

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія забезпечення захисту інформації за рахунок використання
цифрових систем відеоспостереження»

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*

_____Максим ПЛОЩИНСЬКИЙ

Виконав: здобувач вищої освіти групи СЗДМ 61
Максим ПЛОЩИНСЬКИЙ

Керівник: _____Андрій КОТЕНКО_____
к.т.н., доцент

Рецензент: _____

Київ 2026

Кафедра Технічних систем кіберзахисту
 Ступінь вищої освіти магістр
 Спеціальність Кібербезпека та захист інформації
 Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

« _____ » _____ 2025 p.

Площинському Максиму Миколайовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Технологія забезпечення захисту інформації за рахунок використання цифрових систем відеоспостереження»
керівник кваліфікаційної роботи КОТЕНКО Андрій к.т.н., доцент
(ПРИЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій
від «30» жовтня 2025р. № 467
2. Строк подання кваліфікаційної роботи
3. Вихідні дані до кваліфікаційної роботи:
Загрози витоку інформації матеріально-речовим каналом
Цифрова система відеспостереження
Захист інформації від витоку матеріально-речовим каналом
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз загроз витоку інформації матеріально-речовим каналом
2. Аналіз складу системи відеоспостереження та принципу її функціонування
3. На основі проведеного аналізу обґрунтувати доцільність застосування цифрових систем відеоспостереження для забезпечення захисту інформації
5. Перелік графічного матеріалу: Презентаційний матеріал на 13 слайдах
6. Дата видачі завдання

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 _____ Максим ПЛОЩИНСЬКИЙ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ Андрій КОТЕНККО
(підпис) (Ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи: 74 стор., 16 рис., 17 джерел.

Об'єкт дослідження – Процес захисту інформації з обмеженим доступом

Предмет дослідження – Захист інформації з використанням цифрових систем відеоспостереження.

Мета роботи– Обґрунтування доцільності застосування цифрових систем відеоспостереження для забезпечення захисту інформації.

Методи дослідження – системний аналіз, чисельні методи, опрацювання літератури за даною темою.

У роботі досліджено загрози витоку інформації матеріально-речовим каналом. Проаналізовано склад та можливості цифрових систем відеоспостереження.

Ґрунтуючись на проведеному дослідженні зроблено висновок про доцільність застосування цифрових систем відеоспостереження для захисту інформації від витоку матеріально-речовим каналом.

Галузь використання –захист інформації на об'єкті інформаційної діяльності.

Апробація:

А.М. Котенко, М.М. Площинський, ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ЗА РАХУНОК ВИКОРИСТАННЯ ЦИФРОВИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем.* м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.18-19.
https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: МАТЕРІАЛЬНО-РЕЧОВИЙ КАНАЛ, ЗАГРОЗИ ІНФОРМАЦІЇ, СИСТЕМА ВІДЕОСПОСТЕРЕЖЕННЯ, ВІДЕОСПОСЕРВЕР, ВІДЕОКАМЕРА, ІДЕНТИФІКАЦІЯ, ВІДЕОАНАЛІТИКА ,ЦИФРОВИЙ СИГНАЛ.

ABSTRACT

The text part of the bachelor's (master's) qualification work: 74 pages, 16 figures, 17sources.

Object of research – Process of information protection with limited access.

Subject of research – Information protection using digital video surveillance systems.

Purpose of work – Substantiation of the feasibility of using digital video surveillance systems to ensure information protection.

Research methods – system analysis, numerical methods, literature review on this topic.

The paper investigates the threats of information leakage through the material channel. The composition and capabilities of digital video surveillance systems are analyzed.

Based on the research conducted, a conclusion is made about the feasibility of using digital video surveillance systems to protect information from leakage through the material channel.

Field of use - information protection at the object of information activity.

MATERIAL CHANNEL, INFORMATION THREATS, VIDEO SURVEILLANCE SYSTEM, VIDEO SERVER, VIDEO CAMERA, IDENTIFICATION, VIDEO ANALYTICS, DIGITAL SIGNAL.

ЗМІСТ

	стор.
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	8
ВСТУП.....	9
1 ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ НА ОБ’ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ.....	10
1.1 Причини виникнення технічних каналів витоку інформації.....	10
1.2 Матеріально-речовий канал.....	16
1.3 Система відеоспостереження.....	22
2 ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ЇЇ СКЛАДОВІ.....	30
2.1 Класифікація відеокамер.....	30
2.2 Середовища передачі відеоінформації.....	36
2.3 Засоби обробки і реєстрації відеосигналів.....	41
2.4 Пристрої відображення відеоінформації.....	47
3 ЗАСТОСУВАННЯ ЦИФРОВИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ НА ОБ’ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ.....	54
3.1 Розпізнавання образів системою відеоспостереження.....	54
3.2 Відеоаналітика у системах відеоспостереження.....	56
3.3 Забезпечення інформаційної безпеки з використанням інтелектуальних систем відеоспостереження.....	62
ВИСНОВКИ.....	71
ПЕРЕЛІК ПОСИЛАНЬ.....	73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АС – автоматизована система

BMP (Bitmap Picture) – формат зберігання зображень

ОІД – об'єкт інформаційної діяльності

СВС – системи відеоспостереження

ТВЛ – телевізійні лінії

LCD (liquidcrystaldisplay) – рідкокристалічний дисплей

CAP (CommonAlertingProtocol) – протокол передачі повідомлень

RGB – red, green, blue

ВСТУП

Актуальність дослідження. Питання інформаційної безпеки все більше виходять на перший план у сучасному світі. Важливо усвідомлювати стан захищеності ресурсів в інформаційній системі підприємства, щоб протистояти різним видам погроз її безпеки. Тому необхідність здійснення регулярного аналізу загроз та постійного моніторингу безпеки інформаційних систем потребує постійного удосконалення та огляду нових засобів захисту, які можна використовувати для підвищення безпеки.

Одним із технічних каналів витоку інформації є матеріально-речовий, який може принести великих фінансових втрат якщо буде порушена безпека інформації у ньому.

Зважаючи на швидкість розвитку нового світу, завдяки досягненням науки і техніки, було створено СВ, в яких втілено інтелектуальні функції, що дозволяють відстежувати рухомі об'єкти, аналізувати траєкторію руху, нестандартну поведінку, автоматично реєструвати можливі потенційно небезпечні предмети. Як відомо з досвіду, що запобігти проблемі простіше, ніж її вирішувати, саме така концепція закладена в основу інтелектуальних систем відеоспостереження (ІСВ).

Отже, існує необхідність використання таких систем з їх сучасними технологічними рішеннями для забезпечення безпеки інформації матеріально-речового каналу.

У зв'язку з цим можна зробити висновок, що тема магістерської роботи, присвяченої забезпеченню безпеки інформації матеріально-речового каналу є актуальною.

Об'єкт дослідження – Процес захисту інформації з обмеженим доступом

Предмет дослідження – Захист інформації з використанням цифрових систем відеоспостереження.

Мета роботи – Обґрунтування доцільності застосування цифрових систем відеоспостереження для забезпечення захисту інформації.

Наукові завдання:

проаналізувати загрози витоку інформації матеріально-речовим каналом;
проаналізувати склад системи відеоспостереження, та принцип її функціонування;

на основі проведеного аналізу обґрунтувати доцільність застосування цифрових систем відеоспостереження для забезпечення захисту інформації.

Методи дослідження – системний аналіз, чисельні методи, опрацювання літератури за даною темою.

Практичне значення одержаних результатів полягає у обґрунтуванні можливості застосування цифрових систем відеоспостереження для забезпечення захисту інформації від витоку матеріально-речовим каналом.

1 ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

1.1 Причини виникнення технічних каналів витоку інформації

Забезпечення кібербезпеки об'єктів є дуже важливим елементом у загальному комплексі заходів технічного захисту інформації. Несанкціоноване отримання інформації зловмисниками можливе шляхом її перехоплення.

Для того, щоб виявити яким саме чином має здійснюватись захист на ОІД за допомогою СВ необхідно перш за все розуміти, що собою являє ОІД, проаналізувати які існують загрози інформації на ОІД, канали витоку та дослідити засоби захисту.

Згідно розділу 3 НД ТЗІ 1.1-005-07 під об'єктом інформаційної діяльності розуміються будівлі, приміщення, транспортні засоби чи інші інженерно-технічні споруди, функціональне призначення яких передбачає обіг інформації з обмеженим доступом[1].

Загроза – одне з ключових понять у сфері забезпечення інформаційної безпеки. Загроза об'єкту інформаційної безпеки є сукупність факторів і умов, що виникають у процесі взаємодії різних об'єктів (їх елементів) і здатних чинити негативний вплив на конкретний об'єкт інформаційної діяльності [4].

Найбільшими видами загроз є: загрози порушення конфіденційності, загрози порушення цілісності, загрози порушення працездатності (доступності).

Загрози порушення конфіденційності спрямовані на розголошення інформації з обмеженим доступом.

Загрози порушення працездатності (доступності) спрямовані на створення ситуації, коли в результаті навмисних дій знижується працездатність обчислювальної системи, або її ресурси стають недоступними.

Загрози порушення цілісності полягають у спотворенні або зміні неавторизованим користувачем інформації, що зберігається або передається.

Цілісність інформації може бути порушена як зловмисником, так і в результаті об'єктивних впливів зі сторони середовища експлуатації системи [2].

Класифікація загроз може бути проведена за безліччю ознак. Найбільш поширені з них наведені далі:

- 1) За видом властивості інформації, що порушується:
 - загрози конфіденційності - витік, перехват, зняття, копіювання, викрадання, розголошення);
 - загрози цілісності: втрата, знищення, модифікація;
 - загрози доступності: блокування;
 - 2) За характером порушення:
 - порушення конфіденційності даних;
 - порушення працездатності серверів, мережевого обладнання, робочих станцій, незаконне втручання у функціонування серверів, мережевого обладнання, робочих станцій, тощо;
 - 3) За тяжкістю порушення:
 - незначні помилки;
 - дрібне хуліганство;
 - серйозний злочин / природні і техногенні катастрофи;
- За передбаченням наслідків порушника
- умисне порушення;
 - ненавмисне порушення;
- 4) За мотивацією:
 - зловмисне порушення;
 - незловмисне порушення;
 - 5) За закінченістю
 - закінчені;
 - незакінчені;
 - 6) За об'єктом дії:
 - загрози, націлені на всю інформаційну систему;
 - загрози, націлені на окремі компоненти;

- 7) За причиною виникнення
 - загрози, які виникли через недостачу засобів технічного захисту;
 - загрози, які виникли через недостачу організаційних заходів;
- 8) За походженням:
 - антропогенні;
 - техногенні;
 - природні;
- 9) За розміром нанесеної шкоди:
 - незначні;
 - значні;
 - критичні.
- 10) За типовими об'єктами інформатизації
 - загрози безпеці інформації на базі автономної ЕОМ (без підключення до обчислювальної мережі);
 - загрози безпеці інформації на базі локальної обчислювальної мережі (без підключення до розподіленої обчислювальної мережі);
 - загрози безпеці інформації, підключеної до розподіленої обчислювальної мережі;
- 11) За способом реалізації загроз безпеці інформації: загрози спеціальної дії на інформацію: механічної; хімічної; акустичної; біологічної; радіаційної; термічної; електромагнітної (електричні імпульси, електромагнітні випромінювання, магнітне поле), загрози несанкціонованого доступу (НСД), загрози витоку інформації технічними каналами:
 - по радіоканалу;
 - по електричному каналу;
 - по оптичному каналу;
 - по змішаним (параметричним) каналам;
 - загрози витоку по каналам побічних електромагнітних випромінювань і наводок;
- 12) За джерелом загрози, створені порушником:

- внутрішнім;

- зовнішнім;

створені апаратною закладкою:

- вбудованою;

- автономною;

створені шкідливими програмами:

- програмні віруси;

- шкодоносні програми, що можуть поширюватися мережею;

- інші шкідливі програми для здійснення НСД;

13) За використаною вразливістю системи:

- з використанням вразливості програмного забезпечення;

- з використанням вразливості, викликані наявністю апаратної вкладки;

- з використанням вразливості, пов'язаної з реалізацією протоколів мережевої взаємодії і каналів передачі даних;

- з використанням вразливості, викликані недоліками організації технічного захисту інформації від НСД;

- з використанням вразливості системи захисту інформації;

- з використанням вразливості програмно-апаратних засобів при збоях і позаштатних ситуаціях;

14) За об'єктом взаємодії, відносно інформації, яка обробляється на ЕОМ (вузли обчислювальної мережі):

- на відчужених носіях інформації;

- на вбудованих носіях довготривалого зберігання інформації;

- у засобах обробки і зберігання оперативної інформації;

- у портах вводу та виводу інформації;

15) Відносно інформації залежно від її рівня мережевої взаємодії:

- на фізичному рівні;

- на каналному рівні;

- на мережевому рівні;

- на транспортному рівні;
- на сеансовому рівні;
- на презентаційному рівні;
- на прикладному рівні

16) Відносно інформації користувачів або технологічної інформації залежно від способу доступу:

- загрози операційного середовища (до команд, інструкцій);
- загрози дії на технологічну інформацію, не пов'язані з допуском порушника до команд операційної системи (відмова в обслуговуванні при перевантаженні, збій операційної системи);
- загрози програмно-математичної дії;

Канал витоку інформації – сукупність джерела інформації, матеріального носія або середовища поширення, що несе зазначену інформацію сигналу й засобу виділення інформації із сигналу або носія. Класифікація каналів витоку інформації представлена на рис. 1.1.

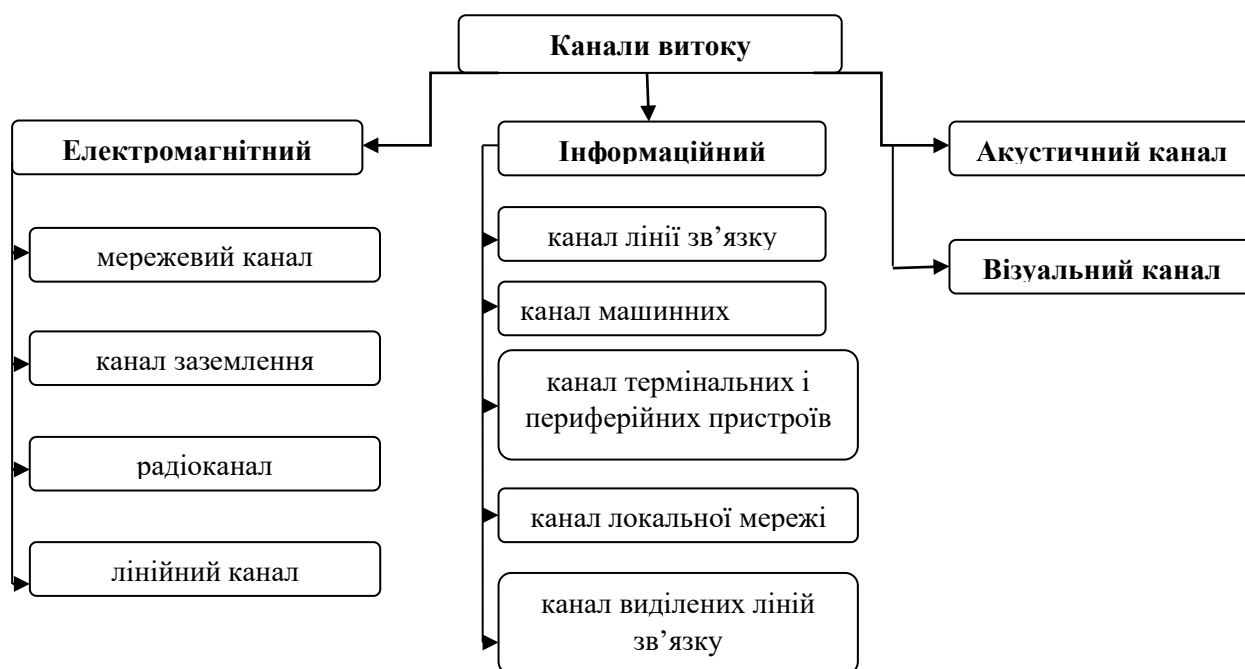


Рис. 1.1 Канали витоку інформації

Каналами витоку інформації на ОІД є:

1. Електромагнітний канал. Причиною його виникнення є електромагнітне поле, пов'язане із проходженням електричного струму а апаратних АС. Електромагнітне поле може індукувати струм в близько розташованих провідних лініях. Електромагнітний канал поділяється:

- радіоканал (високочастотне випромінювання);
- мережевий канал (наведення на мережу);
- канал заземлення (наведення на проведення заземлення);
- лінійний канал (наведення на лінії зв'язку між комп'ютерними системами).

2. Акустичний (віброакустичний) канал. Пов'язаний з поширенням звукових хвиль у повітрі або пружних коливаннях в інших середовищах, що виникають при роботі пристроїв відображення інформації в АС.

3. Візуальний канал. Пов'язаний з можливістю візуального спостереження зломисником за роботою пристроїв відображення інформації АС без проникнення в приміщення, де розташовані компоненти системи. Як засіб одержання інформації в цьому випадку можуть розглядати фотокамери, відеокамери і т.д

4. Інформаційний канал. Пов'язаний з доступом до елементів АС, носіїв інформації, програмного забезпечення, а також з підключенням до ліній зв'язку. Інформаційний канал може бути розділений на:

- канал лінії зв'язку;
- канал виділених ліній зв'язку;
- канал локальної мережі;
- канал машинних носіїв інформації;
- канал термінальних і периферійних пристроїв [1].

Після визначення основних загроз і каналів витоку інформації, необхідно окреслити запобіжні заходи для запобігання несанкціонованому доступу на ОІД, які включають:

для перешкоджання проникненню на контрольовану зону — огороження, двері, ґрати;

для виявлення факту проникнення в контрольовану зону або перебування в ній і сигналізації про це – системи охоронної сигналізації, до складу яких входять сповіщувачі охоронної сигналізації, системи зв'язку, приймально-контрольні прилади;

для виявлення і впізнання порушника (зловмисника) – СВ;

для усунення загрози – засоби фізичної безпеки [3]

Державні служби, правоохоронні органи та приватні силові структури деколи не в змозі охопити в повному обсязі необхідний рівень безпеки всіх об'єктів різних форм власності, тому керівники організацій, установ та підприємств були змушені шукати власні шляхи вирішення проблем безпеки. В першу чергу створюються служби безпеки з широким асортиментом технічних засобів і систем. Однією із основних систем виявлення порушень стала ІСВ, оскільки першочергово аналізує і реагує на порушення у нормальній роботі на ОІД, тож для розуміння важливості обрання саме ІСВ, розглянемо завдання, що вона вирішує і які функції виконує у наступних пунктах.

1.2 Матеріально-речовий канал

Особливість цього каналу викликана специфікою джерел і носіїв інформації в порівнянні з іншими каналами. Джерелами і носіями інформації в ньому є суб'єкти (люди) і матеріальні об'єкти (макро і мікрочастинки), які мають чіткі просторові межі локалізації, за винятком випромінювань радіоактивних речовин. Витік інформації в цих каналах супроводжується фізичним переміщенням людей і матеріальних тіл з інформацією за межами контрольованої зони. Для більш чіткого опису розглянутого каналу доцільно уточнити склад джерел і носіїв інформації.

У загальному випадку структура матеріально-речового каналу представлена на (рис.1.2).



Рис. 1.2 Структура матеріально-речового каналу витоку інформації

Основними джерелами витоку інформації з матеріально-речового каналу є наступні[2], [3]:

- чернетки різних документів і макети матеріалів, вузлів, блоків, пристроїв, що розробляються в ході науково-дослідних і дослідно-конструкторських робіт, які ведуться в організації;
- магнітні та інші носії інформації ПЕОМ, на яких під час експлуатації містилася інформація з обмеженим доступом;
- бракована продукція та її елементи;
- секретні бібліотеки;
- інші місця зберігання матеріальних носіїв ІЗОД.

Перенесення інформації в матеріально-речовому каналі може здійснюватися такими суб'єктами та середовищами:

- співробітниками організації;
- повітряними атмосферними масами;
- рідкими середовищами.

Перенесення інформації в цьому каналі за межі контрольованої зони можливий наступними суб'єктами та об'єктами:

- співробітниками організації;
- повітряними масами атмосфери;
- рідким середовищем;

Ці носії можуть переносити всі види інформації: семантичну і ознаковими, а також демаскуючі речовини.

Семантична інформація міститься в чернетках документів, схем, креслень;

- інформація про видових і сигнальних демаскеруючих ознаках в бракованих вузлах і деталях, в характеристиках радіоактивних випромінювань тощо;

- демаскуючі речовини - в газоподібних, рідких і твердих відходах виробництва.

Приймачі інформації цього каналу досить різноманітні. Це експерти зарубіжної розвідки або конкурента, прилади для фізичного та хімічного аналізу, засоби обчислювальної техніки, приймачі радіоактивних випромінювань та ін [3].

Втрати носіїв з цінною інформацією можливі при відсутності в організації чіткої системи обліку її носіїв. Наприклад, зіпсований співробітником аркуш звіту може бути викинутий їм у кошик для паперу, з якого він буде прибиральницею перенесений в бак для сміття на території організації, а далі при перевантаженні бака або транспортуванні сміття на звалище лист може бути винесений вітром і піднятий перехожим. Звичайно, ймовірність забезпечення випадкового контакту з цим листом зловмисника невелика, але якщо останній активно займається добуванням інформації, то область простору, в якому можливий контакт, значно звужується і ймовірність витоку підвищується.

Відходи можуть продаватися іншим підприємствам для використання у виробництві іншої продукції, очищатися перед зливом у водойми, знищуватися або піддаватися захороненню на час саморуйнування або розпаду. Останні операції виконуються для високотоксичних речовин, утилізація яких іншими способами економічно недоцільна, і для радіоактивних відходів, які не можна нейтралізувати фізичними або хімічними способами.

Різноманіття розглянутих можливостей витоку інформації надає зловмисникові великий вибір шляхів, способів і засобів добування інформації. На основі результатів аналізу кожного з розглянутих каналів можна зробити наступні висновки.

1. Витік семантичної інформації можлива за всіма технічними каналами. По можливостях, а отже за загрозою безпеки інформації їх можна проранжувати в наступній послідовності: радіоелектронний, акустичний і оптичний канали. Проте в деяких конкретних умовах можливі інші ранги каналів, наприклад, коли є реальна передумова для спостереження або фотографування документів.

2. До демаскуючих ознаках об'єктів відносяться:

- ознаки діяльності: рух транспортних машин, звуки, вогні, спалахи, дим, пил;
- здатність відображати і випускати різні випромінювання (електромагнітні, інфрачервоні, теплові), уловлювані спеціальними приладами;
- сліди діяльності: стежки і дороги, залишки виробничих матеріалів, побутове сміття і т.д .;
- характерні обриси (форма), розміри і особливості розташування об'єктів;
- колір поверхні об'єктів, а в деяких випадках і блиск її (блиск скла, відблиск металу);
- тіні, падаючі від об'єктів, а також тіні на поверхні самих об'єктів.
- ознаки, що характеризують фізичні властивості речовини об'єкта (теплопровідність, електропровідність, структура, твердість і т. д.);
- ознаки, що характеризують фізичні поля, створювані об'єктами (електромагнітні, радіаційні, акустичні, гравітаційні та ін.);
- ознаки, що характеризують форму, колір, розміри об'єкту і його елементів;
- просторові ознаки, що характеризують як координати об'єкта, так і їх похідні для рухомого об'єкту;

- ознаки, що характеризують наявність певних зв'язків між об'єктами і їх елементами;

- ознаки, що характеризують результати функціонування об'єктів (задимленість, запиленість, сліди об'єкта на ґрунті, забруднення води і повітря і т. д.).

Виявлення об'єкту проводиться за його демаскуючою ознаками, які діляться на три групи: видові, ознаки діяльності і розташування.

До видовим демаскуючою ознак належать фізичні властивості об'єкта (здатність відбивати випромінювання оптичного і радіолокаційного діапазонів хвиль, випромінювати енергію в тепловому діапазоні) і геометричні властивості (форма, розмір об'єкта та його окремих деталей). Демаскуючі ознаки діяльності проявляються в результаті дій об'єкта (переміщення, зміна навколишнього середовища та ін.). Ознаки розташування характеризуються становищем об'єктів щодо місцевих предметів. При дешифруванні спостерігач має справу не з самими демаскуючими ознаками, а з носіями первинної інформації про них, які можуть мати різну фізичну основу. Носіями демаскуючих ознак є фізичні поля. Отже, параметри фізичних полів об'єктів і є їх демаскуючими ознаками [6], [8].

Найбільшими потенційними можливостями здобування інформації про видові демаскуючі ознаки володіє оптичний канал, в якому інформація видобувається шляхом фотографування. Це обумовлено наступними особливостями фотозображення:

- має найвище дозвіл навіть на великій відстані від об'єкта спостереження, наприклад, при детальній фотозйомці з космосу воно досягає 10-15 см на місцевості;

- має найвищу інформаційну ємність, обумовлену максимумом демаскуючих ознак, у тому числі наявністю такого інформативного ознаки як колір;

- забезпечує відносно низький рівень геометричних спотворень.

Інформаційні ємності телевізійних зображень приблизно на порядок нижче фотозображень. Телевізійні зображення мають гірше дозвіл, підвищений

рівень яскравості спотворень за рахунок нерівномірності спектрально-характеристик яскравості приладів із зарядним зв'язком, підвищений рівень геометричних спотворень за рахунок додаткових спотворень при формуванні електронного растра.

Зображення в ІЧ-діапазоні володіють ще більш низькими інформаційними параметрами. Крім низької роздільної здатності і великих спотворень для зображень в ІЧ-діапазоні характерна крайня мінливість яскравості протягом доби.

Однак, як уже зазначалося при розгляді каналів витоку інформації, зображення в кожному з них містить додаткові ознаки за рахунок різної їхньої природи.

Основним каналом здобуття сигнальних демаскуючих ознак є радіоелектронний. У значно меншому обсязі витік інформації про сигнальних демаскуючих ознаках можлива в акустичному каналі [7].

Для добування інформації зловмисник, як правило, використовує кілька каналів її витоку. Комплексне використання каналів витоку інформації ґрунтується на наступних принципах[8]:

- комплексируємі канали доповнюють один одного за своїми можливостями;

- ефективність комплексування підвищується при зменшенні залежності між джерелами інформації та демаскуючими ознаками в різних каналах.

Комплексування каналів витоку інформації забезпечує:

- збільшення ймовірності виявлення і розпізнавання об'єктів за рахунок розширення їх поточних ознакових структур;

- підвищення достовірності семантичної інформації і точності вимірювання ознак, особливо у разі добування інформації з недостатньо надійних джерел.

Класифікація матеріально-речових каналів витоку інформації[2].

У практиці розвідки широко використовується отримання інформації з відходів виробничої та трудової діяльності. Залежно від профілю роботи

підприємства це можуть бути зіпсовані накладні, фрагменти складаються документів, чернетки листів, браковані заготовки деталей, панелей, кожухів та інших пристроїв для розроблюваних підприємством нових моделей різної техніки. Особливе місце серед такого роду джерел займають залишки бойової техніки і озброєння на випробувальних полігонах.

1.3 Система відеоспостереження

Загально прийнятим визначенням СВ, в інформаційному середовищі є: система відеоспостереження – це програмно-апаратне рішення, яке на основі аналізу відеозображень дозволяє розрізняти, ідентифікувати і відстежувати рухомі об'єкти, що знаходяться в полі зору камер спостереження.

Простішими словами, повноцінна СВ повинна не тільки «спостерігати», а й «реєструвати» все що відбувається, тобто, інтелектуально обробляти сигнал з відеокамери і автоматично фіксувати увагу охорони на підозрілих об'єктах. Так можна знизити витрати на операторів і зменшити вплив «людського фактора». Найбільш поширеними завданнями СВ є:

- контроль проникнення на об'єкт (дім, квартира, великі підприємства, офіси, та ін.);

- здійснювати аналіз подій, як в реальному часі, так і шляхом ретроспективного аналізу;

- здійснювати конфіденційність доступу до даних і відеоматеріалів;

- системи відстеження несанкціонованого перетину кордону великої протяжності, що охороняється (державний кордон);

- підтримка списку осіб, які перебувають на об'єкті, через ідентифікацію особистості людини, що проникають або залишають об'єкт;

- системи контролю і управління доступом на підприємствах та інших ОІД;

- виявлення підозрілої поведінки в торгівельних центрах з метою виявлення крадіїв;

виявлення агресивно налаштованих, нетверезих та інших категорій людей, потенційно небезпечних для оточуючих;

виявлення порушень правопорядку за рахунок розпізнавання облич;

виявлення забутих чи залишених речей на вокзалах, в аеропортах з метою запобігання терористичним актам;

автоматичний збір статистики про переміщення об'єктів;

підрахунок кількості людей в місцях масового скупчення (торгові центри, вокзали, стадіони) з метою збору статистики і забезпечення безпеки;

аналітика даних, отримання від супутника чи безпілотної літачки, для пошуку чи відстеження переміщення людей, техніки;

автоматичне виявлення пожежі;

контроль завантаженості автомобільних доріг і виявлення дорожньо-транспортних пригод;

пошук викрадених автомобілів за допомогою відео спостереження за дорогами;

контроль процесу виробництва і якості виготовленої продукції;

контроль за дотриманням правил дорожнього руху. [4]/

Саме такі функції виконує система відеоспостереження при виявленні різного роду порушення у роботі тієї чи іншої галузі людської діяльності.

Перспективи використання СВ:

- можливість побудови розподілених систем;
- віддалений доступ до управління відео зображень, архівів з будь-якої точки планети, без погіршення якості зображення;
- інтелектуальний детектор руху;
- висока функціональність і можливість налаштування;
- необмежені можливості конфігурації;
- високі характеристики швидкості введення і якості запису;
- автоматичний моніторинг зони, що охороняється та відповідна обробка відеоданих, одержуваних від камер;
- високе розподільна здатність і швидкість запису;

- триплекс: запис, спостереження і перегляд архіву одночасно;
- необмежений час зберігання інформації і необмежене число копій без погіршення якості;
- миттєвий доступ до будь-якої частини архіву відеозаписів;
- наявність системи оповіщення E-mail, відправки SMS-повідомлень про порушення режиму безпеки;
- запис звуку синхронно з відео;
- обробка зображень в реальному часі [5] [6].

Нові СВ все частіше будуються із IP-камер і цифрових систем обробки і/або серверів та відповідного програмного забезпечення. Пристроями для перегляду відеоінформації можуть бути – смартфони, планшети, ноутбуки, традиційні комп'ютери, а також хмарні технології. Тобто відбувається тенденція змін аналогового до цифрового відео спостереження, від дротової до бездротової передачі інформації і звісно вдосконалення звичайної СВ до системи розумної, що має інтелект.

Якщо розглядати елементарні складові СВ, то мінімальна система конфігурації матиме наступний вигляд: відеокамера, канал передачі відеосигналу, пристрій обробки та запису, пристрій відображення.

Структурна схема СВ, зображена на рис. 1.3.

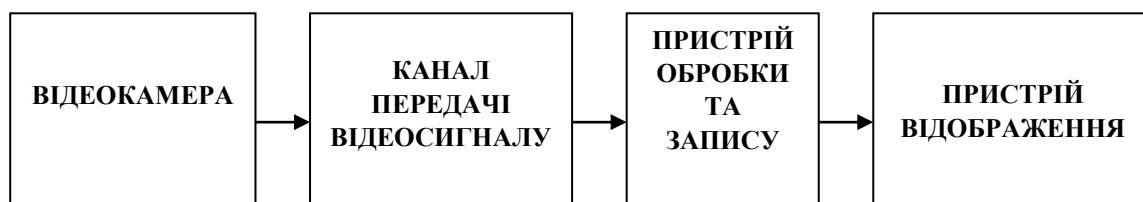


Рис. 1.3 Структурна схема системи відеоспостереження

Відеокамера– основний пристрій складової ІСВ, формує відеосигнал зі світлового потоку, що проходить через її об'єктив та потрапляє на матрицю.

Дуже важливим компонентом будь якої системи відео спостереження є середовище передачі сигналу – кабельна мережа і система живлення. При

побудові СВ з використанням новітніх технологій, кабельна система будується за принципами локальної комп'ютерної мережі і може використовувати різне фізичне середовище для передачі інформації – мідний кабель типу «вита пара», оптичний кабель, бездротова мережа та ін.. Для живлення камер може використовуватись силовий кабель, але останнім часом набирають популярності технології POE (poweroverEthernet), де живлення і дані передаються по одному кабелю – вита пара. Передача відеосигналу від камери до пристрою обробки традиційно проводиться коаксіальним кабелем з хвильовим опором 75 Ом, але все ж таки найбільш прогресивним є застосування кабелю «вита пара».

Найчастіше від якості компонентів і застосовуваних матеріалів кабельної мережі і устаткування живлення залежить якість системи відеоспостереження в цілому. Власне при передачі відеосигналу на відстань і виникають інженерні завдання з побудови якісної СВ, тобто на першому плані при проектуванні і реалізації виходить вибір середовища передачі, грамотного розрахунку кабельної або бездротової мережі з урахуванням постійно зростаючої роздільної здатності відеокамер і пристроїв обробки.

Пристрої обробки та запису – відеореєстратор, відеосервери дозволяють обробляти потоки інформації, одержувані від камер, аналізувати відео потоки, записувати їх і видавати в заданому форматі на монітор і в локальну або глобальну мережу для віддаленого перегляду.

В якості пристроїв відображення інформації для СВ застосовуються комп'ютерні монітори, а також за допомогою прикладних програм або web-браузера на екрані мобільного телефону [7].

Вимоги керівних документів до систем відеоспостереження.

Одним з основних керівних документів включають вимоги до систем відеоспостереження є ДСанПіН 3.3.2.007, СанПіН 239, ДСанПіН 3.3.6-96.. Цей документ містить вимоги раніше виданих керівних документів. Розглянемо основні його положення, що стосуються систем відеоспостереження.

Згідно ДСанПіН 3.3.2.007, СанПіН 239, ДСанПіН 3.3.6-96. системи охоронного телебачення (СОТ) повинні забезпечувати передачу візуальної

інформації про стан охоронних зон, приміщень, периметра і території об'єкта в приміщенні охорони. Застосування охоронного телебачення дозволяє в разі отримання сповіщення про тривогу визначити характер порушення, місце порушення, напрямок руху порушника і визначити оптимальні заходи протидії. Крім того, система охоронного телебачення дозволяє проводити спостереження охоронюваних зон об'єкта.

До складу СОТ, згідно з ГОСТ В 20.57.306–76. Входять[7]:

1.) Обов'язкові пристрої для всіх СОТ:

- відеомонітор;
- лінії зв'язку.
- джерело електроживлення, в тому числі резервний;
- телевізійна камера (ТК);

2.) Додаткові пристрої для конкретних СОТ:

- відеонакопичувач.
- виявитель руху;
- пристрій керування і комутації відеосигналів;

На об'єкті ТК слід обладнати:

- КПП;
- периметр території;
- головний і службові входи;
- приміщення, в яких безпосередньо зосереджені матеріальні цінності,

за винятком сховищ цінностей;

- приміщення, коридори, по яким здійснюється переміщення грошових коштів і матеріальних цінностей;

- інші приміщення за розсудом керівництва (власника) об'єкта або за рекомендацією співробітника підрозділу позавідомчої охорони.

В охороні об'єктів повинні використовуватися системи чорно-білого і кольорового зображення. Встановлення тієї чи іншої системи залежить від необхідної інформативності СОТ, характеристик об'єкту, що охороняється

(розташування на місцевості, освітленість та інших ознак) і можливих цілей (автомобіль, людина і інших цілей).

Робота апаратних засобів СОТ повинна бути синхронізована.

ТК, призначені для контролю території об'єкта або її периметра, повинні розміщуватися в герметичних термокожухах, мають сонцезахисний козирок і повинні бути орієнтовані на місцевості під кутом до лінії горизонту (промені вранішнього та вечірнього сонця не повинні потрапляти в об'єктив ТК). Розміщення ТК повинно перешкоджати їх умисного пошкодження.

У темний час доби, якщо освітленість зони, що охороняється нижче чутливості ТК, об'єкт (зона об'єкта) повинен обладнуватися охоронним освітленням видимого або інфрачервоного діапазону. Зони охоронного освітлення повинні збігатися з зоною огляду ТК. При використанні СОТ кольорового зображення застосування інфрачервоного освітлення недопустимо.

Для спостереження за допомогою однієї ТК великих територій об'єкта рекомендується застосовувати об'єктиви із змінною фокусною відстанню і поворотні пристрої з дистанційним управлінням.

У приміщеннях об'єкта слід використовувати ТК з електронним затвором, укомплектовані об'єктив з ручним регулюванням діафрагми.

Поза приміщень об'єкта (на вулиці) слід комплектувати ТК об'єктивом з автоматичним регулюванням діафрагми.

Для відображення надходить з ТК інформації повинні застосовуватися спеціальні монітори, здатні працювати цілодобово протягом тривалого часу з нерухомим зображенням.

В СОТ слід використовувати виявителі руху, які перетворюють ТК в охоронний сповіщувач, який видає сигнал тривоги на внутрішній пульт охорони об'єкта або ПЦО при появі в нулі зору ТК рухомій цілі.

При необхідності записи телевізійних зображень повинні застосовуватися відеонакопичувач: спеціальні відеомагнітофони (СВМ) з тривалим часом запису або цифрові відеонакопичувач інформації.

Час запису СВМ повинно бути не більше 24 годин на 3-х годинну відеокасету. Використання СВМ з великим часом запису допускається тільки при забезпеченні автоматичного перекладу його, у разі надходження повідомлення про тривогу, режим запису в реальному часі. Повідомлення про тривогу може надходити на відеомагнітофон від візерунок руху або інших систем безпеки об'єкта (охоронної, пожежної, тривожної сигналізації та інших).

Для запису зображення від багатьох МК на один відеонакопичувач необхідно використовувати мультиплексори.

Час реагування СОТ на сигнал сповіщення про тривогу повинно бути не більше часу, достатнього на подолання порушником, які рухаються зі швидкістю 3 м/с, половини зони спостереження ТК по ширині, в будь-якому місці зони.

Допускається використовувати системи з великим часом реагування при наявності функції відкату зображення.

В якості пристроїв керування і комутації відеосигналів, що надходять з телевізійних камер, слід використовувати послідовні перемикачі, квадратори, матричні комутатори. Вони повинні забезпечувати послідовне або поліекранний відтворення зображень від усіх ТК.

Пристрої керування і комутації повинні забезпечувати пріоритетне автоматичне відображення на екрані моніторів зон, звідки надійшло повідомлення про тривогу.

Конструктивно СОТ повинні будуватися за модульним принципом і забезпечувати:

- зручність технічного обслуговування і експлуатації, а також ремонтпридатність;
- взаємозамінність змінних однотипних технічних засобів;
- виключення несанкціонованого доступу до елементів управління;
- санкціонований доступ до всіх елементів, вузлів і блоків, що потребують регулювання, обслуговування або заміни в процесі експлуатації.

Облік вимог і рекомендацій керівних документів дозволить створити надійну систему відеоспостереження.

Висновок до першого розділу:

Встановлено, що існують види інформації які підлягають захисту. Встановлені критерії інформаційної безпеки: конфіденційність, цілісність, доступність

Можна зазначити, що перевага СВ в порівнянні з іншими охоронними системами, полягає у високій інформативності (90% всієї інформації про навколишній світ людина отримує завдяки органам зору).

2 ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ТА ЇЇ СКЛАДОВІ

2.1 Класифікація відеокамер

Відеокамери можна класифікувати за призначенням та особливостями конструкції/

За призначенням відносно місця встановлення (умов експлуатації) камери можна поділити на[7]. [8]:

- зовнішнього використання (вуличні, фасадні)
- внутрішнього використання (для приміщень)

Камери для зовнішнього використання передбачають встановлення на вулиці, а саме на фасадах будівель або спеціальних конструкціях – стовпах, опорах, траверсах. Для такого типу камер одною з вимог є забезпечення працездатності в умовах агресивного середовища – за любых погодних умов. Їх конструкція передбачає корпус або кожух, здатний підтримувати задані температур та вологість. Також зовнішня камера має бути обладнана антивандальним захистом. Окрім цього передбачається, що камера буде встановлена значно далі від монітора спостереження або реєстратора на відміну від внутрішньої, тому камера та середовище передачі даних в такому випадку має забезпечити передачу даних без втрат. За типом конструкції такі камери можуть бути купольними, циліндричними або поворотними.

Камери для внутрішнього використання зазвичай мають менші габарити ніж зовнішні, також на відміну від зовнішніх вимоги до герметичності та антивандальності є значно меншими. Враховуючи, що встановлення камери частіше всього відбувається у вже сформований інтер'єр, повинна бути присутня також естетична складова.

За виконанням камери можна поділити на:

- Циліндричні (Bullet), виконуються у вигляді герметичного циліндру, являючи собою рішення «відеокамера+об'єктив». Могуть оснащуватись

автоматичним регулюванням діафрагми, у такому випадку можна їх застосовувати у якості зовнішніх. Можуть обладнуватись ІЧ-підсвіткою та кронштейном для зручності монтажу



Рис. 2.1 Циліндрична вулична IP відеокамера

- Безкорпусні (модульні) являють собою плату без корпусу, є найкращим рішенням для прихованого спостереження.



Рис. 2.2 Безкорпусна відеокамера

- Купольні (Dome) – відеокамера в корпусі напівсферичної форми, має об'єктив. Зазвичай призначені для монтажу на стелю.

- Поворотні (PTZ) – відмінний варіант для спостереження в реальному часі, оскільки направленість та фокусна відстань може коригуватись оператором.



Рис. 2.3 Поворотнавідеокамера

- Панорамні «риб'яче око» (FishEye) – вид камер, який забезпечує всебічний огляд над зоною відеоспостереження, що дозволяє зменшити кількість камер (і відповідно інфраструктури) на об'єкті. Є ефективною в великих приміщеннях або на відкритому просторі. Неефективна у приміщеннях лабіринтного типу.

- Мініатюрні. Мають дуже компактні розміри – 1*1, 2*2 см. Використовуються, як і безкорпусні, для прихованої зйомки. В силу малих розмірів присутня значна втрата якості.



Рис. 2.4 Мініатюрнівідеокамери

За властивостями технології запису(типом відеосигналу) камери бувають аналоговими та мережевими (так звані IP-камери).

Основні параметри відеокамер[8]:

Основними характеристиками камер, що впливають на якість і вартість:

- 1) кольоровість;
- 2) мінімальна освітленість;
- 3) роздільна здатність;
- 4) характеристика матриці;
- 5) виробник.

Коротко оцінимо кожен з характеристик вищевказаних пунктів:

а) Кольоровість. Камери бувають кольорові і чорно-білі. Може здатися дивним, те що в століття цифрових технологій досі використовуються чорно-білі камери. Адже кольорове зображення дивитися набагато приємніше. Насправді в цьому немає нічого дивного. У першу чергу чорно-білі камери цікаві невисокою вартістю. Чорно-біла камера може коштувати в рази дешевше кольорової. У другу чергу, чорно-білі камери набагато краще бачать в темний час доби, ніж кольорові. Більше того, кольорові камери в темряві абсолютно нічого не бачать. Всі кольорові камери при настанні темряви перемикаються в чорно-білий режим. Але іноді кольорове зображення буває вкрай важливе, наприклад при точній ідентифікації зловмисника (колір волосся, одяг, взуття), тим паче при умові встановлення ІСВ.

б) Мінімальна освітленість – можливість камери якісно розрізняти картинку перед собою в темний час доби. Вимірюється даний параметр в люксах (Лк). Тобто, якщо мінімальна освітленість камери 10Лк, це означає, що при освітленості 10Лк камера буде бачити. А от при освітленості 9Лк – вже ні. Природно чим нижче дане значення, тим при більш низькій освітленості здатна бачити камера, тим краще. Однак виробники часто заявляють для своїх камер рівень «мінімальної освітленості» нижче реального, пояснюючи свої дії тим, що заявлений рівень був виміряний при використанні спеціальних підсилювачів, розташованих у середині камери. Середнім значенням на сьогоднішній день є

освітленість 0,1Лк. Тобто середньостатистична камера «бачить» практично без світла.

в) Роздільна здатність камери – кількісний вимір чіткості зображення. Вимірюється в телевізійних лініях (ТВЛ). Чим більше ТВЛ може показати камера, тим чіткіше буде зображення на моніторі. Середній показник – 420 ТВЛ. Відмінний – 640 ТВЛ. Тут все просто, чим більше ТВЛ, тим краще і дорожче. Проте досвід показує, що людське око насилу розрізняє різницю у роздільній здатності, якщо вона становить менше 50 ТВЛ.

г) Матриця камери – елемент, що сприяє зображенню і перетворює його в електричний сигнал. Це ключовий елемент камери. Розглянемо деякі характеристики матриць:

- розмір матриць. Сама матриця виглядає таким чином: піксель – найдрібніший елемент матриці, що сприймає світло. Чим більше цих елементів і чим вони більше, тим краще. Чим більше пікселів – тим чіткіша картинка, краща передача кольору, яскравіше зображення. Кількість пікселів можна умовно визначити виходячи з роздільної здатності камери. Тобто чим більше ТВЛ заявлено, тим більше пікселів в камері. Розмір пікселів визначається виходячи з розміру матриці (вказується в дюймах). Наприклад «1/3» означає, що розмір матриці третина дюйма. Чим менше число в знаменнику, тим матриця більша, а відповідно краща;

- тип сенсора. На сьогоднішній день найбільш поширеними є два типи сенсорів CMOS (КМОС) і CCD. CMOS – більш сучасна технологія. Матриця CMOS споживає менше енергії, коштує дешевше, ніж CCD, але за якістю поступається.

Після проходження через об'єктив світло фокусується на датчику зображення камери. Датчик зображення складається з великої кількості фотоелементів, і кожен фотоелемент відповідає елементу зображення на датчику зображення, більш відомому під назвою «піксель». Кожен піксель датчика зображення фіксує кількість світла, яке потрапило на нього, і перетворює його в відповідну кількість електронів. Чим яскравіше світло, тим більше породжується

електронів. Існують дві основні технології, які можна використовувати при створенні датчиків зображення:

- ПЗЗ (CCD) (прилад із зарядним зв'язком).
- КМОН (CMOS) (комплементарний метало-оксидний напівпровідник).

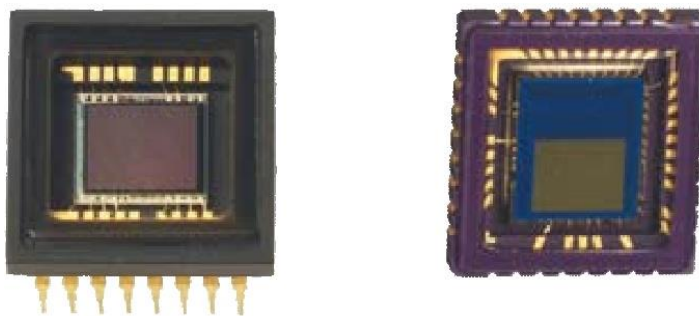


Рис 2.5 Матриці відеокамер ПЗЗ (ліворуч) і КМОН (праворуч).

Хоча ПЗЗ - і КМОН - датчики часто розглядають як конкурентів, кожен з них має свої сильні і слабкі сторони, які роблять їх придатними для різних застосувань. ПЗЗ - датчики виробляються за технологією, яка була спеціально розроблена для виробництва камер. Раніше КМОН - датчики були засновані на стандартній технології, яка вже широко використовувалася, наприклад, в мікросхемах пам'яті ПК. Сучасні КМОН - датчики використовують більш спеціалізовану технологію і їх якість швидко поліпшується.

ПЗЗ - технологія

ПЗЗ - датчики використовуються в камерах вже більше тридцяти років і володіють великою кількістю привабливих властивостей. Якщо коротко, то у них трохи краще світлочутливість і менше шуми, ніж у КМОН - датчиків. Більш висока світлочутливість забезпечує краще зображення при низькому освітленні. Однак вони дорожче і їх складніше вбудовувати в камеру. Крім того, ПЗЗ - датчик може споживати до 100 разів більше потужності, ніж КМОН.

КМОН – технологія.

Сучасні успіхи в розробці КМОН - датчиків наблизили їх до ПЗЗ - суперникам у сенсі якості зображення. КМОН - датчики знижують загальну вартість камери, оскільки містять усю необхідну логіку для побудови камери. КМОН - датчики надають, в порівнянні з ПЗЗ, більше можливостей для інтеграції і більше функцій.

У КМОН - датчиків більш швидке зчитування даних (що є перевагою, якщо потрібні зображення з великою роздільною здатністю), менше потужність розсіювання на рівні кристала, а також менше розмір системи. Мегапіксельні КМОН - датчики більш доступні і дешевше мегапіксельних ПЗС - датчиків .

Та все ж таки найважливішим фактором, що впливає на якість камери, є виробник. Низькоякісне схемне рішення, неякісна збірка можуть бути причиною посереднього відео, при відмінних характеристиках матриці [9].

Відеокамери бувають аналогові та цифрові.

Аналогові відеокамери

Системи відеоспостереження на аналогових камерах сьогодні використовуються в основному на об'єктах з малим числом відстежуваних приміщень. Це можуть бути невеликі офіси, складські приміщення і т.п. Своєю популярністю аналогові камери зобов'язані порівняно низькою вартістю і гарним характеристикам по співвідношенню ціна / якість. Їх конструкція дуже проста та надійна, випробувана часом і складними умовами експлуатації.

Принцип роботи аналогових камер: світловий потік проходить через об'єктив, далі – через групу лінз і потрапляє на ПЗС-матриці, що перетворюють його в відеосигнал, який надходить по коаксіальному кабелю до касетного відеореєстратора (записуючого пристрою) і монітора. При необхідності можлива модернізація аналогових відеокамер в частині передачі сигналу – установка блоку перетворення, міняючого аналоговий сигнал на цифровий, що дає можливість використовувати мультиплексор і єдиний відеореєстратор для декількох аналогових відеокамер[9]. На рис. 2.6 представлений приклад зовнішнього вигляду аналогової відеокамери.



Рис. 2.6 Аналогова відеокамери

Зручність використання аналогових відеокамер полягає в простоті їх налаштування і використання, вони не вимагають складного програмування, через невелике число робочих алгоритмів.

Вибір на користь аналогових відеокамер ґрунтується також на їх широкому асортименті – кожен користувач зможе підібрати камеру за своїм бажанням, будь-якого розміру. В аналогових системах відеоспостереження можна з легкістю поєднувати камери різних виробників.

Безсумнівним мінусом аналогових відеокамер є відсутність кодування сигналу при його передачі, тобто сигнал може перехопити і підмінити сторонній.

Цифрові відеокамери або IP-відеокамери

Пристрій ір-камер: світловий потік проходить через об'єктив лінзи, проектується на світлочутливу матрицю (в основному використовуються напівпровідникові CMOS або CCD матриці), що перетворює світловий сигнал в електричний, потім – в процесор, що обробляє відеосигнал, далі по витій парі або wi-fi до мультиплексору і, нарешті, на відеореєстратор, оснащений жорстким диском певної ємності і монітор.

Деякі моделі IP-камер обладнані звуковим виходом і мікрофоном для побудови зв'язку в обох напрямках, тобто можна вести віддалений діалог зі співрозмовником, що перебуває у зоні огляду такої камери. Крім того,

практично всі моделі цифрових камер підтримують можливість установки на них комплекту зв'язку (вартість таких звукових пристроїв невисока). Встановити обладнання для двостороннього зв'язку на аналогові відеокамери також можливо, однак потребує додаткового кабелю передачі аудіосигналу (в цифрових камерах «транспорт» один — вита пара).



Рис. 2.7ЦифроваIP -відеокамера

Будь-яку IP-відеокамеру можна підключити через мережевий інтерфейс Ethernet-мережі (10/100 Мбіт/с).

Цифрові камери спостереження оснащені тривожними входами / виходами, до якого підключаються тривожні датчики. Спрацьовування будь-якого датчика тривоги викличе негайну реакцію процесора IP-камер: за його командою останній набір кадрів, що містяться в відеобуфері камери до сигналу тривоги, в час і після тривоги буде скомпоновано і відправлено по заданій електронній адресі [11].

2.2 Середовища передачі відеоінформації

Відстань місця розташування відеокамер від поста спостереження вимагає рішення задачі передачі відеосигналів на значні відстані. Кожне з наявних у розпорядженні розробника рішень має свої переваги і недоліки[11].

Проводові лінії передачі інформації

1.) Вита пара (twistedpair) – кабель передачі інформації, який є витою парою мідних дротів (чи декілька пар дротів), поміщених в екрановану оболонку. Пари дротів скручуються між собою з метою зменшення наведень. Вита пара є досить завадостійкою. Існує два типи цього кабелю: неекранована вита пара UTP і екранована вита пара STP. Кабель використовується для передачі даних на швидкості 10-100 Мбіт/с.

Кабелем вита пари користуються в ситуаціях, коли відстань від камери до відеореєстратора або монітора більше двохсот метрів. Якщо говорити про ціну, то такий кабель коштує порівняно дешевше, ніж коаксіальний. Недолік використання такого типу кабелю полягає в тому, що на додаток до кабелю необхідно купувати однопередавальний і одноприймальний пристрій. Тому що завести виту пару на камеру і більшість відеореєстраторів неможливо. Використання додаткових приймачів і передавачів збільшує не тільки вартість системи, але і ризик втратити сигнал, якщо який-небудь з цих двох компонентів вийде з ладу. Варто відзначити, що використання витої пари особливо зручно, коли для запису відеосигналу використовуються цифрові відеореєстратори.

2.) Коаксіальний кабель (coaxialcable) - це кабель з центральним мідним дротом, який оточений шаром ізолюючого матеріалу для того, щоб відокремити центральний провідник від зовнішнього екрану (мідного обплетення або шар алюмінієвої фольги). Існує два типи коаксіального кабелю: тонкий коаксіальний кабель діаметром 5 мм і товстий коаксіальний кабель діаметром 10 мм. Коаксіальний кабель більше захищений від перешкод, ніж вита пара і знижує власне випромінювання. Пропускна спроможність - 50-100 Мбіт/с.

Основна перевага коаксіального кабелю у тому, що для з'єднання камери і відеореєстратора за допомогою «коаксіалу» не потрібно ніяких додаткових пристроїв. До одного кінця кабелю підключається камера, до другого – пристрої відеореєстрації. Основний недолік коаксіального кабелю полягає в тому, що максимальна відстань між камерою і відеореєстратором чи монітором становить 200 м. Якщо відстань більше – необхідно використовувати спеціальні

повторювачі. Висновок: «коаксіал» дуже зручний для невеликих об'єктів, а от для великих об'єктів краще вибрати інший тип кабелю.

3.) Оптиволоконний кабель (fiberoptic) - це оптичне волокно на кремнієвій або пластмасовій основі, поміщене в матеріал з низьким коефіцієнтом заломлення світла, яке закрито зовнішньою оболонкою. Оптичне волокно передає сигнали тільки в одному напрямі, тому кабель складається з двох волокон. На передавальному кінці оптиволоконного кабелю потрібно перетворення електричного сигналу у світловий, а на приймальному кінці зворотне перетворення. Швидкість передачі даних 3Гбит/с.

Переваги такого типу передачі даних є наступні:

- оптиволоконний кабель мініатюрний і легкий.
- для передачі даних на величезну відстань немає необхідності у додаткових підсилювачах.
- якість переданого сигналу дуже висока.

На жаль навіть у такої досконалої системи є свої недоліки. Ціна такого кабелю коливається в межах від 1 до 10 \$ за метр залежно від типу. Не кажучи вже про те, що для роботи з таким кабелем потрібно спеціальне, дуже дороге устаткування і рівень підготовки фахівців повинен бути дуже високим.

Безпроводові лінії передачі.

Останнім часом для передачі відеосигналу широко використовуються локальні комп'ютерні мережі. Для цих цілей існують спеціальні мережеві цифрові камери з вбудованим модемом і внутрішнім мінісервером (це є перевагою для ІСВ). Для формування цифрових файлів застосовуються сучасні методи стиснення зображень JPEG, М-JPEG. Таким камерам можна привласнити свою ІР-адресу і реалізувати віддалений доступ для відеоспостереження через локальну комп'ютерну мережу. Для систем охоронного відеоспостереження існують спеціальні відеосервери, які не тільки забезпечують комутацію сигналів від різних камер, але і роблять запис інформації на вбудований жорсткий диск. За допомогою звичайного комп'ютера можна спостерігати зображення однієї або декількох камер, як реальних, так і архівних. Швидкість оновлення кадрів багато

в чому залежить від завантаження локальної мережі і просторового обсягу зображень. Використовуючи відповідне програмне забезпечення, можна попередньо встановлювати швидкість передачі кадрів і просторову роздільну здатність зображення в пікселях. Якщо важливо розширення, то можна пожертвувати швидкістю передачі кадрів, а коли необхідно оцінювати рух в сюжеті, доцільно зменшити роздільну здатність стандарту зображення[12].

2.3 Засоби обробки і реєстрації відеосигналів

Відеореєстратор (англ. DigitalVideoRecorder, DVR, цифровий відеореєстратор) - пристрій, призначений для запису, зберігання та відтворення відеосигналів, а в деяких випадках і аудіосигналів, що надходять від аналогових відеокамер і мікрофонів в системах відеоспостереження.

Відеореєстратор є альтернативою застарілим рішенням для відео спостереження на базі відеомультимплексора.

Як вже було сказано, для отримання зображення камеру необхідно підключити до відтворюючого пристрою, котрим може виступати монітор, смартфон, планшет, телевізор.

Але у більшості випадків необхідно забезпечити одночасну роботу >1 камери, мати можливість записувати відеодані за більший проміжок часу, ніж це можливо за допомогою домашньої відеокамери, котра має функцію запису на SD носій. Це обумовлюється великою територією, необхідністю максимально охопити межі контрольованої зони.

Відеореєстратором прийнято вважати пристрій для запису, зберігання та відтворення відеоінформації. Так би мовити, даний тип пристроїв можна назвати відеохабом. Принцип роботи відеореєстраторів полягає у конвертації зображення, прийнятого від підключених до нього камер кабелями або бездротовим способом (Wi-Fi), після чого виконується процес стиснення та запису на носій. Для перегляду до відеовиходу реєстратора необхідно підключити монітор або телевізор (рис. 2.8)[12].

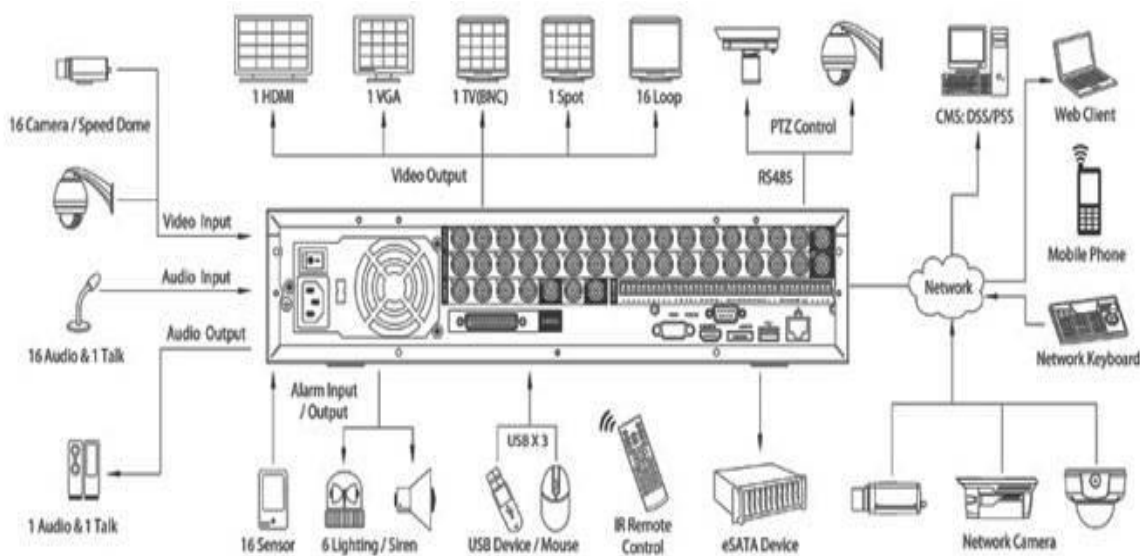


Рис. 2.8 Схема інтерфейсів відеореєстратора

Відеореєстратори можна поділити за можливістю роботи з різними типами відеокамер – цифрові(DVR), мережеві (NVR) та комбіновані (XVR). Спільним для трьох типів є можливість запису відео, відмінність у свою чергу полягає в різних алгоритмах обробки відео.

Мультиплексори (відеокомутатори) - це пристрої, призначені для роботи в складі системи відеоспостереження, що складається з декількох камер. Використовуються для послідовного виведення зображень. Мультиплексори послідовно підключають відеокамери до монітора.

Альтернативою мультиплексора є квадратор - пристрій, призначений для зручного перегляду зображення від декількох відеокамер в режимі реального часу. Квадратор ділить екран на 4 прямокутні частини (або 8 частин в залежності від моделі) і в кожній відображає картинку з камери, підключеної до відповідного відеовходу. Багато моделей квадраторов мають додаткові функції, такі як кадр в кадрі, балансування яскравості зображень відеокамер, автоматичне і ручне «заморожування» кадру, збільшення зображення. Як правило, квадратори встановлюються в невеликі системи відеоспостереження.

Залежно від поставлених задач відеореєстратор може використовуватися:

- для відеоконтролю касових операцій на робочих місцях касирів в магазинах (для аналізу відповідності відеоданих, даних касових терміналів і чеків);
- для організації системи обліку і контролю автотранспорту на парковках і контрольно пропускних пунктів ОІД;
- для автоматичної реєстрації і контролю переміщень залізничних вагонів по території заводів, комбінатів, паливно-заправних комплексів, сховищ;
- при організації територіально-розподілених систем відеоспостереження, в тому числі з єдиним центром моніторингу.

Будова відеореєстратора схожа з комп'ютером або відеосервером і містить в своєму складі аналогово-цифровий перетворювач, процесор, жорсткий диск і інші компоненти. Відеореєстратор на відміну від відеосервера на базі персонального комп'ютера з платою відеозахвату, віграє в швидкості і в якості архівування, при цьому цифровий відеореєстратор коштує дешевше, ніж відеосервер зі схожими параметрами.

Відеореєстратор для відеоспостереження оснащений спеціалізованою операційною системою. Перед записом, оцифровані відеозображення, як правило, піддаються компресії для зменшення займаного ними об'єму на жорсткому диску. Практично всі відеореєстратори можуть працювати як з монохромними, так і з кольоровими відеозображеннями.

Багато відеореєстраторів мають можливість підключення до комп'ютерної мережі для передачі відеозображень на комп'ютери віддалених користувачів:

- функціональність (симплекс, триплекс, пентаплекс);
- число вхідних відеоканалів (від 1 до 16);
- швидкість запису (6 кадрів в секунду, економ варіант, 25 кадрів в секунду для якісного професійного відеоспостереження);
- розширення (чим більше розширення, тим більше простору на жорсткому диску необхідно);
- жорсткий диск або ємність пам'яті (до 1 Тб)

- використовуваний тип компресії;
- можливість підключення зовнішніх накопичувачів інформації;
- можливість підключення аудіоканалів;
- можливість підключення IP-відеокамер;
- можливість роботи в мережі (можливість підключення до віддаленого комп'ютера для відеоспостереження).

На даний момент окремі різновиди відеореєстраторів виділилися в підгрупи, які мають власні назви:

- мережевий відеореєстратор (робота тільки з IP-відеокамерами);
- гібридний відеореєстратор (робота з аналоговими і IP-відеокамерами);
- PC-based DVR (відеореєстратор на базі персонального комп'ютера);
- DVR (робота тільки з аналоговими відеокамерами).

Відеореєстратори симплексні - такі відеореєстратори можуть виконувати одночасно лише одну з операцій: перегляд, запис або відтворення з архіву.

Відеореєстратори дуплексні мають можливість виконання тільки двох операцій, запис і перегляд, запис і відтворення архіву.

Відеореєстратори триплексні з можливістю роботи відразу в трьох режимах, запис, перегляд, архів.

Також відеореєстратори поділяються на:

1) DVR для підключення аналогових охоронних відеокамер NVR для підключення IP (мережевих) камер Hybrid (Гібридні) для підключення і ір камер і аналогових камер.

2) Крім відеореєстраторів досить популярні комп'ютерні цифрові системи відеоспостереження, які складаються з програмного забезпечення і плат відеозахвату для підключення відеокамер спостереження. Таке програмне забезпечення (ПЗ) встановлюється на спеціалізовані і оптимально підібрані комп'ютерні платформи. Створене рішення називають відеосервер.

Головна відмінність комп'ютерних систем відеоспостереження від відеореєстраторів - це більш гнучкий вибір конфігурацій, багатий функціонал

програми для відеоспостереження. З недоліків варто відзначити високу ціну і підвищені вимоги до рівня знань для інсталяторів систем відеоспостереження[13].

Відеосервер.

Відеосервер - пристрій, призначений для роботи в складі гібридної системи відеоспостереження та перетворення аналогового відеосигналу з камери в цифровий формат для подальшої передачі його по комп'ютерній мережі або записи на цифровий носій інформації.

Відеосервер дозволяє розвивати мережеві відеосистеми, не відмовляючись від існуючого аналогового обладнання. Відеосервер додає нові функціональні можливості аналоговому обладнанню.

Багато відеосерверів мають вбудований детектор руху і входи для підключення зовнішніх охоронних датчиків, а також можуть відновлювати події, що передували сигналу тривоги і наступні за ним. Відеосервер прибирає необхідність в супутній периферії: у моніторах, коаксіальних кабелях і відеореєстраторах. Відеореєстратори стають непотрібними тому, що відеозапис може здійснюватися стандартними серверами на основі портативних комп'ютерів.

Відеосервери можуть мати від одного до шістнадцяти аналогових входів для підключення камер і Ethernet-портів для підключення до мережі. Відеосервер може передавати по мережі Ethernet відеозображення зі швидкістю до 25 кадрів в секунду, в залежності від розширення картинки і проникної здатності мережі.

Зрозуміло, відеосервер це рішення високотехнологічне, і розумно застосовувати його там, де важливий контроль над великою кількістю відеокамер, інтелектуальне управління і інтеграція з іншими системами безпеки, де функціоналу звичайних реєстраторів мало.

Відеосервер - це комплексний пристрій, що складається з наступних елементів: блок оцифровки зображення, блок стиснення, веб-сервер, інтерфейси для підключення до мережі і послідовні порти.

Майже всі відеосервери провідних виробників забезпечені блоком цифрових входів, які служать для підключення до відеосерверів зовнішніх охоронних датчиків. Це означає, що можна налаштувати відеосервер на спрацьовування по зовнішній події. Крім того, більшість відеосерверів оснащені аудіоканалом для передачі звуку по мережі.

IP-відеосервер є компактний пристрій, що забезпечує інтелектуальну обробку відео в системах охоронного телевіденія. Відео сервер дозволяє будувати гібридні рішення на базі аналогових камер і цифрових (IP) систем відеоспостереження із застосуванням вбудованої відеоаналітики на протяжних об'єктах.

Відеосервер оснащений відеоаналітикою для автоматичного розпізнавання порушень і позаштатних ситуацій. Алгоритми відеоаналізу, вбудовані в пристрій, дозволяють автоматично детектувати і супроводжувати об'єкти з урахуванням тривимірного простору сцени. Алгоритми стійко працюють в умовах вуличного спостереження і не реагують на зміни освітленості, руху дерев, тіней і сонячних відблисків[13].

Відеосервер підтримує відкритий стандарт IP-безпеки ONVIF (міжнародний стандарт), що істотно спрощує його інтеграцію в системі управління відео і централізоване адміністрування. Відеосервер надає доступ до таких сервісів в рамках міжнародного стандарту ONVIF:

- виявлення пристроїв по протоколу;
- конфігурація мережевого інтерфейсу;
- профілі роботи пристрою;
- потокова передача медіа-даних (відео та аудіо);
- потокова передача мета-даних відеоаналітики;
- конфігурація правил і передача подій;
- оновлення прошивки.

Завдяки протоколу ONVIF відеосервер глибоко інтегрується в системи управління відео і реалізує стандартизовану передачу не тільки відео і аудіо, а й тривожних повідомлень, метаданих для індексування відеоархіву[13].

2.4 Пристрої відображення відеоінформації

Монітори відеоспостереження- це інтерфейсний пристрій виведення відеосигналів від камер або відеореєстраторів.

Монітори охоронного відеоспостереження забезпечують пряму трансляцію відео, як в режимі реального часу, так і відтворення відеоархіву.

Очевидно, що при організації системи відеоспостереження керівники охорони ОІД приділяють багато уваги вибору камер відеоспостереження, і при цьому зовсім забувають про те, що важливим також являються характеристики моніторів відеоспостереження. Якість монітора для трансляції відеоспостереження має бути на високому рівні.

Для охоронних систем відеоспостереження застосовуються спеціальні монітори. Монітори для відеоспостереження відрізняються від неспеціалізованих телевізійних приймачів багатьма технічними характеристиками. У першу чергу це можливістю цілодобової безперебійної роботи. Також монітори відеоспостереження випускаються в металевих корпусах з метою захисту від зовнішніх електромагнітних полів і зниження ризику пожежонебезпеки.

Вважається, що монітори відеоспостереження - це промислові пристрої, і на відміну від побутових телевізорів вони мають більшу кількість роз'ємів для підключення різних пристроїв, у тому числі пристроїв обробки відеосигналів. Приклад застосування моніторів показано на рис. 2.9.



Рис. 2.9 Пристрої відображення відеоінформації

Сучасні монітори відеоспостереження розраховані на безперебійну роботу 24 години на добу 7 днів на тиждень.

За кольоровими характеристиками зображення всі монітори для відеоспостереження можна розділити на [14]:

чорно-білі монітори відеоспостереження;

кольорові монітори відеоспостереження.

Монохромні монітори для охоронного відеоспостереження мають кращу роздільну здатність і контрастність, і більш доступні за ціною.

Кольорові монітори для охоронного відеоспостереження дозволяють краще ідентифікувати різні об'єкти відеоспостереження, а також розрізняти кольори, тони і відтінки зображення. Вибір між цими двома видами відеомоніторів повністю залежить від того, які завдання стоять перед системою відеоспостереження.

У системах охоронного відеоспостереження використовуються два типи моніторів:

відеомонітори з електронно-променевою трубкою – CRT;

відеомонітори на рідких кристалах - LCD, TFT.

Рідкокристалічні монітори (РК) є більш сучасними та функціональними, але деякі користувачі віддають перевагу кінескопним моніторам, адже все залежить від вимог до системи спостереження.

LCD, TFT монітори для систем відеоспостереження вже практично витіснили електронно-променеві моделі моніторів. Але кінескопні відеомонітори мають істотно нижчу вартість.

LCD, TFT відеомонітори обладнані великими розмірами екранів, але при цьому вони компактні, плоскі і легкі за вагою. Також такі відеомонітори не так шкідливі для здоров'я, як електронно-променеві моделі моніторів, оскільки не створюють електромагнітного випромінювання і не викликають перенапруження очей користувачів.

Сучасні рідкокристалічні монітори головним чином забезпечують користувачам перегляд зображення з великою роздільною здатністю і високою якістю.

Охоронні відеомонітори обладнані великою кількістю відеовходів - VGA, HDMI, AV1, AV2, SVIDEO, DisplayPort, BNC, RGB DVI. Така безліч відеовходів на моніторах відеонагляду дозволяє використовувати їх у роботі з будь-якими системами охоронного телебачення.

Зазначимо, що існує практика використання звичайних моніторів і телевізорів в системах відеоспостереження, але таке рішення не виправдовує себе, так як звичайні монітори можуть давати збої в роботі, не витримувати цілодобове функціонування і в цілому сповільнювати роботу системи відеоспостереження.

Сучасні професійні відеомонітори обладнані потужними відео процесорами, які забезпечують формування зображення найвищої якості. Виробники сучасних моніторів для професійного охоронного відеоспостереження випускають моделі з діагоналлю екрана більше метра і можливістю використання для оснащення служб безпеки великих об'єктів. Так це 32, 42, 46 і 55-дюймові моделі моніторів.

Так для масштабної системи охоронного відеоспостереження необхідні великі монітори для перегляду відеозображення одночасно з величезної кількості камер і при цьому щоб якість зображення не втрачалася.

Так відеомонітори мають спеціальну функцію відтворення відео від різних джерел в одному або декількох вікнах одночасно. При цьому можна вибирати, в якій області екрану буде відтворюватися та чи інша картинка з камери.

Сьогодні більшість користувачів професійних систем відеоспостереження віддають перевагу кольоровим LCD-моніторів з роздільною здатністю зображення Full HD і з широким набором додаткових функцій.

Часто можна зустріти, як такі монітори за аналогією з охоронним відеоспостереженням називаються CCTV-моніторами. [15]

Так *монітори CCTV*- це професійні пристрої відображення графіки і аудіосигналів. Монітори для охоронного відеоспостереження можуть експлуатуватися як автономно, так і в складі великих стін відеомоніторингу на центральному пульті охорони.

Характеристики моніторів.

Типи розгортки.

У режимах високої роздільної здатності важливим фактором є тип розгортки відрядкова (Non-Interlaced), або черезрядна розгортка. При відрядковому способі формування зображення всі рядки кадру виводяться протягом одного періоду кадрової розгортки, тобто передача всіх рядків на екрані монітора за один прийом без чергування. Монітори, що мають відрядкову розгортку, дозволяють швидше виводити зображення на екран і менше мерехтять. Усі сучасні монітори є моніторами з відрядковою розгорткою. При черезрядному способі за один період кадрової розгортки виводяться парні рядки зображення, за другий — непарні. Тому кажуть, що один кадр ділиться на два поля. Отже, у випадку черезрядної розгортки частота кадрів знижується вдвічі.

Стандартні VGA-карти при 800x600 підтримують відрядковий спосіб, а 1024x728 — черезрядний. У чому ж їхнє розходження? Монітори з відрядковою розгорткою мають кращі характеристики, тому що вони відтворюють зображення на екрані швидше і без мерехтіння. Вони також виводять більш різкі й чіткі зображення. Усі монітори високої якості відображають зображення у всіх режимах роздільної здатності з відрядковою розгорткою. Монітори, що мають «штатні» режими з черезрядною розгорткою, жодною з провідних фірм, що випускають монітори, не виробляються. Тому не слід купувати монітори з такою розгорткою.

Роздільна здатність монітора

Роздільна здатність означає щільність відображуваного на екрані зображення. Вона визначається кількістю точок або елементів зображення уздовж одного рядка й кількістю горизонтальних рядків. Екран VGA зі здатністю 640x480 точок має 640 точок уздовж рядка і 480 рядків, розгорнутих

на екрані. Чим вища роздільна здатність, тим більше інформації виводиться на екран.

Сьогодні максимально можлива роздільна здатність сягає значення 1800x1440, що значно перевищує здатність кольорового телевізора, яка дорівнює приблизно 800x625 точок. У режимі максимальної роздільної здатності монітора, як правило, працювати не можна (занадто дрібно). Але максимальна роздільна здатність є одним із найважливіших параметрів оцінки якості монітора: чим вища максимальна здатність, тим кращий монітор.

Оптимальна роздільна здатність пов'язана з розмірами кінескопа монітора. Для моніторів із діагоналлю 14" і 15" це 800x600, 17" — 1024x728, для великих — 1280x1024.

Частота регенерації

Це одна з найважливіших характеристик монітора, що визначає швидкість, із якою відбувається відтворення кадру або повне оновлення екрана за одиницю часу. Частота регенерації вимірюється в Hz (Герцах, Гц), де один Герц відповідає одному циклу в секунду. Частота регенерації дисплея і відповідні характеристики графічної плати, з якою працює монітор, визначають мерехтіння зображення для всіх режимів роботи монітора. Чим вища частота регенерації, тим менше мерехтіння екрана і, як наслідок, більш комфортні умови роботи через значно меншу стомлюваність очей користувача. Стандарти VESA визначають сьогодні частоту кадрової розгортки під час відсутності мерехтіння зображення для будь-яких режимів роботи Монітора не менше 85Гц.

Частота рядкової розгортки, що виражається в кілогерцах (КГц), дорівнює кількості рядків, що їх промінь може пробігти за одну секунду. Більш висока частота рядкової розгортки дозволяє виводити на екран зображення і вищою роздільною здатністю. Частота кадрової розгортки, або частота зміни кадрів виражена в герцах (Гц), відповідає частоті кадрів скільки разів промінь формує повне зображення — від верхнього рядка до нижнього — за одну секунду. Чим вища частота кадрової розгортки, тим менший рівень небажаного мерехтіння зображення, на яке мимоволі реагують очі й, отже, менше

навантаження на зір. Зауважимо, що чим більший екран монітора, тим помітнішим є мерехтіння, особливо периферійним (бічним) зором, тому що кут огляду зображення збільшується.

Значення частоти регенерації залежить від використовуваного режиму роздільної здатності, від електричних параметрів монітора і від можливостей відеоадаптера. Мінімально допустима частота кадрової розгортки — 72 Гц але це мінімум, при якому багато користувачів зауважують мерехтіння екрана, особливо в приміщенні, освітленому люмінесцентними лампами. Оптимальною є частота 85 Гц і більше.

Смуга пропускання

Це діапазон частот у МГц, у межах якого гарантована стабільна робота монітора. Смуга пропускання також може бути представлена як швидкодія монітора, із якою він здатний сприйняти графічну інформацію в умовах відтворення зображення з максимальною роздільною здатністю, і розрахована за формулою:

$$W = H_{\max} V_{\max} F_{\max},$$

де:

- $H_{\max}$ — максимальна роздільна здатність по вертикалі, $V_{\max}$ — максимальна роздільна здатність по горизонталі, $F_{\max}$ — максимальна частота кадрів [15].

Висновок до другого розділу.

Проаналізовано склад системи відеоспостереження. Встановлено, що відеокамери бувають аналогові та цифрові, зовнішнього та внутрішнього використання, різні по конструктивному виконанню.

Чутливим елементом відеокамери є матриця яка складається з великої кількості фотодіодів. Матриці бувають двох типів: просторово зарядових зв'язках та зроблені за технологією CMOS з використанням польових транзисторів.

Найважливіші параметри відеокамер це: кольоровість; мінімальна освітленість; роздільна здатність; характеристика матриці; виробник [8].

Для реєстрації відеоінформації застосовуються відеореєстратори та відеосервери. Відеореєстратори бувають аналогові та мережеві.

Середовищем передачі відеоінформації є: провідні лінії типу вита пара, коаксіальний кабель, оптоволокрний кабель; безпроводні комунікації.

З ЗАСТОСУВАННЯ ЦИФРОВИХ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

3.1 Розпізнавання образів системою відеоспостереження

Функція розпізнавання образів СВС стаїневідемною їх функціонала. Такий програмний продукт виділяє обличчя людини і в подальшому ідентифікує його використовуючи наявні в інформаційній базі дані.

В основі алгоритму розпізнавання обличчя покладені наступні методи:

1. Емпіричний метод. Він був створений в епоху зародження комп'ютерних технологій і полягає у виділенні об'єкта із загального фону та дослідженні його з метою виявлення закономірних взаємозв'язків.

2. Метод на основі інваріантних даних. Виявлення характерних особливостей форми обличчя, кордонів окремих його частин, встановленні контрастності і подальше поєднання всіх цих параметрів з метою верифікації особистості.

3. Підхід на основі певних шаблонів, закладених розробниками в нейронну мережу. В даному випадку кожен сегмент зображення порівнюється з існуючими стандартними шаблонами, причому це можна робити з різних ракурсів в будь-якому масштабному вимірі.

В цілому процес розпізнавання виглядає наступним чином [14]:

1. Перш ніж розпізнати обличчя, його потрібно спочатку виявити. Камера фіксує обличчя людини незалежно від її знаходження (окремо чи в натовпі). Сучасні технології здатні розпізнати людину, яка навіть не дивиться в камеру, але знаходиться в допустимих межах повороту голови.

2. Аналіз отриманої інформації. Для проведення аналізу знадобляться фотографії обличчя. Більшість систем не працюють з об'ємними 3D моделями, а використовують 2D формат, оскільки у більшості баз даних зібрані фото саме у 2D форматі. Об'ємні зображення формату 3D використовуються досить рідко, головним чином в цілях безпеки. Обличчя кожної людини аналізується як

мінімум по 68 окремих антропометричних точках (загалом їхня кількість може доходити до кількох тисяч). Також є й інші орієнтири (форма вилиць та підборіддя, розріз очей та відстань між ними, висота лоба і т.д.) (рис. 3.1).

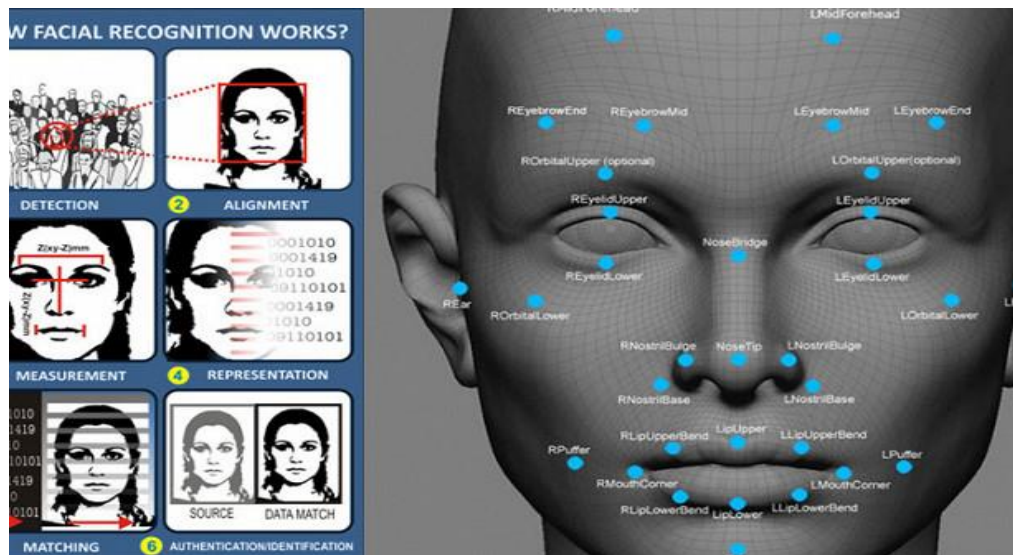


Рис. 3.1 Процес розпізнавання обличчя

3. Виправлення спотворень. Для отримання якомога точнішого результату розпізнаване обличчя повинно дивитися анфас, тобто прямо в камеру. Але таке трапляється рідко, особливо якщо йдеться про розпізнавання людини в натовпі. Щоб підвищити якість розпізнавання, система здійснює додаткове перетворення зображення: прибирає поворот і нахил голови, а також проводить 3D-реконструкцію обличчя з 2D-зображення

4. Цифровізація зображення. Після попереднього етапу аналізу система за допомогою нейромережі складає певний цифровий код обличчя (вектор ознак або FacePrint), який є унікальним для кожної людини. По суті, це якесь число, яке складається з суми характеристик обличчя: відстаней між опорними точками, текстури певних зон на обличчі та ін. Таких характеристик може бути безліч. Основне правило: вони повинні описувати обличчя незалежно від сторонніх факторів: зачіски, макіяжу, вікових змін.

5. Ідентифікація зображення.

Отриманий цифровий код порівнюється з тими, які містяться в базі даних, де представлені фотографії з цифровими ідентифікаторами. Система шукає співпадіння між зафіксованими фото та зразками, доступними в базі даних. Таким чином зростає можливість отримання додаткової інформації про людину.

3.2 Відеоаналітика у системах вілеоспостереження

Відеоаналітика (videoanalytics) - апаратно-програмне забезпечення або технологія, що використовує методи комп'ютерного зору для автоматизованого збору даних на підставі аналізу потокового відео (відеоаналізу). Відеоаналітика спирається на алгоритми обробки зображення і розпізнавання образів, що дозволяє аналізувати відео без прямої участі людини. Відеоаналітика використовується в складі інтелектуальних систем відеоспостереження є її невід'ємною складовою.

Залежно від цілей, відеоаналітика може реалізувати як одну, так і декілька базових функцій[15]:

1) Виявлення об'єктів (objectdetection). Як правило, виявлення об'єктів в полі зору камери проводиться за допомогою відеодетектора руху. Основна відмінність відеоаналітики від ІК-датчиків руху полягає в можливості локалізації (виділення) та незалежного аналізу відразу декількох об'єктів. Якщо рух не є достатньою ознакою для локалізації об'єкта в кадрі, то виявлення може проводитися за допомогою шаблонів. Наприклад, виявлення осіб людей, номерних знаків автомобілів або виявлення малорухомих цілей.

2) Стеження за об'єктами (objecttracking). Алгоритми стеження (супроводу) дозволяють отримати приватну траєкторію руху об'єкта як в полі зору однієї камери, так і узагальнену траєкторію за даними відразу декількох камер. Стеження необхідно, щоб проаналізувати поведінку об'єкта по його траєкторії, наприклад, визначити рух людини проти потоку або рух з підвищеною швидкістю. Крім цього, стеження необхідно для виключення повторних спрацьовувань систем відеоаналітики на одні і ті ж об'єкти.

Професійні системи працюють за правилом «один тривожний об'єкт - одне спрацювання» для досягнення високої продуктивності оператора.

3) Класифікація об'єктів (objectclassification). Деякі системи відеоаналітики класифікують об'єкти для фільтрації оперативних повідомлень або результатів пошуку. Наприклад, типовий класифікатор об'єктів, використовуючи ознаки форми і абсолютні розміри, розподіляє об'єкти на групи: людина, група людей, транспортний засіб. Більш складні класифікатори в системах відеоаналітики можуть визначити стать або поворотну групу людини.

4) Ідентифікація об'єктів (objectidentification). Ідентифікація об'єктів є найбільш складним компонентом систем відеоаналітики. Сучасні системи дозволяють ідентифікувати людей за біометричними ознаками особи або транспортні засоби - за номерними знаками. Ідентифікація може бути реалізована за допомогою додаткових коштів за рамками відеоаналітики: на основі відбитків пальців, банківської карти, квитка, пропуску або ідентифікатора мобільного пристрою.

5) Виявлення (розпізнавання) ситуацій. Відеоаналітика дозволяє не тільки виділяти об'єкти з потокового відео, а й розпізнавати тривожні ситуації на основі аналізу поведінки даного об'єкта, що не дає зробити звичайна система відеоспостереження. Також ситуаційна відеоаналітика може автоматично детектувати перетин сигнальної лінії, падіння людей, заборонену парковку і виникнення пожежі.

Результатами роботи відеоаналітики є події (повідомлення), які можуть бути передані оператору системи відеоспостереження або записані в відеоархів для подальшого пошуку. Крім цього, відеоаналітика формує метадані, тобто структури даних, які описують зміст кожного кадру відеопослідовності. Метадані містять таку інформацію як місце розташування і ідентифікатори об'єктів (як правило, у вигляді тривожної рамки), траєкторію і швидкість руху об'єктів, дані про поділ або злиття об'єктів, дані про виникнення і закінчення тривожної ситуації. Метадані записуються в відеоархів і відтворюються разом з відео.

З точки зору застосування, розрізняють наступні типи відеоаналітики:

Периметральна відеоаналітика (perimeter video analytics) застосовується для охорони протяжних ділянок і периметрів, виявлення вторгнення і перетину сигнальної лінії в «стерильній зоні». Особливість периметральної відеоаналітики відносно рідкісні порушення (тому зона називається «стерильною»), але форма і тип об'єкта не можуть бути чітко визначені, наприклад, людина може повзти або їхати на велосипеді.

Ситуаційна відеоаналітика (situation video analytics) застосовується для розпізнавання тривожних ситуацій, пов'язаних з поведінкою людей або з рухом транспортних засобів. Ситуаційна відеоаналітика може працювати на основі правил, заданих користувачем (наприклад, заборонена парковка в заданій зоні), або на основі накопиченої статистики (наприклад, виявлення в парку в два рази більше людей, ніж зазвичай в цей час доби).

Бізнес-аналітика (business analytics / intelligence, BI) застосовується для управління організацією, оцінки продуктивності персоналу, оптимізації бізнес-процесів і досліджень поведінки клієнтів. Особливість бізнес-аналітики - розвинені засоби узагальнення даних і підготовки звітів, іноді з можливістю виключення персональних даних.

Біометрична відеоаналітика (biometrical video analytics) застосовується для ідентифікації та супроводу осіб за біометричними ознаками особи. Класична біометрія використовує «чорний» і «білий» списки для порівняння зображень людей. Біометрична відеоаналітика може працювати за більш складним сценаріями, наприклад, здійснювати профайлінг людей або зіставляє спостережень безлічі камер в територіально-розподіленій мережі спостереження.

Номерна відеоаналітика застосовується для розпізнавання реєстраційних знаків автомобілів (number plate reading), а так само для аналізу їх руху за даними безлічі камер.

Багатокамерна відеоаналітика (multiple camera tracking video analytics) застосовується для супроводу об'єктів за допомогою безлічі камер. Результатом

роботи багатокамерною відеоаналітики є траєкторія руху об'єкта на плані всій території спостереження.

Технологічна відеоаналітика (technologicalvideoanalytics) застосовується для моніторингу технологічний процесів, забезпечення якості виробництва, підвищення продуктивності.

Відеоаналітика високої чіткості (highdefinitionvideoanalytics) застосовується для відеоаналізу потоків понад один мегапіксель (720p, 1080p і вище). Як правило, в системах відеоспостереження високої чіткості (HD) використовуються принципово нові алгоритми, що використовують багатомасштабнеуявління відеоданих.

Архітектури системи відеоаналітики

З точки зору апаратно-програмної архітектури, розрізняють наступні типи систем відеоаналітики:

Серверна відеоаналітика (servervideoanalytics) передбачає централізовану обробку відеоданих на сервері. Як правило, сервер аналізує відеопотоки від безлічі камер або кодерів на центральному процесорі або на графічному процесорі. Основною перевагою серверної відеоаналітики є можливість комбінування алгоритмів відеоаналітики на одній апаратній платформі. Головний недолік серверної відеоаналітики - необхідність безперервної передачі відео від джерела відеоданих на сервер, що створює навантаження на канали зв'язку. Приклад зображений на рис. 3.2.

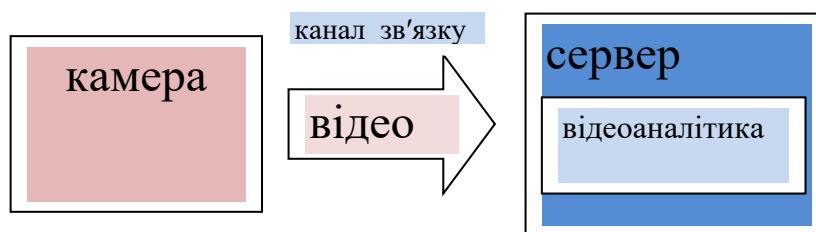


Рис. 3.2 Серверна відеоаналітика

Вбудована відеоаналітика (edgevideoanalytics) реалізується безпосередньо в джерелі відеоданих, тобто в камерах і кодерах. Вбудована відеоаналітика

працює на виділеному процесорі (архітектури DSP, ASIC, FPGA, ARM або x86) пристрою і передає результати (метадані) разом з відеопотоком. Головна перевага вбудованої відеоаналітики полягає в зменшенні навантаження на канали зв'язку і на сервер обробки відеоданих. При відсутності об'єктів або подій відео не передається і не завантажує канали зв'язку, а сервер обробки не декодує стисло відео для відеоаналізу і індексування. У порівнянні з серверною відеоаналітикою, вбудована відеоаналітика дозволяє збільшити в 10-100 разів ефективність використання каналів зв'язку і серверів. Прикладом пристрою з вбудованою відеоаналікою є IP-відеосервер. Приклад зображений на рис. 3.3.

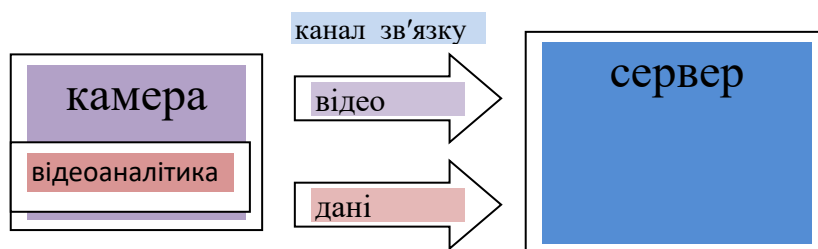


Рис. 3.3 Вбудована відеоаналітика

Розподілена відеоаналітика (distributedvideoanalytics) є гібридним рішенням між серверної і вбудованою відеоаналітикою, в якому обробка розподілена між джерелом відеоданих і центральним устаткуванням. Наприклад, в системі багатокамерного стеження, виявлення об'єктів проводиться в джерелі відеоданих, а зіставлення результатів між декількома джерелами - на сервері. Приклад зображений на рис. 3.4.

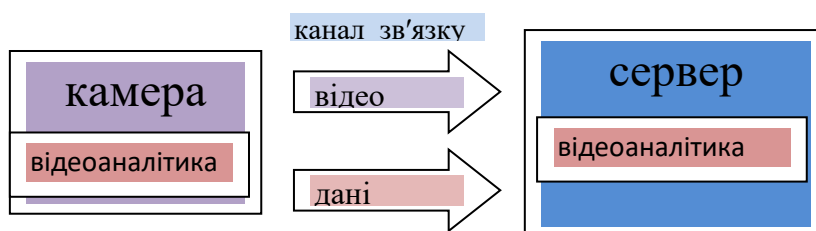


Рис. 3.4 Розподілена відеоаналітика

Загальні переваги відеоаналітики.

Головними перевагами відеоаналітики перед звичайними системами відеоспостереження є автоматичне виділення метаданих з потокового відео без участі оператора. Отримані метадані можуть бути використані для швидкого пошуку в відеоархіву, розсилки тривожних сповіщень та збору статистики.

У порівнянні з «ручним відеоспостереженням», відеоаналітика дозволяє зменшити вартість відеомоніторингу і людського фактора в частині виявлення та часу реагування.

Так як значна частина відеоданих (більше 99%) в системах відеоспостереження не представляє інтересу для користувачів, відеоаналітика дозволяє кардинальним чином зменшити навантаження на канали зв'язку і систему архівування за рахунок фільтрації непотрібних відеоданих.

Головною проблемою багатьох впроваджень відеоаналітики є висока частота помилкових спрацьовувань, яка швидко зменшує економічний ефект технології. Проблема поступово вирішується шляхом вдосконалення алгоритмів відеоаналізу.

Міжнародні стандарти СВ в цілому і відеоаналітика, особливо перебувають на ранньому етапі стандартизації. Наступні міжнародні організації розробляють інтерфейси передачі даних і управління для систем відеоаналітики:

ONVIF (Open Network Video Interface Forum) об'єднує близько 500 виробників і має сильні позиції в Росії, Європі і Японії. Описує інтерфейси взаємодії між IP-камерами, серверами відеоаналітики, відеореєстраторами, системами контролю доступу (СКД) і іншими компонентами. Відмітна риса ONVIF - використання протоколу SOAP для взаємодії між компонентами систем безпеки.

PSIA (Physical Security Interoperability Alliance) об'єднує близько 65 виробників і має сильні позиції в Північній Америці. Відмітна риса PSIA - використання протоколу POST. У порівнянні з ONVIF, інтерфейс PSIA більш простий в реалізації, але менш гнучкий і масштабується.

CAP (Common Alerting Protocol) є протоколом передачі повідомлень про тривожні ситуації. На відміну від ONVIF і PSIA, інтерфейс CAP не спеціалізований для ICB і відеоаналітики[15].

3.3 Забезпечення інформаційної безпеки з використанням інтелектуальних систем відеоспостереження

Інтелектуальна система відеоспостереження NetStation.

Професійна ICB NetStation побудована на багатофункціональному програмному продукті, що дає можливість працювати з аналогово-цифровим відеоспостереженням. ICB NetStation працює з усіма IP-камерами і IP-серверами марки Smartec, а також з обладнанням багатьох інших виробників, в тому числі мегапіксельним, тому надає великі можливості конфігурації системи. Ця система дозволяє здійснювати віддалене відеоспостереження з підтримкою графічних планів eMap, запис, пошук і відтворення відео, управління PTZ-пристроями і може бути встановлено, як на комп'ютер, так і на комп'ютер або смартфон. ICB NetStation розраховане на 32 каналу відео і звуку, а можливість мультисерверної конфігурації дозволяє створювати з його допомогою системи необмеженого масштабу[16], [17].

Програмне забезпечення ICB NetStation призначене для моніторингу відео- і аудіоінформації, що надходить з мережевих і/або аналогових камер відеоспостереження. Крім IP-камер Smartec, ПЗ сумісно з IP-камерами таких провідних виробників, як AXIS, ArecontVision, Bosch, Sony, IQinVision, Lumenera і Sanyo. Воно надає можливість створення і використання гібридної системи з 32 камер. Це дуже актуально при необхідності розширення систем відеоспостереження зі збереженням вже встановлених аналогових камер. Програма ICB NetStation в рівній мірі підходить для створення як невеликих систем, що складаються з 4 камер відеоспостереження, так і великих, в яких задіяно кілька сотень камер, вона складається з серверного та клієнтського додатків і дозволяє створювати різні мультисерверні конфігурації.

Що стосується меню ICB, то пропонується інтуїтивно зрозумілі, але в той же час функціонально насичені налаштування. Для кожного каналу запис програми відеоспостереження NetStation дозволяє створювати свій часовий відрізок, що дозволяє легко відстежувати події, що відбулися. Контрольна панель архіву дає можливість здійснювати «перемотування» записи відеоспостереження в будь-якому напрямку з трьома швидкостями. Також передбачений пошук руху в заданих зонах і створення закладок, здійснювані вручну або автоматично. Слід зазначити можливість створення спеціального альбому скріншотів з камер відеоспостереження, відео яких захищено водяними знаками, а також наявність функції резервного копіювання даних архіву в форматі AVI для їх запису на DVD / CD-носії або мережеве сховище.

Управління PTZ-функціями є за допомогою клавіатури, джойстика, миші або меню ПЗ ICB NetStation. Ця програма відеоспостереження дозволяє вести запис аудіо з 32 мережевих камер відеоспостереження. Потрібний аудіо фрагмент можна легко знайти в архіві, в тому ж місці де зберігаються та відеозаписи. Крім того, можна призначити активацію запису по детектору звуку, а також задати її якість і обсяг. Важливою особливістю ICB NetStation є те, що на всі події з камер, аудіоподії і сигнали з тривожних входів, ПЗ дозволяє призначити виконання специфічних функцій, таких як включення запису, що виходить команда, підключення до клієнта, а також поштові повідомлення.

Також ICB NetStation надає користувачеві можливість необмежену кількість віддалених підключень до «живого» відео, архіву і безлічі функцій. Для карманного персонального комп'ютера (КПК) типу PocketPC і мобільних телефонів безкоштовно пропонується MobileClient, що дозволяє здійснити віддалений доступ до відеоархіву СВ за допомогою бездротового підключення. У цій версії програма відеоспостереження може бути встановлена практично на будь-який КПК або мобільний телефон, що працює під управлінням операційної системи Windows Mobile або Symbian OS.

Останні версії ПО забезпечують багатокористувацький доступ до системи відеоспостереження, сумісні з операційними системами Windows 7 від

Home Premium і вище, підтримують інтеграцію з POS і АТМ терміналами, а також інтерактивні карти об'єктів (eMap). Всі комп'ютерні системи відеоспостереження підтримують можливість повнофункціонального віддаленого адміністрування по мережах 802.11b, 802.11g і 802.3 при будь-якому типі підключення - від модемного до бездротового GPRS-з'єднання. При використанні роботизованих купольних камер відеоспостереження дистанційне керування їх обертанням і масштабуванням проводиться в режимі реального часу.

Програмне забезпечення ICB NetStation підтримує застосовуваний в системах відеоспостереження алгоритм диференціальної компресії відеосигналу. Фактично, прийнятну якість роботи з відеоархівом програма відеоспостереження забезпечує навіть в разі низької модемного або GPRS-підключення.

Ключові можливості ICB NetStation:

- 1) віддалене відеоспостереження і синхронізоване аудіопрослуховування в режимі реального часу;
- 2) віддалений перегляд і прослуховування записаного відео;
- 3) підтримка формату HDTV і мегапіксельних камер;
- 4) повнофункціональне віддалене адміністрування;
- 5) запис відео і аудіо від IP-камер (в тому числі мегапіксельних);
- 6) підтримка дистанційного керування тривожними входами і виходами системи;
- 7) віддалене управління роботизованими купольними телекамерами;
- 8) підтримка до 4 моніторів VGA одночасно: Multiscreen, Spot, перегляд архіву;
- 9) графічний навігатор пошуку в архіві, режим Snap-Shot;
- 10) підтримка інтерактивних графічних планів eMap;
- 11) аналітика: пошук в архіві по руху;
- 12) моніторинг в реальному часі поточної ємності дискового простору;

13) ПЗ для комунікаторів на базі Android, AppleiOS, WinMobile 5/6, Blackberry, Symbian OS і PC на базі Windows;

15) два типи організації BPM (віддалених робочих місць) - за допомогою клієнтського ПЗ і за допомогою WEB-доступу [16].

Інтелектуальна система відеоспостереження OnGuardVideoManager

ICB VideoManager створює мультиканальне відеоспостереження, яке може об'єднувати понад 3000 IP-камер, в тому числі і розсереджених по всьому світу. VideoManager працює з форматами стиснення відео MPEG-4 і MJPEG, має зручні засоби настройки і вбудовані інструменти для аналізу відео, а також надає можливість вибирати розширення IP-камер в діапазоні від базового (320x240 пікселів) до високого (720x480) і управляти поворотними IP- камерами відеоспостереження.

OnGuardVideoManager дозволяє реалізувати системні рішення різного рівня складності відповідно до вимог конкретного об'єкта. Нова програма відеоспостереження має гнучкі налаштування і надає на вибір оператора різні режими відеозапису: безперервний режим, запис окремих кадрів або подій і синхронний запис відео і звуку. При цьому запис і зберігання інформації програма здійснює на стандартних пристроях: на дисках сервера, на мережевих пристроях або на мережі пристроїв зберігання даних.

СВ підтримує різні алгоритми реакції на тривожні події. ICB OnGuardVideoManager подієво-керована, відрізняється оперативністю виведення подієвої відеоінформації на монітори, широкомовної передачі даних відразу декільком додаткам і можливістю обробки складних подій. Нова ICB оперативно реагує на всі тривожні події і запускає відповідні процеси: запис, моніторинг, аналіз подій та ін.

Спільно з додатком OnGuardAlarmMonitoring нова версія відеоспостереження дозволяє виводити мультимедійний графічний план об'єкту з зазначенням місця розташування тривожних точок і відео з встановлених там IP-камер. VideoManager підтримує управління поворотними пристроями камер

відеоспостереження в зворотному приміщенні, автоматичне включення запису по сигналу тривоги і активацію турів патрулювання купольних камер.

Для докладного аналізу отриманих відеоданих ПЗ відеоспостереження має весь необхідний інструментарій. ПЗ дозволяє захистити записи від стирання або перезапису, а також експортувати фрагменти відеозапису в будь-яких стандартних форматах для відтворення за допомогою LenelVideoPlayer або стандартних медіаплеєрів, наприклад, Windows MediaPlayer. Записи, що зберігаються в журналі тривожних подій, дозволяють вибрати через ПЗ карту доступу, що цікавить керівника ОІД чи службу охорони або тривожну точку, і переглянути відеозапис всіх подій, пов'язаних з використанням цієї карти і навіть активністю в даній точці.

Нова СВ використовує програмний додаток IntelligentVideo, який дозволяє налаштовувати зони відеоспостереження та пошук відеозапису тривожних подій для його аналізу. За рахунок цього вивільняється людський ресурс і підвищується ступінь виявлення тривожних подій.[16]

Мережева ICB EverFocusPowerPlus.

Мережева ICB EverFocus для повної підтримки всіх пристроїв, підтримка ІР-камер, аналогових і HD реєстраторів, мобільних DVR. Створення багатовимірних видових матриць, підтримка 640 видових вікон, незалежно від типу пристрою. Підтримка Е-Мар. Завантаження файлу карти об'єкта і багато іншого. У цьому ПО реалізований багаторівневий доступ з можливістю підбору доступних функцій для кожного користувача. POWER PLUS відрізняється максимальною простотою і високою універсальністю.

Особливості ICBEverFocusPowerPlus та її програмного забезпечення:

- 1) Підтримка всіх DVR і Mob DVR EverFocus;
- 2) Підтримка всіх ІР камер і ІР серверів EverFocus;
- 3) Максимальна підтримка 640 вікон відео (10 сторінок по 64 на сторінці);
- 4) Підтримка ОС: Windows XP, Windows 7;
- 5) Браузери: ІЕ 7, ІЕ 8, ІЕ9;

- 6) Відображення в одному мультиекрані до 64 вікон з 6 DVR;
- 7) Вільна конфігурація вікон відображення для кожного DVR;
- 8) Не обмежена кількість записуючих пристроїв;
- 9) Підтримка декількох HDD / поділ архіву;
- 10) Повноекранний режим, миттєвий знімок екрана, запис на запит;
- 11) Підтримка аудіо в 2-х напрямках;
- 12) Перегляд тривог в реальному часі і перегляд тривожного архіву;
- 13) Вбудований сервер тривог;
- 14) Швидкий перегляд запису по тривогам;
- 15) Гнучке розмежування прав користувачів;
- 16) Необмежене число облікових записів;
- 17) Створення груп користувачів;
- 18) Пароль на вхід в систему;
- 19) Підтримка GoogleMap, трекінг по картах;
- 20) Реєстрація подій в базі даних;
- 21) Автоматичне виконання дій у відповідь на події;
- 23) Відправлення E-mail про події.[16]

Приклад функціонального застосування ІСВ на ОІД.

Контроль доступу на ОІД

Завдання: попередження несанкціонованого доступу на територію, контроль доступу в приміщення, перебування сторонніх осіб у недозволеному місці, охорона складів.

Рішення: модуль трекінгу

- дозволяє накреслити лінії контролю периметру в охоронних зонах, при перетині яких модуль видає тривожне повідомлення і виводить відео на екран оператора;
- відстежує рушійні об'єкти в полі зору камери;
- здійснює швидкий пошук в журналі тривожних подій (перетин лінії, вхід в зону, тривале перебування в зоні).

Завдання: автоматичний допуск службового автотранспорту, швидка реакція охорони на потрібний автомобіль, контроль в'їзду стороннього автотранспорту, пошук транспортного засобу, пошук порушника.

Рішення: модуль розпізнавання автомобільних номерів

- дозволяє налаштувати автоматичну реакцію на певний номерний знак (підняття шлагбауму або відкриття воріт);
- дозволяє створити базу автомобілів об'єкта, привласнити кожному ПІБ і посаду власника, марку автомобіля;
- забороняє в'їзд на територію, транспортних засобів, занесенням до чорного списку.

Завдання: попередити запізнення і передчасний вихід з роботи з роботи, несанкціонований доступ на ОІД, повторні проходи.

Рішення: інтеграція з системою контролю доступу

- здійснює автоматичний доступ персоналу на ОІД;
- реєструє всі факти входів / виходів в журналі;
- при здійсненні проходу виводить відео в режим реального часу на монітор оператора;
- дозволяє відстежувати час приходу і відходу певного співробітника.

Завдання: оповіщення про появу людини в зону, що охороняється, запобігання несанкціонованого проникнення на територію ОІД.

Рішення: модуль виявлення осіб

- автоматично виділяє особу з відеопотоку;
- сигналізує при появі людини в зоні, що охороняється;
- показує відеофрагменти, відповідні фрагменту виявлення особи;
- відображає всіх осіб, що з'явилися в камері, за вказаний проміжок часу.

Контроль подій і порушень

Завдання: максимально швидко з'ясувати причину події, знайти порушника за особливими прикметами, відео підтвердження в разі нещасних випадків при недотриманні техніки безпеки.

Рішення: модуль інтерактивного пошуку та перехоплення об'єктів

- знаходить потрібні фрагменти з відеоархіву і в реальному часі по особам, положенню в кадрі, розміром і геометрією об'єкта, фотографією і особливими прикметами;
- формує статистику про об'єкти з зазначеними характеристиками за будь який проміжок часу;
- за допомогою функції між камерного трекінгу відстежує шляхи пересування об'єкта на плані за допомогою IP-камер.

Завдання: оповіщення людей про надзвичайну подію, пошук вогнища і причини загорання, планування евакуації.

Рішення: інтеграція з охоронно-пожежною сигналізацією

- дозволяє налаштувати автоматичну реакцію на певну подію;
- виводить тривожне повідомлення на екран оператора при появі тривоги, спрацювання детектора руху, втраті з'єднання з камерою;
- сповіщає про подію на зазначені номери телефонів, адрес електронної пошти.

Завдання: запобігання шахрайствам, розбір спірних ситуацій.

Рішення: функція «автогум»

- забезпечує автоматичну реакцію на появу руху в заданій зоні;
- виконує автоматичне наближення (наведення) рухомих об'єктів (ступінь збільшення обирається автоматично);
- зберігає кадри у форматі JPEG, PNG, BMP, а відео у форматі – AVI.

Завдання: інформувати про можливе навмисне виведення камери з ладу, забезпечення безперебійного відеоконтролю.

Рішення: детектор саботажу

- визначає і реєструє події, спрямовані на умисне порушення робочого режиму камер спостереження;
- виводить тривожне повідомлення на екран про розфокусування, засвіченні, відвертанні і перекритті камери;

- дозволяє налаштувати різні сценарії обробки подій саботажу відеоспостереження (відправляє повідомлення на електронну пошту або SMS, щоб згенерувати тривогу та ін.).

Висновок по розділу. Існують інтелектуальні системи відеоспостереження які використовуючи відеоаналітику дозволяють розпізнавати образи (обличчя людей, номерні знаки автомобілів і т. ін.).

Відеоаналітика буває серверна, вбудована, розподілена.

Відеоаналітичні можливості СВС роблять можливим її використання для санкціонованого пропуску працівників на ОІД, виявлення порушників інформаційної безпеки і т. ін. Такі функції СВС дозволяють застосовувати її на ОІД для протидії витоку інформації матеріально-речовим каналом.

ВИСНОВОК

Найголовніша причина використання систем відеоспостереження - це прагнення підвищити рівень безпеки і захищеності людей і ОІД. Відеокамери досягли великого успіху в забезпеченні безпеки: тільки факт присутності ввідеокамери відеоспостереження на об'єкті може відлякати злочинця. Але якщо злочин все ж мав місце бути, то наявні записи з камер допоможуть надати допомогу в затриманні і впізнання зловмисника.

В ході роботи встановлено, що існують види інформації які підлягають захисту. Встановлені критерії інформаційної безпеки: конфіденційність, цілісність, доступність. Перевага СВ в порівнянні з іншими охоронними системами, полягає у високій інформативності (90% всієї інформації про навколишній світ людина отримує завдяки органам зору).

Встановлено, що відеокамери бувають аналогові та цифрові, зовнішнього та внутрішнього використання, різні по конструктивному виконанню. Найважливіші параметри відеокамер це: кольоровість; мінімальна освітленість; роздільна здатність; характеристика матриці; виробник.

Для реєстрації відеоінформації застосовуються відеореєстратори та відеосервери. Відеореєстратори бувають аналогові та мережеві. Середовищем передачі відеоінформації є: проводні лінії типу вита пара, коаксіальний кабель, оптоволоконний кабель; безпроводні комунікації.

Встановлено, що існують інтелектуальні системи відеоспостереження які використовуючи відеоаналітику дозволяють розпізнавати образи (обличчя людей, номерні знаки автомобілів і т. ін.). Відеоаналітика буває серверна, вбудована, розподілена.

Відеоаналітичні можливості системи відеоспостереження роблять можливим її використання для санкціонованого пропуску працівників на об'єкт інформаційної діяльності, виявлення порушників інформаційної безпеки і т. ін. Такі функції системи відеоспостереження дозволяють застосовувати її на

системи відеоспостереження для протидії витоку інформації матеріально-речовим каналом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. НД ТЗІ 1.1-005-07 чинний від 12.12.2007р. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.
2. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013
3. Горпенюк А.Я. Організаційно-технічне забезпечення систем захисту. Системи комплексної безпеки об'єктів.
4. Електронний ресурс - https://ohorona.company/cctv?utm_source=google&utm_medium=cpc&utm_campaign=23219748878&utm_content=193666340288-782675386057&utm_term=%D0%B2%D1%96%D0%B4%D0%B5%D0%BE%D1%81%D0%BF%D0%BE%D1%81%D1%82%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%B4%D0%BB%D1%8F%20%D0%B4%D0%BE%D0%BC%D1%83&utm_matchtype=b&utm_device=c&utm_network=g&gclid=EAIaIQobChMI6fCVhdiSkgMVWoN8Bh28Mi26EAAiAAEgLtxPD_BwE&gad_source=1&gad_campaignid=23219748878&gbraid=0AAAAACNT8FnAWKMN6N3T0b6cQk7zxjDiA
5. Сети, святы и автоматизации, комплексне системыбезопасности. Електронний ресурс - <http://spkb.real-soft.ru>
6. Електронні відеоінформаційні системи. Системи безпеки та зв'язку. Електронний ресурс - <http://www.elvis.com.ua>
7. Відеоспостереження для «чайників»// Журнал «ОГО» від 28.02.2013
8. Відеоспостереження. Електронний ресурс - <http://teletec.net.ua>
9. Загальні принципи побудови системи відео спостереження. Моя бібліотека. Електронний ресурс - <http://mybiblioteka.su> - 2015-2016
10. Абдюжанов Рустам «Аналогові відеокамери vs цифрові відеокамери» - 2013. Електронний ресурс - <http://www.cre8tivez.org>

11. Лінії зв'язку передачі даних. Електронний ресурс - <http://oksim.com.ua>
12. Мусієнко Д.І. Проблеми сучасних систем відеоаналитики. Сучасна спеціальна техніка № 2(37), 2014
13. Монітори відеоспостереження. Електронний ресурс - <http://xn--80adageboqrpy5j.com.ua>

ДИПЛОМНА РОБОТА
освітньо-кваліфікаційного рівня
“магістр”

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ
ІНФОРМАЦІЇ ЗА РАХУНОК
ВИКОРИСТАННЯ ЦИФРОВИХ СИСТЕМ
ВІДЕОСПОСТЕРЕЖЕННЯ

Студент: Площинський М.М.
Керівник: Котенко А.М.

2

ОБ'ЄКТ ДОСЛІДЖЕННЯ

- Процес захисту інформації з обмеженим доступом

ПРЕДМЕТ ДОСЛІДЖЕННЯ

- Захист інформації з використанням цифрових систем відеоспостереження

МЕТА РОБОТИ

Обґрунтування доцільності застосування
цифрових систем відеоспостереження для
забезпечення захисту інформації

ОСНОВНІ ЗАВДАННЯ

- аналіз загроз витоку інформації матеріально-речовим каналом;
- аналіз складу системи відеоспостереження, та принципу її функціонування;
- на основі проведеного аналізу обґрунтувати доцільність застосування цифрових систем відеоспостереження для забезпечення захисту інформації.

АКТУАЛЬНІСТЬ

Останнім часом в Україні відбуваються якісні зміни у процесах управління на всіх рівнях, які зумовлені інтенсивним упровадженням новітніх інформаційних технологій. Швидке вдосконалення інформатизації, проникнення її в усі сфери життєво важливих інтересів зумовило необхідність підвищення рівня інформаційної безпеки, адже ціна інформації зростає, а отже методи і засоби несанкціонованого доступу до неї удосконалюються. Тому питання забезпечення інформаційної безпеки на об'єктах інформаційної діяльності та у інформаційно-телекомунікаційних системах дуже актуальне.

КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ



Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (Закон України Про інформацію № 2657-ХІІ від 2 жовтня 1992 року).

МАТЕРІАЛЬНО-РЕЧОВИЙ КАНАЛ ВИТОКУ ІНФОРМАЦІЇ



Склад матеріально-речового каналу витоку інформації

- Джерелами і носіями інформації у матеріально-речовому каналі є матеріальні об'єкти, які мають чіткі просторові межі локалізації.
- Витік інформації в цих каналах супроводжується фізичним переміщенням людей і матеріальних тіл з інформацією за межами контрольованої зони.

Джерела витоку інформації:

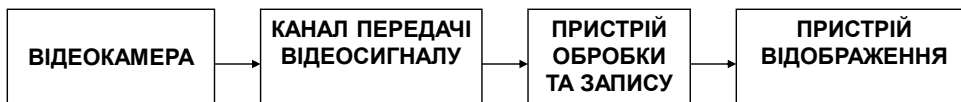
чернетки різних документів і макети матеріалів, вузлів, блоків, пристроїв, що розробляються в ході науково-дослідних і дослідно-конструкторських робіт, які ведуться в організації;

магнітні та інші носії інформації ПЕОМ, на яких під час експлуатації знаходиться інформація з обмеженим доступом;

секретні бібліотеки;

інші місця зберігання матеріальних носіїв ІзОД.

СКЛАД СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ



Відеокамера – основний пристрій складової ІСВ, формує відеосигнал зі світлового потоку, що проходить через її об'єктив та потрапляє на матрицю.

Дуже важливим компонентом будь якої системи відео спостереження є **середовище передачі сигналу** – кабельна мережа і система живлення. При побудові СВ з використанням новітніх технологій, кабельна система будується за принципами локальної комп'ютерної мережі і може використовувати різне фізичне середовище для передачі інформації – мідний кабель типу «вита пара», оптичний кабель, бездротова мережа та ін.. Для живлення камер може використовуватись силовий кабель, але останнім часом набирають популярності технології POE (power over Ethernet), де живлення і дані передаються по одному кабелю.

Пристрої обробки та запису – відеореєстратор, відеосервери дозволяють обробляти потоки інформації, одержувані від камер, аналізувати відео потоки, записувати їх і видавати в заданому форматі на монітор і в локальну або глобальну мережу для віддаленого перегляду.

В якості **пристроїв відображення інформації** для СВ застосовуються комп'ютерні монітори, а також за допомогою прикладних програм або web-браузера на екрані мобільного телефону.

АНАЛОГОВІ ВІДЕОКАМЕРИ VS ЦИФРОВІ ВІДЕОКАМЕРИ

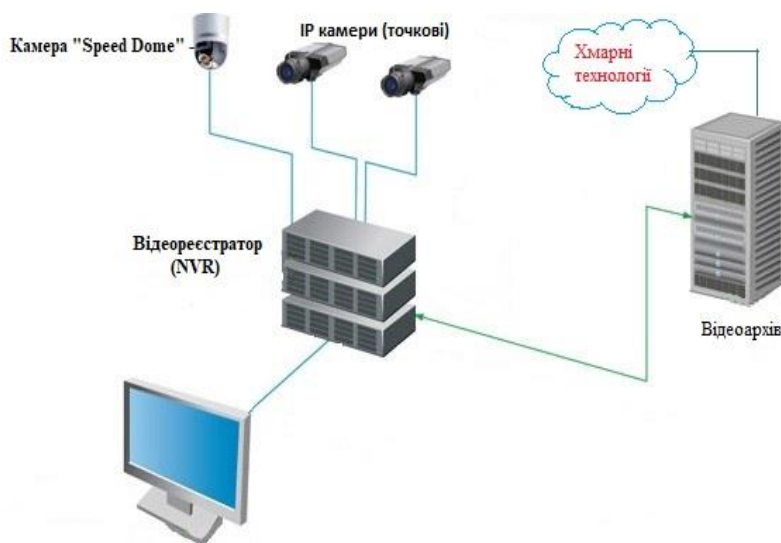


Графічне зображення аналогової відеокамери Графічне зображення цифрової ір-відеокамери

Системи відеоспостереження, побудовані на цифрових відеокамерах, сьогодні порівнянні з вартістю з аналоговими набагато вище. Але діапазон можливостей ір-камер в порівнянні з аналоговими камерами набагато ширше, у них великі перспективи — у найближчому майбутньому цифрове обладнання відеоспостереження повністю витіснить з ринку аналогові системи.

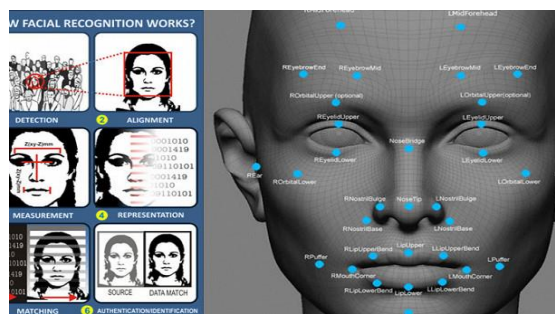
Порівнюючи з точки зору якості, аналогові і цифрові системи відеоспостереження, безсумнівно переважають останні — ір-відеокамери легко інтегрувати в практично будь-які сучасні системи, будь то «розумний будинок», автоматичний контролер контрольно-пропускного пункту і навіть система «розумний місто», годі вже казати за ОД. Завдяки програмним налаштуванням цифрових систем, відсоток помилоків спрацьовувань у них набагато нижче, ніж у аналогових.

СХЕМА ЦИФРОВОЇ СИСТЕМИ ВІДЕОПОСТЕРЕЖЕННЯ



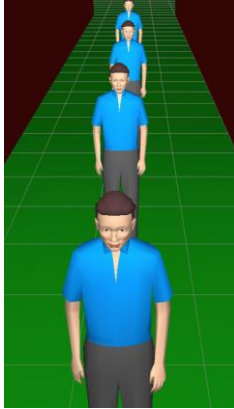
ВІДЕОАНАЛІТИКА

Необхідність застосування розпізнавання обличчя продиктована можливістю створення бази обличч працівників, за якою буде виконуватись контроль доступу на територію приміщення. Це рішення покликано позбавити від ризиків, які несуть в собі нинішні заходи – код-паролі на входних дверях, картки доступу, наявність охоронця. Також вважаю за необхідне створення бази автономерів працівників компанії та налаштувати спрацювання на появу автомобіля з «чужим» номером – це може допомогти у разі заподіяння злочину з використанням транспорту. Таким чином, якщо порушник не володіє інсайдерською інформацією щодо організації такої системи, він скоріш за все буде виявлений на покараний.



Окрім цього, наша система використовує CMS, до якої підключений реєстратор та зовнішня камера, яка веде фіксацію прилеглої території з розпізнаванням автономерів. На базі CMS також реалізоване спрацювання на рух по кожній камері, про що користувач сповіщується листом на e-mail, яке містить скріншот та точний час події. Також CMS спрощує користування відеоархівом за рахунок використання обчислювальних можливостей ПК, на якому вона встановлена, а не реєстратора.

Також для моніторингу проходів всередині приміщення використовується режим коридору, сутність якого полягає в «обрізці» формату зображення зі звичного **16:9** до **9:16**, що дозволяє не займати кадр стінами, а концентрує ресурси камери саме на коридорі, тим самим підвищуючи вірогідність успішного розпізнавання особи, яка потрапила всередину.



Приклад зображення в коридорі досліджуваного ОІД

ФУНКЦІОНАЛЬНІСТЬ СИСТЕМИ ВІДЕОПОСТЕРЕЖЕННЯ

Детектор руху – аналогові відеосистеми.



ВИСНОВКИ

При проведенні досліджень встановлено, що існують види інформації, що підлягають захисту. Критеріями інформаційної безпеки є: конфіденційність, цілісність, доступність.

Встановлено, що до складу системи відеоспостереження входять: відеокамери, середовище передачі відеоінформації, пристрої реєстрації та обробки відеоінформації, пристрої відображення.

Встановлено, що цифрові системи відеоспостереження мають ширші можливості порівняно з аналоговими у питаннях відеоаналітики та інтеграції з комп'ютерними системами.

- Встановлено, що система відеоспостереження може виконувати функції технічної системи охорони.

- З усього викладеного слідує, що цифрові системи відеоспостереження можливо використовувати на об'єктах інформаційної діяльності для забезпечення інформаційної безпеки., а саме притидії витоку інформації матеріально-речовим каналом.