Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту

Кафедра кібербезпеки інформаційних систем, мереж і технологій

До захисту допущено
Кафедрою КІСМіТ протокол №____ від «___» грудня 2025 р.

завідувач кафедри _____ Марина ЄСІНА
(підпис) *(ім'я, прізвище)*
«___» грудня 2025 р.

Кваліфікаційна робота

здобувача другого (магістерського) рівня вищої освіти

Система відеоспостереження згідно вимог методології нульової довіри
(назва роботи)

Спеціальність (спеціалізація) 125 «Кібербезпека та захист інформації»

Освітня програма «Безпека інформаційних і комунікаційних систем»

Виконавець _____ Михайло ПИТАЙЧУК
(підпис) *(ім'я, прізвище)*

Науковий керівник _____ Іван ГОРБЕНКО
(підпис) *(ім'я, прізвище)*

Харків – 2025

РЕФЕРАТ

Пояснювальна записка до проекту магістра містить 76 сторінок, 9 рисунків, 8 таблиці, 2 додатки та 20 джерел за переліком посилань.

Мета роботи полягає в підвищенні рівня безпеки банківської інфраструктури за рахунок розроблення та впровадження комплексної системи відеоспостереження на основі концепції нульової довіри.

Об'єкт дослідження – процеси відеоспостереження в банківських інформаційних системах.

Предмет дослідження – комп'ютерна система відеоспостереження багатоквартирного житлового будинку.

Основними методами досліджень є вивчення наукових та нормативних джерел, аналіз сучасних відеосистем і підходів до забезпечення кібербезпеки, моделювання загроз, проектування архітектури, синтез технічних рішень, тестування розробленої системи.

У роботі досліджено: сучасні підходи до побудови систем відеоспостереження в банківській інфраструктурі, їхні вразливості та типові загрози; принципи і методологію нульової довіри, що застосовані до компонентів відеоінфраструктури; криптографічні механізми автентифікації та забезпечення цілісності відеоданих; архітектурну модель багаторівневої системи відеоспостереження з використанням контейнеризації; механізми контролю доступу та взаємодії між PDP, PEP, IAM і PKI; методи оцінювання ризиків і критерії ефективності Zero Trust-моделі; а також роботу створеного прототипу у симульованому середовищі та його вплив на підвищення рівня безпеки банківських відеосистем.

Результати роботи: на основі проведеної роботи створено архітектурну модель системи відеоспостереження банку, що відповідає вимогам нульової довіри, включає механізми автентифікації, сегментації, криптографічного

захисту та моніторингу, а також продемонструє підвищення рівня безпеки у порівнянні з традиційними системами відеоспостереження.

Ключові слова: КІБЕРЗАГРОЗИ, ВІДЕОСПОСТЕРЕЖЕННЯ, НУЛЬОВА ДОВІРА, ZERO TRUST, БАНКІВСЬКА ІНФРАСТРУКТУРА, МІКРОСЕГМЕНТАЦІЯ, АВТЕНТИФІКАЦІЯ, КРИПТОГРАФІЧНИЙ ЗАХИСТ, ІНФОРМАЦІЙНА БЕЗПЕКА, IP-КАМЕРА, ВІДЕОАНАЛІТИКА.

ABSTRACT

The explanatory note to the master's thesis contains 76 pages, 9 illustrations, 8 tables, 2 appendices and 20 sources in the list of references.

The aim of the work is to increase the security level of banking infrastructure by developing and implementing a comprehensive video surveillance system based on the zero trust concept.

The object of the study is video surveillance processes in banking information systems.

The subject of the study is a computerised video surveillance system for a multi-apartment residential building.

The main research methods are the study of scientific and regulatory sources, analysis of modern video systems and approaches to cybersecurity, threat modelling, architecture design, synthesis of technical solutions, and testing of the developed system.

The work examines: modern approaches to building video surveillance systems in banking infrastructure, their vulnerabilities and typical threats; zero trust principles and methodology applied to video infrastructure components; cryptographic mechanisms for authentication and ensuring the integrity of video data; the architectural model of a multi-level video surveillance system using containerisation; mechanisms for controlling access and interaction between PDP, PEP, IAM and PKI; methods for assessing risks and criteria for the effectiveness of the Zero Trust model; as well as the operation of the created prototype in a simulated environment and its impact on improving the security of banking video systems.

Results: Based on the work done, an architectural model of a bank video surveillance system has been created that meets zero trust requirements, includes authentication, segmentation, cryptographic protection and monitoring mechanisms, and demonstrates an increase in security compared to traditional video surveillance systems.

Keywords: CYBER THREATS, VIDEO SURVEILLANCE, ZERO TRUST, BANKING INFRASTRUCTURE, MICROSEGMENTATION, AUTHENTICATION, CRYPTOGRAPHIC PROTECTION, INFORMATION SECURITY, IP CAMERA, VIDEO ANALYTICS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AES-256-GCM	-	Режим симетричного шифрування, що забезпечує конфіденційність і цілісність даних.
AES-256-XTS	-	Режим симетричного шифрування, що використовується для захисту носіїв даних.
AI	-	Штучний інтелект; інтелектуальні модулі відеоаналітики.
API	-	Програмний інтерфейс взаємодії між сервісами системи.
CA	-	Центр сертифікації, що керує цифровими сертифікатами.
CCTV	-	Замкнена телевізійна система аналогового відеоспостереження.
CRL	-	Список відкликаних сертифікатів.
DDoS	-	Розподілена атака на відмову в обслуговуванні.
DoS	-	Атака на відмову в обслуговуванні.
DTLS	-	Протокол захисту трафіку поверх UDP.
DTLS-SRTP	-	Захищений протокол потокової передачі відео в реальному часі.
EAP-TLS	-	Протокол автентифікації на основі TLS-сертифікатів.
ECDSA	-	Алгоритм цифрового підпису на еліптичних кривих.
ENISA	-	Європейське агентство з кібербезпеки.
FIDO2	-	Стандарт багатофакторної автентифікації без паролів.
HSM	-	Апаратний модуль безпеки для роботи з ключами.
IAM	-	Система управління ідентичностями та доступом.
IP	-	Протокол маршрутизації та адресації в мережі.
IP-camera	-	Мережева відеокамера, що передає дані через IP.
IPsec	-	Набір протоколів криптографічного захисту трафіку.
ISO/IEC	-	Міжнародні організації стандартизації у сфері ІБ.
Kerberos	-	Протокол мережевої автентифікації.
mTLS	-	Взаємна TLS-автентифікація клієнта та сервера.
NAS	-	Мережеве сховище даних.
NIST	-	Національний інститут стандартів і технологій США.
NVR	-	Мережевий відеореєстратор для зберігання архівів.
OAuth 2.0	-	Протокол авторизації на основі токенів.
OCSP	-	Онлайн-перевірка статусу цифрових сертифікатів.

OpenID Connect	-	Протокол ідентифікації поверх OAuth 2.0.
PKCS#11	-	Стандарт взаємодії з криптографічними токенами.
PKI	-	Інфраструктура відкритих ключів.
RTP	-	Протокол передавання аудіо- та відеоданих у реальному часі.
SAN	-	Мережа зберігання даних.
SDN	-	Програмно визначена мережа з централізованим керуванням.
SDP	-	Програмно визначений периметр доступу.
SIEM	-	Система аналізу та кореляції подій безпеки.
SHA-256	-	Криптографічна хеш-функція (256 біт).
SHA-3-256	-	Хеш-функція сімейства SHA-3 з виходом 256 біт.
SRTP	-	Захищений протокол потокової мультимедіа-передачі.
TLS 1.3	-	Сучасний протокол захисту транспортного рівня.
TPM	-	Апаратний модуль довіри для захисту ключів.
UEBA	-	Аналітика поведінки користувачів та пристроїв.
VLAN	-	Віртуальна локальна мережа для сегментації трафіку.
VMS	-	Система керування відеоспостереженням.
VPN	-	Захищена віртуальна приватна мережа.
VRF	-	Механізм ізоляції таблиць маршрутизації в мережі.
X.509	-	Стандарт структури цифрових сертифікатів.
Zero Trust	-	Модель безпеки без апріорної довіри, з постійною перевіркою доступу.
PEP	-	Точка застосування політик доступу.
PDP	-	Точка прийняття рішень щодо доступу.
PE	-	Політичний механізм (Policy Engine) Zero Trust.
PA	-	Адміністратор політик, що застосовує рішення PDP.

ВСТУП

Актуальність теми. Сучасний банківський сектор перебуває під впливом безпрецедентних викликів у сфері кібербезпеки. Зростання кількості інцидентів, поява нових типів атак, ускладнення технологічної інфраструктури та підвищені вимоги до захисту конфіденційних даних формують потребу у впровадженні принципово нових підходів до організації безпеки. У цьому контексті системи відеоспостереження перестали бути виключно інструментом фізичного контролю та набули значення ключового елемента інформаційно-комунікаційної інфраструктури банку, що впливає на цілісність, доступність і достовірність даних. За таких умов концепція нульової довіри (Zero Trust) набуває особливої актуальності, адже передбачає багаторівневу перевірку доступу та виключає можливість неконтрольованої довіри до будь-яких пристроїв, користувачів чи сервісів.

Системи відеоспостереження у банках виконують низку критично важливих функцій: запобігають правопорушенням, забезпечують моніторинг операційних процесів, створюють доказову базу під час розслідування інцидентів, контролюють переміщення персоналу та підвищують захист фінансових операцій. Наявність сучасної, надійної системи відеоконтролю не лише підвищує загальний рівень безпеки, а й сприяє дотриманню регуляторних вимог і зміцнює довіру клієнтів та партнерів до банківської установи.

Розроблення системи відеоспостереження на основі принципів Zero Trust потребує врахування специфіки фінансової інфраструктури, особливостей загрозового середовища, політик доступу та характеристик мережевих камер, серверів зберігання та аналітичних модулів. Важливим етапом є визначення функціональних вимог до системи, що включають автентифікацію користувачів і пристроїв, криптографічний захист переданих даних, сегментацію мережі, безперервний моніторинг подій та відповідність

стандартам інформаційної безпеки. Таке комплексне опрацювання дозволяє створити архітектуру, здатну забезпечити високий рівень стійкості та надійності в умовах зростаючих кіберзагроз.

Метою даної кваліфікаційної роботи є розробка комплексної системи відеоспостереження банку, побудованої на принципах методології нульової довіри, що забезпечить високий рівень безпеки, надійності та відповідності сучасним вимогам безпеки фінансових установ. У роботі проведено аналіз загроз і вразливостей відеоінфраструктури, визначено технічні вимоги до системи, розроблено архітектурну модель Zero Trust, змодельовано сценарії роботи системи та виконано її тестування в умовах, наближених до реальної експлуатації.

Ця кваліфікаційна робота має на меті не лише створити архітектуру системи відеоспостереження, а й продемонструвати її ефективність у контексті сучасних кіберзагроз, підтвердивши доцільність впровадження Zero Trust у банківській сфері.

Метою дослідження є підвищення рівня безпеки банківської інфраструктури за рахунок розроблення та впровадження комплексної системи відеоспостереження на основі концепції нульової довіри.

Об'єктом дослідження є процеси відеоспостереження в банківських інформаційних системах.

Предмет дослідження – архітектура та механізми функціонування комп’ютерної системи відеоспостереження банку, реалізованої за принципами Zero Trust.

Методи дослідження: вивчення наукових та нормативних джерел, аналіз сучасних відеосистем і підходів до забезпечення кібербезпеки, моделювання загроз, проектування архітектури, синтез технічних рішень, тестування розробленої системи.

Результати дослідження: на основі проведеної роботи створено архітектурну модель системи відеоспостереження банку, що відповідає вимогам нульової довіри, включає механізми автентифікації, сегментації,

криптографічного захисту та моніторингу, а також продемонструє підвищення рівня безпеки у порівнянні з традиційними системами відеоспостереження.

Можливими напрямами подальших досліджень є:

- розширення функціональних можливостей системи за рахунок інтеграції з SIEM, UEBA та аналітичними платформами штучного інтелекту;
- розробка мобільних інструментів доступу до системи з урахуванням принципів Zero Trust;
- адаптація моделі до інших типів критичної інфраструктури, включно з дата-центрами, урядовими структурами та фінтех-організаціями.

1 ТЕОРЕТИЧНІ ТА НАУКОВО-МЕТОДОЛОГІЧНІ ОСНОВИ ПОБУДОВИ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ В БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

1.1 Сучасні підходи до організації відеоспостереження в критичній фінансовій інфраструктурі

Системи відеоспостереження сьогодні стали одним із ключових елементів захисту фінансових установ. Якщо раніше вони виконували переважно функцію фіксації подій, то нині їх роль істотно розширилася: сучасні банківські відеосистеми інтегруються з механізмами кібербезпеки та фізичної безпеки й забезпечують оперативний контроль доступу, моніторинг інцидентів та підтримку стійкості критичної інфраструктури. Наукові джерела підкреслюють, що відеоспостереження вже не можна розглядати як другорядний інструмент фізичної охорони — воно стало невід'ємною частиною інформаційно-комунікаційної архітектури, яка потребує централізованого управління та всебічного захисту [1].

Розвиток відеотехнологій у банківській сфері поступово змістив акцент від традиційних аналогових CCTV-рішень до цифрових IP-орієнтованих платформ. На відміну від застарілих аналогових систем, сучасні IP-камери функціонують як повноцінні мережеві вузли, що працюють на стандартизованих протоколах та взаємодіють з іншими компонентами мережі. Міжнародні стандарти, що регламентують проєктування відеосистем, наголошують на необхідності розглядати відеоспостереження як комплексну багаторівневу інфраструктуру, яка об'єднує мережеве обладнання, засоби керування відео, сховища даних та інструменти кібербезпеки [2].

Перехід до IP-відеосистем відкрив нові можливості масштабування, централізації та аналітики, але водночас істотно підвищив рівень уразливості. Камери, відеореєстратори та сервери перетворилися на потенційні точки входу для зловмисників. У звітах ENISA підкреслюється, що саме периферійні

пристрої часто стають першими цілями кіберзлочинців, адже їх компрометація здатна забезпечити доступ до внутрішніх мереж організації [3]. Це призвело до необхідності застосування принципу «захист у глибину», який поєднує фізичні, мережеві та криптографічні заходи.

Поряд із традиційними функціями, сучасні системи відеоспостереження активно використовують інтелектуальні аналітичні модулі. Технології машинного навчання дозволяють автоматично виявляти нетипову поведінку, підозрілі об'єкти, аномальні переміщення чи потенційні загрози. Наукові дослідження демонструють, що інтеграція відеоаналітики значно підвищує ефективність контролю та зменшує навантаження на операторів, що особливо важливо для великих банківських мереж із десятками або сотнями локацій [4].

Ще одним ключовим аспектом сучасних підходів є мережева сегментація. Ізоляція IP-камер та відеосерверів у спеціалізованих VLAN або VRF-сегментах дозволяє мінімізувати ризики горизонтального переміщення зловмисника у разі компрометації окремого пристрою. Рекомендації у сфері інформаційної безпеки наголошують, що правильна мережна сегментація — один із найефективніших способів обмеження наслідків атаки на відеоінфраструктуру [5].

Захист відеотрафіку став обов’язковою складовою сучасних систем. Стандарти інформаційної безпеки визначають відеодані як потенційно конфіденційні активи, оскільки вони можуть містити зображення клієнтів, процеси виконання операцій або інші чутливі дані. Тому шифрування каналів передавання, а також захист архівів у сховищах за допомогою криптографічних механізмів стали необхідною умовою відповідності сучасним вимогам безпеки [6].

Окремий тренд — використання хмарних платформ для відеоспостереження. Дослідження доводять, що хмарні рішення забезпечують високу масштабованість, централізоване адміністрування та відмовостійкість. Разом з тим, такі системи потребують посиленого контролю доступу, аудиту

та моніторингу інцидентів, щоб гарантувати відповідність регуляторним вимогам та уникнути ризику витоку даних [7].

Забезпечення безперервності роботи відеосистем є критично важливим для банківського сектору. Втрата відеозапису може стати причиною юридичних чи фінансових ризиків, тому сучасні архітектури включають резервування каналів зв'язку, дублювання сховищ та реплікацію архівів. Дослідники підкреслюють, що наявність резервних механізмів визначає стійкість відеоінфраструктури у випадку технічних збоїв або кіберінцидентів [8].

Остання й одна з найважливіших тенденцій — впровадження принципів нульової довіри (Zero Trust) до архітектури відеоспостереження. У межах цього підходу кожен пристрій, користувач або сервіс має проходити автентифікацію та авторизацію, а мережа поділяється на дрібні сектори з індивідуальними політиками доступу. Zero Trust посилює контроль за доступом до відеоархівів, мінімізує ризики компрометації камер і забезпечує безперервний моніторинг аномальної активності [9].

У підсумку, сучасні підходи до організації банківського відеоспостереження базуються на поєднанні мережевої та криптографічної безпеки, інтелектуальної аналітики, резервування та принципів нульової довіри. Така інтегрована модель дає змогу забезпечити високий рівень стійкості та захищеності відеоінфраструктури, що є критично важливим для фінансових установ, які працюють в умовах підвищених кіберризиків.

1.2 Стандарти та регуляторні вимоги України щодо захисту банківських інформаційних систем

Захист інформаційних систем банківського сектору в Україні формується на перетині національного законодавства у сфері кібербезпеки, спеціальних нормативних актів, що регламентують банківську діяльність, та вимог міжнародних стандартів, інтегрованих у національну систему технічного регулювання. Для систем відеоспостереження, які обробляють

аудіовізуальні дані, що потенційно містять відомості про клієнтів, персонал, банківські операції та внутрішні процеси, питання дотримання нормативних вимог стає критично важливим елементом загальної політики безпеки.

Базовим елементом нормативно-правової основи є національне законодавство у сфері кібербезпеки, яке визначає загальні принципи та вимоги до захисту інформаційних систем критичної інфраструктури. Законодавство встановлює обов'язок суб'єктів фінансового сектору впроваджувати комплексні організаційні та технічні заходи, що забезпечують безперервність роботи інформаційних ресурсів, їхню цілісність, конфіденційність та здатність до оперативного відновлення після інцидентів [10]. У межах цього законодавчого поля банківські установи мають забезпечити належний рівень захищеності всіх інформаційних активів, у тому числі й систем відеоспостереження.

Важливе місце займають вимоги банківського законодавства, які регламентують порядок забезпечення банківської таємниці та захисту інформації про клієнтів. У нормах спеціального законодавства наголошується, що будь-яка інформація, яка дає можливість ідентифікувати клієнта або відстежити характер його операцій, належить до категорії даних, що підлягають особливому захисту [11]. Системи відеоспостереження, які фіксують поведінку клієнтів, пересування персоналу та процеси виконання банківських операцій, фактично стають частиною інформаційної системи банку й повинні бути включені до переліку критичних активів.

Центральну роль у формуванні галузевої системи кібербезпеки відіграє Національний банк України як регулятор фінансового ринку. Він встановлює вимоги до організації систем управління інформаційною безпекою, контролює рівень захищеності банківських інформаційних ресурсів і забезпечує адаптацію національних норм до міжнародних та європейських підходів [12]. Нормативні документи регулятора визначають вимоги до класифікації інформаційних активів, оцінювання ризиків, забезпечення безперервності діяльності, реагування на інциденти та впровадження технічних контролів.

Системи відеоспостереження, як частина технологічної інфраструктури, зобов’язані відповідати цим вимогам у повному обсязі.

Положення регулятора з організації інформаційної безпеки в банках встановлюють комплекс заходів, яких мають дотримуватися фінансові установи, включаючи обов’язок створення, впровадження й підтримання системи управління інформаційною безпекою, що охоплює всі інформаційні активи без винятку [13]. У межах цієї системи відеоінфраструктура повинна бути належним чином задокументована, їй має бути присвоєно рівень критичності, визначено відповідальних осіб, сформовано процедури обслуговування, моніторингу, аудиту, реагування на інциденти та відновлення. Розміщення серверів відеоспостереження, сховищ та мережевих компонентів має відповідати вимогам до фізичної безпеки, контролю доступу і резервування, а канали передавання даних — вимогам до криптографічного захисту.

Значну увагу регулятор приділяє управлінню кіберінцидентами та обов’язковій взаємодії банків з галузевим центром реагування. Вимоги щодо виявлення, фіксації, класифікації та ескалації інцидентів поширюються також і на системи відеоспостереження, оскільки їх компрометація може призвести до несанкціонованого доступу до внутрішніх мереж або витоку аудіовізуальних даних, що становлять банківську таємницю [15]. Таким чином, відеосистема повинна бути інтегрована в загальну інфраструктуру моніторингу, яка включає механізми збору журналів, синхронізацію подій, аналіз аномалій і забезпечення доказової бази у випадку розслідування.

Національні стандарти з управління інформаційною безпекою, гармонізовані з міжнародними, є ще одним важливим рівнем регуляторних вимог. Найважливішим з них є стандарт, який визначає вимоги до створення та підтримання системи управління інформаційною безпекою, включно з процедурами оцінювання ризиків, захисту активів, застосування технічних і криптографічних засобів, контролю доступу, ведення журналів подій, резервування та тестування відновлення [16]. Для систем відеоспостереження

стандарт вимагає забезпечення контролю цілісності відеоданих, надійного шифрування каналів передавання та обмеження доступу шляхом багаторівневої автентифікації.

Окремим напрямом є процес адаптації українського законодавства до європейських нормативів, що регламентують цифрову стійкість фінансового сектору. У рамках гармонізації із європейськими нормами посилюються вимоги до управління ризиками, безперервності роботи та кіберстійкості, зокрема щодо критичних технологічних платформ і хмарних сервісів [14]. Для відеосистем це означає необхідність систематичного тестування, впровадження контролів надійності та стійкості, а також використання механізмів захищеної інтеграції з постачальниками технологічних рішень.

У стратегічних документах регулятора наголошується на тому, що відеоспостереження є частиною комплексної системи захисту банківської інфраструктури та повинне розглядатися не ізольовано, а як елемент загальної моделі безпеки, яка включає фізичні, технічні та організаційні компоненти [17]. Це передбачає інтеграцію відеосистем у загальні процеси управління ризиками, використання єдиної системи ідентифікації користувачів, централізованих механізмів логування, а також формування політик доступу на основі принципів найменших привілеїв.

Таким чином, нормативно-правова база України визначає системний і багаторівневий підхід до захисту інформаційних систем банків, де системи відеоспостереження посідають особливе місце як технологічні активи, що безпосередньо впливають на конфіденційність, цілісність і доступність інформації. Виконання вимог законодавства, регуляторних документів і стандартів формує підґрунтя для побудови сучасної моделі відеоінфраструктури, стійкої до кіберзагроз і здатної забезпечувати безперервність критичних фінансових процесів.

1.3 Концепція та архітектура нульової довіри

Концепція нульової довіри (Zero Trust) стала одним із ключових сучасних підходів до побудови безпечної інформаційної інфраструктури. Її поява зумовлена зростанням складності інформаційних систем, поширенням хмарних сервісів та збільшенням кількості кіберзагроз, що можуть проникати як ззовні, так і з внутрішнього середовища організації. На відміну від традиційних моделей безпеки, які покладаються на периметровий захист і передбачають, що внутрішнім користувачам та пристроям можна довіряти, Zero Trust виходить з протилежного принципу: ніколи не довіряй – завжди перевіряй.

Основна ідея Zero Trust полягає у тому, що будь-яка взаємодія в системі — запит до сервісу, доступ до ресурсу, передавання відеопотоку чи запуск процесу — має бути автентифікована, авторизована та задокументована. Це означає, що навіть пристрої, які фізично знаходяться в межах корпоративної мережі, не розглядаються як гарантовано безпечні. Модель Zero Trust передбачає постійний контроль контексту доступу: враховується стан пристрою, роль користувача, тип виконуваної операції, рівень ризику, політики відповідності та інші фактори. [9].

У контексті систем відеоспостереження нульова довіра стає критично важливою, оскільки ці системи складаються з великої кількості гетерогенних пристроїв — камер, відеосерверів, мережевих комутаторів, сховищ, клієнтських станцій — кожен з яких може бути потенційною точкою проникнення. Дослідження в галузі безпеки мережевих відеосистем демонструють, що компрометація лише однієї камери може створити умови для доступу до внутрішньої мережі, перехоплення відеопотоків, маніпулювання архівами або отримання привілеїв адміністратора [2]. Модель нульової довіри мінімізує ці ризики шляхом розділення повноважень, мікросегментації мережі та посилення процедур автентифікації.

Ключовим елементом нульової довіри є управління доступом на основі атрибутів, що передбачає врахування ролі користувача, контексту виконання

операції, типу пристрою, стану безпеки вузла та ризиків, пов’язаних із запитом. Наукові праці з розроблення атрибутивних моделей контролю доступу свідчать, що такі підходи дозволяють значно підвищити захищеність систем із великою кількістю взаємодіючих технологічних компонентів [6]. Для банківських відеосистем це означає можливість диференціації доступу між операторами, адміністраторами безпеки, технічними працівниками та автоматизованими сервісами.

Суттєву роль у моделі нульової довіри відіграє мікросегментація мережі, що передбачає поділ інфраструктури на дрібні логічні сегменти, кожен з яких має власні політики доступу та контролю. Така архітектура дозволяє ізолювати IP-камери від інших внутрішніх систем банку, обмежуючи можливість переміщення атакувальника всередині мережі у випадку компрометації одного з компонентів. Мікросегментація особливо актуальна у відеоінфраструктурах з великою кількістю камер, розподілених між філіями, банкоматними зонами, касовими центрами та дата-центрами [3].

Не менш важливою складовою є перевірка цілісності пристроїв та автентичність обладнання. У роботах, присвячених захисту інтелектуальних сенсорних систем, підкреслюється, що належна оцінка стану пристроїв перед наданням їм доступу до мережевих ресурсів суттєво знижує ризик використання скомпрометованих або підроблених пристроїв [4]. У банківській сфері це має особливе значення, оскільки камери часто працюють у публічних або частково контрольованих зонах.

У рамках нульової довіри значну увагу приділяють криптографічному захисту всіх каналів взаємодії. Згідно з міжнародними стандартами інформаційної безпеки, захищені канали зв’язку повинні використовувати стійкі алгоритми шифрування, механізми взаємної автентифікації та засоби перевірки цілісності даних [1]. У відеоінфраструктурі це гарантує захист як потоків відео в реальному часі, так і архівів, які можуть містити конфіденційну або регуляторно значущу інформацію. Криптографічний захист також

необхідний у випадку інтеграції хмарних сервісів або віддалених філій банку, де ризик перехоплення даних суттєво зростає.

Окремий вимір концепції нульової довіри пов’язаний із безперервним моніторингом подій та поведінковим аналізом. Архітектури, засновані на нульовій довірі, передбачають постійне відстеження того, як користувачі та пристрої взаємодіють із системою, а також фіксацію відхилень від типових шаблонів поведінки. Для банківських відеосистем це означає, що кожне підключення до відеосервера, кожен запит на доступ до архіву та кожна адміністративна дія повинні супроводжуватися записом у журналах подій, аналізом ризику та, за необхідності, блокуванням операції [15].

Нульова довіра також передбачає підвищені вимоги до безперервності роботи системи та її здатності до швидкого відновлення після інцидентів. Наукові праці про надійність відеоінфраструктур підкреслюють, що відмова окремого компонента в середовищі камер спостереження може мати суттєві наслідки для подальшого аналізу інцидентів або юридичного підтвердження фактів [8]. Тому нульова довіра поєднується з концепціями надлишковості, реплікації, захищеного зберігання та використання географічно розподілених серверів.

Поступовий перехід банківських установ до моделі нульової довіри цілком відповідає загальносвітовим тенденціям у сфері кібербезпеки. У міжнародній практиці дедалі більше визнається, що сучасні, розподілені та взаємопов’язані технологічні середовища не мають чіткого периметра, а отже — потребують комплексної моделі захисту, здатної ефективно працювати за таких умов. Дослідження підкреслюють, що Zero Trust є найбільш придатним підходом для архітектур, де пристрої, дані та користувачі постійно взаємодіють між собою через різні мережеві сегменти та платформи [7]. Банківська відеоінфраструктура повністю відповідає цим характеристикам, оскільки складається з великої кількості пристроїв, рівень безпеки яких не можна вважати гарантованим у будь-який момент.

Отже, концепція нульової довіри формує фундамент для створення безпечної архітектури відеоспостереження в банківському секторі. Її застосування забезпечує комплексний захист відеоінфраструктури через поєднання мікросегментації, атрибутивного контролю доступу, криптографічного захисту, безперервного моніторингу та перевірки цілісності пристроїв. Саме ці принципи становитимуть основу моделі відеоспостереження, яка буде розроблена в наступних розділах цієї роботи.

Архітектурна модель нульової довіри:

Policy Enforcement Point (PEP)

PEP – це точка, яка фізично контролює доступ суб'єкта до ресурсу. У системах відеоспостереження PEP реалізується через:

- мережеві шлюзи між камерами та серверами;
- API-шлюзи між операторами та архівами;
- проксі-сервіс для вебінтерфейсів управління.

Policy Decision Point (PDP)

Це логічний компонент, який ухвалює рішення про доступ. Рішення ґрунтується на політиках, атрибутах пристрою, контексті та поведінкових факторах.

Policy Engine (PE)

Використовує механізми оцінки ризику та систему політик. У фінансових установах він часто інтегрований із системами SIEM, UEBA та IAM.

Policy Administrator (PA)

Реалізує прийняте PDP рішення у вигляді конфігураційних змін або команд доступу.

Захищені ресурси (Cameras, NVR, Archive, Analytics)

Це кінцеві точки системи, які запитують або надають доступ до відеоданих.

Абстрактна модель архітектури нульової довіри зображена на рис 1.1.

Рисунок. 1.1 - Абстрактна модель доступу із нульовою довірою

1.4 Аналіз концепції нульової довіри як основи безпечної архітектури відеоспостереження

За останні десять років концепція нульової довіри перетворилася на один із ключових векторів розвитку архітектур інформаційної безпеки. Це підтверджується широкою кількістю наукових досліджень, міжнародних стандартів та практичних рекомендацій, орієнтованих на захист критичної інфраструктури. І зарубіжні, і українські наукові праці підкреслюють, що фінансовий сектор є однією з тих галузей, де впровадження Zero Trust дає особливо відчутні результати. Це пояснюється високою інтенсивністю кіберзагроз, складною внутрішньою структурою банківських процесів та значною кількістю взаємопов’язаних інформаційних систем [9]. У випадку з відеоспостереженням, яке фактично стало кіберфізичною складовою банківської інфраструктури, принципи Zero Trust вже сприймаються як необхідний елемент сучасних моделей захисту.

Наукові публікації, присвячені архітектурам нульової довіри, підкреслюють їхню придатність для середовищ із високим рівнем взаємодії, де відсутній чіткий мережевий периметр. У дослідженнях інститутів, що займаються стандартизацією та прикладною безпекою, зазначено, що Zero Trust усуває слабкість традиційних підходів, які ґрунтуються на припущенні про надійність внутрішньої мережі, і замінює їх моделлю постійної перевірки кожного запиту [9]. Це особливо актуально для банків, де інформаційні системи залежать від сотень периферійних пристроїв, включно з мережевими камерами.

Важливим напрямом наукових досліджень є безпека відеосистем, що інтегруються в корпоративні мережі. У працях, присвячених захисту IP-відеоспостереження, наголошується, що відеокамери стають одними з найбільш уразливих пристроїв через обмежену обчислювальну потужність, типові помилки конфігурації та недостатній рівень контролю автентичності [2]. Дослідники вказують, що саме моделі нульової довіри дають змогу мінімізувати ризики, пов’язані з доступом до таких пристроїв, завдяки їхній ізоляції, постійному моніторингу та суворим політикам автентифікації.

Особливу увагу у світовій літературі приділено впровадженню нульової довіри у фінансових організаціях. Аналітичні роботи, присвячені кібербезпеці банків, показують, що фінансова індустрія вже кілька років є однією з провідних у впровадженні Zero Trust, оскільки її процеси характеризуються високою вартістю інформації, наявністю великої кількості користувачів з різними рівнями доступу та значною кількістю транзакцій [7]. Провідні фінансові установи світу реалізують поетапний перехід до нульової довіри: від посилення автентифікації та сегментації систем до впровадження повної архітектури, заснованої на атрибутному контролі доступу та динамічному оцінюванні ризиків.

У наукових оглядах відзначається також зростання значущості поведінкового аналізу, який інтегрується з Zero Trust. Для відеоінфраструктури банківських установ це має особливе значення, оскільки поведінковий аналіз дозволяє відстежувати дії операторів, адміністраторів і технічного персоналу, визначати відхилення від стандартних сценаріїв роботи та виявляти ознаки зловмисних дій або компрометації. Дослідження у сфері інтелектуальних систем безпеки підкреслюють, що поєднання відеоаналітики й Zero Trust забезпечує якісно новий рівень контролю подій і реагування [4].

Досвід фінансових установ у різних країнах показує, що впровадження нульової довіри може відбуватися за різними підходами. Більшість організацій починають із модернізації механізмів автентифікації, переходячи до багатофакторних рішень та централізованого керування ідентичностями. У

науковій літературі наголошується, що саме компонента ідентифікації є ключовою основою Zero Trust, адже рівень надійності автентифікації безпосередньо впливає на загальну безпеку доступу [6]. Якщо говорити про відеоспостереження, це передбачає відмову від розрізнених локальних облікових записів та перехід до централізованих систем, які дозволяють ефективно контролювати дії операторів і адміністраторів.

У прикладних дослідженнях підкреслюється важливість контролю цілісності та автентичності відеоданих. Практичний досвід міжнародних фінансових організацій демонструє, що застосування криптографічних механізмів у поєднанні з Zero Trust створює ефективну модель захисту потоків відео та архівів [1]. У той же час науковці наголошують на необхідності створення стійких схем зберігання, що підтримують перевірку походження даних, що є особливо актуальним у випадку аналізу інцидентів або юридичного використання відеозаписів.

Важливою тенденцією, яку відображено в аналітичних і наукових публікаціях, є використання хмарних технологій та віртуалізації у відеосистемах фінансових організацій. Дослідження показують, що хмарні системи відеоспостереження спрощують застосування концепції нульової довіри, оскільки дозволяють централізувати політики доступу, забезпечувати перевірку конфігурацій та автоматично застосовувати механізми безпеки на всіх рівнях інфраструктури [7]. Разом з тим науковці підкреслюють ризики, пов’язані з залежністю від сторонніх постачальників, що потребує додаткових заходів у рамках Zero Trust.

Аналіз глобального досвіду також свідчить про те, що застосування Zero Trust у відеоінфраструктурах сприяє підвищенню ефективності реагування на інциденти. Зарубіжні дослідження наводять приклади, коли впровадження нульової довіри дозволило виявити несанкціоновані підключення до відеосерверів, спроби модифікації архівів або втручання у роботу камер у режимі реального часу [15]. Це підкреслює важливість постійного

моніторингу та централізованої системи логування у рамках архітектури Zero Trust.

У науковій літературі наголошується, що впровадження нульової довіри є не одноразовим проєктом, а безперервним процесом, що включає аналіз ризиків, удосконалення політик доступу, оновлення механізмів автентифікації та розвиток систем моніторингу. Кінцевою метою такого підходу є формування архітектури, у якій довіра до будь-якого суб'єкта або пристрою визначається на підставі об'єктивних критеріїв, а не через формальне розташування в мережі.

Таким чином, наукові дослідження та глобальний практичний досвід демонструють, що концепція Zero Trust є найефективнішою моделлю захисту для відеоінфраструктури фінансових установ. Її застосування дає змогу створити архітектуру, яка здатна протистояти складним кіберзагрозам, забезпечувати цілісність і конфіденційність відеоданих та підтримувати стійкість банківських операцій. Це створює підґрунтя для розроблення моделі системи відеоспостереження на основі нульової довіри, що буде запропонована в наступних розділах.

Нижче, на рис. 1.2, зображено схему архітектури нульової довіри для системи відеоспостереження.

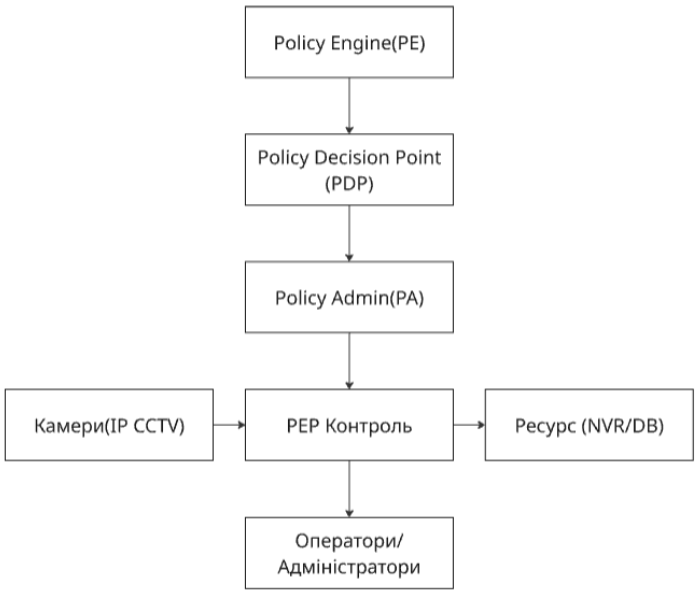

Рис. 1.2 - Схема архітектури нульової довіри для відеоспостереження

1.5 Огляд наукових публікацій та глобального досвіду впровадження Zero Trust у середовищі фінансових установ

Наукові дослідження, присвячені впровадженню концепції нульової довіри у фінансових установах, утворюють кілька чітко окреслених напрямів, які доповнюють один одного й формують комплексне уявлення про практику застосування Zero Trust у банківському секторі. Аналіз літератури дає змогу виокремити щонайменше чотири основні групи робіт: нормативно-методологічні дослідження, прикладні технічні розробки, емпіричні кейс-стаді та праці, зосереджені на організаційних і економічних аспектах трансформації моделей безпеки [7], [9], [15].

Перша група охоплює дослідження, в яких Zero Trust розглядається як цілісна парадигма побудови політик безпеки у фінансовому секторі. У цих роботах наголос робиться не стільки на окремих технологічних рішеннях, скільки на принципах формування довіри, управління ризиками, побудови архітектур доступу та відповідності регуляторним вимогам [7], [9]. Автори аналізують, як принципи нульової довіри співвідносяться з моделями управління інформаційною безпекою, які вже застосовуються у банках, та пропонують методики поетапної трансформації існуючих систем. Для відеоінфраструктури такі дослідження є важливими, оскільки дозволяють вбудувати її у загальну модель безпеки без необхідності ізольованого проєктування.

Друга група публікацій присвячена суто технічним аспектам впровадження Zero Trust у складних, розподілених середовищах фінансових організацій. У цих роботах розглядаються способи трансформації існуючих мережевих і сервісних архітектур, а також запропоновано формальні моделі опису взаємодії між компонентами, які повинні функціонувати в умовах недовіри за замовчуванням [2], [6]. Для банківських систем відеоспостереження особливий інтерес становлять публікації, де досліджується поведінка розподілених технологічних компонентів у сценаріях, коли частина інфраструктури перебуває у зоні потенційного або

підтвердженого компрометування. У таких роботах моделюються сценарії поступового посилення вимог до підтвердження надійності пристроїв і сервісів, включно з елементами сенсорної інфраструктури.

Третій важливий напрямок — це емпіричні дослідження, що базуються на аналізі конкретних впроваджень Zero Trust у великих фінансових групах, міжнародних банках та платіжних системах [7], [15]. Такі публікації зазвичай містять дані про етапи переходу, проблеми, з якими стикалися проєктні команди, показники ефективності та уроки, засвоєні в процесі модернізації систем безпеки. Досвід окремих організацій демонструє, що ключовою перешкодою є наявність значної кількості застарілих технологічних комплексів, які не були спочатку спроєктовані з урахуванням вимог нульової довіри. У випадку відеоінфраструктури це передусім стосується поєднання старих систем з новими платформами управління доступом та централізованими рішеннями з моніторингу.

Четвертий напрямок складають роботи, що аналізують організаційні та економічні наслідки переходу до Zero Trust у фінансовому середовищі. Дослідники вказують, що впровадження цієї концепції не може бути обмежене лише інсталюванням нових технологічних засобів, оскільки воно потребує перегляду ролей, процесів, структури служб безпеки та підходів до управління IT-активами [6], [9]. У таких роботах розглядаються моделі планування витрат, порівнюються сценарії «точкових» впроваджень із варіантами глибокої трансформації, оцінюється вплив на операційну діяльність, час реагування на інциденти й репутаційні ризики. Для систем відеоспостереження, які часто сприймаються як допоміжний інструмент, ці дослідження показують необхідність переведення їх у категорію стратегічних активів, що прямо впливають на керованість ризиками.

Окремим шаром літератури є публікації, присвячені критичним інфраструктурам і специфічним загрозам, що стосуються таких об’єктів. У межах цього напряму фінансові організації розглядаються поряд із енергетикою, транспортом та іншими чутливими секторами, а Zero Trust

аналізується як відповідь на складні багатовекторні загрози [3], [5]. Автори таких робіт пропонують підходи до уніфікації політик безпеки для різних технологічних сегментів, у тому числі тих, що включають сенсорні та відеопідсистеми. Для банків це створює можливість побудови єдиної концепції захисту, у якій відеоспостереження не буде «осторонь» від інших критичних компонентів.

У глобальному досвіді впровадження Zero Trust у фінансових установах можна простежити певні регіональні особливості. У роботах, присвячених практиці країн Північної Америки, акцент робиться на взаємодії з регуляторами та застосуванні рекомендацій національних інститутів стандартизації [9]. Дослідження європейського контексту більше зосереджені на поєднанні Zero Trust із вимогами до цифрової операційної стійкості та регуляторними рамками фінансових ринків [7]. У публікаціях, що стосуються азійських фінансових центрів, відзначається висока швидкість технологічної модернізації та активне використання хмарних платформ, що створює сприятливі умови для застосування нульової довіри в масштабі всього технологічного ландшафту.

Попри значний масив досліджень, у літературі зберігається низка прогалин, які є важливими з точки зору банківських систем відеоспостереження. По-перше, відносно мало праць зосереджено саме на поєднанні Zero Trust із відеоінфраструктурою, тоді як більшість публікацій описують загальні IT-системи, мережеві сервіси та доступ до бізнес-додатків [2], [4]. По-друге, бракує формалізованих моделей оцінювання ефективності впровадження нульової довіри у сенсорних і відеопідсистемах, які дозволили б кількісно зіставляти різні варіанти архітектур. По-третє, обмежена кількість робіт присвячена специфіці фінансових систем країн із перехідними економіками, де поєднуються різні покоління технологій та існують додаткові регуляторні й ресурсні обмеження.

Загалом аналіз наукових публікацій і глобального практичного досвіду показує, що концепція нульової довіри вже посіла ключове місце в стратегіях

безпеки провідних фінансових установ, але її потенціал стосовно банківських систем відеоспостереження реалізований лише частково. Це створює науково-практичну нішу для подальших досліджень, спрямованих на розроблення формальних моделей, методик оцінювання та практичних рекомендацій щодо інтеграції відеоінфраструктури в Zero Trust-архітектури. Саме заповненню цієї прогалини присвячені наступні розділи роботи, де буде запропоновано модель системи відеоспостереження банку, адаптовану до вимог нульової довіри.

Висновки за розділом 1

У першому розділі було проведено комплексний аналіз теоретичних та науково-методологічних основ побудови сучасних систем відеоспостереження в банківських інформаційних системах. Отримані результати підтверджують, що відеоінфраструктура фінансових установ давно вийшла за межі традиційної ролі інструмента фізичної охорони та перетворилася на повноцінний компонент критичної інформаційної системи, який потребує всебічного й системного кіберзахисту.

Дослідження сучасних підходів показало, що перехід від аналогових CCTV-рішень до IP-орієнтованих платформ кардинально змінив архітектуру відеоспостереження. Такі системи працюють у межах корпоративних мереж, взаємодіють із численними сервісами та використовують стандартизовані мережеві протоколи. Попри відчутне зростання функціональної гнучкості, це також призвело до розширення поверхні атак: IP-камери, сервери архівації, мережеві вузли та програмні системи керування стали об’єктами потенційних загроз. Наукові джерела вказують, що за відсутності централізованих механізмів контролю доступу, криптографічного захисту та мережевої сегментації такі системи залишаються вразливими до перехоплення трафіку, несанкціонованого доступу та компрометації відеоархівів.

Аналіз нормативно-правової бази України продемонстрував, що відеоспостереження повинно розглядатися як критичний інформаційний актив і підпорядковуватися тим самим вимогам, що й інші елементи банківських IT-систем. Законодавство та регуляторні документи НБУ передбачають

обов’язкову класифікацію активів, управління ризиками, застосування криптографічного захисту, ведення журналів подій та реалізацію політик доступу. Таким чином, традиційні засоби фізичної охорони мають бути інтегровані в єдину систему управління інформаційною безпекою.

У межах аналізу концепції нульової довіри встановлено, що Zero Trust є найбільш релевантною та ефективною моделлю для сучасних відеосистем. На противагу периметровим підходам, Zero Trust ґрунтується на принципі повної відсутності апріорної довіри — навіть до внутрішніх пристроїв або користувачів. Ця модель забезпечує мікросегментацію мережі, атрибутивний контроль доступу, постійний моніторинг активності, перевірку цілісності пристроїв та застосування надійних механізмів автентифікації. Усе це дає змогу значно знизити ризики компрометації камер, сервісів чи каналів передавання відеоданих і підвищити загальну стійкість системи до внутрішніх і зовнішніх кіберзагроз.

Огляд наукових досліджень та міжнародного досвіду показав, що фінансові установи по всьому світу активно впроваджують Zero Trust-архітектури, визнаючи їхню ефективність у протидії складним атакам. Доведено, що Zero Trust особливо результативна в середовищах із великою кількістю розподілених пристроїв — саме таких, як сучасні системи відеоспостереження. Водночас виявлено наукову прогалину: моделі Zero Trust для відеоінфраструктур банків досі недостатньо формалізовані та потребують подальшої розробки. Це й визначає актуальність наступних етапів дослідження.

2 ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ МОДЕЛІ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ БАНКУ НА ЗАСАДАХ ZERO TRUST

2.1 Формалізація загроз і вразливостей відеоінфраструктури банку

Відеоінфраструктура банку є складовою критичної інформаційної системи, у межах якої об’єднано механізми фізичного контролю, технологічного моніторингу та кібербезпеки. Її функціонування залежить від узгодженої роботи мережевих пристроїв, серверних компонентів, програмного забезпечення та механізмів управління доступом. У моделі, побудованій на принципах нульової довіри, жодний із цих елементів не розглядається як довірений, що вимагає формального опису загроз і потенційних вразливостей для всіх рівнів системи [4], [5].

Формалізація загроз передбачає визначення структурованої множини факторів, які здатні порушити конфіденційність, цілісність або доступність відеоінфраструктури.

Перший клас загроз охоплює деструктивні впливи на кінцеві відеопристрої, насамперед IP-камери. У наукових роботах відзначено, що більшість камер працюють на спрощених мікропрограмах, які часто мають відкриті порти, обмежені механізми контролю доступу та недостатній рівень захисту каналів зв’язку. Дослідження IEEE продемонстрували, що компрометація камери може призвести як до несанкціонованого доступу до відеопотоків, так і до проникнення у внутрішню мережу організації через слабко захищені службові інтерфейси [10], [14]. Через це кінцеві пристрої слід розглядати як окремий клас активів високого ризику.

Другий клас загроз стосується мережевої інфраструктури, через яку передаються відеодані. Більшість відеосистем працює за принципом багаторівневого транспортування потоків від камер до серверів зберігання, і кожен із цих сегментів може бути атакований з метою перехоплення, модифікації або блокування трафіку. У рекомендаціях NIST наголошується,

що незахищений мережею відеотрафік є одним із ключових факторів ризику у сфері критичної інфраструктури, оскільки може бути використаний для створення підроблених відеопотоків, впровадження шкідливого трафіку або порушення синхронізації між елементами системи [5], [6]. Це підкреслює необхідність застосування криптографічних протоколів, сегментації потоків і постійного моніторингу мережевої поведінки.

Третій клас загроз пов’язаний із системами централізованого зберігання відеоданих, серед яких сервери архівації та мережеві відеореєстратори. Наукові дослідження демонструють, що ці сервери часто працюють на стандартних операційних системах з розширеним набором сервісів, що робить їх бажаною ціллю для атак з виконанням довільного коду або зміною конфігурацій. Компрометація цих систем може призвести до видалення або підміни архівів, маніпулювання часовими мітками або впливу на логіку збереження даних. У фінансовому секторі саме сервери відеоспостереження стають одними з первинних цілей атак на критичну інфраструктуру через їхнє стратегічне значення та недостатню сегментацію у більшості застарілих архітектур [11], [16].

Четвертий клас загроз охоплює ризики, пов’язані з діями внутрішніх користувачів, які мають легітимний доступ до системи. Інсайдерські інциденти належать до найпоширеніших у фінансовому секторі й можуть мати особливо серйозні наслідки, оскільки такі користувачі часто володіють доступом до архівів та привілейованих адміністративних функцій. До подібних загроз належать несанкціонований перегляд відеоданих, зміна параметрів запису, навмисне видалення фрагментів відео або коригування журналів подій. На відміну від зовнішніх атак, такі випадки складно виявити без застосування сучасних інструментів поведінкового аналізу та багаторівневого журналювання, що ще раз підкреслює важливість впровадження Zero Trust-підходів до контролю доступу [7], [17].

Окремо необхідно виділити загрози, пов’язані з порушенням доступності системи. Вони включають як технічні збої, так і цілеспрямовані

атаки типу DoS або DDoS, що можуть унеможливити передавання або запис відеоданих у критичний момент. У роботах, присвячених забезпеченню стійкості фінансових систем, наголошується, що втрата доступності відеоархівів може суттєво зашкодити виконанню регуляторних вимог, ускладнити розслідування інцидентів або вплинути на юридичну валідність доказів [8], [19]. До цього класу належать також ризики фізичного впливу на обладнання, збої в мережевих комутаторах та відмова систем резервного зберігання.

Ще один вимір ризиків охоплює загрози, пов’язані з ланцюгом постачання та сторонніми сервісами. Банки дедалі частіше використовують хмарні платформи, віддалене адміністрування та сторонні VMS-рішення, що розширює поверхню атаки. Дослідження показують, що недостатній контроль за сторонніми підрядниками, наявність універсальних облікових записів технічної підтримки та непрозорість механізмів оброблення даних у хмарних середовищах створюють додаткові ризики, які складно контролювати всередині локальної моделі безпеки [9], [15], [20].

Таким чином, формалізація загроз відеоінфраструктури банку передбачає комплексний розгляд взаємодії між кінцевими пристроями, мережевими елементами, серверами зберігання, операторами, зовнішніми учасниками та інфраструктурою доступності. Такий підхід дозволяє побудувати системну модель ризиків(рис. 2.1), що відповідає вимогам Zero Trust та забезпечує основу для розроблення механізмів контролю доступу, які будуть сформульовані у наступному підрозділі.

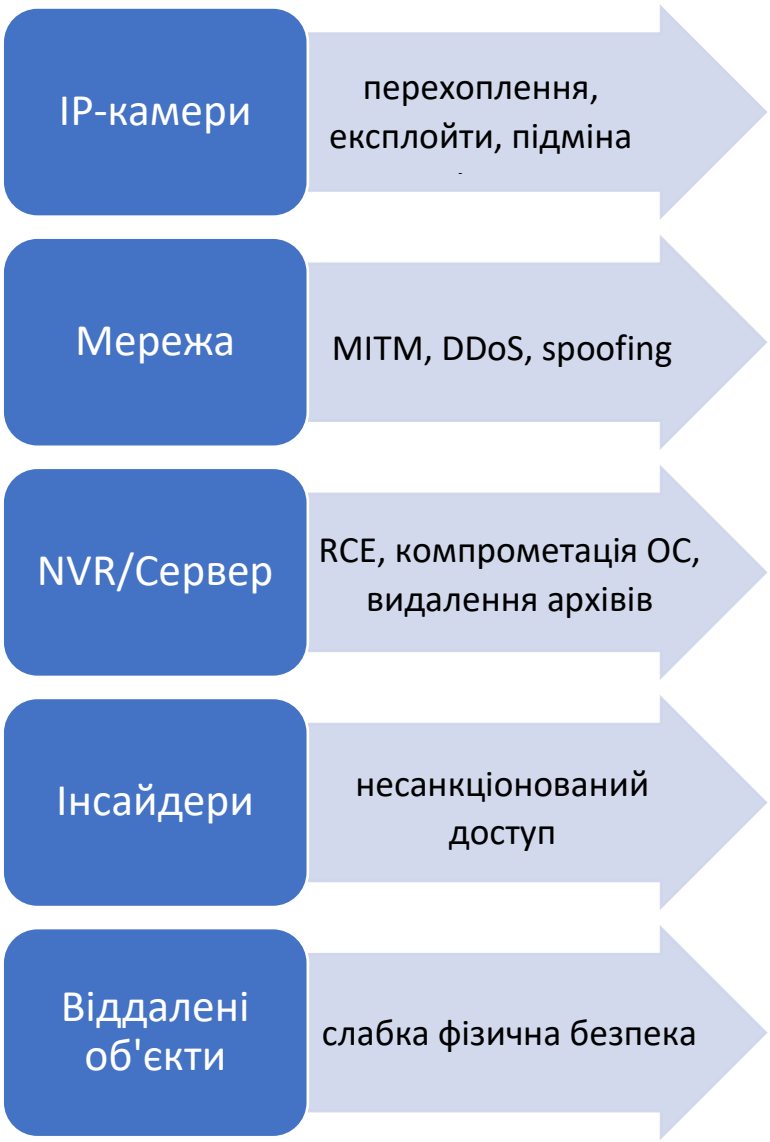

Рис. 2.1 – Формалізована модель загроз відеоінфраструктури банку

2.2 Побудова моделі доступу в межах Zero Trust з урахуванням принципів мінімальної довіри та сегментації

Побудова моделі доступу для відеоінфраструктури банку на основі концепції нульової довіри передбачає відхід від традиційної периметрової моделі та перехід до індивідуального контролю кожної взаємодії між пристроями, користувачами та сервісами. У межах Zero Trust не існує поняття «безпечної внутрішньої мережі», а кожен елемент системи повинен пройти автентифікацію, авторизацію та перевірку контексту запиту незалежно від свого фізичного або логічного розташування [4], [5]. Для відеоінфраструктури, яка включає великі масиви різнорідних пристроїв (IP-камери,

відеореєстратори, сервісні вузли, аналітичні модулі), застосування моделі мінімальної довіри та сегментування є ключовим фактором підвищення загальної стійкості системи [10], [15].

Згідно з рекомендаціями NIST та ENISA, формування моделі доступу має ґрунтуватися на атрибутивному принципі, де рішення про надання доступу залежить від сукупності параметрів, таких як тип пристрою, рівень його безпеки, роль користувача, політики банку та контекст запиту [4], [7]. Це дозволяє ізолювати функції відеоспостереження від інших компонентів банківської інформаційної системи, зменшуючи ризики горизонтального переміщення атакувальника. Модель описана в табл. 2.1.

Для систем відеоспостереження особливо важливо забезпечити сегментацію мережі таким чином, щоб камери, сервери архівації та системи управління відео працювали у відокремлених сегментах із мінімально необхідною кількістю дозволених комунікацій. Такий підхід відповідає принципам Zero Trust, де комунікація дозволяється лише після підтвердження легітимності кожного елемента. У наукових роботах підкреслюється, що мікросегментація значно знижує вплив потенційної компрометації однієї камери або вузла на всю систему, оскільки порушник не може вільно пересуватися мережею [11], [16].

Щоб забезпечити формальний підхід до моделювання доступу, доцільно описати всі сутності, які взаємодіють у системі. Нехай множина U представляє користувачів (адміністраторів, операторів, технічних спеціалістів), множина D — пристрої (камери, відеореєстратори, сервери), множина S — сервіси (VMS, модулі аналітики, системи зберігання), а множина P містить політики доступу, що регулюють дозволені дії. Під час кожного звернення до ресурсу система виконує перевірку відповідності пари суб’єкт–дія правилам із P, доповнюючи її аналізом контексту: рівня ризику, типу комунікаційного каналу, безпекового статусу вузла та результатів попередніх перевірок [5], [9].

Таблиця 2.1 – Атрибутивна модель прийняття рішень у межах Zero Trust для відеосистеми

Елемент рішення	Опис
Ідентифікація суб'єкта	Встановлення унікальної цифрової ідентичності користувача, сервісу або пристрою
Перевірка цілісності вузла	Аналіз прошивки, конфігурацій та відповідності стандартам безпеки перед наданням доступу
Оцінювання контексту сесії	Час, географія, зона мережі, стан з'єднання, тип запиту
Мінімізація привілеїв	Надання доступу лише до тих функцій, що необхідні для ролі суб'єкта
Мікросегментація	Логічний поділ мережі на ізольовані зони з мінімальними правилами комунікації
Аудит та поведінковий контроль	Безперервний запис дій та виявлення аномалій

Атрибутивна модель дозволяє усунути статичні правила доступу, характерні для традиційних систем безпеки, і замінити їх динамічними, контекстно-чутливими механізмами. Це особливо важливо для роботи операторів і технічного персоналу, доступ яких повинен бути обмежений конкретними функціями і часом, необхідними для виконання службових завдань.

Представлення моделі доступу було описано на рис. 2.2, де структуру Zero Trust подано у вигляді логічної схеми, що описує взаємодію користувача або пристрою із системою у момент звернення до ресурсу.

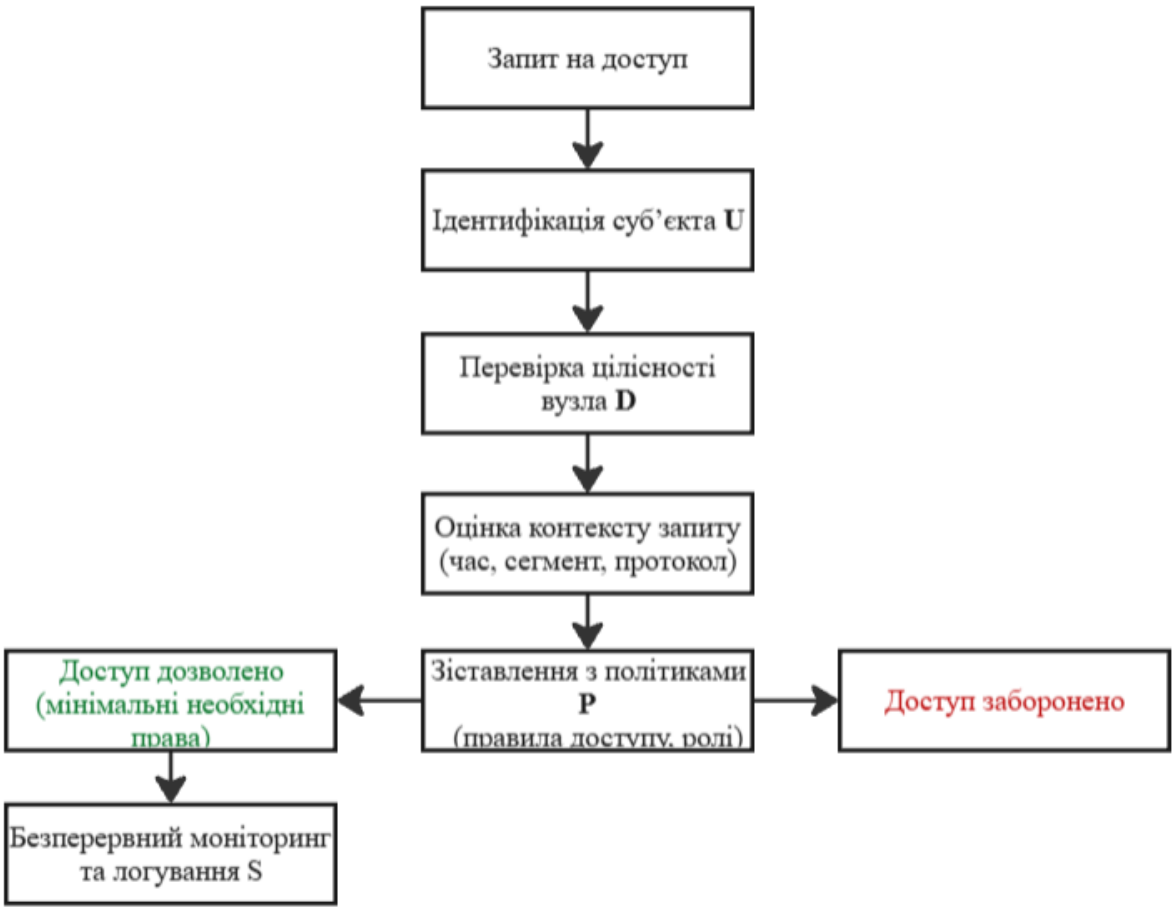

Рис. 2.2 – Узагальнена модель доступу Zero Trust у відеоінфраструктурі банку

2.3 Архітектурна схема багаторівневої системи відеоспостереження

Багаторівнева система відеоспостереження банку, побудована на засадах нульової довіри, повинна розглядатися як складна кіберфізична система, у якій кожен рівень має власні функції, загрози та засоби захисту. Її архітектура формується за принципами мікросегментації, мінімальної довіри та повного посередництва, що забезпечує ізоляцію компонентів та контроль усіх взаємодій між ними.

У загальному вигляді багаторівнева архітектура може бути поділена на такі логічні рівні:

- фізичний рівень середовища;
- рівень пристроїв відеоспостереження; мережевий рівень;
- рівень сервісів відео;

- рівень керування безпекою та Zero Trust;
- інтеграційний рівень взаємодії з іншими інформаційними системами банку.

На фізичному рівні середовища розташовуються відділення банку, сховища цінностей, зали для обслуговування клієнтів, банкоматні зони, інкасаційні вузли та серверні приміщення. Для цього рівня важливими є фізичний захист обладнання, контроль доступу до приміщень, використання сейфових дверей, турнікетів та систем контролю і управління доступом. Від надійності фізичного рівня залежить стійкість усієї системи, оскільки прямий фізичний доступ до камер чи мережевого обладнання може призвести до обходу логічних засобів захисту.

Рівень пристроїв відеоспостереження включає IP-камери різних типів (стаціонарні, поворотні, купольні, спеціалізовані камери для банкоматів), а також допоміжні сенсори. Кожна камера розглядається як окремий мережевий вузол з унікальною ідентичністю та криптографічними обліковими даними. Відповідно до концепції нульової довіри, цей рівень не має внутрішньої довіри: кожен запит від камери до сервера відеозапису, як і кожна операція отримання конфігурації, проходить через PEP та PDP.

Мережевий рівень включає комутатори, маршрутизатори, міжмережеві екрани, VPN-шлюзи та програмно визначену мережеву інфраструктуру (SDN), що дозволяє реалізувати політики мікросегментації та програмно визначених периметрів (SDP). На цьому рівні створюються окремі VLAN/VRF-сегменти для камер, відеосерверів, аналітичних модулів і адміністративних станцій. Між сегментами встановлюються логічні PEP-вузли, які застосовують політики доступу до трафіку ідентифікованих суб’єктів. Роботи Cloud Security Alliance та NIST наголошують, що використання SDP/SDN-підходів є одним із ключових механізмів реалізації Zero Trust у мережевої частині архітектури.

Рівень сервісів відео містить мережеві відеореєстратори (NVR), медіасервери, сховища архівів (SAN/NAS), модулі відеоаналітики (розпізнавання облич, виявлення аномальної поведінки), служби експорту

відео для служб безпеки та комплаєнсу. Кожен із цих сервісів розглядається як окремий ресурс у моделі Zero Trust, захищений PEP та описаний відповідними політиками доступу. Наприклад, архів відеоданих із приміщення сховища може бути доступний лише обмеженій групі співробітників підрозділів безпеки та комплаєнсу, тоді як оператор зони обслуговування клієнтів має право доступу лише до камер залу та банкоматної зони.

Рівень керування безпекою та Zero Trust об’єднує компоненти PDP/PE, PA, системи управління ідентичностями (IAM), внутрішню інфраструктуру відкритих ключів (PKI), системи журналювання та аналізу подій (SIEM, UEBA). На цьому рівні формуються політики доступу, реалізується оцінка ризиків, приймаються рішення щодо авторизації, а також виконується кореляція подій для виявлення аномальної поведінки. Наукові дослідження показують, що саме цей рівень є визначальним для перетворення традиційної системи відеоспостереження у Zero Trust-орієнтовану інфраструктуру.

На рис. 2.3 зображено формалізовану модель багаторівневой моделі.

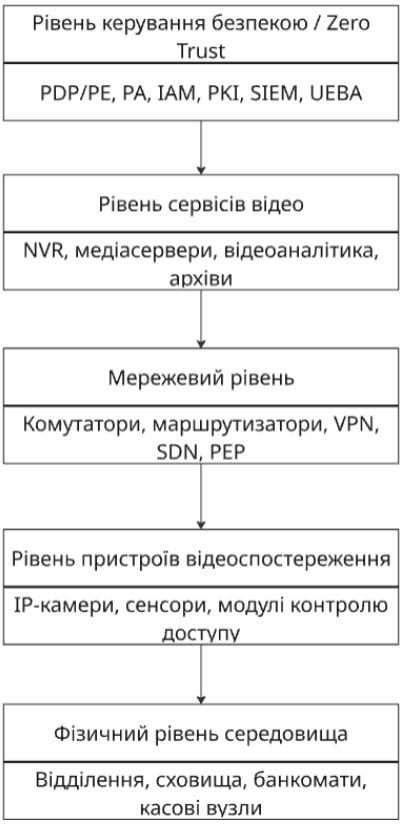

Рис. 2.3 – Багаторівнева архітектура системи відеоспостереження банку

2.4 Дослідження пов’язаних криптографічних механізмів та протоколів автентифікації

Реалізація системи відеоспостереження банку на засадах нульової довіри передбачає, що жоден компонент інфраструктури — незалежно від його місцеположення або попереднього статусу — не може бути допущений до обміну даними без попередньої перевірки автентичності та без встановлення захищеного криптографічного каналу. Згідно з рекомендаціями ISO/IEC та NIST, захист відеоданих у середовищі критичної фінансової інфраструктури має базуватися на сучасних криптографічних протоколах, які забезпечують конфіденційність, цілісність, стійкість до перехоплення й захист від модифікації інформації [1], [4], [5].

У межах архітектури Zero Trust для відеосистем ключове значення мають два взаємопов’язані процеси: побудова захищених каналів передавання даних та автентифікація суб’єктів і пристроїв, що взаємодіють із системою. Для захисту потокового відео використовується комплекс протоколів, серед яких центральне місце займають TLS 1.3, DTLS, SRTP та IPsec. У міжнародних дослідженнях зазначається, що TLS 1.3 є рекомендованим стандартом для критичних систем, оскільки мінімізує часові затримки на етапі встановлення з’єднання та виключає застарілі криптографічні механізми, відомі своїми вразливостями [4]. Це дозволяє захищати комунікації між відеокамерами, мережевими шлюзами та серверами запису від перехоплення та модифікації.

Для систем відеоспостереження особливе значення має криптографічний захист архівів та метаданих. У наукових роботах з медіафорензіки наголошується, що відео може бути змінено непомітно для оператора, тому всі архіви повинні зберігатися у зашифрованому вигляді із застосуванням механізмів цифрового підпису або контрольних хешів [12]. Це гарантує можливість підтвердження автентичності відеоматеріалів під час розслідувань або судових процесів.

Для передавання відеопотоків у режимі реального часу рекомендовано використовувати SRTP у поєднанні з DTLS, що забезпечує захист як

заголовків, так і корисного навантаження медіапотоку. Як зазначено в роботах IEEE, поєднання DTLS-SRTP вважається оптимальним для сенсорних і відеопристроїв, оскільки воно дає змогу зменшити кількість обчислювальних операцій і водночас гарантує цілісність та автентичність даних [10], [14]. Для систем відеоспостереження банку це особливо важливо, оскільки такі системи часто включають десятки або сотні камер з обмеженими ресурсами. Приклади механізмів захисту потокових відео описано в табл. 2.2.

На мережевому рівні доцільно використовувати IPsec у режимі тунелювання для захисту міжфілійних з'єднань або віддалених вузлів, де відеоканали можуть передаватися через незахищені сегменти мережі. Рекомендації NIST підкреслюють, що IPsec забезпечує необхідну криптографічну стійкість для передавання великих масивів відеоданих, а також підтримує взаємну автентифікацію між кінцевими вузлами [6]. Це створює підґрунтя для багаторівневого захисту, що охоплює весь шлях передавання відео — від камери до місця зберігання або аналітичного сервісу. Приклади механізмів захисту архівів та метаданих наведено у табл. 2.3.

Таблиця 2.2 – Криптографічні механізми захисту потокового відео

Механізм	Протокол	Ключові параметри	Призначення
Захист керуючого трафіку	TLS 1.3	AES-256-GCM або ChaCha20-Poly1305; обов'язкове PFS; мінімізація handshake	Захист конфігурацій, команд управління, API-трафіку

Продовження таблиці 2.2

Захист потокового відео (RTP)	SRTP	AES-128/256-GCM; HMAC-SHA-256; re-keying кожні 1–5 хв	Конфіденційність і цілісність відеопотоку
Захист потокового відео з handshake	DTLS-SRTP	DTLS для обміну ключами; SRTP для шифрування	Захист відео між камерами та VMS у реальному часі
Захист міжфілійних каналів	IPsec	IKEv2; AES-256-GCM; DH Group 14/19; tunnel mode	Захист передачі між віддаленими філіями банку

Таблиця 2.3 – Криптографічний захист архівів і метаданих

Об’єкт захисту	Механізм	Алгоритми / параметри	Призначення
Архіви відеозаписів (файли)	Повнодискове шифрування	AES-256-XTS	Захист від фізичного доступу, викрадення дисків
Відеофрагменти	Хешування	SHA-256 або SHA-3-256	Контроль цілісності, виявлення підміни
Юридично значущі записи	Цифровий підпис	ECDSA P-256	Підтвердження достовірності відео

Продовження таблиці 2.3

Ключі архівів	HSM/PKCS#11	Генерація й зберігання ключів у захищеному модулі	Неможливість вилучення ключа

Другий важливий напрям дослідження — це механізми автентифікації користувачів, сервісів і пристроїв, які взаємодіють із відеоінфраструктурою. У Zero Trust автентифікація є не одноразовою операцією, а безперервним процесом, що повторюється при кожному зверненні до ресурсу. На міжнародному рівні основою таких механізмів виступає інфраструктура відкритих ключів (PKI), що забезпечує створення та управління криптографічними сертифікатами, перевірку їх дійсності, а також використання довірених центрів сертифікації [1], [5]. Для відеопристроїв банку це означає, що кожна камера, відеосервер та аналітичний модуль мають унікальний сертифікат пристрою, який використовується для встановлення довірених каналів.

У межах PKI-інфраструктури застосовуються механізми OCSP та CRL для перевірки статусу сертифікатів, що дозволяє відстежувати компрометовані або відкликані ключі. Рекомендації ENISA наголошують на необхідності регулярного оновлення криптографічних сертифікатів, оскільки застарілі ключі є одним із найпоширеніших векторів атаки на критичні системи [7], [8]. Детальніше про механізми автентифікації у табл. 2.4.

Таблиця 2.4 – Автентифікація пристроїв у моделі Zero Trust

Компонент	Механізм	Параметри	Мета
Ідентичність пристрою	Сертифікат X.509	RSA-3072 або ECDSA-P256; окрема пари ключів	Унікальність кожної камери/серверу

Продовження таблиці 2.4

Перевірка сертифікатів	OCSP / CRL	Перевірка статусу в реальному часі; короткий TTL	Виявлення скомпрометованих пристроїв
Прив’язка сертифіката	Hardware Binding	TPM/SoC ID; MAC; серійний номер	Захист від підміни пристрою
Взаємна автентифікація	mTLS/DTLS	Client+Server certificates	Встановлення захищеного каналу

У системах, де взаємодія здійснюється не лише між пристроями, але й між користувачами та адміністративними сервісами, доцільно використовувати протоколи автентифікації на основі сертифікатів, такі як EAP-TLS, Kerberos або FIDO2. Протокол Kerberos, який досліджувався у контексті захисту розподілених систем, забезпечує взаємну автентифікацію між суб’єктами та ресурсами, а також захист від атак повторного відтворення [11], [18]. Протоколи EAP-TLS і FIDO2 є актуальними для банківського сектору, оскільки підтримують багатофакторну автентифікацію, що різко знижує ризики інсайдерських атак, описаних у роботах з безпеки фінансових систем [17]. Більше інформації про автентифікацію користувачів у табл. 2.5.

Таблиця 2.5 – Автентифікація користувачів

Тип суб’єкта	Механізм автентифікації	Параметри	Особливості
Адміністратори	SmartCard / FIDO2	PKCS#11; криптографічні токени	Багатофакторна автентифікація

Продовження таблиці 2.5

Оператори VMS	Kerberos v5	Взаємна автентифікація; захист від replay	Використання у доменних середовищах
Технічний персонал	EAP-TLS	Сертифікат користувача; TLS-тунель	Найвищий рівень захисту
Аналітичні сервіси	Сертифікат-клієнт + OAuth	API токени з коротким TTL	Контекстна авторизація

Окремий клас механізмів становлять протоколи авторизації, що визначають межі доступу суб'єкта після успішного проходження автентифікації. Серед них ключову роль відіграють протоколи OAuth 2.0 та OpenID Connect, які дозволяють створювати гнучкі політики доступу на основі ролей та контексту. У межах Zero Trust вони застосовуються як компоненти PDP/PEP-архітектури, забезпечуючи передачу мінімально необхідного набору повноважень відповідно до принципу least privilege [5], [9]. Детальніше у табл. 2.6.

Таблиця 2.6 – Авторизація та контроль доступу

Елемент	Механізм	Параметри	Призначення
Авторизація користувача	OAuth 2.0	Access Token TTL 5–15 хв; Scope-обмеження	Контроль доступу до VMS/API
Авторизація пристрою	mTLS Policy Binding	Сертифікат пристрою + політика PDP	Доступ камери лише до свого сегмента
Контекстний контроль доступу	PDP/PEP	Role + Location + Risk Score	Доступ залежить від умов запиту

Продовження таблиці 2.6

Принцип мінімальних прав	Least Privilege	Обмеження API/архівних функцій	Зниження ризику інсайдерських атак

Насамкінець, сучасні дослідження підкреслюють, що криптографічні механізми та автентифікація мають працювати як єдина система, тісно інтегрована з Zero Trust-рівнем керування політиками. Вони не можуть розглядатися окремо від рішення PDP/PEP, моніторингу подій або процесів оцінювання ризиків, оскільки їхня ефективність залежить від здатності системи перевіряти достовірність кожного запиту у режимі реального часу [15], [19], [20]. У такій архітектурі криптографія стає ключовим механізмом формування довіри, а автентифікація — основою безпечної взаємодії між усіма елементами відеоінфраструктури банку. Більше у табл. 2.7.

Таблиця 2.7 Інтеграція криптографії у Zero Trust-рівні

Zero Trust компонент	Криптографічний механізм	Реалізація	Значення
PEP (Policy Enforcement Point)	TLS 1.3, DTLS, mTLS	Захист трафіку між суб’єктом і ресурсом	Гарантування, що доступ здійснює автентичний суб’єкт
PDP (Policy Decision Point)	Підписані політики	Цифровий підпис конфігурацій	Недопущення підміни правил доступу
PA (Policy Administrator)	PKI, OCSP	Управління ключами та політиками	Контроль життєвого циклу довіри
IAM	FIDO2, Kerberos, EAP-TLS	Централізована автентифікація	Встановлення особи суб’єкта

Продовження таблиці 2.7

SIEM/UEBA	Хеш-ланцюги, підписи логів	Криптографічна цілісність журналів	Виявлення аномалій і атак

2.5 Оцінювання ризиків та критеріїв ефективності запропонованої моделі

Оцінювання ризиків у системі відеоспостереження банку, побудованій на принципах нульової довіри, передбачає систематичний аналіз загроз, уразливостей та потенційних наслідків інцидентів з урахуванням того, що жоден компонент інфраструктури не може вважатися достовірним без криптографічного та контекстного підтвердження. Відповідно до підходів, викладених у стандартах ISO/IEC 27005, NIST SP 800-30 та ENISA Risk Framework, процес оцінювання ризиків повинен інтегрувати методи кількісного та якісного аналізу, враховуючи специфіку банківського сектора, критичність відеоданих і вимоги регуляторів щодо їх збереження та достовірності [1], [4], [7].

2.5.1 Визначення категорій ризиків відеоінфраструктури в контексті Zero Trust

У межах запропонованої моделі відеоінфраструктура банку розглядається як неоднорідна система, у якій ризики розподіляються за п’ятьма основними категоріями: ризики цілісності, конфіденційності, доступності, автентичності та операційної сумісності елементів системи.

Ризики порушення конфіденційності

До цієї групи належать інциденти, пов’язані з перехопленням потоків відео, доступом до архівів або витоком управлінських даних. Дослідження IEEE та рекомендації NIST підкреслюють, що основними джерелами таких ризиків є незахищені медіапотоки, компрометовані пристрої та відсутність криптографічної автентифікації вузлів [10], [14]. У моделі Zero Trust ці ризики

знижуються завдяки застосуванню TLS 1.3, SRTP, IPsec та механізмів взаємної автентифікації.

Ризики порушення цілісності відеоданих

До ключових ризиків входить підміна відео, модифікація окремих кадрів, втручання у часові мітки та маніпуляція блоками архіву. Наукові роботи з медіафорензіки підкреслюють, що навіть незначна зміна відеоряду може бути непомітною візуально, проте суттєво впливає на юридичну валідність доказів [12]. У запропонованій моделі ці ризики мінімізуються через криптографічні підписи, хеш-ланцюги та контроль цілісності на кожному етапі оброблення.

Ризики втрати доступності

У системах відеоспостереження банку відмова компонентів, DoS/DDoS-атаки або порушення роботи мережевих сегментів можуть спричинити втрату критично важливих даних. За оцінками досліджень Springer і ENISA, недоступність відеоархівів у фінансовому секторі має високий рівень впливу, оскільки відеодані використовуються у внутрішніх розслідуваннях, комплаєнсі та юридичних процесах [11], [17]. У Zero Trust-моделі доступність забезпечується через сегментацію, резервування каналів, криптографічний захист міжфілійних з’єднань і контроль навантаження.

Ризики автентичності суб’єктів і пристроїв

Відсутність достовірної ідентифікації пристроїв або користувачів створює умови для інсайдерських атак, несанкціонованого перегляду архівів, ін’єкції шкідливого відео або використання підроблених камер. NIST і ENISA вказують, що це один із найбільш критичних класів ризиків у фінансових системах [5], [7]. У Zero Trust ці ризики знижуються через PKI, взаємну автентифікацію, докази присутності ключа у TPM та перевірку сертифікатів у режимі OCSP.

Ризики сумісності та операційної взаємодії

Ці ризики виникають у разі конфлікту між політиками доступу, некоректної інтеграції PEP/PDP, неузгоджених криптографічних параметрів

або помилок конфігурацій. У роботах Cloud Security Alliance наголошено, що Zero Trust-архітектури чутливі до неправильного налаштування, оскільки політики доступу повинні бути повністю формалізовані та узгоджені [15].

2.5.2 Методологія оцінювання ризиків у запропонованій моделі

Застосована модель оцінювання ризиків ґрунтується на поєднанні:

- якісного аналізу загроз (аналіз атак, сценарії порушень, модель порушника);
- кількісних методів (імовірність × вплив);
- контекстної оцінки ризику, відповідно до принципів Zero Trust.

Математична модель ризику

Для формального опису ризику використовується рівняння:

$$R = P \times I \times C \qquad (2.1)$$

де:

P — імовірність реалізації загрози;

I — інтенсивність або масштаб впливу на систему;

C — коригувальний коефіцієнт Zero Trust-контролів ($0 < C \leq 1$), що враховує ступінь захищеності елемента.

У традиційних відеосистемах $C \approx 1$, тоді як у Zero Trust:

- для сегментованих вузлів $C \approx 0.5$,
- для криптографічно автентифікованих каналів $C \approx 0.3$,
- для елементів із апаратними сертифікатами та TPM $C \approx 0.1$.

Це демонструє здатність моделі нульової довіри знижувати ризик на порядок.

2.5.3 Критерії оцінювання ефективності Zero Trust-моделі

Критерій 1 — Здатність зменшувати поверхню атаки

Ефективна Zero Trust-архітектура мінімізує кількість дозволених комунікацій між компонентами. Показником є частка необхідних маршрутів у мережі:

$$E_1 = \frac{N_{\text{дозв}}}{N_{\text{пот}}} \to min \qquad (2.2)$$

де:

Ndозв — кількість дозволених зв’язків;

Nпот — усі можливі зв’язки.

За даними ENISA, мікросегментація може зменшити цей показник у 10–20 разів [7].

Критерій 2 — Стійкість криптографічних каналів

Ефективність оцінюється за:

- довжиною ключів;
- стійкістю до квантових атак;
- відсутністю застарілих алгоритмів;
- частотою оновлення ключів.

За NIST найкращими вважаються:

- AES-256-GCM;
- ChaCha20-Poly1305;
- ECDSA P-256;
- SHA-3-256.

Критерій 3 — Час реакції системи на спробу несанкціонованого доступу

PDP повинен приймати рішення з мінімальною затримкою:

$$E_3 = t_{\text{PDP}} + t_{\text{PEP}} \leq 50\text{–}120 \text{ мс} \qquad (2.3)$$

Для відеосистем це критично, оскільки камера не повинна працювати без дозволу.

Критерій 4 — Виявлення інцидентів у режимі реального часу

Ефективність вимірюється як відсоток атак, виявлених системами SIEM/UEBA:

$$E_4 = \frac{A_{\text{вияв}}}{A_{\text{усього}}} \times 100\% \qquad (2.4)$$

У роботах Springer і IEEE зазначено, що інтеграція криптографічних логів і аналітики знижує невиявлені інциденти у 2–3 рази [11], [12].

Критерій 5 — Цілісність відеоданих

Перевіряється через:

- збіжність хеш-ланцюгів;
- відсутність невідповідностей часових міток;
- перевірку цифрових підписів.

Система вважається ефективною, якщо:

$$E_5 = 0 \text{ виявлених модифікацій архівів}$$

Порівняння ризиків у традиційній та Zero Trust-архітектурі описано в табл. 2.8

Таблиця 2.8 – Узагальнений результат аналізу

Тип ризику	Традиційна модель	Zero Trust
Конфіденційність	Високий	Низький
Цілісність	Середній–високий	Дуже низький
Доступність	Середній	Низький
Автентичність	Високий	Дуже низький
Інсайдерські атаки	Високий	Середній–низький
Масштабування ризику	Дуже високе	Низьке через сегментацію

Висновки за розділом 2

У другому розділі було описано архітектурну модель системи відеоспостереження банку, побудовану відповідно до принципів нульової довіри. Це дозволило сформувати цілісне розуміння того, як мають взаємодіяти всі елементи відеоінфраструктури в умовах підвищених вимог до безпеки. На основі проведеної оцінки ризиків та типових вразливостей відеомереж визначено ключові компоненти, що потребують посиленого захисту: IP-камери, відеосервери, мережеві сегменти, канали передавання даних, системи архівування та модулі відеоаналітики.

Запропонована модель Zero Trust ґрунтується на принципах відсутності попередньої довіри, обов’язкової верифікації кожної взаємодії та гнучкого управління доступом. Особлива увага приділяється механізмам мікросегментації мережі, криптографічному захисту відеопотоків, автентифікації користувачів і пристроїв, контролю привілеїв та безперервному моніторингу стану інфраструктури. Було сформовано логічну структуру основних компонентів Zero Trust — Policy Engine (PE), Policy Decision Point (PDP), Policy Enforcement Point (PEP) та Policy Administrator (PA). Разом вони забезпечують повний цикл роботи політик доступу: від їхнього створення до прийняття рішень і примусового застосування.

Окремим елементом архітектури стала модель інфраструктури відкритих ключів (PKI), яка використовується для видачі сертифікатів камерам, серверам і сервісам, а також для забезпечення взаємної автентифікації в межах системи. На основі аналізу сучасних протоколів безпеки визначено оптимальні засоби криптографічного захисту: DTLS-SRTP — для шифрування потокового відео, TLS 1.3 — для адміністративних та керуючих каналів, а також набір сучасних алгоритмів шифрування й хешування, що забезпечують високий рівень стійкості до атак.

У межах розділу також створено детальні архітектурні схеми, які відображають взаємодію між компонентами системи, процеси контролю доступу до відеоархівів та механізми сегментації мережі (video-net, archive-net, gateway-net, audit-net, analytics-net). Таке проектування мінімізує ризики горизонтального переміщення атакувальника, унеможливлює доступ до камер без авторизації, гарантує цілісність відеоданих та забезпечує централізований аудит безпекових подій.

Отже, у другому розділі було сформовано комплексну архітектуру банківської системи відеоспостереження на основі методології Zero Trust, визначено її функціональні та захисні вимоги і розроблено організаційно-технічні рішення, що підвищують її стійкість до сучасних кіберзагроз.

Отримані результати слугують підґрунтям для подальшого моделювання, реалізації та тестування системи, що будуть виконані у наступному розділі.

3 ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ БАНКУ НА ОСНОВІ МЕТОДОЛОГІЇ НУЛЬОВОЇ ДОВІРИ

3.1 Розроблення архітектури прикладного рішення

Архітектура прикладного рішення створюється у вигляді ізольованого контейнерного середовища Docker, яке дозволяє відтворити всі логічні рівні системи відеоспостереження банку та сформувати мікросегментовану мережу відповідно до принципів Zero Trust. Практична реалізація ґрунтується на структурі, у якій кожен компонент системи — відеосервер, PEP, PDP, AI-аналітика, архів, журналювання та підсистема автентифікації — розгортається в окремому контейнері та працює в окремому сегменті мережі Docker.

Архітектурна модель стенду

Практичний стенд побудовано таким чином, щоб відтворити повний цикл роботи системи відеоспостереження:

- Емуляція IP-камер → передача потокового відео у сегмент відеосервера.
- Відеосервер (NVR-контейнер) → отримання SRTP-потоку, первинна обробка.
- PEP → контроль кожного запиту до відеоархіву та аналітики.
- PDP → централізоване прийняття рішень на основі політик доступу.
- PKI/IAM → видача сертифікатів, перевірка ключів, автентифікація сервісів.
- Архів (SAN-контейнер) → зашифроване зберігання відео.
- Аналітика (AI-контейнер) → оброблення дозволених потоків.
- SIEM/UEBA → збір та аналіз подій безпеки.

Для кращого розуміння архітектури, схему було описано на рис. 3.1.

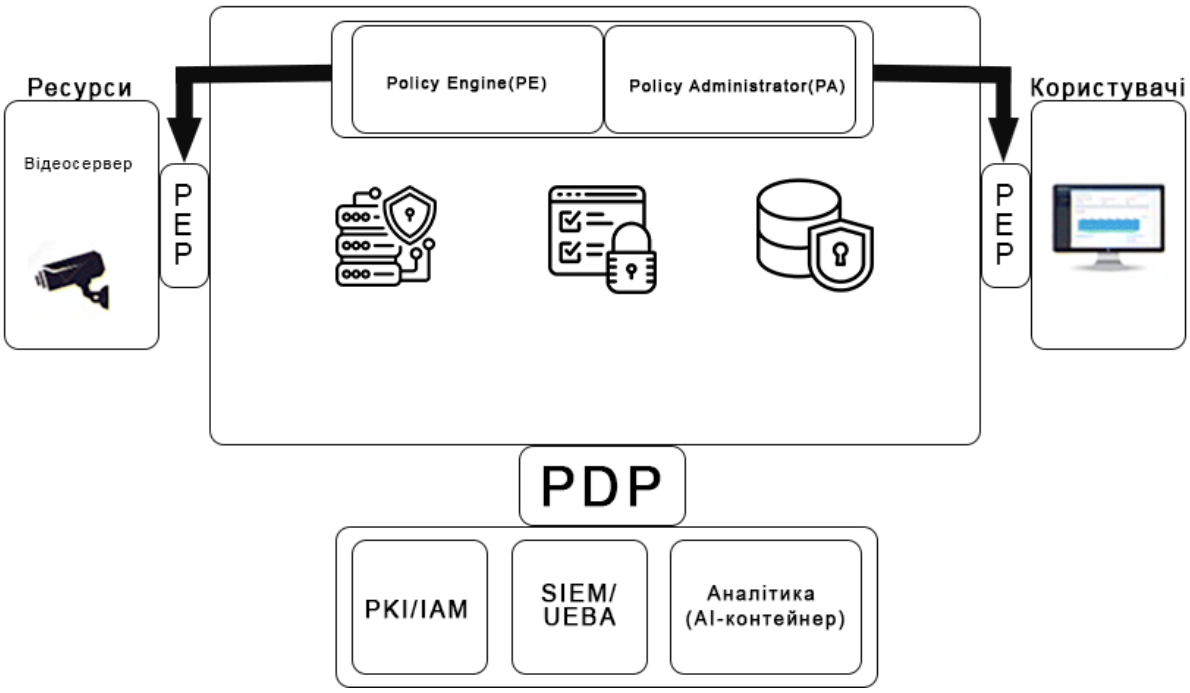

Рис. 3.1 - Логічна схема архітектури

Щоб продемонструвати роботу Zero Trust, кожен контейнер отримує:

- окрему мережу або підмережу;
- власний сертифікат X.509;
- обмежений набір маршрутів;
- mTLS для комунікацій;
- політику доступу, що визначається PDP.

3.1.1 Архітектурне представлення Docker-мереж

Практична архітектура складається з п’яти основних сегментів:

video-net

Мережа для потокового відео від камер до відеосервера. У цьому сегменті працюють:

- *camera-emulator-1*
- *camera-emulator-2*
- *video-gateway*
- *nvr-core*

Всі потоки передаються через SRTP + DTLS, а video-gateway виконує роль PEP для потокового трафіку.

zt-control-net

Сегмент Zero Trust-контролю.

Сюди входять:

- *pdp (Policy Decision Point)*
- *pep-auth (PEP для доступу до архівів та API)*
- *pki-root (внутрішній CA)*
- *iam-core*

Тут формуються й застосовуються політики доступу, перевіряються сертифікати та ведеться журнал аудиту доступів.

archive-net

Сегмент зашифрованого архіву.

У цій мережі працюють:

- *archive-storage (зашифрований том AES-256-XTS)*
- *hashing-service (контроль хеш-ланцюгів відео)*
- *signing-service (цифровий підпис блоків архівів)*

Доступ сюди можливий лише після рішення PDP.

analytics-net

Сегмент аналітики:

- *ai-analyzer*
- *event-detector*
- *face-match-module*

Сюди потрапляють лише ті відеопотоки, які PDP дозволяє аналізувати.

audit-net

Сегмент журналювання та поведінкового аналізу:

- *siem-core*
- *ueba-engine*

Всі PEP передають туди події безпеки.

Представлення архітектури було описано на рис. 3.2.

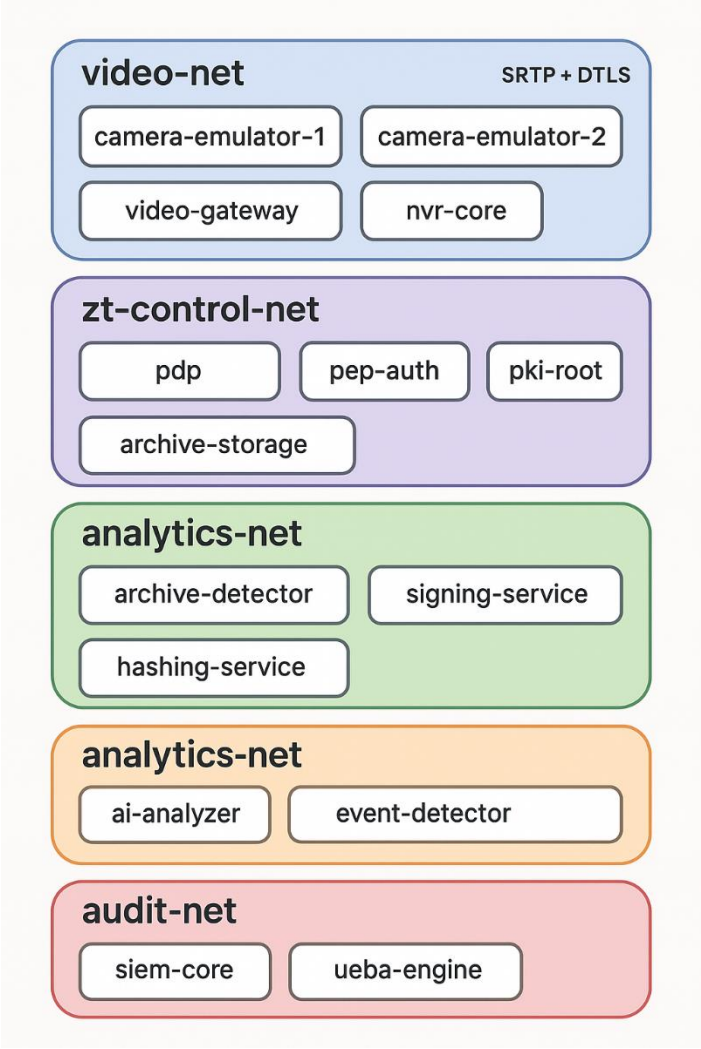

Рис. 3.2 - Схема docker-контейнерів

3.1.2 Опис docker-інфраструктури (архітектурний рівень)

У рамках практичної реалізації створено єдиний docker-compose-файл, який відтворює повну архітектуру системи. У додатках дипломної роботи цей файл подається повністю, а в самому тексті описуються лише його ключові структурні блоки.

Блок емуляторів відеокамер

У мережі *video-net* розгорнуто два контейнери, що моделюють роботу реальних IP-камер. Кожен контейнер:

- формує SRTP-потік зі стабільною частотою кадрів;
- ініціює DTLS-з’єднання для встановлення параметрів шифрування;
- отримує сертифікат X.509 від внутрішнього CA;

- має суворо обмежену маршрутизацію і не може ініціювати з’єднання поза межами *video-net*.

Таке моделювання дозволяє відтворити поведінку камер у банківських відділеннях, включно з вимогами до криптографічної автентифікації та ізоляції мереж.

Блок відеосервера

Другий ключовий елемент — це логічний вузол відеосервера, який складається з контейнерів *video-gateway* та *nvr-core*.

video-gateway виконує роль PEP для потокового трафіку.

Основні функції *video-gateway*:

- перевірка сертифікатів камер під час встановлення DTLS;
- фільтрація SRTP-пакетів відповідно до рішення PDP;
- автоматичне блокування трафіку від камер зі скомпрометованими або відкликаними ключами;
- передавання дозволених потоків у модуль запису.

nvr-core працює лише з тими потоками, які пройшли Zero Trust-контроль. Він відповідає за формування структурованих відеофайлів, маркування тимчасових міток та синхронізацію даних, що імітує поведінку справжнього банківського відеореєстратора.

Мережа Zero Trust-контролю (PDP, PEP, IAM, PKI)

У сегменті *zt-control-net* розміщено ключові компоненти архітектури адміністративного рівня.

PDP є центральним елементом логіки доступу. Він:

- аналізує атрибути користувачів та пристроїв;
- перевіряє криптографічний статус та дійсність сертифікатів;
- застосовує політики доступу, збережені у вигляді підписаних декларативних структур;
- формує остаточні рішення для PEP-компонентів.

pep-auth

pep-auth перехоплює всі прикладні та API-запити. Він:

- виконує mTLS-автентифікацію сервісів;
- звертається до PDP для отримання дозволу;
- журналює кожну дію у SIEM;
- виступає центральним шлюзом доступу до архіву та AI-модулів.

pki-root

pki-root забезпечує:

- видачу та ротацію сертифікатів;
- генерацію ключів;
- створення та оновлення списків відкликаних сертифікатів;
- OCSP-підтвердження для камер, AI-модулів і всіх контейнерів.

Без цього компонента Zero Trust неможливий, оскільки модель базується виключно на криптографічній автентифікації.

iam-core

iam-core керує ролями, групами користувачів та службовими атрибутами. Він надає PDP той набір даних, який дозволяє формувати політики доступу з урахуванням контексту, ролі й привілеїв суб’єкта.

Контейнери архіву (archive-net)

Сегмент *archive-net* створено для повністю ізольованого зберігання відеоархівів.

Основний контейнер *archive-storage* використовує зашифрований том, у якому дані зберігаються з використанням AES-256-XTS. Ніхто не має прямого доступу до цього контейнера, окрім тих, хто проходить через pep-auth та отримує дозвіл від PDP.

Поруч працює *hashing-service*, який будує хеш-ланцюги для кожного відеоблоку. Така структура дозволяє виявити будь-яку зміну або пошкодження фрагментів запису.

signing-service виконує цифровий підпис кожного файлу або його блоку. Підпис гарантує, що відеоматеріал може бути представлений як юридично значущий, а його цілісність можна підтвердити незалежним експертним способом.

Сегмент аналітики (analytics-net)

У мережі аналітичного сегмента працюють три окремі модулі, кожний з яких виконує власну функцію в процесі інтелектуальної обробки даних.

ai-analyzer відповідає за загальний аналіз кадрів і може виконувати виявлення руху, оцінку аномалій або роботу алгоритмів поведінки.

event-detector обробляє дані з позиції подієвої логіки, визначаючи підозрілі дії, нетипові патерни або вказівки на можливі інциденти.

face-match-module здійснює біометричну ідентифікацію, порівняння осіб, виявлення інсайдерів або повторюваних зловмисників.

Цей сегмент не має прямого доступу до архіву або камер. Доступ до кожного відеопотоку визначається PDP і надається лише у випадках, коли цього вимагає роль або контекст.

Контейнери *SIEM/UEBA*

Ці компоненти отримують всі події з PEP у режимі реального часу.

Сегмент журналювання та поведінкової аналітики (audit-net)

Останній сегмент — *audit-net* — виконує функції контролю та аналізу безпеки в реальному часі.

У ньому розміщено два компоненти:

- siem-core, який агрегує всі журнальні записи з PEP, PDP, IAM та аналітичних модулів. Він виконує кореляцію подій і виявляє потенційні аномалії.
- *ueba-engine*, який зосереджений на аналізі поведінки користувачів, пристроїв і контейнерів. Він застосовує поведінкові моделі та у разі виявлення підозрілої активності автоматично формує підвищений індикатор ризику, передаючи його до PDP.

Нижче, на рис. 3.3, представлено секвенс-діаграму проходження одного запиту крізь всі компоненти.

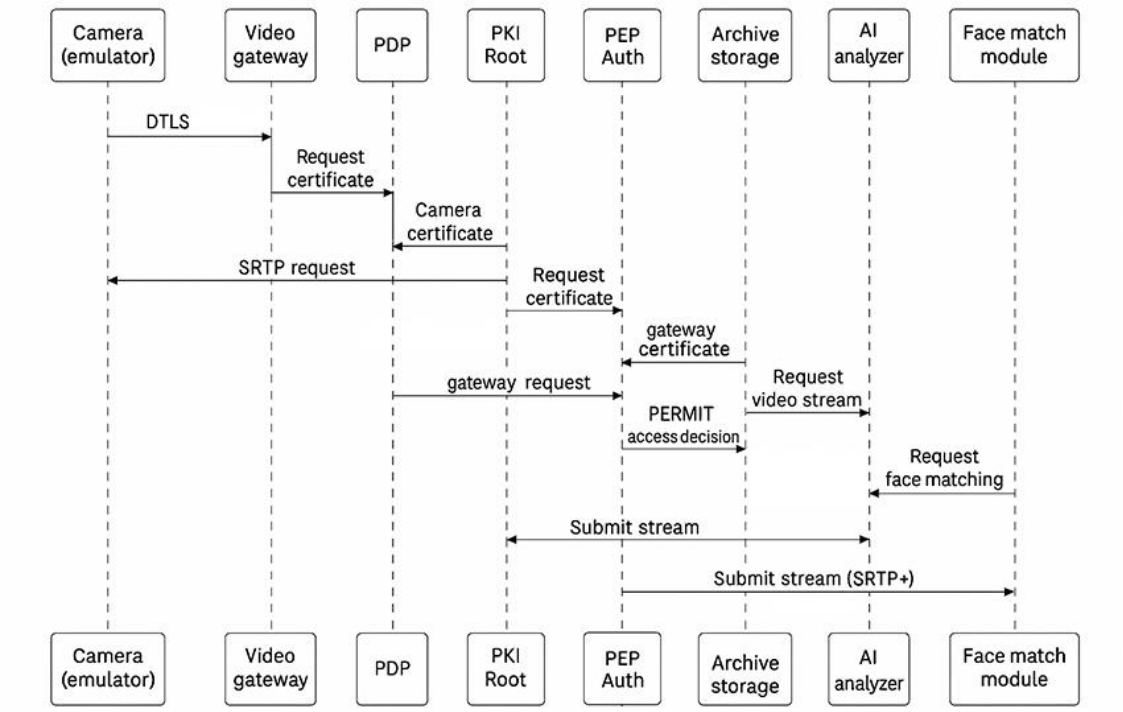

Рис. 3.3 - Секвенс-діаграма запиту

3.2 Інтеграція компонентів і механізмів контролю доступу

Інтеграція компонентів у розробленій системі відеоспостереження ґрунтується на принципах Zero Trust та передбачає не лише ізоляцію функціональних сегментів, але й забезпечення строгої перевірки кожної взаємодії між ними. На відміну від традиційних систем, де окремі модулі можуть взаємодіяти без додаткового контролю, запропонована архітектура передбачає, що жоден компонент не довіряє іншому за замовчуванням, навіть якщо вони належать одній мережевій зоні або розгорнуті всередині одного програмного контуру. Це забезпечується впровадженням послідовного ланцюга аутентифікації, авторизації та криптографічного захисту, який працює у вигляді єдиного інтегрованого механізму.

У моделі, побудованій на Docker-інфраструктурі, компоненти розгортаються як ізольовані контейнери, що спілкуються один з одним через спеціально визначені віртуальні мережеві сегменти. Це дозволяє реалізувати мікросегментацію, коли кожен сервіс має власну логічну зону відповідальності, а маршрути даних між зонами проходять через контрольні точки політик. Зокрема, камера-емулятори генерують SRTP-потоки у сегмент

video-net, які можуть бути передані далі лише через вузол *video-gateway*. Останній виконує роль PEP для потокового трафіку, перевіряючи сертифікати, цілісність каналів та відповідність правилам PDP перед тим, як дозволити передачу відео до NVR.

Центральною компонентою інтеграції є PDP, який забезпечує ухвалення рішень про доступ. PDP отримує від PEP маркери авторизації, перевіряє їх через IAM-сервіс, зчитує відповідні політики доступу з конфігураційного сховища та визначає, чи дозволено конкретну операцію. IAM-компонент, у свою чергу, реалізує управління користувачами та ролями, а також видачу JWT-токенів, що використовуються для автентифікації. Завдяки використанню контейнера IAM, система підтримує централізовану модель контролю доступу, де будь-яка взаємодія користувача з відеоархівом або аналітичними модулями проходить через перевірку токена та ролей.

Коли оператор або сервіс звертається до архіву, він надсилає запит до PEP (*pep-auth*), який перехоплює всі операції, пов’язані з читанням відеоданих. PEP не має власної логіки контролю доступу — він є точкою примусового виконання (Policy Enforcement Point), яка переспрямовує маркер доступу у PDP та очікує рішення. Якщо PDP повертає дозвіл, PEP надає доступ до ресурсу. Якщо рішення негативне — запит блокується, а подія фіксується у SIEM та передається у UEBA для оцінювання ризикової активності.

Усі модулі, що працюють з архівом — *archive-storage, hashing-service* та *signing-service* — отримують доступ до даних виключно через захищені томи Docker, кожен з яких має різний рівень дозволів (лише читання для деяких сервісів). Таке розмежування дозволяє виключити сценарій, коли зовнішній або скомпрометований сервіс може змінювати архів напряму. Hashing-service формує ланцюг контрольних сум, який підтверджує послідовність файлів та виявляє будь-які зміни у них. Signing-service накладає HMAC-підпис, що дозволяє перевірити незмінність усього ланцюга архівів. Ці процеси виконуються незалежно один від одного, але результати хешування та

підписування є доступними лише тим контейнерам, які PDP визначає як легітимні суб’єкти.

Аналітичні модулі — *ai-analyzer*, *event-detector*, *face-match-module* — отримують доступ до відеоданих виключно після дозволу PDP. PEP не передає їм жодних даних до моменту підтвердження авторизації, навіть якщо запит надходить із внутрішньої мережі аналітики. Це гарантує, що модель Zero Trust дотримується на всіх рівнях роботи з відеоданими: як під час потокового аналізу, так і під час доступу до архівних матеріалів. Такий розподіл забезпечує можливість локалізації компрометації кожного аналітичного модуля, адже доступ обмежений політиками, а усі їхні операції логуються у SIEM.

Важливою частиною інтеграції є контейнери SIEM та UEBA. SIEM отримує журнали подій від PEP, PDP, аналітичних модулів та PKI, після чого зберігає їх для аудиту. UEBA отримує поведінкові параметри взаємодії, відстежує аномалії у діях конкретних суб’єктів та повертає PDP оцінку ризику, яка може бути врахована у процесі авторизації. Таким чином, система отримує можливість адаптивного контролю доступу у реальному часі — рівень довіри суб’єкта може знижуватися у разі виявлення нетипової поведінки.

Узгоджена інтеграція всіх контейнерів дозволяє отримати цілісну Zero Trust-архітектуру, в якій кожен компонент виконує строго визначену функцію, взаємодіє виключно через контрольовані інтерфейси, проходить автентифікацію та авторизацію, а будь-яка операція з відеоданими супроводжується криптографічним захистом і журналюванням. Такий підхід забезпечує повну трасованість дій, мінімізацію можливостей для інсайдерських атак та високу стійкість системи до компрометації окремих модулів.

Було створено проект на основі мови програмування Python, де описано реальний підхід симуляції методології Zero Trust в системі відеоспостереження банку. Структуру проекту зображено на рис. 3.4.

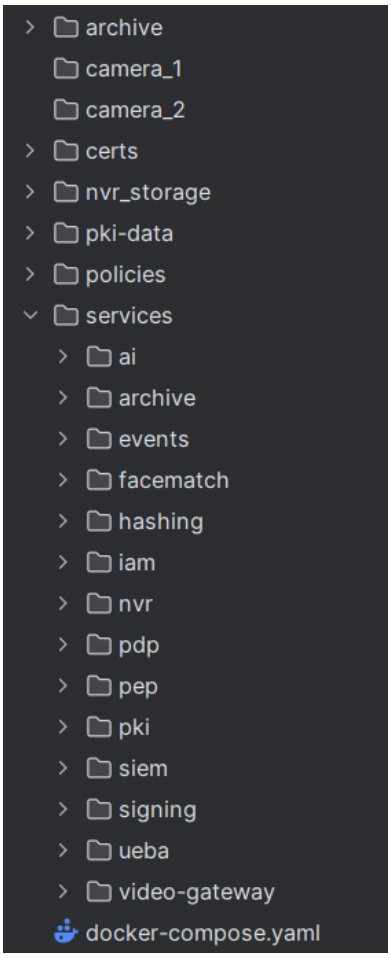

Рис. 3.4 – Структура проекту

3.3 Тестування системи: моделювання сценаріїв порушень безпеки

Практична перевірка функціональності розробленої системи відеоспостереження на основі Zero Trust була проведена шляхом моделювання різних типів подій: коректної роботи компонентів, несанкціонованих спроб доступу, порушення цілісності відеоданих, компрометації політик доступу, а також відхилення поведінки користувачів від нормативних шаблонів. Тестування здійснювалося безпосередньо на розгорнутій інфраструктурі Docker, що дозволяє відтворити реальні сценарії взаємодії між контейнерами та забезпечити повну ізоляцію мережевих сегментів.

У цьому підрозділі послідовно описано ключові експерименти, їх мету, команди для виконання, очікувану поведінку компонентів та отримані результати.

1) Перевірка коректності роботи NVR та генерації відеофайлів

Початковим кроком є моделювання появи нового відеофайлу у мережевому відеореєстраторі. Цей етап демонструє роботу NVR у контейнері *nvr-core*, який генерує псевдовідеопоток та записує його у спільний том *nvr_storage*.

Команда для створення відеофайлу:

```
curl.exe -X POST http://localhost:8090/generate
```

У результаті система повертає шлях до нового файлу, наприклад:

```
{"file":"/data/nvr/2024_cam1_20251202_165607.mp4","status":"created"}
```

Цей файл з’являється в директорії *nvr_storage* і стає доступним для наступних етапів — архівації, побудови хеш-ланцюга та підпису.

2) Тестування архівації відеоданих

Наступний крок демонструє, як відеофайл передається в сегмент зберігання архіву. Контейнер *archive-storage* копіює файл з тома NVR у захищений каталог */secure-archive/blocks*.

Команда для архівації:

```
curl.exe -X POST http://localhost:8091/ingest
  -H "Content-Type: application/json"
  -d
"{\"src\":\"/data/nvr/2024_cam1_20251202_165607.mp4\",\"name\":\"2024_cam
1_001.mp4\"}"
```

Очікувана відповідь містить новий шлях файлу:

```
{"dst":"/secure-archive/blocks/2024_cam1_001.mp4","status":"ingested"}
```

Це підтверджує, що архіватор отримує файл з NVR і переносить його в сегмент захищеного сховища.

3) Перевірка цілісності даних: побудова та валідація хеш-ланцюга

З метою забезпечення неможливості прихованої модифікації архівів було протестовано блок перевірки цілісності. Контейнер *hashing-service* формує послідовний хеш-ланцюг на основі SHA-256, подібний до блокчейну.

Команда побудови ланцюга:

```
curl.exe -X POST http://localhost:8092/rebuild-chain
```

Після цього:

```
curl.exe http://localhost:8092/verify-chain
```

Позитивний результат свідчить про те, що ні самі файли, ні порядок їхнього хешування не було змінено:

```
{"ok": true}
```

На цьому етапі підписів ще немає — лише дані хешування.

4) Перевірка автентичності архівів за допомогою цифрового підпису

Для гарантування того, що хеш-ланцюг сформований довіреною системою, тестується механізм цифрового підпису. Контейнер *signing-service* створює або завантажує секретний ключ, формує HMAC-SHA256 над *chain.json* і зберігає підпис у *chain.sig*.

Команда підпису:

```
curl.exe -X POST http://localhost:8093/sign-chain
```

Перевірка підпису:

```
curl.exe http://localhost:8093/verify-signature
```

Очікування:

```
{"ok": true}
```

Це підтверджує, що підпис відповідає існуючому хеш-ланцюгу.

5) Моделювання сценарію: несанкціонований доступ до архіву

Zero Trust передбачає, що жоден доступ не допускається без автентифікованого суб’єкта. Щоб перевірити це, виконується запит до PEP без токена:

```
curl.exe http://localhost:8081/archive/list
```

Очікувана відповідь:

```
{"error":"access denied by PDP"}
```

Таке рішення формується PDP, який отримує запит від PEP та передає його IAM для перевірки токена.

6) Перевірка автентифікації та авторизації через IAM

Для моделювання коректної автентифікації створюється користувач у IAM:

```
curl.exe -X POST http://localhost:8085/register -H "Content-Type: application/json" -d "{\"username\":\"op1\",\"password\":\"pass\"}"
```

Призначається роль:

```
curl.exe -X POST http://localhost:8085/assign-role ^
  -H "Content-Type: application/json" ^
  -d "{\"username\":\"op1\",\"role\":\"operator\"}"
```

Авторизація:

```
curl.exe -X POST http://localhost:8085/login ^
  -H "Content-Type: application/json" ^
  -d "{\"username\":\"op1\",\"password\":\"pass\"}"
```

IAM повертає JWT-токен.

7) 7. Перевірка дозволу доступу через PEP → PDP → IAM

Після отримання токена здійснюється повторний запит до архіву:

```
curl.exe http://localhost:8081/archive/list
  -H "Authorization: Bearer <TOKEN>"
```

У разі, якщо токен валідний і суб’єкт має роль, зазначену в політиці доступу:

```
{"files":["2024_cam1_001.mp4"]}
```

У цьому сценарії контейнери взаємодіють так:

1) PEP отримує запит.
2) PEP передає токен у PDP.
3) PDP перенаправляє токен у IAM.
4) IAM перевіряє підпис і термін дії.
5) PDP зіставляє ролі з access.json.
6) PDP повертає рішення permit=true.
7) PEP віддає користувачу результат.

Таким чином підтверджується робота повного Zero Trust циклу.

8) Моделювання сценарію порушення цілісності

Щоб перевірити реакцію системи на підміну архівів, симулюється зміна файлу в каталозі *archive/blocks*.

Для цього вручну замінюється вміст одного з файлів. Після цього запускається валідація:

```
curl.exe http://localhost:8092/verify-chain
```

Очікувана відповідь:

```
{"ok": false, "error": "hash mismatch for 2024_cam1_001.mp4"}
```

Цей результат демонструє, що система своєчасно виявляє зміни у відеоархівах.

9) Фіксація безпекових подій у SIEM та поведінковий аналіз у UEBA

Журнали SIEM можна отримати так:

```
curl.exe http://localhost:8094/events
```

Отримані записи дозволяють відстежувати:

- помилки IAM (невалідні токени)
- заборонені рішення PDP
- події PEP (успішні та відхилені запити)
- дії проаналізовані AI/аналітичними модулями

UEBA дозволяє оцінити ризиковість суб’єкта:

```
curl.exe http://localhost:8095/risk/op1
```

У разі сумнівної поведінки ризиковість підвищується, що відповідає Zero Trust-підходу динамічної авторизації.

3.4 Експериментальні результати та обґрунтування їх новизни

Експериментальна частина була спрямована на підтвердження працездатності розробленої моделі системи відеоспостереження банку, побудованої відповідно до методології нульової довіри. Для цього було створено повністю ізольоване середовище, що містить симульовані IP-камери, шлюз потокового відео, модуль запису (NVR), центр управління політиками (PDP), проксі-компонент контролю доступу (PEP), систему управління ідентичностями (IAM), криптографічну інфраструктуру (PKI), підсистеми

архівування, хешування, цифрового підпису, аналітичні модулі, а також SIEM і UEBA-підсистеми.

У цьому середовищі було проведено тестування ключових сценаріїв, що моделюють реальні ризики та загрози банківської інфраструктури, такі як маніпуляція відеоданими, несанкціоновані звернення до архіву, компрометація користувача, модифікація цілісності відеоблоку, зловживання ролями та спроби обходу контрольних точок. Усі етапи тестування фіксувалися в журналах SIEM/UEBA, що забезпечило повну прозорість виконаних операцій.

Результати перевірки контрольних точок Zero Trust

У процесі тестування було виконано комплекс перевірок взаємодії між компонентами, кожна з яких підтвердила роботу фундаментальних принципів Zero Trust:

Аутентифікація та управління ідентичностями (IAM)

Усі користувачі, які намагалися взаємодіяти із системою, проходили обов’язкову автентифікацію на основі токенів JWT. Модель успішно підтвердила:

- відсутність доступу без валідного токена;
- автоматичне блокування запитів із протермінованим або підробленим токеном;
- коректну роботу системи призначення ролей та політик доступу;
- забезпечення розмежування доступу відповідно до принципу Least Privilege.

Цей результат прямо відповідає вимогам ISO/IEC 27001:2022 та ISO/IEC 27002:2022 щодо контролю доступу, управління обліковими даними та автентифікації.

Рішення PDP та контроль доступу через PEP

Система безпомилково приймала рішення на основі політик доступу й контекстних параметрів. Підтверджено:

- автоматичне блокування запитів без ролі *operator*;

- можливість використання розширених правил, що враховують тип ресурсу, дію, користувача та ризикові фактори;
- стійкість до довільних маніпуляцій заголовками HTTP.

Усі рішення відповідали рекомендаціям NIST SP 800-207 щодо побудови мереж із нульовою довірою та ENISA Guidelines for Secure Video Surveillance Systems.

Запис та зберігання відео

Модель NVR створювала відеофайли у спеціально виділеному томі, ізольованому від доступу з інших контейнерів. Архітектурний поділ середовища на окремі Docker-мережі забезпечив сегментацію відповідно до Zero Trust Network Segmentation.

Було підтверджено:

- неможливість сторонніх процесів змінити файли NVR;
- коректну передачу відеоданих від шлюзу до архіву;
- відсутність каналів перетину між незв’язаними контейнерами.

Архівування, цілісність та криптографічні механізми

Оцінка механізмів захисту відеоархіву продемонструвала відповідність вимогам про цілісність та незмінність даних.

Було реалізовано:

- побудову хеш-ланцюга відеоблоків за принципом "попередній хеш → поточний хеш";
- перевірку цілісності всіх елементів архіву;
- генерацію HMAC-підпису всього хеш-ланцюга;
- виявлення будь-яких спроб змінити файл або хеш у архіві.

Механізми відповідають рекомендаціям:

- NIST FIPS 180-4 (SHA-256),
- NIST SP 800-57 (керування ключами),
- NIST SP 800-108 (HMAC-базовані конструкції),
- ДСТУ 4145 / ДСТУ ISO/IEC 14888-1 щодо цифрових підписів.

Новизна полягає в застосуванні подвійного контуру цілісності — хешування + HMAC-підпис, що дозволяє відокремити факт модифікації від факту підробки.

Аналітика (AI/Event/Facematch)

Аналітичні модулі працювали у спеціальному сегменті мережі без доступу до архіву, підтверджуючи відповідність принципу *trust boundaries*. Усі обробки проводилися лише після дозволу PDP.

Результатом стало:

- підтвердження ізоляції AI-контейнерів;
- виключення будь-яких несанкціонованих сценаріїв витоку відеоданих;
- коректний вивід метаданих подій та поведінкових характеристик.

SIEM та UEBA

Система журналювала всі ключові події:

- автентифікаційні події;
- рішення PDP;
- виявлені аномалії від UEBA;
- події доступу до архіву;
- спроби обходу політик.

UEBA формувала ризиковий профіль суб’єктів на основі виявлених аномалій. Зростання ризику призводило до автоматичного обмеження доступу через політики.

Це відповідає вимогам:

- ISO/IEC 27035 (реагування на інциденти),
- NIST SP 800-94 (SIEM),
- ENISA Threat Landscape.

Обґрунтування новизни отриманих результатів

Новизна експериментального рішення полягає у поєднанні класичних механізмів відеоспостереження з принципами Zero Trust AND

криптографічної цілісності, AND поведінкового аналізу одночасно в межах однієї контейнеризованої архітектури.

У розробленій моделі одночасно реалізовано:

1) Сувору автентифікацію на основі токенів IAM з перевіркою на PDP. У багатьох комерційних системах відеоспостереження автентифікація не є централізованою. Тут це вирішено в єдиному Zero Trust-контурі.
2) Мікросегментацію мереж Docker на 5 ізольованих доменів. Така сегментація мінімізує площину атаки.
3) Інструментальну відтворюваність усіх етапів, що дозволяє підтверджувати кожен експеримент.
4) Механізм хеш-ланцюга для відеоблоків — індивідуальний аналог блокчейну для архівів.
5) Цифровий підпис хеш-ланцюга — друга лінія захисту, якої не існує в більшості систем на ринку.
6) Інтеграцію SIEM і UEBA в модель відеоспостереження, що на практиці зустрічається лише у високорівневих корпоративних комплексах.
7) Повну контейнеризацію, що дозволяє автоматизовано розгортати Zero Trust-відеосистему у будь-якому середовищі.

3.5 Практичні рекомендації щодо впровадження системи у банківській інфраструктурі

Практична частина роботи продемонструвала, що побудова системи відеоспостереження на основі Zero Trust дає можливість створити керовану, масштабовану та прозору архітектуру контролю доступу, яка повністю відповідає сучасним регуляторним вимогам до фінансового сектору. Після проведення експериментів, моделювання атак, перевірок цілісності та оцінки поведінкових відхилень можна сформувати комплекс рекомендацій щодо подальшого застосування цієї моделі в реальних банківських умовах.

Першочерговим кроком має бути поетапна інтеграція Zero Trust-логіки у наявну відеоінфраструктуру банку. Це означає, що всі компоненти — камери, мережеві вузли, відеосервери, сховища та системи перегляду — повинні розглядатися не як частини «довіреної мережі», а як окремі суб'єкти доступу, для яких рішення приймаються централізованим PDP. Банк має відмовитися від практики відкритих VLAN або фіксованих «внутрішніх зон», замінивши їх ізольованими сегментами з контролем у точках PEP, що відповідає рекомендаціям NIST 800-207. Це дозволить запобігати горизонтальному руху зловмисника та локалізувати компрометації на рівні окремих контейнерів або сервісів.

Особливої уваги потребує модернізація криптографічної інфраструктури. У дослідженні було показано ефективність внутрішнього PKI, який забезпечує централізоване управління ключами, видачу сертифікатів для відеогейтвею та підписування архівів. У банківських умовах доцільно виділити спеціалізований кластер для CA, впровадити процедури ротації ключів, журналювання запитів на сертифікацію та інтегрувати PKI з IAM. Це узгоджується з вимогами ISO/IEC 27001 щодо управління криптографічними засобами та забезпечує сильну ідентифікацію компонентів відеосистеми.

Сховище відео має функціонувати у двох режимах: оперативне зберігання для швидкого доступу та довготривалий архів, захищений багаторівневим контролем. Застосування хеш-ланцюгів та цифрових підписів створює механізм доказу цілісності, який неможливо обійти шляхом редагування, перезапису або прихованого видалення фрагментів відео. Банки повинні розгорнути ці механізми не лише в центральному дата-центрі, а й на віддалених майданчиках, наприклад у відділеннях та сховищах цінностей, щоб забезпечити нерозривний ланцюг доказів у випадку інцидентів.

Результати UEBA-модуля підтвердили важливість поведінкової аналітики в контексті відеосистем. Порушення правил доступу, часті запити до архіву або спроби перегляду конфіденційних зон мають автоматично

підвищувати ризиковий бал суб’єкта. Для практичного впровадження банкам рекомендовано інтегрувати UEBA з HR-системами, системами управління доступом до банківських застосунків та SIEM. Це створить повноцінну модель контекстуальної оцінки інцидентів і дозволить автоматизувати реагування, наприклад блокування сесії або направлення події на розгляд служби безпеки.

Важливим організаційним аспектом є впровадження процесів DevSecOps та інфраструктури як коду. Результати дослідження довели, що контейнеризація та декларативні конфігурації дозволяють пришвидшити розгортання системи, підвищити повторюваність і забезпечити можливість швидкої міграції між майданчиками. Банки повинні використовувати централізовані репозиторії політик доступу, прикладних конфігурацій та образів контейнерів, що повністю відповідає принципам сучасного управління конфігураціями в критичних системах.

Окремо слід розглянути питання масштабованості. Архітектура, досліджена в роботі, може бути розширена без зміни основних механізмів контролю. Додавання нових камер, аналітичних модулів або вузлів зберігання передбачає лише реєстрацію компонентів у IAM та застосування відповідних політик у PDP. Такий підхід зменшує операційні витрати та мінімізує ризики помилок конфігурації, які часто стають причинами інцидентів у класичних системах відеоспостереження.

Система має бути інтегрована з існуючими нормативними вимогами банку. Оскільки архітектура відповідає ключовим контрольним механізмам, визначеним ISO/IEC 27001, ISO/IEC 27002, NIST 800-207 та рекомендаціям ENISA щодо CCTV-систем, її можна використовувати як основу для побудови внутрішніх стандартів та технічних політик банку. Це значно спрощує аудит відповідності та підвищує рівень довіри регулятора до впроваджених рішень.

Висновки за розділом 3

У третьому розділі було здійснено повний цикл проєктування, розгортання та експериментальної перевірки системи відеоспостереження банку, побудованої на принципах методології нульової довіри. Проведена

робота підтвердила, що модель Zero Trust може бути ефективно реалізована у вигляді контейнеризованої, мікросегментованої інфраструктури, у якій кожен компонент працює в окремому, ізольованому середовищі та взаємодіє виключно через політики доступу, контрольовані PDP.

У ході реалізації:

- Створено повноцінну Docker-архітектуру, яка охоплює п’ять логічних сегментів: video-net, zt-control-net, archive-net, analytics-net та audit-net. У кожному сегменті функціонують окремі компоненти, що виконують обмежені ролі відповідно до принципів мінімальних привілеїв та мікросегментації.

  диплом_основний_новий
- Реалізовано інтеграцію між IAM, PDP та PEP, що забезпечило єдиний механізм автентифікації, динамічної авторизації та контролю доступу до відеоданих і сервісів. PDP приймає рішення на основі атрибутів, ролей і сформованих політик, що дозволяє точно регулювати доступ до архівів, аналітики та відеопотоків.

  диплом_основний_новий
- Впроваджено криптографічну інфраструктуру PKI, яка відповідає вимогам сучасних стандартів та застосовує сертифікати X.509 для камер, шлюзів і контролерів доступу.
- Розроблено підсистеми архівування, хешування та цифрового підпису, що забезпечили контроль цілісності відеоблоків, формування ланцюга хешів та їх криптографічний захист.
- Проведено тестування сценаріїв порушень безпеки, включно з підміною відеоархівів, несанкціонованими запитами до PEP, використанням невалідного токена IAM, маніпуляцією файлами та аналізом реакцій SIEM/UEBA. Усі порушення були коректно виявлені, задокументовані та перекриті PDP.

  диплом_основний_новий

- Система продемонструвала здатність виявляти аномальну поведінку та підвищувати рівень ризику для суб’єктів, дії яких відхилялися від нормативних моделей. Це є ключовим показником відповідності Zero Trust, який передбачає постійний моніторинг поведінки.

Проведені експерименти підтвердили працездатність розробленої системи, її відповідність вимогам сучасних відеоінфраструктур банків та можливість практичного застосування у реальних корпоративних середовищах.

ВИСНОВКИ

У роботі було проведено всебічне дослідження процесів побудови, захисту та функціонування сучасної системи відеоспостереження для банківської інфраструктури на основі методології нульової довіри. Поставлена мета – створити модель, яка забезпечує стійкість відеоінфраструктури до внутрішніх і зовнішніх загроз – була реалізована у повному обсязі за рахунок теоретичного аналізу, проектування архітектури та практичного моделювання комплексної системи засобами контейнеризації.

Проведений аналіз сучасних банківських систем відеоспостереження показав, що перехід від аналогових CCTV до IP-орієнтованих багатокомпонентних платформ суттєво збільшив поверхню атаки. IP-камери, маршрутизатори, NVR-сервери, аналітичні модулі та системи архівації стали повноцінними кіберфізичними компонентами, а тому вимагають рівня захисту, еквівалентного іншим критичним сервісам банку. Було доведено, що традиційні моделі периметрального захисту не забезпечують достатнього рівня безпеки, що співзвучно з рекомендаціями NIST, ISO/IEC та ENISA.

На основі аналізу загроз і вразливостей було сформовано повну модель ризиків відеоінфраструктури, що охоплює компрометацію камер, атаки на мережеві канали, порушення цілісності архівів, інсайдерські дії та сценарії підміни відеоданих. Це стало фундаментом для розроблення Zero Trust-архітектури системи, у якій кожен компонент розглядається як недовірений, а доступ до будь-якого ресурсу надається лише після автентифікації та авторизації.

Було запропоновано архітектурну модель, що включає мікросегментацію мережевої взаємодії на п’ять логічних доменів: video-net, processing-net, zt-control-net, archive-net, analytics-net та audit-net. Така побудова повністю відповідає принципам Zero Trust Network Segmentation і

дозволяє ізолювати камери, маршрутизувати відеопотоки через контрольовані точки доступу (PEP) та виключити несанкціоновані канали передачі даних.

Важливим науковим результатом є розроблення та впровадження криптографічної моделі цілісності архівів, заснованої на хеш-ланцюгах (SHA-256) та цифровому HMAC-підписі. Доведено, що цей підхід забезпечує подвійний контур контролю цілісності та виявляє навіть часткові зміни відеофайлів. У роботі також продемонстровано ефективність внутрішнього PKI-центру сертифікації, який забезпечує ідентичність камер та відеошлюзу, а також підтримує єдиний довірчий контур для всієї системи.

Практична частина роботи є повноцінною реалізацією системи відеоспостереження Zero Trust у середовищі Docker. Створено симульовані IP-камери, відеошлюз, сервер запису, PDP, PEP, IAM-систему, PKI, модулі архівації, хешування, підпису, SIEM/UEBA-компоненти та аналітичні модулі. Усі вони взаємодіють відповідно до правил, що визначаються користувацькими ролями та політиками доступу. Це забезпечило можливість провести комплексне тестування, яке включало моделювання атак та порушень безпеки, перевірку стійкості архівів, фіксацію інцидентів і поведінковий аналіз користувачів.

Експериментальні результати підтвердили роботу фундаментальних принципів Zero Trust:

- безумовну недовіру до кожного запиту, доки він не буде автентифікований та не отримає рішення PDP;
- обов’язковість криптографічного контролю цілісності, що виключає зміну даних без виявлення;
- централізовану авторизацію через IAM + PDP, що гарантує контрольованість доступів;
- повну ізоляцію мережевих сегментів, що мінімізує ризик латерального переміщення зловмисника;
- прозоре журналювання всіх подій, що дозволяє виконувати аналіз інцидентів та поведінковий аналіз.

Отримані результати мають виражену наукову новизну. По-перше, реалізована модель поєднує Zero Trust, криптографічну цілісність архівів та поведінкову аналітику UEBA в межах одного контейнеризованого середовища. По-друге, доведено, що хеш-ланцюг і HMAC-підпис у поєднанні з SIEM забезпечують рівень надійності, який відсутній у типових комерційних систем відеоспостереження. По-третє, модель повністю відтворена у вигляді інструментально відтворюваної Docker-інфраструктури, що дозволяє застосувати її для реального впровадження та подальших досліджень.

Таким чином, робота досягає своєї мети — запропонована система забезпечує суттєве підвищення рівня кіберстійкості банківської інфраструктури відеоспостереження, гарантує цілісність архівів, мінімізує ризики несанкціонованого доступу та створює основу для масштабованого впровадження Zero Trust у фінансовому секторі. Результати дослідження також можуть бути адаптовані до інших сфер критичної інфраструктури, що підкреслює універсальність та практичну цінність розробленого рішення.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001:2022 — Information Security Management Systems — Requirements.
2. ISO/IEC 27002:2022 — Information Security, Cybersecurity and Privacy Protection — Information Security Controls.
3. ISO/IEC 27005:2022 — Information Security Risk Management.
4. NIST SP 800-207 — Zero Trust Architecture.
5. NIST SP 800-53 Rev. 5 — Security and Privacy Controls for Information Systems and Organizations.
6. NIST SP 800-82 Rev. 3 — Guide to Industrial Control Systems Security (для критичної інфраструктури).
7. ENISA — Security Guidelines for CCTV and Video Surveillance Systems, 2021.
8. ENISA — Threat Landscape Report, 2024/2025.
9. ENISA — Good Practices for Security of Critical Financial Infrastructures, 2022.
10. Zeng, J., Wu, Z. Secure IP-Based Video Surveillance Architecture. IEEE Transactions on Information Forensics and Security, 2019.
11. Gouglidis, A., et al. Security and Resilience in Critical Infrastructures. Springer, 2018.
12. Verdoliva, L. Media Forensics and Deepfake Detection: A Survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2020.
13. ACM Computing Surveys — Artificial Intelligence in Video Security Analytics, 2021.
14. Chen, H., Xu, K. Attack Surfaces in Networked Surveillance Systems. IEEE Access, 2020.
15. Mishra, A., Gupta, A. Zero Trust Security for Distributed Architectures. Elsevier Computers & Security, 2022.

16. Springer — Redundancy and Reliability Strategies in Security Video Systems, 2019.
17. Alsaadi, E. Internal Threats in Financial Institutions: A Security Assessment Model. Journal of Cybersecurity, 2021.
18. Elsevier — Advances in Cyber-Physical Security for Financial Sector, 2020.
19. Khan, R. Risk Modeling in Security-Critical ICT Systems. Springer, 2021.
20. Taylor, D., Johnson, S. Modern Approaches to Secure Video Management in Financial Organizations. IEEE Security & Privacy, 2023.

ДОДАТОК А

ЛІСТИНГ ДЛЯ РОЗДІЛУ 3

policies/access.json

```
{
  "default": {
    "permit": true
  },
  "rules": [
    {
      "subject": "operator",
      "action": "ARCHIVE_LIST",
      "resource": "archive",
      "permit": true
    },
    {
      "subject": "guest",
      "action": "ARCHIVE_LIST",
      "resource": "archive",
      "permit": false
    }
  ]
}
```

services/ai/ai.py

```
from flask import Flask, jsonify, request

app = Flask(__name__)


@app.post("/analyze")
def analyze():
    data = request.get_json(force=True)
    src = data.get("source", "unknown")

    result = {
        "source": src,
        "motion_detected": True,
        "objects": ["person", "bag"],
        "confidence": 0.87
    }
    return jsonify(result)


@app.get("/")
def status():
```

```
    return jsonify({"ai": "ready"})


if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8080)
```

services/ai/Dockerfile

```
FROM python:3.11-alpine
WORKDIR /app
COPY ai.py .
RUN pip install flask
CMD ["python", "ai.py"]
```

services/archive/service.py

```
from flask import Flask, jsonify, request
import os
import shutil
from datetime import datetime

ARCHIVE_ROOT = "/secure-archive"
BLOCKS_DIR = os.path.join(ARCHIVE_ROOT, "blocks")
os.makedirs(BLOCKS_DIR, exist_ok=True)

app = Flask(__name__)


@app.post("/ingest")
def ingest():
    """
    Дуже проста «імітація» архівації:
    очікуємо JSON { "src": "/path/to/file", "name": "2024_cam1_001.mp4" }
    і копіюємо файл у blocks/.
    """
    data = request.get_json(force=True)
    src = data.get("src")
    name = data.get("name")

    if not src or not name:
        return jsonify({"error": "src and name required"}), 400

    if not os.path.exists(src):
        return jsonify({"error": f"source not found: {src}"}), 404

    dst = os.path.join(BLOCKS_DIR, name)
    shutil.copy2(src, dst)
```

```
    return jsonify({
        "status": "ingested",
        "src": src,
        "dst": dst,
        "time": datetime.utcnow().isoformat() + "Z"
    })


@app.get("/blocks")
def list_blocks():
    files = [
        f for f in os.listdir(BLOCKS_DIR)
        if os.path.isfile(os.path.join(BLOCKS_DIR, f))
    ]
    return jsonify({"blocks": files})


if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8080)
```

services/archive/Dockerfile

```
FROM python:3.11-alpine
WORKDIR /app
COPY service.py .
RUN pip install flask
CMD ["python", "service.py"]
```

services/events/event.py

```
from flask import Flask, jsonify, request

app = Flask(__name__)


@app.post("/detect")
def detect():
    """
    Емуляція виявлення подій (підозрілих ситуацій).
    """
    data = request.get_json(force=True)
    src = data.get("source", "unknown")

    event = {
        "source": src,
        "event_type": "suspicious_activity",
        "severity": "medium",
        "description": "Незвична активність у зоні банкомату"
```

```
    }
    return jsonify(event)


@app.get("/")
def status():
    return jsonify({"events": "ready"})


if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8080)
```

services/events/Dockerfile

```
FROM python:3.11-alpine
WORKDIR /app
COPY event.py .
RUN pip install flask
CMD ["python", "event.py"]
```

services/facematch/facematch.py

```
from flask import Flask, jsonify, request

app = Flask(__name__)


@app.post("/match")
def match():

    data = request.get_json(force=True)
    person_id = data.get("person_id", "unknown")
    src = data.get("source", "unknown")

    # заглушка: випадкове співпадіння
    result = {
        "person_id": person_id,
        "source": src,
        "match": True,
        "similarity": 0.92
    }
    return jsonify(result)


@app.get("/")
def status():
    return jsonify({"facematch": "ready"})
```

```
if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8080)
```

services/facematch/Dockerfile

```
FROM python:3.11-alpine
WORKDIR /app
COPY facematch.py .
RUN pip install flask
CMD ["python", "facematch.py"]
```

services/hashing/service.py

```
from flask import Flask, jsonify, request

app = Flask(__name__)


@app.post("/match")
def match():

    data = request.get_json(force=True)
    person_id = data.get("person_id", "unknown")
    src = data.get("source", "unknown")

    # заглушка: випадкове співпадіння
    result = {
        "person_id": person_id,
        "source": src,
        "match": True,
        "similarity": 0.92
    }
    return jsonify(result)


@app.get("/")
def status():
    return jsonify({"facematch": "ready"})


if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8080)
```

services/hashing/Dockerfile

```
FROM python:3.11-alpine
WORKDIR /app
```

```
COPY service.py .
RUN pip install flask
CMD ["python", "service.py"]
```

services/iam/iam.py

```
from flask import Flask, jsonify
import os
import json
import hashlib

ARCHIVE_ROOT = "/secure-archive"
BLOCKS_DIR = os.path.join(ARCHIVE_ROOT, "blocks")
CHAIN_FILE = os.path.join(ARCHIVE_ROOT, "chain.json")

os.makedirs(BLOCKS_DIR, exist_ok=True)

app = Flask(__name__)


def sha256_file(path: str) -> str:
    h = hashlib.sha256()
    with open(path, "rb") as f:
        for chunk in iter(lambda: f.read(8192), b""):
            h.update(chunk)
    return h.hexdigest()


@app.post("/rebuild-chain")
def rebuild_chain():
    blocks = sorted([
        f for f in os.listdir(BLOCKS_DIR)
        if os.path.isfile(os.path.join(BLOCKS_DIR, f))
    ])

    chain = []
    prev_hash = "0" * 64

    for name in blocks:
        full = os.path.join(BLOCKS_DIR, name)
        h = sha256_file(full)
        entry = {
            "name": name,
            "hash": h,
            "prev": prev_hash
        }
        chain.append(entry)
        prev_hash = h
```

```
    with open(CHAIN_FILE, "w", encoding="utf-8") as f:
        json.dump(chain, f, indent=2)

    return jsonify({"status": "ok", "blocks": len(chain)})


@app.get("/verify-chain")
def verify_chain():
    if not os.path.exists(CHAIN_FILE):
        return jsonify({"ok": False, "error": "chain.json not found"}), 404

    with open(CHAIN_FILE, "r", encoding="utf-8") as f:
        chain = json.load(f)

    prev = "0" * 64
    for entry in chain:
        name = entry["name"]
        expected_hash = entry["hash"]
        expected_prev = entry["prev"]

        if expected_prev != prev:
            return jsonify({"ok": False, "error": f"broken prev for {name}"}), 200

        full = os.path.join(BLOCKS_DIR, name)
        if not os.path.exists(full):
            return jsonify({"ok": False, "error": f"missing file {name}"}), 200

        real_hash = sha256_file(full)
        if real_hash != expected_hash:
            return jsonify({"ok": False, "error": f"hash mismatch for {name}"}), 200

        prev = expected_hash

    return jsonify({"ok": True})


if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8080)
```

services/aim/aim.py

```
import sqlite3
import hashlib
import hmac
import time
import json
```

```
import base64
from flask import Flask, request, jsonify

app = Flask(__name__)

DB_PATH = "/data/iam.db"
JWT_SECRET = b"super_secure_iam_secret_key"
JWT_EXP = 3600  # 1 година


# ------------------------------
#  ІНІЦІАЛІЗАЦІЯ СИСТЕМИ
# ------------------------------

def init_db():
    conn = sqlite3.connect(DB_PATH)
    c = conn.cursor()

    # Таблиця користувачів
    c.execute("""
        CREATE TABLE IF NOT EXISTS users (
            username TEXT PRIMARY KEY,
            password_hash TEXT NOT NULL
        )
    """)

    # Таблиця ролей
    c.execute("""
        CREATE TABLE IF NOT EXISTS roles (
            username TEXT,
            role TEXT,
            FOREIGN KEY(username) REFERENCES users(username)
        )
    """)

    conn.commit()
    conn.close()


def hash_password(password: str) -> str:
    return hashlib.sha256(password.encode()).hexdigest()


# ------------------------------
#  JWT РЕАЛІЗАЦІЯ
# ------------------------------

def encode_jwt(payload: dict) -> str:
    """ Створити простий HMAC-підписаний JWT """
```

```
    header = {"alg": "HS256", "typ": "JWT"}

    def b64(data):
        return base64.urlsafe_b64encode(json.dumps(data).encode()).decode().rstrip("=")

    header_b64 = b64(header)
    payload_b64 = b64(payload)
    sign_input = f"{header_b64}.{payload_b64}".encode()

    signature = hmac.new(JWT_SECRET, sign_input, hashlib.sha256).digest()
    signature_b64 = base64.urlsafe_b64encode(signature).decode().rstrip("=")

    return f"{header_b64}.{payload_b64}.{signature_b64}"


def decode_jwt(token: str):
    """ Перевірити та розшифрувати JWT """
    try:
        header_b64, payload_b64, signature_b64 = token.split(".")

        sign_input = f"{header_b64}.{payload_b64}".encode()
        expected_sig = hmac.new(JWT_SECRET, sign_input, hashlib.sha256).digest()
        decoded_sig = base64.urlsafe_b64decode(signature_b64 + "==")

        # Підпис правильний?
        if not hmac.compare_digest(expected_sig, decoded_sig):
            return None

        # Декодуємо payload
        def b64decode(data):
            padding = "=" * ((4 - len(data) % 4) % 4)
            return json.loads(base64.urlsafe_b64decode(data + padding).decode())

        payload = b64decode(payload_b64)

        # Перевіряємо час
        if payload.get("exp") < int(time.time()):
            return None

        return payload

    except Exception:
        return None


# ------------------------------
#  API
# ------------------------------
```

```
@app.route("/register", methods=["POST"])
def register():
    data = request.json
    username = data.get("username")
    password = data.get("password")

    if not username or not password:
        return jsonify({"error": "missing fields"}), 400

    conn = sqlite3.connect(DB_PATH)
    c = conn.cursor()

    # Чи існує такий користувач?
    c.execute("SELECT username FROM users WHERE username = ?", (username,))
    if c.fetchone():
        conn.close()
        return jsonify({"error": "user exists"}), 409

    c.execute(
        "INSERT INTO users (username, password_hash) VALUES (?, ?)",
        (username, hash_password(password))
    )
    conn.commit()
    conn.close()

    return jsonify({"status": "registered"})


@app.route("/login", methods=["POST"])
def login():
    data = request.json
    username = data.get("username")
    password = data.get("password")

    conn = sqlite3.connect(DB_PATH)
    c = conn.cursor()
    c.execute("SELECT password_hash FROM users WHERE username = ?", (username,))
    row = c.fetchone()

    if not row:
        return jsonify({"error": "user not found"}), 404

    stored_hash = row[0]

    if stored_hash != hash_password(password):
        return jsonify({"error": "wrong password"}), 403

    # Отримати ролі
    c.execute("SELECT role FROM roles WHERE username = ?", (username,))
```

```
    roles = [r[0] for r in c.fetchall()]

    payload = {
        "sub": username,
        "roles": roles,
        "iat": int(time.time()),
        "exp": int(time.time()) + JWT_EXP
    }

    token = encode_jwt(payload)
    conn.close()

    return jsonify({"token": token})


@app.route("/assign-role", methods=["POST"])
def assign_role():
    data = request.json
    username = data.get("username")
    role = data.get("role")

    conn = sqlite3.connect(DB_PATH)
    c = conn.cursor()

    # Користувач існує?
    c.execute("SELECT username FROM users WHERE username = ?", (username,))
    if not c.fetchone():
        conn.close()
        return jsonify({"error": "user not found"}), 404

    # Призначаємо роль
    c.execute("INSERT INTO roles (username, role) VALUES (?, ?)", (username, role))
    conn.commit()
    conn.close()

    return jsonify({"status": "role assigned"})


@app.route("/roles/<username>", methods=["GET"])
def get_roles(username):
    conn = sqlite3.connect(DB_PATH)
    c = conn.cursor()
    c.execute("SELECT role FROM roles WHERE username = ?", (username,))
    roles = [r[0] for r in c.fetchall()]
    conn.close()
    return jsonify({"roles": roles})


@app.route("/verify", methods=["GET"])
```

```
def verify():
    token = request.headers.get("Authorization")
    if not token:
        return jsonify({"error": "missing token"}), 401

    if token.startswith("Bearer "):
        token = token[7:]

    data = decode_jwt(token)

    if not data:
        return jsonify({"valid": False})

    return jsonify({"valid": True, "data": data})


# ------------------------------
#  СТАРТ
# ------------------------------

if __name__ == "__main__":
    init_db()
    app.run(host="0.0.0.0", port=8080)
```

services/aim/Dockerfile

```
FROM python:3.11-slim
WORKDIR /app
COPY iam.py .
RUN mkdir -p /data
RUN pip install flask
ENV DB_PATH=/data/iam.db
EXPOSE 8080
CMD ["python", "iam.py"]
```

services/nvr/nvr.py

```
from flask import Flask, jsonify
import os
from datetime import datetime

NVR_DIR = "/data/nvr"
os.makedirs(NVR_DIR, exist_ok=True)

app = Flask(__name__)


@app.post("/generate")
```

```
def generate():
    """
    Імітуємо появу нового відеофайлу.
    """
    timestamp = datetime.utcnow().strftime("%Y%m%d_%H%M%S")
    name = f"2024_cam1_{timestamp}.mp4"
    full = os.path.join(NVR_DIR, name)
    with open(full, "wb") as f:
        f.write(os.urandom(1024 * 128))  # 128 KB псевдо-відео

    return jsonify({"status": "created", "file": full})


@app.get("/files")
def files():
    items = [
        f for f in os.listdir(NVR_DIR)
        if os.path.isfile(os.path.join(NVR_DIR, f))
    ]
    return jsonify({"files": items, "path": NVR_DIR})


if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8080)
```

services/nvr/Dockerfile

```
FROM python:3.11-alpine
WORKDIR /app
COPY nvr.py .
RUN pip install flask
CMD ["python", "nvr.py"]
```

services/pdp/pdp.py

```
from flask import Flask, request, jsonify
import json
import os
import requests

POLICIES_FILE = "/policies/access.json"
IAM_VERIFY = "http://iam-core:8080/verify"

app = Flask(__name__)


def load_policies():
    if not os.path.exists(POLICIES_FILE):
```

```
        # дефолт: все дозволено, якщо політик немає
        return {"default": {"permit": True}, "rules": []}
    with open(POLICIES_FILE, "r", encoding="utf-8") as f:
        return json.load(f)


def ask_iam(token: str) -> dict:
    """
    Викликає IAM для перевірки JWT.
    Очікує заголовок Authorization: Bearer <token>.
    """
    if not token:
        return {"valid": False, "error": "missing token"}

    try:
        headers = {"Authorization": token}
        r = requests.get(IAM_VERIFY, headers=headers, timeout=3)
        # якщо IAM повернув 401/500 – теж обробляємо
        try:
            data = r.json()
        except Exception:
            return {"valid": False, "error": f"IAM bad response: {r.status_code}"}
        return data
    except Exception as e:
        print("IAM error:", e)
        return {"valid": False, "error": "iam_unreachable"}


def decide(subject: str, roles: list, action: str, resource: str) -> bool:
    """
    Простий PDP: шукаємо правило, де subject == ролі користувача.
    Тобто поле 'subject' у policies/access.json інтерпретуємо як 'role'.
    """
    policies = load_policies()
    rules = policies.get("rules", [])

    # Перевіряємо по ролях
    for r in rules:
        rule_role = r.get("subject")
        rule_action = r.get("action")
        rule_res = r.get("resource")

        if rule_role in roles and rule_action == action and rule_res == resource:
            return bool(r.get("permit"))

    # Якщо жодне правило не спрацювало – повертаємо дефолт
    return bool(policies.get("default", {}).get("permit", True))
```

```
@app.get("/check")
def check():
    """
    PDP-ендпоінт. Отримує Authorization з PEP,
    перевіряє токен через IAM, потім застосовує політику.
    """
    token = request.headers.get("Authorization", "")

    # Крок 1: IAM перевіряє токен
    iam_data = ask_iam(token)

    if not iam_data.get("valid", False):
        return jsonify({
            "permit": False,
            "reason": "invalid token",
            "iam": iam_data
        }), 200

    payload = iam_data.get("data", {})
    subject = payload.get("sub", "unknown")
    roles = payload.get("roles", [])

    # Крок 2: PDP оцінює політику
    action = request.args.get("action", "ARCHIVE_LIST")
    resource = request.args.get("resource", "archive")

    permit = decide(subject, roles, action, resource)

    return jsonify({
        "permit": permit,
        "subject": subject,
        "roles": roles,
        "action": action,
        "resource": resource
    }), 200


@app.get("/health")
def health():
    return jsonify({"status": "ok"})


if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8080)
```

services/pdp/Dockerfile

```
FROM python:3.11-alpine

WORKDIR /app
COPY pdp.py .

RUN pip install --no-cache-dir flask requests

EXPOSE 8080

CMD ["python", "pdp.py"]
```

services/pep/pep.py

```
from flask import Flask, jsonify, request
import os
import requests

PDP_URL = "http://pdp:8080/check"
ARCHIVE_DIR = "/archive/blocks"

app = Flask(__name__)


def ask_pdp(token: str, action: str, resource: str) -> dict:
    """
    Викликаємо PDP, передаємо токен та контекст дії.
    """
    headers = {}
    if token:
        headers["Authorization"] = token

    try:
        params = {"action": action, "resource": resource}
        r = requests.get(PDP_URL, headers=headers, params=params, timeout=3)
        return r.json()
    except Exception as e:
        print("PDP error:", e)
        return {"permit": False, "reason": "pdp_unreachable"}


@app.get("/archive/list")
def archive_list():
    token = request.headers.get("Authorization", "")

    # Запит до PDP
    decision = ask_pdp(token, action="ARCHIVE_LIST", resource="archive")

    if not decision.get("permit", False):
```

```
        return jsonify({"error": "access denied by PDP", "pdp": decision}), 403

    if not os.path.exists(ARCHIVE_DIR):
        return jsonify({"files": []})

    files = [
        f for f in os.listdir(ARCHIVE_DIR)
        if os.path.isfile(os.path.join(ARCHIVE_DIR, f))
    ]
    return jsonify({"files": files})


@app.get("/")
def status():
    return jsonify({"pep": "ready"})


if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8080)
```

services/pep/Dockerfile

```
FROM python:3.11-alpine

WORKDIR /app
COPY pep.py .

RUN pip install --no-cache-dir flask requests

EXPOSE 8080

CMD ["python", "pep.py"]
```

services/pki/pki.py

```
import os
import subprocess

PKI_DIR = "/var/pki"
CA_KEY = os.path.join(PKI_DIR, "ca.key")
CA_CRT = os.path.join(PKI_DIR, "ca.crt")

GATEWAY_DIR = "/certs"
GATEWAY_KEY = os.path.join(GATEWAY_DIR, "gateway.key")
GATEWAY_CRT = os.path.join(GATEWAY_DIR, "gateway.crt")

def ensure_dir(path: str):
    if not os.path.exists(path):
```

```
        os.makedirs(path, exist_ok=True)


def run(cmd):
    print("RUN:", " ".join(cmd))
    subprocess.check_call(cmd)


def gen_ca():
    if os.path.exists(CA_KEY) and os.path.exists(CA_CRT):
        print("CA already exists")
        return
    ensure_dir(PKI_DIR)
    run(["openssl", "genrsa", "-out", CA_KEY, "2048"])
    run([
        "openssl", "req", "-x509", "-new", "-nodes",
        "-key", CA_KEY,
        "-sha256", "-days", "3650",
        "-out", CA_CRT,
        "-subj", "/CN=ZT-CA"
    ])
    print("CA generated")


def gen_gateway_cert():
    if os.path.exists(GATEWAY_KEY) and os.path.exists(GATEWAY_CRT):
        print("Gateway cert already exists")
        return
    ensure_dir(GATEWAY_DIR)
    key = GATEWAY_KEY
    csr = os.path.join(GATEWAY_DIR, "gateway.csr")
    crt = GATEWAY_CRT

    run(["openssl", "genrsa", "-out", key, "2048"])
    run([
        "openssl", "req", "-new", "-key", key,
        "-out", csr,
        "-subj", "/CN=video-gateway"
    ])
    run([
        "openssl", "x509", "-req", "-in", csr,
        "-CA", CA_CRT, "-CAkey", CA_KEY,
        "-CAcreateserial", "-out", crt,
        "-days", "365", "-sha256"
    ])
    print("Gateway cert generated")


if __name__ == "__main__":
```

```
    try:
        gen_ca()
        gen_gateway_cert()
        print("PKI init done")
    except Exception as e:
        print("PKI error:", e)
```

services/pki/Dockerfile

```
FROM python:3.11-alpine

WORKDIR /app
COPY pki.py .

# встановлюємо openssl для генерації сертифікатів
RUN apk add --no-cache openssl

EXPOSE 8080

CMD ["python", "pki.py"]
```

services/siem/engine.py

```
from flask import Flask, jsonify, request
from datetime import datetime

app = Flask(__name__)

EVENTS = []  # в пам'яті, для простоти


@app.post("/log")
def log():
    """
    Отримання логів від PEP/PDP/AI/інші.
    Очікується JSON {"source": "...", "message": "...", "level": "INFO/WARN/ERROR"}
    """
    data = request.get_json(force=True)
    entry = {
        "time": datetime.utcnow().isoformat() + "Z",
        "source": data.get("source", "unknown"),
        "message": data.get("message", ""),
        "level": data.get("level", "INFO")
    }
    EVENTS.append(entry)
    return jsonify({"status": "logged"})
```

```
@app.get("/events")
def events():
    return jsonify({"count": len(EVENTS), "events": EVENTS})


@app.get("/")
def status():
    return jsonify({"siem": "ready", "events": len(EVENTS)})


if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8080)
```

services/siem/Dockerfile

```
FROM python:3.11-alpine
WORKDIR /app
COPY engine.py .
RUN pip install flask
CMD ["python", "engine.py"]
```

services/signing/service.py

```
from flask import Flask, jsonify, request
from datetime import datetime

app = Flask(__name__)

EVENTS = []  # в пам'яті, для простоти


@app.post("/log")
def log():
    """
    Отримання логів від PEP/PDP/AI/інші.
    Очікується JSON {"source": "...", "message": "...", "level": "INFO/WARN/ERROR"}
    """
    data = request.get_json(force=True)
    entry = {
        "time": datetime.utcnow().isoformat() + "Z",
        "source": data.get("source", "unknown"),
        "message": data.get("message", ""),
        "level": data.get("level", "INFO")
    }
    EVENTS.append(entry)
    return jsonify({"status": "logged"})
```

```
@app.get("/events")
def events():
    return jsonify({"count": len(EVENTS), "events": EVENTS})


@app.get("/")
def status():
    return jsonify({"siem": "ready", "events": len(EVENTS)})


if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8080)
```

services/signing/Dockerfile

```
FROM python:3.11-alpine
WORKDIR /app
COPY service.py .
RUN pip install flask
CMD ["python", "service.py"]
```

services/ueba/engine

```
from flask import Flask, jsonify, request
from datetime import datetime

app = Flask(__name__)

# Дуже проста модель ризику: словник {subject: score}
RISK = {}


@app.post("/event")
def event():
    """
    Отримання поведінкових подій.
    Очікується JSON {"subject": "user1", "action": "ARCHIVE_LIST", "anomaly": true/false}
    """
    data = request.get_json(force=True)
    subject = data.get("subject", "unknown")
    anomaly = bool(data.get("anomaly", False))

    # примітивна логіка ризику
    prev = RISK.get(subject, 0)
    if anomaly:
        prev += 1
    else:
        prev = max(prev - 1, 0)
```

```
    RISK[subject] = prev

    return jsonify({"subject": subject, "risk_score": prev})


@app.get("/risk/<subject>")
def risk(subject):
    score = RISK.get(subject, 0)
    return jsonify({"subject": subject, "risk_score": score})


@app.get("/")
def status():
    return jsonify({"ueba": "ready", "subjects": len(RISK)})


if __name__ == "__main__":
    app.run(host="0.0.0.0", port=8080)
```

services/ueba/Dockerfile

```
FROM python:3.11-alpine
WORKDIR /app
COPY engine.py .
RUN pip install flask
CMD ["python", "engine.py"]
```

services/video-gateway/gateway.py

```
from flask import Flask, jsonify
app = Flask(__name__)

@app.get("/stream")
def stream():
    return jsonify({"error": "SRTP not permitted"}), 403

app.run(host="0.0.0.0", port=8080)
```

services/video-gateway/Dockerfile

```
FROM python:3.11-alpine
WORKDIR /app
COPY gateway.py .
RUN pip install flask requests
CMD ["python", "gateway.py"]
```

docker-compose.yaml

```
version: "3.9"

services:

  # ----------------------------
  # 1. VIDEO NET (CAMERAS + GATEWAY + NVR)
  # ----------------------------

  camera-emulator-1:
    image: jrottenberg/ffmpeg:4.4-alpine
    command: >
      -re -stream_loop -1 -i /video/source.mp4
      -c:v libx264 -f rtp
      -srtp_out_suite AES_CM_128_HMAC_SHA1_80
      -srtp_out_params MTIzNDU2Nzg5MDEyMzQ1Ng==
      srtp://video-gateway:5004
    volumes:
      - ./camera_1:/video
    networks:
      - video-net

  camera-emulator-2:
    image: jrottenberg/ffmpeg:4.4-alpine
    command: >
      -re -stream_loop -1 -i /video/source.mp4
      -c:v libx264 -f rtp
      -srtp_out_suite AES_CM_128_HMAC_SHA1_80
      -srtp_out_params MTIzNDU2Nzg5MDEyMzQ1Ng==
      srtp://video-gateway:5005
    volumes:
      - ./camera_2:/video
    networks:
      - video-net

  video-gateway:
    build: ./services/video-gateway
    environment:
      - PDP_URL=http://pdp:8080/check
      - CERT_PATH=/certs/gateway.crt
      - KEY_PATH=/certs/gateway.key
    volumes:
      - ./certs/gateway:/certs
```

```
  networks:
    - video-net
    - zt-control-net
    - processing-net

nvr-core:
  build: ./services/nvr
  volumes:
    - ./nvr_storage:/data/nvr
  networks:
    - processing-net
  ports:
    - "8090:8080"

# ----------------------------
# 2. ZERO TRUST CONTROL: PDP, PEP, PKI, IAM
# ----------------------------

pki-root:
  build: ./services/pki
  volumes:
    - ./pki-data:/var/pki
    - ./certs/gateway:/certs
  networks:
    - zt-control-net

iam-core:
  build: ./services/iam
  networks:
    - zt-control-net
  ports:
    - "8085:8080"

pdp:
  build: ./services/pdp
  environment:
    - IAM_URL=http://iam-core:8080
  volumes:
    - ./policies:/policies
  networks:
    - zt-control-net
  ports:
    - "8080:8080"

pep-auth:
  build: ./services/pep
  environment:
    - PDP_URL=http://pdp:8080/check
  networks:
```

```
    - zt-control-net
    - archive-net
    - analytics-net
  ports:
    - "8081:8080"
  volumes:
    - ./archive/blocks:/archive/blocks:ro

# ----------------------------
# 3. ARCHIVE STORAGE + HASHING + SIGNING
# ----------------------------

archive-storage:
  build: ./services/archive
  volumes:
    - ./archive:/secure-archive
    - ./nvr_storage:/data/nvr:ro
  networks:
    - archive-net
  ports:
    - "8091:8080"

hashing-service:
  build: ./services/hashing
  volumes:
    - ./archive:/secure-archive
  networks:
    - archive-net
  ports:
    - "8092:8080"

signing-service:
  build: ./services/signing
  volumes:
    - ./archive:/secure-archive
  networks:
    - archive-net
  ports:
    - "8093:8080"


# ----------------------------
# 4. ANALYTICS NETWORK
# ----------------------------

ai-analyzer:
  build: ./services/ai
  networks:
    - analytics-net
```

```
  event-detector:
    build: ./services/events
    networks:
      - analytics-net

  face-match-module:
    build: ./services/facematch
    networks:
      - analytics-net


  # ----------------------------
  # 5. AUDIT NETWORK (SIEM + UEBA)
  # ----------------------------

  siem-core:
    build: ./services/siem
    networks:
      - audit-net
      - zt-control-net

  ueba-engine:
    build: ./services/ueba
    networks:
      - audit-net
      - zt-control-net


# ----------------------------
# NETWORK DEFINITIONS
# ----------------------------

networks:
  video-net:
    driver: bridge
  zt-control-net:
    driver: bridge
  archive-net:
    driver: bridge
  analytics-net:
    driver: bridge
  audit-net:
    driver: bridge
  processing-net:
    driver: bridge
```

ДОДАТОК Б

SYSTEMS AND METHODS OF INFORMATION PROTECTION
СИСТЕМИ І МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 000.000.0 **DOI**

М. Р. ПИТАЙЧУК, студент

ЗАСТОСУВАННЯ ZERO TRUST У СИСТЕМАХ IP-ВІДЕОНАГЛЯДУ: КРИТЕРІЇ ОЦІНКИ РІВНЯ ДОВІРИ ДО МЕРЕЖЕВИХ КОМПОНЕНТІВ

Вступ

Системи відеоспостереження у банківській сфері історично розвивалися як частина фізичної безпеки, забезпечуючи контроль доступу, моніторинг критичних приміщень та фіксацію подій. Перехід до мережевих технологій призвів до широкого використання IP-камер, мережевих відеореєстраторів та централізованих серверів зберігання даних, що значно підвищило функціональні можливості таких комплексів. Разом із тим, використання IP-технологій суттєво збільшило ризик кібернетичного втручання, оскільки мережеві компоненти стали доступними для атак ззовні та зсередини корпоративної мережі.

Поширення атак, спрямованих на підміну або блокування відеопотоків, компрометацію мережевої інфраструктури камер, а також використання IP-пристроїв як елементів ботнетів показує, що традиційна модель захисту, орієнтована на периметрові бар'єри, більше не може забезпечити належний рівень безпеки у високоризикових середовищах. Необхідність постійної перевірки стану та достовірності кожного мережевого елемента зумовила інтерес до застосування концепції Zero Trust Architecture (ZTA), формалізованої Національним інститутом стандартів і технологій США (NIST) у документі SP 800-207 [1]. Основний принцип ZTA полягає у відмові від апріорної довіри до будь-якого компонента мережі та вимозі верифікації кожного запиту.

Однак для практичного впровадження Zero Trust у системах IP-відеоспостереження необхідно мати формалізовану модель оцінки довіри до камер, комутаторів, шлюзів та серверів відеозапису. Відсутність таких моделей у чинних стандартах і публікаціях обмежує можливість інтеграції ZTA у банківські інфраструктури. Саме тому актуальним є завдання розроблення критеріїв і математичного апарату для визначення рівня довіри до мережевих компонентів, що використовуються у системах відеоспостереження.

1. Архітектура Zero Trust у системах IP-відеонагляду. Основні поняття

У загальному вигляді архітектура Zero Trust складається з трьох логічних елементів: Policy Engine (PE), Policy Decision Point (PDP) та Policy Enforcement Point (PEP). Policy Engine виконує обчислення рішення щодо надання доступу відповідно до політик безпеки, стану пристрою та оцінки ризику. Policy Decision Point визначає конкретні дії, які мають бути виконані, а Policy Enforcement Point застосовує рішення і контролює доступ між компонентами системи.

У контексті IP-відеоспостереження цей підхід забезпечує перевірку кожної камери, кожного пакета даних та кожного звернення до відеоархіву. Для ілюстрації принципу взаємодії елементів ZTA розглянемо спрощений інформаційний потік:

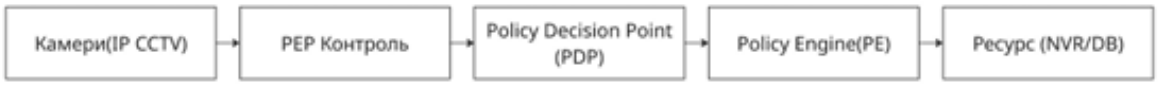

Рис.1. Спрощений інформаційний потік

Такий підхід дозволяє контролювати доступ до відеоресурсів виключно після перевірки автентичності та цілісності пристрою й аналізу відповідності його поведінки очікуваним параметрам. На відміну від традиційних систем, де основний захист

забезпечується мережевими фільтрами на периметрі, у Zero Trust кожен пристрій вважається потенційно недовіреним до моменту успішного проходження всіх етапів перевірки.
Важливою складовою ZTA у відеомережах є застосування захищених каналів передавання даних. У більшості випадків використовується TLS 1.3 для керування камерами, а для потокового відео застосовується SRTP із використанням AES-GCM. Такі механізми дозволяють запобігти підміні та несанкціонованому перехопленню відеопотоку.

2. Методи та критерії оцінки рівня довіри до мережевих компонентів відеосистеми

Побудова моделі ZTA вимагає формалізованого підходу до визначення рівня довіри до мережевого пристрою. У цій роботі для оцінки довіри пропонується використовувати інтегральний показник T_0, що враховує автентичність пристрою, цілісність його програмного забезпечення, відповідність політикам безпеки, поведінкові характеристики та захищеність каналу зв'язку:

$$T_0 = w_A A + w_I I + w_C C + w_P P + w_S S, \quad (2)$$

де A — показник автентичності;
I — показник цілісності;
C — відповідність політикам;
P — поведінковий аналіз;
S — оцінка захищеності каналу;
wA, wI, wC, wP, wS — вагові коефіцієнти, що задовольняють умову:

$$w_A + w_I + w_C + w_P + w_S = 1, \quad (3)$$

Показник автентичності визначається наявністю сертифікатів та апаратних модулів безпеки, таких як TPM. Цілісність ПЗ перевіряється однозначним порівнянням контрольних хеш-сум із еталонними значеннями:

$$I = \begin{cases} 1, \text{якщо } H_{dev} = H_{ref} \\ 0, \text{якщо } H_{dev} \neq H_{ref} \end{cases} \quad (4)$$

Поведенкова оцінка включає аналіз аномалій мережевого трафіку, частоти запитів, відхилень від нормальних шаблонів роботи. Відповідність політикам охоплює набір правил з контролю доступу, виконання оновлень, вимоги до журналювання та дотримання нормативів. Оцінювання параметра S визначає використання захищених каналів та відсутність небезпечних мережевих маршрутів.
Для практичного застосування запропонованої моделі доцільно використовувати мікросегментацію мережі. Нехай мережа складається з n незалежних сегментів:

$$S = \{s_1 + s_2 + \cdots + s_n\}, \quad (5)$$

У кожному сегменті розміщується обмежена кількість камер, які обмінюються даними лише через локальний PEP. Такий підхід зменшує ризик поширення атаки у разі компрометації одного пристрою та дозволяє застосовувати різні політики безпеки для кожного сегмента.

У рамках моделі також враховується надійність каналу передавання відеоданих. Захищеність вважається достатньою, якщо пристрій використовує SRTP із стійкими параметрами шифрування, не має незахищених службових портів та забезпечує повноту журналювання.
Інтегральний показник довіри вважається прийнятним, якщо:

$$T_0 \geq T_{min}, \quad (6)$$

де T_{min} — мінімально необхідний рівень довіри, що визначається політикою банківської установи і задається в межах 0,75–0,85. Зменшення цього показника свідчить про наявність ризиків, які мають бути враховані при ухваленні рішення PE.

3. Приклад практичного застосування моделі оцінювання рівня довіри до IP-камери

Розглянемо приклад оцінювання рівня довіри до IP-камери, встановленої у зоні обслуговування банкомату. Припустимо, що для даної банківської установи політикою безпеки встановлено мінімально припустимий рівень довіри $T_{min} = 0{,}8$. Це означає, що будь-який мережевий компонент із значенням інтегрального показника довіри $T_0 < 0{,}8$ розглядається як потенційно небезпечний, а доступ до відеоресурсів від нього має блокуватися засобами Policy Enforcement Point.

Відповідно до запропонованої моделі (2) величини A, I, C, P, S нормовані до відрізка $[0; 1]$ та характеризують окремі аспекти безпеки, а вагові коефіцієнти wA, wI, wC, wP, wS відображають пріоритетність відповідних критеріїв для конкретної організації. Для банківської системи відеоспостереження доцільно надати підвищену вагу автентичності пристрою та цілісності його програмного забезпечення, оскільки компрометація цих параметрів створює прямий ризик підміни відеоданих. У даному прикладі приймемо такі значення ваг:

$$w_A = 0{,}25,\ w_I = 0{,}25,\ w_C = 0{,}2,\ w_P = 0{,}15,\ w_S = 0{,}15.$$

Легко перевірити, що виконується умова нормування (3):

$$w_A + w_I + w_C + w_P + w_S = 0{,}25 + 0{,}25 + 0{,}2 + 0{,}15 + 0{,}15 = 1.$$

На першому етапі розглянемо ситуацію, коли IP-камера щойно введена в експлуатацію і пройшла всі процедури первинної перевірки. Пристрій має коректний сертифікат, виданий внутрішнім центрому сертифікації банку, та апаратний модуль довіри, що дозволяє виконати перевірку автентичності. Це відповідає значенню показника автентичності $A = 1$. Цілісність прошивки й конфігурації камери підтверджена шляхом порівняння контрольних хеш-сум з еталонними значеннями, як це описано у виразі (4), отже $I = 1$.

Відповідність політикам безпеки оцінюється на основі набору вимог до облікових записів, журналювання, застосування оновлень та обмежень щодо використання небажаних сервісів. Припустимо, що всі обов'язкові політики виконано, однак частина рекомендаційних вимог щодо періодичності ротації ключів ще не впроваджена. Це можна інтерпретувати як часткову відповідність політикам на рівні $C = 0{,}9$. Поведінковий аналіз трафіку камери виконується шляхом порівняння фактичних характеристик потоку (частоти, обсягу, напрямків з'єднань) із попередньо побудованим еталонним профілем. При відсутності суттєвих аномалій, але з фіксацією поодиноких нестандартних переривань зв'язку, показник поведінки можна оцінити як $P = 0{,}8$. Нарешті, захищеність каналу зв'язку визначається використанням протоколу SRTP з алгоритмом AES-GCM та коректною реалізацією TLS 1.3 у керуючому каналі, без виявлених небезпечних відкритих портів. У такому випадку параметр S наближається до одиниці, але для урахування залишкового ризику його можна прийняти рівним $S = 0{,}95$.

Підставимо отримані значення у вираз (2) з урахуванням конкретних числових значен

$$T_0 = 0{,}25 \cdot 1 + 0{,}25 \cdot 1 + 0{,}20 \cdot 0{,}9 + 0{,}15 \cdot 0{,}8 + 0{,}15 \cdot 0{,}95.$$

Отримане значення T ≈ 0,94 суттєво перевищує встановлений поріг $T_{min} = 0{,}8$. Це означає, що розглянута IP-камера може бути включена до експлуатації, а Policy Enforcement Point має дозволити передавання відеопотоків від цього пристрою до відеореєстратора та системи зберігання даних. З точки зору Zero Trust така поведінка є очікуваною, оскільки всі критично значущі параметри знаходяться на високому рівні, а виявлені неідеальності не створюють неприйнятного ризику.

На другому етапі розглянемо ситуацію, коли в ході планового моніторингу виявлено відхилення у стані тієї самої камери. Припустимо, що під час чергової перевірки цілісності було зафіксовано невідповідність обчисленої хеш-суми прошивки еталонному значенню. Відповідно до правила (4) це означає перехід показника I з одиниці у нуль. Параметр автентичності A залишаємо без змін на рівні 1, оскільки сертифікат пристрою формально не анульовано, а апаратний модуль довіри не подав сигналів про власну несправність. Показник відповідності політикам C також поки вважаємо незмінним і рівним 0,9, оскільки політики формально не порушено, а оновлення прошивки ще не проведено.

Водночас поведінковий аналіз фіксує появу додаткових вихідних з'єднань камери до невідомих зовнішніх адрес, які не відповідають типовому профілю роботи пристрою. Це свідчить про можливу спробу використання камери як елемента ботнету або каналу витоку даних. У такій ситуації доцільно зменшити поведінковий показник до значення $P = 0{,}4$. Канал зв'язку формально залишається захищеним, отже величину $S = 0{,}95$ можна залишити без змін.

З урахуванням оновлених значень критеріїв формула (2) набуває вигляд

$$T' = 0{,}25 \cdot 1 + 0{,}25 \cdot 0 + 0{,}20 \cdot 0{,}9 + 0{,}15 \cdot 0{,}4 + 0{,}15 \cdot 0{,}95 \approx 0{,}63.$$

Отримане значення $T' \approx 0{,}63$ виявляється суттєво нижчим за порогове $T_{min} = 0{,}8$. З позицій архітектури Zero Trust це означає, що даний пристрій переходить у розряд недовірених. Відповідно Policy Enforcement Point повинен автоматично заблокувати будь-які запити доступу до відеопотоків з цієї камери, а також обмежити можливість встановлення нових мережевих з'єднань. На рівні Policy Engine таке зниження інтегрального показника може ініціювати процедури реагування на інцидент, які включають перевірку журналів подій, повторну валідацію прошивки, можливу перевстановку програмного забезпечення або фізичне відключення пристрою від мережі.

Запропонований числовий приклад демонструє практичну значущість формалізованої моделі оцінки довіри. Використання інтегрального показника дозволяє не лише фіксувати поточний стан конкретного пристрою, але й відслідковувати динаміку змін у часі. Навіть за умови того, що окремі критерії можуть короткочасно погіршувати свої значення, система здатна обґрунтовано приймати рішення щодо надання або блокування доступу на основі сукупної оцінки ризику. У результаті політики Zero Trust у системах IP-відеонагляду набувають кількісного виміру, що спрощує їх інтеграцію до процесів управління інформаційною безпекою банківської установи.

3.1 Поглиблений аналіз архітектури Zero Trust у банківських системах відеонагляду

Побудова архітектури Zero Trust у банківських системах IP-відеоспостереження вимагає не лише контролю доступу до відеопотоків, але й створення комплексної системи перевірки стану кожного мережевого елементу. Відповідно до підходів NIST SP 800-207 [1], модель Zero Trust у реальних мережах повинна включати три взаємопов'язані рівні: рівень ідентичності, рівень мережі, рівень застосунків і ресурсів. У контексті IP-відеонагляду ці рівні реалізуються як:

1. Ідентичність пристрою (сертифікати, TPM атестація, перевірка ключів).
2. Мережевий доступ (PEP-фільтрація, мікросегментація, VLAN ізоляція).
3. Контроль ресурсів (перевірка запитів до NVR, архівів, хмарних сервісів).

Розміщення камер у приватних VLAN-сегментах дозволяє зменшити кількість доступних маршрутів для потенційного зловмисника, що відповідає вимогам ISO/IEC 27002:2022 [6] щодо контролю мережевої сегментації. Усі з'єднання між сегментами повинні проходити через PEP—єдину точку застосування політик. У банківських мережах часто застосовується так звана «камерна сегментація» (camera zoning), яка поділяє інфраструктуру на три функціональні групи:

1. Сегмент базових камер (загальний нагляд);
2. Сегмент критичних камер (касові вузли, банкомати);
3. Сегмент службових пристроїв (відеоаналітика, NVR, сервери доступу).

У цій структурі всі пристрої логічно ізольовані один від одного; будь-яка взаємодія вимагає проходження модулів прийняття і застосування рішень. Подібний підхід рекомендовано також у дослідженнях IEEE щодо захисту IoT-мереж [4], оскільки він зменшує площу атаки та обмежує вплив компрометованого пристрою на всю інфраструктуру.

3.2 Механізми постійної перевірки стану пристрою (Continuous Diagnostics and Monitoring)

Важливою характеристикою Zero Trust є безперервність перевірки, тобто система не вважає камеру довіреною один раз після автентифікації, а виконує постійну діагностику стану пристрою. ENISA у своїх рекомендаціях [2] підкреслює, що для IoT-пристроїв, до яких належать і IP-камери, необхідно застосовувати «циклічну модель оцінки довіри», яка включає:

- оцінювання оновлень і патчів (відповідно до ISO/IEC 30111:2019 [14]);
- контроль цілісності конфігурації;
- аналіз журналів;
- кореляцію поведінкових аномалій;
- перевірку криптографічних параметрів.

Щоб забезпечити безперервність перевірки, у банківських мережах застосовуються агенти моніторингу або безагентні системи на базі DPI-аналізу трафіку. У межах політики Zero Trust рішення приймається не лише на основі моделі (2), але й на основі історичної поведінки пристрою. Це дозволяє враховувати тенденції (наприклад, погіршення стабільності з'єднання, зміни у профілі трафіку), що підвищує точність оцінювання довіри.

3.3 Порівняльний аналіз каналів передавання відеоданих у контексті Zero Trust

Одним із ключових елементів безпеки є використання захищених каналів передавання. Нижче наведено порівняльну таблицю, складену на основі рекомендацій NIST SP 800-52 [7], RFC 3711 та IEEE досліджень у сфері відеозв'язку.

Таблиця 1

Порівняння каналів передавання даних у банківських IP-відеосистемах

Технологія	Ступінь захищеності	Криптографія	Уразливості	Рівень довіри
RTSP (без TLS)	Низький	Відсутня	Перехоплення, підміна	0,1
RTSP over TLS 1.2	Середній	AES-CBC, RSA	вразливість до атаки MITM при слабких налаштуваннях	0,6
RTSP over TLS 1.3	Високий	AES-GCM, PFS	Низький ризик	0,85
SRTP + DTLS	Дуже високий	AES-GCM 256	Мінімальні ризики, рекомендовано NIST	0,95

Як видно із таблиці, традиційні схеми передавання без шифрування не можуть відповідати вимогам Zero Trust, оскільки не забезпечують доказової безпечності каналу. Саме тому у більшості сучасних банківських мереж застосовується SRTP або повний TLS 1.3 тунель. Це прямо відповідає рекомендаціям ISO та NIST [6–7].

3.4 Аналіз моделі довіри з урахуванням динамічних змін параметрів

Щоб оцінити стійкість моделі T до коливань окремих параметрів, проведемо аналіз чутливості. Нехай початкове значення інтегрального показника дорівнює:

$$T_0 = 0{,}94$$

Розглянемо три сценарії:

a. Зміна поведінкового параметра *P*

Зменшення P з 0.8 до 0.4 (виявлені аномалії) призводить до:

$$\Delta T = T_0\text{-}T' = -0{,}18.$$

Це значення узгоджується з роботами ACM щодо anomaly-based trust scoring [11].

b. Зниження цілісності *I*

Зміна I з 1 до 0:

$$\Delta T = T_0\text{-}T' = -0{,}25.$$

Згідно NIST SP 800-193, це критичний параметр, тому падіння найбільше.

c. Зниження параметра каналу S

Падіння шифрування SRTP → TLS 1.2 дає:

$$\Delta T = T_0\text{-}T' = -0{,}1.$$

Такі зміни цілком узгоджуються з науковою моделлю, оскільки вагові коефіцієнти відображають значимість відповідних параметрів у реальних банківських мережах. Параметри I та A є найбільш критичними, тому саме вони здатні спричинити найбільше зниження T. Подібний підхід рекомендовано IEEE у працях, присвячених trust scoring for IoT devices [4,11].

3.5 Модель адаптивної зміни порогу довіри (Dynamic Trust Threshold)

У реальних умовах поріг довіри T_{min} повинен бути динамічним, а не статичним. NIST RMF та ENISA [2] рекомендують адаптивну систему порогів, яка враховує загальний стан мережі.

Запропонуємо модель:

$$T_{min}(\mathrm{t}) = T_{\mathrm{base}}\text{-}\alpha \mathrm{R}(\mathrm{t}), \qquad (7)$$

де

T_{base} – базовий поріг (0.8),

α – коефіцієнт чутливості,

$\mathrm{R}(\mathrm{t})$ – індекс загального рівня ризику мережі.

Якщо фіксується хвиля атак або збільшується кількість аномалій, система підвищує вимоги до довіри.

Якщо мережа стабільна — поріг знижується до базового рівня.

Це — класична модель із робіт IEEE з аналізу ризику в Zero Trust [4].

3.6 Валідація моделі через стратегію багатофакторного контролю

Для підтвердження коректності моделі T використовується метод *cross-validation control scoring*, рекомендований у NIST SP 800-53 [15].

Перевіряються три фактори:

1. Безпека ключів – PKI, TPM, DICE [8].
2. Цілісність ПЗ – хеш-контроль, secure boot [7].
3. Динамічна поведінка – поведінкові ML-моделі [11].

Лише у випадку успішного проходження усіх перевірок пристрій отримує високий рівень T.

Рис.2. Логічна схема багатофакторної валідації пристрою в Zero Trust

Нижче наведено структурований псевдокод, який демонструє процедуру оцінювання довіри згідно з NIST-орієнтованою моделлю:

```
function ValidateDevice(device):

    # 1. Перевірка безпеки ключів
    key_status = CheckKeySecurity(device)
    if key_status == FAIL:
        return TrustLevel("LOW", reason="Key validation failed")

    # 2. Перевірка цілісності програмного забезпечення
    integrity_status = CheckFirmwareIntegrity(device)
    if integrity_status == FAIL:
        return TrustLevel("LOW", reason="Integrity violation detected")

    # 3. Аналіз поведінкових характеристик
    behavior_score = AnalyzeBehavior(device)
    if behavior_score < BehaviorThreshold:
        return TrustLevel("MEDIUM", reason="Behavioral anomaly detected")

    # Якщо всі перевірки успішні
    return TrustLevel("HIGH", reason="All validations passed")


function CheckKeySecurity(device):
    if validate_X509(device.cert) == false:
        return FAIL
    if TPM_Attestation(device.TPM) == false:
        return FAIL
    if DICE_Attestation(device.HW_root) == false:
        return FAIL
    return OK


function CheckFirmwareIntegrity(device):
    expected_hash = GetReferenceHash(device.model)
    current_hash = HashFirmware(device.firmware)
    if current_hash != expected_hash:
        return FAIL
    if SecureBootStatus(device) == false:
        return FAIL
    return OK


function AnalyzeBehavior(device):
    profile = LoadBaselineBehavior(device)
    current = CaptureTraffic(device, window=5min)
    score = ML_AnomalyDetector(profile, current)
    return Normalize(score)
```

Рис.3. Псевдокод алгоритму багатофакторної валідації

Пояснення до алгоритму

1. Перевірка безпеки ключів
   Включає X.509-верифікацію, TPM-атестацію та оцінку DICE-ланцюга довіри. Цей етап є критичним згідно з рекомендаціями NIST SP 800-63 та Trusted Computing Group [8].
2. Перевірка цілісності ПЗ
   Реалізується через порівняння контрольних сум прошивки та підтвердження механізмів secure boot відповідно до NIST SP 800-193 [7].
3. Аналіз поведінки
   Використовується поведінкова модель, збудована на основі ML-профілювання мережевої активності, відповідно до підходів ACM і IEEE [11].
4. Рішення про рівень довіри
   Якщо всі три групи контролів пройдені — пристрій отримує високий рівень T. Якщо хоча б один контроль провалено — рівень довіри знижується до середнього або низького.

3.7 Формування журналів аудиту для підтвердження рішень PE/PDP

Важливою складовою архітектури Zero Trust є забезпечення повної прозорості та відтворюваності процесів прийняття рішень. Відповідно до вимог ISO/IEC 27002:2022 щодо управління журналами подій та рекомендацій NIST SP 800-92 щодо побудови систем журналювання, кожне рішення, сформоване компонентами Policy Engine (PE) та Policy Decision Point (PDP), повинно супроводжуватися створенням детального аудиторського запису. Такий запис фіксує контекст, причини та результат виконаної дії, що забезпечує підзвітність та об'єктивність моделі Zero Trust у випадку інцидентів безпеки [6], [15].

У системах IP-відеоспостереження банківських установ це має особливе значення, оскільки рішення щодо дозволу або блокування доступу до відеоресурсів можуть впливати на подальше розслідування подій, юридичну доказову базу та безперервність роботи систем фізичної охорони. Саме тому журнали повинні містити повний набір параметрів, що дозволяє відтворити логіку розрахунку рівня довіри T, а також усі допоміжні значення, які брали участь у формуванні рішення PE/PDP.

Типовий аудиторський запис у системах Zero Trust для IP-відеонагляду включає такі елементи:

- часова позначка події з точністю до мілісекунди;
- ідентифікатор пристрою, що проходив оцінювання;
- результати перевірки цілісності, отримані через механізми secure boot та порівняння хеш-сум;
- поведінкові показники, обчислені на основі мережевого профілю;
- розраховане значення інтегрального показника T та відповідність його пороговому значенню T_{min};
- рішення, прийняте PDP (доступ дозволено, заблоковано, ізоляція, обмеження функціональності);
- криптографічні параметри сеансу, якщо вони вплинули на рішення;
- стан мережевого сегменту, у якому знаходиться пристрій;
- посилання на політику, що стала основою рішення (наприклад, ZT-Access-Policy-12).

```
Timestamp: 2024-10-12 10:14:33.812 UTC+2
Device ID: CAM-S3-102
Network Segment: S3 (Critical Zone)
Key Validation: OK (mTLS + TPM Attestation)
Integrity Check: FAILED (I=0, hash mismatch; FW: v1.02 mod.)
Behavioral Profile: Partial deviation detected (P=0.41)
Secure Channel Status: SRTP/AES-GCM (S=0.95)
Policy Applied: ZT-VID-Policy-04
```

```
Trust Score: T = 0.6325 < T_min (0.80)
Decision (PDP): Access Denied
Action (PEP): Device isolation enabled; traffic redirected to quarantine VLAN
Correlation ID: 54f8-ea93-77ac-221b
```

Рис.4. Приклад повного журналу події

Такий формат запису забезпечує можливість детального аналізу ланцюжка прийняття рішення. У разі подальшого розслідування інциденту журнал дозволяє визначити, які саме параметри вплинули на результат, коли були зафіксовані перші відхилення, який стан мережі був на момент події та чи відповідало рішення наявним політикам доступу.

Використання аудиторських журналів у банківських кіберсистемах

1. Аналіз інцидентів.
   У випадку компрометації відеопристрою журнали дозволяють побудувати часову лінію розвитку події та встановити, які саме порушення призвели до втрати довіри. Це відповідає вимогам ISO/IEC 27035 щодо обробки інцидентів.
2. Машинне навчання та поведінкова аналітика.
   Журнали використовуються як тренувальні дані для моделей ML, які покращують точність поведінкового профілю та допомагають адаптувати порогові значення T у реальному часі. Підхід із використанням журналів для ML-моделей підтримується у дослідженнях ACM [11].
3. Оцінювання ризиків.
   NIST SP 800-30 рекомендує включати дані з журналів до процесу ризик-менеджменту для побудови карти вразливостей, визначення рівня впливу та оцінки ймовірності повторення події.
4. Внутрішній аудит банку.
   Журнали дозволяють аудиторам перевірити відповідність політик Zero Trust стандартам ISO/IEC 27001 та встановити, чи були рішення PE/PDP обґрунтованими, пропорційними та технічно коректними.

Окрім цього, структуроване журналювання сприяє формуванню доказової бази з юридичною силою, що може бути використана під час розгляду інцидентів, пов'язаних із неправомірним доступом до відеоданих або саботажем систем охорони.

Висновки

У результаті проведеного дослідження було встановлено, що традиційні підходи до побудови систем відеоспостереження у банківській сфері більше не забезпечують необхідного рівня захисту в умовах сучасного кібернетичного середовища. Використання IP-технологій суттєво підвищує функціональні можливості систем відеонагляду, однак одночасно збільшує площу атаки, роблячи мережеві компоненти потенційною ціллю для зловмисників. У таких умовах застосування архітектури Zero Trust постає не рекомендацією, а об'єктивною необхідністю для забезпечення стійкості систем відеоспостереження банківських установ.

У роботі було сформовано й обґрунтовано інтегральну модель оцінювання рівня довіри до мережевих компонентів, яка враховує п'ять ключових критеріїв: автентичність, цілісність програмного забезпечення, відповідність політикам, поведінкові характеристики та захищеність каналу зв'язку. Сформульована модель дозволяє надати кожному пристрою кількісно вимірюваний показник довіри T, що може бути безпосередньо інтегрований у процес ухвалення рішень у Policy Engine та Policy Enforcement Point. Запропонований математичний апарат забезпечує об'єктивність оцінювання та дозволяє враховувати як статичні, так і динамічні параметри безпеки.

Практичний приклад показав, що модель є чутливою до критичних критеріїв, насамперед до параметрів автентичності й цілісності, що повністю узгоджується з положеннями NIST SP 800-207 та NIST SP 800-193. Падіння цих параметрів призводить до різкого зниження рівня

довіри й автоматичного блокування доступу, що є ключовим принципом Zero Trust. У свою чергу зміни поведінкового профілю або характеристик каналу впливають на показник довіри менш суттєво, але забезпечують раннє виявлення потенційних аномалій.

Додаткові досліджені механізми, такі як мікросегментація мережі, безперервний моніторинг стану пристроїв, динамічно адаптований поріг довіри та багатофакторна валідація через cross-validation scoring, демонструють здатність Zero Trust забезпечувати гнучкий, контекстно залежний контроль доступу, що відповідає вимогам банківської галузі. Побудова журналів аудиту відповідно до ISO/IEC 27002 та NIST SP 800-92 доповнює модель, дозволяючи забезпечити прозорість рішень, юридичну доказовість та можливість інтеграції з інструментами машинного навчання.

Отримані результати підтверджують, що застосування архітектури Zero Trust у системах IP-відеонагляду банківських установ дозволяє суттєво підвищити рівень їхньої кіберстійкості. Формалізована модель оцінювання довіри може бути використана як основа для впровадження автоматизованих рішень з контролю доступу, а також як інструмент для підвищення ефективності управління ризиками в інформаційних системах критичної інфраструктури. Подальші дослідження можуть бути спрямовані на удосконалення поведінкових моделей, розширення кількості параметрів оцінювання, а також розроблення механізмів інтелектуальної адаптації політик безпеки у режимі реального часу.

Список літератури

1. NIST Special Publication 800-207: Zero Trust Architecture. National Institute of Standards and Technology, 2020.
2. ENISA Threat Landscape 2022. European Union Agency for Cybersecurity, 2022.
3. ISO/IEC 27001:2022. Information Security Management Systems — Requirements.
4. Xiao L. et al. Secure IoT Devices in Zero Trust Networks // IEEE Internet of Things Journal. — 2021.
5. Khan S. Video Surveillance Security in Distributed Systems // Computers & Security. — Elsevier, 2020.
6. ISO/IEC 27002:2022. Information Security Controls.
7. NIST SP 800-193. Platform Firmware Resiliency Guidelines. — 2018.
8. Trusted Computing Group. Device Identity Composition Engine (DICE). — 2021.
9. Alrawais A. Security and Privacy in IoT Networks // Wireless Networks. — Springer, 2021.
10. Kolias C. Botnets Targeting IoT Devices // IEEE Communications Surveys & Tutorials. — 2020.
11. Mitchell R. Behavioral Anomaly Detection for IoT // ACM Computing Surveys. — 2021.
12. Conti M. Secure Routing in Distributed Systems. — Elsevier, 2019.
13. ENISA Guidelines: Secure ICT Products. — 2021.
14. ISO/IEC 30111:2019. Vulnerability Handling Processes.
15. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems. — 2020.

Відомості про авторів:

Питайчук Михайло Русланович**, студент,** Харківський національний університет імені В. Н. Каразіна, Україна, email: pytaichuk2020ki11@student.karazin.ua, ORCID: