлення з'єднання). 16–символьні імена об'єктів в NETBIOS розподіляються динамічно.

NETBIOS має власну DNS, яка може взаємодіяти з інтернетівський. Ім'я об'єкта при роботі з NETBIOS не може починатися з символу *.

Додатки можуть знайти через NETBIOS потрібні їм ресурси, встановити зв'язок і послати або отримати інформацію. NETBIOS використовує для служби імен порт 137, для служби дейтаграм – порт 138, а для сесій – порт 139. Будь–яка

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		53

сесія починається з NETBIOS–запиту, завдання IP–адреси і визначення TCP–порту віддаленого об'єкта, далі йде обмін NETBIOS–повідомленнями, після чого сесія закривається.

Сесія здійснює обмін інформацією між двома NETBIOS – додатками. Довжина повідомлення лежить в межах від 0 до 131 071 байт. Припустимо одночасне встановлення декількох сесій між двома об'єктами.

При організації IP–транспорту через NETBIOS IP–дейтаграмма вкладається в NETBIOS–пакет. Інформаційний обмін відбувається в цьому випадку без встановлення зв'язку між об'єктами. Імена NETBIOS повинні містити в собі IP–адреси. Так, частина NETBIOS–адреси може мати вигляд IP.XX.XX. XX.XX, де IP вказує на тип операції (IP через Netbios), а XX. XX. XX.XX – IP– адреса.

Система NETBIOS має власну систему команд (call, listen, hang up, send, receive, session status, reset, cancel, adapter status, unlink, remote program load) і примітивів для роботи з дейтаграммами (send datagram, send broadcast datagram, receive datagram , receive broadcast datagram).

Всі кінцеві вузли NETBIOS діляться на три типи:

- широкомовні («b») вузли;
- вузли точка–точка («p»);
- вузли змішаного типу («m»).

IP–адреса може асоціюватися з одним із зазначених типів. В–вузли встановлюють зв'язок зі своїм партнером за допомогою широкомовних запитів. Р– і М–вузли для цієї мети використовують netbios сервер імен (NBNS) і сервер розподілу дейтаграм (NBDD).

NetBIOS забезпечує:

- реєстрацію і перевірку мережеских імен;
- встановлення і розрив з'єднань;
- зв'язок з підтвердженням доставки інформації;
- зв'язок без підтвердження доставки інформації;
- підтримку управління і моніторингу драйвера і мережевої карти.

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.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		55

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.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		56

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 C. 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.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		57

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.

4.2 Захист розробленого програмного забезпечення

Дані які використовуються у даній роботі захищаються алгоритмом ДСТУ 7564:2014 («Купина»). В Україні на основі консервативного підходу із залученням відомих і добре досліджених конструкцій була розроблена геш-функція, що базується на новому блоковому шифрі „Калина” (ДСТУ 7624:2014).

Національний стандарт ДСТУ 7564:2014 визначає криптографічну функцію гешування „Купина”, додатковий режим її застосування для формування коду автентифікації повідомлення (імітовставки), а також значення для перевірки реалізацій.

Для скорочення обсягу тексту національного стандарту була застосована математична нотація, що дозволяє отримати точний і компактний запис.

Водночас, такий підхід може ускладнювати сприйняття сутності алгоритму для фахівців, що не мають фундаментальної криптологічної освіти.

У роботі наводиться розгорнутий альтернативний опис функції гешування „Купина” із позначеннями, традиційними для галузі комп’ютерних наук.

Термінологія та позначення

Вектор ініціалізації – бітова послідовність фіксованої довжини (512 або 1024 біта), що використовується як початкове значення при обчисленні геш-значення.

Внутрішній стан – бітова послідовність фіксованої довжини (512 або 1024 біта), що є проміжним значенням на кожній ітерації перетворення функції

гешування, а також вхідним та вихідним значеннями перетворень P і Q ; для цих перетворень внутрішній стан подається як матриця розміром $8 \times s$ байт.

Геш-значення (геш-вектор) – бітова послідовність фіксованої довжини ($n = 8 \cdot s, s \in \{1, 2, \dots, 64\}$), що є результатом роботи функції гешування.

Доповнення – вставка додаткових біт у кінець повідомлення для отримання кратності довжини бітової послідовності довжині внутрішнього стану функції гешування.

Повідомлення – бітова послідовність довжини від 0 біт (порожній рядок) до $2^{96} - 1$ біт.

Функція стиснення – ітеративне перетворення, що відображає l -бітний блок повідомлення та l -бітне значення, отримане функцією стиснення на попередньому кроці, у нове l -бітне значення.

Далі використовуються наступні позначення:

- $\oplus$ – додавання за модулем 2 (XOR);
- $0x$ – префікс числа, що записане у шістнадцятковій системі числення;
- $a \bmod b$ – ціле невід’ємне число, що дорівнює залишку від ділення цілого числа a на натуральне число b ;
- B_i – i -й байт вхідної послідовності;
- C^i – константа перетворення XORRoundKey або Add64RoundKey для i -го циклу;
- c – кількість стовпців внутрішнього стану в матричному поданні;
- ϕ – функція стиснення;
- H – визначена у стандарті функція гешування;
- $H(M)$ – результат обчислення функції гешування для повідомлення M (гешзначення);
- IV – вектор ініціалізації;
- l – розмір внутрішнього стану функції гешування (у бітах), $l \in \{512, 1024\}$;
- M – повідомлення;

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		59

- m_i – i -й блок повідомлення M ;
- n – довжина обчисленого геш-значення;
- N – довжина повідомлення M без доповнення;
- P, Q – складові перетворення функції стиснення;
- P_{512} – перетворення P для 512-бітного внутрішнього стану;
- P_{1024} – перетворення P для 1024-бітного внутрішнього стану;
- Q_{512} – перетворення Q для 512-бітного внутрішнього стану;
- Q_{1024} – перетворення Q для 1024-бітного внутрішнього стану;
- r – кількість ітерацій у перетвореннях P і Q ($r = t$ в ДСТУ 7564:2014);
- S – внутрішній стан геш-функції;
- t – кількість блоків m , з яких складається повідомлення M , включаючи доповнення;
- v_i – i -й біт вхідної послідовності;
- Ω – завершальне перетворення;
- Купина- n – режим використання функції гешування з усіченням обчисленого гешзначення до розміру n біт.

Загальні положення

Під функцією гешування H розуміється залежне від вектора ініціалізації IV відображення послідовності біт M у геш-значення $H(M)$ фіксованої довжини n .

ДСТУ 7564:2014 визначає функцію гешування, яка виконує перетворення «Купина-256» або «Купина-512», що забезпечують обчислення геш-значення з довжинами 256 або 512 біт відповідно.

Геш-значення довжиною 256 бітів додатково може бути усічено до бітової послідовності довжиною від 8 до 248 біт з кроком у 8 біт, 512 бітів може бути усічене до бітової послідовності довжиною від 264 до 504 біт з кроком у 8 біт.

Режим роботи для формування геш-значення довжиною n біт позначається як «Купина- n ».

Основними режимами роботи функції ґешування, що рекомендуються до застосування, є «Купина-256», «Купина-384» і «Купина-512».

Структура перетворення

Функція ґешування, визначена в ДСТУ 7564:2014, формує ґеш-значення для повідомлення, що складається з бітової послідовності довжини від 0 біт (порожній рядок) до $2^{96}-1$ біт.

При формуванні ґеш-значення повідомлення доповнюється, далі поділяється на l -бітні блоки $m_0, \dots, m_t$, після чого виконується обробка кожного блоку шляхом ітеративного виконання функції стиснення φ .

При цьому формуються значення $h_i = \varphi(h_{i-1}, m_i)$ де $i = 1, \dots, t$, а початкове значення $h_0 = IV$.

Після обробки останнього блоку повідомлення результуюче ґеш-значення обчислюється як $H(M) = \Omega(h_t)$, де Ω – завершальне перетворення, що повертає n - бітне значення, кратне 8 ($0 < n \leq l/2$).

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		61

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку 5.1 зображено розроблене у бакалаврської дипломної роботі система кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи: Навігаційного меню яке викликається натисканням правої клавіші маніпулятора миші; Функціональних кнопок ПЗ; Верхнього меню; Розділу обрання групи.



Рисунок 5.1 – Головне вікно ПЗ

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

На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення.

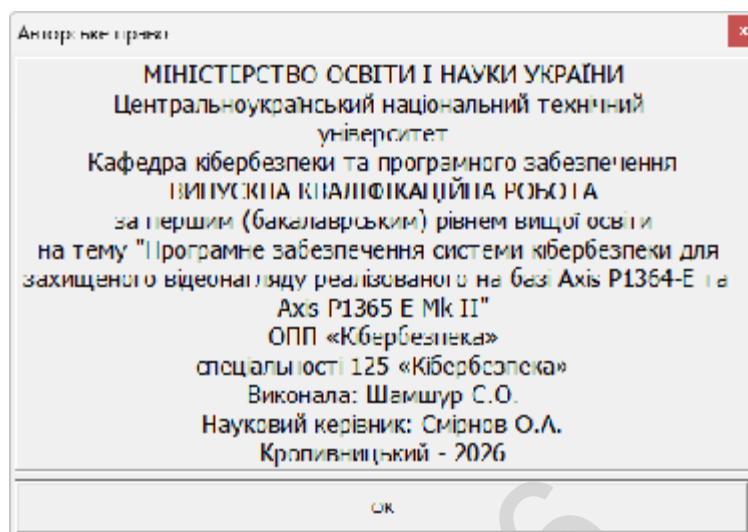


Рисунок 5.2 – Авторське право

Розглянемо процес впровадження програмного забезпечення, це процес налаштування програмного забезпечення під певні умови використання, а також навчання користувачів роботі з програмним продуктом. Впровадження програмного забезпечення це усі дії, що роблять розроблену програмну систему 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:

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		63

- Випуск.
- Встановлення та активація.
- Деактивація.
- Адаптація.
- Оновлення.
- Вмонтування.
- Відстежування версій.
- Видалення.
- Вилучення з обігу.

При впровадженні програмного забезпечення потрібно урахувати наступні дії:

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

– 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.

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 ІТс).
- 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 ІТс.
- Сформулювати такі очікувані результати, які з високою ймовірністю є елементами набору ОТ.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		65

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.
- Помилки інтерфейсу.
- Помилки у зовнішніх структурах даних або в доступі до зовнішньої бази даних.
- Помилки характеристик (необхідна ємність пам'яті і т.д.).
- Помилки ініціалізації та завершення.

Обрано умови розповсюдження – Shareware. Під умовно-безплатним програмним забезпеченням можна розуміти спосіб або метод розповсюдження комерційного ПЗ на ринку (тобто на шляху до кінцевого користувача), при якому випробувачеві пропонується обмежена за можливостями (не повнофункціональна або демонстраційна версія), терміном дії (тріал версія) або версія з вбудованим набридливим нагадуванням про необхідність оплати використання програми.

В угоді про використання (ліцензії для кінцевого користувача, EULA) також може бути обумовлена заборона на комерційне або професійне (не тестове) її використання. Основний принцип умовно-безплатного ПЗ - «спробуй, перш ніж купити» (try before you buy). ПЗ що поширюється як умовно-безплатний, надається користувачам безоплатно. Звичайно користувач платить тільки за час завантаження файлів через Інтернет або за носій (CD диск, флешку, ключ). Протягом певного терміну, що становить зазвичай тридцять днів, він може користуватися програмою, тестувати її, освоювати її можливості. Якщо після закінчення цього терміну користувач вирішить продовжити використання ПЗ, він зобов'язаний купити його (zareєstrуватися), заплативши авторові певну суму. В іншому випадку користувач повинен припинити використання ПЗ та видалити його зі свого комп'ютера.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		66

6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

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

Рішення завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.
- Досліджена система для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.
- На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II.

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

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

Програма реалізована на мові високого рівня Python. Дана мова програмування дозволяє найбільш ефективно обробляти дані призначені для

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		67

системи кібербезпеки для захищеного відеонагляду реалізованого на базі Axis P1364-E та Axis P1365-E Mk II. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи кібербезпеки й включає програми, що реалізують її функції.

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

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

Для підвищення рівня безпеки запропоновано застосовувати алгоритм ДСТУ 7564:2014.

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

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		68

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 p.
2. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 p.
3. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 p.
4. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 p.
5. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 p.
6. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 p.
7. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 p.
8. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21-61.
9. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А, Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.: Видавничий центр “Кафедра”, 2025.– 320 с.
10. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка*. 2025. Том 1 № 29. С.704–716, 2025
11. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		69

systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224.

12. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.

13. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.

14. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.

15. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings*, 2024, 3909, pp. 227–241.

16. 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.

17. 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.

18. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. № 2(26), С. 170–188.

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

20. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.

21. 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.

22. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.

23. Akhalaia, G., Iavich, M., Iashvili, G., Prysiashnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». *CEUR Workshop Proceedings*, 2023, 3550, pp. 313-320.

24. 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

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

26. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». *CEUR Workshop Proceedings*, Volume 3504, 2023, pp. 1-11.

27. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: *Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.

28. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». *Кібербезпека: освіта, наука, техніка*, №3(19), 2023, С. 176-196.

29. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». *II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2023)»* м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.

30. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». *VII міжнародна науково-практична конференція “Інформаційна безпека та комп'ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення*, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.

31. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». *VII міжнародна науково-практична конференція “Інформаційна безпека та комп'ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення*, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.

32. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 2(72), С. 170-178.

33. 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,

34. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». *Journal of Ambient Intelligence and Humanized Computing* Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.

35. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління*, № 2(70). 2022. С. 28-37.

36. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 3(69). С. 93-98.

37. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»*, № 2 (307). С. 46-52. 2022.

38. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		73

захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89.

39. 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

40. 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.

41. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». *2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020*, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.

42. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». *CEUR Workshop Proceedings Volume 2805*, 2020, Pages 44-58.

43. 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.

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

45. 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.

					ВКРБ-125.26.0046.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		74

46. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 122-131.
47. 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.
48. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». *Lecture Notes in Networks and Systems*, vol 152. Springer, Cham. 2021, pp 66-84.
49. 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.
50. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I., Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 166-171.
51. 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.
52. 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.

53. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 125-136.

54. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». *International Journal of Computer Network and Information Security (IJCNIS)*. Vol. 12, No. 3, 2020. PP.33-43.

55. 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.

56. 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.

57. 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.

58. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, Vol 2588, P. 215-227, 2019.

59. 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.