ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Удосконалення системи захисту технічних каналів передачі інформації приміщення за допомогою систем відео спостереження»

на здобуття освітнього ступеня магістра
зі спеціальності __125 - Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Микита КРОЩЕНКО

Виконав: здобувач вищої освіти групи СЗДМ 61
Микита КРОЩЕНКО

Керівник: НІМЧЕНКО Тетяна
к.т.н. , доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___125-Кібербезпека та захист інформації_____
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Крощенку Микиті Віталійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Удосконалення системи захисту технічних каналів передачі інформації приміщення за допомогою систем відео спостереження»
керівник кваліфікаційної роботи: НІМЧЕНКО Тетяна, к.т.н., доцент
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. №467

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: опорний об'єкт інформаційної діяльності, технічні канали витоку інформації, вимоги до захисту інформації з обмеженим доступом, сучасні засоби багатофакторної ідентифікації та автентифікації користувача при роботі з інформацією з обмеженим доступом.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Захист інформації на об'єктах інформаційної діяльності.
4.2. Огляд методів і засобів ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.
4.3. Розробка та вдосконалення механізмів багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом

5. Перелік графічного матеріалу: ___Презентаційний матеріал на слайдах.

6. Дата видачі завдання 15.10.2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Микита КРОЩЕНКО.

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Тетяна НІМЧЕНКО

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, чотирьох розділів, загальних висновків та переліку посилань. Орієнтовний обсяг роботи становить 98 сторінок; у тексті збережено графічні матеріали, таблиці та структурні схеми. Бібліографічний список налічує 30 позицій.

Метою кваліфікаційної роботи є підвищення ефективності захисту технічних каналів передачі інформації приміщення шляхом удосконалення системи відеоспостереження, застосування засобів відеоаналітики та організаційно-технічних заходів контролю об’єкта інформаційної діяльності.

У роботі проаналізовано роль відеоаналітики в індустрії безпеки, нормативно-правове забезпечення інформаційної безпеки України, порядок проведення обстеження об’єкта з обмеженим доступом, а також підходи до розроблення комплексної системи захисту з використанням IP-відеоспостереження. Обґрунтовано доцільність інтеграції камер спостереження, відеореєстраторів, систем зберігання даних, засобів контролю доступу та процедур кіберзахисту відеоінформації.

Практичне значення результатів полягає у можливості використання запропонованих рішень під час проектування, модернізації та експлуатації систем відеоспостереження на об’єктах інформаційної діяльності, де обробляється інформація з обмеженим доступом.

Апробація:

Т.В. Німченко, М.В. Крощенко, ПЕРСПЕКТИВИ ЗАХИСТУ ПРИМІЩЕНЬ ЗА ДОПОМОГОЮ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.10-11. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ВІДЕОСПОСТЕРЕЖЕННЯ, ВІДЕОАНАЛІТИКА, IP-КАМЕРА, ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ, КОНТРОЛЬ ДОСТУПУ, КІБЕРБЕЗПЕКА.

ABSTRACT

The qualification work consists of an introduction, four sections, general conclusions and a list of references. The approximate volume of the work is 98 pages; figures, tables and structural diagrams are preserved in the text. The reference list contains 30 sources.

The purpose of the qualification work is to improve the effectiveness of protection of technical information transmission channels in premises by improving a video surveillance system, using video analytics tools and applying organizational and technical measures for controlling an information activity facility.

The work analyzes the role of video analytics in the security industry, the regulatory framework for information security in Ukraine, the procedure for inspecting a restricted-access facility, and approaches to developing an integrated protection system based on IP video surveillance. The feasibility of integrating surveillance cameras, video recorders, data storage systems, access control tools and cybersecurity procedures for video information is substantiated.

The practical value of the results lies in their application during the design, modernization and operation of video surveillance systems at information activity facilities where restricted-access information is processed.

Keywords: TECHNICAL INFORMATION PROTECTION, INFORMATION ACTIVITY FACILITY, VIDEO SURVEILLANCE, VIDEO ANALYTICS, IP CAMERA, TECHNICAL INFORMATION LEAKAGE CHANNELS, ACCESS CONTROL, CYBERSECURITY.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ОІД	–	Об’єкт інформаційної діяльності
ІзОД	–	Інформація з обмеженим доступом
ТЗІ	–	Технічний захист інформації
ТКВІ	–	Технічні канали витоку інформації
ОТЗС	–	Об’єкт технічного захисту систем
ТЗО	–	Технічні засоби охорони
ТСО	–	Технічна система охорони
ТЗОС	–	Технічні засоби охоронної сигналізації
ІКМ		Інформаційно-комунікаційна мережа

ВСТУП

Інтенсивне зростання та впровадження інформаційних технологій поступово змінює сучасну реальність, охоплюючи практично всі сфери життєдіяльності людини. Цифрові інструменти стають невід'ємною частиною повсякденного життя, професійної діяльності, освіти, науки, медицини та державного управління. Формування відкритого кіберсередовища сприяє розширенню прав, свобод і можливостей людини, забезпечує швидкий доступ до інформаційних ресурсів, підвищує рівень соціальної взаємодії та мобільності, збагачує суспільний розвиток і створює глобальний інтерактивний простір для обміну ідеями, науковими результатами та інноваційними рішеннями. Завдяки цифровим платформам суттєво зростає роль знань і інформації як стратегічного ресурсу розвитку сучасного суспільства [1-4].

Зазначені процеси також позитивно впливають на діяльність органів державної влади та місцевого самоврядування, стимулюючи їхню підзвітність, ефективність і прозорість. Використання електронних сервісів, відкритих реєстрів і систем електронного урядування сприяє активнішій участі громадян у прийнятті управлінських рішень, підвищує довіру до влади та створює передумови для зменшення корупційних ризиків. У такий спосіб інформаційні технології стають важливим інструментом демократизації суспільних процесів і зміцнення правової держави.

Разом із тим стрімка цифровізація та широке використання інформаційних систем зумовили появу нових викликів і загроз для національної й міжнародної безпеки. Залежність критично важливих процесів від цифрової інфраструктури робить їх уразливими до зовнішнього втручання. Окрім технічних збоїв і ненавмисних інцидентів, дедалі частіше фіксуються цілеспрямовані кібератаки, ініційовані окремими державами, організованими злочинними угрупованнями або приватними особами з політичних, економічних, ідеологічних чи інших

мотивів. Такі дії можуть бути спрямовані як на окремі організації, так і на цілі сектори економіки чи системи державного управління.

Значного поширення набули протиправні дії, пов'язані з несанкціонованим отриманням, накопиченням, обробкою та розповсюдженням персональної інформації, а також із фінансовими махінаціями, крадіжками та шахрайством у мережі Інтернет. З розвитком електронної комерції та дистанційних фінансових сервісів зростає кількість випадків зловживань, що завдають шкоди як окремим громадянам, так і бізнес-структурам. Кіберзлочинна діяльність дедалі частіше має транснаціональний характер, що істотно ускладнює її виявлення, розслідування та притягнення винних осіб до відповідальності, а також створює реальну загрозу інтересам особи, суспільства загалом і держави.

За таких умов однією з ключових проблем сучасності стає забезпечення інформаційної безпеки, зокрема захист даних, які становлять комерційну, службову або іншу охоронювану законом таємницю. Це питання є надзвичайно актуальним як для приватного життя громадян, так і для стабільного функціонування підприємств, установ та організацій незалежно від форми власності й сфери діяльності. Ефективна система захисту інформації повинна поєднувати правові, організаційні та технічні заходи, спрямовані на запобігання несанкціонованому доступу, втраті або спотворенню даних.

До інформації з обмеженим доступом належать управлінські, науково-технічні, фінансові, комерційні та інші відомості, що мають суттєву матеріальну або стратегічну цінність. Їх витік або неправомірне використання може призвести до значних фінансових збитків, підриву ділової репутації, порушення стабільності роботи організацій, втрати конкурентних переваг, а в окремих випадках — створити загрозу безпеці, життю чи здоров'ю людей. Саме тому питання захисту такої інформації потребує комплексного та системного підходу.

Серед усього різноманіття технічних засобів забезпечення інформаційної та фізичної безпеки особливе місце посідають системи відеоспостереження. Камери фіксації зображення широко застосовуються у громадських просторах,

адміністративних і житлових будівлях, на об’єктах критичної інфраструктури, у транспортних системах, а також на приватних територіях. Відеореєстрація стала звичним елементом повсякденного середовища — від банківських установ і торговельних закладів до вуличних просторів та транспортних засобів. Навіть у віддалених або природних зонах контроль може здійснюватися за допомогою сучасних мобільних комплексів та безпілотних літальних апаратів [5-7]..

Відеоспостереження має суттєві переваги порівняно з іншими компонентами охоронних систем, оскільки забезпечує не лише фіксацію факту правопорушення, а й можливість подальшого аналізу подій, встановлення особи правопорушника або ідентифікації об’єкта. Крім того, сама наявність камер часто виконує превентивну функцію, знижуючи ймовірність вчинення протиправних дій. Саме ця функціональна здатність відеоконтролю є предметом дослідження у межах дипломної роботи. Розпізнавання індивідуальних ознак можливе лише за умови належної якості відеозображення, використання сучасних алгоритмів обробки даних, а також за наявності відповідних інформаційних баз даних, що містять параметри, необхідні для коректної та надійної ідентифікації людей або транспортних засобів у реальних умовах експлуатації систем безпеки.

РОЗДІЛ 1.

ВПЛИВ ВІДЕОАНАЛІТИКИ НА ІНДУСТРІЮ БЕЗПЕКИ

Активна цифрова трансформація охоплює практично всі сфери діяльності, пов’язані зі збиранням, обробкою та передаванням інформації. В умовах постійного зростання обсягів даних дедалі більше організацій прагнуть не лише накопичувати інформацію, а й здійснювати її глибокий аналіз з метою отримання структурованих відомостей, що сприяють підвищенню ефективності управління та економічної результативності. Подібна тенденція набула поширення і в галузі фізичної безпеки, де значні масиви даних тривалий час залишалися малозатребуваним побічним результатом функціонування систем контролю доступу та відеоспостереження. На сучасному етапі ситуація суттєво змінюється.

1.1 Історія розвитку відеоспостереження та відеоаналітики

Історія розвитку відеоспостереження та відеоаналітики тісно пов’язана із загальною еволюцією технічних засобів безпеки, засобів передавання інформації та обчислювальної техніки. Поява відеоспостереження була зумовлена потребою у візуальному контролі об’єктів, процесів і територій у реальному часі без безпосередньої присутності людини. Перші системи відеоспостереження виникли у середині XX століття й мали суто експериментальний характер, однак уже на початковому етапі продемонстрували значний потенціал для застосування у сфері безпеки, промисловості та оборони.

Перші відомі системи відеоспостереження були створені у 1940-х роках і використовувалися переважно у військових цілях. Одним із перших прикладів є система, розроблена в Німеччині для спостереження за випробуваннями ракет Фау-2, яка дозволяла передавати відеозображення з камери на монітор оператора. Ці системи були аналоговими, мали низьку роздільну здатність і працювали виключно в режимі реального часу без можливості запису. Основним їх

обмеженням була відсутність засобів збереження відеоінформації, що унеможливлювало подальший аналіз подій [11, 24]..

У 1950–1960-х роках відеоспостереження почало поступово впроваджуватися у цивільній сфері, насамперед для контролю громадських місць, транспортних об’єктів і промислових підприємств. Поява магнітних носіїв інформації та відеомагнітофонів стала ключовим етапом розвитку, оскільки забезпечила можливість запису відеосигналу та його відтворення. Аналогові камери того періоду характеризувалися громіздкими розмірами, високим енергоспоживанням і низькою якістю зображення, проте вже тоді вони дозволяли фіксувати події та використовувати записи як доказову базу.

Подальший розвиток відеоспостереження у 1970–1980-х роках був пов’язаний із широким розповсюдженням замкнених телевізійних систем, відомих як CCTV. Такі системи активно застосовувалися у банках, магазинах, на вокзалах, в аеропортах і на промислових об’єктах. З’явилися перші стандартизовані формати відеосигналу, зокрема PAL і NTSC, що сприяло уніфікації обладнання та спростило його інтеграцію. Відеореєстратори на магнітній стрічці дозволяли зберігати значні обсяги інформації, хоча пошук потрібних фрагментів залишався складним і трудомістким процесом [11, 12]..

На цьому етапі відеоспостереження виконувало переважно пасивну функцію, а ефективність системи значною мірою залежала від уважності оператора, який здійснював безперервний візуальний контроль. Будь-які події фіксувалися лише постфактум, а реагування на інциденти часто відбувалося із запізненням. Водночас саме в цей період сформувалися основні принципи побудови систем відеоспостереження, такі як зонування об’єкта, вибір кутів огляду, резервування обладнання та організація відеоархівів.

Революційні зміни у сфері відеоспостереження відбулися наприкінці 1990-х – на початку 2000-х років із появою цифрових технологій. Перехід від аналогового до цифрового відео став визначальним етапом, що суттєво розширив функціональні можливості систем. Замість відеомагнітофонів почали

використовуватися цифрові відеореєстратори, які здійснювали оцифрування сигналу, його стиснення та збереження на жорстких дисках. Це значно підвищило якість зображення, спростило доступ до архівів і дало змогу реалізувати функції пошуку за часом, датою та подіями.

Подальший розвиток комп'ютерної техніки та мережевих технологій сприяв появі IP-відеоспостереження, яке стало якісно новим етапом еволюції систем безпеки. IP-камери почали передавати відеопотік безпосередньо мережею передачі даних, що дозволило відмовитися від спеціалізованої кабельної інфраструктури та використовувати стандартні локальні й глобальні мережі. Це забезпечило масштабованість систем, централізоване адміністрування та можливість віддаленого доступу до відеоінформації з будь-якої точки світу [14, 21]..

Саме з розвитком цифрових і мережевих технологій розпочався активний етап формування відеоаналітики як окремого напряму. Перші алгоритми відеоаналізу були доволі простими та базувалися на детектуванні руху шляхом порівняння послідовних кадрів. Такі алгоритми дозволяли автоматично запускати запис відео або формувати сповіщення, однак мали низьку стійкість до змін освітлення, погодних умов і фонових перешкод [25-27]..

У 2000–2010-х роках відеоаналітика почала активно розвиватися завдяки зростанню обчислювальних потужностей, появі багатоядерних процесорів і спеціалізованих графічних прискорювачів. Алгоритми аналізу стали складнішими та точнішими, з'явилися функції розпізнавання об'єктів, трекінгу руху, підрахунку людей і транспортних засобів, аналізу поведінкових сценаріїв. Відеоспостереження поступово трансформувалося з інструменту фіксації подій у систему підтримки прийняття рішень.

Важливим етапом у розвитку відеоаналітики стало впровадження методів машинного навчання, а згодом і глибинних нейронних мереж. Ці технології дозволили перейти від жорстко заданих правил до адаптивних моделей, здатних навчатися на великих масивах даних. Завдяки цьому стало можливим

розпізнавання облич, номерних знаків транспортних засобів, визначення статі, віку та емоційного стану людей, а також виявлення складних подій і аномалій у поведінці [28-30]..

Сучасні системи відеоаналітики здатні працювати в режимі реального часу, інтегруватися з іншими підсистемами безпеки та інформаційними системами підприємств, формувати аналітичні звіти та прогнози. Вони широко застосовуються не лише у сфері безпеки, а й у торгівлі, логістиці, транспорті, медицині, промисловості та міському управлінні в рамках концепції «розумного міста». Відеоаналітика використовується для оптимізації бізнес-процесів, аналізу потоків людей і транспорту, підвищення якості обслуговування та зменшення операційних витрат.

Подальший розвиток відеоспостереження та відеоаналітики пов’язується з поширенням технологій штучного інтелекту, обчислень на периферії мережі, хмарних сервісів і інтеграції з великими даними. Зростає роль кібербезпеки та захисту персональних даних, що зумовлює необхідність удосконалення правового регулювання та етичних підходів до використання відеоінформації. У перспективі системи відеоаналітики дедалі більше виконуватимуть превентивну функцію, прогнозуючи розвиток подій і запобігаючи загрозам ще до їх реалізації, що робить їх одним із ключових елементів сучасних комплексних систем безпеки та управління.

Використання відеоаналітики дало змогу по-новому оцінити потенціал відеоданих і стало важливим чинником розвитку рішень у сфері безпеки. У сегменті відеоспостереження аналітичні технології значно розширили перелік прикладних сценаріїв, надавши користувачам інструменти для автоматизованого отримання корисної інформації з відеопотоків, зокрема для підтримки управлінських і бізнес-рішень.

1.2 Перехід до IP-відеоспостереження та мережевих рішень

Паралельно з цим у сфері охоронних систем відбувається перехід від аналогових технологій до мережевих IP-рішень. У системах IP-відеоспостереження широко застосовуються відкриті стандарти, що спрощує процеси інсталяції, масштабування та оновлення обладнання, а також забезпечує сумісність пристроїв різних виробників у межах єдиної системи. Однією з ключових переваг IP-відеокамер є наявність вбудованих механізмів виявлення руху. Детектор руху являє собою програмно-апаратний модуль, призначений для фіксації переміщення об’єктів у зоні спостереження камери. Така функція є базовою формою відеоаналітики, проте вона має низку істотних обмежень. Зміни освітлення, атмосферні опади, механічні коливання камери, а також поява дрібних об’єктів, зокрема птахів або комах, можуть спричиняти значну кількість хибних спрацьовувань. З огляду на це системи з простим виявленням руху найчастіше застосовуються у внутрішніх приміщеннях. Водночас багато виробників ототожнюють відеоаналітику саме з такими вбудованими детекторами [14, 24]..

Разом із тим окремі розробники вкладають у поняття відеоаналітики значно ширший зміст. Сучасний ринок систем безпеки пропонує рішення, побудовані на основі технологій комп’ютерного зору. Такі системи не обмежуються лише спостереженням і збереженням відеоархівів, а здатні в режимі реального часу виявляти потенційно небезпечні ситуації та автоматично інформувати оператора. Це дає змогу суттєво зменшити навантаження на персонал служби безпеки навіть на великих об’єктах, обладнаних сотнями камер, і мінімізувати вплив людського чинника, реалізуючи принцип централізованого контролю. Системи відеоспостереження з комп’ютерним зором здатні автоматично розпізнавати людей, транспортні засоби та різноманітні події, зокрема загоряння, задимлення, залишені предмети або нестандартні дії, а також здійснювати автоматичне

наведення поворотних камер для отримання детальнішого зображення. Уся зафіксована інформація відображається на інтерактивній карті об’єкта.

Аналітична карта разом із деталізованим відеопотоком може виводитися на різні засоби відображення, включно з моніторами, відеостінами, сенсорними терміналами та мобільними пристроями. Пошук подій у відеоархіві здійснюється за низкою параметрів, зокрема за часовими мітками, типом об’єкта, номером камери, характером події або коментарями оператора. Такі системи підтримують роботу з аналоговими та IP-камерами, а також із тепловізійними пристроями, що забезпечує можливість поетапної модернізації вже наявних систем відеоспостереження та розширення їх функціональних можливостей.

1.3 Сутність, функції та алгоритми відеоаналітики

В основі відеоаналітики лежить процес автоматизованого аналізу, обробки та класифікації відеопотоку в режимі реального часу або з мінімальною затримкою. Йдеться не про звичайне виявлення руху в кадрі, а про комплексну інтерпретацію відеоданих із метою розуміння змісту подій, що відбуваються у полі зору камери. Ефективні аналітичні алгоритми використовують не лише зміну піксельних значень між послідовними кадрами, а й додаткові ознаки та контекстну інформацію, що дозволяє значно точніше описувати об’єкти, їх поведінку та взаємодію з навколишнім середовищем [25-30]..

Початковим етапом функціонування будь-якої системи відеоаналітики є отримання відеозображення з камери спостереження. За принципом дії така камера подібна до людського зору, оскільки вона фіксує світловий потік і формує безперервний потік цифрових даних. Якість вихідного зображення, роздільна здатність, частота кадрів і умови освітлення безпосередньо впливають на точність подальшого аналізу. Саме тому на цьому етапі важливе значення мають попередня обробка відео, фільтрація шумів та корекція спотворень.

Подальший аналіз передбачає виділення сцени спостереження та формування моделі фону. Фонова модель відображає статичні елементи зображення, які не змінюються протягом певного часу. Після її визначення будь-які нові або рухомі елементи в полі зору можуть бути оперативно виявлені та відокремлені від статичного оточення. Цей етап є критично важливим, оскільки помилки у побудові фону можуть призводити до появи хибних об’єктів або, навпаки, до втрати значущої інформації.

Наступним кроком є аналіз і порівняння виявлених об’єктів із заздалегідь сформованими класами на основі сукупності характеристик. До таких параметрів належать геометричні розміри, форма, колірні ознаки, швидкість переміщення, напрям і траєкторія руху, а також інші просторово-часові показники. У більш складних системах можуть враховуватися поведінкові шаблони та взаємодія між кількома об’єктами. Обробка цих даних здійснюється із застосуванням алгоритмів комп’ютерного зору, методів машинного навчання та статистичного аналізу, що дозволяє підвищити точність класифікації та адаптивність системи до змін умов спостереження.

1.4 Практичне застосування відеоаналітики у системах безпеки

Важливим напрямом застосування відеоаналітики є забезпечення охорони периметра, де ключовим завданням виступає своєчасне виявлення фактів несанкціонованого проникнення на контрольовану територію в автоматичному режимі. Такі системи здатні відрізняти людину від тварини або випадкових рухів навколишніх об’єктів, що суттєво знижує кількість помилкових тривог. Оперативне виявлення порушення дозволяє значно скоротити час реагування та підвищити загальний рівень безпеки об’єкта.

Крім того, сучасні аналітичні системи надають можливість формування віртуальних зон, контрольних ліній і логічних тригерів у межах поля зору камери. Це дозволяє реалізувати гнучкі сценарії реагування, наприклад, фіксацію перетину забороненої межі, затримку перебування об’єкта в певній зоні або зміну напрямку руху. Завдяки цьому користувач може налаштовувати індивідуальні протоколи сповіщення залежно від конкретних умов експлуатації, типу об’єкта та рівня потенційної загрози.

Узагальнюючи, можна зазначити, що повноцінна відеоаналітика не зводиться до використання простих камер із функцією фіксації руху. Вона являє собою інтелектуальне програмно-апаратне рішення, орієнтоване на глибокий і змістовний аналіз відеоінформації, а не лише на виявлення змін у зображенні. Такий підхід забезпечує значно вищий рівень адаптивності системи, дозволяє враховувати складні умови спостереження та істотно скорочує кількість хибних спрацювань порівняно з традиційними технологіями.

Основна цінність відеоаналітики полягає у її здатності підвищувати оперативність реагування, автоматизувати процеси моніторингу та зменшувати навантаження на оператора. У підсумку це забезпечує користувачеві більш надійний, точний і результативний контроль за безпекою об’єкта, що робить відеоаналітичні системи важливим елементом сучасних комплексів безпеки.

Аналіз відеоданих, або відеоаналітика, являє собою комплекс апаратних і програмних засобів, що базується на сучасних методах комп’ютерного зору, цифрової обробки сигналів та алгоритмах штучного інтелекту і призначений для автоматизованого отримання, інтерпретації та узагальнення інформації з потокового відеосигналу. Такі системи здатні без безпосередньої участі людини виявляти на відео події, сцени та об’єкти відповідно до наперед заданих критеріїв,

правил або моделей поведінки. Основною метою відеоаналітики є перетворення великого обсягу неструктурованих відеоданих у зрозумілу, формалізовану та корисну для прийняття рішень інформацію. Найчастіше відеоаналітика застосовується у системах відеоспостереження з метою підвищення їх ефективності у сферах безпеки, охорони громадського порядку, оптимізації бізнес-процесів, управління інфраструктурою, транспортом, а також під час проведення наукових і прикладних досліджень.

Розвиток відеоаналітичних систем зумовлений стрімким зростанням кількості камер спостереження та обсягів відеоінформації, які неможливо ефективно обробляти виключно силами операторів. Автоматизація аналізу відео дозволяє суттєво підвищити масштабованість систем спостереження, зменшити вплив людського фактору та забезпечити безперервний контроль об’єктів у режимі реального часу. Крім того, відеоаналітика відкриває можливості для прогнозування подій та попередження потенційно небезпечних ситуацій ще на ранніх етапах їх розвитку.

Залежно від поставлених завдань відеоаналіз може реалізовувати одну або декілька базових функцій, які формують основу будь-якої інтелектуальної системи відеоспостереження. Однією з ключових функцій є виявлення об’єктів, яке зазвичай здійснюється з використанням відеодетекторів руху або більш складних алгоритмів сегментації зображення. На відміну від традиційних інфрачервоних датчиків, відеоаналітичні системи забезпечують точну просторову локалізацію цілей, визначення їх контурів і параметрів, а також дають змогу одночасно виділяти, аналізувати та відстежувати декілька об’єктів у межах поля зору однієї або кількох камер. Це особливо важливо для складних сцен з високою щільністю руху.

Наступною важливою функцією є стеження за об’єктами, яке реалізується за допомогою алгоритмів супроводу та трекінгу. Такі алгоритми дозволяють формувати індивідуальні траєкторії руху кожної цілі, аналізувати зміну її положення у часі та зберігати історію переміщень. Стеження може здійснюватися як у межах однієї камери, так і на основі даних, отриманих з кількох камер спостереження, об’єднаних у єдину систему. Це дає змогу відновлювати повний маршрут об’єкта на великій території, що є надзвичайно важливим для задач безпеки та розслідування інцидентів.

Завдяки аналізу траєкторій руху відеоаналітичні системи можуть виявляти поведінкові особливості та відхилення від нормальних сценаріїв. Зокрема, можливе автоматичне визначення аномальних дій, таких як пересування проти основного потоку людей або транспорту, різка зміна напрямку руху, зупинки у нетипових місцях, тривале перебування в одній зоні або переміщення з надмірно високою чи низькою швидкістю. Такі ознаки часто використовуються як індикатори потенційно небезпечної або підозрілої поведінки.

Класифікація об’єктів застосовується для впорядкування результатів аналізу та зменшення кількості нерелевантних або хибних повідомлень. У простих реалізаціях класифікація ґрунтується на геометричних ознаках, пропорціях та габаритах об’єктів, що дозволяє розрізняти людей, групи людей, легкові та вантажні транспортні засоби. Такий підхід дає змогу адаптувати логіку реагування системи залежно від типу виявленого об’єкта. Більш розвинені системи здатні визначати додаткові характеристики, зокрема стать людини, приблизний вік, наявність аксесуарів або належність до певної демографічної групи, що суттєво розширює аналітичні можливості.

Найскладнішим і водночас найбільш технологічно насиченим компонентом відеоаналітики є ідентифікація об’єктів. Сучасні програмні рішення дозволяють

встановлювати особу за біометричними параметрами обличчя, порівнюючи їх з еталонними зразками у базах даних, або ідентифікувати транспортні засоби за номерними знаками, маркою, моделлю та кольором. Процеси ідентифікації потребують високої якості відеозображення, значних обчислювальних ресурсів та використання складних алгоритмів машинного навчання. Окрім суто відеоаналітичних методів, ідентифікація може доповнюватися іншими засобами, зокрема використанням відбитків пальців, банківських карток, електронних пропусків чи ідентифікаторів мобільних пристроїв, що дозволяє створювати багатофакторні системи контролю доступу.

Важливе місце у відеоаналітиці посідає розпізнавання ситуацій і подій. Такі системи здатні не лише виділяти окремі об’єкти, а й аналізувати їх взаємодію між собою та з навколишнім середовищем. Ситуаційна аналітика дозволяє автоматично фіксувати перетин контрольних ліній, входження або вихід із визначених зон, падіння людей, порушення правил паркування, появу залишених або зникнення контрольованих предметів, скупчення людей, а також виявляти ознаки пожежі, задимлення чи інших надзвичайних ситуацій. Завдяки цьому система може не лише реєструвати події, а й оцінювати рівень їх небезпеки та ініціювати відповідні дії.

Сучасні системи відеоспостереження, як правило, будуються за модульним принципом, що забезпечує їх гнучкість та масштабованість. Базовий функціонал може поступово розширюватися інтелектуальними модулями для розпізнавання номерів транспортних засобів, автоматичного керування поворотними камерами, супроводу цілей, міжкамерного трекінгу об’єктів, ідентифікації осіб, аналізу поведінки та формування тривожних сповіщень. Такий підхід дозволяє адаптувати систему до конкретних умов експлуатації та вимог замовника без повної заміни обладнання.

Застосування відеоаналізу сприяє істотному зниженню витрат на відеомоніторинг, оскільки зменшує залежність від постійної присутності оператора та скорочує час реагування на критичні події. Автоматична фільтрація відеоінформації дозволяє зосередити увагу персоналу лише на дійсно важливих інцидентах, ігноруючи рутинні або незначні події. Крім того, завдяки попередній обробці та аналізу даних зменшується навантаження на канали зв'язку та системи зберігання інформації, що є особливо актуальним для великих розподілених систем. У підсумку відеоаналітика виступає ключовим елементом сучасних інтелектуальних систем безпеки, забезпечуючи більш високий рівень контролю, надійності та ефективності управління відеоінформацією.

Разом із численними перевагами системи відеоаналітики мають і низку суттєвих недоліків та обмежень, які необхідно враховувати під час їх проєктування, впровадження та експлуатації. Однією з основних проблем залишаються хибні спрацювання, що виникають через складність і мінливість реальних умов спостереження. До таких умов належать зміни освітлення протягом доби, погодні явища, тіні, відблиски, динамічний фон, велика кількість об'єктів у кадрі, часткові перекриття цілей, а також технічні обмеження самих камер. Хибні тривоги знижують довіру користувачів до системи та можуть призводити до перевантаження операторів, що негативно впливає на загальну ефективність відеомоніторингу. Усунення або мінімізація цієї проблеми можливі шляхом подальшого вдосконалення алгоритмів аналізу, використання адаптивних моделей, поєднання декількох методів детектування, а також коректного налаштування параметрів системи з урахуванням конкретних умов експлуатації. Ще одним обмежувальним чинником є відносно висока вартість впровадження таких систем, яка включає витрати на обладнання, програмне забезпечення, обчислювальні ресурси, зберігання даних та обслуговування.

Розвиток інтелектуальної відеоаналітики здійснюється переважно у двох основних напрямах — трекінгу та ідентифікації об’єктів. Саме на основі правил, моделей і сценаріїв, закладених в алгоритми аналізу, формується функціональність, необхідна для побудови сучасних і ефективних систем відеоспостереження. Поєднання цих напрямів дозволяє не лише фіксувати наявність об’єктів у кадрі, а й відстежувати їхню поведінку, встановлювати взаємозв’язки між подіями та здійснювати глибший аналіз ситуацій.

Трекінг полягає у визначенні положення одного або кількох рухомих об’єктів у часі за даними відеокамери. Алгоритм аналізує послідовність кадрів, встановлює відповідність між об’єктами на суміжних кадрах та визначає їх координати відносно зображення або сцени спостереження. У складних випадках трекінг повинен враховувати зникнення об’єктів з поля зору, їх повторну появу, часткові або повні перекриття іншими об’єктами, зміну масштабу та перспективи. Біометрична ідентифікація, у свою чергу, є методом підтвердження особи або перевірки належності документів їх власнику шляхом розпізнавання та зіставлення біометричних характеристик. До таких характеристик належать риси обличчя, відбитки пальців, геометрія руки, особливості зорового апарату, а також інші унікальні фізіологічні або поведінкові ознаки, що дозволяють з високою ймовірністю встановити особу.

Система візуального спостереження зазвичай включає два ключові етапи обробки інформації: подання та локалізацію цільового об’єкта, а також фільтрацію, узагальнення й інтеграцію отриманих даних. На першому етапі здійснюється виділення об’єкта з відеоряду та визначення його просторових характеристик, тоді як на другому етапі результати аналізу накопичуються, уточнюються та використовуються для формування висновків або прийняття рішень. До задач трекінгу також належить інтелектуальний пошук у відеоархівах, який дозволяє оперативно знаходити необхідні фрагменти відеозапису навіть за

відсутності точної інформації про час або місце події, що істотно підвищує ефективність роботи операторів і служб безпеки.

Ситуаційні відеодетектори з високою точністю розпізнають людей, транспортні засоби та інші об’єкти спостереження, використовуючи сукупність просторових, часових і поведінкових ознак. У режимі реального часу вони здатні виділяти події, пов’язані з переміщенням об’єктів уздовж заданих ліній або в межах визначених зон, а також враховувати часові обмеження та послідовність дій. Серед таких подій можна виокремити перетин контрольної лінії у визначеному напрямку, появу або зникнення об’єкта в зоні спостереження, його зупинку, тривале перебування в зоні, фіксацію залишених або вилучених предметів, а також інші сценарії, що можуть свідчити про потенційну загрозу або порушення встановлених правил.

Окрему групу становлять сервісні детектори, призначені для контролю працездатності та коректного функціонування відеокамер і всієї системи спостереження загалом. Вони дозволяють своєчасно виявляти спроби навмисного пошкодження обладнання, зміну положення камери, перекриття або засмічення об’єктива, втрату фокусування, надмірне засвічування, різку зміну фону чи інші фактори, що погіршують якість відеореєстрації. Використання таких детекторів підвищує надійність системи та дозволяє оперативно реагувати на технічні несправності.

Детектори так званих «теплих» і «холодних» зон використовуються переважно у сфері торгівлі, маркетингу та управління простором для аналізу поведінки відвідувачів. Вони дають змогу визначати ділянки з найбільшою концентрацією уваги клієнтів, оцінювати інтенсивність потоків людей та тривалість їх перебування в різних зонах. Отримані дані можуть використовуватися для оптимізації розташування товарів, планування

торговельних площ, оцінювання ефективності рекламних кампаній і прийняття управлінських рішень.

Відеодетектори не замінюють оператора повністю, а виконують допоміжну та підтримувальну функцію, привертаючи його увагу до потенційно небезпечних або нестандартних ситуацій. Повна автоматизація процесу виявлення та оцінки порушень наразі є неможливою через імовірнісний характер алгоритмів та складність реальних сценаріїв. Це необхідно враховувати під час проєктування систем відеоспостереження з функціями відеоаналізу, забезпечуючи раціональний розподіл завдань між автоматизованими модулями та людиною-оператором.

Розпізнавання номерних знаків транспортних засобів є однією з найбільш затребуваних і практично важливих функцій сучасних систем відеоспостереження. За умови правильної побудови, розташування камер і коректного налаштування програмного забезпечення можна досягти високої точності розпізнавання навіть у складних умовах. Водночас залишаються ситуації, пов’язані з забрудненням номерів, складними погодними умовами або нестандартними шрифтами, які потребують участі оператора для прийняття остаточних рішень у разі помилкового допуску або відмови.

Функціональні можливості систем відеоспостереження з відеоаналітикою постійно розширюються, що сприяє зростанню сфер їх застосування. Окрім завдань безпеки, відеоаналіз активно використовується для підрахунку об’єктів, аналізу розподілу людей з побудовою теплових карт, виявлення скупчень, оцінювання завантаженості приміщень і територій, а також для оптимізації транспортних потоків та управління інфраструктурою.

До перспективних напрямів розвитку відеоаналітики належать прогнозування поведінки об’єктів або виникнення подій на основі накопичених даних, інтелектуальне стиснення відеоконтенту з урахуванням інтересів користувача, пріоритизація подій за рівнем важливості, формування похідних відеоданих для аналітики та автоматичне видалення або анонімізація персональної інформації з відеоряду з метою дотримання вимог конфіденційності.

На початкових етапах створення автоматизованих відеоінформаційних систем ефективним і економічно доцільним інструментом є комп’ютерне моделювання, яке передбачає використання програмних засобів як віртуальних моделей реальних систем. Моделювання дозволяє досліджувати поведінку алгоритмів, оцінювати їх ефективність, виявляти слабкі місця та оптимізувати параметри ще до впровадження системи в реальних умовах.

Найбільш актуальними завданнями, що вирішуються засобами відеоаналітики, залишаються детектування подій, розпізнавання номерів транспортних засобів та ідентифікація облич. Системи відеоспостереження дозволяють організувати контроль об’єктів різного рівня складності — від невеликих приміщень до масштабних інфраструктурних комплексів, при цьому робота оперативного персоналу не потребує високої спеціалізованої підготовки завдяки інтуїтивним інтерфейсам та автоматизованим засобам підтримки прийняття рішень.

Для запису та зберігання відеоданих застосовуються як спеціалізовані цифрові відеореєстратори, так і персональні комп’ютери з платами відеозахоплення. Відеореєстратори поєднують функції мультиплексування, виявлення руху, архівування та передавання даних мережею, забезпечуючи компактність і відносну простоту експлуатації. Комп’ютерні системи, у свою

чергу, характеризуються ширшими функціональними можливостями, вищою продуктивністю, гнучкістю налаштувань і можливістю створення великих відеоархівів, що робить їх доцільними для використання у складних і масштабних системах відеоспостереження з розвиненою відеоаналітикою.

Конкурентоспроможною альтернативою традиційним аналоговим системам є мережеві системи IP-відеоспостереження, побудовані на основі цифрових IP-камер. Такі системи використовують наявну локальну або глобальну мережеву інфраструктуру, що дає змогу істотно скоротити витрати на прокладання окремих кабельних ліній і спростити процес інтеграції відеоспостереження в загальну інформаційну систему підприємства або організації. IP-камери забезпечують передачу відеоданих у цифровому форматі, що дозволяє зберігати високу якість зображення на всіх етапах обробки, масштабувати систему без значних апаратних змін та здійснювати централізоване адміністрування з будь-якого комп’ютера або серверного вузла, підключеного до мережі. Попри вищу початкову вартість у порівнянні з аналоговими рішеннями, подальший розвиток технологій, здешевлення компонентів і зростання масового виробництва сприяють поступовому підвищенню доступності IP-систем і розширенню сфер їх застосування.

Відеоспостереження може реалізовуватися у різних формах і конфігураціях залежно від функціонального призначення, масштабів об’єкта та умов експлуатації. Одним із найбільш поширених напрямів є охоронне відеоспостереження, орієнтоване насамперед на забезпечення фізичної безпеки об’єктів, контролю доступу та запобігання несанкціонованим діям. Така система, як правило, включає сукупність відеокамер різного типу, засобів обробки та аналізу відеосигналів, пристроїв відображення інформації для операторів, а також модулів запису, архівування і зберігання відеоданих. Побудова системи відеоспостереження для центральних зон, прилеглих територій і внутрішніх

приміщень здійснюється із застосуванням керованих високочутливих камер, які можуть призначатися як для внутрішнього, так і для зовнішнього монтажу з урахуванням вимог до захисту від пилу, вологи та механічних впливів.

Охоронне відеоспостереження забезпечує безперервний контроль за визначеною зоною у денний і нічний час завдяки використанню інфрачервоного підсвічування, високочутливих матриць та алгоритмів покращення зображення. Важливою функцією є можливість автоматичного запису відеоінформації у разі спрацювання датчиків руху або програмних відеодетекторів, що дозволяє суттєво зменшити обсяг архівних даних і зосередитися на фіксації лише значущих подій. У поєднанні з відеоаналітикою такі системи можуть автоматично формувати тривожні сповіщення та передавати їх відповідальним особам у режимі реального часу.

Окрему групу становить технологічне або промислове відеоспостереження, яке використовується на виробничих об’єктах, підприємствах енергетики, транспорту, гірничодобувної промисловості та інших галузях із підвищеними вимогами до надійності обладнання. Для таких умов застосовуються камери у спеціальних захищених корпусах, здатні стабільно функціонувати за підвищених або знижених температур, у запиленому чи агресивному середовищі, за наявності постійних вібрацій та під впливом несприятливих метеорологічних факторів. Основною вимогою до таких систем є безперервність роботи, стійкість до зовнішніх впливів і мінімальна потреба в обслуговуванні, оскільки зупинка відеоконтролю на промисловому об’єкті може призвести до серйозних виробничих або техногенних ризиків.

Подальший розвиток систем відеоспостереження нерозривно пов’язаний із активним упровадженням елементів штучного інтелекту, машинного навчання та глибинних нейронних мереж. Це дозволяє перейти від традиційного пасивного

спостереження, коли оператор лише фіксує події, до інтелектуального управління безпекою об’єкта. Сучасні системи здатні не лише реєструвати відеоподії у режимі реального часу, а й здійснювати глибокий аналіз поведінкових моделей людей і транспортних засобів, визначати відхилення від нормального сценарію, виявляти підозрілі дії, прогнозувати можливі загрози та пропонувати варіанти реагування.

Завдяки використанню інтелектуальних алгоритмів значною мірою автоматизується процес прийняття рішень у системах безпеки. Система може самостійно класифікувати події за рівнем небезпеки, відокремлювати помилкові або незначущі спрацювання від реальних загроз і передавати оператору лише релевантну та пріоритетну інформацію. Це істотно знижує психологічне та інформаційне навантаження на персонал служби безпеки, мінімізує ризик пропуску критичних подій і підвищує загальну ефективність контролю, особливо на великих об’єктах із розгалуженою інфраструктурою та значною кількістю зон спостереження.

Крім того, інтелектуальні системи відеоспостереження забезпечують можливість інтеграції з іншими підсистемами безпеки, такими як системи контролю доступу, охоронної та пожежної сигналізації, обліку робочого часу або управління будівлями. Така інтеграція формує єдиний інформаційний простір, у межах якого всі події аналізуються комплексно, що підвищує оперативність реагування та дозволяє більш ефективно управляти ресурсами. У довгостроковій перспективі розвиток таких систем сприятиме створенню адаптивних, самонавчальних комплексів безпеки, здатних самостійно підлаштовуватися під зміну умов експлуатації та рівень потенційних загроз.

Особливе значення відеоаналітика набуває у комплексі з іншими підсистемами безпеки, такими як системи контролю та управління доступом,

охоронна і пожежна сигналізація, інженерні та технологічні датчики, системи моніторингу навколишнього середовища, а також автоматизовані системи управління будівлями. Інтеграція всіх цих компонентів у єдину інформаційно-аналітичну платформу дозволяє формувати цілісну, узгоджену та максимально повну картину подій на об’єкті в режимі реального часу. У такій системі відеоаналітика виконує роль центрального елемента візуального підтвердження подій, доповнюючи та уточнюючи сигнали, що надходять від інших підсистем.

Наприклад, поєднання даних відеоспостереження з інформацією про доступ до приміщень дає змогу не лише зафіксувати сам факт порушення, а й детально встановити його причини, послідовність дій, коло причетних осіб та можливі наслідки. Якщо система контролю доступу фіксує несанкціоноване відкриття дверей, відеоаналітика дозволяє миттєво візуально перевірити ситуацію, ідентифікувати особу, оцінити її поведінку та передати оператору повну інформацію для прийняття обґрунтованого рішення. Такий підхід значно підвищує оперативність реагування та зменшує ймовірність помилкових або запізнілих дій.

Значною перевагою сучасних систем відеоспостереження є можливість накопичення, систематизації та тривалого зберігання великих масивів відеоданих із можливістю швидкого доступу до них. Архівні записи використовуються не лише для розслідування інцидентів, аналізу конфліктних ситуацій і підтвердження фактів правопорушень, а й для глибокої аналітичної оцінки ефективності організації безпеки загалом. На основі накопичених даних можуть формуватися статистичні звіти, що відображають частоту виникнення подій, часові піки активності, типові сценарії порушень або зони підвищеного ризику.

Аналіз таких статистичних даних дозволяє виявляти слабкі місця у системі охорони, коригувати схеми розміщення відеокамер, оптимізувати маршрути

пересування охоронного персоналу, удосконалювати пропускний режим і приймати обґрунтовані управлінські рішення. У довгостроковій перспективі це сприяє не лише підвищенню рівня безпеки, а й зменшенню експлуатаційних витрат завдяки більш раціональному використанню технічних і людських ресурсів.

У навчальних закладах, адміністративних будівлях і спеціалізованих об’єктах з обмеженим доступом відеоаналітика набуває дедалі більшого значення не лише як елемент системи безпеки, а і як ефективний інструмент організаційного та управлінського забезпечення діяльності установи. Її використання дозволяє отримувати об’єктивну та систематизовану інформацію про реальні процеси, що відбуваються всередині будівель і на прилеглих територіях, без необхідності постійної присутності відповідального персоналу. Завдяки автоматизованому аналізу відеоданих адміністрація отримує можливість приймати обґрунтовані управлінські рішення на основі фактичних показників, а не суб’єктивних оцінок.

Одним із важливих напрямів застосування відеоаналітики є контроль наповненості аудиторій, залів, коридорів і допоміжних приміщень. Система може автоматично визначати кількість людей у приміщенні в різні часові проміжки, фіксувати пікові навантаження та періоди мінімальної активності. Такі дані є надзвичайно корисними для оптимізації використання навчальних і робочих площ, планування розкладів занять, нарад або інших заходів, а також для раціонального розподілу потоків відвідувачів і персоналу. У результаті зменшується перевантаження окремих зон і підвищується загальний комфорт перебування людей у будівлі.

Відеоаналітика також забезпечує можливість відстеження дотримання встановлених правил поведінки та внутрішнього розпорядку. Це може

стосуватися контролю доступу до окремих приміщень, фіксації перебування сторонніх осіб у зонах з обмеженим доступом, а також виявлення порушень дисципліни. У навчальних закладах такі функції дозволяють аналізувати своєчасність відвідування занять, переміщення студентів між корпусами, дотримання встановлених маршрутів руху, що особливо актуально для великих кампусів або багатоповерхових будівель зі складною планувальною структурою.

Аналіз інтенсивності переміщення студентів, викладачів і обслуговуючого персоналу в різні часові періоди дає змогу оцінити ефективність організації навчального або робочого процесу. На основі таких даних можна виявляти нераціональні маршрути руху, перевантажені переходи чи коридори, а також визначати потребу в зміні логістики всередині будівлі. Це сприяє підвищенню рівня безпеки, скороченню часу на переміщення та загальному покращенню умов праці й навчання.

Отримана за допомогою відеоаналітики інформація може використовуватися для вдосконалення управлінських рішень, підвищення рівня дисципліни та формування більш безпечного і комфортного середовища. Зокрема, результати аналізу дозволяють коригувати розклади занять, оптимізувати навантаження на аудиторний фонд, визначати потребу в додаткових заходах контролю або, навпаки, зменшувати надмірні обмеження. Таким чином, відеоаналітика стає інструментом комплексного управління ресурсами закладу.

Окрім організаційних завдань, важливу роль відеоаналітика відіграє у сфері забезпечення безпеки та охорони праці. Системи здатні автоматично виявляти потенційно небезпечні ситуації, зокрема скупчення людей у вузьких проходах, коридорах або на сходових клітинах, що може призводити до підвищення ризику травмування. Також можливе фіксування випадків блокування евакуаційних

виходів, захаращення проходів або порушення правил пожежної безпеки, що є критично важливим у разі виникнення надзвичайних ситуацій.

Своєчасне виявлення таких факторів дозволяє оперативно реагувати на потенційні загрози, вживати профілактичних заходів і запобігати розвитку небезпечних сценаріїв. У цьому контексті відеоаналітика виконує не лише функцію контролю, а й стає ефективним засобом превентивного управління безпекою. Вона дає змогу мінімізувати ризики для життя та здоров'я людей, підвищити рівень готовності об'єкта до надзвичайних ситуацій і забезпечити дотримання нормативних вимог у сфері охорони праці та пожежної безпеки.

Таким чином, використання відеоаналітики у навчальних і адміністративних будівлях сприяє підвищенню ефективності управління, оптимізації внутрішніх процесів і створенню безпечного, контрольованого та комфортного середовища. Її впровадження дозволяє перейти від реактивних заходів до системного та превентивного підходу в організації діяльності об'єктів з масовим перебуванням людей та обмеженим доступом.

Окрему увагу під час впровадження систем відеоспостереження необхідно приділяти питанням надійності, відмовостійкості та безперервності їх функціонування. Для об'єктів із підвищеними вимогами до безпеки обов'язковими є резервування серверного обладнання, каналів передачі даних, мережевих компонентів і систем зберігання інформації. Використання кластерних рішень, дублювання ключових вузлів і впровадження автоматичного перемикання у разі відмови забезпечують стабільну роботу системи навіть за аварійних умов.

Важливу роль відіграє застосування джерел безперебійного живлення та резервних систем електропостачання, які гарантують працездатність

відеоспостереження у разі аварійних або планових відключень електроенергії. Безперервність функціонування системи є критично важливою для підтримання постійного контролю за обстановкою, особливо на стратегічних, інфраструктурних або соціально значущих об’єктах.

Не менш важливим аспектом є захист відеоінформації від несанкціонованого доступу, внутрішніх зловживань і зовнішніх кібератак. Сучасні системи відеоспостереження повинні використовувати криптографічні засоби захисту даних, шифрування відеопотоків і архівів, багаторівневу автентифікацію користувачів та чітке розмежування прав доступу. Це дозволяє запобігти витоку конфіденційної інформації, підміні відеоданих або несанкціонованому видаленню архівних записів, що особливо важливо у випадках використання системи для контролю приміщень із обмеженим доступом або обробки чутливої інформації.

Окрім технічних заходів захисту, важливе значення мають організаційні аспекти, зокрема регламентація доступу персоналу до системи, ведення журналів подій, аудит дій користувачів і регулярне оновлення програмного забезпечення. Комплексний підхід до забезпечення інформаційної безпеки дозволяє значно підвищити надійність системи та знизити ризики компрометації даних.

Отже, аналітичне відеоспостереження є одним із ключових елементів сучасних комплексних систем безпеки. Його впровадження забезпечує не лише підвищення рівня захисту об’єктів і своєчасне виявлення загроз, а й сприяє оптимізації управлінських процесів, зменшенню впливу людського фактора та раціональному використанню матеріальних, технічних і людських ресурсів. За умови грамотного проєктування, правильної інтеграції з іншими підсистемами та належної експлуатації такі системи стають ефективним інструментом превентивного захисту, що дозволяє підтримувати стабільне, контрольоване й

безпечне функціонування об’єктів із підвищеними вимогами до безпеки в умовах сучасних викликів і загроз.

Класифікація відеокамер

Основним функціональним елементом будь-якої системи відеоспостереження є відеокамера, яка забезпечує безпосереднє отримання візуальної інформації про об’єкт спостереження та формує первинні дані для подальшої обробки, зберігання й аналізу. Саме від технічних характеристик відеокамери, її надійності та відповідності умовам експлуатації значною мірою залежить ефективність усієї системи відеоспостереження. Під час проєктування таких систем особливо важливим є комплексний підхід до вибору типу камер, визначення оптимальних місць їх встановлення, висоти монтажу та кутів огляду. Як правило, відеокамери монтують у важкодоступних і максимально високих точках, що дозволяє суттєво розширити сектор огляду, зменшити кількість «сліпих зон» і унеможливити їх умисне пошкодження або виведення з ладу зловмисниками.

На сучасному ринку систем відеоспостереження представлені два базові типи камер — аналогові та цифрові, які, у свою чергу, можуть бути як дротовими, так і бездротовими. Аналогові камери є простішими за конструкцією та тривалий час використовувалися як стандартне рішення, однак їх можливості обмежені рівнем роздільної здатності та функціональністю. Цифрові камери, навпаки, забезпечують високу якість зображення, підтримують передачу даних мережею

та дозволяють використовувати сучасні алгоритми відеоаналітики, що робить їх більш перспективними для складних і масштабних систем безпеки.

За умовами експлуатації відеокамери поділяються на вуличні та внутрішні. Вуличні (зовнішні) камери призначені для роботи в умовах впливу навколишнього середовища, тому оснащуються міцними захисними корпусами або кожухами, які забезпечують стабільну роботу при значних коливаннях температури, підвищеній вологості, впливі пилу та атмосферних опадів. Такі камери часто мають антивандальний захист, стійкість до механічних ударів і вбудоване інфрачервоне підсвічування для ефективного нічного спостереження. З огляду на значну віддаленість від пунктів спостереження або серверних приміщень, вуличні камери повинні забезпечувати стабільну передачу відеосигналу на великі відстані без істотної втрати якості. За конструктивним виконанням вони можуть бути купольними, циліндричними або поворотними, що дозволяє обирати оптимальний варіант залежно від конфігурації території. У деяких випадках для зовнішнього спостереження допускається використання внутрішніх камер, поміщених у спеціальні герметичні захисні кожухи.

Відеокамери для приміщень (внутрішні) мають компактніші габарити та конструктивно орієнтовані на гармонійне поєднання з інтер’єром. Їх корпус зазвичай виготовляється з пластику або легких сплавів і не потребує високого рівня герметичності. Кріплення таких камер розраховані на менші механічні навантаження, а додаткові захисні елементи, зокрема сонцезахисні козирки чи посилені кронштейни, як правило, відсутні. Водночас внутрішні камери часто оснащуються ширококутними об’єктивами, що дозволяє контролювати значні площі приміщень із мінімальною кількістю пристроїв.

За способом передачі кольору відеокамери поділяються на чорно-білі, кольорові та камери типу «день/ніч». Чорно-білі камери формують зображення

без передачі кольору, проте характеризуються високою світлочутливістю та здатні працювати за мінімального рівня освітленості, що робить їх придатними для умов слабкого світла. Кольорові камери забезпечують передачу кольорового зображення, однак вимагають достатнього освітлення для коректної роботи. Камери типу «день/ніч» поєднують переваги обох рішень і автоматично переходять у чорно-білий режим при зниженні освітленості, забезпечуючи високу деталізацію зображення як удень, так і вночі. Саме цей тип камер є найбільш універсальним і широко застосовується для зовнішнього та внутрішнього відеоспостереження.

За форм-фактором розрізняють циліндричні (Bullet), корпусні (Box), модульні, мініатюрні, купольні (Dome), поворотні (PTZ) та панорамні камери типу «риб'яче око». Циліндричні камери являють собою герметичні пристрої з вбудованим об'єктивом і часто оснащуються інфрачервоним підсвічуванням та регульованим кронштейном для точного налаштування напрямку огляду. Корпусні камери зазвичай постачаються без об'єктива, що дозволяє гнучко підібрати оптичну систему з необхідними характеристиками. Модульні камери виконані у вигляді відкритої плати без корпусу та використовуються переважно для прихованого або вбудованого спостереження. Мініатюрні камери мають надкомпактні розміри й застосовуються у випадках, коли необхідна мінімальна помітність пристрою. Купольні камери відрізняються універсальністю монтажу, захищеністю та естетичним виглядом, а поворотні PTZ-камери забезпечують дистанційне керування напрямком огляду, нахилом і масштабуванням зображення. Камери з об'єктивом «риб'яче око» дозволяють отримати панорамне або кругове зображення контрольованої зони, зменшуючи потребу у встановленні кількох окремих камер.

За ступенем захищеності відеокамери класифікують на пиловологозахищені, антивандальні та вибухозахищені. Пиловологозахист

позначається індексом IP, де числові значення визначають рівень захисту від проникнення пилу та вологи. Антивандальні камери мають індекс IK, що характеризує їхню стійкість до механічних ударів і навмисних пошкоджень. Вибухозахищені камери з маркуванням Ex призначені для використання у вибухонебезпечних середовищах, таких як промислові підприємства, склади горючих матеріалів або об’єкти нафтохімічної галузі.

За способом передачі сигналу розрізняють провідні та бездротові камери. Провідні рішення є традиційними, стабільними та надійними і можуть використовувати оптоволоконні лінії, виту пару або коаксіальний кабель. Оптоволокно застосовується в територіально розподілених системах для передачі сигналу на десятки кілометрів без підсилювачів, вита пара використовується як економічно доцільне та захищене рішення, а коаксіальний кабель забезпечує просту й стабільну передачу сигналу на відстані до кількох сотень метрів. Бездротові камери не потребують прокладання кабельних трас, спрощують монтаж і передають дані через мережеві протоколи за умови наявності стабільного живлення та маршрутизатора, що робить їх зручними для тимчасових або мобільних систем відеоспостереження.

За технологією перетворення сигналу в зображення камери поділяються на аналогові та цифрові (IP). Аналогові камери працюють у форматі CVBS або в удосконалених форматах AHD, TVI та CVI, які забезпечують передачу відео з мегапіксельною роздільною здатністю на значні відстані без затримок. Ці формати дозволяють модернізувати існуючі аналогові системи шляхом часткової заміни камер і використання гібридних відеореєстраторів. Цифрові IP-камери мають вбудований кодер і передають вже оброблений цифровий потік по мережевих кабелях або бездротових каналах зв’язку. Вони забезпечують високу якість зображення, гнучкість масштабування та простоту інтеграції з

комп’ютерними системами, проте є дорожчими та несумісними з класичними аналоговими рішеннями.

Аналогові системи відеоспостереження історично стали першими і до сьогодні широко застосовуються завдяки простоті, надійності та невисокій вартості. Аналогові відеокамери перетворюють світловий потік, сфокусований на світлочутливій матриці, у електричний відеосигнал, що передається на пристрої відображення або запису. Незважаючи на обмежені можливості порівняно з цифровими системами, аналогові рішення залишаються актуальними, зокрема через значну кількість уже встановленого обладнання та його безперебійну роботу. Аналогові камери можуть бути провідними або безпровідними, причому останні зазвичай використовуються для тимчасових систем спостереження, тоді як провідні — для постійного зовнішнього контролю об’єктів.

Основними характеристиками, за якими оцінюється аналогова відеокамера, є сукупність технічних і експлуатаційних параметрів. До них належить світлочутливість, що визначає мінімальний рівень освітлення, за якого можливе впевнене розпізнавання об’єктів у кадрі, а також динамічний діапазон, який характеризує здатність камери одночасно коректно відтворювати яскраві та затемнені ділянки зображення. Важливу роль відіграє кут огляду, що визначає просторове охоплення контрольованої зони, а також параметри електроживлення, зокрема робоча напруга та споживана потужність. Додатково враховується підтримуваний телевізійний стандарт формування відеосигналу, тип зображення (кольоровий або монохромний), роздільна здатність, яка визначає деталізацію картинки, та співвідношення сигналу до шуму, що впливає на чіткість і стабільність відеопотоку. Серед виробників аналогового відеообладнання, продукція яких набула широкого поширення, доцільно відзначити такі компанії, як Dahua, HikVision та Atis.

Аналогові відеокамери мають низку переваг, що обумовлюють їх подальше використання у багатьох системах безпеки. Передусім це відносно невисока вартість обладнання та сумісність компонентів різних виробників, що спрощує модернізацію або розширення системи. Процес інсталяції таких камер не потребує складних технічних рішень, а запис відео здійснюється без втрати часових фрагментів. Налаштування параметрів зазвичай реалізується через вбудоване меню, що робить експлуатацію зрозумілою для персоналу. Крім того, передбачена можливість підключення мікрофонів, а також доступний широкий вибір змінної відеооптики для різних умов спостереження.

Водночас аналогові системи відеоспостереження мають і суттєві обмеження. Кількість камер, які можуть стабільно функціонувати в межах однієї мережі, зазвичай є невеликою. Відсутність механізмів шифрування знижує рівень захищеності переданих даних, а прокладені поруч кабельні лінії можуть створювати електромагнітні завади. Роздільна здатність зображення залишається відносно низькою, а відтворення відео на персональному комп’ютері можливе лише за наявності додаткового обладнання. Такі системи не забезпечують віддаленого перегляду через мережу Інтернет, а для передачі аудіосигналу необхідне прокладання окремого кабелю. Крім цього, відсутні функції цифрового масштабування та дистанційного керування рухом камери через один канал зв’язку.

Цифрові системи відеоспостереження становлять якісно новий етап розвитку галузі. Ключовою їх особливістю є можливість передавання відеозображення на будь-які обчислювальні пристрої за допомогою різноманітних телекомунікаційних мереж. Для цього цифрові камери використовують міжмережевий протокол IP, у межах якого інформація передається у вигляді цифрового потоку через Ethernet-мережі або бездротові канали зв’язку. Порівняно з аналоговими рішеннями такі камери забезпечують

значно вищу якість зображення. Хоча на початкових етапах розвитку цифрові системи поступалися за стабільністю, стрімке зростання роздільної здатності та кількості мегапікселів призвело до суттєвого підвищення їх ефективності, що робить їх особливо придатними для завдань ідентифікації осіб і подій.

Цифрові системи доцільно застосовувати в умовах необхідності оперативного контролю значних територій, оскільки швидкість обробки та передавання даних у таких пристроях є вищою, ніж у аналогових. Сучасні технології дозволяють миттєво перетворювати відеосигнал у цифрову форму та передавати його на сервери або реєстратори з використанням стандартних комунікаційних кабелів. Додатковою перевагою є можливість одночасної обробки інформації з кількох камер, її паралельного відображення на моніторах та збереження на жорстких дисках.

До основних переваг цифрових камер належить передавання сигналу без спотворень, висока деталізація зображення, можливість перегляду в режимі реального часу з будь-якого пристрою та організація віддаленого доступу. Передача даних від кількох камер може здійснюватися одним кабелем, що спрощує інфраструктуру мережі, а кількість підключених пристроїв може досягати десятків або сотень. Додатково підтримується бездротове з’єднання, живлення через мережевий кабель за технологією PoE, автономна робота без використання окремого відеореєстратора, а також передача відео і звуку в межах одного каналу.

Разом з тим цифрові системи мають і певні недоліки. Їх впровадження потребує значних фінансових витрат, а зберігання великих обсягів відеоданих вимагає збільшених ресурсів пам’яті. У процесі передавання інформації можлива незначна затримка, а монтаж і налаштування системи зазвичай потребують участі

кваліфікованих фахівців. Крім того, якість і швидкість трансляції відео значною мірою залежать від рівня завантаженості мережі.

Для забезпечення безпеки на масштабних об’єктах широкого застосування набули камери з поворотним механізмом. Такі пристрої дозволяють контролювати значні площі без зміни фокусної відстані об’єктива, а керування напрямком огляду може здійснюватися як у ручному режимі, так і за заздалегідь заданими сценаріями. Використання подібних камер забезпечує ефективний нагляд за персоналом у службових приміщеннях, торговельних залах або на виробничих ділянках.

Купольні цифрові камери монтуються на стелі та мають напівсферичну форму, що забезпечує широкий панорамний огляд. Завдяки роботі трансфокатора та високій швидкості повороту механізму досягається майже повне охоплення простору. Незважаючи на відносно високу вартість, такі пристрої гарантують якісний контроль у режимі реального часу. Вони придатні для використання як у приміщеннях, так і на відкритих територіях, а наявність інфрачервоного підсвічування дозволяє здійснювати спостереження в умовах недостатнього освітлення та в нічний період.

Також у системах відеоспостереження застосовуються міні-відеокамери. Використання мініатюрних камер є доцільним у випадках, коли необхідно організувати приховане спостереження за об’єктом або окремою особою. Такі пристрої характеризуються надзвичайно малими габаритами та, як правило, маскуються під елементи інтер’єру. У міні-камерах використовується цифрова оптика типу «вушко голки» з діаметром об’єктива до 1 мм. Незважаючи на відносно невисоку роздільну здатність, її характеристик достатньо для виконання завдань, пов’язаних із прихованим відеоконтролем, що відповідає специфіці застосування таких пристроїв.

IP-відеокамери є різновидом цифрових камер відеоспостереження, ключовою особливістю яких є передача відеопотоку у цифровому форматі через мережі Ethernet і Token Ring з використанням протоколу IP. Такі камери мають можливість підключення до локальних і глобальних мереж, зокрема LAN, WAN та бездротових мереж Wi-Fi. IP-камери виконують не лише функцію запису відео, але й є сучасними мережевими передавачами, що забезпечують трансляцію відеоданих у будь-яку точку світу за допомогою інтернет-протоколів.

Більшість сучасних IP-камер оснащені додатковими функціональними можливостями, серед яких наявність вбудованого мікрофона для запису звуку, датчиків руху, можливість підключення зовнішніх спеціалізованих датчиків, а також автоматичне надсилання повідомлень електронною поштою у разі виникнення подій. Асортимент IP-камер на сучасному ринку представлений великою кількістю виробників, кожен з яких пропонує широкий модельний ряд. Серед найбільш відомих компаній доцільно виділити Samsung, Hikvision, Dahua, Axis, Panasonic, D-Link, Atis, Smartec та низку інших.

Кількість користувачів IP-відеокамер постійно зростає, і для багатьох споживачів такі системи вже стали не інноваційним рішенням, а необхідним інструментом забезпечення безпеки. Для роботи з IP-камерами можуть використовуватися як стандартні веб-браузери, так і спеціалізоване програмне забезпечення для мережевого відеоспостереження, яке зазвичай постачається разом із пристроєм. При цьому користувач має можливість самостійно визначати рівень доступу до відеоданих відповідно до власних налаштувань і політики інформаційної безпеки. Камери можуть бути як повністю захищеними, так і відкритими для публічного перегляду, наприклад у випадку трансляцій з масових заходів або відомих туристичних об’єктів.

IP-відеокамери забезпечують можливість візуального контролю як на локальних об’єктах, так і на територіально віддалених майданчиках. Це дозволяє ефективно вирішувати завдання автоматичного контролю за роботою обладнання в умовах відсутності персоналу, зокрема на підземних об’єктах, промислових майданчиках або великих відкритих територіях. За потреби організації прихованого спостереження можуть використовуватися мініатюрні IP-камери, які дозволяють непомітно здійснювати відеоконтроль та дистанційно керувати пристроєм через мережу Інтернет. Водночас слід підкреслити, що приховане відеоспостереження на території України є незаконним і може здійснюватися виключно правоохоронними органами за наявності відповідного судового дозволу.

До переваг бездротових камер відеоспостереження належить простота конструкції та можливість встановлення практично в будь-якому місці приміщення, висока швидкість передавання даних, значна роздільна здатність зображення, а також можливість організації відеоспостереження у заміських будинках або на віддалених об’єктах. Такі системи забезпечують дистанційний контроль через мережу Інтернет, можуть бути встановлені без залучення спеціалістів та здатні працювати в автономному режимі.

Важливим напрямом розвитку є інтеграція відеоспостереження з іншими системами безпеки. Інтегровані системи безпеки можуть функціонувати на територіально розподілених об’єктах, але керуватися з єдиного центру. Комплексна інтегрована система зазвичай включає систему відеоспостереження, систему контролю доступу для обліку робочого часу персоналу та визначення його зонального місцезнаходження, систему автоматичного розпізнавання номерних знаків на в’їздах і парковках, а також охоронну та пожежну сигналізацію і системи пожежогасіння. Найбільш ефективне виконання охоронних функцій досягається шляхом поєднання відеодетекторів руху та

охоронних датчиків, що дозволяє оперативно інформувати оператора про виникнення небажаних подій у конкретній зоні.

1.5 Висновки по розділу

У першому розділі встановлено, що відеоаналітика є не лише засобом фіксації подій, а й інтелектуальним інструментом підтримки рішень у системах безпеки. Перехід від аналогових CCTV-систем до IP-відеоспостереження створив умови для централізованого управління, масштабування та інтеграції відеоданих з іншими підсистемами захисту.

Показано, що застосування алгоритмів комп'ютерного зору, виявлення руху, класифікації об'єктів та сценарного аналізу підвищує оперативність реагування на порушення режиму безпеки. Разом із тим ефективність відеоаналітики безпосередньо залежить від якості зображення, коректного вибору камер, умов освітлення, пропускної здатності мережі та захищеності відеоархіву.

Отже, відеоспостереження доцільно розглядати як елемент комплексної системи технічного захисту інформації, який поєднує фізичний контроль, документування подій, підтримку розслідування інцидентів та профілактику несанкціонованого доступу.

РОЗДІЛ 2. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1 Нормативно-правові засади інформаційної безпеки України

Забезпечення інформаційної безпеки України та захист її національних інтересів в інформаційній сфері передбачає пріоритетний розвиток системи нормативно-правового регулювання суспільних відносин у цій галузі, протидію внутрішнім і зовнішнім загрозам, а також упорядкування правотворчого процесу. Важливу роль у цьому відіграє формування цілісної та узгодженої законодавчої бази, що визначає правові засади функціонування інформаційної сфери та механізми її захисту.

Подальший розвиток системи інформаційної безпеки України має ґрунтуватися на неухильному дотриманні та практичній реалізації чинних правових норм, що регулюють інформаційні відносини, а також на їх системному вдосконаленні з урахуванням сучасних технологічних і безпекових викликів. При цьому ключове значення зберігає саме техніко-правовий характер регулювання, який поєднує юридичні механізми з організаційними та інженерно-технічними засобами захисту інформації.

Нормативно-правове регулювання у сфері інформаційної безпеки України базується на Конституції України, яка закріплює право кожного на інформацію, свободу думки і слова, а також визначає обов'язок держави забезпечувати захист суверенітету, територіальної цілісності та національної безпеки. Конституційні положення слугують основою для формування галузевого законодавства, що деталізує порядок реалізації інформаційних прав і встановлює обмеження, зумовлені інтересами безпеки, громадського порядку та захисту прав інших осіб.

2.2 Законодавче регулювання захисту інформації та персональних даних

Закон України «Про інформацію» виконує системоутворюючу функцію у сфері інформаційних відносин, визначаючи принципи інформаційної діяльності, класифікацію інформації за режимом доступу, права та обов'язки суб'єктів, а також загальні засади захисту інформації. Його положення конкретизуються у спеціальних законах, зокрема у Законах України «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю», «Про доступ до публічної інформації», «Про захист персональних даних», «Про основні засади забезпечення кібербезпеки України».

Інформаційна безпека є складовою загальної системи національної безпеки та водночас важливим компонентом інформаційного забезпечення особи,

суспільства і держави. Вона орієнтована на захист інформаційних ресурсів, а також законних прав та інтересів суб'єктів інформаційних відносин. Зміст поняття «інформаційна безпека» розкривається у практичній діяльності, наукових дослідженнях і нормативно-правових актах, що регулюють відносини у сфері створення, зберігання, обробки, передавання та використання інформації.

Для створення й підтримання належного рівня національної безпеки в інформаційній сфері в Україні розробляється система правових норм, які регулюють відповідні суспільні відносини, визначають основні напрями діяльності органів державного управління, формуються або трансформуються органи та сили забезпечення інформаційної безпеки, а також механізми контролю і нагляду за їх діяльністю.

Одним із базових нормативно-правових актів у цій сфері є Закон України «Про інформацію». У статті 1 цього Закону визначено, що захист інформації — це сукупність правових, адміністративних, організаційних, технічних та інших заходів, спрямованих на забезпечення збереження та цілісності інформації, а також встановлення належного порядку доступу до неї. Об'єктом захисту визначається інформація як будь-які відомості та/або дані, що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Відповідно до статті 4 Закону України «Про інформацію», суб'єктами інформаційних відносин є фізичні особи, юридичні особи, об'єднання громадян та суб'єкти владних повноважень, тоді як об'єктом інформаційних відносин виступає інформація. Під суб'єктами владних повноважень розуміються органи державної влади, органи місцевого самоврядування, а також інші суб'єкти, які здійснюють владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень. Закон також закріплює, що процес захисту інформації охоплює комплекс правових, адміністративних,

організаційних і технічних заходів, спрямованих на забезпечення її збереження, цілісності та контрольованого доступу.

Важливим елементом нормативно-правового забезпечення інформаційної безпеки є Закон України «Про доступ до публічної інформації». Відповідно до цього Закону, публічна інформація визначається як відображена та задокументована будь-якими засобами і на будь-яких носіях інформація, що була отримана або створена суб'єктами владних повноважень у процесі виконання своїх функцій, передбачених чинним законодавством, або перебуває у їх володінні, а також у володінні інших розпорядників публічної інформації.

Стаття 24 зазначеного Закону встановлює відповідальність за порушення законодавства про доступ до публічної інформації. Зокрема, відповідальність настає у випадках ненадання відповіді на запит, ненадання або несвоєчасного надання інформації, безпідставної відмови у задоволенні запиту, неоприлюднення інформації відповідно до вимог закону, надання недостовірної, неточної чи неповної інформації, необґрунтованого віднесення інформації до категорії з обмеженим доступом, нездійснення реєстрації документів, а також навмисного приховування чи знищення інформації або документів. Особи, які вважають, що їхні права та законні інтереси були порушені розпорядниками інформації, мають право на відшкодування матеріальної та моральної шкоди у порядку, встановленому законодавством України.

У цілому нормативно-правова база України у сфері інформаційної безпеки створює правові передумови для захисту інформаційних ресурсів, забезпечення прозорості діяльності органів влади та реалізації прав громадян на доступ до інформації, що є необхідною умовою стабільного розвитку інформаційного суспільства.

Таємною визнається інформація, режим доступу до якої встановлюється відповідно до вимог чинного законодавства, а її неправомірне розголошення здатне спричинити негативні наслідки для окремої особи, суспільства або держави. До цієї категорії належать відомості, що містять державну, банківську, професійну таємницю, дані досудового розслідування, а також інші види інформації з обмеженим доступом, визначені нормативно-правовими актами. Така інформація підлягає спеціальній охороні та використовується лише в межах, передбачених законом.

Конфіденційною вважається інформація, доступ до якої обмежується фізичними чи юридичними особами, за винятком суб'єктів владних повноважень, і яка може поширюватися виключно за згодою власника та відповідно до встановлених ним умов. Водночас законодавством визначено перелік відомостей, які не можуть бути віднесені до конфіденційних, оскільки вони становлять суспільний інтерес або мають бути відкритими для забезпечення прозорості діяльності органів влади.

Службова інформація охоплює відомості, що відповідно до законодавчих вимог можуть бути тимчасово обмежені в доступі. До неї належать матеріали, що містяться у внутрішніх документах органів державної влади, зокрема службове листування, аналітичні довідки, доповідні записки та рекомендації, якщо вони стосуються формування напрямів діяльності установи, реалізації контрольних або наглядових функцій, а також процесу підготовки управлінських рішень до моменту їх публічного обговорення чи затвердження. Крім того, до службових можуть бути віднесені відомості, отримані під час оперативно-розшукової або контррозвідувальної діяльності, а також у сфері оборони, за умови, що вони не класифіковані як державна таємниця. Документи з такою інформацією маркуються відповідним грифом і надаються для ознайомлення лише у

встановленому порядку. При цьому переліки відомостей, які органи влади відносять до службових, не можуть бути повністю закритими для доступу.

Особливу роль у правовому забезпеченні інформаційної безпеки відіграє Закон України «Про державну таємницю», який визначає порядок віднесення інформації до державної таємниці, ступені її секретності, умови доступу громадян до секретних відомостей і механізми охорони таких даних. Законодавчо встановлюється відповідальність за порушення режиму секретності, що підкреслює важливість дотримання визначених процедур під час роботи з інформацією, розголошення якої може завдати шкоди національній безпеці.

З метою забезпечення належного захисту державної таємниці впроваджується комплекс організаційно-правових заходів. Серед них — уніфіковані вимоги до створення, використання, зберігання, передавання, транспортування й обліку матеріальних носіїв секретних відомостей, обмеження щодо їх оприлюднення або передачі іноземним суб’єктам, а також дозвільний порядок здійснення діяльності, пов’язаної з такою інформацією. Встановлюються спеціальні правила доступу громадян до секретних даних, визначається режим секретності для органів та установ, діяльність яких пов’язана з державною таємницею, а також запроваджуються обмеження щодо перебування і діяльності іноземців та іноземних юридичних осіб. Важливе значення мають технічні й криптографічні засоби захисту, які забезпечують недопущення витоку або спотворення секретної інформації.

Законодавство у сфері національної безпеки визначає ключові засади та принципи захисту держави, суспільства і громадян. Ним закріплюються базові національні інтереси України, зокрема стратегічний курс на європейську та євроатлантичну інтеграцію, формується система управління у секторі безпеки й оборони, визначаються напрями стратегічного планування, обсяг фінансового

забезпечення відповідних структур, склад Збройних Сил України, а також механізми цивільного контролю у цій сфері.

2.3 Нормативні вимоги до технічного захисту інформації

Важливу роль у забезпеченні інформаційної безпеки відіграють державні стандарти у сфері технічного захисту інформації. Вони визначають об’єкти та цілі захисту, основні організаційні й технічні засади запобігання несанкціонованому доступу до інформації, порушенню її цілісності або витоку, що може завдати шкоди державі, організаціям чи громадянам. Технічний захист інформації реалізується шляхом створення цілісної системи захисних заходів, яка формується поетапно: від ідентифікації та аналізу загроз до впровадження захисних рішень і подальшого контролю їх ефективності.

Центральним органом у сфері спеціального зв’язку та захисту інформації є Державна служба спеціального зв’язку та захисту інформації України. Вона забезпечує функціонування та розвиток урядового і конфіденційного зв’язку, реалізує державну політику у галузях криптографічного й технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом, а також спеціального поштового і фельд’єгерського зв’язку.

Правові та організаційні засади технічного захисту інформації визначаються окремими нормативними положеннями, які регламентують охорону важливої для держави, суспільства та особи інформації. До суб’єктів системи технічного захисту належать спеціально уповноважені державні органи, установи та організації, науково-дослідні й виробничі структури, військові частини, підприємства різних форм власності, а також навчальні заклади, що здійснюють підготовку та підвищення кваліфікації фахівців у цій галузі.

Концептуальні засади технічного захисту інформації визначають державну політику щодо застосування інженерно-технічних заходів у сфері безпеки інформації. Технічний захист розглядається як невід'ємний елемент національної безпеки та реалізується через функціонування системи, що об'єднує суб'єктів, нормативно-правове забезпечення і матеріально-технічну базу, спрямовані на досягнення спільної мети — захист інформаційних ресурсів.

Окремі державні стандарти встановлюють єдину термінологію та визначення у сфері технічного захисту інформації. Закріплені в них поняття є обов'язковими для застосування в нормативній, організаційній і технічній документації, а також використовуються у процесах стандартизації та при підготовці навчально-методичних матеріалів. Інші стандарти регламентують порядок організації та виконання робіт із технічного захисту інформації, що забезпечує уніфікований і системний підхід до реалізації заходів безпеки.

Завданням Державного стандарту України ДСТУ 3396.1-96 є встановлення регламентованого порядку виконання робіт у сфері технічного захисту інформації. Процес реалізації заходів протидії загрозам або їхньої нейтралізації передбачає низку послідовних дій, серед яких проведення комплексного обстеження підприємства, установи або організації, розроблення та впровадження організаційних, первинних і основних технічних заходів із застосуванням засобів ТЗІ, приймання виконаних робіт, а також атестація засобів або систем забезпечення інформаційної безпеки на відповідність вимогам нормативних документів у сфері ТЗІ.

Система нормативних документів ТЗІ включає низку ключових положень, що регламентують різні етапи роботи. НД ТЗІ 1.6-003-04 визначає основи створення моделей загроз для інформації на об'єктах інформаційної діяльності, включаючи порядок їх розроблення, побудови та оформлення. НД ТЗІ 1.1-005-07

регламентує організацію та поетапне виконання робіт зі створення комплексів ТЗІ на об’єктах державної влади, місцевого самоврядування, військових формувань, підприємств, установ та організацій, забезпечуючи захист від витоку інформації з обмеженим доступом технічними каналами. НД ТЗІ 3.3-001-07 визначає порядок розроблення та впровадження заходів із захисту інформації на етапі проєктування і реалізації комплексів ТЗІ, включаючи вимоги до підготовки пояснювальної записки, паспортів комплексу та приміщень, де обробляється інформація з обмеженим доступом. НД ТЗІ 3.1-001-07 регламентує проведення передпроектних робіт, порядок обстеження об’єктів інформаційної діяльності, складання акту обстеження та розроблення технічного завдання на створення комплексу ТЗІ, що забезпечує запобігання витоку інформації технічними каналами.

Положення про протидію технічним розвідкам встановлює організаційні та інженерно-технічні вимоги для захисту об’єктів оборонно-промислового комплексу, військової та спеціальної техніки, об’єктів мобілізаційного значення та інших стратегічних установ, що використовуються в інтересах оборони й безпеки держави. НД ТЗІ 2.1-002-07 визначає загальні принципи проведення випробувань комплексів ТЗІ на об’єктах інформаційної діяльності, спрямованих на перевірку повноти та достатності реалізованих заходів, атестацію системи та підготовку висновків із застосуванням відповідних методик і програм.

Таким чином, збереження та подальший розвиток технічної інформації про правові норми і закони України у сфері інформаційної безпеки є необхідною умовою формування ефективної, стійкої та керованої системи захисту інформації. Чітка нормативно-правова регламентація дозволяє забезпечити узгодженість дій суб’єктів інформаційних відносин, підвищити рівень правової визначеності та створити надійні механізми протидії сучасним інформаційним і кіберзагрозам, не порушуючи при цьому фундаментальних прав і свобод людини.

2.4 Висновки по розділу

У другому розділі систематизовано нормативно-правові засади захисту інформації та застосування систем відеоспостереження на об’єктах інформаційної діяльності. Встановлено, що проектування таких систем повинно враховувати вимоги законодавства України у сфері інформації, захисту персональних даних, кібербезпеки та технічного захисту інформації.

Обґрунтовано необхідність поєднання національних нормативних документів із міжнародними стандартами ISO/IEC 27001, ISO/IEC 27002, IEC 62676, рекомендаціями NIST, ONVIF, CIS та OWASP щодо управління ризиками, кіберзахисту мережевих пристроїв і забезпечення конфіденційності відеоданих.

Зроблено висновок, що правомірна та безпечна експлуатація систем відеоспостереження потребує документованої політики доступу до відеоархівів, визначення строків зберігання записів, захисту каналів передавання даних, журналювання дій користувачів та регулярного контролю технічного стану обладнання.

РОЗДІЛ 3. АКТ ОБСТЕЖЕННЯ НА ОБ’ЄКТІ З ОБМЕЖЕНИМ ДОСТУПОМ

3.1 Загальна характеристика об’єкта обстеження

Загальні відомості про об’єкт

Об’єктом інформаційної діяльності є багатоповерхова офісна будівля бізнес-центру «Лідер», розташована на окремій контрольованій території у межах міської забудови. Будівля використовується для розміщення офісних приміщень комерційних організацій, адміністративних підрозділів, а також допоміжної

інфраструктури, необхідної для забезпечення безперервної роботи орендарів та персоналу бізнес-центру.

Бізнес-центр є багатофункціональним об’єктом, у межах якого здійснюється значна кількість інформаційних процесів, пов’язаних з підготовкою, обробкою, передачею та зберіганням службової, комерційної та конфіденційної інформації. Частина інформації може належати до категорії інформації з обмеженим доступом, що зумовлює необхідність впровадження комплексу організаційних та технічних заходів захисту.

Будівля має 7 поверхів, з яких 7-й поверх є технічним та використовується для розміщення інженерного обладнання, серверних приміщень, вентиляційних установок та інших допоміжних технічних засобів. На об’єкті здійснюється постійна інформаційна діяльність із використанням комп’ютерної техніки, телекомунікаційних систем та автоматизованих інформаційних систем.

Режим роботи

Бізнес-центр «Лідер» працює цілодобово, що зумовлено особливостями діяльності орендарів та необхідністю забезпечення безперервного доступу до офісних приміщень і інформаційних ресурсів. Доступ працівників і відвідувачів регламентується системою контролю та управління доступом із використанням персональних ідентифікаторів, електронних пропусків та журналів обліку відвідувачів.

Прибирання приміщень проводиться двічі на день відповідно до затвердженого графіка:

ранкове – з 7.00 до 9.00;

вечірнє – з 16.00 до 18.00.

Під час проведення прибирання доступ до окремих приміщень може обмежуватися, а роботи виконуються під контролем служби охорони або відповідальних осіб.

Охорона об’єкта здійснюється цілодобово з використанням технічних засобів охорони та фізичної охорони. Постійно функціонує черговий пост охорони, який здійснює моніторинг стану систем безпеки та реагування на позаштатні ситуації.

Вхід до будівлі здійснюється через:

1 основний центральний вхід, обладнаний системами контролю доступу та відеоспостереження;

2 запасні входи (службові), які використовуються для евакуації, обслуговування та технічних потреб і перебувають під постійним контролем.

Штат працівників

Загальна чисельність персоналу, що постійно перебуває на об’єкті, становить 700 осіб, з яких 630 — штатні працівники офісів компаній-орендарів. Значна кількість персоналу та відвідувачів створює підвищене навантаження на системи безпеки та потребує чіткого регламентування доступу до приміщень і інформаційних ресурсів.

У тому числі:

Керівництво бізнес-центру – 10 осіб. Організовує та контролює роботу об’єкта, відповідає за дотримання вимог безпеки та режиму інформаційної діяльності.

Адміністративний персонал – 45 осіб. Забезпечує управління орендними, організаційними та технічними процесами, веде документацію та працює з інформаційними системами.

Офісні працівники компаній-орендарів – близько 630 осіб. Здійснюють основну інформаційну, фінансову та комерційну діяльність.

Служба охорони – 10 осіб. Забезпечує фізичну та технічну охорону об’єкта, контроль доступу та реагування на інциденти.

Технічний персонал – 5 осіб. Забезпечує обслуговування інженерних, електротехнічних та інформаційно-комунікаційних систем будівлі.

Всього: 700 осіб.

Характеристика складових ОІД

Аналіз фізичного середовища офісної будівлі

Об’єкт інформаційної діяльності – семиповерхова офісна будівля бізнес-центру «Лідер», що розташована в умовах щільної міської забудови. Навколо будівлі знаходяться житлові та адміністративні споруди, автостоянка, проїжджі частини та пішохідні зони, що створює потенційні ризики несанкціонованого доступу та технічного зняття інформації.

Фізичне середовище об’єкта характеризується наявністю значної кількості зовнішніх огороджувальних конструкцій, інженерних комунікацій та зон загального користування, які можуть бути використані як потенційні канали витоку інформації.

Можливі точки зняття інформації:

- вікна офісних приміщень, у яких циркулює інформація з обмеженим доступом;
- технічні приміщення, серверні та комунікаційні шахти;
- місця загального користування (коридори, ліфтові холи, зони очікування).

Архітектурно-будівельні особливості приміщень

Огорожа території:

Територія бізнес-центру огороджена по периметру з метою обмеження доступу сторонніх осіб.

Висота огорожі – 2500 мм.

- Склад – металеві секції з елементами контролю доступу.
- В’їзні ворота – металеві, автоматизовані, з дистанційним керуванням.

Будівля:

- Товщина зовнішніх стін – 450 мм, що забезпечує достатній рівень механічної міцності та часткове екранування зовнішніх впливів.
- Висота міжповерхових перекриттів – 3000 мм.
- Матеріал зовнішніх стін – залізобетон та цегла.
- Перекриття – залізобетонні плити товщиною 160 мм.
- Підлога – бетонна стяжка товщиною 120 мм.

- Покриття підлоги – керамограніт та ламінат (8–10 мм).

Вікна:

- Металопластикові з двокамерним склопакетом.

Товщина скла – 4 мм.

Частина вікон обладнана жалюзі для зменшення можливості візуального спостереження ззовні.

Двері:

- Внутрішні – дерев’яні та металопластикові, одно- та двостулкові.
- Зовнішні – металопластикові з посиленим профілем та багатокамерним склопакетом, обладнані замками та елементами контролю доступу.

Технічні засоби охорони та контролю

Контрольована зона (КЗ) визначена наказом адміністрації бізнес-центру та обмежена периметром будівлі. У межах КЗ встановлено режим обмеженого доступу та впроваджено комплекс технічних і організаційних заходів безпеки.

ОІД обладнано системами пожежної сигналізації, системами контролю та управління доступом, а також системами відеоспостереження, інтегрованими в єдину інформаційно-аналітичну платформу.

3.2 Аналіз наявної системи відеоспостереження та технічних засобів

Система відеоспостереження одного поверху на базі AJAX SYSTEMS включає:

Зовнішні IP-камери Ajax OutdoorCam – 3 шт.

Роздільна здатність: до 4 Мп

Кут огляду: 110°

Нічне бачення (IR): до 35 м

Ступінь захисту: IP65

Вбудований детектор руху з AI-фільтрацією помилкових спрацювань

Внутрішні IP-камери Ajax IndoorCam – 4 шт.

Роздільна здатність: Full HD / 2K

Кут огляду: 130°

Підтримка шифрування відеопотоку

Інтеграція з іншими підсистемами безпеки AJAX

Також до складу системи входять:

централізований відеореєстратор із хмарним та локальним зберіганням даних;

монітори для чергового персоналу охорони;

комутаційне обладнання та захищені канали передачі даних.

Будівля підключена до пульта охорони, що забезпечує безперервний моніторинг стану безпеки об’єкта та оперативне реагування на події.

Системи комунікацій підприємства

Таблиця 1 – Системи комунікацій БЦ «Лідер»

Вид комунікації

Спосіб підключення

Електроживлення

Підключено до міської електромережі через власну трансформаторну підстанцію бізнес-центру. Трансформаторна підстанція розташована за межами контрольованої зони (КЗ) та обслуговує також сторонніх споживачів.

Система опалення

Підключена до міської тепломережі. Система опалення централізована, двотрубна, з використанням металевих труб та радіаторів. Основні магістралі проходять за межами КЗ, внутрішні контури – у межах будівлі.

Система каналізації

Підключена до міської мережі каналізації, яка проходить за межами КЗ. Внутрішня каналізаційна система виконана з полімерних труб.

Система водопостачання

Підключена до міського водоканалу. Подача холодної та гарячої води здійснюється через центральні магістралі, що виходять за межі КЗ. Внутрішня система – комбінована, з використанням металевих та поліпропіленових труб.

Заземлення

Усі електроприлади, серверне та офісне обладнання заземлені на єдиний замкнений контур заземлення будівлі, який повністю знаходиться в межах КЗ.

Телефонний зв’язок

Підключений до міської телефонної мережі через провайдера телекомунікаційних послуг. На бізнес-центр виділено багатоканальні телефонні лінії для адміністрації, служби охорони та орендарів. Лінії зв’язку виходять за межі КЗ.

Система вентиляції

Приточно-витяжна, штучна, з механічним спонуканням. Вентиляційні установки розміщені в технічних приміщеннях та на технічному (7-му) поверсі будівлі.

кінець таблиці

Обстеження інформаційного середовища

Інформаційне середовище бізнес-центру «Лідер» включає сукупність технічних, програмних та організаційних засобів, за допомогою яких здійснюється створення, обробка, зберігання та передача інформації. Основна частина інформаційних процесів пов’язана з діяльністю комерційних організацій-орендарів, адміністрації бізнес-центру та служби охорони.

Інформація обробляється з використанням персональних комп’ютерів, серверного обладнання, локальних обчислювальних мереж та зовнішніх телекомунікаційних каналів. Наявність великої кількості користувачів і різнорідних інформаційних потоків потребує впровадження системного підходу до захисту інформації, з урахуванням вимог чинного законодавства та нормативних документів у сфері технічного захисту інформації.

Категорування інформації

Таблиця 2 – Категорування інформації

Інформація	Носій	Режим доступу і правовий режим	Має доступ
Службово-ділова інформація	Електронний та паперовий	Відкрита	Працівники компаній-орендарів, адміністрація БЦ
Комерційна інформація	Електронний	З обмеженим доступом, конфіденційна	Керівництво та уповноважені працівники компаній
Адміністративна інформація	Електронний та паперовий	З обмеженим доступом	Адміністрація бізнес-центру
Технічна інформація (плани, схеми, системи безпеки)	Електронний та паперовий	Конфіденційна	Служба безпеки та технічний персонал

Інформація систем відеоспостереження

Електронний

З обмеженим доступом

Служба охорони, адміністрація БЦ

кінець таблиці

Режим доступу і правовий режим

Доступ до інформації в бізнес-центрі «Лідер» регламентується внутрішніми нормативними документами, договорами з орендарями та чинним законодавством України. Інформація з обмеженим доступом зберігається та обробляється з використанням організаційних і технічних заходів захисту. Доступ до конфіденційної та службової інформації надається виключно уповноваженим особам відповідно до їх посадових обов’язків.

Результати аналізу наявності в установі

В результаті обстеження ОІД бізнес-центру «Лідер» встановлено, що на об’єкті наказом адміністрації бізнес-центру затверджена контрольована зона (КЗ), яка забезпечується периметральною огорожею будівлі, системою контролю доступу та цілодобовою охороною.

У ході обстеження також встановлено, що можливими місцями перехоплення інформації з обмеженим доступом (ІзОД) з використанням технічних засобів розвідки можуть бути транспортні засоби, що розташовуються на прилеглій території, а також сусідні будівлі міської забудови. З огляду на багатоповерхову структуру будівлі та значну кількість вікон, існує потенційна можливість зняття мовної та візуальної інформації ззовні.

Зняття інформації відповідно до планування будівлі також можливе у разі несанкціонованого проникнення порушника до офісних приміщень, переговорних кімнат, серверних та технічних приміщень.

На момент обстеження на об’єкті відсутня затверджена модель загроз для інформації з обмеженим доступом, що може призводити до зниження ефективності заходів із забезпечення захисту інформації, нераціонального використання технічних та організаційних засобів захисту, а також до необґрунтованих фінансових витрат.

На об’єкті використовуються технічні засоби, що відповідають чинним вимогам нормативних документів та призначені для обробки, зберігання і передавання інформації.

До технічних засобів, що належать до ДТЗС, відносяться:

- системи відеоспостереження;
- освітлювальні прилади;
- засоби пожежної сигналізації;
- системи охоронної сигналізації;
- мережеве та серверне обладнання.

Таблиця 3 – Аналіз існуючих технічних каналів витоку інформації на ОІД

Загроза

Канал

За рахунок чого реалізується

Витік мовної інформації

Прямий акустичний

Підслуховування та перехоплення інформації за допомогою високочутливих мікрофонів і спрямованих акустичних засобів через вікна, двері та вентиляційні отвори.

Віброакустичний

Перехоплення інформації за допомогою контактних датчиків, встановлених на будівельних конструкціях та інженерних комунікаціях за умови доступу сторонніх осіб.

Оптико-електронний (лазерний)

Опромінення лазерним променем поверхонь, що вібрують під дією мовного сигналу (скло вікон, елементи фасаду).

Витік візуальної інформації

Прямий оптичний

Спостереження за приміщеннями через вікна, фото- та відеозйомка документів і екранів моніторів із використанням оптичних та цифрових засобів.

Витік інформації, що обробляється ТЗПІ

Електромагнітний

Перехоплення побічних електромагнітних випромінювань і наведень (ПЕМВН) від елементів технічних засобів обробки інформації.

Електричний

Зняття інформаційних сигналів з ліній електроживлення та заземлення.

кінець таблиці

На об’єкті наявні такі засоби технічного захисту інформації (ТЗІ):

- засоби контролю доступу до приміщень;
- системи відеоспостереження з обмеженим доступом до архівів;
- мережеві засоби сегментації та контролю доступу до інформаційних ресурсів.

Інвентарна та технічна документація щодо впроваджених заходів із захисту інформації зберігається в адміністрації бізнес-центру та у відповідальних підрозділах.

До систем пожежної та охоронної сигналізації передбачена можливість інтеграції комплексу технічного захисту інформації.

3.3 Аналіз каналів витоку інформації та зон контролю

Модель загроз інформаційній безпеці об’єкта інформаційної діяльності бізнес-центру «Лідер» розробляється з метою визначення можливих джерел загроз, способів їх реалізації, потенційних порушників та технічних каналів витоку інформації з обмеженим доступом і є підґрунтям для формування вимог до комплексної системи захисту інформації та вибору адекватних організаційних і технічних заходів безпеки. Під загрозою інформаційній безпеці розуміється сукупність умов і факторів, реалізація яких може призвести до порушення

конфіденційності, цілісності або доступності інформації, що створюється, обробляється, зберігається та передається на об’єкті.

На об’єкті інформаційної діяльності обробляється службова інформація адміністрації бізнес-центру, комерційна інформація компаній-орендарів, персональні дані працівників і відвідувачів, а також технічна інформація про функціонування систем безпеки та інженерних комунікацій, порушення режиму захисту яких може спричинити матеріальні збитки, репутаційні втрати та негативні правові наслідки. Потенційними порушниками інформаційної безпеки можуть виступати як зовнішні особи, що не мають санкціонованого доступу до об’єкта або перебувають на прилеглій території, так і внутрішні користувачі у вигляді працівників компаній-орендарів, адміністративного та технічного персоналу, а також співробітників служби охорони, причому найбільш небезпечними є комбіновані загрози, пов’язані зі змовою внутрішніх і зовнішніх порушників.

До основних загроз інформаційній безпеці об’єкта належать несанкціонований доступ до приміщень і технічних зон, порушення режиму доступу до інформаційних ресурсів, витік інформації через технічні канали, перехоплення даних під час передавання каналами зв’язку, компрометація технічних засобів, навмисні або ненавмисні дії персоналу, вплив шкідливого програмного забезпечення, а також відмови технічних систем і порушення їх працездатності. Аналіз технічних каналів витоку інформації показує, що для бізнес-центру «Лідер» характерна наявність значної кількості потенційних каналів витоку, обумовлених архітектурно-будівельними особливостями будівлі, щільністю інженерних комунікацій і постійною інтенсивною інформаційною діяльністю.

Одними з найбільш імовірних є акустичні канали витоку, що виникають у процесі службових і ділових розмов персоналу, переговорів у конференц-залах та телефонних розмов і можуть реалізовуватися через віконні та дверні прорізи, вентиляційні канали, міжповерхові перекриття, стіни та комунікаційні шахти, зокрема із застосуванням спрямованих мікрофонів або лазерних систем зняття мовної інформації ззовні будівлі.

Віброакустичні канали витоку пов’язані з передаванням коливань від джерел звуку на тверді конструкції будівлі, такі як вікна, стіни, перекриття та металеві елементи інженерних систем, з яких інформація може зчитуватися спеціальними технічними засобами за межами контрольованої зони.

Оптичні або візуальні канали витоку реалізуються шляхом безпосереднього спостереження або фіксації зображень робочих місць, екранів моніторів, документів та інших носіїв інформації через вікна або з використанням фото- та відеотехніки, при цьому ризик зростає за відсутності жалюзі, неправильного розміщення робочих місць і недотримання режимних вимог.

Електромагнітні канали витоку інформації виникають унаслідок побічних електромагнітних випромінювань і наведень, що супроводжують роботу комп’ютерної, мережевої та периферійної техніки, а також кабельних ліній, і можуть бути використані для перехоплення інформації як через ефір, так і через суміжні комунікації або контури заземлення.

Окрему групу ризиків становлять канали витоку через інженерні комунікації, зокрема системи електроживлення, заземлення, вентиляції, опалення та трубопроводи, через які інформація може передаватися у вигляді наведень або механічних коливань за межі контрольованої зони.

Значну загрозу для інформаційної безпеки також становлять канали витоку через телекомунікаційні мережі, у тому числі локальні обчислювальні мережі, телефонні лінії, інтернет-з’єднання та бездротові канали зв’язку, особливо у випадках використання незахищених протоколів передавання даних, недостатнього рівня автентифікації користувачів або помилок конфігурації мережевого обладнання.

Узагальнений аналіз свідчить про те, що найбільш імовірними для об’єкта інформаційної діяльності бізнес-центру «Лідер» є акустичні, віброакустичні, оптичні, електромагнітні та мережеві канали витоку інформації, що зумовлює необхідність урахування зазначених загроз під час проєктування та впровадження комплексної системи захисту інформації з використанням взаємопов’язаних організаційних, інженерно-технічних і програмних заходів безпеки.

3.4 Висновки по розділу

У третьому розділі виконано обстеження об’єкта з обмеженим доступом та визначено основні умови, що впливають на побудову системи відеоспостереження. Оцінено зони контролю, можливі маршрути несанкціонованого доступу, місця розміщення камер, а також вимоги до фіксації подій у критичних ділянках приміщення.

Визначено, що акт обстеження є основним вихідним документом для подальшого проектування системи захисту, оскільки він фіксує межі контрольованої зони, технічні умови встановлення обладнання, обмеження щодо освітлення, кабельної інфраструктури та доступу до відеореєстраторів.

Отже, якісне обстеження об’єкта дозволяє перейти від загальних рекомендацій до конкретних технічних рішень, обґрунтувати вибір обладнання та сформувати вимоги до експлуатації системи відеоспостереження.

РОЗДІЛ 4. РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ОБ’ЄКТА З ОБМЕЖЕНИМ ДОСТУПОМ

4.1 Вибір обладнання та загальна архітектура системи відеоспостереження

Для вибору оптимального технічного рішення було проведено порівняння сучасних зовнішніх IP-камер з урахуванням вимог до об’єктів інформаційної діяльності з обмеженим доступом. Основними критеріями відбору обладнання стали: роздільна здатність відео, чутливість матриці, наявність інфрачервоного підсвічування для нічної зйомки, підтримка сучасних кодеків стиснення відео, можливість інтеграції з існуючою мережею IP-відеоспостереження, підтримка функцій відеоаналітики, а також відповідність вимогам експлуатації в умовах зовнішнього середовища.

Зовнішні камери повинні мати антивандальне виконання та захист від впливу атмосферних факторів не нижче класу IP66 або IP67, що забезпечує стійкість до пилу, опадів і перепадів температур. Також важливою вимогою є підтримка широкого динамічного діапазону (WDR), який дозволяє отримувати чітке зображення за складних умов освітлення, зокрема при наявності різких контрастів між світлими та затемненими ділянками сцени. Для забезпечення цілодобового контролю доцільно використовувати камери з вбудованим інфрачервоним підсвічуванням дальністю не менше 30–50 метрів.

Внутрішні камери відеоспостереження, призначені для контролю коридорів, холів, входів до офісних приміщень і зон обмеженого доступу, мають відповідати іншим технічним вимогам. Для таких камер пріоритетними є компактність, непомітність встановлення, висока роздільна здатність і точна передача кольорів. Оскільки внутрішні приміщення характеризуються стабільнішими умовами освітлення, вимоги до інфрачервоного підсвічування можуть бути нижчими, проте бажаною є наявність функцій компенсації засвічення та цифрового шумозаглушення.

Для підвищення рівня захисту інформації з обмеженим доступом рекомендовано використовувати IP-камери з підтримкою шифрування відеопотоків та автентифікації доступу до налаштувань і архівів. Це відповідає вимогам технічного захисту інформації та знижує ризик несанкціонованого доступу до відеоданих через мережу. Також важливою є підтримка протоколів ONVIF, що забезпечує сумісність обладнання різних виробників і спрощує інтеграцію нових камер у вже функціонуючу систему.

У рамках проєктування комплексної системи захисту доцільно передбачити використання мережевого відеореєстратора (NVR), який забезпечуватиме централізований прийом, обробку, запис і зберігання відеоданих з усіх

встановлених камер. Відеореєстратор повинен підтримувати необхідну кількість каналів із запасом для подальшого розширення системи, сучасні алгоритми стиснення відео (H.264/H.265), а також функції резервного копіювання та відмовостійкої роботи.

Зберігання відеоархіву рекомендовано організувати з урахуванням вимог нормативних документів у сфері технічного захисту інформації. Для цього слід використовувати жорсткі диски, призначені для безперервної роботи у системах відеоспостереження, а також передбачити розмежування прав доступу до архівних даних. Термін зберігання відеоінформації визначається внутрішніми нормативними документами підприємства та може коригуватися залежно від категорії приміщень і рівня ризику [8, 15, 20]..

Окрему увагу необхідно приділити мережевій інфраструктурі системи відеоспостереження. Для підключення IP-камер доцільно використовувати керовані комутатори з підтримкою технології Power over Ethernet (PoE), що дозволяє одночасно передавати дані та живлення по одному кабелю. Це спрощує монтаж системи, зменшує кількість допоміжного обладнання та підвищує загальну надійність. Керовані комутатори також забезпечують можливість сегментації мережі, що є важливим з точки зору інформаційної безпеки.

У межах комплексної системи захисту об’єкта відеоспостереження має бути інтегроване з іншими підсистемами безпеки, зокрема системою контролю та управління доступом і охоронною сигналізацією. Така інтеграція дозволяє реалізувати сценарії автоматичного реагування, наприклад, початок запису з камер при спрацюванні датчиків або фіксацію відеоподій, пов’язаних із проходом осіб через контрольовані точки доступу.

Таким чином, вибір обладнання для розширення системи відеоспостереження бізнес-центру «Лідер» здійснюється з урахуванням вимог до об’єктів з обмеженим доступом, чинних нормативно-правових актів у сфері технічного захисту інформації та практичних умов експлуатації. Запропоноване технічне рішення дозволяє підвищити рівень фізичної та інформаційної безпеки, знизити ризики витоку інформації та створити надійну основу для подальшого розвитку комплексної системи захисту об’єкта.

Для вибору оптимального технічного рішення було проведено порівняння сучасних зовнішніх IP-камер.

4.2 Порівняльний аналіз камер та обґрунтування вибору обладнання

Таблиця 5 – Порівняння характеристик зовнішніх IP-камер

Виробник і модель
Характеристики

Ajax OutdoorCam
Роздільна здатність – до 4 Мп
Кут огляду – до 110°
Фокусна відстань – фіксована
Наявність Ethernet (PoE) – так
Світлочутливість – 0,01 лк
Дальність ІЧ-підсвітки – до 35 м
Живлення – PoE / DC 12V
Стандарт стиснення – H.264 / H.265
Клас захисту – IP65

Hikvision DS-2CD1021-I

Роздільна здатність – 2 Мп

Кут огляду – 105,8°

Фокусна відстань – 2,8 мм

Наявність Ethernet – так

Світлочутливість – 0,01 лк

Дальність ІЧ-підсвітки – до 30 м

Живлення – PoE / DC 12V

Стандарт стиснення – H.264 / H.264+

Dahua IPC-HFW1230S

Роздільна здатність – 2 Мп

Кут огляду – 103°

Фокусна відстань – 2,8 мм

Наявність Ethernet – так

Світлочутливість – 0,01 лк

Дальність ІЧ-підсвітки – до 30 м

Живлення – PoE / DC 12V

Стандарт стиснення – H.264

кінець таблиці

Проведене порівняння внутрішніх IP-камер здійснювалося з урахуванням специфіки об’єкта інформаційної діяльності, на якому обробляється інформація з обмеженим доступом. Основними критеріями оцінювання стали роздільна здатність і деталізація зображення, стабільність роботи у режимі тривалої експлуатації, можливість гнучкого налаштування кута огляду, підтримка програмних обмежень зон спостереження (privacy masks), а також відповідність вимогам технічного та правового захисту інформації.

Особлива увага приділялася можливості програмного обмеження поля зору камери. Функція маскування приватних зон дозволяє виключити з відеозапису ділянки, на яких можуть відображатися монітори робочих станцій, конфіденційні документи або інші носії інформації з обмеженим доступом. Такий підхід відповідає вимогам законодавства України у сфері захисту інформації та персональних даних і дозволяє мінімізувати ризики ненавмисного розголошення відомостей у процесі відеоспостереження.

Також важливим параметром є відсутність або можливість апаратного та програмного відключення аудіоканалу. Запис звуку в офісних приміщеннях може створювати додаткові загрози витоку конфіденційної інформації, зокрема під час службових нарад, переговорів або обговорення внутрішніх питань діяльності організації. Тому пріоритет надається моделям камер, у яких мікрофон відсутній або може бути повністю деактивований без можливості несанкціонованого повторного увімкнення.

Внутрішні IP-камери повинні забезпечувати стабільну роботу за умов штучного освітлення, мати функції цифрового шумозаглушення, автоматичного балансу білого та компенсації засвічення. Це дозволяє отримувати якісне зображення незалежно від часу доби та інтенсивності освітлення, що є критично важливим для коректної ідентифікації осіб і аналізу подій у разі виникнення інцидентів безпеки.

За результатами порівняльного аналізу було обрано модель внутрішньої IP-камери, яка оптимально поєднує необхідні технічні характеристики, надійність і можливість інтеграції з існуючою системою відеоспостереження. Обрана камера підтримує високу роздільну здатність, має широкий кут огляду з можливістю його коригування, забезпечує стабільну передачу відеоданих мережею та підтримує

сучасні алгоритми стиснення, що зменшує навантаження на мережеву інфраструктуру і системи зберігання даних.

Розміщення внутрішніх камер у кутах приміщення дозволяє забезпечити максимальне покриття простору та виключити наявність сліпих зон. При цьому монтаж здійснюється з урахуванням висоти стель, розташування робочих місць і шляхів пересування персоналу. Камери орієнтуються таким чином, щоб основна увага приділялася зонам входу, проходам і місцям загального користування, а не робочим поверхням співробітників.

Вибір і розміщення камер відеоспостереження також узгоджуються з вимогами нормативних документів у сфері технічного захисту інформації. Зокрема, під час проєктування враховуються положення ДСТУ та нормативних документів ТЗІ щодо недопущення витоку інформації технічними каналами. Камери не повинні створювати умов для оптичного спостереження за носіями інформації з обмеженим доступом, а вся відеоінформація, що зберігається, підлягає захисту від несанкціонованого доступу.

Додатково передбачається централізоване керування внутрішніми камерами через захищений інтерфейс адміністратора з розмежуванням прав доступу. Це дозволяє забезпечити контроль за налаштуваннями системи, переглядом відеоархівів і використанням аналітичних функцій лише уповноваженими особами. Такий підхід відповідає принципам інформаційної безпеки та вимогам чинного законодавства України щодо захисту інформації.

У результаті впровадження запропонованого комплексу зовнішніх і внутрішніх IP-камер формується цілісна система відеоспостереження, здатна забезпечити ефективний контроль за периметром і внутрішнім простором бізнес-центру «Лідер». Це дозволяє істотно підвищити рівень фізичної та інформаційної

безпеки об’єкта, зменшити ризики несанкціонованого доступу та створити додатковий рівень захисту інформації з обмеженим доступом у межах комплексної системи безпеки.

Внутрішні камери доцільно встановити у всіх кутах офісного приміщення для забезпечення відсутності сліпих зон всередині відкритого простору. Основною вимогою до внутрішньої камери є висока якість зображення для ідентифікації осіб, відсутність або можливість відключення аудіоканалу, а також обмеження огляду таким чином, щоб не фіксувати екрани моніторів та документи. Для цього було виконано порівняння внутрішніх IP-камер.

Таблиця 6 – Порівняння характеристик внутрішніх IP-камер

Виробник і модель
Характеристики

Ajax IndoorCam
Роздільна здатність – Full HD / 2K
Кут огляду – до 130°
Фокусна відстань – фіксована
Наявність Ethernet – так
Світлочутливість – 0,01 лк
Можливість запису звуку – програмно вимикається
Наявність ІЧ-підсвітки – так
Живлення – PoE / DC 12V
Стандарт стиснення – H.264 / H.265

Hikvision DS-2CD1331-I
Роздільна здатність – 3 Мп

Кут огляду – 106°

Фокусна відстань – 2,8 мм

Наявність Ethernet – так

Світлочутливість – 0,01 лк

Можливість запису звуку – відсутня

Наявність ІЧ-підсвітки – так

Живлення – PoE / DC 12V

Стандарт стиснення – H.264 / H.264+

Dahua IPC-HDW1431SP

Роздільна здатність – 4 Мп

Кут огляду – 105,8°

Фокусна відстань – 2,8 мм

Наявність Ethernet – так

Світлочутливість – 0,01 лк

Можливість запису звуку – відсутня

Наявність ІЧ-підсвітки – так

Живлення – PoE / DC 12V

Стандарт стиснення – H.265

кінець таблиці

З урахуванням технічних характеристик, вимог до інформаційної безпеки та уніфікації обладнання, оптимальним вибором для внутрішнього використання є Ajax IndoorCam.

4.3 Розрахунок вартості та економічне обґрунтування

Існуюча система відеоспостереження бізнес-центру «Лідер» включає IP-камери, мережевий комутатор з підтримкою PoE, мережевий відеореєстратор, монітори для відображення відеоінформації, а також розгалужену кабельну інфраструктуру з резервом підключень. Наявність такої базової технічної основи дозволяє здійснити модернізацію системи без необхідності заміни основних вузлів, що суттєво зменшує загальні фінансові витрати та скорочує строки впровадження проєктних рішень.

Модернізація передбачає розширення кількості камер відеоспостереження з метою підвищення рівня контролю за прилеглою територією та внутрішніми приміщеннями об’єкта з обмеженим доступом. Вибір обладнання здійснювався з урахуванням технічних характеристик, сумісності з наявною інфраструктурою, відповідності вимогам технічного захисту інформації, а також економічної доцільності.

Для організації зовнішнього відеоспостереження обрано камери Ajax OutdoorCam, які забезпечують високу роздільну здатність, значну дальність інфрачервоної підсвітки та повну інтеграцію з екосистемою AJAX SYSTEMS. Це дозволяє використовувати єдиний програмний інтерфейс для керування системою безпеки та спрощує експлуатацію. Орієнтовна вартість однієї камери становить 5 500 грн. Загальна кількість зовнішніх камер — 5 одиниць.

Для внутрішнього відеоспостереження застосовуються камери Ajax IndoorCam, які відповідають вимогам до якості зображення, мають компактне виконання та підтримують програмні засоби обмеження зон огляду. Орієнтовна вартість однієї внутрішньої камери становить 4 200 грн. Загальна кількість внутрішніх камер — 6 одиниць.

Для підключення додаткових камер використовується мережевий кабель типу «вита пара», який відповідає вимогам для передачі цифрового відеосигналу та живлення PoE. Загальна довжина кабелю, необхідна для реалізації проєкту, становить 60 метрів. Орієнтовна вартість одного метра кабелю — 10 грн, що забезпечує мінімальні витрати на розширення кабельної інфраструктури завдяки наявному резерву прокладання.

Орієнтовна вартість обладнання:

- Ajax OutdoorCam — 5 500 грн × 5 шт. = 27 500 грн
- Ajax IndoorCam — 4 200 грн × 6 шт. = 25 200 грн
- Мережевий кабель — 60 м × 10 грн/м = 600 грн

Крім основного обладнання, у розрахунок включено додатковий резерв кабельної продукції для прокладання альтернативних маршрутів та компенсації можливих втрат під час монтажу, що підвищує надійність системи та відповідає вимогам відмовостійкості.

Загальна вартість модернізації системи відеоспостереження:

5 500 × 5 + 4 200 × 6 + 600 × 15 = **82 700 грн

Отримана сума є орієнтовною та не враховує витрати на монтажні роботи, пусконалагоджувальні заходи та можливе додаткове програмне забезпечення. Водночас, з урахуванням того, що основна інфраструктура вже функціонує, вартість робіт з інсталяції буде мінімальною та не потребуватиме залучення значних матеріальних ресурсів.

У цілому запропонована модернізація є економічно обґрунтованою та доцільною, оскільки забезпечує істотне підвищення рівня фізичної та інформаційної безпеки об’єкта з обмеженим доступом при порівняно невеликих фінансових витратах. Впровадження додаткових камер відеоспостереження дозволяє знизити ризики несанкціонованого доступу, своєчасно виявляти потенційні загрози та забезпечити виконання вимог чинного законодавства України у сфері технічного захисту інформації.

4.4 Оцінка ефективності запропонованих технічних рішень

Ефективність запропонованих технічних рішень оцінюється за сукупністю організаційних, технічних та інформаційних критеріїв. До основних критеріїв належать зменшення кількості неконтрольованих зон, підвищення якості відеофіксації, скорочення часу реагування на інциденти, забезпечення збереження відеоданих та обмеження доступу до архівів.

Запропонована модернізація забезпечує більш повне покриття периметра, вхідних груп, коридорів та приміщень загального користування. Використання IP-камер із підтримкою відеоаналітики дозволяє підвищити ймовірність раннього виявлення порушень режиму доступу, а захищена мережева інфраструктура зменшує ризики несанкціонованого втручання в роботу системи.

Практичний ефект від впровадження системи полягає у підвищенні рівня контролю об’єкта інформаційної діяльності, створенні доказової бази для розслідування інцидентів, посиленні дисципліни доступу та підвищенні загального рівня технічного захисту інформації.

4.5 Висновки по розділу

У четвертому розділі запропоновано комплексну систему захисту об’єкта з обмеженим доступом на основі відеоспостереження, відеоаналітики, мережевої інфраструктури, засобів запису та організаційних процедур контролю.

Обґрунтовано доцільність застосування IP-камер з необхідною роздільною здатністю, відеореєстратора, захищеного сховища даних та контрольованих каналів передавання відеопотоку.

Показано, що підвищення ефективності захисту досягається за рахунок раціонального розміщення камер, мінімізації сліпих зон, використання сценаріїв відеоаналітики, обмеження доступу до відеоархіву та ведення журналів подій. Важливою умовою є кіберзахист IP-обладнання, зокрема зміна стандартних паролів, сегментація мережі, оновлення прошивок і шифрування віддаленого доступу.

Результати розділу підтверджують, що система відеоспостереження повинна функціонувати як частина комплексної системи технічного захисту інформації, а не як ізольований засіб охорони.

ВИСНОВКИ

У ході розробки комплексної системи захисту об’єкта з обмеженим доступом бізнес-центру «Лідер» було проведено детальний аналіз існуючого стану системи відеоспостереження, архітектурно-планувальних особливостей будівлі, режиму її експлуатації, характеру діяльності орендарів, а також потенційних внутрішніх і зовнішніх загроз витоку інформації. Особлива увага приділялася оцінюванню ризиків, пов’язаних із несанкціонованим доступом сторонніх осіб, можливістю візуального або технічного перехоплення інформації, а також недоліками у покритті зон спостереження. За результатами аналізу встановлено, що наявна система безпеки загалом забезпечує базовий рівень контролю та відповідає мінімальним експлуатаційним вимогам, проте має суттєвий резерв для підвищення ефективності за рахунок цільового розширення та оптимізації технічних засобів відеоспостереження.

Запропоноване встановлення додаткових зовнішніх і внутрішніх IP-камер дозволяє істотно підвищити рівень контролю за прилеглою територією бізнес-центру, вхідними групами, шляхами пересування відвідувачів і персоналу, а також внутрішніми зонами загального користування. Це, у свою чергу, сприяє зменшенню ймовірності несанкціонованого проникнення до приміщень, у яких може здійснюватися обробка, зберігання або обговорення інформації з обмеженим доступом. Розширення системи відеоспостереження також дозволяє мінімізувати ризики дистанційного перехоплення мовної та візуальної інформації шляхом своєчасного виявлення сторонніх осіб, підозрілих дій або нетипових ситуацій поблизу об’єкта.

Особливу увагу в межах проєкту приділено правильному вибору місць встановлення камер відеоспостереження та орієнтації їх поля зору. Такий підхід

дозволяє забезпечити достатній рівень ідентифікації осіб, фіксації подій і контролю ситуації без порушення вимог щодо захисту конфіденційної інформації, персональних даних та комерційної таємниці. Запропоновані рішення відповідають принципам технічного захисту інформації та не створюють передумов для оптичного спостереження за екранами моніторів, документами або іншими носіями інформації з обмеженим доступом.

Використання обладнання AJAX SYSTEMS у межах модернізації системи відеоспостереження є технічно, організаційно та економічно обґрунтованим рішенням. Обрані камери забезпечують високу якість зображення, стабільну роботу в різних умовах освітлення, захист каналів передавання даних за рахунок використання сучасних криптографічних механізмів, а також повну інтеграцію з іншими підсистемами безпеки. Можливість об’єднання відеоспостереження з охоронною сигналізацією, системами контролю доступу та централізованим програмним забезпеченням створює передумови для побудови єдиного інформаційно-аналітичного середовища безпеки об’єкта.

Уніфікація обладнання в межах однієї екосистеми значно спрощує експлуатацію, технічне обслуговування та адміністрування системи захисту. Це зменшує вимоги до кваліфікації обслуговуючого персоналу, скорочує час реагування на технічні несправності та знижує експлуатаційні витрати у довгостроковій перспективі. Крім того, обрана платформа дозволяє без суттєвих труднощів здійснювати подальше масштабування системи у разі розширення бізнес-центру, зміни режиму доступу або підвищення вимог до безпеки.

Проведений розрахунок вартості модернізації системи відеоспостереження показав, що реалізація запропонованих заходів не потребує значних фінансових витрат, оскільки може бути виконана на базі вже наявної інфраструктури з використанням резервних можливостей мережевого, комутаційного та

реєструючого обладнання. Такий підхід дозволяє оптимально використати наявні ресурси, уникнути дублювання функцій та зменшити капітальні витрати. Економічна доцільність проєкту також обумовлена потенційним зниженням ризиків інцидентів безпеки, матеріальних збитків і репутаційних втрат, пов’язаних із можливим витоком інформації.

Таким чином, реалізація запропонованих технічних і організаційних заходів у межах розробленої комплексної системи захисту сприятиме суттєвому підвищенню рівня фізичної та інформаційної безпеки бізнес-центру «Лідер». Запропоноване рішення забезпечує відповідність сучасним вимогам у сфері захисту інформації, враховує положення чинного законодавства та нормативних документів у галузі технічного захисту інформації, а також створює надійну основу для подальшого розвитку та вдосконалення системи безпеки об’єкта з обмеженим доступом у довгостроковій перспективі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2657-12

2. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

3. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2297-17

4. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2163-19

5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Київ: Держстандарт України, 1997.

6. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Київ: Держстандарт України, 1997.

7. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Київ: Держстандарт України, 1998.

8. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: ISO, 2022.

9. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection - Information security controls. Geneva: ISO, 2022.

10. ISO/IEC 27701:2019. Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Geneva: ISO, 2019.

11. IEC 62676-1-1:2013. Video surveillance systems for use in security applications - Part 1-1: System requirements - General. Geneva: IEC, 2013.

12. IEC 62676-1-2:2013. Video surveillance systems for use in security applications - Part 1-2: System requirements - Performance requirements for video transmission. Geneva: IEC, 2013.

13. IEC 62676-4:2014. Video surveillance systems for use in security applications - Part 4: Application guidelines. Geneva: IEC, 2014.

14. ONVIF. ONVIF Profiles: Profile S, Profile T and Profile M for IP-based physical security products. URL: https://www.onvif.org/profiles/

15. NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg: NIST, 2020.

16. NIST Special Publication 800-207. Zero Trust Architecture. Gaithersburg: NIST, 2020.

17. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments. Gaithersburg: NIST, 2012.

18. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. Gaithersburg: NIST, 2017.

19. ENISA. Guidelines for Securing the Internet of Things. Heraklion: European Union Agency for Cybersecurity, 2020.

20. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, 2016.

21. ETSI EN 303 645. Cyber Security for Consumer Internet of Things: Baseline Requirements. Sophia Antipolis: ETSI, 2020.

22. OWASP Foundation. OWASP Internet of Things Top 10 2018. URL: https://owasp.org/www-project-internet-of-things/

23. Center for Internet Security. CIS Critical Security Controls Version 8.1. East Greenbush: CIS, 2024.

24. Axis Communications. Network Video Fundamentals: Technical Guide. Lund: Axis Communications, 2023.

25. Szeliski R. Computer Vision: Algorithms and Applications. 2nd ed. Cham: Springer, 2022.

26. Gonzalez R. C., Woods R. E. Digital Image Processing. 4th ed. New York: Pearson, 2018.

27. Forsyth D. A., Ponce J. Computer Vision: A Modern Approach. 2nd ed. Boston: Pearson, 2012.

28. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge: MIT Press, 2016.

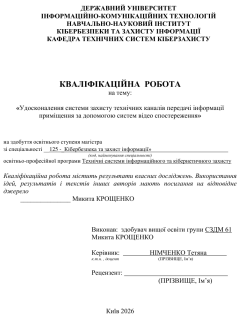
29. Bishop C. M. Pattern Recognition and Machine Learning. New York: Springer, 2006.

30. Kalbo N., Mirsky Y., Shabtai A., Elovici Y. The Security of IP-Based Video Surveillance Systems. ACM Computing Surveys, 2020. URL: https://arxiv.org/abs/1910.10749

ДОДАТКИ

Удосконалення системи захисту технічних каналів передачі інформації приміщення за допомогою систем відеоспостереження

- Магістерська робота: Микита КРОЩЕНКО
- Спеціальність 125 «Кібербезпека та захист інформації»
- Фокус: технічні канали витоку інформації, IP-відеоспостереження та відеоаналітика



ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА
на тему:

«Удосконалення системи захисту технічних каналів передачі інформації приміщення за допомогою систем відео спостереження»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
(код найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кіберзахисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Микита КРОЩЕНКО

Виконав: здобувач вищої освіти групи СЗІІМ 61
Микита КРОЩЕНКО

Керівник: _____ НІМЧЕНКО Тетяна _____
(ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2026

Актуальність дослідження

- Конфіденційна інформація має високий рівень конфіденційності та правового захисту.
- Матеріально-речові канали можуть призводити до витоку через документи, носії, відходи, доступ до приміщень.
- Системи відеоспостереження і контролю доступу формують базовий контур фізичного та інформаційного захисту.

Мета, об’єкт і предмет роботи

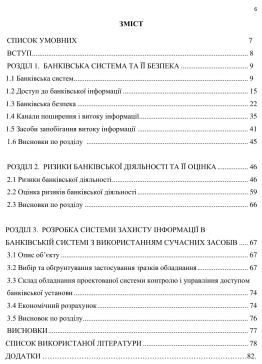
- Мета: підвищення ефективності захисту технічних матеріально-речових каналів передачі інформації об’єкта інформаційної діяльності.
- Об’єкт: система захисту каналів витоку конфіденційної інформації ОІД.
- Предмет: система захисту технічних матеріально-речових каналів із використанням відеоспостереження.

Основні завдання дослідження

- Проаналізувати об’єкт інформаційної діяльності та підходи до захисту конфіденційної інформації.
- Визначити ризики об’єкта інформаційної діяльності та оцінити небезпечні зони витоку.
- Розробити систему захисту інформації з використанням сучасних засобів відеоспостереження і СКУД.

Структура магістерської роботи

- Розділ 1 - об’єкт інформаційної діяльності, доступ до інформації.
- Розділ 2 - ризики об’єкта інформаційної діяльності та їх оцінювання.
- обладнання та економічним розрахунком.



6

ЗМІСТ

Конфіденційна інформація як об’єкт захисту

- Конфіденційна інформація поділяється на відкриту та інформацію з обмеженим доступом.
- захисту і внутрішні регламенти.
- Захист має поєднувати правові, організаційні та технічні заходи.

Матеріально-речові канали витоку інформації

- Канал формується через матеріальні носії, документи, відходи, друковані матеріали, носії пам’яті.
- Небезпека посилюється при неконтрольованому доступі до службових зон та робочих місць.
- Ефективний захист потребує зонування приміщень і реєстрації подій доступу.

Загрози об’єкту інформаційної діяльності

- Несанкціонований доступ до приміщень та службових зон.
- Винесення або копіювання документів і матеріальних носіїв.
- Порушення режиму зберігання інформації, людський фактор, недосконалий контроль подій.

Оцінка ризиків об’єкта інформаційної діяльності

- Ризик розглядається як поєднання ймовірності реалізації загрози та можливих збитків.
- Для ОІД критичними є операційні, інформаційні, репутаційні та правові наслідки інцидентів.
-
  засобів захисту.

Концепція захисту об’єкта

- Контроль периметра: камери, турнікети, електронні замки, датчики подій.
- Контроль службових приміщень: реєстрація входу/виходу, архів відео, журнал інцидентів.
- Контроль критичних зон: серверна, касова зона, архів, зона роботи з документами.

Система відеоспостереження

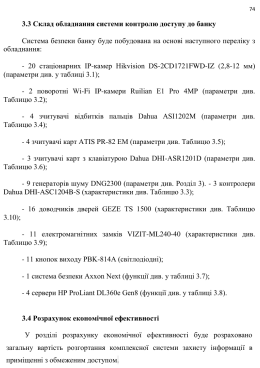
- Відеоспостереження забезпечує фіксацію подій, підтвердження інцидентів і профілактику порушень режиму.
- Камери доцільно розміщувати на входах, у коридорах, касових і службових приміщеннях.
- Архів відео має бути захищений від несанкціонованої зміни або видалення.

Система контролю і управління доступом

- СКУД забезпечує ідентифікацію користувачів, розмежування прав доступу та журналювання подій.
- Елементи: контролери, зчитувачі, електромагнітні замки, карти доступу, програмний модуль керування.
- Інтеграція СКУД з відеоспостереженням підвищує доказовість та оперативність реагування.

Обладнання проєктованої системи

- До складу системи входять IP-камери, відеореєстратор, комутатори, накопичувачі, контролери доступу.
- Вибір обладнання здійснюється за критеріями надійності, сумісності, вартості та достатності для об’єкта інформаційної діяльності.
-



74

3.3 Склад обладнання системи контролю доступу до банку

Система безпеки банку буде побудована на основі наступного переліку з обладнання:

- 20 стаціонарних IP-камер Hikvision DS-2CD1721FWD-IZ (2,8-12 мм) (параметри див. у таблиці 3.1);

- 2 поворотні Wi-Fi IP-камери Ruilian E1 Pro 4MP (параметри див. Таблицю 3.2);

- 4 зчитувачі відбитків пальців Dahua ASI1202M (параметри див. Таблицю 3.4);

- 4 зчитувачі карт ATIS PR-82 EM (параметри див. Таблицю 3.5);

- 3 зчитувачі карт з клавіатурою Dahua DHI-ASR1201D (параметри див. Таблицю 3.6);

- 9 генераторів шуму DNG2300 (параметри див. Розділ 3). - 3 контролери Dahua DHI-ASC1204B-S (характеристики див. Таблицю 3.3);

- 16 доводчиків дверей GEZE TS 1500 (характеристики див. Таблицю 3.10);

- 11 електромагнітних замків VIZIT-ML240-40 (характеристики див. Таблицю 3.9);

- 11 кнопок виходу PBK-814A (світлодіоди);

- 1 система безпеки Axxon Next (функції див. у таблиці 3.7);

- 4 сервери HP ProLiant DL360e Gen8 (функції див. у таблиці 3.8).

3.4 Розрахунок економічної ефективності

У розділі розрахунку економічної ефективності буде розраховано загальну вартість розгортання комплексної системи захисту інформації в приміщенні з обмеженим доступом.

Очікуваний ефект від впровадження

- Зменшення ризику несанкціонованого доступу до зон обробки конфіденційної інформації.
-
- Формування доказової бази під час розслідування інцидентів і порушень режиму.

Практичні рекомендації

- Виконати зонування приміщень за рівнем доступу до інформації.
- Налаштувати політику зберігання відеоархіву та журналів подій.
- Проводити регулярний аудит доступів, тестування обладнання і навчання персоналу.

Висновки

- Проаналізовано об’єкт інформаційної діяльності, конфіденційну інформацію та канали її витоку.
- Визначено ризики об’єкта інформаційної діяльності, пов’язані з матеріально-речовими каналами.
- підвищення рівня безпеки.