МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ

Конспект лекцій
для здобувачів першого (бакалаврського) рівня вищої освіти
галузі знань 12/F «Інформаційні технології»
спеціальності 126/F6 «Інформаційні системи та технології»
освітньої програми «Інформаційні системи та технології охорони і безпеки»
денної та заочної форм навчання

Луцьк 2026

УДК 004.65 (07)
С 75

Рекомендовано до видання вченою радою факультету КІТ ЛНТУ, протокол № від « » 20 року.

Голова вченої ради факультету КІТ І. С. Кондіус

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки Н. П. Поліщук

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № від « » 20 року.

Завідувач кафедри КІБ Т. В. Терлецький

Укладачі: Т. В. Терлецький, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

О. Л. Кайдик, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

Рецензент: С. М. Костючко, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

Відповідальний за випуск: Т. В. Терлецький, завідувач кафедри комп'ютерної інженерії та безпеки, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

С75 **Системи відеоспостереження**: Конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти галузі знань 12/F «Інформаційні технології» спеціальності 126/F6 «Інформаційні системи та технології» ОП «Інформаційні системи та технології охорони і безпеки» денної та заочної форм навчання / укл. Терлецький Т. В., Кайдик О. Л. Луцьк: ЛНТУ, 2026. 209 с.

У методичному виданні висвітлено матеріал, який необхідний для опанування принципів проектування систем відеоспостереження фахівцям спеціальності 126/F6 «Інформаційні системи та технології» для реалізації відповідних проектних рішень.

ЗМІСТ

Лекція 1. Загальні відомості про системи відеоспостереження

План:

Принцип побудови систем відеоспостереження та їх призначення. Фізичні основи та основні характеристики телевізійних систем. Основні терміни та визначення телевізійних систем.

Системи відеоспостереження (СВС) є одним з основних компонентів інтегрованих (комплексних) систем забезпечення безпеки об'єктів і фізичних осіб і займають важливе місце в їх загальній структурі. Подібні системи останнім часом застосовують досить широко для охорони периметрів і об'єктів, для контроля поведінки відвідувачів, для спостереження за виробничими процесами і в багатьох інших областях на підприємствах, на транспорті, в офісних та житлових приміщеннях, готелях, навчальних закладах, магазинах, торгових центрах, котеджах тощо.

Як правило, при охороні реального об'єкта сучасні СВС інтегровані в комплексну охоронну систему забезпечення безпеки разом з системами контролю доступу та охоронно-пожежної сигналізації, хоча, звичайно, вони можуть бути встановлені і незалежно.

Використання систем відеоспостереження за об'єктами охорони останнім часом набуває масового розповсюдження. Ці системи, залежно від поставленої основної задачі, можуть носити струмуючий або прихований характер. Якщо це стримуюча зловмисників система, то необхідно так спланувати розміщення відеокамер і моніторів, щоб вони були на виду оточуючих. Якщо ж спроектована система призначається для прихованого відеоспостереження – потрібно приділити особливу увагу типу і розмірам телекамери, її маскування, прихованості проводки, системі освітлення і аналогічних питань.

Відеоспостереження, також як промислове, транспортне, підземне і підводне телебачення та інші системи, відноситься до телевізійних систем спеціального призначення. Ці системи називають замкнутим (закритим) прикладним телебаченням Closed Circuit Television (CCTV). Вони призначені для обмеженого числа глядачів, на противагу системам мовного телебачення.

CCTV можуть бути побудовані на основі відеокамер різних типів і являти собою як просту одноточкову відеосистему так і складну багатокілометрову систему охорони периметра. Встановлення цих систем в більшості випадків передбачає забезпечення цілодобового відеоспостереження на об'єкті.

Основні функції СВС – вести відеомоніторинг певних ділянок території об'єкта і надавати візуальну інформацію оператору служби безпеки у вигляді, зручному для сприйняття, подальшої обробки та зберігання. Оскільки основним завданням відеоспостереження в структурі технічних засобів забезпечення безпеки є недопущення проникнення на об'єкт охорони сторонніх осіб, основними місцями використання СВС є різні в'їзні ворота, периметр огорожі, двері, а також під'їзні шляхи і прилегла територія. Усередині приміщень об'єктами уваги традиційно є внутрішні двері, сходові клітини та майданчики

біля ліфтів, входи в технічні приміщення. У разі необхідності вирішення специфічних завдань служби безпеки (наприклад, в торговому підприємстві або офісному приміщенні) відеокамери СВС можуть бути націлені на певні важливі зони, наприклад зону прийому відвідувачів або зону здійснення касових операцій. Крім того, матеріали відеоспостереження часто є найважливішою фактичною основою проведення службового розслідування, а в деяких випадках єдиним достовірним, незаперечним і незалежним свідченням як елемент судових розглядів.

Конструктивно сучасні СВС складаються з відеокамер різного рівня технологічної складності, засобів обробки сигналів і їх реєстрації, комплексу пристроїв відображення зображення (різних моніторів) і пристроїв управління. Як правило, СВС мають автономне електроживлення і захищені від стороннього вторгнення канали зв'язку. Завдяки сучасним комп'ютерним технологіям оператор служби безпеки має можливість сприймати інформацію з усіх встановлених відеокамер, управляти ними (повертати і збільшувати зображення) в реальному часі, автоматично фіксувати інформацію, що надходить на жорсткий диск комп'ютера тощо.

Часто камери відеоспостереження доповнюються пристроями детектування руху – в цьому випадку запис зображення може вестись не постійно, а з моменту виникнення руху в підконтрольному просторі (відповідно, автоматично простежуючи рух і звертаючи увагу оператора на ситуацію, що виникла). До числа додаткових можливостей СВС відноситься розширення спектра фіксованої інформації про навколишній простір за рахунок реєстрації аудіоінформації, що надходить із зовнішніх мікрофонів (в тому числі сигналів, синхронізованих з даними відеокамер).

Система відеоспостереження є однією з основ інформаційного забезпечення оперативної роботи служби безпеки.

Під час розгляду даного курсу буде розглянуті питання, які необхідні для усвідомленого проектування СВС і оптимального підбору обладнання таких систем.

Потрібно пам'ятати, що розгляд технічних характеристик СВС без урахування реальних умов їх експлуатації призведе до низької ефективності використання подібних систем.

Принцип побудови СВС та їх призначення. Системи відеоспостереження призначені для підвищення рівня безпеки об'єкта і для мінімізації можливих наслідків небажаних впливів на людей, на матеріальні цінності і на інформаційні ресурси. Небажані впливи із зовнішнього (по відношенню до охоронюваної зони) середовища можуть бути як усвідомленими (з боку кримінальних елементів), так і результатом техногенних катастроф або стихійних лих. У загальному вигляді СВС умовно можна розглядати як замкнуту систему управління, що складається з відповідних елементів.

Приймальний пристрій сприймає вплив із зовнішнього середовища (оптичне зображення об'єкта на матриці відеокамери) і перетворює його в вид, прийнятний для прийняття рішення.

Пристрій пам’яті зберігає отриману відеокамерою інформацію про можливу небезпеку. У пристрої пам’яті електронного приладу або комп’ютера можуть зберігатися порогові значення напруги або коду, що відповідають тривожній ситуації, інформація про дозволені тимчасових «вікнах» тощо.

Пристрій рішення, на входи якого приходять сигнали з двох попередніх пристроїв, формує сигнал тривоги при виконанні встановлених умов – в цьому випадку реалізується функція відеоконтролю. В якості вирішального пристрою, як правило, виступає оператор, проте останнім часом йому на допомогу все більше приходять такі технічні засоби, як детектори руху, детектори залишених предметів, системи автоматичного розпізнавання осіб людей або автомобільних номерів. Якщо в якості вирішального пристрою виступає оператор, то на екрані монітора повинне бути присутнє зображення контрольованої зони. В цьому випадку реалізується функція відеоспостереження. Якщо пристроєм рішення є електронний пристрій, зокрема комп’ютер, то на його вході повинен бути відповідний відеосигнал. Таким чином, вирішальний пристрій виробляє сигнал для виконавчого пристрою.

Виконавчий пристрій може автоматично впливати на зовнішнє середовище – по тривозі включати сирену, стробо-спалах, виконавчі механізми тощо, а крім того, він може включати пристрій відеореєстрації, а також керувати роботою пристроїв зв’язку.

Пристрій відеореєстрації служить для організації протоколу подій, тобто запису відеосигналів з аналізуючого і виконавчого пристроїв, що надалі дозволяє здійснювати розслідування подій, що відбулися. Крім того, відеозапис дозволяє зменшити і вплив «людського фактору» охорони.

Пристрій зв’язку служить для передачі тривожної інформації силам реагування. Передача інформації може здійснюватися за допомогою локальних комп’ютерних мереж, Інтернету, електронної пошти, телефонних мереж тощо.

Сили реагування (охорона, МНС і тощо) безпосередньо діють на запобігання негативних явищ зовнішнього середовища з метою мінімізації втрат в зоні, що охороняється. Функціонування сил реагування неодмінно має враховуватися в роботі СВС. Без урахування їх роботи (так званого «людського фактору») СВС може перетворитися на безплідний комплект дорогого обладнання.

Ефективність системи забезпечення безпеки визначається швидкістю її реагування на зовнішні впливи: для виключення розвитку подій за несприятливим сценарієм швидкість відповідних дій сил реагування повинна бути вищою, ніж швидкість небажаних впливів із зовнішнього середовища. З цією метою для гальмування дій кримінальних елементів використовуються засоби механічного укріплення об’єкта та вандалозахищеність обладнання СВН (спеціальні кріплення, приховане прокладання кабелів тощо), так як для їх нейтралізації зловмисникам потрібен час. З цією ж метою застосовують резервне електроживлення.

Крім того, слід мати на увазі, що такі параметри ефективності СВС, як необхідна роздільна здатність і швидкість поновлення візуальної інформації,

визначаються конкретним завданням, що випливає з особливостей установки відеокамер.

Перевага СВС в порівнянні з іншими системами забезпечення безпеки полягає в їх високій інформативності (90% всієї інформації про навколишній світ людина отримує завдяки зору).

Фізичні основи та основні характеристики телевізійних систем. Потрібно згадати основи теорії світла та ока людини.

Світло – це електромагнітне випромінювання. Людське око може реагувати на це випромінювання і розрізняти частоти, які сприймаються оком як колір. Видиме світло займає діапазон від 380 нм до 780 нм (рис. 1.1). Щоб легше було запам’ятати, ми наближено приймемо кордону діапазону рівними 400 нм і 700 нм.

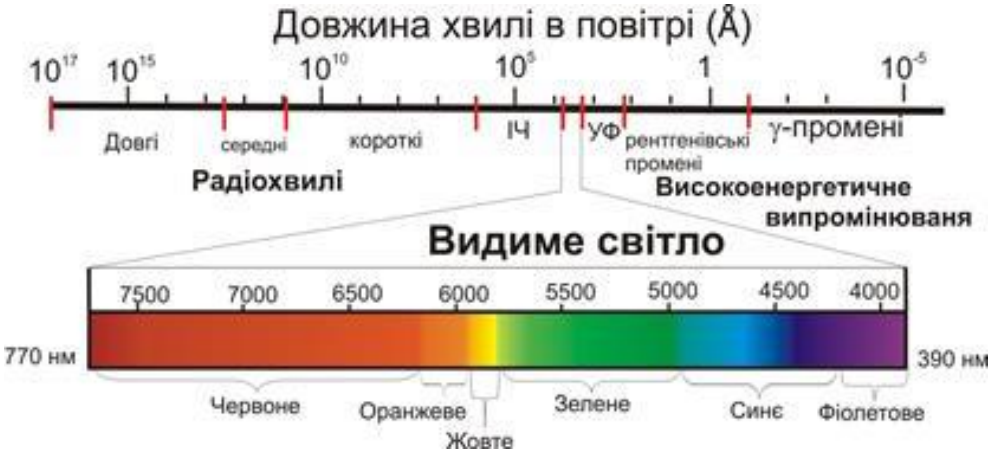


Рисунок 1.1 – Спектри електромагнітного випромінювання

Око найбільш чутливе до зеленого кольору. Іншими словами, якщо зібрати всі довжини хвиль з однаковою енергією, то зелений матиме найбільший «вихід» на сітківці. Частоти вище фіолетового (довжини хвиль коротше 400 нм) і нижче червоного (довжини понад 700 нм) не сприймаються «середнім» людським оком. Чутливість людського ока – це статистична величина. Є люди з «колірною сліпотою», чия спектральна чутливість відрізняється. Деякі люди з «колірною сліпотою» не бачать червоний колір, інші не розрізняють блакитний. Натреноване професійне око художника або фотографа може розвинути дуже високу чутливість, розрізняючи такі частоти (кольори), які іншим можуть здаватися однаковими. Деякі можуть навіть вийти за мінімальну і максимальну межу частот, тобто розрізняти темно-фіолетовий або червоний колір, невидимий для інших індивідів.

Максимум спектральної чутливості лежить в діапазоні зеленого кольору (близько 555 нм).

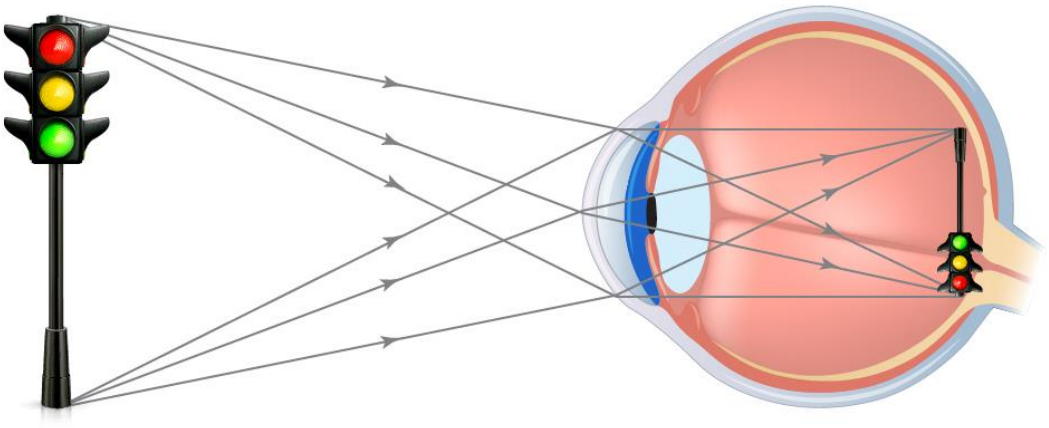


Рисунок 1.2 – Принцип формування зображення людським оком

На рисунку1.2 ми бачимо очну лінзу (кришталик), яка і фокусує зображення на сітківці. Сітківка – це насправді «фоточутлива область», що складається з мільйонів клітин – колб і паличок. Ці клітини можна розглядати як частину нашої нервової системи. Колбочки чутливі до середньої і яскравої інтенсивності світла і відповідають за сприйняття кольору. Палички чутливі до низьких рівнів світла і не здатні розрізняти кольори. Вночі ми бачимо завдяки паличок, тому в темряві ми не можемо розрізняти кольори.

Число колбочок в кожному оці приблизно становить 10 млн., а паличок – близько 100 млн. Колбочки сконцентровані навколо області проходження оптичної осі. Ця область забарвлена жовтим пігментом і називається жовтою плямою. Жовта пляма є основною областю, яку обробляє наш мозок, і, хоча вона дуже мала, концентрація колб в ній становить близько 50000 шт. Середня фокусна відстань ока (тобто відстань між кришталиком і сітківкою при розгляданні нескінченно віддаленого об’єкта) становить близько 17 мм. Така фокусна відстань дає різке зображення в просторовому куті, рівному приблизно 30°. Це також і розмір області, де найбільше колбочок. Саме тому кут в 30° вважається стандартним кутом зору.

Концентрація колбочок зростає у напрямку до центру оптичної осі, досягаючи максимуму лише на 10°. Кожна з клітин-колбочок з’єднується з мозком окремим зоровим нервом, по якому електричні імпульси посилаються в мозок. Звичайно, око бачить і під набагато більшим кутом, так як сітківка охоплює просторовий кут майже в 90°, і колбочки є і поза жовтої плями, але до одного нерву в цьому випадку приєднана група колбочок. В цій області ми бачимо не так чітко, як в області, де до кожної колбочки приєднаний окремий нерв, тому ця частина сітківки називається областю периферичного зору.

«Блок обробки зображення» в головному мозку сконцентрована на 30°, хоча бачимо ми краще (гострота зору) приблизно на 10°. Обробка підтримується постійними рухами очі у всіх напрямках, що аналогічно панорамній головці в відеоспостереженні.

В SLR-камерах (однооб'єктивних дзеркальних фотоапаратах) стандартний кут зору в 30° досягається за допомогою 50-мм об'єктива, для 2/3" камери – це 16-мм об'єктив, для 1/2" камери – 12-мм і для 1/3" камери – 8-мм об'єктив. Іншими словами, зображення, отримані за допомогою будь-якого типу камер з відповідними стандартними об'єктивами, матимуть досить близькі розміри і перспективу, схожу на те, що ми бачимо своїми очима.

Об'єктиви з меншою фокусною відстанню дають більш широкий кут зору і називаються ширококутними об'єктивами. Об'єктив з великою фокусною відстанню звужує кут зору, і тому здається, що він наближає віддалені об'єкти, звідси і назва: телеоб'єктив («теле» означає далекий). Ще одне цікаве питання, що стосується відеоспостереження, пов'язаний з тим, що, знаючи фокусну відстань ока і максимальний діаметр розкриття райдужної оболонки, що дорівнює приблизно 6 мм, ми можемо знайти еквівалентне F-число ока (яке ми обговоримо пізніше): $F_{ока}=l/d$=17/6=2,8 мм.

З повністю розкритою райдужною оболонкою ми можемо досить добре бачити в повний місяць (освітленість об'єктів дорівнює приблизно 0,1 люкса). Пам'ятайте це число, коли будете порівнювати мінімальні характеристики освітленості для різних камер.

Фокусування, яку виконує око, щоб людина могла бачити об'єкти на різних відстанях, досягається за рахунок зміни товщини кришталика (лінзи). Товщина кришталика змінюється циліарними м'язами. Якщо око в порядку, воно може фокусуватися від нескінченності до мінімальної відстані, яка дорівнює приблизно 20 см в ранньому дитинстві, 25 см (відстань найкращого бачення) – у віці 20 років, 50 см – в 40 років і 5 м – в 60 років. Якщо ми дивимося на дуже віддалений об'єкт, тобто око фокусується на нескінченність, циліарні м'язи розслаблюються, і лінза стає тонкою.

Якщо ж око не може фокусуватися на нескінченності, то такий дефект зору називається короткозорістю або міопією. У цьому випадку потрібні окуляри, які допоможуть «дефективній» очній лінзі сфокусувати зображення на сітківці. Такі окуляри іноді називають зменшувальними окулярами, тому що вони мають негативний фокус (або діоптрії).

Діоптрія – це величина, яка є зворотною до фокусної відстані лінзи, де фокус виражений в метрах. Зменшувальні окуляри мають негативні діоптрії. Так, «зменшувальні» окуляри в -0.5 діоптрій, наприклад, мають негативний фокус, рівний 1/(- 0.5)=-2 м.

Інший дефект очей полягає в тому, що око не може сфокусуватися на дуже близькі зображення, тобто очна лінза з тих чи інших причин не може стати досить товстою. Цей дефект називається далекозорістю або гіперметропією.

Людям з гіперметропією, щоб розгледіти близькі предмети, потрібні окуляри. Такі окуляри повинні мати характеристики, протилежні розглянутим вище, тобто вони повинні збільшувати зображення і мати позитивний фокус (або діоптрії).

Коли ми дивимося на об’єкт двома очима, то в мозок проектується зоровий образ, що створює стереоскопічний ефект, і ми сприймаємо об’ємність простору. Якщо прикрити одне око, то буде дуже важко сприймати «тривимірність» оточуючого нас простору.

Відстань між очима (60-70 мм) забезпечує наше сприйняття тривимірного простору аж до 10-15 метрів. На більш далекій відстані дуже важко судити, який із двох предметів розташований ближче. Ви можете провести такий експеримент: подивіться на два досить віддалених від вас, але віддалених на різні відстані, що знаходяться в повітрі об’єкта. Якщо ми дивимося, скажімо, на два дерева, мозок робить висновок про відстані на основі землі і перспективи того, що знаходиться перед нами, але перспективний «рішення» в цьому випадку буде зроблено не на основі «стереоскопічного механізму» очей.

Зображення на сітківці перевернуто, адже така природа оптичної рефракції, і ми абсолютно не помічаємо дрібних рухів очей, які відбуваються в усіх напрямках, коли ми дивимося на щось. Все це розшифровується і контролюється мозком.

Численні експерименти і тести показали, що людське око може розрізнити саме більше 5-6 пар ліній на міліметр. Цей показник має на увазі оптимальну відстань між оком і об’єктом 30 см, тобто, коли ми, наприклад, читаємо досить невеликий текст. Це дає мінімальний кут приблизно в 1/60 градуса. Таким чином, це значення 1/60 градуса вважається межею кутової роздільної здатності для нормального зору. Ми можемо використовувати кутову роздільну здатність очей для кращого розуміння того, як людина сприймає дрібні деталі, що потім дозволить нам застосувати наші теоретичні знання на практиці.

При розрахунку оптимальної дистанції між спостерігачем і монітором існує проста рекомендація, яка передбачає множити висоту екрану монітора на сім. Взагалі, необхідно розуміти, що відстань до монітора – це вкрай важливий аспект психофізіологічного сприйняття деталей в зображенні. Людині, яка дивиться в монітор, абсолютно не потрібно знаходитися дуже близько до екрану, але і дуже далеко від екрану розташовуватися теж не варто.

Основні терміни та визначення телевізійних систем. Відеокамера – пристрій для перетворення оптичного зображення в електричний відеосигнал; первинне джерело відеосигналу в складі CCTV.

Відеоканал – сукупність технічних засобів системи охоронного телебачення, що забезпечує передачу телевізійного зображення від однієї відеокамери до екрану відеомонітора в складі CCTV.

Відеомонітор – пристрій відображення відеоінформації.

Відеореєстратор – пристрій, призначений для запису, відтворення і зберігання відеоінформації в складі CCTV.

Замкнуте телебачення – телебачення, яке використовується в різних галузях науки і техніки і, на відміну від ефірного телебачення непризначене для масової аудиторії.

Квадратор – пристрій комутації відеосигналу, який дозволяє одночасно виводити на екран відеомонітора зображення від чотирьох джерел відеосигналу, розміщуючи їх у відповідних сегментах екрану;

Матричний комутатор – пристрій комутації відеосигналу, що дозволяє автоматично або вручну перемикати декілька джерел відеосигналу на кілька виходів.

Мультиплексор – пристрій комутації відеосигналу, дозволяє одночасно виводити зображення від декількох відеокамер на один відеомонітор і формувати послідовності зображення від всіх камер для запису на відеореєстратор.

Несанкціоновані дії (НСД) – навмисні дії, спрямовані на порушення правильності функціонування CCTV.

Детектор руху – пристрій або дія CCTV, що формують сигнал сповіщення про тривогу при виявленні руху в полі зору відеокамери.

Пункт відеоспостереження – приміщення або частина приміщення, в якому розташована приймальна апаратура і чергові оператори CCTV.

Роздільна здатність відеокамери – параметр, що визначає можливість відеокамери передавати в вихідному сигналі дрібні деталі зображення. Визначається як число переходів (у видимій частині растра) від чорного до білого або назад, що може бути передано камерою. Вимірюється в телевізійних лініях (ТВЛ) по горизонталі і вертикалі.

Телевізійна система замкнутого типу – сукупність технічних засобів, що забезпечують реалізацію замкнутого телебачення.

Телевізійний відеосигнал – сигнал, що несе інформацію про телевізійному зображенні.

Технічний засіб CCTV (ТЗ CCTV) – конструктивно і функціонально закінчений пристрій, що входить до складу CCTV.

Чутливість відеокамери – нижня межа робочого діапазону освітленості в полі зору відеокамери, при якій роздільна здатність і відношення сигнал/шум відеокамери повинні бути не менше заданих значень.

Контрольні питання:

1. Дайте розгорнуте визначення терміну CCTV та поясніть основну відмінність між системами мовного телебачення та замкнутими системами.
2. Опишіть роль систем відеоспостереження у складі інтегрованих комплексів безпеки.
3. У чому полягає різниця між стримуючим та прихованим відеоспостереженням?
4. Який діапазон довжин хвиль охоплює видиме світло і чому важливо враховувати пік чутливості ока на позначці 555 нм?
5. Поясніть функціональну відмінність між паличками та колбочками сітківки ока.
6. Що таке «стандартний кут зору» і які об’єктиви його забезпечують?

7. У чому полягає принципова різниця між квадратором та мультиплексором?

8. Як межа кутової роздільної здатності ока впливає на розрахунок відстані до монітора?

9. Поясніть механізм виникнення та спосіб корекції міопії та гіперметропії.

10. Сформулюйте основний принцип ефективності системи безпеки з точки зору часу реагування.

Література: [1-6, 12-19].

Тема 2. Характеристики та функціональні можливості пристроїв формування зображення

План:

Будова та принцип роботи відеокамер. Класифікаційні ознаки відеокамер. Технічні характеристики відеокамер. Типи та розмірний ряд світлочутливих матриць. Фокусна відстань, кут огляду і лінійне поле сцени спостереження. Типи об'єктивів. Апертура або світлосила об'єктива. Види кріплення змінних об'єктивів. Регулювання діафрагми. Різкість зображення та її глибина. Електронний затвор. Функція Sense-Up/DSS. Роздільна здатність. Стандарти форматів зображення. Вбудована інфрачервона підсвітка. Інфрачервоний фільтр IGR (режим день/ніч). Чутливість (світлочутливість, мінімальне освітлення). Якість відеосигналу (відношення сигнал/шум). Технології подавлення шумів DNR (3D-DNR, 2D-DNR). Частота кадрів. Бітрейт. Технології компенсації засвічування (HLC, BLC, WDR, DWDR). Системи стабілізації зображення. Класи захисту відеокамер IK (антивандальні) та IP (від пилу і вологи). Функція Privacy Mask прихованих зон. OSD меню відеокамер та її функції (DIS, AGC, AWB тощо). Бортові носії інформації.

Будова та принцип роботи відеокамер. Відеокамера – головний і обов'язковий компонент будь-якої СВС. Використання відеокамер надає оператору можливість здійснювати одночасне спостереження декількох досить віддалених місць, контролювати зміну ситуації в цих зонах і здійснювати відеозапис.

Будь-яка відеокамера містить фотоелектричний перетворювач, який є світлочутливим пристроєм, що перетворює оптичне зображення зони спостереження в електричний відеосигнал. Світлочутливим пристроєм служить давач зображення - матриця, в площині якої фокусується світло, що проходить через об'єктив. Матриця містить велику кількості фотоелементів, кожен з яких відповідає елементу зображення – пікселю (від англійського Pixel – Picture Element). Кожен фотоелемент фіксує кількість світла, яке на нього потрапляє, і перетворює його у відповідний заряд електронів. Чим яскравіше світло, тим більший заряд.

Класифікаційні ознаки відеокамер. Сучасні камери класифікуються насамперед за типом вихідного сигналу на аналогові та цифрові, хоча ця межа стає все більш розмитою через розвиток гібридних систем.

Ядром будь-якої відеокамери є сенсор (матриця), який перетворює світло на електричний заряд. Класифікація за типом сенсора є однією з найважливіших технічних ознак, оскільки вона безпосередньо впливає на світлочутливість, динамічний діапазон та швидкість роботи камери. Всі відеокамери класифікують за типом сенсора на матриці з зарядним зв'язком (CCD) і сенсори з комплементарною метал-оксидною структурою (CMOS).

Світлочутливість та динамічний діапазон також належить до класифікаційних ознак відеокамер. Перша характеризує здатність камери бачити в ночі, а друга визначає здатність її одночасно відображати деталі у дуже темних і дуже світлих ділянках кадру.

Фокусна відстань та кут огляду належать до класифікаційних ознак, які говорять про розмір сцени спостереження.

Класифікація сучасних відеокамер загалом у системах безпеки є розгалуженою, оскільки вибір конкретної моделі залежить від умов експлуатації, мети спостереження та бюджету.

Ось основні критерії, за якими поділяють дане обладнання.

1. За типом передачі сигналу

Це фундаментальна відмінність, яка визначає архітектуру всієї системи:

– IP-камери (Цифрові): Передають дані у форматі цифрового потоку через локальну мережу (Ethernet). Мають високу роздільну здатність, аналітичні функції (розпізнавання облич, номерів) та можливість живлення через PoE (Power over Ethernet);

– аналогові (HD-TVI, HD-CVI, AHD): Сучасні стандарти дозволяють передавати сигнал високої чіткості по коаксіальному кабелю. Вони дешевші та простіші в налаштуванні, але обмежені в інтелектуальних функціях.

2. За місцем встановлення:

– внутрішні (призначені виключно для приміщень і не захищені від вологи та екстремальних температур);

– вуличні (мають захисний герметичний корпус (стандарт IP66/IP67) та систему підігріву для роботи взимку).

3. За формою корпусу:

– купольні (Dome) – напівсферичні камери, які часто встановлюють на стелях. Завдяки формі важко зрозуміти, куди саме спрямований об'єктив;

– циліндричні (Bullet) – класичні вуличні камери з козирком. Зручні для спрямованого спостереження за конкретними зонами (ворота, проходи);

– поворотні (PTZ) – камери, якими можна керувати дистанційно (повертати, нахиляти, наближати зображення за допомогою оптичного зуму);

– кубічні (Cube) – компактні рішення для офісів або квартир, часто мають вбудований мікрофон та Wi-Fi.

4. За типом об'єктива:

– фіксований (має незмінну фокусну відстань (наприклад, 2.8 мм для широкого кута або 4 мм для деталізації));

– варіофокальний (дозволяє вручну налаштувати кут огляду під час монтажу);

– моторизований (дозволяє змінювати фокусну відстань дистанційно через програмне забезпечення).

Додаткові параметри вибору:

– дальність ІЧ-підсвітки (наскільки далеко камера «бачить» у повній темряві);

– світлочутливість (здатність видавати кольорове зображення при низькому освітленні (технології типу ColorVu або DarkFighter));

– WDR (Wide Dynamic Range) (функція, що дозволяє бачити деталі в тіні, навіть якщо в кадр потрапляє яскраве світло (наприклад, сонце у вікні)).

Технічні характеристики відеокамер. Технічні характеристики відеокамер визначають якість зображення, надійність роботи в різних умовах та аналітичні можливості системи.

Нижче наведено ключові параметри, на які варто звернути увагу при виборі відеокамер.

1. Параметри зображення.

Роздільна здатність (Resolution): вимірюється в мегапікселях (Мп).

– 2 Мп (Full HD): базовий рівень для загального огляду приміщень;

– 4-5 Мп: оптимальний баланс для вулиці (дозволяє ідентифікувати обличчя на відстані 5–10 м);

– 8 Мп (4K) та 12 Мп: для об’єктів з високими вимогами до деталізації (каси, парковки).

Світлочутливість (Lux): здатність камери бачити при слабкому освітленні. Показник 0,001 Lux і нижче дозволяє отримати кольорову картинку навіть вночі (технології типу ColorVu або Full-color).

Частота кадрів (FPS): для плавного відео стандартом є 25-30 к/с. Для спостереження за об’єктами, що швидко рухаються (авто), іноді використовують 50-60 к/с.

2. Оптична система та кути огляду.

Фокусна відстань об’єктива (мм) прямо впливає на те, що ви побачите:

– 2.8 мм: широкий кут (близько 100°-110°). Підходить для малих кімнат або загального огляду подвір’я;

– 4 мм: середній кут (80°-90°). Краща деталізація на середніх відстанях;

– 6-12 мм: вузький кут. Використовується для спостереження за коридорами або конкретними точками (в’їзні ворота).

3. Функції покращення зображення (DSP-функції).

Це програмно-апаратні алгоритми, що «рятують» картинку в складних умовах:

– WDR (Wide Dynamic Range): апаратний WDR (120 дБ і вище) необхідний, якщо камера дивиться проти сонця або на вікно. Він вирівнює яскраві та темні ділянки;

– 3D DNR: цифрове придушення шумів (особливо важливо для «чистої» картинки вночі);

– BLC/HLC: компенсація задньої та передньої засвітки (наприклад, від фар авто).

4. Інтелектуальні можливості (AI & Analytics).

Сучасні професійні камери (лінійки AcuSense, WizSense) мають вбудований нейропроцесор (NPU):

– класифікація об’єктів: відрізняє людину або транспорт від тварин чи гілок дерев (зменшує хибні тривоги на 90%);

– детекція обличь та номерних знаків: автоматичне розпізнавання та пошук в базі даних;

– Smart Dual Light: камера працює в ІЧ-режимі (невидимо), але при виявленні людини вмикає біле LED-світло для кольорового запису та психологічного впливу.

5. Конструктивні характеристики.

Ступінь захисту IP: для вулиці мінімум IP67 (захист від води та пилу).

Антивандальний захист IK: клас IK10 означає, що корпус витримає удар молотком.

Живлення PoE (Power over Ethernet): передача живлення та даних по одному кабелю «вита пара».

Кодеки стиснення: підтримка H.265+ важлива для економії місця на жорсткому диску (економить до 70–80% обсягу порівняно зі старими форматами).

Типи та розмірний ряд світлочутливих матриць. Відомі дві основні технології створення матриць: ПЗЗ – прилад із зарядним зв’язком (в англомовній літературі використовується термін CCD – Charge Coupled Device) і КМОП – комплементарний металооксидний напівпровідник (в англ. літературі CMOS – Complementary Metal Oxide Semiconductor). Кожна з них має сильні і слабкі сторони, що робить їх придатними для різних застосувань.

ПЗЗ-матриці свого часу були спеціально розроблені для виробництва відеокамер. Вони мають малі шуми і високу світлочутливість, що забезпечує краще зображення при малому освітленні. Однак вони більш складні у виготовленні, відносно дорогі і споживають набагато більше потужності, ніж КМОП- матриці. Окрім цього, якщо у поле зору камери потрапить занадто яскравий об’єкт (сонце, фара), то ПЗЗ матриця дасть розмивчасте зображення.

КМОП-матриці засновані на стандартній і давно відомої технології, яка широко використовується, наприклад, у виробництві мікросхем пам’яті. У КМОП-матрицях використовуються польові транзистори з ізольованим затвором і з каналами різної провідності. Ці матриці мають меншу світлочутливість ніж ПЗЗ матриці, що стає очевидним при поганому освітленні.

Продовженням КМОП матриць стали PIXIM матриці. Ключовим моментом PIXIM матриць є «присутність» аналого-цифрового перетворювача

безпосередньо в кожному пікселі матриці, і незалежна мікропроцесорна обробка сигналу в режимі реального часу.

У PIXIM матрицях для кожного пікселя проводиться «замір» інтенсивності освітлення. Після цього для кожного пікселя підбирається найкращий час експозиції з п’яти можливих значень. Такий підхід називається мультисемплінгом і дозволяє працювати з динамічним діапазоном освітленості сцени, оброблюваної матрицею, до 120дБ.

Таким чином, основою сучасної відеокамери є матриця, яка представляє собою прямокутну світлочутливу напівпровідникову пластинку з певним відношенням сторін, перетворюючу падаюче на неї світло в електричні заряди, які використовуються для отримання вихідного відеосигналу за допомогою спеціальної електронної схеми. Чим більше число елементів розкладання – пікселів, тим менш помітна дискретність результуючого зображення.

На сьогоднішній день існує багато різновидів камер для відеоспостереження. Для того щоб правильно вибрати відеокамеру, необхідно для початку зрозуміти, для яких потреб їх планується використовувати, а також визначитися з кількістю камер та їх технічними характеристиками.

У деяких випадках, коли потрібно мати дуже широкий огляд (кут зору) або навпаки максимально «наблизити» віддалений об’єкт доцільно вибирати відеокамеру з правильним значенням формату (розміру) матриці. Як впливає формат матриці на ширину поля зору добре продемонстровано на нижче поданих фотографіях.

Показник формату матриці представляє собою розмір діагоналі, і виражений в дюймах. Вимірювати діагональ матриці прийнято у відіконових дюймах. Ця одиниця виміру, рівна 2/3 звичайного дюйма (16,9 мм).

Оскільки, від формату залежить кут огляду камери (рис. 2.1), тому установка відеокамер проводиться після вибору обладнання з потрібним кутом огляду. Також від матриці залежить і те, які об’єктиви можна встановлювати на камеру (в разі, якщо сама модель допускає зміну об’єктива).

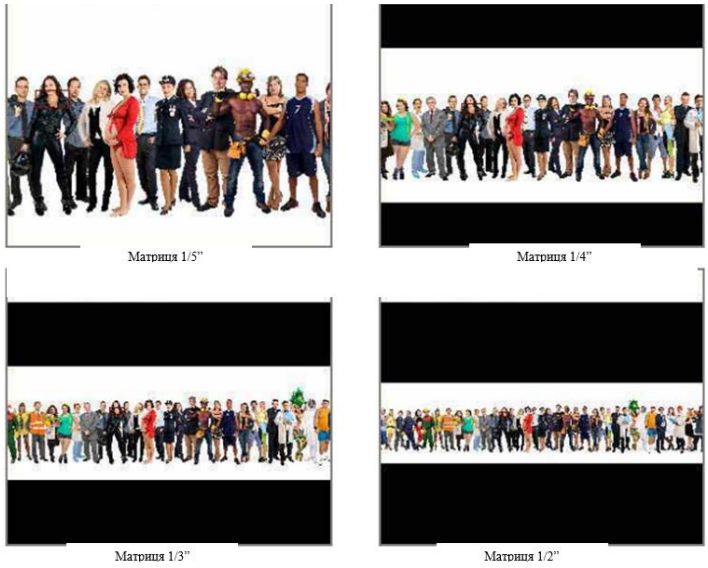


Рисунок 2.1 – вплив формату матриці на розмір сцени

У СВС використовують два основних формати кадра – 4:3 і 16:9.

Формат матриць подано в таблиці 2.1.

Таблиця 2.1 – Розміри матриць з форматом кадра 4:3 та 16:9

Формат матриці 4:3				Формат матриці 16:9			
Розмір матриці	Ширина, мм	Висота, мм	Діагональ, мм	Розмір матриці	Ширина, мм	Висота, мм	Діагональ, мм
1″	13,54	10,16	16,93	1″	14,76	8,3	16,93
2/3″	9,04	6,78	11,28	2/3″	9,84	5,54	11,28
½″	6,77	5,08	8,47	½″	7,38	4,15	8,47
½,5″	5,42	4,06	6,77	½,5″	5,9	3,32	6,77
½,7″	5,02	3,76	6,27	½,7″	5,47	3,07	6,27
½,8″	4,84	3,63	6,05	½,8″	5,27	2,96	6,05
1/3″	4,52	3,39	5,64	1/3″	4,92	2,77	5,64
¼″	3,39	2,54	4,23	¼″	3,69	2,08	4,23

Знання формату матриці необхідне для вибору потрібного об’єктива: оскільки, діаметр окружності, в якій відображається сфокусоване об’єктивом зображення, має відповідати діагоналі матриці. Так як матриця має форму прямокутника, то на неї припадає лише частина проектованого кругового зображення. Якщо формати матриці і об’єктиву співпадають, то прямокутник матриці точно вписується в коло.

Роздільна здатність матриці – це загальна кількість пікселів, що беруть участь у створенні зображення кадра. Цей параметр зазвичай наводиться у вигляді добутку кількості пікселів за горизонтом на кількість пікселів за вертикаллю.

Кожна матриця відеокамери складається з світлочутливих елементів, називаються пікселями. Від кількості пікселів в матриці залежить її роздільна здатність - деталізація зображення.

Пікселі, які беруть участь у створенні зображення сцени, називаються ефективними пікселями. Саме кількість ефективних пікселів враховують при оцінці цього параметра відеокамери.

По периметру матриці розташовані додаткові пікселі, які використовуються для різних вимірювань. Наприклад, для визначення "рівня чорного". Ці пікселі наводяться в описі матриць, коли потрібно вказати загальну кількість пікселів. Тому в характеристиках відеокамер часто можна побачити такий запис: кількість ефективних пікселів: 2308x1712, загальна кількість пікселів: 2384x1734.

Для того, щоб окремо визначити роздільну здатність по горизонталі і вертикалі слід врахувати співвідношення сторін матриці. Так для матриці формату 4:3 кількість пікселів за висотою визначається $n_в$ як:

$$n_в = 0{,}75 n_м, \tag{2.1}$$

де 0,75 – коефіцієнт, який враховує співвідношення сторін матриці; $n_м$ – загальна кількість пікселів матриці, шт.

Кількість пікселів матриці за шириною

$$n_ш = \sqrt{\frac{n_м}{0{,}75}}\,. \qquad (2.2)$$

Таблиця 2.2 – Роздільні здатності типових відеокамер

Тип камери	Загальна кількість пікселів, $n_м$ шт	Кількість пікселів за висотою, $n_в$ шт	Кількість пікселів за шириною, $n_ш$ шт
HD 720	921.600	720	1280
1.3 MPix	1.310.720	1024	1280
HD 1080	2.073.600	1080	1920
2 MPix	1.920.000	1200	1600
3 MPix	3.145.728	1536	2048
5 MPix	4.915.200	1920	2560

Кількість пікселів завжди вказується в паспорті на відеокамеру. На ринку відеокамер на початку 2019 р. даний сегмент представлений від 1D до 12 Мп – найбільший попит був на 2 Мп камери, станом на початок 2025 р. домінують 3 і 5 Мп.

Чутливість матриці – це її здатність реагувати на падаюче світло, генеруючи пропорційний цьому світловому потоку заряд фотоелектронів в відео сенсорі.

Чутливість матриці виражається двома параметрами – інтегральною чутливістю і спектральною чутливістю.

Спектральна чутливість – це залежність чутливості від довжини хвилі падаючого світла (т. е. від кольору).

У порівнянні з людським оком спектральна чутливість більшості камер, більш широка і простягається як в інфрачервоний, так і в ультрафіолетовий діапазон хвиль.

Таким чином, на відміну від ока, спектральна чутливість матриць дозволяє реєструвати випромінювання в значно ширшому діапазоні хвиль.

Щоб в світлий час доби інфрачервоний діапазон хвиль з небосхилу не створював паразитне засвічення на зображенні, матрицю камери завжди захищають спеціальним інфрачервоним фільтром.

У темний час доби, коли виникає необхідність використовувати ІЧ прожектор, інфрачервоний фільтр з матриці видаляють.

У характеристиках відеокамер, що володіють можливістю видаляти ІЧ фільтр, зазвичай вказують – механічно зрушується ІЧ-фільтр або просто ICR (Infrared Cut filter mechanically Removable) фільтр.

З широким розповсюдженням пристроїв інфрачервоного підсвічування, чутливість камер в цьому діапазоні хвиль стали збільшувати. В результаті з’явилися різновиди матриць, які мають підвищену чутливість в ІЧ області.

Для збільшення чутливості матриць деякі виробники використовують мікролінзи, що встановлюються над кожним пікселем.

Оскільки матриці добре «бачать» і в ультрафіолетової області спектра, який широко використовується в медицині, то в деяких випадках об’єктив

відеокамери потрібно закривати спеціальним фільтром, що захищає матрицю від УФ випромінювання.

Інтегральна чутливість – це коефіцієнт пропорційності між величиною загального падаючого світлового потоку і фотоструму, що виникає в матриці (в міліамперах).

У системах відеоспостереження для оцінки чутливості використовують два параметра, які характеризують можливість відеокамери працювати при слабкому освітленні – «чутливість» і «мінімальна освітленість».

Чутливість – таке мінімальне значення освітленості сцени, при якій сигнал на виході камери відповідає відмінній якості зображення.

Мінімальна освітленість – таке мінімальне значення освітленості сцени, при якій камера створює ледь помітне зображення.

Чутливість і мінімальна освітленість мають розмірність люкс.

Формулювання чутливості для цього випадку виглядає так: чутливість відеокамери – це таке мінімальне значення отвору діафрагми, при якій розмах відеосигналу на виході камери дорівнює 1 вольт при освітленості тестової таблиці у 2000 люкс джерелом з колірною температурою 3200 градусів Кельвіна.

Апертура або світлосила об'єктива. Об'єктив в CCTV – оптична система, яка формує зображення на світлочутливому елементі відеокамери (відео сенсорі).

Об'єктив складається з групи передніх лінз, діафрагми і групи задніх лінз. Група передніх лінз формує задані кути зору об'єктива. Група задніх лінз забезпечує розмір світлової плями, відповідного формату відео сенсора.

Між групою передніх і задніх лінз присутня діафрагма, необхідна для регулювання кількості світла, що потрапляє на відео сенсор відеокамери.

Діафрагмою називається непрозора перепона з отвором, що розташована на шляху світлового потоку .

Діафрагма складається з пелюсток (ірисів), кількість яких може бути від 3 до 20. Чим більше пелюсток в діафрагми, тим більше отвір діафрагми наближається до кола, створюючи тим самим рівномірно освітлену світлову пляму на відео сенсорі.

Шкала значень діафрагми стандартизована і утворює наступний ряд відносних отворів: 1:0,7; 1:1; 1:1,4; 1:2; 1:2,8; 1:4; 1:5,6; 1:8; 1:11; 1:16; 1:22; 1:32; 1:45; 1:64.

Зовнішній вигляд ірисової діафрагми, з різними значеннями відносних отворів, наведено на рисунку 2.2.

Знаменники відносних отворів (2; 2,8; ...) називаються діафрагмовими числами.

При зміні отвору діафрагми змінюється і глибина різко зображуваного простору сцени. Повністю відкрита діафрагма створює мінімальну глибину різкості, а при закритій діафрагмі максимальну.

Крім цього величина отвору діафрагми дозволяє управляти чіткістю створюваного зображення. При повністю відкритій діафрагмі чіткість

мінімальна, а при закритті діафрагми, існує таке її значення, при якому чіткість максимальна.

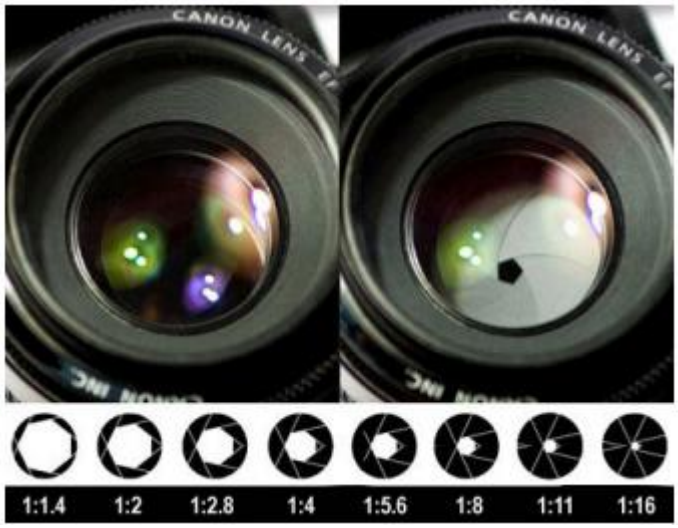


Рисунок 2.2 – Розкриття діафрагми за відповідних значень відносних отворів

Типи об'єктивів. За оптичними властивостями об'єктиви бувають сферичні і асферичні.

Сферичні об'єктиви набули більшого поширення в зв'язку з тим, що вони виготовляються з сферичних лінз, які дешеві у виготовленні і технологічні. Істотним недоліком цих об'єктивів є сферичні аберації, які погіршують якість зображення (роздільну здатність) і обмежують максимально можливий отвір діафрагми (F-число таких об'єктивів зазвичай має величину F/1.2 - F/1.4).

Асферичний об'єктив зовні відрізняється від сферичних об'єктивів видом передньої лінзи. У таких об'єктивів аберраційні спотворення мають незначну величину, що дозволяє їм мати F-число F/0.75 - F/0.8. Таке мале значення F-числа в середньому в три рази збільшує світловий потік, що проходить на відеокамеру.

Застосування асферических об'єктивів дозволяє камері в умовах гіршої освітленості формувати якісне зображення на відміну від сферичної оптики.

Просвітлений об'єктив зменшує світлорозсіювання на шляху проходження світлового потоку до відео сенсора. Для зменшення світлорозсіювання в об'єктиві на лінзи, які мають контакт з повітрям, наносять спеціальне покриття.

У просвітлених об'єктивів світловий потік послаблюється в середньому на 10%, в той час як у непросвітленого об'єктива ослаблення доходить до 33%.

Зображення, що отримується з просвітленого об'єктива, має значно більший контраст, що збільшує кількість градацій яскравості в ділянках слабкої освітленості. В результаті елементи зображення в темних ділянках сцени стають краще помітні.

Просвітлений об'єктив вимагає дбайливого ставлення, так як покриття, нанесене на поверхню лінз, легко пошкоджується при попаданні на них масел і інших жирів.

Об’єктиви за фокусною відстанню поділяються на:

– об’єктиви з постійною фокусною відстанню (монофокальні – статичні або фіксовані);

– об’єктиви з фокусною відстанню, яку змінюють вручну (варіооб’єктиви, варіофокальні);

– об’єктиви з фокусною відстанню, змінною дистанційно за допомогою пульта управління (трансфокатор, трансфокаторні).

Монофокальні об’єктиви характеризуються фіксованою величиною фокусної відстані. Споживач не зможе самостійно регулювати кут огляду або здійснювати механічне фокусування. Основний плюс монофокальних об’єктивів – проста установка і низька вартість.

Варіфокальні об’єктиви мають ряд вигідних відмінностей. Наприклад, можна регулювати фокусну відстань об’єктива і змінювати кут огляду камери. При встановленні передбачене ручне регулювання кута огляду, також необхідно навести фокус на той об’єкт, який планується знімати. Таке налаштування проводиться тільки один раз. Наступні зміни знадобляться, якщо буде потрібен інший кут огляду. Подібний варіант відеоспостереження можна використовувати у різних випадках, тому варіофокальні об’єктиви вважаються універсальними.

Трансфокатори (зум-об’єктиви) як правило, встановлюються на камери вуличного відеоспостереження. Обумовлено це тим, що вони дають можливість регулювати не тільки кут огляду, а й виконувати масштабування площі спостереження. Цей тип об’єктива використовується і в PTZ-відеокамерах. У них різкість, фокусна відстань і кут огляду встановлюються за допомогою дистанційного пульта управління.

Фокусна відстань, кут огляду і лінійне поле сцени спостереження. Фокусна відстань в охоронному телебаченні є основним параметром, з допомогою якого користувач може вибирати необхідні ділянки сцени для виведення зображення на монітор. Фокусна відстань має прямий зв’язок з кутом зору об’єктива. Чим більша фокусна відстань об’єктива (5.6 мм більше 2.8 мм), тим вужчий кут його зору, і навпаки, чим менше фокусна відстань, тим ширше кут зору (рис. 2.3).

Рисунок 2.3 – Вигляд сцени за різних фокусних відстанях об’єктива

Правильний вибір фокусної відстані у об’єктива створює передумови для вирішення основних завдань, які стоять перед системами відеоспостереження, а саме: виявити, розрізнити і ідентифікувати об’єкт спостереження.

Фокусна відстань оптики людського ока – відстань від центру кришталика до поверхні сітківки складає приблизно 17 мм.

Об’єктиви, що відповідають оптиці людського ока для матриці розміром 1 дюйм мають фокусну відстань 25 мм, для 2/3-дюймовою – 16 мм, для 1/2-дюймової – 12,5 мм, для 1/3-дюймовою – 8 мм, а для 1/4-дюймової – 6 мм.

Чим більше типорозмір матриці, тим вища якість одержуваного зображення. Найчіткіше зображення видає відеокамера на матриці CCD 1/2", але така матриця буде найдорожчою.

Для того, щоб відображення зони об’єкта спостереження повністю потрапляло на поверхню матриці, повинна виконуватись рівність:

$$\frac{f}{v} = \frac{D}{V}. \tag{2.3}$$

Звідси

$$f = v\frac{D}{V}. \tag{2.4}$$

У відповідності до даних рисунка 2.4, фокусна відстань об’єктива

$f = 4{,}8\dfrac{2500}{330} = 36{,}36$ мм.

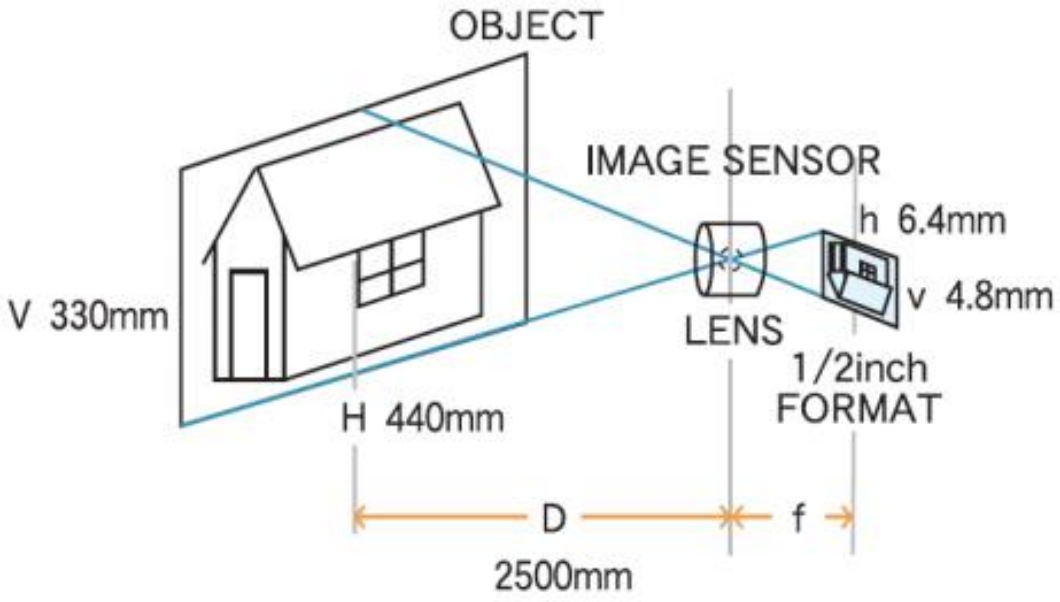


Рисунок 2.4 – Схема до визначення фокуса об’єктива: f – фокусна відстань лінзи об’єктива, v – висота матриці сенсора відеокамери, h – ширина матриці сенсора відеокамери, D – відстань до об’єкта спостереження, V – висота об’єкта спостереження

Під час вибору фокусної відстані об’єктива слід враховувати, що кут ясного зору людини по горизонталі складає приблизно 36°, що відповідає фокусної відстані ~ 6,9 мм (для відеокамери з розміром матриці 1/3"). Тому відеокамери з фокусною відстанню об’єктива менше 6,9 мм будуть візуально віддаляти зображення, більше 6,9 мм – відповідно наближати.

Кут огляду об’єктива визначає величину видимого об’єкта і масштаб зображення в кадрі.

На рисунку 2.5 подано схему, яка пояснює залежність фокусної відстані *f* об’єктива і розміру *h* спроектованого зображення на матрицю відеокамери.

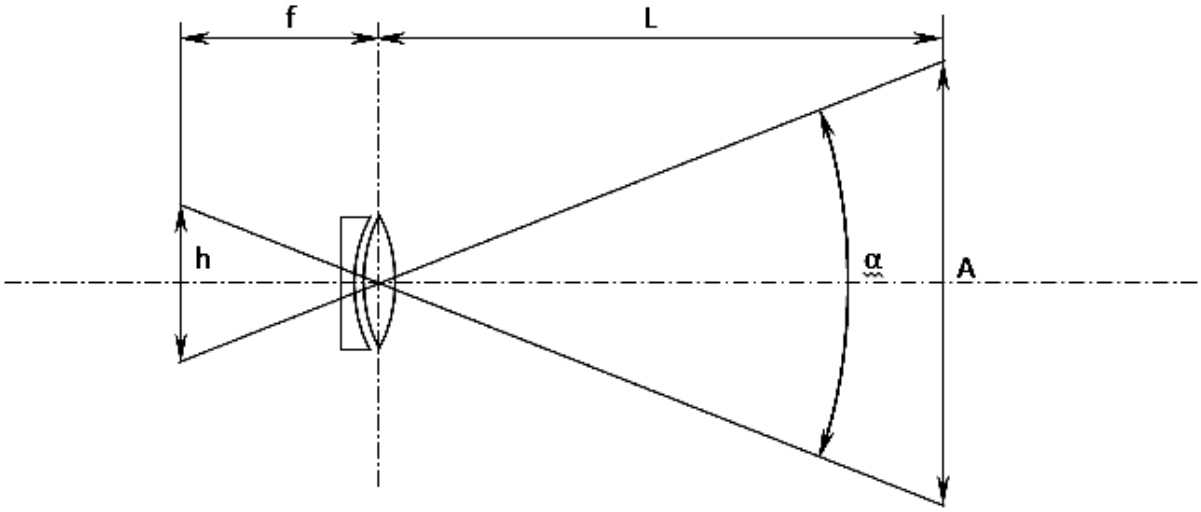


Рисунок 2.5 –. Оптична схема отримання зображення на матриці відеокамери: *A* – розмір об’єкта спостереження, *f* – фокусна відстань, *h* – розмір матриці, *L* – відстань до об’єкта спостереження, α – кут огляду

Згідно наведеної схеми видно, що на величину кута огляду впливає фокусна відстань об’єктива і розмір матриці. Кут огляду, стосовно рисунка 2.5, визначають за формулою:

$$\alpha = 2arctg\frac{h}{2f}, \tag{2.5}$$

де *f* – фокусна відстань об’єктива (мм), *h* – розмір матриці відеокамери (мм).

Вертикальний і горизонтальний кут огляду матриць різний, так як ширина і висота їх відмінні.

Вертикальний кут визначається як:

$$\alpha_в = 2arctg\frac{h_в}{2f}, \tag{2.6}$$

де $h_в$ – висота матриці (мм).

Горизонтальний кут визначається як:

$$\alpha_г = 2arctg\frac{h_г}{2f}, \qquad (2.7)$$

де $h_г$ – ширина матриці (мм).

Регулювання діафрагми. Відносний отвір – це відношення діаметра отвору діафрагми до його фокусної відстані. Величина відносного отвору записується як 1:2.8.

На кільці регулювання діафрагми об’єктива (в основному, фотографічних) нанесена шкала з знаменників відносних отворів (діафрагмові числа: 2,8; 4; 5,6; 8; 11; 16; 22), відповідних різним значенням отворів діафрагми.

Переклад діафрагми на одну поділку змінює відносний отвір в 1,4 рази, що дає збільшення або зменшення освітленості оптичного зображення в два рази, за винятком перших двох чисел діафрагми, у яких такої зміни може і не бути.

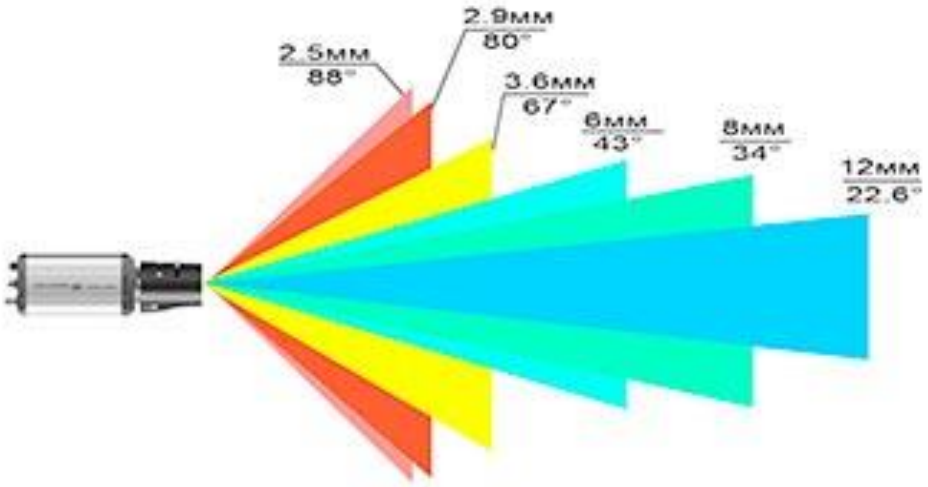


Рисунок 2.6 – Відношення кута огляду об’єктива до фокусної відстані для матриці 1.3”

Види кріплення змінних об’єктивів. У паспортах відеокамер (корпусних) зі змінним об’єктивом вказується вид кріплення об’єктива (Lens Mount), який визначає конструктивну їх сумісність.

Існує два варіанти виконання відеокамер в залежності від відстані від площини розташування матриці до місця встановлення об’єктива – C-Mount і CS-Mount. Це відстань в обох варіантах різниться приблизно на 5 мм, відповідно до чого випускають і об’єктиви з кріпленням C або CS.

Щоб зображення було чітко сфокусоване на матриці, необхідно, щоб з відеокамерою C експлуатувався об’єктив C (рис. 2.7), а з відеокамерою CS - об’єктив CS, в іншому випадку зображення виявиться розфокусованим.

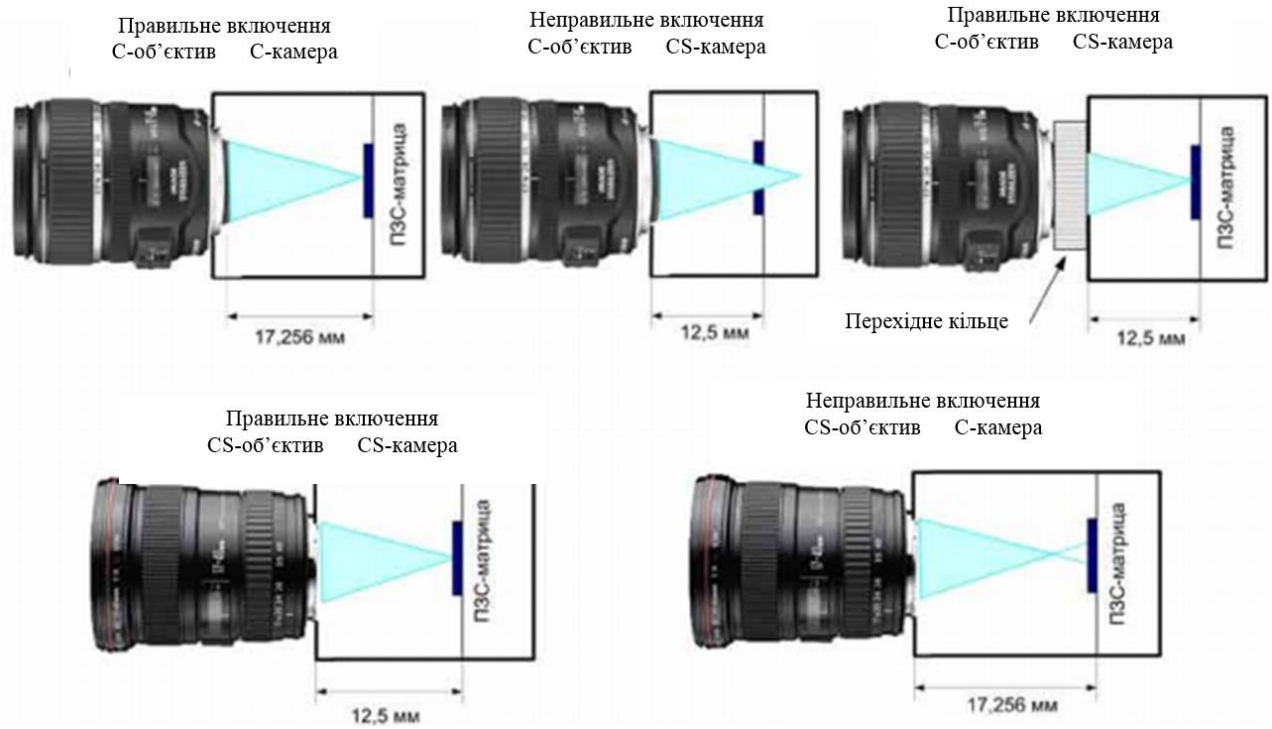


Рисунок 2.7 – Кріплення об'єктивів корпусних камер

Можливий єдиний варіант змішаного з'єднання: з відеокамерою CS може використовуватися об'єктив С, але тільки за умови, що між ним і відеокамерою буде встановлено спеціальне перехідне кільце C/CS.

При установленні об'єктиву з «CS» – кріплення на відеокамеру, розраховану на «С» – кріплення, зображення виявляється сфокусованим перед площиною ПЗС матриці. Виправити таку ситуацію неможливо.

Деякі відеокамери мають вбудоване різьбове кільце з великим ходом, що дозволяє відмовитися від використання CS-кільця і гарантує гарне фокусування при налаштуванні зворотного фокуса.

Різкість зображення та її глибина. Різкість – це стан лінз об'єктива, що забезпечує відсутність розмитості на контурах великих об'єктів при якому зображення максимально контрастне.

Різкість зображення об'єкта, віддаленого від відеокамери на якусь відстань, досягається за допомогою органів налаштування, розташованих на об'єктиві.

Глибиною різкості називається властивість об'єктива зображати в одній площині і практично з однаковою різкістю предмети, віддалені від об'єктива на різні відстані.

У практичній діяльності глибина різкості характеризується ближньою і далекою межами, в яких зображення різке.

Ілюстрація глибини різкості приведена на рисунку 2.8 видно, що різкість цифр і міліметрових штрихів на лінійці не однакова. Лінійка відображається різко від 14,5 см до 19,5 см.

Глибина різкості відеокамери протягом доби змінюється. Пов’язано це з тим, що зміна освітленості сцени викликає у об’єктива з автоматичною діафрагмою зміну отвору діафрагми.

Рисунок 2.8 – Пояснення до глибини різкості зображення

На рисунку 2.9 пояснюється як зміна отвору діафрагми формує глибину різкості різної величини.

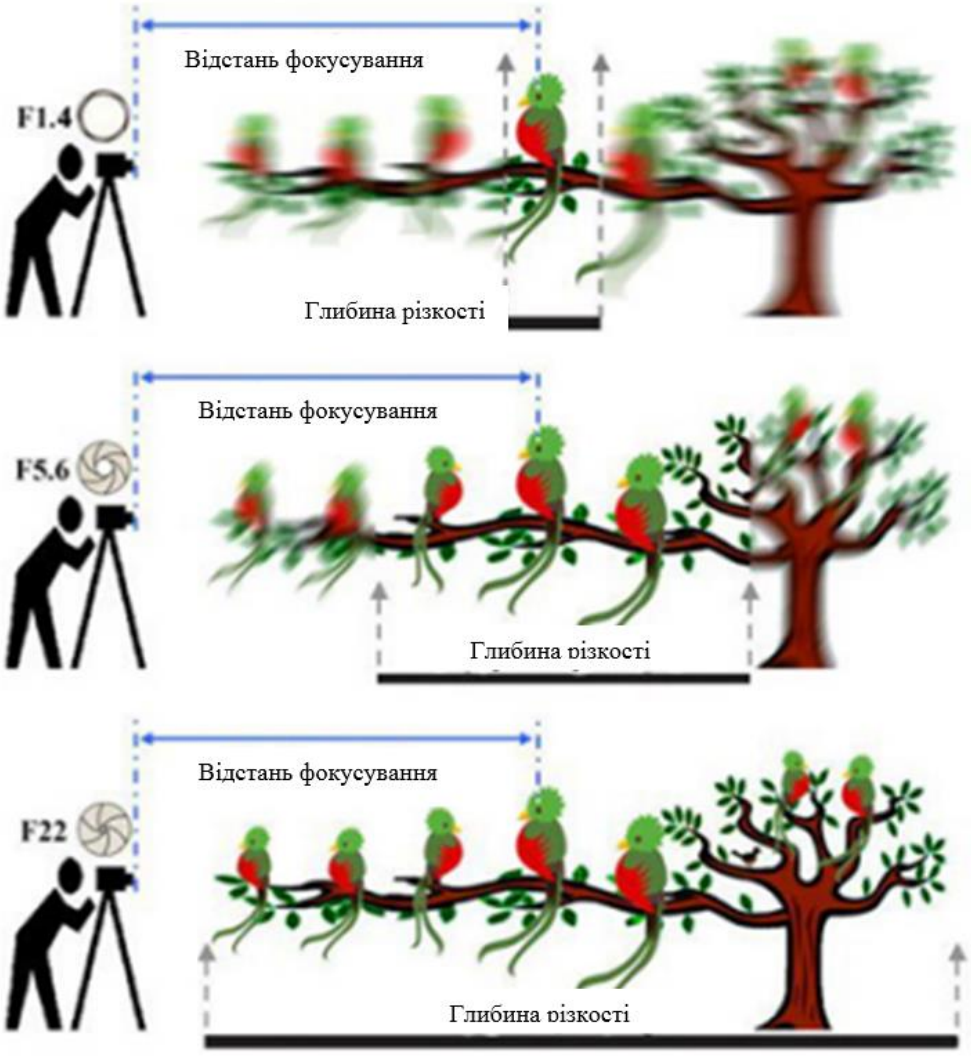


Рисунок 2.9 – Вплив отвору діафрагми на різкості зображення

Якщо діафрагма повністю відкрита, то всі промені сходяться в фокусі на поверхні ПЗЗ матриці.

Якщо закрити об’єктив діафрагмою, то промені зійдуться в тій же точці фокуса, але допустимий гурток розсіювання буде перебувати від площини ПЗЗ матриці значно далі і як наслідок глибина різкості буде більшою.

Знаючи цю властивість об’єктива необхідно враховувати його при проектуванні секторів спостереження, не допускаючи втрату різкості на контрольованих службою безпеки ділянках.

Електронний затвор (Electronic Shutter). Електронний затвор, або Electronic Shutter, є фундаментальною функцією сучасних камер відеоспостереження (CCTV). На відміну від механічного затвора, який фізично відкриває та закриває доступ світла до плівки чи сенсора, електронний затвор виконує цю функцію цифровим способом, контролюючи час, протягом якого світлочутливий сенсор (CCD або CMOS) накопичує електричний заряд (сигнал) від отриманого світла.

Робота електронного затвора зводиться до управління часом експозиції (витримкою). Це період, протягом якого пікселі сенсора збирають фотони світла.

Початок експозиції – заряд (накопичене світло) на сенсорі скидається до нуля.

Накопичення світла – протягом певного, дуже короткого проміжку часу (витримки), пікселі накопичують заряд, пропорційний кількості світла, що на них потрапляє.

Кінець експозиції – після закінчення часу витримки накопичений заряд зчитується, перетворюється на цифровий сигнал і формує один кадр зображення.

Швидкість електронного затвора відеокамери – це час, за який матриця камери «дивиться» на об’єкт, а отже, час накопичення світла. Даний параметр вимірюється як обернена величина до часу експозиції (наприклад, 1/30 с, 1/1000 с, 1/100000 с).

Повільна швидкість затвора (довга витримка, наприклад, 1/50 с): Дозволяє сенсору накопичити більше світла, що ідеально підходить для слабкого освітлення. Однак це підвищує ризик розмиття рухомих об’єктів (рис. 2.10).

Висока швидкість затвора (коротка витримка, наприклад, 1/5000 с): Скорочує час накопичення світла, що ідеально для яскравого освітлення або для фіксації швидкого руху (наприклад, номерних знаків автомобілів), роблячи зображення різким, але може призвести до його затемнення.

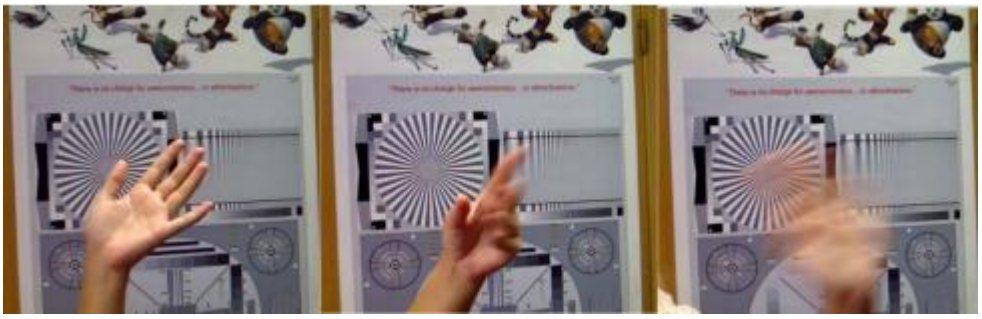


Рисунок 2.10 – Зображення стоп-кадра за витримки 1/250, 1/125 і 1/50

У системах відеоспостереження електронний затвор має два основні режими налаштування: автоматичний і фіксований.

Автоматичний електронний затвор (AES/Auto Shutter) – стандартний режим роботи більшості відеокамер. У такому режимі камера автоматично регулює швидкість затвора залежно від рівня освітлення в сцені, щоб підтримувати постійну яскравість зображення. Коли світла багато, затвор прискорюється (наприклад, до 1/1000 с) для запобігання пересвічуванню. Коли світла мало, затвор уповільнюється (наприклад, до базового значення 1/50 с), щоб «зловити» більше світла і зберегти яскравість.

Фіксована швидкість затвора (Manual Shutter) передбачає можливість встановлення потрібного значення швидкості вручну оператором або інсталятором. Це робиться для вирішення специфічних завдань:

– фіксації руху, якщо потрібно гарантовано захоплювати чіткі зображення рухомих об’єктів (наприклад, у місцях проїзду транспорту), встановлюється висока швидкість (наприклад, 1/2000 с);

– усунення мерехтіння, якщо у регіонах з частотою електромережі 50 Гц (наприклад, Європа, Україна) для запобігання смугам від люмінесцентних ламп швидкість затвора часто фіксують на 1/50 с або 1/100 с, а у регіонах з 60 Гц (наприклад, США) – на 1/60 с або 1/120 с;

Якщо діафрагма об’єктива контролює кількість світла, що потрапляє на сенсор, то електронний затвор контролює час накопичення цього світла. У тандемі вони забезпечують правильну експозицію. Камери з автоматичною діафрагмою (Auto Iris) точніше контролюють світло разом з електронним затвором.

Коли електронний затвор вже не може уповільнитися (досягнувши, наприклад, 1/50 с), для додаткового освітлення зображення вмикається функція AGC (Automatic Gain Control), який підсилює сигнал, але одночасно підсилює і шум.

При проектуванні CCTV для критичних зон, де є швидкий рух (наприклад, дороги, входи/виходи), необхідно обмежувати автоматичний режим затвора або встановлювати його на високу фіксовану швидкість, щоб запобігти розмиттю.

Незважаючи на ризик затемнення зображення, чіткість рухомих об’єктів є пріоритетом для доказової бази. Таким чином, електронний затвор є

фундаментальним параметром, що визначає якість фіксації динамічних подій у системі відеоспостереження.

Функція Sense-Up/DSS: збільшення світлочутливості в CCTV. Функція Sense-Up (у перекладі як «підвищення чутливості») або її синонім DSS (Digital Slow Shutter), що означає «цифровий повільний затвор», є ключовою технологією в сучасних камерах відеоспостереження. Її головна мета – забезпечити якісне, світле зображення в умовах надзвичайно низького освітлення, де звичайні камери вже не справляються.

Sense-Up/DSS працює за принципом накопичення світла. Звичайна камера відеоспостереження працює з певною фіксованою частотою кадрів, зазвичай 25 або 30 кадрів на секунду (fps), що відповідає часу експозиції 1/25 або 1/30 секунди. Коли освітлення падає до критичного рівня, цього часу експозиції недостатньо для захоплення світла, і зображення стає темним та шумним.

Функція Sense-Up штучно збільшує час витримки для кожного кадру. Замість того, щоб формувати один кадр за 1/30 секунди, камера може «накопичувати» світло протягом 1/15, 1/10 чи 1/5 секунди або навіть довше.

Ефективність Sense-Up часто вимірюється в кратності (X-кратне збільшення витримки) або вказується максимальний час витримки. Наприклад, налаштування Sense-Up x10 означає, що час витримки збільшується в 10 разів від базового, що дозволяє отримати набагато світліше зображення.

До переваг використання Sense-Up слід віднести: можливість отримати кольорове або якісне чорно-біле зображення навіть у майже повній темряві, де ІЧ підсвічування може бути недостатнім або небажаним; дозволяє зберегти кольорове зображення довше, оскільки накопичення світла може бути достатнім для роботи кольорового фільтра (це важливо для ідентифікації об’єктів, наприклад, кольору одягу, автомобіля); ефективність в місцях із надзвичайно слабким, але присутнім освітленням (наприклад, від далеких ліхтарів або місячного світла).

Попри значні переваги у світлочутливості, Sense-Up/DSS має суттєвий недолік, який необхідно враховувати при проектуванні – ефект розмиття руху. На низьких рівнях Sense-Up (x2-x4) розмиття може бути незначним, але помітним, а на високих рівнях (x8 і вище) рухома людина чи автомобіль перетвориться на нечітку смугу, що унеможливлює ідентифікацію обличчя чи номерного знака. Також до недоліків слід віднести обмеження в частоті кадрів. Так, якщо камера накопичує світло протягом, наприклад, 1/5 секунди, вона фізично не може формувати більше 5 кадрів на секунду. Фактична частота кадрів запису значно знижується, що погіршує плавність відео та ускладнює перегляд динамічних подій.

Таким чином, функцію Sense-Up/DSS слід використовувати з обережністю, враховуючи специфіку об’єкта спостереження. Вона ідеально підходить для моніторингу статичних зон, де рух є мінімальним або несуттєвим, а головне завдання – загальний огляд ситуації та виявлення присутності. Це стосується складських приміщень вночі та охорони периметра, де важливо помітити лише появу.

Цю функцію не рекомендується використовувати для критичних зон, де необхідно чітке розпізнавання обличь або номерних знаків у русі (наприклад, точки входу/виходу, пропускні пункти), оскільки розмиття руху знищить доказову цінність запису.

Отже, Sense-Up/DSS є потужним інструментом для підвищення чутливості камери в умовах сутінків або мінімального освітлення. Однак його використання – це завжди компроміс між яскравістю (чутливістю) та чіткістю рухомих об'єктів (розмиттям). Успішне проектування вимагає балансу між цими двома факторами.

Роздільна здатність. Роздільна здатність відеозображення – це кількість пікселів, з яких складається кадр відео, що визначає його чіткість та якість (див. табл. 2.3). Вона вимірюється як добуток ширини на висоту в пікселях (наприклад, 1920x1080). Вища роздільна здатність означає більше пікселів, що призводить до детальнішого та чіткішого зображення.

Роздільну здатність в старих аналогових камерах вказують в ТВЛ (телевізійних лініях), або за назвою стандарту (формату) відеозображення.

Існує зв'язок між роздільною здатністю та форматами відеозображення. Він полягає в тому, що формати визначають стандартизовану роздільну здатність, яка впливає на якість, деталізацію та чіткість зображення. Чим вища роздільна здатність у форматі, тим більше деталей може відображати зображення, але це також вимагає більших обчислювальних ресурсів для обробки та зберігання.

Стандарти форматів зображення. Сфера відеоспостереження (CCTV) оперує багатьма стандартами, які визначають, як відеозображення захоплюється, передається, обробляється та зберігається. Ці стандарти можна умовно розділити на ті, що стосуються технології передачі/сигналу (аналогові, цифрові), роздільної здатності (якість зображення) та стиснення (ефективність зберігання та передачі).

Таблиця 2.3 – Роздільні здатності типових відеокамер

Тип камери	Загальна кількість пікселів, $n_м$ шт	Кількість пікселів за висотою, $n_в$ шт	Кількість пікселів за шириною, $n_ш$ шт
HD 720	921.600	720	1280
1.3 MPix	1.310.720	1024	1280
HD 1080	2.073.600	1080	1920
2 MPix	1.920.000	1200	1600
3 MPix	3.145.728	1536	2048
5 MPix	4.915.200	1920	2560

Початкові аналогові системи використовували стандарти CVBS (Composite Video Baseband Signal) із застарілою роздільною здатністю, яка обмежувалась телевізійними нормами PAL (576 ліній) або NTSC (480 ліній).

Зовсім недавно здавалося, що аналогові камери остаточно відійдуть у минуле і повсюдно будуть замінені на IP-відеокамери, які дають зображення з

високою роздільною здатністю, хорошою чіткістю і деталізацією. Така ситуація склалася через те, що до недавнього часу навіть найкращі аналогові камери не могли запропонувати картинку більшу за 960H (стандарт з роздільною здатністю 960x480 або 700 ТВЛ, що відповідає приблизно 0,7 Мп). Старі ж камери з роздільною здатністю CIF і D1 давали ще менше (рис. 2.11).

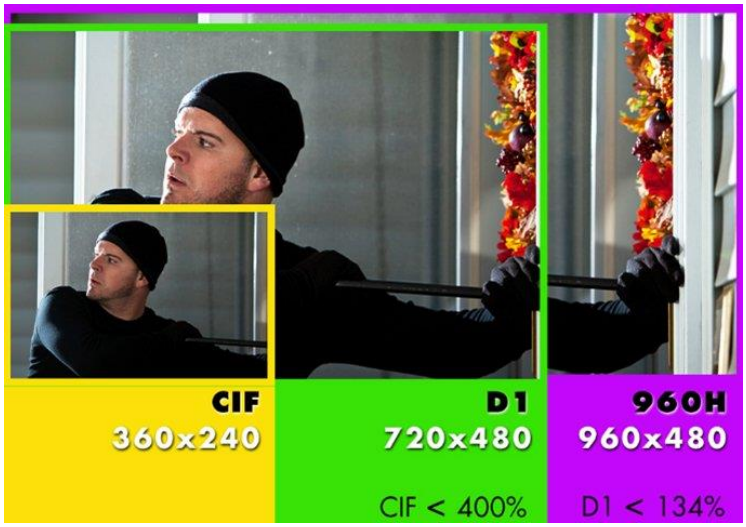


Рисунок 2.11 – Порівняння роздільної здатності різних форматів

У той же час IP-відеокамери стандартно пропонували зображення HD і Full HD якості з роздільною здатністю, відповідно, 720p (1280x720) і 1080p (1920x1080) (зараз на ринку присутні камери з роздільною здатністю більше 10 Мп) (рис.2.12).

Рисунок 2.12 – Порівняння розміру картинок різних форматів

В аналоговому відеоспостереження стався прорив, коли одночасно з'явилося декілька його нових стандартів (AHD, HD-TVI, HD-CVI), які практично зрівнялися з цифровим, завдяки можливості отримувати відео високої якості при порівняно низькій вартості обладнання.

Усі аналогові камери умовно поділяють на: камери застарілих стандартів (960H та меншої роздільної здатності), камери нових стандартів з високою роздільною здатністю картинки (HD-CVI, HD-TVI, AHD, MHD та інші).

Коротко розглянемо аналогові камери з низькою роздільною здатністю і докладніше зупинимося на нових стандартах.

Камери стандартів CIF, VGA, D1 і 960H називають просто аналоговими або камерами CVBS. Їх основні особливості – низька роздільна здатність відео і невелика відстань, на яку його можна передати (рис. 2.13).

Рисунок 2.13 – Кадр сцени з: а – камери CVBS; б – камери AHD

В іншому вони майже нічим не відрізняються від моделей з підтримкою нових стандартів: для передачі сигналу використовується коаксіальний кабель (або вита пара + конвертери сигналу), для запису відео використовується відеореєстратор DVR або гібридний - з підтримкою стандарту камери.

Роздільну здатність в старих аналогових камерах вказують в ТВЛ (телевізійних лініях), або за назвою стандарту (формату) відеозображення.

Роздільна здатність для різних форматів відео подано на рисунку 2.14.

До аналогових камер застарілих стандартів, які ще можна зустріти, відносяться:

– камери VGA - 640x480 пікселів (приблизно 380 ТВЛ);

– камери D1 - 720x480 пікселів (приблизно 420 ТВЛ);

–камери 960H - 960x582 пікселів (приблизно 700 ТВЛ) та інші.

Аналогові камери нових стандартів (AHD, HD-TVI, HD-CVI тощо). Завдяки використанню сучасних технологій камери нових стандартів істотно відрізняються за якістю картинки і деякими іншими показниками від старих. Такі відеокамери також називають HD-аналоговими камерами.

AHD (Analog High Definition) – аналогове відеоспостереження високої чіткості. AHD камери підтримують передачу сигналу як за коаксіальним кабелям, так і по витій парі. Від IP відеоспостереження цю технологію вигідно відрізняє дальність передачі відеосигналу – до 500 метрів без додаткових проміжних пристроїв. Крім того, цей стандарт повністю відкритий для всіх виробників, що саме собою знімає питання сумісності обладнання.

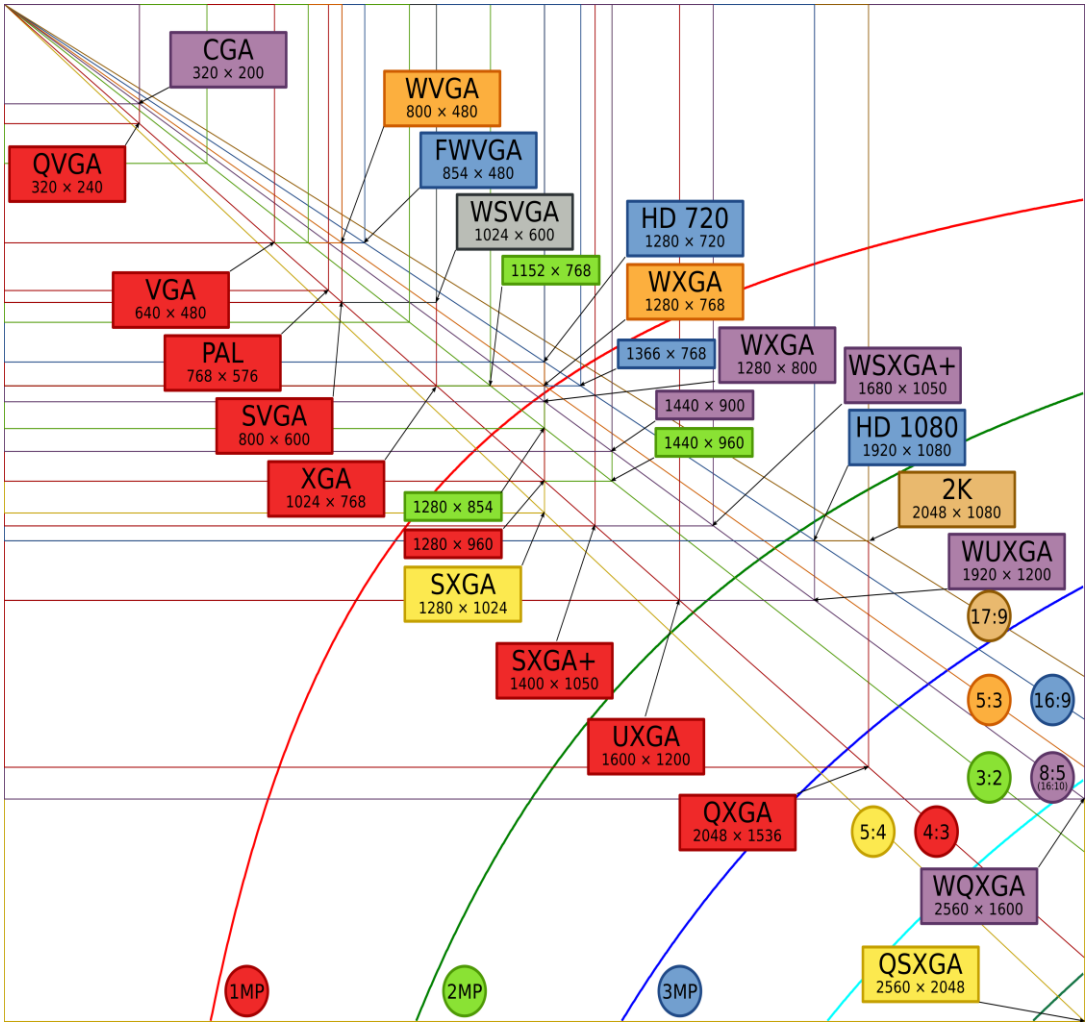


Рисунок 2.14 – Існуючі формати зображення

AHD камери дають зображення високої чіткості з роздільною здатністю 720p, 960p і 1080p. Вони можуть передавати 3 типу сигналу: відео, звук і управління. Відеопотік передається без затримок в реальному часі відеосигналу кабелем на відстань до 500 метрів без істотного загасання сигналу. Передача відеосигналу AHD можлива і за витою парою, але з використанням спеціальних приймально-передавальних пристроїв. У цьому випадку дальність передачі знижується до 150-200 метрів.

Технологія HD-TVI (торгова марка Hikvision). За якісним коаксіальним кабелем вона дозволяє передати сигнал на відстань до 500 метрів, причому комутаційні вироби (роз'єми тощо) можуть мати середню якість. На апаратному рівні HD-TVI відеоспостереження підтримує звичайні аналогові камери.

Особливості HD-TVI камер:

– відео високої чіткості з роздільною здатністю 720p і 1080p;

– передача 3-х типів сигналу: відео, звук і управління;

– відео без затримок, в реальному часі;

– сумісні з реєстраторами інших торгових марок, які використовують цю ж технологію.

Технологія HD-CVI (торгова марка Dahua). Даний стандарт має ряд функцій автоматичної корекції відеосигналу, що дозволяє значно зменшити його спотворення при використанні довгих ліній зв'язку. Крім того, однієї лінії досить для одночасної передачі відео і аудіосигналу, а також команд управління поворотними пристроями і трансфокаторами (PTZ).

Камери HD-CVI за характеристиками майже не відрізняються від камер HD-TVI і AHD:

– передають сигнал на відстань до 500 метрів за коаксіальним кабелем;

– передають всі 3 типи сигналу в одному кабелі;

– відео йде без затримок; картинка високої якості від 720p і вище.

Передача сигналу можлива і за витою парою до 150-200 метрів, з використанням конвертерів. Однак, камери та реєстратори HD-CVI сумісні тільки з обладнанням цього ж виробника, або тих, хто має ліцензію на використання цієї технології.

Отже, всі ці три технології практично нічим не відрізняються одна від одної, а просто реалізуються в пристроях різних компаній.

Вбудована інфрачервона підсвітка. Вбудована інфрачервона (ІЧ) підсвітка у відеокамерах є ключовою функцією, що дозволяє камерам здійснювати якісне відеоспостереження в умовах слабкого освітлення або повної темряви.

В основі роботи ІЧ-підсвітки лежить використання невидимого для людського ока світлового спектра. Відеокамера, як і будь-який оптичний пристрій, потребує світла для формування зображення, але коли видимого освітлення недостатньо, в гру вступає інфрачервоний діапазон, який знаходиться за межами червоного кольору. Камера оснащена кільцем інфрачервоних світлодіодів (LED), розташованих навколо об'єктива. Ці діоди випромінюють світло з довжиною хвилі, найчастіше близько 850 нанометрів.

Секрет успіху полягає у двох елементах. По-перше, світло цих діодів є непомітним для людини, що дозволяє камері вести спостереження приховано. По-друге, сенсор камери (CMOS або CCD), на відміну від людського ока, чутливий до цього ІЧ-світла.

Основну роль у переході до нічного режиму відіграє інфрачервоний відсікаючий фільтр (IR Cut Filter). Вдень цей фільтр розміщений перед сенсором, щоб блокувати ІЧ-світло і запобігти спотворенню кольорів (адже надлишок інфрачервоного світла змушує білі об'єкти виглядати рожевими).

Коли рівень навколишнього освітлення падає до критичної позначки, камера автоматично вмикає ІЧ-світлодіоди, а фільтр механічно відсувається. У цей момент камера переходить у монохроматичний (чорно-білий) режим. Чорно-біле зображення краще, оскільки кожен піксель сенсора використовується для захоплення ІЧ-світла, а не для фільтрації кольорів, що максимізує чутливість і забезпечує чіткість зображення в темряві.

Виробники пропонують два основні варіанти підсвітки, які впливають на скритність:

– 850 нм (це найбільш поширений і потужний тип. Він дає кращу дальність і яскравість нічного бачення, але при цьому інколи можна побачити слабке червоне світіння від самих діодів, що може демаскувати камеру);

– 940 нм (цей тип забезпечує повну невидимість підсвітки, що ідеально для прихованого спостереження. Однак, за фізичними законами, таке світло гірше відбивається, тому його ефективна дальність менша).

Інфрачервоний фільтр IGR (режим день/ніч). Інфрачервоний відсікаючий фільтр (ICR) – це механічний пристрій, який розташовується між об’єктивом та світлочутливим сенсором камери і виконує дві діаметрально протилежні функції в залежності від часу доби.

У денний час, коли освітлення є достатнім, людське око та сенсор камери сприймають видимий спектр світла. Однак сонячне світло також містить велику кількість інфрачервоного (ІЧ) світла.

У режимі «День» фільтр активний і знаходиться перед сенсором. Фільтр блокує (відсікає) ІЧ-світло, пропускаючи лише видимий спектр. Це запобігає спотворенню кольорів. Без цього фільтра всі зображення мали б рожево-фіолетовий відтінок, оскільки сенсор «бачить» більше ІЧ-світла, ніж людина рис. 2.15).ї

Рисунок 2.15 – Пояснення до впливу ІЧ фільтра на створення зображення

У нічний час або при слабкому освітленні, камера переходить у режим нічного бачення, використовуючи власну інфрачервону підсвітку. Фільтр механічно відсувається. Це дозволяє ІЧ-світлу від вбудованих діодів безперешкодно потрапляти на сенсор. Камера переходить у монохроматичний (чорно-білий) режим. Чорно-біле зображення є більш чутливим до ІЧ-світла, що дозволяє отримувати чітке зображення навіть у повній темряві.

Чутливість (світлочутливість, мінімальне освітлення). Чутливість – це ключова технічна характеристика відеокамер, яка визначає їхню здатність формувати якісне зображення в умовах низької освітленості. Цей параметр важливий для систем відеоспостереження, особливо для забезпечення ефективної роботи вночі або в погано освітлених приміщеннях.

Чутливість відеокамери або мінімальне освітлення – це найменший рівень освітленості об’єкта, при якому камера може видати зображення з допустимим рівнем шуму та достатньою якістю для ідентифікації об'єктів/подій. Вона

зазвичай виражається у одиницях освітленості – люксах (Лк). Чим нижче це значення (чим більше нулів після коми), тим краще камера «бачить» у темряві.

Для розуміння умов спостереження, за яких допустимий рівень освітлення забезпечить достатню якість зображення, представимо потрібні значення у люксах (табл. 2.4).

Таблиця 2.4 – Значення освітленості за відповідних умов

Умова освітлення	Приблизне значення (Лк)
Сонячний день	50 000-100 000
Похмурий день (вулиця)	10 000
Денне офісне освітлення	300-500
Вуличне освітлення (ніч)	1-10
Повний місяць	0,1
Безмісячна зоряна ніч	0,001
Камера високої чутливості (наприклад, ColorVu)	до 0,0005

Мінімальне освітлення залежить не лише від матриці, але й від інших елементів камери. Загалом чинники, що впливатимуть на чутливість відеокамери наступні: світлочутливість матриці, світлосила об’єктива, цифрова обробка (DSP) та наявність ІЧ-підсвічування.

Світлочутливість матриці характеризує фізичну здатність світлочутливого елемента (пікселя) вловлювати світло. Вона є ключовою характеристикою об’єктива, яка визначає його здатність пропускати світло на світлочутливу матрицю камери і характеризує ступінь ослаблення світлового потоку оптичною системою.

Світлосила найчастіше виражається через максимальне відносне отвір об’єктива, яке позначається як діафрагмове число або F-число (наприклад, f/1.4, F2.8, 1:4). Чим менше це число (наприклад, f/1.4 порівняно з f/4), тим вищою є світлосила об’єктива. Об’єктиви з великою світлосилою (наприклад, f/1.2, f/1.4, f/2.8) називають світлосильними.

Діафрагмове число F є обернено пропорційним світлосилі та розраховується як відношення фокусної відстані f об'єктива до ефективного діаметра його вхідної зіниці: F = D/f (де D – діаметр максимально відкритої діафрагми).

Світлосила впливає на тривалість витримки, глибину різкого зображення та характеризує якість об’єктива. Чим більше світла потрапляє на матрицю, тим коротша витримка потрібна для отримання правильної яскравості кадру, що важливо при зйомці в умовах поганого освітлення, тим менша глибина різкого зображення і краща оптика.

При виборі відеокамери для спостереження, особливо вночі або в темних приміщеннях, показник мінімальної освітленості є особливо важливим. Так,

камера з чутливістю 0,1 Лк забезпечить придатне зображення при повному місяці, а камера з чутливістю 0,001 Лк дозволить «бачити» у майже повній темряві, як під безмісячним зоряним небом без використання ІЧ-підсвічування.

Якість відеосигналу (відношення сигнал/шум). Кожна відеокамера на своєму виході формує відеосигнал, якість якого характеризується параметром – відношення сигнал/шум. Відношення сигнал/шум (Signal-to-Noise Ratio (SNR)) – це відношення максимального рівня сигналу до рівня шуму матриці та інших електронних компонентів відеокамери виражене в децибелах. Іншими словами – показує, наскільки корисний сигнал (інформація про зображення) переважає фоновий шум (небажані перешкоди).

Співвідношення сигнал/шум у децибелах (дБ) обчислюється за формулою, що використовує логарифм відношення потужностей:

$$SNR_{\text{дБ}} = 10 \cdot \log_{10}\left(\frac{P_{\text{сигналу}}}{P_{\text{шуму}}}\right). \tag{2.8}$$

Або, якщо використовувати амплітуди напруги, так як потужність пропорційна квадрату напруги, то:

$$SNR_{\text{дБ}} = 20 \cdot \log_{10}\left(\frac{U_{\text{сигналу}}}{U_{\text{шуму}}}\right). \tag{2.9}$$

Чим більше значення цього параметра тим менше проявляється шум на зображенні. Так, наприклад, відеокамера з параметром с/ш 52 дБ дає на зображенні менше шумів, ніж камера, що має с/ш 48 дБ.

Шуми проявляються на відеозображенні сцени в темних її ділянках в результаті поганого освітлення і виглядають як кольоровий чи чорно-білий «сніг» або зернистість.

Якість відеосигналу камери напряму залежить від розміру її матриці – чим менший формат матриці тим вищій рівень шумів, а отже – нижча чутливість.

На рисунку 2.16 продемонстровано зміну якості зображення за різного відношення сигнал/шум. З наведеного прикладу видно, що досить непогана якість картинки отримується вже при 30 Дб, але в сучасних камерах для отримання якісного відео S/N повинно бути не нижче 40 Дб (табл 2.5).

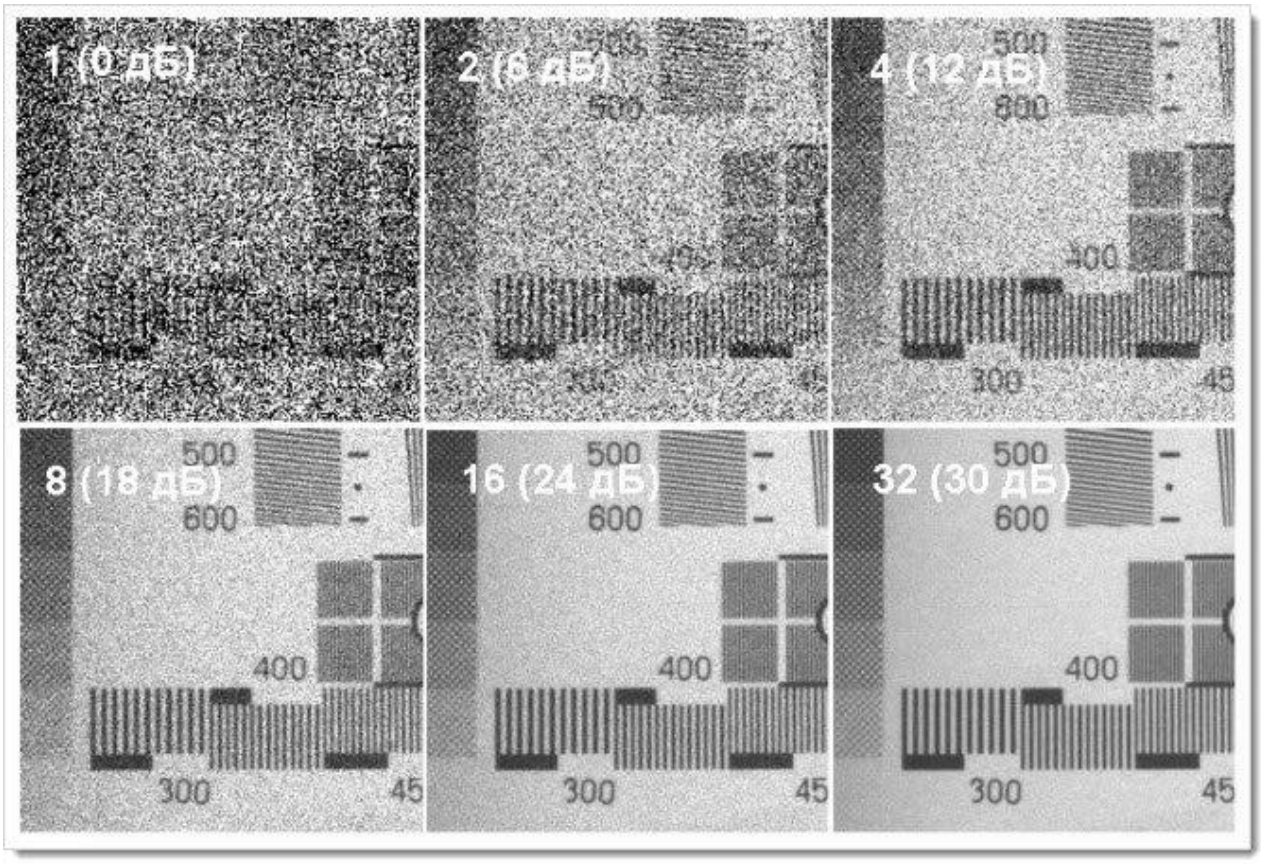


Рисунок 2.16 – Якість зображення при різних відношеннях сигнал/шум

Таблиця 2.5 – Градація якості відео

Значення С/Ш	Якість зображення (типово)
< 30 дБ	Погано (сильний, помітний «сніг» або зернистість)
40 дБ	Добре (шум присутній, але не сильно заважає)
> 45 дБ	Дуже добре (шум практично непомітний для людського ока)
50-60 дБ	Відмінна якість, характерна для професійного студійного обладнання

Шум у відеокамері, який виглядає як кольорова чи чорно-біла зернистість, може виникати з кількох джерел: тепловий шум, шум підсилення та дробовий шум.

Тепловий шум генерується електронними компонентами матриці та підсилювачів, особливо при високій температурі або тривалій експозиції.

Шум підсилення виникає, коли камера автоматично підвищує коефіцієнт підсилення відеосигналу для роботи в умовах низької освітленості. Підсилюється як корисний сигнал, так і шум.

У свою чергу, дробовий шум виникає через випадковий характер надходження фотонів світла на сенсор, помітний при дуже низькому освітленні.

За рекомендаціями CCIR (The International Radio Consultative Committee), існує п’ять градацій якості відеосигналу в залежності від відношення сигнал/шум, які подано в таблиці 2.6 та 2.7.

Таблиця 2.6 – Градація якості відео за CCIR (шкала погіршення)

Оцінка	Значення	Опис
5	Непомітне	Дефекти не помітні (якість ідеальна)
4	Помітне, але не дратівливе	Дефект можна побачити, але він не заважає перегляду
3	Трохи дратівливе	Дефект помітний і трохи відволікає
2	Дратівливе	Дефект значно погіршує враження від перегляду
1	Дуже дратівливе	Дефект робить зображення непридатним для перегляду

Таблиця 2.7 – Градація якості відео за CCIR (шкала якості)

Оцінка	Значення	Опис
5	Відмінна	Найвища можлива якість (без помітних дефектів)
4	Добра	Якість зображення висока, дефекти ледь помітні
3	Задовільна	Якість прийнятна, дефекти помітні, але не критичні
2	Погана	Якість низька, суттєво помітні дефекти
1	Дуже погана	Якість неприйнятна, зображення майже нерозбірливе

Існує й інший спосіб визначення якості сигналу – шкала IRE (Institute of Radio Engineers). У цьому випадку повний відеосигнал (1 вольт – повний розмах відеосигнал, 0,7 вольта без синхросуміші) приймається за 100 одиниць IRE. Допустимим вважається сигнал близько 30 IRE. Деякі виробники, наприклад BURLE, допустимим вважають сигнал 25 IRE, інші – 50 IRE.

На практиці більшість виробників використовують градацію якості відео за рекомендаціями CCIR.

Технології подавлення шумів DNR (3D-DNR, 2D-DNR). Цифрове шумозаглушення (DNR, Digital Noise Reduction) є важливою технологією в сучасних системах відеоспостереження, спрямованою на покращення якості зображення та оптимізацію використання системних ресурсів (рис. 2.17). Шум, по суті, є небажаними артефактами або статичним втручанням у відеосигнал, які неминуче виникають у процесі електронної комунікації та підсилення.

Рисунок 2.17– Зображення сцени без (ліворуч) і з DNR (праворуч)

Візуально шум проявляється у вигляді різних артефактів, що погіршують чіткість запису, включаючи зернистість, плямистості, туман та прозорі колірні блоки. Ці дефекти значно ускладнюють ідентифікацію об’єктів та знижують ефективність аналітичних функцій.

Слід зазначити, що у міру розвитку технологій відображення та підвищення роздільної здатності (наприклад, UHD 4K та 8K CCTV), проблема цифрового шуму стає ще більш актуальною. Більші роздільні здатності вимагають більших сенсорів або більшої кількості пікселів на одиницю площі, що може вимагати більше світла або більшого посилення, а сам шум стає більш очевидним на великому екрані. Отже, DNR, особливо вдосконалені версії, є не просто додатковою функцією, а необхідним компонентом для забезпечення кришталево чистого зображення у високій роздільній здатності.

Технології цифрового шумозаглушення поділяються на два основні класи, які визначають, як алгоритм аналізує та фільтрує небажані артефакти.

Просторова фільтрація (2D-DNR) – це метод, який використовує виключно інформацію з поточного кадру для зменшення присутнього шуму. Алгоритм аналізує сусідні пікселі (в межах однієї площини зображення) і застосовує фільтри для вирівнювання або згладжування зернистих областей. Мета полягає у виявленні та згладжуванні гранулярних зон, намагаючись зберегти якомога більше оригінальних деталей. Просторова редукція є ефективним методом для усунення статичного шуму, але її використання є обмеженим у динамічних сценаріях.

Часова фільтрація – це метод, який порівнює поточний кадр із попередніми кадрами у послідовності. Принцип роботи полягає у виявленні

«дивних» пікселів або артефактів, які не з’являються послідовно від кадру до кадру, та ідентифікації їх як шуму. Наприклад, якщо певний піксель випадково яскравий в одному кадрі, але має нормальну інтенсивність у наступному, він, ймовірно, є шумом. Цей метод дозволяє досягти значно більшого зниження шуму порівняно з просторовою фільтрацією, оскільки він використовує більшу кількість даних (багато кадрів) для визначення статичних та динамічних компонентів сцени.

Перевага використання DNR полягає не тільки у підвищенні якості зображення, але й у значному збереженні пропускної здатності та зниженні розміру відеофайлів. Це досягається завдяки тому, що шум є високочастотною, хаотичною інформацією, яку відеокодеки (наприклад, H.264 або H.265) змушені кодувати. Усунення цього шуму дозволяє кодеку працювати значно ефективніше.

Технологія 2D-DNR, також відома як DNR 2, є базовою формою цифрового шумозаглушення, яка історично була розроблена для роботи з посиленими зображеннями в умовах низької освітленості.

Основний механізм 2D-DNR полягає у покадровому аналізі зображення. Алгоритм використовує фільтри для ідентифікації та корекції «поганих» пікселів, аналізуючи їх відносно сусідніх пікселів в межах того самого кадру. Це ефективно усуває такі візуальні порушення, як дробовий шум та варіації інтенсивності світла

2D-DNR демонструє високу ефективність при очищенні статичних (нерухомих) частин кадру. Наприклад, при перегляді нічного відеоспостереження, область, найближча до камери, може виглядати чіткою завдяки 2D-DNR.

Ця технологія зазвичай реалізується в бюджетних камерах або в системах, які використовують камери низької роздільної здатності. Простота її алгоритму забезпечує менше обчислювальне навантаження.

Незважаючи на переваги в очищенні статичного фону, 2D-DNR має суттєві недоліки, які обмежують його застосування у професійних системах, особливо при необхідності захоплення динамічних сцен.

Головне обмеження 2D-DNR полягає у його схильності до створення артефактів руху. Оскільки технологія використовує просту часову редукцію, порівнюючи кадри послідовно, вона недостатньо точно розрізняє справжній рух об’єкта від випадкового шуму. Коли алгоритм намагається агресивно знизити шум у рухомій області, він помилково застосовує фільтрацію до самого рухомого об’єкта, що призводить до розмивання зображення або залишення шлейфів. Це робить ідентифікацію рухомих об’єктів ускладненою або неможливою.

Практика показує, що 2D-DNR працює найкраще на передньому плані, але області, віддалені від камери, часто залишаються «шумовими». Це означає, що ефективна дистанція, на якій можлива надійна ідентифікація об’єктів у темний час доби, значно зменшується. Інженери, які проектують системи безпеки, повинні усвідомлювати, що вибір камери лише з 2D-DNR не дозволить

досягти необхідної якості зображення для розпізнавання об’єктів на великих відстанях в умовах недостатньої освітленості.

Ці недоліки підкреслюють, чому чиста 2D-DNR система не вважається достатньою для сучасних вимог відеоспостереження, особливо там, де важливе захоплення динамічних подій з високою чіткістю.

3D-DNR (тривимірне шумозаглушення) є більш технологічним та ефективним рішенням, яке класифікується як просторово-часова фільтрація. Ця технологія розроблена спеціально для зйомки вночі або в тьмяно освітлених місцях, де шум, спричинений темновим струмом і посиленням, є найбільш критичним.

Принцип роботи 3D-DNR полягає у двовимірному підході.

Просторовий аналіз діє подібно до 2D-DNR, алгоритм аналізує пікселі в межах поточного кадру, ідентифікуючи локалізований шум та зернистість.

При часовому аналізі, на відміну від 2D-DNR, 3D-DNR порівнює поточний кадр із даними, отриманими з кількох попередніх або послідовних кадрів. Це дозволяє значно знизити рівень шуму до мінімуму, ефективно відрізняючи статичний шум від справжнього візуального сигналу.

Завдяки додатковому аналізу у часовій осі, 3D-DNR не лише зменшує шум, але й здатен відновлювати інформацію, втрачену через його наявність. Це призводить до значно чистішого та чіткішого зображення, яке краще зберігає деталі.

Головна перевага 3D-DNR над 2D-DNR, що вирішує проблему артефактів руху, полягає у використанні інтелектуального модуля компенсації руху. Успішність 3D-DNR повністю залежить від цього модуля, який використовує алгоритми для аналізу руху між вхідним відео та попередніми кадрами, розраховуючи ймовірність того, чи є зміна пікселів шумом чи реальним рухом.

Залежно від результатів аналізу руху, 3D-DNR динамічно застосовує різні рівні фільтрації до різних зон кадру.

Якщо рух не виявлено, 3D-DNR застосовує агресивне часове згладжування, щоб максимально видалити шум та відновити деталі. Якщо ж рух виявлено, система або застосовує менш агресивний часовий фільтр, або переходить до використання 2D-DNR, яка обробляє лише поточний кадр.

Ця динамічна адаптація гарантує, що 3D-DNR є набагато кращим вибором для відео з великою кількістю руху. Він ефективно зменшує зернистість без створення розмиття руху або шлейфів, які були типовою проблемою 2D-DNR.

Ефективність модуля компенсації руху є прямим індикатором потужності та якості вбудованого процесора обробки зображення (ISP/DSP). Якщо алгоритми оцінки руху не є досконалими або апаратне забезпечення недостатньо потужне, 3D-DNR може дати збій: помилково застосувати фільтрацію до рухомої області, викликавши артефакти післязображення. Таким чином, наявність 3D-DNR у технічній специфікації камери свідчить про використання високоякісного, потужного DSP/ISP, здатного до складної

обробки зображень у реальному часі. Це є вирішальним фактором при виборі обладнання для професійних систем.

Окрім усунення шуму та збереження чіткості руху, 3D-DNR виконує додаткові функції, що підвищують загальну якість відеосигналу.

Технологія компенсує спотворення зображення, спричинені помилками змішування кольорів, які є поширеними у режимах низької освітленості. Це досягається шляхом екстраполяції та видалення навіть найдрібніших дефектних пікселів. В результаті, 3D-DNR забезпечує кращу кольорову відтворюваність та більш точне зображення при складному освітленні.

Крім того, 3D-DNR необхідний для роботи з великими, високо роздільними відеопотоками, такими як 4MP і вище. Оскільки шум більш помітний при більших роздільних здатностях, 3D-DNR забезпечує додаткову потужність і функціональність, необхідну для отримання чистих записів, зберігаючи деталі, які могли б бути втрачені при використанні менш складних 2D-фільтрів.

Вибір між технологіями 2D-DNR та 3D-DNR повинен ґрунтуватися на ретельному аналізі вимог до сцени, наявності руху та необхідної якості ідентифікації. 3D-DNR є значно більш потужним і гнучким рішенням, що вимагає, однак, більш продуктивного апаратного забезпечення.

Вибір між технологіями 2D-DNR та 3D-DNR повинен ґрунтуватися на ретельному аналізі вимог до сцени, наявності руху та необхідної якості ідентифікації (табл. 2.8). 3D-DNR є значно більш потужним і гнучким рішенням, що вимагає, однак, більш продуктивного апаратного забезпечення.

Операційна цінність технологій DNR виходить за рамки простого покращення якості зображення; вона має прямий фінансовий вплив на загальну вартість володіння системою.

Таблиця 2.8 – Порівняльний аналіз архітектур 2D-DNR та 3D-DNR

Параметр	2D-DNR (Spatial/Temporal)	3D-DNR (Spatio-Temporal)
Механізм фільтрації	Аналіз у межах поточного кадру та/або проста послідовність	Аналіз у межах кадру + порівняння кількох послідовних кадрів
Ключова перевага	Ефективне очищення статичних областей	Висока ефективність при низькій освітленості та русі
Ефективність при русі	Слабкість; схильність до Motion Blur та шлейфів	Висока; використовує модуль компенсації руху
Оптимізація для сцени	Статичні сцени, низька роздільна здатність	Динамічні сцени, висока роздільна здатність (4K/8K)
Обчислювальне навантаження	Нижче; бюджетна реалізація	Вище; вимагає потужного DSP/ISP

Найбільш значуща економічна перевага DNR полягає в його здатності знижувати вимоги до пропускної здатності та сховища. Цифровий шум є хаотичною інформацією, яку кодеки стиснення (наприклад, H.265) намагаються зберегти. Усунення цього шуму за допомогою DNR значно підвищує ефективність алгоритмів стиснення, оскільки залишається лише корисна інформація. Це веде до різкого зниження бітрейту. Зменшення бітрейту, своєю

чергою, мінімізує необхідний обсяг дискового простору для зберігання архіву, що є прямою економією на NVR/DVR та хмарних сервісах.

В умовах низької освітленості шум може викликати хаотичні коливання яскравості пікселів. Системи виявлення руху (Video Motion Detection) можуть помилково інтерпретувати ці шумовий «мерехтіння» як справжній рух. Якісне шумозаглушення, особливо 3D-DNR, фільтрує ці шумове тло, значно знижуючи кількість хибних спрацьовувань (false alarms). Це підвищує надійність системи та зменшує операційне навантаження на персонал, який повинен перевіряти хибні сповіщення.

Слід зазначити, що хоча 3D-DNR забезпечує вищу якість, його розширений алгоритм (порівняння кадрів у часі) вимагає значно більшої обчислювальної потужності DSP. Для здійснення порівняння та компенсації руху потрібна буферизація та зберігання даних попередніх кадрів. Це неминуче призводить до більшого навантаження на процесор та потенційно може збільшити затримку відеопотоку. У більшості стандартних систем відеоспостереження ця затримка є незначною, проте у критично важливих системах, де необхідний мінімальний час відгуку (наприклад, для керування PTZ-камерами в реальному часі), інженери повинні враховувати, що використання найбільш агресивних налаштувань 3D-DNR є компромісом між максимальною якістю зображення та мінімальною латенцією.

Сучасні та висококласні камери відеоспостереження відходять від використання 2D-DNR або 3D-DNR як єдиного рішення, натомість інтегруючи їх у єдиний динамічний, або гібридний (Motion-Adaptive), алгоритм. Цей підхід дозволяє оптимізувати обробку, застосовуючи найбільш підходящий метод до кожної області кадру.

У гібридній системі функції розподіляються наступним чином:

– 2D-DNR, як менш ресурсоємний, застосовується для ефективного декодування та очищення статичних частин сцени (наприклад, стін, фонових об’єктів). Це дозволяє зберігати обчислювальну потужність;

– 3D-DNR застосовується виключно до зон кадру, де модуль компенсації руху виявив активність. Це гарантує, що рухомі об’єкти будуть захоплені з максимальною чіткістю, без розмиття руху, одночасно зменшуючи шум у цій динамічній зоні.

Результатом цього динамічного поєднання є створення надчистого та деталізованого зображення при низькій освітленості, яке є одночасно чітким, ясним та динамічним, що критично важливо для ефективного відеоспостереження.

DNR не працює ізольовано, а є частиною комплексного стека обробки зображення. Його ефективність має бути інтегрована з іншими технологіями для забезпечення оптимальної якості відео такими як WDR/HDR та іншими.

При проектуванні систем відеоспостереження, технічні спеціалісти повинні керуватися наступними принципами вибору технології шумозаглушення.

У зонах, де необхідна висока точність ідентифікації об’єктів (в’їзди, точки контролю доступу, громадські місця), і де присутній значний рух, обов’язковим є використання 3D-DNR або гібридних рішень. Ці системи мають пріоритет над системами з низьким рівнем шуму та високою чіткістю руху.

2D-DNR може бути достатнім для внутрішніх, добре освітлених зон або у випадках, коли використовуються низькороздільні камери, а виявлення руху не є важливим або відбувається лише на передньому плані.

Оскільки якість 3D-DNR є прямим відображенням потужності процесора, що відповідає за обробку зображення, інженерам рекомендується звертати увагу на моделі камер, які поєднують 3D-DNR з іншими передовими функціями (наприклад, WDR, HLC), оскільки це свідчить про наявність комплексного та потужного стека обробки зображення.

Частота кадрів. Частота кадрів, або FPS (Frames Per Second), є ключовим показником продуктивності, що використовується для вимірювання швидкості, з якою вихідний пристрій, зазвичай графічний процесор, генерує повні, зображення за одну секунду. FPS є прямим індикатором можливостей джерела графічного потоку. Чим вищий FPS, тим більше візуальної інформації доступно системі відображення за одиницю часу. Частота кадрів за секунду часто виражається в Герцах (1 Гц = 1 кадр/с).

Однак для глибокого аналізу та суб’єктивного сприйняття плавності руху більш релевантним показником є кадровий час (Frametime). Frametime вимірюється в мілісекундах (мс) і являє собою час, необхідний для генерації та рендерингу лише одного кадру. Frametime є обернено пропорційним FPS; це відношення описується формулою Frametime = 1000/FPS. Наприклад, при 60 FPS кадровий час становить приблизно 16.67 мс, а при 144 FPS – приблизно 6.94 мс. Експертний аналіз показує, що саме стабільність Frametime, а не лише високий середній FPS, є визначальною умовою для забезпечення плавної взаємодії користувача з візуальним контентом.

Хоча одиниці FPS та Герц (Hz) технічно еквівалентні (1 FPS = 1 Hz), вони описують різні фізичні процеси та ролі в конвеєрі відображення. Герц використовується для вимірювання частоти оновлення монітора, що вказує, скільки разів за секунду екран оновлює зображення. Незалежно від того, чи графічна карта генерує 10 FPS чи 200 FPS, монітор із частотою 60 Гц оновлюватиме свій екран 60 разів на секунду.

Історично склалися три основні стандартні частоти кадрів, які домінують у телебаченні та цифровому кіно: 24p, 25p і 30p. Ці стандарти відображають компроміс між необхідністю плавного руху та технічними обмеженнями обладнання.

У кінематографі 24 FPS (24p) став універсальним стандартом для звукового кіно. Це мінімальна частота, яка була достатньою для якісної синхронізації зі звуковою доріжкою та, що важливіше, для маскування мерехтіння. Проекційні системи зазвичай використовували механічний затвор, який показував кожен кадр двічі або тричі, доводячи ефективну частоту до 48 Гц або 72 Гц. Це перевищувало критичну частоту злиття мерехтінь для

центрального зору, створюючи ілюзію безперервного світла. Натомість, німе кіно часто використовувало значно нижчі частоти (16-18 FPS), які забезпечували лише мінімальну ілюзію руху, але призводили до помітного мерехтіння.

Цифрові стандарти 25p та 30p, поширені в телевізійному мовленні, часто є технічним артефактом, який походить від частоти електромереж: 50 Гц у Європі (що призвело до 25p/50i PAL) та 60 Гц у Північній Америці (що призвело до 30p/60i NTSC). Це демонструє, що не фізіологічні чи художні, а чисто інженерні та економічні чинники визначили глобальні стандарти відео.

При запису відеоінформації на відеореєстраторах або серверах, частоту кадрів можна змінювати в широких межах (від 1 до 30 к/с).

Для аналогових і HD-SDI відеокамер це можна робити тільки через OSD меню камери.

Для IP камер змінити частоту кадрів можна безпосередньо в меню камери, використовуючи браузер.

Зниження частоти кадрів при записі істотно знижує відео потік, що економить ресурс жорсткого диска і збільшує можливість тривалості запису. Разом з тим зниження частоти кадрів унеможливлює переглянути рух об’єкта у всіх його фазах.

Припустимо, що перша камера знімає людину, що біжить з частотою 25 к/с, а друга 3 к/с. У чому ми побачимо різницю на отриманому зображенні? Різниця тільки в тому, що перша камера збереже за 1 секунду 25 положень бігуна, а друга тільки 3. Причому до різкості зображення частота кадрів, не має ніякого відношення.

Якщо у камери затвор стояв в положенні 1/50 секунди, то кожен кадр з 25 або 3 буде змазаний однаково, а величина цього буде, визначається тільки швидкістю бігуна.

Коли потрібно зробити так, щоб кожен кадр з 25 або 3 був різким, і змазування зображення відсутнє, всього лише доведеться змінити значення затвора (витримки) у відеокамери.

Значення електронного затвора доцільно встановити в діапазоні 1/100-1/250 секунди і більше в залежності від сцени, що знімається.

Бітрейт. Бітрейт (Bitrate) є поняттям у цифровій інженерії, що визначає швидкість проходження оцифрованої мінімальної одиниці інформації, відомої як біт (двійковий код), за один часовий проміжок, зазвичай за 1 секунду. У спрощеному розумінні, бітрейт є швидкістю потоку проходження бітів або швидкістю передачі інформації через конкретний канал.

Цей показник використовується для ефективного вимірювання швидкості виконання передачі так званих «корисних» даних. У контексті цифрової інформації необхідно розрізняти два поняття: корисна інформація, яка містить лише безпосередньо збережені дані, та повна інформація, що є симбіозом корисної та службової інформації, необхідної для її зберігання або передачі.

Ефективність сучасних систем компресії полягає саме у мінімізації службової інформації та максимізації щільності корисних даних.

Бітрейт має подвійне інженерне значення. З одного боку, він слугує пропускною характеристикою конкретного пристрою або каналу, визначаючи його максимальний розмір. З іншого боку, він є величиною, що характеризує сам потік інформації, який передається за певний часовий відрізок, встановлюючи мінімальний розмір, необхідний для його відтворення.

Для стандартизованого вимірювання бітрейту використовуються одиниці кілобіти за секунду (kbps) та мегабіти за секунду (Mbps).

Важливе значення в інженерних розрахунках має строге розмежування між бітами (b) та Байтами (B). Усі стандарти бітрейту для потокового передавання даних та кодування медіа зазвичай вимірюються в бітах (Mb/s або kb/s). Необхідно суворо дотримуватися використання великої та малої літери (Mb/s проти MB/s), оскільки плутанина призводить до помилок у розрахунках пропускної здатності, враховуючи, що 1 MB/s (Мегабайт за секунду) дорівнює 8 Mb/s (Мегабітів за секунду).

Типові діапазони бітрейтів суттєво варіюються залежно від застосування. Наприклад, у системах відеоспостереження амплітуда бітрейту може бути досить широкою – від 8 до 320 кбіт/с, причому для сцен, багатих на швидко змінні зображення, необхідний більший показник, тоді як для статичних зображень достатньо і невеликого бітрейту.

Основними типами швидкості передачі даних є: постійний бітрейт (CBR) і змінний бітрейт (VBR). При відеозапису різноманітних сценаріїв, бітрейт істотно впливає на якість отриманого в результаті відеофайлу. Зйомка динамічних сцен, постійного потоку людей або автомобілів і насичених кольорів істотно відрізняється від зйомки квартири або порожнього офісного коридору.

Для динамічних сценаріїв потрібна велика пропускна здатність і бітрейт, а для менш динамічних – малий бітрейт. Практично всі сучасні відеореєстратори і IP-камери підтримують функцію вибору бітрейта – постійного чи змінного під час запису відео.

При постійному бітрейті, фіксована швидкість кодування використовується протягом усього треку або відеофайлу. При постійній швидкості, якість зображення може мати відчутні відмінності на статичних і динамічних ділянках відеозапису, так як динамічні сцени вимагають більшої пропускної здатності передачі даних.

За постійного бітрейта потрібно обирати малу швидкість кодування на об’єктах відеоспостереження зі статичним сценарієм (передпокої, коридори, задні двори, стіни, спальні) і велику швидкість на динамічних об'єктах (вулиці, транспорт, кпп і т. п.).

Так як відеозапис ведеться з постійною швидкістю, при цьому варіанті передачі даних легше передбачити кінцевий розмір файлу, а значить, планування зберігання записаної відеоінформації простіше контролювати: обсяг даних ніколи не змінюється. Існує і недолік: мінімальний бітрейт дуже сильно впливає на якість відеозображення в гіршу сторону.

Змінний бітрейт відрізняє автоматична змінна швидкість передачі даних. Наприклад, на відрізку відеозапису зі статичної сценою – швидкість передачі автоматично знижується, а на динамічних ділянках зі складними умовами, відповідно, зростає.

При цьому варіанті швидкості кодування, потрібна висока пропускна здатність передачі даних.

Безсумнівно, при змінному бітрейті якість записаного відеофайлу значно перевершує якість постійного бітрейта, вона стабільна, проте відеозапис займає незрівнянно більший і непередбачуваний обсяг, в результаті чого планування зі зберігання відеоматеріалу практично не піддається контролю.

Кожен кадр має певний об'єм, який залежить від роздільної здатності камери, глибини кольору. Перш ніж визначити потрібний об'єм архіву потрібно встановити величини бітрейта наявних відеокамер.

Розмір нестислого кадру $v_к$ визначається як:

$$v_к = n_ш n_в n_б, \tag{2.10}$$

де $n_в$ – кількість пікселів за висотою матриці, шт;

$n_ш$ – кількість пікселів за шириною матриці, шт;

$n_б$ – кількість біт, які кодують колір точки (глибина кольору).

Наприклад, для відеокамер з роздільною здатністю 1024x768 загальна кількість пікселів 786432 шт.

Для кодування чорно-білого зображення використовується 1 біт (2^1=2 кольори), для 16 кольорів – 4 біт (2^4=16 кольорів), для 256 кольорів – 8 біт (2^8 =256), для 16 мільйонів кольорів – 24 біта (2^8=256 різних варіантів представлення кольору для кожного каналу (256×256×256=16777216 кольорів, або 2^{24}=16777216 кольорів).

Сучасні IP-відеокамери відображають зображення з глибиною 24 біта.

Отже, розмір нестислого кадра 786432x24=18874368 біта, або 18874368/8=2359296 байт, або 2359296/1024=2304 Кбайт.

Щоб передати цей один кадр за секунду без стиснення потрібен потік, швидкість якого 2304x1x8=18432 Кбіт/с, або 18432/1024=18 Мбіт/с. Ця величина дуже велика і щоб зменшити її використовують кодеки – програми стиснення (кодування) інформації.

Розмір стисненого кадру і відповідно бітрейт залежить від типу кодека і рівня компресії.

Бітрейт і-ї камери визначається як:

$$b_i = \frac{8 n_к v_к}{k_{ст} x 1024}, \text{ (Мбіт/с)} \tag{2.11}$$

де $v_к$ – розмір нестисненого кадру, Кбайт; $n_к$ – кількість кадрів за одиницю часу, шт; $k_{ст}$ – коефіцієнт, який враховує ступінь стиснення кадру кодеком.

Бітрейт камер зазначається в їх технічній документації.

Технології компенсації засвічування (HLC, BLC, WDR, DWDR). Застосування в відеокамерах високошвидкісних процесорів дозволило реалізувати нові можливості, що значно поліпшують характеристики зображення і дозволяють вирішувати абсолютно нове коло завдань.

Поширеними проблемами відеоспостереження є:

– окремі яскраві об’єкти, що потрапляють в кадр (фари, лампи, ліхтарі), які засвічують частину зображення, і через які неможливо розглянути важливі деталі;

– занадто яскраве освітлення на задньому плані (сонячна вулиця за скляними дверима приміщення або за вікном тощо), на тлі якого ближні об'єкти відображаються занадто темними.

Для їх вирішення існує кілька функцій (технологій), що застосовуються в камерах спостереження.

Динамічний діапазон є фундаментальним викликом у сфері відеоспостереження, який визначає співвідношення між найбільш яскравою та найтемнішою ділянкою, яку сенсор може одночасно зафіксувати в одному кадрі. У реальних умовах спостереження, особливо на вхідних зонах, де відбувається перехід між яскравим сонячним світлом ззовні та тьмяним внутрішнім освітленням, різниця в освітленні може бути надто сильною для стандартного обладнання.

Проблема полягає в тому, що звичайні камери, зіткнувшись із високим контрастом, схильні вибирати середню експозицію. Це призводить до того, що деталі у світлих ділянках стають «перетриманими» або засвіченими, тоді як деталі у тіньових ділянках залишаються «недотриманими». В результаті, неможливо розглянути конкретні деталі на затемнених об’єктах. Це фізичне обмеження сенсора є причиною того, що технології, які справді вирішують цю проблему (як True WDR), вимагають спеціалізованого апаратного забезпечення, що прямо корелює з вищою вартістю кінцевого обладнання.

Технології компенсації та розширення динамічного діапазону можна чітко розділити за їхнім підходом до обробки даних, що визначає їхню ефективність і місце в ієрархії рішень для систем безпеки.

Існують коригувальні (компенсаційні) технології – BLC (Backlight Compensation) та HLC (Highlight Compensation). Вони є програмними рішеннями, що використовують цифрові сигнальні процесори для маніпуляції та регулювання освітлення на основі єдиної захопленої експозиції. Їхнє призначення – зробити цільовий об'єкт видимим шляхом внесення змін у вже існуючі дані.

На противагу їм існують розширювальні технології, представлені WDR (Wide Dynamic Range). True WDR ґрунтується на захопленні кількох експозицій, що є справжнім апаратним розширенням можливостей сенсора. Такий архітектурний підхід забезпечує чітку ієрархію ефективності: апаратне розширення (True WDR) забезпечує найвищу якість, оскільки збирає більше фундаментальних даних. Програмне розширення (DWDR) пропонує компроміс,

а компенсаційні методи (BLC/HLC) є найбільш вузькоспеціалізованими і менш універсальними.

BLC є технологією, призначеною для боротьби з ефектом заднього засвічування. Ця ситуація виникає, коли яскраве світло, що надходить із-за об'єкта (наприклад, через вікно або вхід), призводить до затемнення або появи силуетів об'єктів на передньому плані.

Механізм BLC реалізується через цифрові сигнальні процесори. Вони покращують експозицію всього зображення, поділяючи його на сегменти та регулюючи освітлення відповідно до потреб затемнених ділянок. Головна мета BLC – освітлення об'єктів на передньому плані, що робить їх більш деталізованими та природно освітленими. BLC ідеально підходить для приміщень з яскравим заднім підсвічуванням.

Ефективність використання режиму BLC показана на рисунку 2.18.

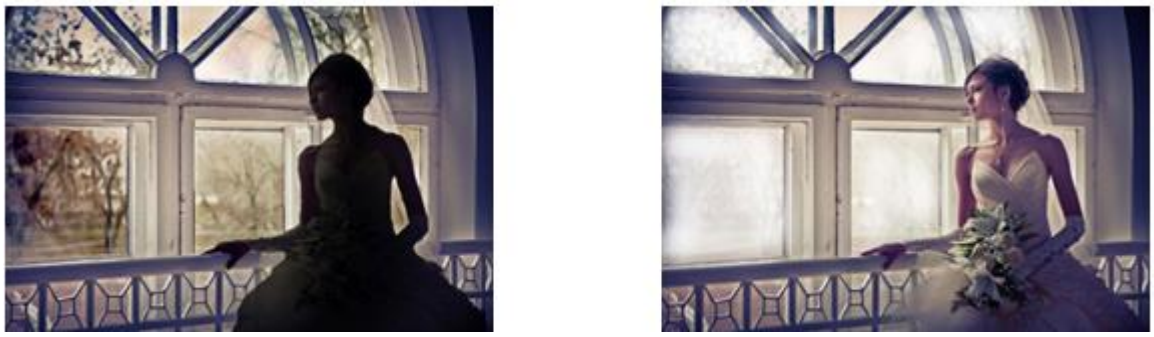


Рисунок 2.18 – Однаковий кадр отриманий без та з функцією BLC

Проте BLC є технологією компромісу. Вона працює, роблячи яскравішою всю сцену або цільові сегменти, замість того, щоб балансувати освітлення між контрастними ділянками, як це робить WDR. Головний недолік полягає в тому, що підвищення експозиції для освітлення переднього плану неминуче призводить до надмірного освітлення і втрати деталізації у вже яскравих зонах. В результаті світлі ділянки фону можуть стати «практично білими». BLC свідомо віддає перевагу деталям у критичній зоні (передній план), жертвуючи фоновою інформацією.

HLC (компенсація яскравого засвічування) – це спеціалізований DSP-алгоритм, призначений для боротьби з точковими, високоінтенсивними джерелами світла, такими як фари автомобілів або прожектори (рис. 2.19).

Рисунок 2.19 – Приклад застосування технології HLC

Технологія HLC працює шляхом автоматичного виявлення зон сильного засвічення та локального зменшення їхньої експозиції. Це ефективно мінімізує «сліпучий ефект», спричинений яскравими променями. Особливе застосування HLC знаходить у нічному спостереженні за транспортом. Завдяки приглушенню світла фар HLC дозволяє отримати необмежений огляд номерних знаків, що є ключовим для ідентифікації на паркувальних майданчиках та вулицях у нічний час. Таким чином, HLC перетворює проблему засвічування на можливість ідентифікації.

Важливо, що HLC фокусується виключно на боротьбі з яскравими джерелами світла і, на відміну від BLC, не покращує деталізацію затемненого переднього плану. Це підкреслює їхню функціональну спеціалізацію: BLC вирішує проблему темного об'єкта, HLC – проблему надмірно яскравого джерела.

True WDR є найбільш досконалою технологією для керування складними умовами освітлення. Це апаратне рішення, яке використовує спеціалізовані датчики та потужні процесори для захоплення більшого діапазону освітлення.

Принцип True WDR ґрунтується на захопленні кількох варіантів одного й того ж кадру з різними рівнями експозиції: один короткий кадр – для світлих ділянок, і один довгий кадр – для темних ділянок. Потім ці недотримані та перетримані зображення миттєво об'єднуються в єдиний, чіткий і збалансований кадр. Цей процес вимагає винятково швидкого та чутливого датчика.

True WDR забезпечує чудову якість зображення, одночасно зберігаючи деталізацію як у світлих, так і в тіньових областях. Камери, що використовують цю технологію, здатні досягати динамічного діапазону 120 дБ і більше. Цей високий показник дБ є ключовим індикатором справжнього, високопродуктивного WDR. Технологія є ідеальною для здійснення відеозапису в місцях, де контраст освітлення надто сильний, наприклад, на входах у магазини, в банках або на вітринах. На відміну від BLC/HLC, які коригують дані, True WDR фізично збирає більше фундаментальних даних, що гарантує максимальну цінність.

DWDR (Digital Wide Dynamic Range) – це програмна версія WDR. На відміну від апаратного WDR, DWDR не вимагає спеціалізованого апаратного забезпечення і не використовує багаторазову експозицію.

DWDR покладається на цифрову обробку сигналів і програмні алгоритми тонального відображення, щоб покращити якість зображення після його захоплення. Він програмно збільшує яскравість темних ділянок і зменшує яскравість світлих. Це робить його менш ефективним, ніж True WDR, оскільки він лише маніпулює існуючими даними.

Хоча DWDR покращує якість зображення порівняно зі стандартними камерами, його ефективність обмежена, особливо в умовах екстремального високого контрасту. Він не може відновити деталі, які були втрачені через фізичні обмеження сенсора при одній експозиції.

Ключова перевага DWDR – його економічна доступність. Оскільки він є програмним рішенням, він значно дешевше True WDR. Це робить його привабливим варіантом для бюджетних інсталяцій або зон із помірними проблемами освітлення. DWDR є більш енергоефективним порівняно з WDR, що потребує потужних процесорів. Однак інтегратори повинні бути обережними: використання терміну WDR без зазначення апаратної основи або дБ-рейтингу може приховувати той факт, що камера використовує лише програмний DWDR.

Розуміння того, як кожна технологія реалізується (апаратний чи програмний підхід), є ключем до вибору системи, що відповідає вимогам до якості та бюджету.

True WDR є найскладнішим і найдорожчим, оскільки вимагає спеціалізованого апаратного забезпечення для обробки та злиття кількох експозицій. З іншого боку, BLC та HLC, будучи програмними рішеннями, мають низьку вартість і мінімальні вимоги до обладнання. DWDR займає проміжне положення, пропонуючи програмне покращення, яке значно доступніше, ніж апаратний WDR. Ця різниця в реалізації безпосередньо впливає на максимальний динамічний діапазон, яким може керувати камера.

Збереження деталей в екстремальних умовах освітлення є найважливішим показником для систем безпеки.

WDR (True) є лідером за збереженням деталей, оскільки він ефективно керує високим контрастом, зберігаючи інформацію в тінях і світлах одночасно. Це важливо для ідентифікації. DWDR, хоча й покращує загальну картину, не може відновити деталі, які були втрачені сенсором під час захоплення, що обмежує його ефективність у крайніх умовах.

BLC покращує деталізацію темного переднього плану, але ціна цього – втрата деталізації в яскравому фоні через неминуче пересвітлення. З іншого боку, HLC має унікальну спеціалізацію: вона зберігає деталі, прилеглі до сліпучого точкового джерела світла, що є необхідним для фіксації номерних знаків, але не покращує деталізацію темного тла.

Вибір відповідної технології визначається пріоритетами і функціональними вимогами сцени спостереження (табл. 2.9).

Незважаючи на те, що WDR є найдосконалішим, технології BLC і HLC можуть бути використані в синергії або як самостійні рішення. Багато виробників, включаючи Dahua, Hikvision та Uniview, пропонують камери з комбінацією цих функцій, що забезпечує універсальність.

Якщо True WDR використовується як основний засіб балансування, компенсаційні функції можуть застосовуватися для тонкого налаштування. Наприклад, в умовах, де автомобільні фари створюють сильне засвічування, а об'єкти навколо є темними, може бути доцільним застосування WDR для загального балансу в поєднанні з HLC для чіткого захоплення номерних знаків. Критерій вибору залежить від того, яка частина кадру є важливою для інтегратора. Відеокамери з WDR та BLC здатні створювати якісне відео в будь-

яких умовах, але WDR забезпечує ширший діапазон і краще збереження деталей (рис. 2.20).

Для забезпечення максимальної якості відеоспостереження, інтегратори повинні керуватися принципом мінімізації навантаження на сенсор. Незважаючи на просування технологій WDR та компенсаційних функцій, не рекомендується направляти відеокамери спостереження прямо в бік джерел яскравого світла та поверхонь, що відбивають світло.

Таблиця 2.9 – Рекомендації до застосування технології компенсації в CCTV

Сценарій освітлення	Ключова проблема	Критична деталізація	Рекомендована технологія	Обґрунтування
Вхід у будівлю (день)	Сильний контраст світла/тіні	Обличчя, предмети, загальне тло	WDR (True)	Зберігає високу деталізацію в тінях і світлах
Приміщення з великим вікном	Заднє засвічування	Об’єкти на передньому плані	BLC	Освітлення затемнених фігур, ігнорування фону
Вуличне спостереження вночі	Яскраві фари автомобілів	Номерні знаки	HLC	Приглушує сліпуче світло для ідентифікації
Помірний контраст, бюджетний об’єкт	Дещо темні тіні	Загальна чіткість	DWDR	Доступне покращення з мінімальними апаратними витратами

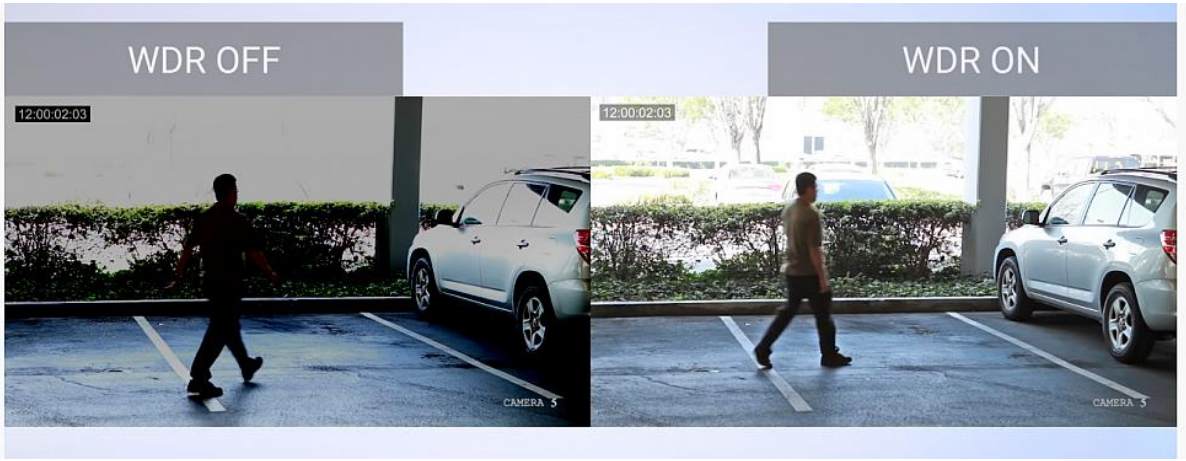


Рисунок 2.20 – Приклади відображення кадру в різних режимах

При виборі обладнання для контрастних умов слід завжди перевіряти технічні характеристики, зокрема заявлене значення динамічного діапазону в децибелах (дБ). Це єдиний надійний спосіб відрізнити True WDR від DWDR, забезпечуючи відповідність обраного обладнання очікуванням клієнта щодо якості зображення.

Системи стабілізації зображення. Стабілізація зображення (Image Stabilization, IS) є фундаментальною вимогою в сучасній практиці відеоспостереження. Основна функціональна задача IS полягає у мінімізації негативних наслідків так званої «камеральної тряски» – мимовільних рухів, які виникають при зйомці в динамічних умовах. Ці рухи знижують різкість та деталізацію зображення, особливо в умовах недостатнього освітлення, коли камера змушена використовувати довшу витримку. Якщо технології стабілізації не застосовуються, результат часто є розмитим та містить надмірний шум, що робить його непридатним для професійного використання.

Історично склалося, що системи стабілізації поділяються на дві основні категорії: апаратні (або оптико-механічні), які включають OIS та IBIS, та програмні (або цифрові), до яких належать EIS та AIS. Сучасні професійні робочі процеси розглядають якісну стабілізацію як необхідну передумову для успішного пост-продакшну. Кадр, захоплений із значною нестабільністю, ускладнює або унеможливлює точний кольоровий грейдинг, створення складних масок, а також трекінг об’єктів та рухів, що є стандартними операціями у відео обробці.

Апаратні методи є безвтратними, оскільки вони фізично коригують шлях світла або положення сенсора до того, як зображення буде зафіксовано. Це запобігає необхідності цифрового обрізання та інтерполяції, зберігаючи повну роздільну здатність кадру.

OIS (Optical Image Stabilization) реалізується безпосередньо в об’єктиві камери. Її механізм базується на використанні високоточних мікроприводів, які здатні переміщувати одну або кілька груп лінз у площині, перпендикулярній оптичній осі. Таке переміщення протидіє кутовим відхиленням камери, відомим як хитання та поворот.

OIS демонструє високу ефективність при роботі з телеоб’єктивами. Це обумовлено тим, що на довгих фокусних відстанях навіть мінімальний кутовий рух призводить до значного зсуву зображення на матриці. Основний недолік OIS полягає в тому, що ця технологія має бути інтегрована в кожен окремий об’єктив, що збільшує їхню вартість та складність конструкції.

IBIS (In-Body Image Stabilization) або стабілізація зсувом матриці (Sensor-Shift) є сучасною альтернативою, яка розміщена у корпусі камери. Вона працює за принципом компенсації руху шляхом фізичного переміщення самого сенсора зображення. Завдяки високоточним механізмам IBIS здатна компенсувати рухи по п’яти осях: хитання, поворот, обертання, а також горизонтальне та вертикальне зміщення.

Технічний аналіз показує, що IBIS забезпечує значно вищу частоту корекції, ніж традиційна OIS. Деякі системи, як зазначено, здатні коригувати

положення сенсора до 5000 разів на секунду, що є у п’ять разів вищим показником, ніж у типових OIS-систем. Це призводить до помітно кращої плавності відеоряду. Ключовою перевагою IBIS є її універсальність: система працює з будь-яким встановленим об'єктивом, включаючи оптику, яка не має вбудованої OIS.

При комбінуванні OIS на об’єктиві та IBIS на корпусі камери (гібридна апаратна стабілізація) досягається максимальна ефективність. Хоча загальновизнано, що жодна внутрішня система не може повністю замінити зовнішній фізичний гімбал для екстремальних сценаріїв, подвійна стабілізація є найкращим внутрішнім рішенням для досягнення стабільності.

EIS (Electronic Image Stabilization) є програмним методом, який працює після захоплення кадру. На відміну від OIS/IBIS, EIS є втратним, оскільки він покладається на цифрове маніпулювання та інтерполяцію.

Принцип дії EIS полягає у використанні даних з внутрішніх датчиків, таких як гіроскопи, для виявлення руху камери. Камера захоплює зображення з області сенсора, яка є більшою, ніж фінальний вихідний кадр. Коли виявляється тремтіння, EIS зміщує (рухає) область зйомки у межах більшої рамки, компенсуючи рух і зберігаючи центральну частину стабільною.

Цей процес вимагає обрізання країв кадру (так званого кропу), що неминуче призводить до звуження поля зору. Чим агресивніша стабілізація потрібна, тим сильнішим буде кроп. Це може призвести до помітного погіршення якості зображення та втрати деталізації, якщо обрізання надмірне або якщо вихідний матеріал мав недостатню роздільну здатність.

Сучасні відеокамери, призначені для динамічних сцен, широко використовують поєднання різних технологій.

HIS (Hybrid Image Stabilization) передбачає одночасне використання OIS (або IBIS) та EIS. Цей підхід використовує найкращі якості обох сторін: апаратна частина (OIS) відповідає за компенсацію більших, низькочастотних рухів, тоді як електронна частина (EIS) відповідає за точне налаштування та згладжування менших, високочастотних тремтінь, які OIS могла пропустити.

Ключова технічна перевага HIS полягає в оптимізації втрат EIS. Оскільки OIS бере на себе більшу частину роботи з компенсації, EIS не потребує застосування екстремального коефіцієнта обрізання (кропу). Це мінімізує вплив на фінальний кадр і його роздільну здатність, дозволяючи отримувати одні з найплавніших відео, доступних на мобільних платформах, і є особливо корисним при використанні цифрового зуму або зйомки в умовах недостатнього освітлення.

AIS (Artificial Intelligence Image Stabilization) є еволюцією EIS. Цей тип стабілізації інтегрує передові алгоритми машинного навчання для аналізу та прогнозування руху камери. Завдяки цій здатності до прогнозування, сучасні гібридні системи, що використовують AI-алгоритми, можуть досягати рівня плавності, який імітує зйомку на професійний зовнішній гімбал.

Хоча AIS функціонально належить до EIS, вона особливо ефективна у складних сценаріях. Завдяки інтелектуальній обробці та, ймовірно, складному

композитингу (поєднанню кількох кадрів), AIS забезпечує високу деталізацію та різкість в умовах, які раніше були недосяжні без штатива.

Класи захисту відеокамер ІК (антивандальні) та IP (від пилу і вологи). Системи відеоспостереження є важливими інструментами для забезпечення безпеки, контролю процесів та моніторингу різних об'єктів. Однак, надійність їх залежить не лише від якості відеофіксації та функціональних можливостей, але й від фізичної стійкості самого обладнання до зовнішніх загроз.

Аналіз загроз показує, що системи піддаються ризикам двох основних категорій: віддалені (кібератаки, злом, перехоплення трафіку, видалення даних) та фізичні атаки. Фізичні атаки, які включають навмисне пошкодження, вилучення накопичувачів або встановлення шкідливого програмного забезпечення, вимагають прямої взаємодії з обладнанням. Якщо пристрій встановлений на вулиці або у громадському місці, його корпус стає найслабшою ланкою, яка повинна протистояти як агресивному навколишньому середовищу (волога, пил, екстремальні температури), так і цілеспрямованому вандалізму.

Забезпечення належного рівня фізичного захисту є необхідною умовою для тривалого та безперебійного функціонування системи. Ігнорування вимог до захисту корпусу може призвести до непередбачених витрат на ремонт або повну заміну обладнання, що є особливо актуальним в умовах вуличної експлуатації.

Міжнародні стандарти, які класифікують стійкість корпусів електронних пристроїв, включають два ключові показники, які завжди слід розглядати в комплексі: IK (Impact Protection) та IP (Ingress Protection).

Стандарт IP (Ingress Protection, захист від проникнення), згідно з IEC 60529, визначає рівень захисту електричних пристроїв від проникнення твердих тіл, таких як пил, а також рідин, тобто вологи.

Стандарт IK (Impact Protection, захист від удару), згідно з IEC 62262, класифікує стійкість корпусу до механічних ударів, що є прямим індикатором його антивандальних властивостей.

Дані позначення відносяться не тільки до камер відеоспостереження, а й до будь-яких інших електронних пристроїв, які мають захисний корпус. Даними цифрами в основному маркуються камери, призначені для вуличного встановлення, оскільки саме в цьому випадку виникає потреба в захисному корпусі, який буде перешкоджати проникненню вологи і пилу.

Ці стандарти є синергетичними та взаємодоповнюючими. Високий рейтинг IK гарантує, що корпус витримає фізичний вплив, але якщо корпус не має достатнього IP-захисту, внутрішня електроніка може бути вразливою до вологи та пилу. Навпаки, якщо пристрій має високий IP, але низький IK, один сильний удар може порушити його герметичність, що, у свою чергу, призведе до проникнення вологи та швидкого виходу з ладу. Тому для зовнішніх або громадських об'єктів необхідно враховувати обидва показники.

Ступінь захисту IP, як правило, має 2 цифри, які позначають рівень захисту пристрою. IP рейтинг можна розглядати як точну класифікацію ступеня захисту камери відеоспостереження від проникнення твердих частинок і рідин, і зазвичай він має вигляд «IP66».

Перше число інформує про ступінь захисту (табл. 2.10), що забезпечується корпусом камери від проникнення твердих частинок, і може лежати в діапазоні від 0 (відсутність захисту) до 6 (найвищий рівень захисту).

Рівень IP6X є обов'язковим для будь-якого зовнішнього або промислового відеоспостереження, оскільки він забезпечує повний захист від пилу та дрібних твердих частинок, що запобігає пошкодженню чутливої оптики та електроніки.

Друге число надає інформацію про рівень захисту камери від води (табл. 2.11). Діапазон значень другого числа може варіюватися від 0 до 8.

Таблиця 2.10 – Ступені захисту від твердих тіл

Цифра (X1)	Опис захисту від твердих тіл
0	Не має захисту
1	Витримує тверді предмети понад 5 см, наприклад, рука
2	Витримує тверді предмети понад 1,2 см, наприклад, палець
3	Витримує тверді предмети більш як 0,25 см, наприклад викрутка
4	Витримує тверді предмети більш як 0,1 см, наприклад тонкий провід
5	Може обмежити проникнення твердого пилу без відкладень
6	Повністю захищена від проникнення пилу та відкладень

Таблиця 2.11 – Ступені захисту від вологи

Цифра (X1)	Опис захисту від твердих тіл
0	Не має захисту
2	Захист від вертикально крапельної води
3	Захист від розпорошення води з кутом до 15 градусів
4	Захист від розпорошення води з кутом до 60 градусів
5	Захист від розпилення води з усіх боків. Допустимо незначне проникнення
6	Слабкий струмінь води. Можливе несуттєве проникнення всередину
7	Захист від сильного струменя. Незначне проникнення води
8	Занурення у воду короткий час на глибину до 1 метра
9	Тривале занурення у воду під тиском

Для зовнішнього використання, згідно з рекомендаціями, зазвичай необхідні IP65, IP66 або IP67, оскільки ці рівні забезпечують високий ступінь захисту від пилу, дощу та сильних струменів води.

Враховуючи ці таблиці, можна створити наступну класифікацію для відеокамер:

– захист до IP44 – відеокамера з низьким рівнем захисту корпусу, яка не призначена для вуличного або зовнішнього встановлення і використовується виключно всередині приміщення, володіючи стабільним середовищем;

– захист від IP44 до IP65 – стійкі до атмосферних явищ камери, які без проблем можуть встановлюватися зовні приміщення, але потребують додаткового захисту. Зазвичай комплектуються кожухом чи встановлюються під спеціальним карнизом;

– захист від IP66 до IP67 – всепогодна відеокамера, яка має високий захист корпусу, тому без проблем може протистояти сильним вітрам та опадам. Може розміщуватись під захисним карнизом і без нього;

– захист IP68 – повний захист корпусу, тому може занурюватись у воду, але не рекомендується.

При виборі обладнання для зовнішнього моніторингу часто виникає питання про доцільність вибору між IP66 та IP67, оскільки обидва класи забезпечують повний пилозахист. Ключова відмінність полягає у вологозахисті: IP66 захищає від сильних струменів води, тоді як IP67 – від короткочасного занурення.

На перший погляд, IP67 здається завжди кращим. Однак, інженерний аналіз вимагає оцінки умов експлуатації. Якщо камера встановлена високо (наприклад, на фасаді будівлі або на стовпі), ризик повного занурення у воду дорівнює нулю. У таких випадках IP66 є абсолютно достатнім для протидії сильним атмосферним опадам. Перехід до IP67 стає критично важливим лише у зонах, де можливе накопичення води, затоплення або необхідність регулярного промивання обладнання зануренням. Таким чином, вибір між IP66 та IP67 повинен базуватися на аналізі висоти встановлення та ризику затоплення, а не лише на загальній вимозі «зовнішнє використання». Необґрунтоване завищення вимоги до IPX7 або IPX8 може необґрунтовано збільшити вартість проекту без додавання реальної експлуатаційної цінності в конкретному середовищі.

Клас IK є стандартом, який класифікує ступінь захисту корпусу від механічних ударів. Він визначає, наскільки пристрій стійкий до фізичного пошкодження, що вимірюється в джоулях (Дж). Основне призначення IK у відеоспостереженні – захист від вандалізму або випадкових сильних ударів (наприклад, у місцях з інтенсивним рухом або промислових об’єктах).

Оцінка ударостійкості проводиться шляхом контрольованого тестування. Тест на ударну оцінку IK враховує енергію удару в джоулях, масу ударного елемента (молотка), його радіус, матеріал, а також висоту вільного падіння (рис.2.21).

Рисунок 2.21 – Рівень захисту за IK-класифікацією

Визначити, наскільки міцним є захист для камери відеоспостереження, можна за параметром IK, який передбачає наступну класифікацію для електронних пристроїв:

– IK00 – захист відсутній (така відеокамера може розбитися від будь-якого удару);

– IK01-IK06 – витримує невеликі удари, сила яких не перевищує 1 Дж (максимум від випадкових впливів, без умисного пошкодження);

– IK07-IK08 – розраховані на більш сильні удари від 2 до 5 Дж (можуть експлуатуватися в умовах з більш високими ризиками);

– IK09-IK10 – максимально захищені, витримуючи силу до 10 та до 20 Дж відповідно (саме вони краще за інші варіанти здатні протистояти вандалізму).

Рівень IK08 зазвичай вважається достатнім для протистояння випадковим пошкодженням або легким актам вандалізму, які можуть статися у громадських місцях. Однак, IK10 є стандартом, який забезпечує опір цілеспрямованому та сильному удару, еквівалентному падінню 5 кг маси з висоти 400 мм.

Це вищий рівень захисту є обов’язковим для обладнання, фізична цілісність якого є важливою і де ціна відмови системи є надзвичайно високою. До таких об’єктів відносяться: промислові системи, обладнання міської інфраструктури, критичні точки контролю доступу. При проектуванні систем безпеки технічний спеціаліст повинен класифікувати об’єкт не просто за його розташуванням («вуличний»), а за ступенем підготовки потенційного зловмисника та стратегічною важливістю даних, що виправдовує перехід від IK08 до максимального IK10.

Конструктивні особливості корпусу мають прямий вплив на досягнення високого рейтингу IK. Антивандальні камери часто виконуються у купольній формі.

Круглі або купольні вольєри є оптимальними з погляду ударостійкості, оскільки вони ефективно розсіюють енергію удару на більшу площу. Якщо об’єкт потрапляє в круглий пристрій, енергія удару не концентрується в певній точці, а поширюється на оточення. На відміну від прямокутних корпусів, де

кути є найслабшими місцями, кругла форма забезпечує кращий захист. Таким чином, грамотне проектування геометрії є ключовим фактором для підвищення класу IK. Крім того, купольні моделі часто мають непрозорий корпус, що приховує напрямок зйомки, що слугує додатковим стримуючим фактором для зловмисників.

Рекомендації що до комбінації захисту IK та IP для відеокамер подано в таблиці 2.12.

Таблиця 2.12 – Рекомендовані комбінації захисту IK та IP для відеокамер

Середовище застосування	Ризик	Мінімальний IP-рейтинг (пил + вода)	Мінімальний IK-рейтинг (удар)	Рекомендована комбінація
Внутрішні офісні приміщення	Низький (від випадкового дотику)	IP20 (захист від об'єктів >12.5 мм, без вологозахисту)	IK03 (0.35 Дж)	IP20/IK03
Вуличне спостереження (низький ризик вандалізму)	Високий (атмосферні впливи)	IP65, IP66 або IP67 (пилонепроникний, стійкість до струменів/занурення)	IK07 (2 Дж)	IP66/IK07
Громадські місця (парки, школи, станції)	Високий (вандалізм, сильні атмосферні впливи)	IP66, IP67	IK08 (5 Дж)	IP67/IK08
Промислові об'єкти, міська інфраструктура, зони високого ризику	Максимальний (цілеспрямоване знищення, агресивне середовище)	IP67, IP68 (занурення, повний пилозахист)	IK10 (20 Дж)	IP68/IK10

Необхідно підкреслити, що справжній антивандальний захист для зовнішнього використання є трикомпонентною вимогою. Він охоплює не лише стійкість до ударів, а й герметичність та кліматичну стійкість, яка включає термозахист (встановлення кожуха для захисту від холоду або підвищених температур). Ігнорування кліматичної стійкості, навіть за наявності високих IK та IP, може призвести до швидкої поломки електроніки в умовах різких температурних коливань.

Функція Privacy Mask прихованих зон. Маскування приватності, відоме також як Video Masking або Image Masking, є важливою функцією, інтегрованою в сучасні IP-камери та системи управління відео (VMS). Її основне призначення полягає в обфускації – приховуванні, затемненні, розмитті або пікселізації – строго визначених, чутливих ділянок у полі зору камери (рис. 2.22). Цей механізм поважає приватні простори, які знаходяться поблизу областей, що виправдано перебувають під наглядом.

Маскування прихованих зон набуває першорядного значення у ситуаціях, коли електронний моніторинг є незаконним або неприйнятним, особливо там, де фізичні особи мають обґрунтоване очікування приватності. Приклади таких зон включають вікна приватних резиденцій, внутрішній простір сусідніх офісів або, в гіпотетичних випадках некоректної установки, навіть такі місця, як роздягальні чи ванні кімнати. Функція Privacy Mask гарантує, що, хоча навколишні території можуть ефективно моніторитися, ці чутливі простори уникають випадкового чи постійного спостереження, що дозволяє системі відеоспостереження функціонувати відповідно до принципів мінімізації даних.

Рисунок 2.22 – Приклад застосування Privacy Mask

Функціональність Privacy Mask можна класифікувати за двома основними критеріями: ступінь постійності та механізм застосування (статичний чи динамічний). Ці класифікації визначають, як система збалансовує конфіденційність та операційну необхідність моніторингу.

Постійні маски є базовим та найбільш радикальним інструментом мінімізації даних. Області, визначені як Permanent Privacy Mask, завжди залишаються закритими (замаскованими) у всіх клієнтських додатках VMS.

Цей тип маскування застосовується для зон, які не вимагають жодного спостереження, як приватні чи публічні простори, де стеження заборонене. Ключова перевага постійного маскування полягає у його інтеграції з аналітикою системи: рухома детекція (Motion Detection) автоматично виключається з областей, покритих постійними масками. Це є подвійною перевагою: це не лише технічно реалізує мінімізацію даних (оскільки рух у цій зоні не викликає запису), але й усуває проблему хибних спрацювань від нерелевантних об’єктів (наприклад, дерев, що хитаються на задньому плані).

На відміну від постійних масок, підйомні маски (Liftable Privacy Mask) призначені для областей, які є чутливими, але можуть вимагати розкриття у виняткових, надзвичайних ситуаціях (наприклад, розслідування інциденту чи загроз).

Функція підйомної маски перетворює технічне обмеження на елемент юридичного комплаєнсу та підзвітності. Розкриття області дозволено лише користувачам із спеціальними, заздалегідь визначеними правами доступу. Якщо користувач VMS, який увійшов у систему, не має необхідних дозволів, система вимагає авторизації та схвалення від уповноваженого користувача для тимчасового підйому маски.

Для забезпечення пропорційності, система дозволяє налаштувати тайм-аут для піднятих масок. Це гарантує, що після завершення необхідності тимчасового доступу, конфіденційність автоматично відновлюється. Такі механізми управління доступом, авторизації та автоматичного відновлення конфіденційності створюють необхідний аудиторський слід, що підтверджує, що дані були розкриті виключно на підставі принципу «необхідності доступу».

Найбільш прогресивним рішенням у сфері захисту приватності є динамічне маскування, яке використовує можливості штучного інтелекту та аналітики Edge. Прикладом такої технології є Axis Live Privacy Shield, яка здатна маскувати рухомі об’єкти (зокрема людей або номерні знаки) у відеопотоках із повною частотою кадрів у режимі поточного часу.

Механізм роботи динамічного маскування полягає у постійному порівнянні поточного зображення із заздалегідь встановленою фоновою сценою. Коли виявляється рух, технологія застосовує докладний, динамічний і прозорий фільтр до області зміни. Це дозволяє рухомим об’єктам виглядати прозорими або розмитими на тлі. Цей процес відбувається миттєво, ефективно усуваючи збір ідентифікаційних персональних даних.

Динамічне маскування є пропорційним рішенням, оскільки воно дозволяє операторам бачити рух, активність та ситуаційну обізнаність, що важливо для моніторингу процесів (наприклад, у логістиці чи виробництві), але запобігає ідентифікації окремих осіб.

Системи, що використовують динамічне маскування, можуть бути налаштовані для доставки окремого відеопотоку, де маскування не застосовується. Цей оригінальний потік доступний лише високоавторизованим особам у разі інциденту, що зберігає принцип цільового обмеження. Крім того, користувачі можуть виключати певні області з динамічного маскування (наприклад, конвеєрну стрічку), де спостереження за об’єктами є необхідним.

OSD меню відеокамер та її функції (DIS, AGC, AWB тощо). OSD (від англ. On-Screen Display) – це екранне меню, яке накладається поверх відеозображення на моніторі. Воно дозволяє адміністратору або користувачеві налаштовувати основні параметри зображення та функції відеокамери прямо через монітор спостереження або відеореєстратор (за допомогою коаксіального керування або джойстика на кабелі камери).

OSD-меню надає доступ до широкого спектру налаштувань, які оптимізують якість зображення та функціональність камери залежно від умов освітлення та конкретних вимог спостереження (табл. 2.13).

Таблиця 2.13 – Типові налаштування OSD-меню

Абревіатура	Повна назва (англ.)	Призначення
AGC	Automatic Gain Control	Автоматичне регулювання підсилення. Функція посилює слабкий відеосигнал за умов недостатнього освітлення (наприклад, вночі), щоб зробити зображення світлішим
AWB	Automatic White Balance	Автоматичний баланс білого. Забезпечує правильну передачу кольорів, автоматично налаштовуючи колірну температуру відповідно до поточного освітлення
DIS	Digital Image Stabilization	Цифрова стабілізація зображення. Функція зменшує розмиття та тремтіння зображення, спричинене вібрацією камери (наприклад, від вітру або механічних впливів)
DNR	Digital Noise Reduction	Цифрове зменшення шумів. Алгоритм обробки, який прибирає зернистість (шуми) на зображенні, особливо помітну за низького освітлення та при активній AGC. Існують версії 2D-DNR та більш просунута 3D-DNR
WDR/DWDR	Wide Dynamic Range	Широкий динамічний діапазон. Дозволяє камері одночасно відображати деталі як у дуже світлих, так і в дуже темних областях сцени, що критично важливо, наприклад, при зйомці проти світла
BLC/HLC	Back Light Compensation / High Light Compensation	Компенсація засвічення фону / Компенсація яскравого освітлення. BLC висвітлює об'єкт на передньому плані, коли за ним знаходиться яскраве джерело світла. HLC зменшує інтенсивність дуже яскравих точок
Shutter	Затвор (витримка)	Налаштування часу експозиції світлочутливого елемента. Впливає на чіткість рухомих об’єктів та загальну яскравість
Day/Night	Режим День/Ніч	Перемикання між кольоровим (день) та чорно-білим (ніч, з використанням ІЧ-фільтра) режимами
Privacy Mask	Маска приватності	Дозволяє приховати (затемнити) небажані для огляду зони кадру (наприклад, вікна сусідніх будинків)
Motion Det.	Детектор руху	Налаштування зони та чутливості виявлення руху

Доступ до OSD-меню найчастіше здійснюється одним із двох способів:

– через джойстик/кнопки (якщо камера має фізичний джойстик або кнопки на сигнальному кабелі або корпусі);

– через відеореєстратор (коаксіальне керування). У сучасних аналогових (HD-TVI, HD-CVI, AHD, CVBS) та деяких IP-камерах, OSD-меню можна

викликати та керувати ним за допомогою меню реєстратора через той самий коаксіальний кабель або мережевий протокол (функція PTZ або «коаксіальне керування»).

Бортові носії інформації. Бортові носії інформації – це пристрої для локального зберігання відеозаписів, які встановлюються безпосередньо в корпус відеокамери. Вони дозволяють камері працювати автономно (без постійного підключення до відеореєстратора чи хмарного сервісу) або слугують резервним сховищем.

Основним типом бортового носія для переважної більшості сучасних відеокамер є карта пам'яті (табл. 2.14).

Найпоширенішим форматом є microSD-карта. Вони використовуються в IP-камерах, Wi-Fi камерах та інших моделях, де потрібна компактність і локальна автономність.

Таблиця 2.14 – Характеристики карт пам'яті для відеоспостереження

Характеристика	Пояснення
Форм-фактор	MicroSD (найпоширеніший). За обсягом поділяються на: SDHC (до 32 ГБ) та SDXC (від 32 ГБ до 2 ТБ)
Клас швидкості	Вказує на мінімальну швидкість запису. Для Full HD і 4K камер потрібна висока швидкість. Звертайте увагу на: Class 10 або UHS Speed Class (U1/U3), а також Video Speed Class (V10, V30)
Спеціалізація	Рекомендується використовувати карти з позначенням «High Endurance» (висока витривалість). Вони розроблені спеціально для безперервного циклічного перезапису, що є типовим для відеоспостереження, і мають підвищений ресурс
Обсяг	Найпоширеніші обсяги: 64 ГБ, 128 ГБ, 256 ГБ. Обсяг впливає на глибину архіву (скільки днів запису зберігатиметься)

Камера записує на карту, коли спрацьовує детектор руху, або веде безперервний запис. Якщо з'єднання з мережею чи реєстратором втрачено, карта виступає як буфер.

Хоча карти пам'яті домінують, у деяких спеціалізованих або великогабаритних камерах можуть зустрічатися інші типи:

– вбудована eMMC/Flash-пам'ять. Невеликий обсяг вбудованої пам'яті (зазвичай 4-8 ГБ), інтегрованої в плату камери. Використовується для зберігання операційної системи, налаштувань та як буфер для критичних моментів, але не для тривалого архіву;

– вбудований SSD/HDD-накопичувач: використовується у деяких професійних або PTZ-камерах (поворотних), де потрібен дуже великий обсяг локального архіву. Це по суті мініатюрний відеореєстратор, інтегрований у корпус камери.

Контрольні питання:

1. Розкрийте фізичний принцип перетворення оптичного зображення в електричний сигнал у пікселі матриці.
2. Проаналізуйте порівняльні характеристики ПЗЗ (CCD) та КМОП (CMOS) матриць. Які фактори зумовили домінування КМОП-технології в сучасних системах?
3. У чому полягає технологічна перевага матриць PIXIM при спостереженні сцен з високим контрастом освітлення?
4. Поясніть походження терміна "відіконовий дюйм". Яка фізична діагональ матриці формату 1/2" у міліметрах?
5. Розрахуйте кількість пікселів за шириною та висотою для камери з загальною роздільною здатністю 1.3 Мп при форматі кадра 4:3.
6. Яка роль ICR-фільтра у відеокамерах "день/ніч" та як його відсутність впливає на спектральну чутливість системи?
7. Визначте взаємозв'язок між фокусною відстанню об'єктива та кутом огляду. Як розрахувати фокусну відстань для ідентифікації об’єкта на заданій відстані?
8. Порівняйте сферичну та асферичну оптику. Чому асферичні об'єктиви вважаються більш ефективними для систем нічного бачення?
9. Опишіть механічну сумісність стандартів C-mount та CS-mount. Які наслідки матиме встановлення CS-об'єктива на C-камеру
10. Як зміна освітленості протягом доби впливає на глибину різкості зображення в камерах з автоматичною діафрагмою?
11. У чому полягає принципова різниця між електронним та механічним затвором у відеокамерах?
12. Як швидкість електронного затвора (витримка) впливає на якість зображення рухомих об’єктів та яскравість кадру?
13. Яке призначення функції Sense-Up (DSS) і який її головний недолік при спостереженні за динамічними сценами?
14. Поясніть принцип роботи інфрачервоного відсікаючого фільтра (ICR) у режимах «день» та «ніч».
15. Що таке чутливість відеокамери, у яких одиницях вона вимірюється та від яких основних чинників залежить?
16. Порівняйте технології цифрового шумозаглушення 2D-DNR та 3D-DNR: у чому полягає їхня технологічна відмінність та переваги?
17. Яка різниця між апаратною технологією True WDR та програмною DWDR при роботі в умовах складного освітлення?
18. Для вирішення яких специфічних завдань використовуються функції BLC та HLC?
19. Охарактеризуйте класи захисту IP та IK: за що відповідає кожна цифра в їхньому маркуванні?

Література: **[1-3, 5].**

Тема 3. Аналогові та IP системи

План:

Формування відеосигналу в аналогових та IP камерах. AHD, CVI, TVI-технології. Типи компресії даних. Протоколи передачі даних у відеоспостереженні. Особливості підключення та вимоги до живлення відеокамер.

Формування відеосигналу в аналогових та IP камерах. Сучасна індустрія відеоспостереження переживає фундаментальну трансформацію, зумовлену конвергенцією оптичних технологій, напівпровідникової мікроелектроніки та передових методів цифрової обробки сигналів. Питання формування відеосигналу перестало бути тривіальною задачею перетворення світлового потоку в електричний імпульс; нині це складний, багатоступеневий процес, що охоплює квантову взаємодію фотонів з кремнієвою підкладкою, складні алгоритми інтерполяції кольору, математичне моделювання для компресії даних та інкапсуляцію в мережеві протоколи реального часу.

Всі відеокамери діляться на 2 великі групи: аналогові та цифрові. Основна їх відмінність полягає в способі обробки і передачі відеосигналу.

В основі будь-якої відеокамери, незалежно від її типу (аналогова чи IP), лежить фотоелектричний перетворювач – сенсор зображення. Його задача полягає в дискретизації оптичного зображення як у просторі (на пікселі), так і в амплітуді (на рівні заряду).

У CCD-сенсорах (Charge-Coupled Device) процес зчитування базується на послідовному переміщенні зарядових пакетів через структуру приладу до єдиного вихідного вузла. Тут механізм перенесення заряду полягає у застосуванні системи MOS-конденсаторів. Подаючи послідовність тактових імпульсів на електроди, потенціальні ями зміщуються, перетягуючи електрони до виходу. Ефективність перенесення заряду у сучасних CCD перевищує 99.999%, що є важливим для збереження цілісності сигналу у великих масивах.

Найпоширенішою в відеоспостереженні є архітектура Interline Transfer (IT-CCD). У ній кожен стовпець фотодіодів має сусідній вертикальний регістр зсуву, захищений від світла металевою маскою. Це дозволяє реалізувати глобальний електронний затвор: заряд миттєво переноситься в захищену зону, а потім повільно зчитується, поки фотодіоди накопичують наступний кадр.

Перетворення заряду в напругу відбувається лише на виході сенсора в блоці зарядо-чутливого підсилювача. Оскільки всі пікселі проходять через один і той самий підсилювач, CCD-сенсори характеризуються високою однорідністю, але обмеженою швидкістю зчитування та високим енергоспоживанням через необхідність розгойдування ємнісних навантажень тактовими шинами.

У свою чергу технологія CMOS (Complementary Metal-Oxide Semiconductor) інтегрує активні елементи підсилення безпосередньо в кожному пікселі, що фундаментально змінює парадигму зчитування.

Сучасні CMOS-сенсори використовують архітектуру 4T (чотири транзистори на піксель). Вона включає: фотодіод (PD), транзистор передачі (дозволяє ізолювати фотодіод від вузла зчитування), транзистор скидання, витоковий повторювач (діє як буферний підсилювач) і транзистор вибору рядка.

CMOS-сенсори використовують стовпцево-паралельну архітектуру АЦП. Це означає, що тисячі АЦП працюють одночасно, що забезпечує надвисоку пропускну здатність, низьке енергоспоживання та можливість довільного доступу до частин сенсора.

В аналогових камерах сигнал після сенсора може проходити часткову цифрову обробку, але потім знову перетворюється в аналог. В IP-камерах сигнал залишається в цифровому домені.

Ключовим параметром є розрядність АЦП. Типові сенсори відеоспостереження використовують 10-бітні або 12-бітні АЦП.

Таким чином, в аналоговій камері зображення, сформоване на матриці CCD або CMOS, надходить в аналоговому вигляді до блоку обробки відеосигналу. Там воно обробляється та оцифровується, а для подальшої передачі знову перетворюється в аналоговий сигнал (його також називають композитним сигналом). За коаксіальним кабелем цей відеосигнал передається на монітор (якщо потрібно) і на відеореєстратор, який оцифровує, кодує і стискає його для запису.

У цифровій камері сигнал не перетворюється назад з цифрового формату в аналоговий для передачі, а відправляється на реєстратор саме в цифровому вигляді. При цьому перед передачею він може кодуватися і стискатися – так відбувається в IP-камерах, або ж передаватися без стикання і некодованим – так відбувається в HD-SDI камерах. Через суттєві відмінності IP і HD-SDI технологій відеоспостереження, хоча обидві вони і належать до цифрових, їх розносять в окремі типи. Для передачі сигналу з IP-камер використовуються мережеві кабелі (вита пара) або оптоволокно. Для передачі відеосигналу з HD-SDI камер використовується коаксіальний кабель або оптоволокно.

Таким чином, існує три типи відеокамер для спостереження, згідно з реалізованими в них технологій обробки і передачі сигналу:

– аналогові камери;

– IP-камери;

– HD-SDI камери.

Аналогові камери мають багато переваг:

– низька вартість;

– простота розгортання системи відеоспостереження з їх використанням;

– гарна якість зображення (у нових стандартів), в тому числі рухомих і віддалених об’єктів;

– стійкість до збоїв, властивим мережевих систем: хакерських і вірусних атак, втрати зв’язку;

– можливість розгортання і модернізація системи з використанням вже існуючої кабельної інфраструктури;

– відсутність втрат і затримок сигналу.

До їх недоліків можна віднести:

– погану масштабованість встановлених систем;

– незахищеність передачі сигналу;

– складність використання для передачі сигналу мережевої інфраструктури, це можливо тільки при оснащенні спеціальними перехідниками, які погіршують якість відео;

– необхідність прокладки додаткового кабелю живлення.

З вище викладеного можна побачити, що процеси формування відеосигналу демонструють фундаментальну дивергенцію технологій. Аналогові HD-системи досягли піку інженерної думки в області модуляції та аналогової схемотехніки, дозволивши передавати цифрову якість (4K) через застарілі фізичні середовища з нульовою затримкою. Вони залишаються ідеальним вибором для модернізації існуючих об’єктів та систем, де критична реакція в реальному часі.

Натомість IP-камери перетворилися на автономні комп’ютерні системи. Їх складність змістилася з фізичного рівня передачі сигналу на рівень обчислювальної обробки та мережевих протоколів. Формування сигналу тут – це не просто створення відеопотоку, а генерація структурованих даних, інтегрованих у глобальні інформаційні системи. Розуміння глибинних процесів є необхідним базисом для проектування надійних систем безпеки.

AHD, CVI, TVI-технології. Сучасна індустрія відеоспостереження у 2025-2026 роках перебуває на етапі глибокої трансформації, де традиційні аналогові рішення не лише зберігають свою актуальність, але й успішно конкурують із мережевими IP-системами в сегментах, де критичними є надійність, вартість та кібербезпека. Виникнення та розвиток стандартів передачі відео високої чіткості через коаксіальний кабель, таких як Analog High Definition (AHD), High Definition Composite Video Interface (HD-CVI) та High Definition Transport Video Interface (HD-TVI), дозволили індустрії подолати обмеження стандартної чіткості (CVBS), запропонувавши роздільну здатність до 4K (8 Мп) без необхідності повної заміни існуючої кабельної інфраструктури. Аналіз показує, що станом на 2026 рік аналогові системи все ще охоплюють від 40% до 50% глобальних інсталяцій, що підкреслює їхню ринкову живучість та адаптивність.

Розуміння походження кожної технології є ключовим для оцінки їхнього поточного стану та стратегій виробників. Кожен із трьох основних стандартів виник як відповідь на технологічний вакуум, що утворився між застарілим аналоговим відео та дорогим цифровим IP-спостереженням.

Технологія HD-CVI була офіційно представлена компанією Dahua Technology у 2012 році, ставши першим масовим рішенням для передачі сигналу 720p та 1080p через коаксіал після обмеженого успіху стандарту HD-SDI. Dahua обрала стратегію закритого, але ліцензованого стандарту, де компанія виступає єдиним розробником процесорів цифрової обробки сигналів

(DSP) та плат відеореєстраторів, що забезпечує жорстку стандартизацію та контроль якості в межах екосистеми CVI.

У відповідь на успіх Dahua, каліфорнійська компанія Techpoint Inc. у 2014 році випустила стандарт HD-TVI. На відміну від конкурента, Techpoint позиціонувала свій стандарт як відкриту платформу, що дозволило сотням виробників, включаючи такого гіганта як Hikvision, впроваджувати цю технологію у свої пристрої. Цей крок сприяв надзвичайно швидкому поширенню TVI та появі великої кількості сумісних компонентів від різних брендів, хоча й створив певні виклики у вигляді появи на ринку дешевих і менш надійних варіацій.

Стандарт AHD, розроблений південнокорейською корпорацією NextChip, спочатку орієнтувався на максимально бюджетний сегмент. Його головною перевагою стала зворотна сумісність з традиційними аналоговими системами 960H та CVBS на рівні сигналу, що зробило його найпростішим інструментом для поетапної модернізації старих об’єктів. Згодом, після прийняття стандарту брендом Hanwha Vision (Samsung), AHD набув легітимності в корпоративному та державному секторах, позбувшись репутації виключно «дешевого» рішення.

Фундаментальною відмінністю аналогових HD-технологій від IP-систем є метод обробки даних. В IP-камері відео стискається та кодується безпосередньо в пристрої, що перетворює її на автономний комп’ютер, тоді як камери HD-over-Coax передають нестиснений або мінімально оброблений сигнал на відеореєстратор (DVR), який виконує основну роботу з кодування та зберігання.

Технологія HD-TVI використовує специфічну схему модуляції, відому як Pulse-Amplitude Modulation with Level Shifting (PAM-LS), яка забезпечує передачу цифрових відеоданих високої чіткості через аналогове середовище коаксіального кабелю. Це дозволяє підтримувати стабільність сигналу та мінімізувати затримки. HD-CVI базується на квадратурній амплітудній модуляції, яка ефективно розділяє сигнали яскравості та кольоровості, усуваючи перехресні спотворення, що були головною проблемою старих телевізійних стандартів PAL та NTSC.

Однією з найбільш значущих інновацій у цих протоколах стала здатність передавати по одному кабелю не лише відео, а й аудіо, сигнали керування PTZ (Up-the-Coax або UTC) та навіть живлення (Power over Coax – PoC). Це значно спрощує монтаж, дозволяючи використовувати один кабель RG59 замість комбінованих рішень.

Сучасні системи AHD, CVI та TVI підтримують широкий спектр роздільних здатностей, що робить їх універсальними для різних сценаріїв. У 2026 році стандартом де-факто для нових інсталяцій стала роздільна здатність 4K (8 Мп), яка забезпечує чітке розпізнавання обличь на відстані до 10 метрів та детальне читання номерних знаків.

Незважаючи на високу роздільну здатність, аналогові системи часто мають обмеження щодо частоти кадрів у форматі 4K (зазвичай 7-15 FPS), що є компромісом між об’ємом даних та пропускною здатністю аналогового тракту.

Проте для більшості завдань безпеки, де важлива деталізація статичних або повільно рухомих об’єктів, такої частоти цілком достатньо.

Ефективність систем HD-over-Coax залежить від якості кабельної продукції та правильності підбору компонентів передачі. Основне середовище – коаксіальний кабель з хвильовим опором 75 Ом.

Традиційний кабель RG59, який десятиліттями був стандартом для аналогового CCTV, у 2026 році залишається придатним для модернізації систем 1080p, але має серйозні обмеження для 4K на великих дистанціях. Кабель RG6, завдяки більшому центральному провіднику та кращому екрануванню (фольга плюс обплетення), забезпечує менше загасання сигналу на високих частотах.

При передачі сигналу 4K частотний спектр розширюється, що призводить до зростання втрат. Наприклад, на частоті 50 МГц (типовій для аналогового HD) втрати в RG59 складають – 2.4 дБ на 100 футів, тоді як у RG6 – лише 1.7 дБ. Це безпосередньо впливає на максимальну довжину траси без спотворення кольорів або появи шумів.

Використання кабелів Cat5e або Cat6 разом із відеобалунами є популярною альтернативою, особливо в нових будівлях, де СКМ (структурована кабельна мережа) вже прокладена. Пасивні балуни дозволяють передавати сигнал на відстань до 300 метрів для 1080p, проте для 4K ця відстань скорочується до 100-150 метрів через високий рівень згасання та чутливість до наводок. Активні пристрої (підсилювачі) можуть розширити ці межі до 1200 метрів і більше, але це вимагає додаткового живлення та налаштування частотної компенсації (рівні Low, Medium, High).

Хоча на папері всі три стандарти забезпечують схожі характеристики, практичні тести виявляють тонкі відмінності в алгоритмах обробки зображення.

Аналіз відеопотоків у складних умовах освітлення показує, що системи HD-TVI від Hikvision часто мають перевагу в чіткості дрібних деталей та контрастності, що особливо помітно при роботі з ІЧ-підсвіткою. У свою чергу, AHD-камери демонструють більш точну передачу кольорів та менш агресивне цифрове придушення шумів, що робить картинку більш природною в денний час. Технологія HD-CVI від Dahua славиться своєю стабільністю на наддовгих дистанціях (до 1 км для 720p) та мінімальною кількістю артефактів при швидкому русі об’єктів у кадрі.

Оскільки сигнали HD-over-Coax передаються в аналоговій формі, вони залишаються вразливими до зовнішніх електромагнітних завад від силових ліній, ліфтових двигунів та радіовипромінювання. У середовищах з високим рівнем перешкод цифрові формати (наприклад, EX-SDI) показують ідеально чисту картинку до моменту повного зникнення сигналу, тоді як AHD, CVI та TVI починають демонструвати горизонтальні шуми або «змазування» зображення. TVI вважається найбільш захищеним серед аналогових стандартів завдяки використанню технології PAM-LS, яка має кращі властивості фільтрації шумів.

Одним із найсильніших аргументів на користь аналогових HD-технологій у 2026 році є їхня економічна ефективність. Згідно з дослідженнями

інсталяційних компаній, вартість обладнання для системи на 20 камер формату AHD/TVI становить приблизно $2,800, тоді як аналогічна IP-система з NVR та PoE-комутаторами обійдеться мінімум у $4,500.

Використання існуючих коаксіальних ліній при модернізації дозволяє досягти якості 4K, заощадивши до 70% бюджету на будівельних роботах та перепрокладці кабелю. Це робить аналогове HD пріоритетним вибором для великих об'єктів, де кабельну інфраструктуру фізично важко або дорого замінити (історичні будівлі, склади, великі промислові зони).

У 2026 році питання затримки сигналу та мережевої безпеки стали важливими для багатьох замовників.

IP-камери, незалежно від потужності процесора, мають затримку від 1000 до 3000 мілісекунд, що зумовлено часом на кодування відео в камері, передачу пакетів через мережу та декодування в реєстраторі або клієнтському ПЗ. В системах AHD, TVI та CVI передача сигналу відбувається миттєво, що є важливим для операторів, які керують PTZ-камерами в реальному часі або здійснюють моніторинг у казино та банках.

Щодо кібербезпеки, аналогові камери мають природну перевагу – вони не мають IP-адрес і не підключені безпосередньо до комп'ютерної мережі. Це створює так званий «повітряний зазор», що робить камеру неможливою ціллю для хакерських атак. Єдиним вразливим пристроєм у такій системі є відеореєстратор, захистити який значно простіше, ніж десятки окремих мережевих камер.

Протягом тривалого часу головним недоліком аналогових HD-систем була їхня закритість: камери Dahua не працювали з реєстраторами Hikvision і навпаки. Проте у 2025-2026 роках цей бар'єр практично зник завдяки появі гібридних відеореєстраторів, відомих як XVR або Pentabrid.

Сучасний Pentabrid DVR є універсальним хабом, який автоматично детектує та підтримує: AHD (відкритий стандарт NextChip), HD-TVI (від Hikvision/Techpoint), HD-CVI (від Dahua), CVBS (старий аналоговий сигнал), IP (мережа через ONVIF).

Це дозволяє інсталяторам комбінувати кращі камери різних брендів в одній системі, використовуючи, наприклад, 4K TVI камери для зовнішнього спостереження та бюджетні AHD для складських приміщень, записуючи все на один гібридний пристрій. Додатково, більшість сучасних камер тепер випускаються як «4-в-1», де потрібний протокол вибирається перемикачем на кабелі або через OSD-меню.

Глобальний ринок відеоспостереження у 2026 році характеризується чітким розподілом сфер впливу між основними технологічними провайдерами.

Hikvision залишається лідером у сегменті HD-TVI під брендом TurboHD. Їхні рішення 2025-2026 років фокусуються на технології ColorVu (кольорове зображення 24/7) та інтеграції Acusense – алгоритмів глибокого навчання (AI) на стороні реєстратора, які дозволяють класифікувати людей та транспортні засоби навіть для аналогових камер.

Dahua Technology продовжує розвивати HD-CVI, пропонуючи унікальні функції, такі як передача аудіо мовної якості через коаксіал та технологію Starlight для надчутливого нічного бачення. Їхні реєстратори XVR5000 та XVR7000 серій є стандартом надійності для комерційних об'єктів.

Hanwha Vision (Samsung) та Digital Watchdog успішно розвивають лінійки AHD та TVI для ринків, де діють обмеження NDAA (закон про національну оборону США), пропонуючи високоякісні корейські та американські альтернативи китайським гігантам.

Таким чином, аналіз технологій AHD, HD-CVI та HD-TVI станом на 2026 рік свідчить про те, що аналогове відео високої чіткості пройшло шлях від тимчасового рішення до зрілого, високотехнологічного стандарту. Незважаючи на постійний тиск з боку IP-технологій, ці стандарти залишаються незамінними для модернізації існуючих об'єктів, де капітальні витрати на заміну кабелів були б надмірними.

Головним вектором розвитку на 2026 рік стала «інтелектуалізація» аналогових систем. Завдяки тому, що сучасні відеореєстратори (XVR/DVR) отримали потужні нейропроцесори, користувачі тепер можуть отримувати сповіщення про вторгнення людей або появу автівок у заборонених зонах, використовуючи звичайні аналогові камери десятирічної давнини. Це фактично зрівняло можливості аналітики бюджетних аналогових та дорогих мережевих систем.

Сукупність факторів – нульова затримка, висока кібербезпека, простота встановлення та вдвічі менша ціна гарантує, що стандарти AHD, CVI та TVI будуть займати значну частку ринку безпеки протягом усього поточного десятиліття. Інвесторам та системним інтеграторам рекомендується розглядати ці технології як надійний, перевірений часом фундамент для побудови систем відеоспостереження, особливо в умовах обмежених бюджетів та високих вимог до відмовостійкості інфраструктури.

Типи компресії даних. Стрімкий розвиток інфраструктури відеоспостереження протягом останніх двох десятиліть призвів до виникнення протиріччя між зростаючими вимогами до якості зображення та обмеженими ресурсами систем зберігання і передачі даних. Перехід від аналогових систем до мережевих IP-камер високої роздільної здатності (UHD 4K, 8K) поставив перед галуззю завдання розробки алгоритмів, здатних експоненціально зменшувати обсяги інформації без втрати цінності матеріалу. Сучасна компресія відео – це не просто процес зменшення розміру файлів, а складна екосистема математичних методів, що базуються на розумінні людського зору, динаміки сцен спостереження та можливостей апаратної обробки в реальному часі.

Процес кодування відеоданих ґрунтується на виявленні та усуненні трьох видів надмірності: просторової (всередині кадру), часової (між кадрами) та статистичної (ентропійної). Мета стиснення полягає у створенні компактного представлення відеопотоку, що дозволяє мінімізувати бітрейт – швидкість передачі цифрових даних у бітах за секунду (bps). Вища роздільна здатність і

частота кадрів вимагають пропорційного збільшення бітрейту для збереження чіткості, що робить вибір кодека визначальним фактором вартості володіння системою.

Загалом в основі всіх сучасних стандартів лежать два фундаментальні підходи.

Просторова компресія розглядає кожен кадр як незалежне статичне зображення. Вона використовує методи, подібні до JPEG, видаляючи дрібні деталі, які є малопомітними для людського ока. Цей підхід мінімізує затримку передачі, але є вкрай неефективним з точки зору обсягу даних, оскільки не враховує подібність між послідовними кадрами.

Часова компресія використовує той факт, що в більшості сцен спостереження фон залишається статичним, а змінюються лише невеликі ділянки, де відбувається рух. Це дозволяє кодувати лише відмінності між поточним та опорним кадрами. Дана методологія реалізується через структуру групи кадрів, яка складається з кадрів різних типів:

– I-кадри (повністю самодостатні кадри, що містять всю інформацію про сцену і слугують опорними точками для відновлення відео);

– P-кадри (зберігають лише вектори руху та зміни відносно попереднього I або P кадру);

– B-кадри (найбільш ефективні для стиснення, оскільки використовують інформацію як з минулих, так і з майбутніх кадрів).

Математично ефективність компресії виражається через складність квантування та оцінку руху. При фіксованому бітрейті збільшення частоти кадрів (FPS) призводить до зменшення обсягу даних на кожен окремий кадр, що може спричиняти появу артефактів – візуальних спотворень, спричинених недостатньою кількістю бітів.

Історія галузі демонструє послідовне заміщення старих форматів більш досконалими, де кожне нове покоління забезпечує приблизно 50% покращення ефективності при значному зростанні вимог до обчислювальних ресурсів.

При підключенні аналогових камер до цифрового відеореєстратора стиснення відеоматеріалів виконується реєстратором на центральному пункті. У той же час IP-камера самостійно виконує стиснення, а потім передає стислі відеодані на мережевий відеореєстратор.

Застосування IP-камер дозволяє використовувати різні технології стиснення в одній системі. З огляду на це проектувальник систем повинен мати чітке розуміння про ці технології. Знаючи, в яких випадках слід застосовувати ту чи іншу технологію, можна отримати оптимальні результати при проектуванні систем відеоспостереження.

Стискання рухомого і нерухомого зображення можна здійснювати з втратами чи без них. Під час стикання без втрат кожен піксель зберігається у незмінному вигляді, і як наслідок – після декомпресії отримується ідентичне зображення. У цьому випадку коефіцієнт стискання, який відповідає за зменшення об’єму даних, досить малий. А без ефективного стискання більшість локальних мереж, що передають великий об’єм даних, «лягли» б за короткий

проміжок часу. З огляду на це – даний підхід в IP-системах не використовується.

З метою ефективного стискання великого об’єму даних створено низку методів та стандартів стискання з втратами. В основі них лежить ідея скорочення деталей, які не видні людському оку, і збільшення за рахунок цього коефіцієнта стискання.

Методи стискання також визначаються двома різними підходами до стандартів стискання: кадрове і міжкадрове (потокове) стискання.

Технології кадрового стиснення дозволяють стискати відеодані за допомогою застосування алгоритму стиснення стосовно кожного кадру (рис. 3.1), знятого камерою. Кінцевим результатом є серія окремо стислих зображень.

Потрібно пам’ятати, що людське око нормально сприймає відеопотік від 16 к/с і більше як повноцінне відео без переривання руху.

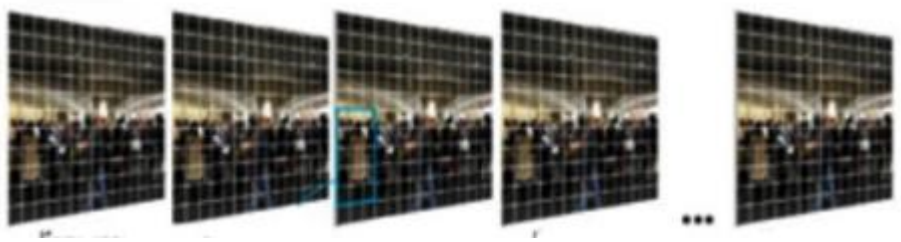


Рисунок 3.1 – Формування відеопотоку кадровим кодеком

Стиснення відеоданих з використанням технології кадрового стиснення має ряд переваг в порівнянні з більш складними технологіями міжкадрового стиснення. По-перше, отриманий в результаті покадрового стиснення відеоматеріал є серією окремо стислих кадрів, які не потребують інформації про інші кадри, – їх можна швидше стискати та передавати з камери з меншою затримкою. По-друге, так як кожен кадр є незалежним і не формується з декількох кадрів, то доступ до відеозапису можна отримати більш оперативно. Швидкий доступ підвищує ефективність розслідувань і може підвищити криміналістичну значимість відеозапису. У ситуаціях, що вимагають забезпечення максимального рівня безпеки, надання всього відеозапису як послідовності незалежних кадрів дозволяє виключити сумніви в цілісності відеоматеріалу як переконливого доказу на підставі наявності неповних кадрів, створених в процесі стиснення.

Технології міжкадрового стиснення засновані на стисканні даних в межах одного кадру і аналізі змін між кадрами (рис. 3.2). В результаті формується відеопотік зі стисненням декількох кадрів, замість серії окремих кадрів. Зазвичай при міжкадровому стисненні зберігаються тільки інкрементні зміни між кадрами, а цілі кадри зберігаються тільки періодично. Хоча ця технологія дозволяє ефективніше використовувати смугу пропускання, її застосування може призвести до втрати даних внаслідок відсутності цілих кадрів. Алгоритми міжкадрового кодування також часто називають тимчасовим кодуванням

(кодуванням в тимчасовій області), так як вони засновані на розподілі даних у часі.

Рисунок 3.2 – Формування відеопотоку міжкадровим кодеком.264

В IP-камерах зараз переважно використовуються наступні типи кодеків: H.264, H265 (потокові) і MJPEG (покадровий).

Недоліками покадрових кодеків є більш низький коефіцієнт стиснення в порівнянні з кодеками, які виконують стиснення послідовності зображень і блокова структура даних у MJPEG (дроблення зображення на квадрати 8x8 пікселів)

У кодеку H.264 в кадрі виділяються тільки рухомі об’єкти, і інформація про них кодується в проміжних кадрах. Повне зображення передається тільки через задані проміжки в якості опорного кадру. H.264 дозволяє формувати якісний відеосигнал зі значно меншим цифровим потоком, ніж MJPEG, але при цьому вимоги до продуктивності процесора досить високі. Через ресурсоємкий процес обробки кодека H.264 на відображення, його рекомендується використовувати для запису архіву. При цьому навантаження на процесор мінімальний, а глибина архіву може бути збільшена в рази. Для відображення даний кодек можна застосовувати на об’єктах де не важлива деталізація картинки. Через низький потік з IP-камер кодек H.264 не навантажує мережу між робочими станціями моніторингу і сервером, що теж важливо для об’єктів з істотної кількістю камер.

Недолік полягає в тому, що не всі кадри можуть бути придатними, наприклад, для ідентифікації.

Таким чином – кожен тип стиснення і кожен кодек призначені для конкретної цілям. Вибираючи камеру потрібно визначитися з тими завданнями, які камера буде забезпечувати. Виходячи з тактики охорони, формуються вимоги на передачу даних. При цьому не всі камери здатні передавати повні дані одночасно і в H.264 і в MJPEG. Потрібно заздалегідь уточнити про можливість камер передавати необхідні потоки.

Протоколи передачі даних у відеоспостереженні. Протоколи передачі даних у відеоспостереженні забезпечують обмін відео, аудіо та керуючими сигналами. Основу IP-систем складають стек TCP/IP, RTSP (управління потоком), ONVIF (сумісність пристроїв) та H.264/H.265 (стиснення), тоді як аналогові системи використовують CVBS та інтерфейс RS-485. Вони дозволяють переглядати відео в реальному часі, керувати PTZ-камерами та передавати дані на реєстратори (NVR/DVR).

Основні протоколи IP-відеоспостереження:

– RTSP (Real Time Streaming Protocol) керує потоками медіаданих (старт/стоп, пауза) від камер, забезпечуючи перегляд відео в реальному часі;

– ONVIF (Open Network Video Interface Forum) загальногалузевий стандарт, що забезпечує сумісність IP-пристроїв різних виробників (відео, аудіо, PTZ);

– TCP/IP (Transmission Control Protocol/Internet Protocol) базовий стек протоколів, де TCP забезпечує надійну доставку, а IP – адресацію пакетів;

– HTTP/HTTPS (HyperText Transfer Protocol) використовується для налаштування камер через веб-інтерфейс та передачі даних;

– FTP (File Transfer Protocol) застосовується для передачі архівів відео або знімків на сервер;

– RTCP (RTP Control Protocol) працює спільно з RTP для керування потоками та контролю якості.

Протоколи аналогових систем:

– CVBS (Composite Video Baseband Signal) стандарт передачі аналогового відеосигналу;

– RS-485 фізичний інтерфейс, що використовується для передачі команд управління на PTZ-камери (поворот, зум) за допомогою протоколів Pelco-D, Pelco-P.

Особливості підключення та вимоги до живлення відеокамер. Розвиток сучасних систем безпеки вимагає глибокого розуміння фізичних процесів передачі даних та енергії. Проектування надійної інфраструктури відеоспостереження не обмежується лише вибором камер з високою роздільною здатністю; воно охоплює складний комплекс розрахунків, що включає опір провідників, бюджет потужності мережевого обладнання, захист від атмосферних явищ та відповідність нормативно-правовим актам. Ефективність системи прямо залежить від синергії між вибраним форматом сигналу та якістю кабельної мережі, що забезпечує безперебійне функціонування об’єкта в критичних умовах.

Відеоспостереження на основі аналогових систем високої чіткості та мережевих IP-систем має специфічні особливості підключення, які визначають дальність трансляції та вимоги до пасивного обладнання.

В індустрії аналогових систем відеоспостереження використовують коаксіальний кабель для передачі сигналу через BNC-з’єднання.

Монтаж IP-мереж часто є простішим завдяки можливості використання одного кабелю для підключення декількох камер через комутатори, а також підтримці віддаленого доступу безпосередньо до кожної камери через смартфон або ПК.

Проте IP-системи мають і недоліки. Вони потребують вищої кваліфікації персоналу для налаштування мережевого обладнання та безпеки. Крім того, при виникненні проблем у локальній мережі можуть спостерігатися затримки зображення на декілька секунд. Важливою особливістю модернізації є те, що IP-камери неможливо підключити до старих коаксіальних мереж без

використання спеціальних перетворювачів, що вимагає повної заміни кабельної структури на виту пару.

Вибір джерела живлення є важливим етапом проектування. Більшість камер працюють від напруги 12V DC, 24V AC або отримують енергію через технологію PoE.

Блок живлення 12V DC є найбільш розповсюдженим варіантом для внутрішніх та вуличних камер. Він забезпечує стабільне живлення через стандартні адаптери або централізовані блоки живлення. Проте при великих відстанях від джерела до камери виникає проблема падіння напруги, що може призвести до некоректної роботи пристрою.

Системи 24V AC частіше застосовуються в промислових об'єктах та для живлення великих PTZ-камер. Змінний струм краще переносить довгі кабельні траси з меншими втратами напруги. Такі системи можуть підтримувати камери з високим енергоспоживанням, включаючи моделі з потужними обігрівачами та склоочисниками, де споживання може перевищувати 20-50 Вт. Категорично заборонено підключати камери 12V DC до джерел 24V AC, оскільки це призведе до миттєвого вигорання плати управління.

Потужність, яку споживає камера, залежить від її функціонального наповнення. Основні компоненти, що впливають на споживання: матриця, процесор обробки зображення, інфрачервоне підсвічування та двигуни повороту/зуму.

Бездротові камери залежать від сили сигналу, що вимірюється в dBm. Оскільки це логарифмічна шкала, кожні 3 dBm падіння означають зменшення потужності сигналу вдвічі.

Для стабільної роботи камери 4K рекомендується рівень не нижче 67 dBm. Діапазон 2.4 GHz має кращу проникаючу здатність крізь стіни, але обмежений лише трьома неперекривними каналами (1, 6, 11), що часто призводить до перевантаження ефіру. Діапазон 5 GHz пропонує вищу швидкість та менше перешкод, проте його дальність обмежена (до 30 м у приміщенні).

Найчастішою причиною відмови камер є корозія RJ45 або BNC роз'ємів.

Для захисту рекомендується:

– використання герметичних монтажних коробок класу IP66+;

– обов'язкове створення «дрип-петлі» (вигину кабелю донизу перед входом у стіну, щоб вода стікала з кабелю, а не затікала всередину);

– нанесення діелектричної змазки на контакти для запобігання окисленню;

– розміщення силікагелю всередині корпусу камери для абсорбції конденсату, що виникає при зміні температури.

Прямі удари блискавки та електромагнітні наведення можуть вивести з ладу всю систему. Для захисту використовуються спеціальні пристрої SPD (Surge Protective Devices).

Ефективність SPD залежить від якості заземлення. Опір заземлюючого контуру повинен бути менше 5 Ом (в ідеалі менше 4 Ом для систем безпеки).

Це забезпечує безпечне відведення імпульсного струму в ґрунт. У проектах ZANDZ для досягнення таких показників використовується сталева обміднена смуга перерізом 30х4 мм на глибині 0,7 м.

Встановлення систем відеоспостереження регулюється законодавством про захист персональних даних:

– згода персоналу (при використанні камер з мікрофонами в офісах необхідно отримати письмову згоду працівників);

– заборонені зони (категорично заборонено встановлювати камери в санвузлах, роздягальнях та зонах відпочинку);

– громадські місця (дозволяється встановлення камер за умови розміщення попереджувальних табличок про здійснення відеозйомки).

Таким чином, підключення та живлення відеокамер вимагає комплексного підходу, що поєднує знання мережевих протоколів, електротехніки та фізики середовища. Вибір між аналоговими системами та IP-рішеннями визначає топологію кабельної мережі. Розрахунок падіння напруги на лініях 12V залишається критичним фактором для надійності вуличних систем. Захист від вологи та блискавки, а також правильний розрахунок резервного живлення гарантують безперебійну роботу системи безпеки в будь-яких екстремальних умовах, забезпечуючи цілісність даних та захист об’єкта.

Контрольні питання:

1. У чому полягає фундаментальна відмінність у способі обробки та передачі сигналу між аналоговими та IP-камерами?
2. Порівняйте технології сенсорів CCD та CMOS: які переваги має архітектура CMOS для сучасного відеоспостереження?
3. Які існують три основні типи відеокамер за технологією обробки сигналу та які кабелі використовуються для кожної з них?
4. Назвіть ключові переваги та недоліки аналогових систем відеоспостереження.
5. Які три стандарти передачі відео високої чіткості через коаксіальний кабель домінують на ринку та хто є їхніми основними розробниками?
6. У чому полягає економічна та технічна доцільність використання гібридних відеореєстраторів?
7. Поясніть різницю між кадровим та міжкадровим стисненням даних.
8. Яку роль відіграють I, P та B-кадри у процесі часової компресії відеопотоку?
9. Які основні мережеві протоколи використовуються в IP-відеоспостереженні для передачі потокового відео та забезпечення сумісності пристроїв?
10. Які існують вимоги до живлення відеокамер та які фізичні заходи захисту рекомендуються для запобігання пошкодженню обладнання?

Література: [2, 5].

Тема 4. Нічне бачення

План:

Принцип роботи ІЧ-підсвічування для нічного бачення. Типи та характеристики ІЧ-підсвічування. Розрахунок дальності ІЧ-підсвічування.

Принцип роботи ІЧ-підсвічування для нічного бачення. З погіршенням освітленості можна спостерігати різке зменшення глибини бачення та кута спостереження камери, погіршення детальності картинки об'єкта відображення.

Еволюція технологій нічного бачення в індустрії безпеки пройшла шлях від громіздких прожекторів видимого світла до витончених напівпровідникових систем, що працюють у невидимому для людини спектрі. Центральне місце в цій еволюції посідає інфрачервоне (ІЧ) підсвічування, яке дозволяє камерам формувати високоякісне зображення в умовах повної темряви, зберігаючи при цьому конфіденційність спостереження.

Сама ідея ІЧ підсвічування базується на тому, що відеокамера має можливість створити на ПЗЗ або КМОП матриці зображення при освітленні сцени джерелом світла аж до 1000 нм, де людський зір вже не працює.

Людське око здатне бачити в більш вузькому діапазоні від 380 до 730нм.

Отже, інфрачервона область від 730нм до 1000нм може бути використана для створення джерел випромінювання, які непомітні або погано помітні для людського ока, але створюють нормальні умови освітленості для відеокамер.

В даний час інфрачервоне підсвічування в основному створюється в ближньому ІЧ діапазоні хвиль від 850нм до 880нм і рідше в діапазоні 920Нм - 950нм.

Пристрої підсвічування – інфрачервоні (ІЧ) освітлювачі, які рекомендовано використовувати в місцях, де для нормальної роботи відеокамери існуючої освітленості недостатньо. Їх застосування обумовлено наступними обставинами:

– протяжністю спектральної чутливості відеокамер в ІЧ-області;

– непомітністю або малопомітністю підсвічування для зловмисників (проте слід враховувати, що реально непомітними для людського ока є джерела інфрачервоного випромінювання з довжиною хвилі випромінювання, починаючи приблизно з 920 нм і більше);

– можливістю здійснення непомітного підсвічування там, де звичайне підсвічування може викликати незадоволення навколишніх в силу своєї яскравості або через те, що вона може негативно впливати на сприйняття історичних пам'яток і споруд;

– непомітністю, а значить, меншою схильністю прояву вандалізму;

– можливістю перекладу відеоспостереження головним чином в ІЧ-область при використанні відеокамер з ІЧ-пропускаючими фільтрами (навіть в денний час), щоб уникнути впливу відблисків на точність автоматичного розпізнавання автомобільних номерів.

В процесі експлуатації вуличних відеокамер з ІЧ підсвічуванням, встановлених в загальному корпусі з відеокамерою, виникають негативні моменти в їх роботі.

Так, у нічну пору реальний кут огляду зменшується внаслідок не відповідності кута освітлення і глибини бачення камери з дальністю освітлення (глибина бачення суттєво зменшується).

Також негативно проявляється засвічення близько розташованих до камери об’єктів, в тому випадку, коли потужність прожектора розрахована на більш далекі відстані.

Якщо об’єкт рухається в бік камери з ІЧ підсвічуванням, перебуваючи на великій відстані, то на екрані монітора він «дрібний» і не дуже добре його видно.

Підійшовши зовсім близько до камери об’єкт, стає «крупним», але засвіченим (див. рис. 4.1) і теж нерозбірливим. На середній відстані все начебто нормально, але хочеться побачити об’єкт крупніше.

Усунути такий ефект можна ввівши в алгоритм роботи ЧК підсвічування адаптацію з рівня освітленості об’єкта спостереження.

Суть адаптації полягає в тому, що за рівнем освітленості регулюється сила світла, вбудованого ІЧ прожектора, тобто утворюється своєрідний зворотний зв’язок між камерою і блоком підсвічування.

Рисунок 4.1 – Кадр без адаптивного підсвічування (фото зліва) та з адаптивним підсвічуванням (фото справа)

В результаті адаптивне підсвічування змінює свою потужність, залежно від інтенсивності відбитого від об’єкта світла.

При наближенні об’єкту до камери, потужність підсвічування зменшується, і можна розглянути його в умовах оптимальної за інтенсивністю освітленості.

Типи та характеристики ІЧ-підсвічування. В даний час, ІЧ підсвічування використовується в двох варіантах виконання:

– у вигляді окремо встановлюється модуля, конструктивно ніяк не пов’язаного з відеокамерою.

– у вигляді модуля, який вмонтований в корпус відеокамери (адаптивне ІЧ підсвічування – рис. 2).

ІЧ підсвічування має ряд специфічних особливостей, які необхідно враховувати в процесі їх вибору та монтажу.

Рисунок 2 – Відеокамера з адаптивним ІЧ освітлювачем та двома ІЧ прожекторами

ІЧ-освітлювачі характеризуються такими основними параметрами:

– кутом освітлювального сектора;

– радіусом (дальністю) дії;

– довжиною хвилі випромінюваного світла;

– струмом (потужністю) споживання.

Загально відомо, що прилади з ІЧ випромінюванням мають схожі основні властивості, як і інші джерела світла. Одним з основних параметрів світлодіода є довжина хвилі випромінюваного ІЧ світла. У матрицях відеокамер спостерігають спад чутливості зі збільшенням довжини хвилі до області ІЧ діапазону. З огляду на це зазвичай вибирають світлодіоди, основна випромінювальна здатність яких припадає на довжину хвилі 850 нм. У цих світлодіодів можна помітити червонувате світіння в темряві, тому що їх спектральна характеристика частково потрапляє в область видимого спектру. Повністю невидиме випромінювання мають світлодіоди з максимумом спектральної характеристики, що припадає на 930-950 нм. Якщо при організації CCTV немає необхідності в організації прихованого ІЧ підсвічування, то не варто прагнути встановлювати подібні освітлювачі, оскільки чутливість матриць відеокамери в цій області нижча ніж в діапазоні 830-850 нм.

Конструктивно ІЧ-освітлювачі можуть бути виконані на основі галогенних ламп і з застосуванням світлодіодів.

ІЧ-освітлювачі на основі галогенних ламп (IR-Lamps) з встановленими перед ними ІЧ-фільтрами характеризуються рядом недоліків:

– значною потужністю споживання (в залежності від моделі від 20 до 500 Вт);

– діапазоном довжин хвиль 730...830 нм, що практично потрапляє в область видимого людиною світла, тому подібний ІЧ освітлювач досить легко може бути виявлений;

– порівняно невеликим терміном служби галогенних ламп (1000...2000 годин) через надмірне нагрівання всередині освітлювача.

Ці недоліки сприяли впровадженню в освітлення нових технологій, одна з яких – твердотілі ІЧ-світлодіоди (IR-LED), об'єднані в матричну структуру. Вони не такі потужні, як галогенні лампи, але мають велику ефективність і випромінюють значну кількість світла. Освітлювачі з використанням світлодіодів ІЧ-діапазону мають наступні переваги:

– істотно меншу потужність споживання (від 5 до 50 Вт);

– досить великий термін служби (понад 100000 годин);

– малі габарити і масу;

– більшу безпекою при експлуатації.

В цілому можна сказати, що ІЧ-освітлювачі на базі галогенних ламп найчастіше використовуються у вуличних умовах для освітлення досить віддалених об'єктів, а твердотільні освітлювачі на базі ІЧ-світлодіодів частіше застосовуються в приміщеннях, на сходинкових майданчиках і вони можуть бути закамуфльовані під різні предмети: таблички з номерами квартир, головки болтів тощо.

Останнім часом збільшилася кількість відеокамер із вбудованою в їх корпуси світлодіодним адаптивним ІЧ-підсвічуванням. Крім того, ІЧ-світлодіоди встановлюються в зовнішні панелі відеодомофонів (нерідко за темним склом).

Класичний варіант розташування світлодіодів підсвічування – навколо або поруч з об'єктивом, в одному корпусі з самої відеокамери. Одним з недоліків такого розташування є взаємний вплив теплового випромінювання світлодіодів і відеокамери. При цьому тепло, що випромінюється світлодіодами, збільшує шуми матриці відеокамери, що негативно позначається на чутливості пристрою в темний час доби. Ще одним мінусом такого рішення є відблиски від поверхні оглядового скла, які можуть створювати світлодіоди. Наприклад, при забрудненні оглядового вікна відеокамери. Воно буде все більше і більше підсвічувати цей бруд, що особливо чутливо для купольних відеокамер. Щоб впоратися з цим явищем, виробники присувають бленду об'єктива впритул до оглядового скла і додатково використовують для об'єктива і світлодіодів два незалежні скла, розділених герметичною шайбою.

Щоб уникнути подібних моментів рекомендується застосовувати зовнішні ІЧ прожектори для відеоспостереження. Один такий потужний прожектор здатний висвітлювати весь контрольований камерами простір, забезпечуючи практично денне освітлення.

ІЧ прожектор – спеціальний прилад, що оснащується вбудованими світлодіодами, які випромінюють світло в інфрачервоному спектрі.

Будь-який ІЧ прожектор працює в невидимому для людського ока спектрі випромінювання.

При виборі інфрачервоного прожектора для відеоспостереження важливо враховувати основні характеристики даних приладів, в залежності від яких може різнитися сфера їх застосування. Перед придбанням ІЧ прожектора необхідно звертати увагу на наступні 4 параметри: довжина хвилі; дальність можливого виявлення об'єкта; кут підсвічування; кількість споживаної енергії.

Від довжини хвилі залежить те, чи зможе людина помітити дію підсвічування.

Від дальності виявлення залежить максимальна відстань дії інфрачервоного підсвічування, при якому камера здатна розрізнити фігуру людини. Збільшити дальність дії підсвічування можна шляхом зменшення кута випромінювання і концентрації пучка світла на віддаленій ділянці. Також дальність виявлення залежить і від чутливості сенсора самої камери.

Хороша якість зображення досягається тільки в тому випадку, коли кут випромінювання підсвічування більше кута огляду камери - тільки при цьому забезпечується рівномірне освітлення всієї ділянки без сліпих зон.

Кількість споживаної енергії інфрачервоними прожекторами знаходиться в межах 0,4-1 А, робоча напруга становить 12 В, як і у будь-яких інших слабкострумових приладах. Щоб правильно підібрати ІЧ прожектор і камеру відеоспостереження під конкретні потреби необхідно в деталях проаналізувати, в яких умовах буде використовуватися обладнання.

При виборі варто враховувати такий важливий момент, як відмінність ІЧ прожекторів по дальності можливого випромінювання. За цим параметром дані прилади поділяються на 3 групи: ближні; середні; дальні.

Ближні прожектори здатні забезпечувати освітлення на відстань від 1,5 до 10 метрів. Зазвичай подібні прилади використовуються для забезпечення нічного освітлення в банках, офісах, лікарнях, касах і багатьох інших місцях, де нічний відеоспостереження дійсно необхідно без застосування звичайних джерел світла.

Середні прожектори інфрачервоного підсвічування зазвичай використовуються для забезпечення нічного відеоспостереження на великих відкритих територіях, коли необхідно висвітлити весь простір ділянки. Подібні прилади здатні забезпечувати висвітлення з дальністю до 60 м, і широким кутом огляду 120-160°.

Далекобійні інфрачервоні прожектори, як правило, забезпечують вузькоспрямований пучок світла, здатний концентруватися на віддаленому об’єкті до 300 м. Кут огляду у них відповідний – від 20 до 60°. Прожектори зі збільшеною дальністю використовуються в клубах, театрах, кінотеатрах, де застосування звичайних джерел світла для забезпечення умов відеоспостереження було б неприйнятним. Також ІЧ прожектори великої дальності використовуються на дорогах для відеофіксації ситуації на дорогах, які не засліплюють при цьому водіїв, і не створюють аварійних ситуацій.

За кутами освітлення прожектори умовно діляться на ширококутні (заливає освітлення), що мають, як правило, невелику дальність; прожектори середніх кутів, а також прожектори гостронаправлені з великою дальністю, малі кути освітлення яких обумовлені незначною потужністю випромінювання світлодіодних освітлювачів, що не перевищує 5-10 Вт.

Розрахунок дальності ІЧ-підсвічування. Сучасні системи ІЧ-підсвічування використовують напівпровідникові світлодіоди (LED), ККД яких становить від 0,06 до 0,35. При розрахунку дальності необхідно враховувати

теплову деградацію: протягом першої години роботи потужність ІЧ-LED може зменшуватися на 15–20% через нагрівання кристала, що безпосередньо впливає на дальність виявлення.

Вибір між довжинами хвиль 850 нм та 940 нм є стратегічним компромісом між дальністю та непомітністю. Довжина хвилі 850 нм вважається «напівприхованою», оскільки вона викликає слабке червоне світіння світлодіодів, видиме людським оком. Це зумовлено тим, що спектральний розподіл енергії діода має форму дзвона, край якого заходить у видимий червоний діапазон.

Натомість, 940 нм є повністю невидимим діапазоном («ковертне підсвічування»), що важливе для військових та спеціальних застосувань. Однак, більшість CMOS-сенсорів мають значно нижчу квантову ефективність на цій довжині хвилі. Як наслідок, дальність дії підсвітки 940 нм зазвичай на 30–50% менша, ніж у аналогів на 850 нм при однаковій енергозатратності.

Об’єктив камери діє як збирач фотонів, і його апертура (F-число) має нелінійний вплив на кількість енергії, що потрапляє на сенсор. Оскільки кількість світла пропорційна площі апертури, зміна F-числа в $\sqrt{2}$ разів призводить до дворазової зміни освітленості сенсора.

Об’єктив з F/1.0 пропускає на 250% більше інфрачервоної енергії, ніж об’єктив з F/1.6. Таким чином, використання високоякісної світлосильної оптики дозволяє пропорційно зменшити потужність ІЧ-прожекторів або збільшити дальність спостереження без заміни освітлювального обладнання. Важливо також враховувати зсув фокуса в ІЧ-діапазоні; оскільки індекс заломлення скла залежить від довжини хвилі, звичайні об’єктиви можуть давати розмите зображення вночі, якщо вони не мають спеціального ІЧ-коригованого покриття.

Розрахунок дальності підсвічування неможливий без оцінки відбивної здатності об’єктів у сцені. Альбедо – це безрозмірна величина, що характеризує здатність поверхні відбивати падаюче випромінювання (табл. 4.1). У ближньому ІЧ-діапазоні відбивна здатність багатьох матеріалів суттєво відрізняється від їхнього вигляду у видимому світлі.

Особливу увагу слід приділяти асфальтовому покриттю. Новий асфальт містить велику кількість бітумного в’яжучого, яке майже повністю поглинає ІЧ-промені. З часом, внаслідок зносу та окислення, на поверхні оголюється щебінь, що призводить до зростання альбедо і, відповідно, до збільшення видимої дальності підсвічування на старих дорогах.

Атмосфера не є абсолютно прозорим середовищем для інфрачервоного випромінювання і тому при сильному дощі дальність роботи ІЧ-підсвітки скорочується в десятки разів, що необхідно враховувати при проектуванні систем периметрального захисту великої протяжності.

При проектуванні систем з активним ІЧ-освітленням рекомендується використовувати комплексний підхід, що включає енергетичний бюджет системи та просторове планування.

Таблиця 4.1 – Коефіцієнти відбиття (Альбедо) поширених матеріалів у ближньому ІЧ-діапазоні

Матеріал	Альбедо (0.7 - 1.1 мкм)	Вплив на дальність підсвічування
Свіжий сніг	0.80-0.90	Максимальна дальність; ризик переосвітлення
Зелена трава	0.45-0.55	У 2.2 рази вища ефективність порівняно з білим папером
Бетон (новий)	0.35-0.45	Добра відбивна здатність; стабільний результат
Старий асфальт	0.15-0.25	Середня дальність; покращується з віком
Новий асфальт	0.05-0.10	Мінімальна дальність; потребує потужного підсвічування
Чорна тканина	0.10-0.80	Непередбачувано; може виглядати білою в ІЧ
Вода	0.05-0.08	Поглинає ІЧ; об’єкти на воді майже не підсвічуються

Розрахунок необхідної потужності живлення для камер з ІЧ-підсвічуванням повинен враховувати пікові навантаження. Згідно з рекомендаціями, сумарну номінальну потужність камер слід множити на коефіцієнт 1,3 для врахування пускових струмів та втрат у кабелях. Також необхідно додавати 30% запасу на деградацію компонентів та майбутнє розширення.

Для збільшення дистанції часто використовують декілька прожекторів. Сумарна дальність розраховується за формулою, що базується на законі зворотних квадратів:

$$D_{total} = D_{unit} \times \sqrt{N} \tag{4.1}$$

де D_{unit} – дальність одного прожектора, а N – кількість прожекторів.

Наприклад, чотири прожектори з дальністю 50 м дозволять «бачити» на відстані $50x\sqrt{4} = 100м.$

При проектуванні слід уникати встановлення підсвітки занадто близько до об’єктива камери, щоб зменшити відбиття від пилу, комах та опадів безпосередньо в лінзу. Технологія Adaptive IR (Smart IR) дозволяє динамічно змінювати потужність випромінювання залежно від положення об’єкта в кадрі, запобігаючи засвіченню облич при наближенні людини до камери.

На основі сказаного можна сформулювати ключові принципи розрахунку та впровадження ІЧ-підсвічування:

– для більшості завдань безпеки оптимальним є вибір 850 нм завдяки кращій чутливості сенсорів (довжину 940 нм слід обирати лише при жорстких

вимогах до повної невидимості джерела світла, закладаючи 50% запас за потужністю);

– світлосильні об’єктиви з низьким F-числом (F/1.2 та менше) є більш ефективним способом збільшення дальності, ніж нарощування потужності LED-масивів;

– розрахунок повинен базуватися на найменш відбивному об’єкті (наприклад, новому асфальті або темному одязі), щоб гарантувати надійність системи в найгірших сценаріях;

– при плануванні систем для роботи в тумані або під час дощу необхідно передбачати значний надлишок потужності або інтегрувати термальні камери, які працюють у довгохвильовому ІЧ-діапазоні (8-14 мкм) і не залежать від зовнішнього підсвічування;

– проектна дальність повинна відповідати цільовому рівню оперативної задачі (наприклад, 250 PPM для ідентифікації на входах), а не просто маркетинговим заявам про «видимість» на певну дистанцію.

Таким чином, сучасне проектування ІЧ-систем переходить від емпіричного підбору до точного математичного моделювання, що дозволяє створювати системи відеоспостереження з гарантованою ефективністю в будь-який час доби.

Контрольні питання:

1. У чому полягає основна відмінність між сприйняттям світла людським оком та матрицею відеокамери в контексті інфрачервоного діапазону?
2. Порівняйте довжини хвиль ІЧ-підсвічування 850 нм та 940 нм: які їхні переваги та недоліки щодо помітності та дальності дії?
3. Які негативні ефекти виникають при використанні потужного ІЧ-підсвічування на близьких відстанях і як їх усуває функція Adaptive IR (Smart IR)?
4. Назвіть основні переваги світлодіодних (IR-LED) освітлювачів порівняно з галогенними ІЧ-лампами.
5. Чому вбудоване в корпус камери ІЧ-підсвічування може негативно впливати на чутливість матриці та якість зображення?
6. Як класифікують ІЧ-прожектори за дальністю дії та які завдання виконує кожна з груп (ближні, середні, дальні)?
7. Яким має бути співвідношення між кутом випромінювання підсвічування та кутом огляду камери для забезпечення якісного зображення?
8. Що таке Альбедо і як зміна стану асфальтового покриття (новий проти старого) впливає на дальність нічного бачення?
9. Як апертура об’єктива впливає на кількість інфрачервоної енергії, що потрапляє на сенсор, та на загальну дальність підсвічування?
10. За якою формулою розраховується сумарна дальність при використанні декількох однакових ІЧ-прожекторів?

Література: [2].

Тема 5. Приймально-передавальні тракти та комутаційне обладнання

План:

Типи кабелів та їх основні технічні характеристики. Методика визначення максимально допустимої довжини кабелю за критерієм надійної синхронізації. Роз'єми відеотрактів та їх призначення. Методики монтажу роз'ємів BNC та RJ45. Інжектори, сплітери та репітери відеосигналу. Комутатори, маршрутизатори. Топології IP відеоспостереження. Методика визначення загальної швидкості інформаційного потоку. Методика вибору пропускної здатності мережі. Методика визначення кількості фізичних підмереж. Методика визначення максимально допустимих потоків від кожної відеокамери.

Типи кабелів та їх основні технічні характеристики (приймально-передавальні тракти). Проектування та впровадження CCTV на сучасному етапі розвитку технологій безпеки вимагає комплексного розуміння фізичних процесів, що відбуваються в середовищі передачі сигналів. Кабельна інфраструктура є фундаментом, на якому будується вся архітектура системи, і її неправильний вибір або некоректний монтаж можуть нівелювати переваги найдорожчого обладнання. Еволюція від аналогових систем низької роздільної здатності до цифрових IP-рішень та форматів аналогового відео високої чіткості (AHD, HD-TVI, HD-CVI) зумовила появу різноманітних типів кабелів, кожен з яких має специфічні технічні параметри, обмеження та сфери оптимального застосування.

Відстань місця розташування відеокамер від поста спостереження (або відеосервера) вимагає рішення задачі передачі відеосигналів на значні відстані. Кожне вирішення цього питання має свої переваги і недоліки.

Стандартним і найбільш поширеним рішенням передачі відеосигналів є використання коаксіального кабелю з хвильовим опором 75 Ом (рис. 5.1). Цей кабель протягом десятиліть залишався основним засобом передачі відеосигналу в системах безпеки. Його конструкція, що включає центральний провідник, діелектрик, екрануюче обплетення та зовнішню оболонку (рис. 5.1), забезпечує високу стійкість до електромагнітних завад та можливість передачі високочастотних сигналів з мінімальними втратами. Використання ж кабелів з імпедансом 50 Ом, що є стандартом для радіозв'язку, призводить до неузгодженості ліній, виникнення відбитих хвиль та суттєвого погіршення якості зображення.

Як правило, в залежності від внесеного кабелем загасання прийнятну якість зображення може бути досягнуто, якщо відеокамера віддалена від поста спостереження на відстань не більше 200-300 м. При великих відстанях для компенсації втрат в кабелі потрібно використовувати магістральні відеопідсилювачі.

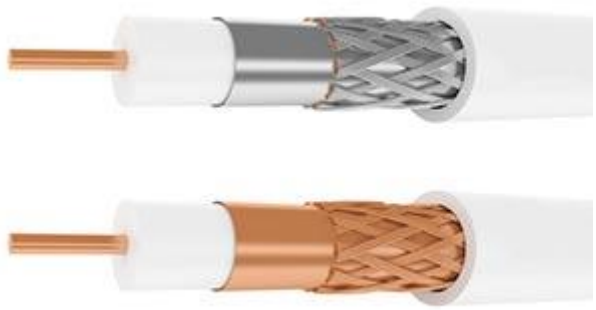


Рисунок 5.1 – Коаксіальний кабель з хвильовим опором 75 Ом

Найбільш часто для відеоспостереження використовуються кабелі марки РК-75-2-13, РК-75-4-12 (РК – радіочастотний кабель), або імпортні аналоги – RG-59, RG-6, RG-11. При виборі коаксіального кабелю необхідно враховувати такі важливі параметри, як довжина і місце прокладки (всередині приміщення або на вулиці), і в залежності від цього вибирати потрібну марку проводу.

При значній відстані камер від відеореєстратора і один від одного (довжина лінії понад 200-300 метрів), сигнал може значно ослабнути: тут діє проста аксіома – чим кабель довший і тонший, тим більше втрат сигналу. Так що при виборі дуже важливо враховувати відстань прокладки, і, виходячи з нього, вже вибирати відповідний кабель для систем відеоспостереження.

Наприклад, РК-75-2-13 прокладають при довжині лінії, що не перевищує 100 метрів, а при більш значних відстанях (від 100 до 300 метрів) використовують марки РК-75-3-..., при відстанях понад 300 метрів зазвичай застосовують UTP (про це нижче).

Кабель RG-6 відрізняється від своїх аналогів РК-75 в першу чергу тим, що має більший діаметр центрального провідника і оболонки. Також він здатний пропускати дещо більший діапазон частот, ніж РК-75.

AHD камери здатні забезпечувати передачу відеосигналу на відстань до 500 метрів по звичайному коаксіальному кабелі, за умови використання якісної моделі кабелю RG-59.

Наведемо таблицю, що відображає залежність типу дроту від відстані (табл. 5.1).

Кабель RG-59 вважається галузевим стандартом для традиційних аналогових систем. Завдяки меншому діаметру він легше вкладається у кабель-канали та гнучкий при монтажі в обмежених просторах. Однак при переході на формати HD-over-coax (AHD, TVI, CVI) втрати на високих частотах у RG-59 стають критичними, що змушує інженерів використовувати RG-6. RG-6 має товстішу центральну жилу, що забезпечує кращу якість сигналу на великих відстанях та ширшу смугу пропускання, необхідну для сучасних цифрових сигналів. RG-11 є найбільш потужним і водночас жорстким варіантом, який використовується переважно для магістральних ліній на великих підприємствах, де відстані між камерою та реєстратором перевищують 400 метрів.

Таблиця 5.1 – Марки кабелю та рекомендовані для них відстані передачі сигналу

Марка кабелю	Рекомендована відстань до відеокамери, не більше, м
РК-75-1,5-11	50
РК-75-2-11	300
РК-75-2-11а	200
РК-75-2-13	350
РК-75-3-32	450
РК-75-3,7-32а	600
РК-75-4-11	600
РК-75-4-11а	600
РК-75-4-12	600
РК-75-4-15	600
РК-75-4-16	600
РК-75-4,9-32а	750
РК-75-9-12	Магістральний
РК-75-9-13	Магістральний
RG-59	230
RG-6	300
RG-11	Магістральний

Однією з найбільш поширених помилок при виборі кабелю є використання варіантів з центральним провідником із мідненої сталі. У системах кабельного телебачення такі кабелі ефективні завдяки скін-ефекту, оскільки сигнал високої частоти рухається лише по тонкому шару міді на поверхні. Проте в системах CCTV відеосигнал має значну низькочастотну складову, для якої опір сталевого осердя є занадто високим. Це призводить до падіння напруги, втрати деталізації та виникнення завад. Для професійного відеоспостереження важливим є використання кабелів з чистою мідною жилою.

Екранування також відіграє вирішальну роль у підтримці чистоти сигналу. Стандартом для безпекових систем є мідне обплетення з щільністю покриття не менше 95%. Комбінація алюмінієвої фольги та мідного обплетення забезпечує захист як від низькочастотних магнітних полів, так і від високочастотних радіоперешкод.

Вибираючи коаксіальний кабель для відеоспостереження, потрібно переконайтися в тому, щоб центральний провідник був повністю мідним, в іншому випадку сигнал буде дуже слабким.

Плюси. Основною перевагою даного типу кабелю є його висока стійкість до перешкод, доступна ціна, здатність передачі як відео, так і аудіо сигналу.

Мінуси. До недоліків коаксіального кабелю можна віднести високу вартість конекторів, легку пошкоджуваність, обмеження по відстані прокладання.

Як було сказано, при довжині ліній, що перевищує 300 м, застосовують магістральні відеопідсилювачі, причому для підвищення відношення сигнал/шум їх бажано розташовувати якомога ближче до відеокамер.

Основними параметрами магістральних відеопідсилювачів є:

– коефіцієнт посилення (бажано регульований);

– вхідний і вихідний опір, 75 Ом;

– ширина смуги пропускання;

– зручність монтажу;

– діапазон робочих температур;

– допуск на величину напруги живлення;

– вплив пульсацій напруги живлення на параметри вихідного відеосигналу;

– наявність захисту від переполюсування напруги живлення;

– наявність захисту по відеовиходу від короткого замикання.

У випадках, коли живлення відеокамери та передача сигналу здійснюється з однієї точки найзручніше використовувати комбінований кабель для систем відеоспостереження. Він підходить як для аналогових, так і для цифрових пристроїв. Це все той же коаксіальний провід з опором 75 Ом, але вже в одній зв'язці з проводами живлення. Завдяки такому сплетіння живлення камер і передача сигналу може забезпечуватися без прокладки додаткових проводів. Така конструкція дозволяє передавати відеосигнал та напругу живлення 12В або 24В по одній кабельний лінії, що суттєво зменшує трудовитрати та кількість витратних матеріалів. Також на додаток до всього в такому кабелі можуть бути дроти для підключення додаткових функціональних елементів (наприклад, мікрофона), і для здійснення управління камерою (наприклад, для управління повертають пристроєм камери). Як приклад можна привести кабель ККСЕВ, який має крім коаксіальної жили розділені дроти для живлення і аудіо сигналу. Комбінований високочастотний кабель (КВК) з жилами живлення є одним з найдорожчих. Він застосовується при створенні системи відеоспостереження, в якій кожна камера буде підключатися до мережі за допомогою окремого блоку живлення, кожен вихід +12 якого оснащений індивідуальним запобіжником, або при невеликій кількості камер. Серед найбільш часто використовуваних комбінованих кабелів для відеоспостереження можна назвати наступні марки: КВК-2П, КВК-В-2. Найбільш поширеними є модифікації з перерізом жил живлення 0.5 мм² та 0.75 мм².

Переріз жили живлення безпосередньо впливає на максимальну відстань, на якій камера може отримувати стабільне живлення без критичного падіння напруги. При довжині лінії понад 50-70 метрів рекомендується використовувати жили перерізом не менше 0.75 мм², щоб уникнути некоректної роботи ІЧ-підсвітки або самовільного перезавантаження камери в нічний час. Оболонка кабелів КВК-П виготовляється зі світлостабілізованого поліетилену чорного кольору, що забезпечує стійкість до ультрафіолетового випромінювання, вологи та температурних перепадів від -50°С до +60°С.

Кабель «вита пара» став домінуючим у системах IP-відеоспостереження завдяки здатності передавати великі обсяги цифрових даних та підтримці технології Power over Ethernet (PoE). Конструкція кабелю базується на принципі скручування провідників парами, що дозволяє мінімізувати перехресні завади та вплив зовнішніх полів.

Зазвичай кабель вита пара використання в тих випадках, коли дальність лінії від камери до пристрою прийому сигналу становить від 300 до 1000 м (відстань можливої прокладки робочої лінії відеоспостереження за допомогою витої пари може становити до 3 км.). Зручність використання цього типу кабелю для систем відеоспостереження полягає в великій кількості провідників під одною опліткою. Завдяки цьому можна по одній лінії підвести і живлення до камер, і здійснити передачу основних сигналів (відео, аудіо), і задіяти проводку для забезпечення управління камерою, а також для підключення додаткової камери.

Якість міді у витій парі є вирішальною. На ринку часто зустрічається дешевий кабель CCA (Copper Clad Aluminum – алюміній плакований міддю). Використання CCA у системах відеоспостереження, особливо з PoE, є вкрай ризикованим через високий опір алюмінію, його ламкість та схильність до швидкого окислення в місцях контакту. Для надійних інсталяцій необхідно використовувати тільки чисто мідний кабель.

В аналоговому відеоспостереженні, до застосування витої пари зазвичай вдаються у випадках великої відстані від камери відеоспостереження до відеореєстратора. Внаслідок великої протяжності кабельної лінії на відеосигнал в більшості випадків накладаються перешкоди, які заважають сприйняттю зображення з камери. Перешкоди можуть виникати не тільки при великих відстанях – частою причиною їх виникнення є так званий «радіофон», або прокладений по близькості силовий кабель, який також може накладати перешкоди на коаксіальний кабель. Так чому ж при великих відстанях кабельних ліній перевага віддається саме витій парі? Справа в тому, що вита пара має 8 попарно скручених між собою провідників, кожен з яких має індивідуальну ізоляцію, і на додаток до всього покритих загальної пластиковою оболонкою. Основною особливістю, яка дозволяє даному кабелю не боятися перешкод є саме скручування двох провідників, кожен з яких має різну полярність – один «+», інший «-». Приймач віднімає з позитивного сигналу негативний, і в результаті відбувається те, що корисний сигнал посилюється вдвічі, а перешкоди повністю зникають. Внаслідок цього такий кабель має дуже хороший захист від радіоперешкод, і при своєму вдалому співвідношенні ціна/якість представляється хорошим варіантом для побудови системи відеоспостереження на велику відстань.

Внаслідок своїх технічних характеристик, вита пара має дуже високий питомий опір, що негативним чином позначається на передачі відеосигналу на відстань понад 200 метрів, тому при необхідності організації відеоспостереження на великі відстані на обох кінцях кабелю закріплюються спеціальні приймачі, які існують 2 типів:

– пасивні приймачі;

– активні передавачі.

Передавачі встановлюються на стороні камери, а приймачі на стороні приймаючого обладнання. Пасивні передавачі застосовуються для передачі відеосигналу на невеликі відстані – 150-500м, оскільки не здатні компенсувати всі перешкоди. Основною особливістю є те, що для роботи даного типу пристроїв не потрібно подачі електроживлення. При великої протяжності кабельних ліній застосовують активні передавачі, здатні забезпечувати передачу сигналу на відстань до 4 км, в залежності від специфікації. Для роботи активних приймально-передавальних пристроїв необхідна наявність живлення з напругою 12В. При правильній організації системи дальність передачі може досягати 3000-4000 м.

Рисунок 5.2 – Пасивні відео балуни (передавач/приймач) для передачі відеосигналу за витою парою

Використання балунів з роз’ємами RJ45 полегшує монтаж, дозволяючи обтискати кабель стандартним інструментом. Сучасні 4-канальні балуни дозволяють передавати відео від чотирьох камер по одному кабелю Cat5e, що значно спрощує кабельне господарство об’єкта.

Щоб успішно організувати відеоспостереження з використанням даних технічних засобів, необхідно дотримуватися таких правил:

– використовувати тільки сумісні між собою приймачі і передавачі;

– для досягнення кращого результату слід застосовувати тільки активні приймачі, бажано з можливістю регулювання посилення (коригування АЧХ – амплітудно-частотної характеристики);

– використовувати кабель з мінімальними значеннями ємності між провідниками.

Сигнал може послаблюватися як за рахунок опору лінії, так і за рахунок ємності кабелю внаслідок передачі високочастотного сигналу, а оскільки вита пара застосовується для організації відеоспостереження на далекі відстані, необхідно максимально знизити ризик втрати сигналу шляхом його посилення. Саме для посилення сигналу з камери і застосовуються активні приймально-передаючі пристрої. Оскільки діапазон частот сигналу знаходиться в досить

широких межах, ослаблення може бути нерівномірним – для забезпечення мінімальних відмінностей між зображенням на моніторі, і зображенням з відеокамери, високі частоти необхідно посилювати більше, ніж низькі. Для цього необхідно провести корекцію АЧХ, що може бути виконано тільки з використанням активних приймачів і передавачів.

Залежно від особливостей будови розрізняють кілька видів кабелю «вита пара» – UTP, FTP, STP. Категорія кабелю визначає його частотні характеристики та здатність підтримувати певні швидкості передачі даних.
UTP кабель найпростіший, він не має захисних екрануючих оболонок, і являє собою 8 ізольованих, попарно скручених провідників, поміщених в загальну захисну оболонку.

FTP кабель відрізняється наявністю загальної фольгованої екрануючої оболонки. Завдяки її наявності даний кабель можна прокладати поруч з кабелями електропроводки та іншими джерелами перешкод. Дуже важливо стежити за збереженням фольгованого екрану, і не перевищувати мінімальний радіус вигину - не більше 8 зовнішніх діаметрів кабелю. Зовнішній захист кабелю може бути виконана як з ПВХ так і твердого поліетилену.

STP кабель також має загальну захисну оболонку, але вже не з фольги, а з мідного обплетення. Крім цього, кожен провідник в такому кабелі цільномідний, ізольований поліолефіном, і має індивідуальний захисний екран з фольги. Зовнішня ізоляція як правило виконується з вогнестійкого ПВХ. Застосування даного типу кабелю необхідно у випадках прокладки понад 90 метрів при наявності численних джерел перешкод. При прокладанні STP кабелю необхідно заземлити екран, інакше він буде працювати подібно до антени, яка притягувала електромагнітне випромінювання!

Ступінь захисту від перешкод також залежить від категорії кабелю витої пари. Чим вище категорія - тим вище захист. Зазвичай для потреб відеоспостереження застосовується кабель категорії 5е, який при оптимальному співвідношенні ціна/якість здатний забезпечити передачу відеосигналу на відстань 2-3 тис. метрів.

Для великих протяженностей застосовуються більш високі категорії кабелів, які здатні забезпечити найкращий захист від перешкод:

– кабель 8 категорії має поліпшений захист від перешкод завдяки наявності додаткової екрануючої оболонки, що відводить перешкоди від кабелю;

– для створення віддаленого спостереження на відстані від 4 тис. метрів рекомендовано застосування кабелю «вита пара» 7 і вище категорії, з використанням потужних активних підсилювачів;

– кабелі категорій 5 і 5е працюють в діапазоні частот 100 мГц і 125 мГц, і здатні передавати дані з камер зі швидкістю 100-1000 Мбіт/сек. Це достатньо для більшості IP-камер з роздільною здатністю до 4K;

– кабелі категорії Cat 6 працюють на частотах до 250 МГц, забезпечуючи кращу якість сигналу та менші втрати на великих відстанях;

– кабелі категорії Cat 6A підтримують частоту 500 МГц та швидкість передачі даних до 10 Гбіт/с на відстані до 100 метрів (рекомендуються для систем з високим навантаженням та потужним PoE++);

– у кабелі 7 категорії екрановану оболонку має кожна пара, а також є загальний захисний екран під загальною опліткою. Діапазон частот 600-700 мГц, швидкість передачі 100 Гбіт/с, використовуються у середовищах з критично високим рівнем перешкод.

Оптоволоконний кабель є найефективнішим рішенням для реалізації відеоспостереження на великі відстані, але висока вартість не дозволяє використовувати його повсюдно.

Оптоволоконний кабель є незамінним у випадках, коли відстань передачі перевищує 100 метрів (для IP) або 500 метрів (для аналогу), а також в умовах екстремальних електромагнітних завад. В оптичному волокні інформація передається у вигляді світлових імпульсів, що забезпечує повну гальванічну розв'язку та імунітет до згаданих завад.

Вибір типу волокна залежить від необхідної дальності передачі та бюджету проекту.

Одномодове волокно має дуже малий діаметр ядра (8-10 мікрон), що дозволяє проходити лише одному променю світла (моді). Це мінімізує дисперсію та дозволяє передавати дані на відстані до 40-100 км без підсилення. Використовує лазерні джерела світла.

Багатомодове волокно має ширше ядро (50 або 62,5 мікрон), по якому світло поширюється за декількома траєкторіями. Це призводить до міжмодової дисперсії, що обмежує дальність передачі значенням до 2 км. Використовує дешевші LED або VCSEL джерела світла.

В сучасних системах безпеки для магістральних каналів та зв'язку між будівлями перевага віддається одномодовому волокну OS2, оскільки воно забезпечує найкращу масштабованість та запас за дальністю.

Для інтеграції аналогових камер у оптоволоконну мережу використовуються відео-оптичні перетворювачі. Типовий комплект складається з передавача (TX), що підключається до камери через BNC, та приймача (RX), що підключається до реєстратора. Ці пристрої здатні транслювати відео високої чіткості (1080P/4K) на відстані до 20-80 км по одному волокну за технологією WDM (wavelength-division multiplexing), де відео йде на одній довжині хвилі (наприклад, 1310 нм), а дані управління PTZ – на іншій (наприклад, 1550 нм).

Таким чином, вибір кабелю є результатом компромісу між дальністю, роздільною здатністю та умовами довкілля.

Для локальних аналогових систем (до 150 м) найбільш доцільним є використання комбінованого кабелю КВК з мідним коаксіальним елементом RG-59 та PE-оболонкою для вулиці або PVC для приміщень.

Для середніх та великих IP-систем з використанням PoE++ пріоритетом є кабель витої пари категорії Cat 6A з мідними провідниками 23 AWG, бажано екранований (F/UTP), для забезпечення термічної стабільності в пучках.

Для магістральних каналів та об’єктів критичної інфраструктури безальтернативним є одномодове оптоволокно OS2 в оболонці LSZH, що забезпечує необмежену смугу пропускання та пожежну безпеку.

В умовах високих електромагнітних завад (промислові цехи, ліфтові шахти) необхідно використовувати виту пару STP або повністю переходити на оптоволокно, щоб гарантувати стабільність відеопотоку.

Розуміння фізичних принципів роботи коаксіальних, мідних та оптичних трактів дозволяє проектувати системи відеоспостереження, які не лише відповідають сьогоднішнім вимогам, а й мають достатній запас для модернізації у майбутньому. Ключовим фактором успіху залишається використання високоякісних матеріалів – чистої міді, надійного екранування та хімічно стійких оболонок.

Методика визначення максимально допустимої довжини кабелю за критерієм надійної синхронізації. Надійність функціонування систем аналогового та гібридного відеоспостереження залежить від цілісності сигналу синхронізації, який забезпечує часовий зв’язок між джерелом зображення (камерою) та пристроєм обробки (відеореєстратором або монітором). Хоча деградація амплітуди яскравості або насиченості кольорів часто розглядається як основна ознака подовження кабельної лінії, збій системи зазвичай відбувається саме через втрату синхронізації, що проявляється у вигляді «зриву» кадру, горизонтального зсуву або повної відсутності відеосигналу. Визначення максимально допустимої довжини кабелю вимагає розуміння фізичних процесів розповсюдження електромагнітних хвиль у провідниках, механізмів загасання на високих частотах та архітектури вузлів сепарації синхроімпульсів у приймальному обладнанні.

Загасання сигналу є фізичним обмеженням будь-якого коаксіального тракту, що вимірюється в децибелах на одиницю довжини (зазвичай на 100 футів або 30 метрів). Чим вища частота сигналу, тим вищі втрати, що пояснює складність передачі зображення у форматі 4K по коаксіальним лініям.

Кабель має реальні втрати, тому відбувається поділ відеосигналу між кабелем і вхідним опором. Допустиме значення втрат 6 дБ – це прийнятна величина втрат при передачі відеосигналу.

Щоб відеосистеми працювали стійко потрібно щоб рівень видеосигналу був не менше 0,5 В (тобто зменшення напруги на навантаженні в 2 рази в порівнянні зі стандратною 1 В, по напрузі це відповідає 6 дБ).

Наприклад, допустиме зменшення розмаху відеосигналу на навантаженні не більше ніж в 2 рази забезпечується граничним значенням сумарного активного опору коаксіального кабелю, що не повинне перевищувати $R_{каб}$=150 Ом (або 75 Ом без втрат відеосигналу).

Максимально допустима довжина коаксіального кабелю за критерієм надійної синхронізації:

$$L = \frac{150}{R_{пог}}, \tag{5.1}$$

де 150 – граничне значення сумарного активного опору коаксіального кабелю, Ом, $R_{пог}$ – сумарний погонний опір центральної жили і оплітки, Ом.

Наведемо приклади визначення граничної довжини кабелю.

Кабель CV-K: Жила 14,8 Ом/100м і оплітка 5,26 Ом/100м. Визначаємо погонний опір: R=0,148+0,0526=0,2006 Ом/м. L = 150: 0,2006 = 747 м.

Кабель Rexant: Опір жили 90 Ом/100м і оплітки в 13 Ом/100м. R = 0,9 + 0,13 = 1,03 Ом / м. L = 150:1,03 = 145 м.

Кабель КВК-П-2: житла 23 Ом/100м і оплітки 2,7 Ом/100м. R = 0,23 + 0,027 = 0,257 Ом / м. L = 150: 0,257 = 583 м.

Роз'єми відеотрактів та їх призначення. Еволюція інтерфейсів відеотрактів відображає фундаментальні зміни в методах обробки, передачі та візуалізації інформації. Від перших аналогових стандартів, що базувалися на принципах електронно-променевих трубок, до сучасних пакетних протоколів, здатних транслювати зображення з роздільною здатністю 16K, кожен роз'єм створювався як відповідь на технічні виклики свого часу. Розуміння фізичних параметрів, протокольної логіки та експлуатаційних особливостей цих інтерфейсів є важливим для забезпечення цілісності сигналу в складних мультимедійних системах.

Композитне відео стало першим масовим стандартом, що об'єднав усі компоненти відеосигналу – яскравість, кольоровість та синхронізацію в один електричний потік. Фізично цей інтерфейс найчастіше реалізовувався через роз'єм RCA, де жовтий колір маркував відеоканал.

Стандарт S-Video з'явився як відповідь на недоліки композитного сигналу. Його ключовою інновацією стало фізичне розділення інформації про яскравість та колір на два окремі провідники всередині одного кабелю. Це дозволило уникнути процесу фільтрації, необхідного для композитного сигналу, що значно підвищило чіткість зображення та точність передачі кольорів.

Найпоширенішим роз'ємом для S-Video став 4-піновий Mini-DIN. Незважаючи на покращення якості, S-Video залишався стандартом стандартної чіткості і не підтримував прогресивну розгортку. В індустрії цей інтерфейс використовувався переважно в напівпрофесійному обладнанні, такому як S-VHS плеєри та ранні цифрові камери.

Розроблений IBM у 1987 році, інтерфейс VGA став стандартом де-факто для персональних комп'ютерів на понад два десятиліття. Використовуючи 15-контактний роз'єм High-Density D-sub (DE-15), він передає аналогові сигнали трьох основних кольорів (RGB) разом із сигналами горизонтальної та вертикальної синхронізації.

Технічно VGA був розрахований на роботу з ЕПТ-моніторами, де аналогова природа сигналу відповідала фізиці управління електронним променем. Хоча VGA теоретично підтримує роздільну здатність до Full HD (1920x1080), на високих частотах сигнал стає вкрай чутливим до якості екранування кабелю. Будь-які електромагнітні наведення проявляються у вигляді розмиття або тремтіння зображення. З появою цифрових РК-панелей

необхідність подвійного перетворення (цифра-аналог у відеокарті та аналог-цифра в моніторі) стала вузьким місцем, що призвело до розробки цифрових стандартів.

Цифровий візуальний інтерфейс (DVI), випущений у 1999 році групою Digital Display Working Group, мав на меті стандартизацію передачі цифрового відео без втрат якості, притаманних аналоговим трактам. DVI базується на протоколі, який мінімізує кількість переходів між станами сигналу для зменшення електромагнітного випромінювання.

Однією з унікальних характеристик DVI стала його гібридна природа. Роз'єм був сконструйований таким чином, щоб підтримувати як цифрову, так і аналогову передачу, що полегшувало перехід від VGA.

HDMI став найбільш успішним інтерфейсом у сегменті споживчої електроніки. З'явившись наприкінці 2003 року, він запропонував революційну для свого часу концепцію: передачу нестисненого цифрового відео та багатоканального аудіо високої чіткості через один компактний кабель.

На відміну від HDMI та DVI, які використовують безперервний потік даних, DisplayPort, розроблений асоціацією VESA, базується на пакетній передачі даних. Це робить його ближчим за архітектурою до протоколів комп'ютерних мереж, дозволяючи вбудовувати різні типи даних у загальний потік.

Поява роз'єму USB Type-C змінила парадигму підключення периферії, об'єднавши передачу живлення, даних та відео в одному овальному роз'ємі.

Розділення коаксіальних радіочастотних кабелів здійснюють з використанням «байонетних» (байонетна фіксація – встановити та провернути) роз'ємів типу BNC. За виконанням та функціональним призначенням даний тип роз'ємів поділяють на: BNC-роз'єм, BNC Т-конектор, BNC баррел-конектор, BNC-термінатор. Зовнішнє їх представлення та призначення подано в таблиці 5.2.

Таблиця 5.2 – Радіочастотні роз'єми BNC

Зовнішній вигляд	Призначення
	BNC роз'єм кріпитися на відповідних торцях коаксіального кабелю і використовують його для підключення до апаратури.
	BNC Т-конектор являє собою трійник, що забезпечує поділ відеосигналу на два споживача. Амплітуда напруги в кожному напрямку зменшиться в 2 рази.
	BNC баррел-конектор використовують для подовження кабельних ліній.
	BNC-термінатор (узгоджувач) являє собою узгоджене за хвильовим опором навантаження. Застосовується на довгих лініях.

Для підключення до обладнання оптико-волоконний кабель використовують роз’ємами LC, SC і FC (рис. 5.3).

Рисунок 5.3 – Роз’єми для підключення оптико-волоконного кабелю

Для збільшення швидкості передачі до 10 Гбіт і сумісності з 10GE мережами розроблені і починають активно застосовуватися моделі SFP +.

Оптичний бюджет або енергетичний потенціал лінії враховує всі втрати, присутні на ній.

При передачі інформації по оптико-волоконному кабелю втрати відбуваються в місцях з’єднань і мають наступні значення:

– конектори - від 0,3 дБ;

– місця зварювання - від 0.02 дБ;

– механічні з’єднувачі - від 0,7 дБ.

Конектори типу FC використовують в одномодових (одне оптичне волокно) системах.

Для фіксації конектора FC на розетці використовується накидна гайка з різьбою М8х0,75.

Конектори типу FC стійкі до впливу вібрацій і ударів, що дозволяє застосовувати їх на рухомих об’єктах, а також на спорудах, розташованих поблизу залізниць.

Конектори типу SC використовують в одномодових і багатомодових системах.

Корпус конектора SC в поперечному перерізі прямокутний. Наконечник не пов’язаний жорстко з корпусом і хвостовиком.

Підключення та відключення конектора SC здійснюється лінійно (push-pull), що оберігає наконечники конекторів від прокручування один щодо одного в момент фіксації в адаптері.

До недоліків конекторів SC слід віднести меншу механічну міцність у порівнянні з конекторами типів FC. Це обмежує застосування конекторів типу SC на рухомих об’єктах.

Конектори з одномодовим волокном зазвичай мають блакитний колір, а з багатомодовим сірий.

Конектори типу LC – малогабаритний варіант SC-конекторів. Він також має прямокутний перетин корпусу.

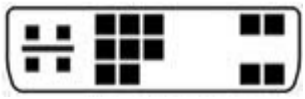
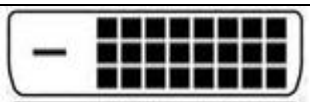
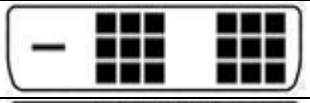
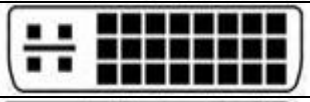
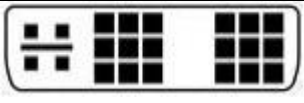
Конструкція виповнюється на пластмасовій основі і забезпечена засувкою. Внаслідок цього підключення конектора здійснюється складним чином.

Наконечник виготовляється з кераміки і має діаметр 1,25 мм.

Зустрічаються як багатомодові, так і одномодові варіанти цих конекторів.

Зовнішній вигляд роз'ємів для передачі відеосигналу на монітор та їх призначення подано в таблиці 5.3.

Таблиця 5.3 – Роз'єми моніторів

Зовнішній вигляд	Назва та призначення
	BNC – основний тип з'єднання для передачі композитного відеосигналу CVBS
	VGA - (Video Graphics Array) – компонентний аналоговий інтерфейс. Всі сигнали на контактах з TTL рівнем. Тільки приймає відео (звук відсутній).
	HDMI – (High Definition Multimedia Interface) інтерфейс для передачі відеосигналу високої чіткості і звуку.
	S-Video – (Separate Video) компонентний аналоговий відеоінтерфейс використовується тільки для передачі сигналу телебачення стандартної чіткості і непридатний для HDTV. Для передачі звуку необхідний окремий кабель.
	RCA - компонентний аналоговий відеоінтерфейс.
	DVI (digital visual interface) - Компонентний аналого-цифровий інтерфейс. DVI-A - тільки аналоговий сигнал.
	DVI-D (Dual link) - тільки цифровий сигнал.
	DVI-D (Single link) - тільки цифровий сигнал.
	DVI-I (Dual link) - аналоговий і цифровий сигнал.
	DVI-I (Single link) - аналоговий і цифровий сигнал.

Методики монтажу роз'ємів BNC та RJ-45. Для оброблення коаксіального кабелю при обтискання роз'ємів рекомендується використовувати спеціальні кліщі і пристрої для обрізки.

Пристрій для обрізки кабелю складається з трьох лез (рис. 5.4):

– леза, що прорізає кабель до центрального провідника;

– леза, що перерізає зовнішню ізоляцію і екран кабелю;

– леза, що прорізає тільки зовнішню ізоляцію кабелю.

Коаксіальний кабель затискають в роз'ємі і роблять кілька обертів, забезпечуючи обрізку непотрібних частин кабелю.

Опресовування роз'єму BNC (рис. 5.6) на кабелі здійснюють наступним чином:

1. На центральний провідник кабелю надіти центральний контакт роз'єму.

2. Вставити центральний контакт, надітий на кабель в обтискний пристрій (рис. 5.5) і обтиснути його.

3. Одягти на кабель фіксуючу трубку.

4. Вставити кабель в роз'єм, попередньо розпушивши екран.

5. Засувати трубку на роз'єм.

6. Вставити фіксуючу трубку в пристрій обтиску і обтиснути його.

Рисунок 5.4 – Ніж для обрізки коаксіального кабелю

Рисунок 5.5 – Кліщі для обтискання роз'ємів BNC

Рисунок 5.6 – BNC роз’єм у розібраному стані (обтискний)

Коаксіальні кабелі можна обробляти за допомогою роз’ємів F типу, а підключатися до обладнання через перехідник F-BNC (рис. 5.7).

Роз’єми F типу зручні в застосуванні за рахунок того, що при роботі з ними відсутня потреба в додаткових інструментах.

Рисунок 5.7 – Приклад використання роз’єму F типу та перехідника F-BNC

Центральний контакт роз’єму виконує центральна жила коаксіального кабелю, а сам F роз’єм просто накручується на коаксіальний кабель. Якщо використовується F роз’єм під обтиск, то необхідно обтиснути його.

Для оброблення кабелю типу «вита пара» з 4-ма парами провідників використовують конектори 8P8S, які ще мають назву – RJ-45. Для їх опресовування застосовують спеціальні кліщі (рис. 5.8).

Рисунок 5.8 – Кліщі для опресування конектора 8P8S

Даний кабель можна обтикати декількома способами, які залежать від конкретного випадку.

Варіант №1 – прямий 8-провідникової кабель типу вита пара.

Прямий спосіб обтискання використовується, коли потрібно з’єднати два пристрої:

– з одного боку - ПК, принтер, копіювальний апарат, телевізор;

– з іншого боку - роутер, комутатор.

Особливістю способу вважається однакове обжимання обох кінців дроту, з цієї ж причини спосіб і називається прямим.

Існує два взаємозамінних типи – А і В.

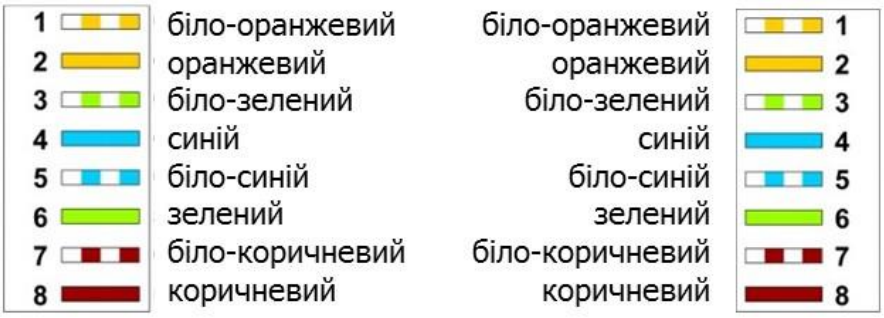


Рисунок 5.9 – Схема розмінування 8-ми жильного кабелю для прямого з’єднання комп’ютера з пристроєм комутації

Тип А відрізняється від типу В розташуванням провідників, що знаходяться на 1, 2, 3 і 6 позиціях, тобто біло-зелений/зелений міняють місцями з біло-помаранчевим/помаранчевим.

Можна здійснювати обтискання обома способами, якість передачі даних від цього не зміниться. Головне – дотримуватися по черговість жил.

Варіант №2 - 8-провідникової кросове (перехресний спосіб).

Перехресне обтискання може використовуватись, якщо потрібно з’єднати два стаціонарних комп’ютера, два ноутбука або два комутуючих пристрої.

Кросовер застосовується все ж рідше, так як сучасне обладнання вміє в автоматичному режимі визначати тип кабелю і при необхідності міняти подачу сигналу. Нова технологія називається авто-MDIX. Однак частина пристроїв, що справно функціонує роками, може з часом потребувати повторного перехресного обтискання.

При перехресному обтисканні зберігається можливість використання типів А і В.

Рисунок 5.10 – Схема розмінування 8-ми жильного кабелю для перехресного з’єднання

Щоб задіяти тип А, необхідно поміняти всі ті ж 4 позиції: 1, 2, 3 і 6 – біло-зелений/зелений провідники з біло-помаранчевим/помаранчевим.

Проводи кабелю не зачищають вставляють в роз'єм RJ-45 і обжимають.

При обтиску 4-х жильного кабелю, кольори йдуть, також, як і при 8 жильному обтиску, але використовують тільки 1, 2, 3 і 6 контакти.

Інжектори, сплітери та репітери відеосигналу. Сучасна архітектура CCTV вимагає безпрецедентної гнучкості та надійності в управлінні потоками даних високої чіткості. В умовах стрімкої цифровізації виникає потреба у подоланні фізичних обмежень стандартних інтерфейсів передачі відеосигналу. Основними інструментами для вирішення цих завдань є інжектори, сплітери та репітери – пристрої, що забезпечують цілісність сигналу, його розподіл між множинними споживачами та живлення активних компонентів мережі.

Для підключення IP камери до мережного обладнання у випадках, коли камера або комутатор не підтримує режим PoE, використовують інжектори або сплітери.

Інжектор – пристрій, що забезпечує передачу по UTP кабелю разом з потоком даних і напругу живлення (рис. 5.11).

Рисунок 5.11 – Інжектор для живлення по витій парі

Сплітер (розподілювач) – це пристрій, призначений для клонування вхідного сигналу з одного джерела на кілька виходів. У цифрових системах цей процес включає не лише електричне копіювання сигналу, а й складну логіку узгодження параметрів між джерелом та всіма підключеними дисплеями.

Таким чином, сплітер дозволяє відокремити напругу живлення від потоку даних, переданих в UTP кабелі, для підключення їх до відповідних входів IP камери або мережевого устаткування.

Пасивні сплітери, часто представлені у формі Y-подібних кабелів, позбавлені внутрішньої електроніки для підсилення (рис. 5.12). Вони розділяють вхідну енергію сигналу між виходами, що призводить до падіння напруги та невідповідності імпедансу. Такі пристрої можуть працювати лише на дуже коротких відстанях (до 1-2 метрів) та з низькими роздільними здатностями. Більше того, пасивні розгалужувачі не дозволяють моніторам коректно ідентифікувати себе джерелу через канал DDC (Display Data Channel), що часто робить передачу зображення неможливою.

Рис. Пасивний сплітер

Активні сплітери, які ще називають дистриб’ютор-ампліфікаторами, використовують зовнішнє живлення для повної регенерації кожної копії сигналу.

Основним ворогом стабільної передачі на великі відстані є загасання та фазове тремтіння. У мідних кабелях ці явища зумовлені ємнісним опором та ефектом близькості, що призводить до розмиття фронтів цифрових імпульсів. Коли рівень сигналу падає нижче порогу розпізнавання приймачем, виникають помилки бітів, які проявляються у вигляді «снігу», мерехтіння або повної втрати зображення.

Репітери (повторювачі) розроблені спеціально для боротьби з цими явищами. На відміну від простих перехідників, активний репітер виконує функцію еквалізації та відновлення тактової частоти. Він приймає ослаблений сигнал, очищує його від наведених шумів та підсилює до стандартних рівнів перед подальшою трансляцією. Це дозволяє значно розширити максимальну довжину кабельної траси, яка для пасивного HDMI кабелю зазвичай обмежена 10-15 метрами для роздільної здатності 4K.

Коли довжина траси перевищує можливості репітерів, застосовуються системи подовження, які конвертують відеосигнал для передачі через альтернативні середовища.

Живлення камер по PoE незважаючи на зручність і перспективність має певне обмеження. Довжина кабелю, який транслює відеопотік і напруга живлення від комутатора до камери відеоспостереження, обмежується 100 метрами (92 м). Цей поріг можна перебороти декількома способами:

– застосуванням PoE репітерів (повторювачів);

– використанням конвертерів VDSL2.

Репітери, або повторювачі, підключаються через кожні 90-100 метрів і дозволяють значно збільшити протяжність лінії від комутатора до відеокамери (рис. 5.13). Конвертери VDSL2 або пристрої Ethernet Extender призначені для підключення камер високої роздільної здатності по кабелю на відстані більше 100 метрів. Максимальна довжина сполучної лінії із застосуванням провідників перетином 0,5 мм може досягати 1500 метрів.

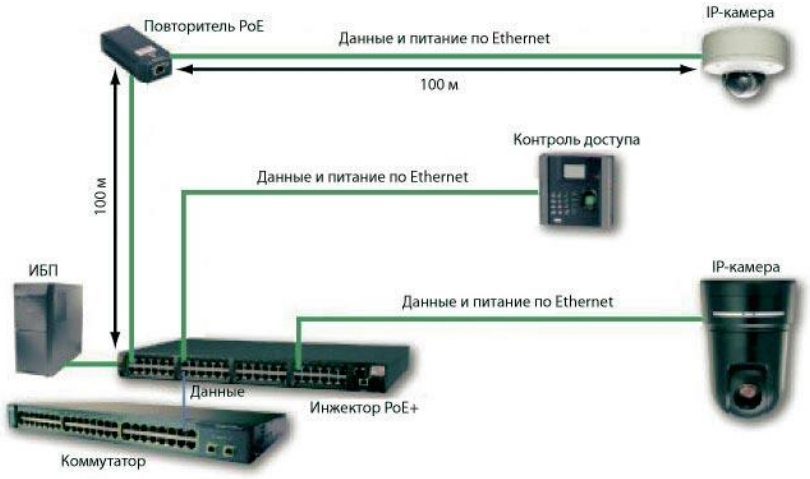


Рисунок 5.13 – Приклад використання повторювача

Можна подати напругу живлення на IP відеокамеру без застосування технології PoE. Для цього так само існує кілька способів. Найпростіший спосіб подати живлення на IP камери по витій парі і вимагає невеликої переробки LAN кабелю. Інжектор для живлення по витій парі.

Справа в тому, що дві виті пари такого кабелю не використовуються для передачі сигналу, і їх можна використовувати для подачі напруги живлення від окремого джерела на IP камеру. Для цього необхідно розрізати оболонку кабелю, і вивести назовні дві вільні пари. Потім провідники пар з'єднуються паралельно для збільшення перетину дроту. Після цього від зовнішнього джерела постійної напруги можна подавати живлення на IP камеру. При перетині пари 0,4 мм^2 (один провідник 0,2 мм^2) можна розташувати відеокамеру від джерела живлення на відстані до 70-80 метрів при споживаної потужності не більше 5 Вт.

Комутатори, маршрутизатори. Сучасні системи відеоспостереження пройшли шлях від локальних аналогових замкнутих контурів до складних розподілених IP-мереж, де комутатори та маршрутизатори відіграють роль центральної нервової системи. Перехід на цифрову передачу даних вимагає від інженерів та архітекторів систем безпеки розуміння мережевих стандартів, оскільки якість зображення, надійність архіву та захищеність від кіберзагроз тепер безпосередньо залежать від конфігурації активного мережевого обладнання. Використання професійних комутаторів дозволяє не лише забезпечити передачу гігабайт відеоінформації в реальному часі, але й вирішити питання централізованого живлення кінцевих пристроїв, що є важливим фактором при розгортанні масштабних систем.

Часто плутають назви хаб, комутатор, маршрутизатор, роутер, звалюючи всі терміни до купи. З якої потім виникає плутанина, і замовник просто не може отримати правильно налаштовану систему IP-відеоспостереження.

Хаб – пристрій без мікросхем пам'яті та процесора, що служить для передачі широкоформатного сигналу. Наприклад, сигнал від комп'ютера на принтер буде переданий через всі порти, і тільки принтер відгукнеться та

виконає команду. Мережа ж буде перевантажена зайвим потоком інформаційних пакетів. Сьогодні хаби практично не виробляються.

Маршрутизатор або роутер – пристрій для комутації IP-мереж. Тобто, він відповідає за передачу IP-трафіку між мережами, надання бездротового зв'язку WiFi, роботу сервісів DHCP, NAT тощо. Зрозуміло, що на борту маршрутизатора встановлено процесор, ПЗП та інші елементи смартпристроїв. Завдяки маршрутизатору локальна система IP-відеоспостереження має вихід до інтернету.

Комутатор (світч) – це розумний пристрій, тобто у ньому встановлено процесор. Комутатор визначає MAC-адреси пристроїв і вже до них «прив'язує» трафік. MAC-адреси пристроїв зберігаються в енергонезалежній пам'яті (ПЗП). Тобто, всі маршрути передачі даних між пристроями будуть миттєво відновлені при подачі живлення на пристрій. Таким чином, комутатор домагається розвантаження мережі від зайвих інформаційних пакетів, і прискорює трафік.

Комутатори (залежно від моделі) підтримують швидкість передачі даних 10, 100 Мбіт/с, 1 Гбіт/с і більше. Візуально цей параметр визначити складно без вивчення техпаспорта на пристрій. Хоча позначення 10/100 Мбіт/с можна побачити найчастіше на корпусі комутатора біля портів.

PoE-комутатори є вже невіддільною частиною цифрової системи відеоспостереження для дому і тим більше для великого промислового чи комерційного підприємства. Ці пристрої призначені для побудови розгалуженої схеми IP-відеоспостереження, організації стійкої комунікації між пристроями, розвантаження комутаційних ліній від зайвого трафіку.

Технологія PoE стала фундаментальним стандартом для індустрії відеоспостереження, дозволяючи передавати електричну енергію та цифрові дані через один кабель «вита пара» (PoE розшифровується як Power over Ethernet – живлення через інтерфейс передачі даних Ethernet). Це не тільки знижує витрати на кабельну продукцію, але й дозволяє створювати гнучкі системи, де камери можуть бути встановлені у важкодоступних місцях без необхідності підведення окремих ліній 220В.

Щоб зробити правильний вибір PoE-комутатора, потрібно оцінити кілька пунктів: кількість портів, тип комутатора, швидкість передачі даних, потрібна потужність споживання, відстань до камер і потрібна напруга живлення споживача.

Кількість портів залежить від кількості цифрових камер, які будуть працювати у системі відеоспостереження. На практиці застосовують пристрої із запасом кількості портів до 30% для розширення та подальшої модернізації системи відеоспостереження.

Є пристрої некеровані та керовані. Перші використовують мережеві налаштування «як є». Другі дозволяють фільтрувати трафік, здійснювати контроль доступу, моніторити та керувати мережевими налаштуваннями SNMP, підвищувати якість обслуговування QoS, працювати з VLAN тощо. До керованих PoE-комутаторів відносять SMART комутатори (пристрої з обмеженими функціями керованих).

Яку швидкість може підтримувати конкретна модель комутатора, можете визначити рядок 10/100/1000Base-T (наприклад) у паспорті пристрою. Розраховуйте необхідну швидкість на портах пристрою з урахуванням роздільної здатності камери. Загальна швидкість обчислюється шляхом підсумовування цього параметра всіх камер.

Знаючи вимоги камер по потужності, можна обчислити необхідну потужність PoE-комутатора. На практиці камери можуть споживати від 4 до 95 Вт (проста IP-камера і роботизована PTZ, з моторизованим об'єктивом). Щоб розібратися, яку потужність може надати комутатор на портах, використовуйте розшифровку стандартів пристрою:

– стандарт PoE IEEE 802.3af (тип 1) – потужність на портах 15.4 Вт;

– стандарт PoE IEEE 802.3at (тип 2) PoE+ – потужність на портах 30 Вт;

– стандарт PoE IEEE 802.3bt/UPoE (тип 3) PoE++ – потужність на портах 60 Вт;

– стандарт PoE IEEE 802.3bt (тип 4) PoE++ – потужність на портах 90-95 Вт.

Стандарт 802.3af, представлений у 2003 році, був достатнім для перших поколінь IP-камер та телефонії. Проте поява камер з потужним інфрачервоним підсвічуванням та поворотними механізмами вимагала впровадження стандарту 802.3at (PoE+), який подвоїв доступний бюджет енергії до 30 Вт на порт. Найсучасніший стандарт 802.3bt використовує всі чотири пари провідників у кабелі, що дозволяє передавати до 90-100 Вт. Це важливо для мультисенсорних камер або камер, що працюють у екстремальних кліматичних умовах, де значна частина енергії витрачається на внутрішній обігрів корпусу.

Тут важливим аспектом є фізика передачі енергії. Втрати потужності в кабелі обумовлені його опором і описуються законом Джоуля-Ленца: $P=I^2xR$. При використанні стандарту 802.3bt, перехід на використання чотирьох пар замість двох дозволяє знизити опір R та підвищити ефективність передачі енергії, зменшуючи нагрів кабелю в пучках, що особливо важливо при щільному монтажі в серверних стійках.

При проєктуванні живлення беріть реальні значення, які враховують втрати кабелю. Вони на 15-20% менше зазначених виробником.

Вибір категорії кабелю безпосередньо впливає на максимальну відстань та стабільність роботи системи. Кабель категорії Cat5e є мінімально допустимим, але для систем з використанням PoE+ та PoE++ рекомендується перехід на Cat6 або Cat6a. Категорія Cat6 має менший опір і кращі характеристики теплопровідності завдяки більшому перерізу мідних жил. Це дозволяє підтримувати стабільну роботу потужних PTZ-камер на великих відстанях без критичного падіння напруги, яке може призвести до циклічних перезавантажень пристрою при активації ІЧ-фільтра або приводу двигуна. Для передачі 90 Вт за стандартом 802.3bt використання Cat6a стає індустріальним стандартом, оскільки цей кабель розрахований на вищі частоти та краще розсіювання тепла.

Маршрутизатор у системі відеоспостереження виконує роль шлюзу, що з'єднує локальну ізольовану мережу камер із зовнішнім світом. Основна проблема полягає у забезпеченні зручного доступу для користувачів при збереженні максимальної закритості системи від зовнішніх атак.

Проектування мережевої частини системи відеоспостереження вимагає комплексного підходу, що поєднує знання електротехніки, мережевих протоколів та кібербезпеки. Для створення сучасної та надійної системи рекомендується:

1. Використовувати керовані комутатори (L2/L2+) як мінімальний стандарт, що дозволяє розділити трафік через VLAN, налаштувати QoS та забезпечити віддалену діагностику системи;
2. Забезпечити запас потужності PoE і додавати 20% резерву для запобігання перевантаженню блоку живлення комутатора;
3. Впроваджувати багаторівневу безпек;
4. Обирати обладнання з функціями автоматизації;
5. Розраховувати пропускну здатність з урахуванням пікових навантажень.

Комутатори та маршрутизатори сьогодні є не просто допоміжним приладдям, а фундаментом, на якому будується вся інтелектуальна система безпеки. Тільки професійна мережева інфраструктура здатна розкрити весь потенціал сучасних камер та аналітичних алгоритмів на базі штучного інтелекту.

Топології IP відеоспостереження. У сучасному ландшафті систем безпеки перехід від аналогових систем до мережевого (IP) відеоспостереження став фундаментальним зрушенням, яке вимагає від інженерів та проектувальників глибоких знань у галузі побудови комп'ютерних мереж. Вибір топології – способу з'єднання камер, комутаторів та серверів – є рішенням, що визначає життєздатність системи, її здатність до розширення, надійність у критичних ситуаціях та загальну вартість володіння. Мережева топологія не просто описує схему розташування кабелів; вона є логічним фундаментом, на якому базується якість передачі відеопотоків, швидкість реакції на інциденти та стійкість до мережевих збоїв.

При аналізі систем IP-відеоспостереження необхідно розрізняти фізичну та логічну топології. Фізична топологія описує реальне розміщення кабелів, маршрутизаторів та кінцевих пристроїв у просторі. Це «залізо», яке можна побачити в дата-центрах або на стінах будівель. Логічна топологія, навпаки, визначає шлях, яким дані фактично подорожують мережею. Часто виникають ситуації, коли фізично мережа побудована як зірка (всі камери підключені до одного центру), але логічно вона працює як шина або кільце залежно від налаштувань мережевих протоколів.

Розуміння обох рівнів є необхідним для ефективного пошуку несправностей. Фізична структура може бути бездоганною, але неправильно налаштована логічна топологія може призвести до колізій, затримок або втрати пакетів, що у відеоспостереженні означає втрату критично важливих секунд

запису. Сучасні мережеві дизайни повинні враховувати такі фактори, як обсяг трафіку, вимоги до доступності системи та фінансові обмеження

У проектуванні систем відеоспостереження використовуються шість основних топологій, кожна з яких має власні переваги та ризики.

Топологія «зірка» є найбільш поширеною в сучасних офісних та локальних мережах. Кожна камера підключається безпосередньо до центрального пристрою, зазвичай комутатора або маршрутизатора. Якщо в центрі стоїть сервер – це «активна зірка», якщо комутатор – «пасивна».

Переваги цієї схеми для відеоспостереження важко переоцінити. По-перше, вихід з ладу однієї камери або пошкодження її кабелю ніяк не впливає на решту системи. По-друге, всі точки підключення зосереджені в одному місці, що значно полегшує контроль та локалізацію несправностей. Кожен вузол має виділений канал зв’язку, що усуває проблему колізій і забезпечує стабільну пропускну здатність для відеопотоків високої чіткості.

Проте «зірка» має і свою «ахіллесову п’яту»: центральний вузол є єдиною точкою відмови. Якщо комутатор виходить з ладу, вся система припиняє роботу. Також ця топологія вимагає найбільшої кількості кабелю, оскільки від кожної камери потрібно тягнути окрему лінію до центру, що здорожує інсталяцію, особливо на великих об’єктах.

У топології «шина» всі пристрої підключаються до одного центрального кабелю, який називається магістраллю або шиною. Цей метод був популярним на світанку мережевих технологій завдяки дешевизні та простоті розводки. Сигнал від однієї камери поширюється в обидві сторони і зчитується потрібним отримувачем. На кінцях шини обов’язково встановлюються термінатори для поглинання електричних сигналів.

Для сучасного відеоспостереження шина практично не застосовується через критичні недоліки. Будь-яке пошкодження центрального кабелю паралізує всю мережу. Крім того, пропускна здатність каналу поділяється між усіма учасниками; лише одна камера може передавати дані в певний момент часу. У системах з десятками камер високої роздільної здатності це миттєво призводить до колапсу через колізії та перевантаження. Хоча вона залишається в деяких простих лабораторіях або застарілих коаксіальних мережах, професійні проекти її уникають.

У кільцевій мережі кожен пристрій має два зв’язки з сусідами, утворюючи замкнутий шлях для даних. Дані передаються по колу, зазвичай в одному напрямку. У застарілих системах використовувався «маркер» – спеціальний пакет, який давав право на передачу даних, що забезпечувало впорядкованість трафіку.

Основним недоліком класичного кільця є те, що вихід з ладу одного вузла розриває весь ланцюг. Проте сучасні комутатори використовують логічні методи блокування одного порту для запобігання «кільцевим штормам», і миттєво розблоковують його при обриві основної лінії. Це забезпечує резервний шлях без значних витрат на прокладку дублюючих кабелів від кожної точки до центру, як у «зірці».

Топологія «сітки» передбачає, що кожен вузол може з’єднуватися з кількома іншими, створюючи багато шляхів для передачі даних. Це найдорожчий, але й найнадійніший варіант. У дротових мережах він зустрічається рідко через колосальні витрати на кабель, але став справжнім проривом у бездротовому відеоспостереженні.

У великих портах, на складах або відкритих територіях, де неможливо прокласти кабель, бездротові Mesh-вузли діють як динамічні ретранслятори. Кожен вузол не тільки передає відео зі своєї камери, але й допомагає сусідам «дотягнутися» до шлюзу.

Головна перевага тут – усунення «сліпих зон». Якщо між камерою та центром з’явилася перешкода (наприклад, металевий контейнер), Mesh-мережа автоматично знайде інший шлях через сусідній вузол. Проте існують і обмеження: кожен «стрибок» знижує пропускну здатність.

Топологія «зірка» залишається найбільш популярною завдяки своїй передбачуваності та простоті керування. Проте у масштабних проектах «зірки» на поверхах зазвичай об’єднуються у «дерево» (рис. 5.14), де поверхові комутатори підключаються до центрального комутатора. Такий підхід дозволяє локалізувати трафік всередині сегментів та забезпечити гігабітні або десятигігабітні магістралі для агрегованих потоків.

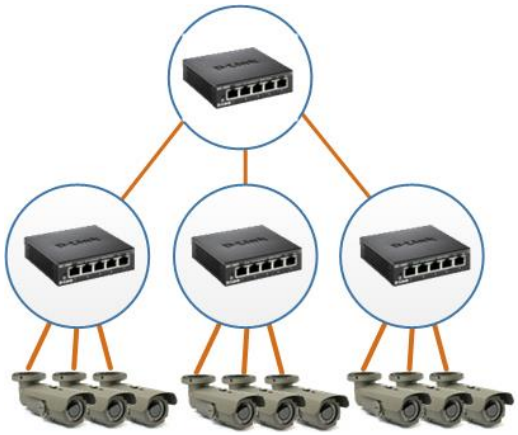


Рисунок 5.14 – Топологія «дерево»

У випадках, коли камери розташовані вздовж доріг або на периметрі великого заводу, прокладання окремого кабелю від кожної камери до центру є недоцільним. Тут застосовується кільцева топологія, де комутатори з’єднуються послідовно в петлю. Для усунення логічних петель та забезпечення миттєвого перемикання при обриві використовуються спеціальні протоколи.

Протокол Rapid Spanning Tree Protocol (RSTP) є вдосконаленням класичного STP і забезпечує відновлення мережі за 1-2 секунди. Хоча це швидко для звичайної передачі даних, для відеоспостереження така затримка може призвести до втрати ключових кадрів та розриву сесії запису.

Альтернативою є протокол Ethernet Ring Protection Switching (ERPS), регламентований стандартом ITU-T G.8032. Він розроблений спеціально для кільцевих мереж і гарантує час відновлення менше 50 мілісекунд. Це настільки

швидко, що відеопотік продовжує транслюватися без видимих затримок або переривань. ERPS також дозволяє будувати складні багатокільцеві структури, що робить його ідеальним для проектів «Безпечне місто».

Топологія інформаційної мережі створюється на основі інформації про трьох її складових:

– величина максимального потоку, який створений всіма відеокамерами системи відеоспостереження;

– величина максимального потоку, який здатна передавати мережа (пропускна здатність);

– величина максимального потоку на один порт, який здатне забезпечити мережеве обладнання.

Проектування мережі системи IP відеоспостереження потрібно починати із визначення максимальних інформаційних потоків, створюваних усіма відеокамерами системи.

Результуюче значення потоку від кожної камери залежить від її роздільної здатності, від використовуваних кодеків стиснення, обраної частоти кадрів, інтенсивності руху в полі зору камери.

Крім зображення камера може транслювати і звук, що не суттєво, але, тим не менш, збільшує загальний трафік.

Знаходження сумарного значення максимальних інформаційних потоків на початковому етапі проектування дозволяє:

– визначити кількість інформаційних підмереж, за допомогою яких можна доставити весь обсяг відео та аудіо інформації від камер до сервера (серверів);

– розробити структуру і склад інформаційної підмережі.

Методика визначення загальної швидкості інформаційного потоку. Для визначення швидкості інформаційного потоку від кожної камери можна використовувати калькулятор або скористатися таблицями.

Наведені в таблиці швидкості потоків, відповідають інтенсивності руху в кадрі вище середнього значення при ступені стиснення, який не створює видимі артефакти на зображенні.

Вибір кодека потокового (H.264) або покадрового (MJPEG) стиснення визначається завданнями, що стоять перед відеокамерою і необхідністю детального (покадрового) перегляду записаного архіву.

У випадках, коли інтенсивність руху перед відеокамерою може істотно збільшитися, наприклад, на станціях метрополітену в години пік, швидкість потоку для кодека MJPEG може зрости на 15-20%, а для H.264 до двох разів і більше.

Сумарна швидкість інформаційних потоків від всіх IP відеокамер визначається як:

$$B = \sum_{i=1}^{n} \sum_{j=1}^{k} V(i, j) \quad , \tag{5.2}$$

де B – сумарна швидкість потоків від всіх відеокамер; V (i, j) – швидкість j-го «потоку» від i-ой відеокамери; k – загальна кількість «потоків», переданих камерою; n – загальна кількість IP відеокамер.

Термін потоки, використовуваний в меню IP камер для завдання характеристик додатковим потокам і вибору їх кількості, взято в лапки. Пов'язано це з тим, що від камери йде всього один цифровий потік. При формуванні цього потоку інформація про основний і додаткових «потоках» буде перетворюватися в пакети зі своїми адресами доставки. І вже ці пакети в загальному інформаційному потоці передаються по мережі.

Для збільшення надійності роботи мережі в частині запобігання непередбачених перевантажень, від зміни інтенсивності руху перед відеокамерами, доцільно розрахункові значення швидкості потоку збільшити на 25-30 відсотків.

Методика вибору пропускної здатності мережі. Пропускна здатність мережі визначається обраним середовищем передачі сигналу. Як середовище передачі даних використовуються різні види кабелів: коаксіальний кабель, кабель на основі екранованої і неекранованої витої пари і оптоволоконний кабель.

Найбільш популярним видом середовища передачі даних на невеликі відстані (до 100 м) визнана неекранована вита пара (UTP), яка включена практично в усі сучасні стандарти і технології локальних мереж забезпечуючи пропускну здатність до 100 Мбіт/с.

Екранована вита пара (STP/FTP категорії 6) дозволяє збільшити пропускну здатність до 1000 Мбіт/с.

Оптоволоконний кабель широко застосовується як для побудови локальних зв'язків, так і для побудови магістралей глобальних мереж. Оптоволоконний кабель може забезпечити дуже високу пропускну здатність каналу (до декількох Тбит/с) і передачу на значні відстані до декількох десятків кілометрів без проміжного посилення сигналу.

Рекомендації з проектування мереж наступні:

1. Кабель вибирається однаковим на всю мережу (найчастіше використовується вита пара 5 (5e) і 6 категорії);
2. На довгих ділянках мережі рекомендується використовувати екранований кабель це зменшує можливість втрати пакетів;
3. Між комутаторами Gigabit Ethernet рекомендується використовувати оптоволоконне з'єднання;
4. В деяких випадках слід розглядати можливість бездротових мереж (тут слід особливу увагу приділяти безпеці);
5. Рекомендується використовувати обладнання, по можливості, від одного відомого виробника;
6. Вибирати обладнання потрібно по співвідношенню ціна/якість;
7. Продуктивність кумутуючого обладнання повинна бути вище продуктивності машин для обробки потоків даних;

8. Облік масштабованості (залишати в резерв 10 % портів і до 30 % пропускної здатності);

9. Ядро мережі, проміжні комутатори, сервери запису управління повинні бути об’єднані за резервними лініями зв’язку, ключове комунікаційне обладнання також резервується;

10. Резервування даних на дублюючий сервер через комутатори з відзеркаленням портів.

Методика визначення кількості фізичних підмереж. Виходячи з сумарної швидкості інформаційного потоку від всіх IP відеокамер (B_{max}) і обраної пропускної здатності мережі (W) можна визначити кількість інформаційних підмереж, які необхідно створити. Така кількість підмереж забезпечить доставку відеосигналів від відеокамер до сервера без видимих затримок.

Кількість підмереж визначається як:

$$M = \frac{B_{\max}}{0.8W}, \tag{5.3}$$

де M – кількість підмереж; B_{max} – сумарна швидкість потоків від всіх відеокамер; W – пропускна здатність мережі; 0,8 – коефіцієнт, що характеризує максимально допустиме завантаження мережі (80%).

Наприклад, мережа побудована на кабелі вита пара UTP Cat.6 забезпечує максимальну швидкість передачі W = 1Гбіт/с. Сумарна швидкість потоку від всіх IP відеокамер B_{max} = 4Гбіт/с. Отже, для вирішення завдання доведеться створювати 5 підмереж: 4Гбіт/с / (0,8*1Гбіт / с) = 5.

Методика визначення максимально допустимих потоків від кожної відеокамери. Вирішення цього завдання має дуже багато варіантів, але разом з цим існують основні принципи розподілу потоків і знаходження результуючих швидкостей на ділянках мережі, які ми розглянемо.

При побудові мережі використовується активне обладнання, призначене для розподілу/об’єднання потоків і трансляції їх від відеокамери до сервера (серверів).

Розподіл/об’єднання потоків здійснюють комутатори, які бувають двох типів (рис 5.15).

а) б)

Рисунок 5.15 – Типи комутаторів: а – простий, б – з комбо-портом

Максимальне завантаження порту комутатора зазначена в його технічних характеристиках. При завантаженні всіх портів комутатора, загальний інформаційний потік не повинен перевищувати значення максимальної пропускної спроможності комутатора. Для виконання цієї умови потрібно визначити максимально допустиму швидкість потоку на кожен порт. На рисунку 5.18 наведено графік, який дозволяє для різних комутаторів знаходити максимально допустимий потік на порт.

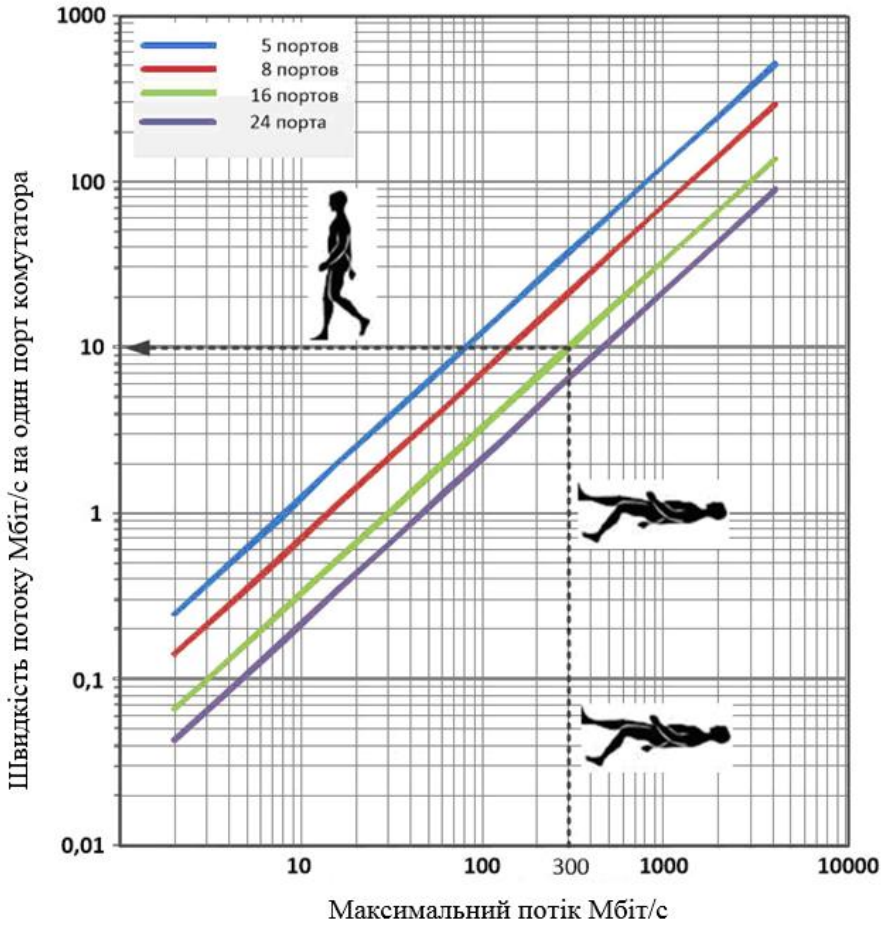


Рисунок 5.18 – Діаграма визначення максимальної швидкості потоку на один порт

При використанні простого комутатора в мережі, коли до всіх портів крім одного підключені відеокамери, а останній порт підключений до іншого комутатора (комутатор №2, рис.5.19) максимальний допустимий потік на один порт, за умови, що $2\sum_{i=1}^{N-1} V_i < W$, визначається як:

$$V_2 = \frac{V_1}{N-1}, \tag{5.4}$$

де V_i – швидкість потоку, що входить в кожен порт комутатора.

Якщо порт, що залишився – підключений до магістралі (комутатор №1, рис.5.17), то максимальний допустимий потік на порт, визначається як:

$$V_1 = \frac{0.8W}{2(N-1)}, \quad (5.5)$$

де $V_{1(2)}$ – максимальна швидкість одного порту у комунікатора №1(2); N – загальна кількість портів; W – максимальна допустима швидкість передачі інформації комутатора (пропускна здатність мережі); 0,8 – коефіцієнт, який характеризує максимально допустиме завантаження мережі.

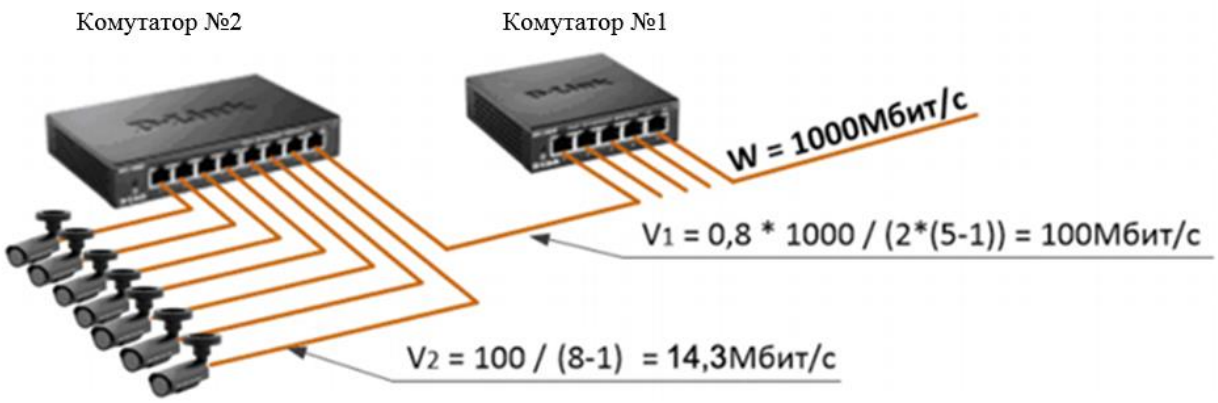


Рисунок 5.117 – Приклад розподілу потоків на порт комутатора

При такому підключенні ресурс магістралі використовується на 50%. Тобто, при роботі мережі на кабелі вита пара з максимально допустимою швидкістю 100 Мбіт/с, комутатор зможе використовувати тільки 50 Мбіт/с.

Для використання ресурсу мережі на всі 100% потрібно застосовувати комутатори з комбо-портом. При цьому максимальна швидкість через кожен порт може бути визначена в такий спосіб:

$$V = \frac{0.8W}{N}, \quad (5.6)$$

де V – максимальна швидкість одного порту; N – загальна кількість портів; W – допустима швидкість передачі інформації комутатора; 0,8 – коефіцієнт, який характеризує максимально допустиме завантаження мережі.

Не слід забувати, що розрахункове значення швидкості потоку через порт не має перевищувати значення цього ж параметра в паспорті комутатора.

З вище сказаного випливає, що відеокамера повинна бути налаштована таким чином, щоб її потік не перевищував розрахункове значення допустимої швидкості потоку через порт комутатора, до якого вона буде підключена.

Контрольні питання:

1. Чому для систем відеоспостереження стандартом є коаксіальний кабель саме з хвильовим опором 75 Ом, і до чого призведе використання кабелю з опором 50 Ом?
2. Які фізичні параметри коаксіального кабелю безпосередньо впливають на втрату сигналу при збільшенні довжини лінії?
3. У чому полягає перевага комбінованого кабелю (наприклад, КВК) та які існують обмеження щодо перерізу його жил живлення при збільшенні відстані до камери?
4. Який фізичний принцип роботи витої пари дозволяє їй ефективно пригнічувати електромагнітні перешкоди на великих відстанях?
5. Чим відрізняються пасивні відео-балуни від активних передавачів і в яких випадках необхідно використовувати пристрої з можливістю корекції АЧХ?
6. У яких сценаріях використання одномодового оптоволоконного кабелю є безальтернативним рішенням порівняно з мідними провідниками?
7. За яким критерієм розраховується максимально допустима довжина коаксіального кабелю для надійної роботи системи?
8. Яка принципова різниця в логіці роботи між хабом, комутатором та маршрутизатором у структурі мережі IP-відеоспостереження?
9. Порівняйте стандарти PoE (802.3af, 802.3at, 802.3bt): яку максимальну потужність на порт вони можуть забезпечити і для яких типів камер призначені?
10. Які переваги та недоліки має топологія «зірка» порівняно з «кільцевою» топологією при побудові територіально розподілених систем?

Література: [1-6].

Тема 6. Способи і типове обладнання живлення відеокамер

План:

Типи та технічні характеристики джерел живлення. Кліматичні та електричні шафи. Основні компоненти електричних шаф для живлення відеокамер. PoE технологія живлення та її стандарти. Розрахунок потужності та вибір кабелів. Типові проблеми живлення відеокамер та шляхи їх вирішення.

Типи та технічні характеристики джерел живлення. Ефективність сучасної системи відеоспостереження визначається не лише роздільною здатністю оптичних сенсорів або інтелектуальними алгоритмами аналітики, а насамперед стабільністю та надійністю її енергетичного живлення. Будь-яка перерва у подачі живлення або деградація його якості призводить до прогалин у системі безпеки, втрати важливих даних та передчасного виходу з ладу дорогого обладнання.

Система живлення відеоспостереження виконує роль перехідної ланки між нестабільною мережею змінного струму високої напруги та чутливою електронікою камер і реєстраторів, що потребують низьковольтного постійного струму. Процес проектування починається з розрахунку енергетичного балансу, де враховується номінальне споживання кожного вузла. Стандартна практика передбачає використання коефіцієнта запасу потужності не менше 30 %, що дозволяє системі стабільно функціонувати під час пікових навантажень, таких як активація інфрачервоного підсвічування, запуск поворотних механізмів PTZ-камер або робота в умовах низьких температур.

В індустрії безпеки домінують два основні типи архітектур перетворення: трансформаторні та імпульсні джерела живлення. Трансформаторні блоки, що базуються на класичній схемі зі знижувальним трансформатором, випрямлячем та фільтром, вирізняються високою надійністю та низьким рівнем високочастотних завад. Проте їхня низька енергоефективність, значні габарити та чутливість до коливань вхідної напруги призвели до того, що вони витісняються імпульсними рішеннями.

Імпульсні блоки живлення використовують принцип широтно-імпульсної модуляції, що дозволяє досягти коефіцієнта корисної дії на рівні 85-98 %. Такі пристрої здатні працювати у широкому діапазоні вхідної напруги (від 100 В до 265 В), забезпечуючи при цьому стабілізовані 12 В або 24 В на виході. Це важливо для об’єктів з нестабільним електропостачанням, де просідання напруги є регулярним явищем.

Вибір конструкції джерела живлення залежить від масштабу системи та умов монтажу. Найбільш поширеними є наступні типи джерел живлення:

1. Адаптери типу «вилка», які призначені для індивідуального живлення однієї камери або реєстратора. Це компактні пластикові пристрої, що безпосередньо вставляються в розетку;

2. Металеві перфоровані корпуси, які відомі серед інженерів як «сітки». Вони забезпечують ефективне пасивне охолодження за рахунок природної конвекції та дозволяють підключати кілька камер через загальну клемну колодку. Часто оснащуються регулятором вихідної напруги для компенсації втрат на довгих лініях;

3. Технологія живлення PoE, яка інтегрована безпосередньо в мережеву інфраструктуру, для IP-відеоспостереження. Це дозволяє передавати дані та енергію по одному кабелю «вита пара» категорій Cat5e або Cat6, що суттєво знижує вартість монтажних робіт та мінімізує кількість точок відмови;

4. Металеві бокси (шафи живлення, кліматичні шафи) – централізовані рішення, що закриваються на замок. Усередині розміщується блок живлення, плата розв’язки із запобіжниками на кожен канал та місце для акумулятора тощо;

5. Джерела живлення на DIN-рейку – використовуються в промислових системах відеоспостереження, де обладнання монтується в загальні електротехнічні шафи.

Адаптери типу «виделка» (рис. 6.1) мають вигляд закритого пластикового боксу з внутрішньої апаратною частиною, кабелем живлення і виделкою.

Рисунок 6.1 – Адаптери живлення типу «виделка»

Блоки живлення в перфорованому корпусі являють собою металевий перфорований бокс, всередині якого знаходиться вся апаратна частина пристрою (рис. 6.2). Завдяки перфорації забезпечується хороший тепловідвід, вентиляція і захист від перегріву.

Рисунок 6.2 – Блоки живлення в перфорованому корпусі

Подібні блоки живлення не мають в комплекті кабелів, замість цього вони обладнані клемною колодкою для підключення проводів живлення, і регуляторами напруги.

Перфоровані БЖ розраховані на більшу потужність, однак для захисту пристрою від зовнішніх факторів необхідно помістити його в захисний бокс.

Захищені блоки живлення в металевих коробах встановлюються стаціонарно в опалювальних приміщеннях і мають вигляд металевого ящика з дверцятами (рис. 6.3). БЖ даного типу набагато більш надійні і функціональні в порівнянні з попередніми. У великій металевий бокс можна встановити акумуляторну батарею, і простий БЖ перетворюється вже в ДБЖ.

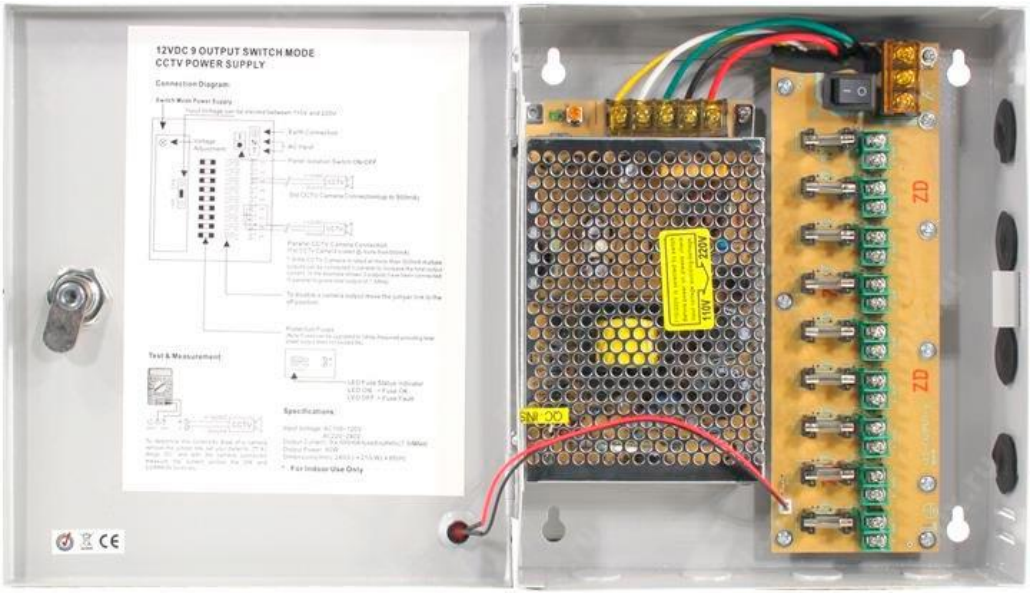


Рисунок 6.3 – Блоки живлення в металевому корпусі

Для стаціонарних систем відеоспостереження рекомендується використання саме таких БЖ зважаючи на їх підвищену надійність, а також хорошого захисту від доступу сторонніх осіб.

Блоки безперебійного і резервного живлення дозволяють зберегти обладнання від стрибків електричного струму, які іноді відбуваються в системі. Їх найчастіше встановлюють для гібридної або аналогової структури відеоспостереження. У випадку з IP-обладнанням живлення відеокамер відбувається за технологією PoE із використанням PoE комутаторів.

Кліматичні та електричні шафи. Еволюція систем безпеки протягом останніх десятиліть призвела до фундаментальної зміни парадигми в проектуванні інфраструктури відеоспостереження. Сучасні системи перейшли від закритих аналогових контурів до складних, інтелектуальних IP-мереж, де кожна точка збору даних є фактично мікро-сервером. У цих умовах фізична оболонка, що захищає активне обладнання – комутатори, відеореєстратори, блоки живлення та пристрої передачі даних – набуває важливого значення. Кліматичні та електричні монтажні шафи перестали бути просто контейнерами; вони перетворилися на складні інженерні системи, що забезпечують безперебійне функціонування цифрових активів в умовах температурних екстремумів, високої вологості, агресивного промислового середовища та ризиків вандалізму.

Архітектура монтажних систем для відеоспостереження будується на принципах модульності та відповідності міжнародним стандартам. Основним стандартом ширини для телекомунікаційного та серверного обладнання є 19 дюймів (482,6 мм), що дозволяє уніфікувати розміщення пристроїв різних виробників у єдиному конструктиві. Одиницею вимірювання висоти в таких системах є юніт (1U), що дорівнює 44,45 мм. Розуміння цієї градації є основою для правильного підбору шафи, виходячи з обсягу обладнання, яке планується до встановлення.

Настінні монтажні шафи є базовим елементом для побудови локальних вузлів комутації на об'єктах з обмеженою кількістю камер. Вони зазвичай використовуються всередині приміщень – у коридорах, на сходових майданчиках або в технічних нішах. Провідним виробником таких систем в Україні є компанія CMS, чий асортимент дозволяє задовольнити потреби як бюджетних, так і високонавантажених проектів.

Для центральних вузлів відеоспостереження, де агрегуються потоки з сотень камер, використовуються підлогові шафи висотою до 45U. Ці конструкції розраховані на розміщення масивних дискових полиць, потужних серверів та мережевих екранів. Вантажопідйомність таких моделей може досягати 800 кг.

У випадках, коли обладнання розміщується в окремих закритих серверних кімнатах з контролем доступу та потужними системами кондиціонування, використання закритих шаф може бути надлишковим. Тут доцільно застосовувати одинарні або подвійні (дворамні) стійки. Дворамні стійки забезпечують високу стабільність і здатні витримувати навантаження до 1000 кг, при цьому вони значно легші та мобільніші за закриті шафи.

Для специфічних завдань, наприклад, встановлення обладнання в обмеженому просторі під стелею або всередині меблевих конструкцій, застосовуються стійки-кронштейни серії Cube (Cube1, Cube2, Cube3). Вони мають компактний розмір 9U (550x550x550 мм) і можуть бути укомплектовані роликами для легкого переміщення в межах офісу. Ціна таких рішень станом на початок 2026 року коливається від 3500 до 5922 грн залежно від ступеня посилення конструкції.

Зовнішнє встановлення систем відеоспостереження ставить перед інженерами найскладніші виклики. Кліматичні (всепогодні) шафи розроблені для того, щоб нівелювати агресивний вплив довкілля: від арктичних морозів до тропічної спеки та високої вологості.

Таким чином, кліматичні шафи (рис. 6.4) – це спеціалізоване обладнання, призначене для захисту чутливого устаткування системи від несприятливих зовнішніх кліматичних умов (температури, вологості, пилу). Вони забезпечують стабільний внутрішній мікроклімат завдяки системам контролю температури та вологості. Основне застосування кліматичних шаф – це встановлення обладнання на відкритому повітрі або в приміщеннях без належного клімат-контролю.

Основою кліматичної стійкості шафи є її здатність підтримувати стабільний мікроклімат. Провідні українські виробники, такі як УХЛ-МАШ та IPCOM, використовують різні підходи до термоізоляції.

Система активної терморегуляції зазвичай включає два ключові модулі – нагрівальний і вентеляційний.

Нагрівальний модуль, наприклад, у шафах УХЛ-МАШ використовується потужністю 100 Вт, а в посилених моделях IPCOM – вентилятор опалення потужністю до 400 Вт. Це необхідно не лише для підтримки температури, а й для запобігання утворенню конденсату на платах пристроїв.

Рисунок 6.4 – Кліматична шафа CSV 12U всепогодна

Для охолодження обладнання кліматичних шаф використовуються блоки осьових вентиляторів. Модель IPCOM ШКК 24U оснащена чотирма вентиляторами, кожен з яких забезпечує потік повітря 160 м³/год. Для захисту від пилу вентиляційні отвори закриваються фільтрами з класом захисту IP21 або IP54.

Для професійного підбору обладнання інженери використовують розрахункові формули, що враховують об'єм шафи та градієнт температур. Базова формула розрахунку теплової потужності для обігріву виглядає так:

$$P = \frac{V \Delta T K}{860}, \tag{6.1}$$

де V – внутрішній об'єм шафи в кубічних метрах; ΔT – різниця між необхідною температурою всередині та мінімальною зовні; K – коефіцієнт теплопередачі матеріалу (для металевих шаф без ізоляції K=3,0-4,0 (для приміщень), для стандартної ізоляції типу «сандвіч» K=1,0-1,9 (вуличні шафи), для утеплених з подвійною ізоляцією – K = 0,6-0,9 (екстремальні умови)).

Отже, вибір монтажної шафи для системи відеоспостереження є стратегічним рішенням, що визначає життєздатність всієї мережі безпеки. Можна керуватися наступними рекомендаціями для вибору типу шафи:

1. Для зовнішнього встановлення важливим є наявність активної системи терморегуляції та якісної ізоляції (алюфом або мінеральна вата). Використання звичайних електричних щитків IP54 без обігріву для розміщення відеореєстраторів призводить до виходу з ладу жорстких дисків у перший же зимовий сезон;

2. У місцях загального доступу слід віддавати перевагу антивандальним шафам з товщиною металу від 1,5 мм та багатоточковими системами замикання («крабовими» замками). Це не лише захищає від крадіжки обладнання, а й запобігає спробам фізичного втручання в роботу системи відеоспостереження;

3. Доцільне використання кабельних організаторів та блоків розеток (PDU), що не є розкішшю, а технічною необхідністю. Хаотичне розміщення кабелів перешкоджає охолодженню та значно ускладнює пошук несправностей під час сервісного обслуговування;

4. Для критичних об'єктів інфраструктури обов'язковим є впровадження систем віддаленого моніторингу температури та вологості. Це дозволяє перейти від реактивного до проактивного обслуговування, попереджаючи аварії до їх виникнення;

5. При виборі постачальника слід вимагати сертифікати відповідності ДСТУ EN 62208 та протоколи випробувань на пожежну безпеку. Це гарантує юридичну чистоту проекту та безпеку експлуатації.

Основні компоненти електричних шаф для живлення відеокамер. Перед тим як безпосередньо монтувати відеоспостереження, потрібно створити ескізний проект системи, де потрібно зобразити місця розташування відеокамер, шлях прокладання кабелю тощо.

Матеріали які будуть потрібні для монтажу аналогової системи відеоспостереження наступні: кабель для живлення всієї системи від мережі 220В, відеореєстратор, блок живлення, джерело безперебійного живлення, конектори марки BNC, розподільчі коробки зі ступенем захисту мінімум IP52, модульний розрядник, модульні розетки та клемні роз'єми.

Для підведення живлення до шафи, де буде здійснено монтаж, найкраще використовувати марку ВВГнг-Ls 3х1,5мм^2, а для комутації в слабкострумовому щиті – ПУГВ 1,5мм^2. Можна також використати кабель КВК-П 2х 0,75мм^2. Його не потрібно плутати з КВК-В. Марка КВК-П – це вуличний варіант, а КВК-В – для прокладання всередині будинку. Він не захищений від ультрафіолету.

Слабкострумова щитова, де розташовуються відеореєстратор, блок живлення та інше обладнання, можна перебувати віддалено від загальної щитової 220В.

У першу чергу до щитової потрібно підвести електрику.

Кабель ВВГнг-Ls 3х1,5мм^2 можна прокласти в стіні чи спеціальних коробах від розподільчого щита 220V до слабкострумової шафи. Подавати живлення до нього потрібно від окремого модульного автомата розподільчого щита з номінальним струмом 10А (рис. 6.5).

У слабкострумовому щитку кабель живлення потрібно заводити на клеми автоматичного вимикача. Він буде для цієї шафи ввідним. А вже безпосередньо від нього підключати модульні розетки і розрядник (блискавкозахист).

Блискавкорозрядник (або пристрій захисту від імпульсних перенапруг – ПЗІП) – це електричний пристрій, що захищає електрообладнання, миттєво відводячи високу напругу, спричинену блискавкою, в землю. Він є частиною системи зовнішнього захисту, яка перехоплює розряд та запобігає пошкодженню техніки, підключеної до мережі.

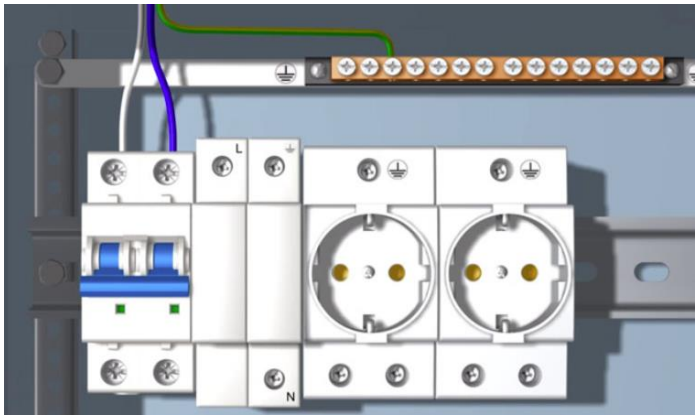


Рисунок 6.5 – Приклад встановлення автомата в шафі на DIM рейку та під’єднання вхідної напруги

Підключення розрядника проводиться за наведеною нижче схемою (рис. 6.6). Білий і чорний провід – це фаза, синій – нуль, жовто-зелений – заземлення.

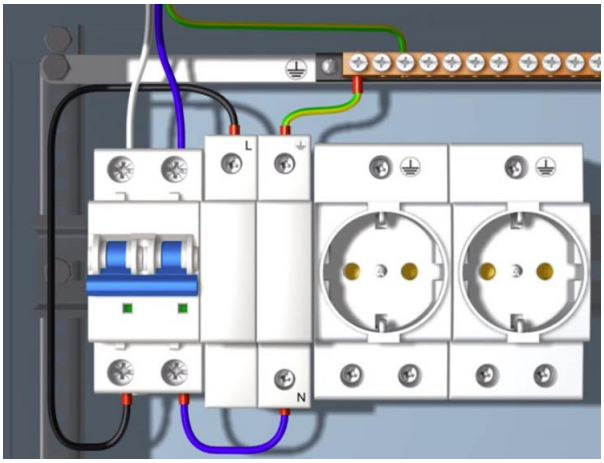


Рисунок 6.6 – Підключення блискавкорозрядника

Підключення бортових розеток шафи здійснюється за наступним принципом (рис.6.7).

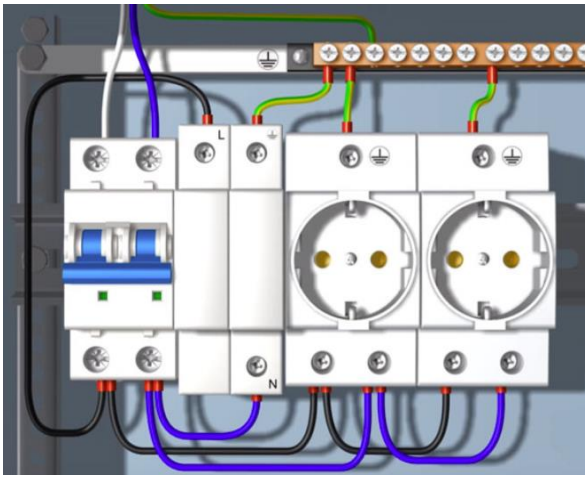


Рисунок 6.7 – Підключення розеток в шафі

У цій шафі потрібно також розмістити відеореєстратор, блок живлення і джерело безперебійного живлення (ДБЖ).

Далі від розеток через звичайну вилку потрібно подати живлення до ДБЖ (рис. 6.8). Якщо блок живлення не має кабелю з виделкою в комплекті, тоді потрібно використати кабель ПВС і звичайну євровилку.

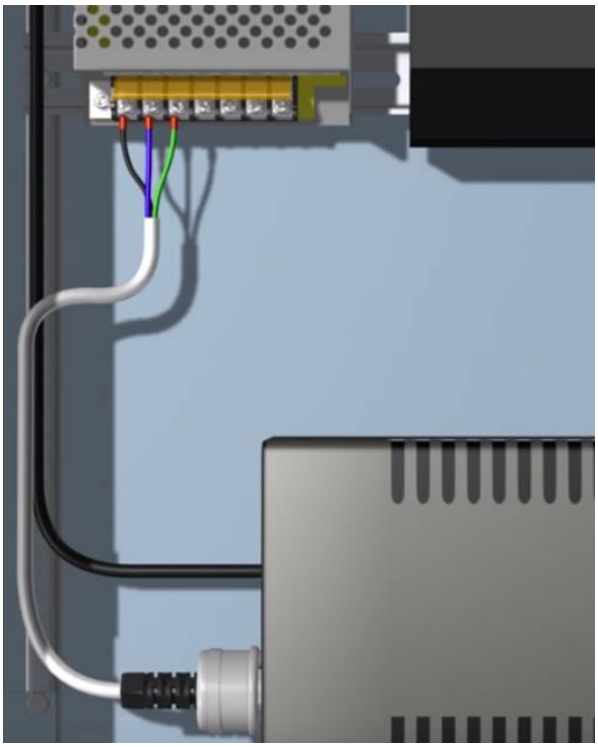


Рисунок 6.8 – Підключення ДБЖ

На один кінець дроту потрібно встановити вилку, а інший зачистити і під’єднати до блоку на клеми живлення 220В, позначені як L і N (рис. 6.9).

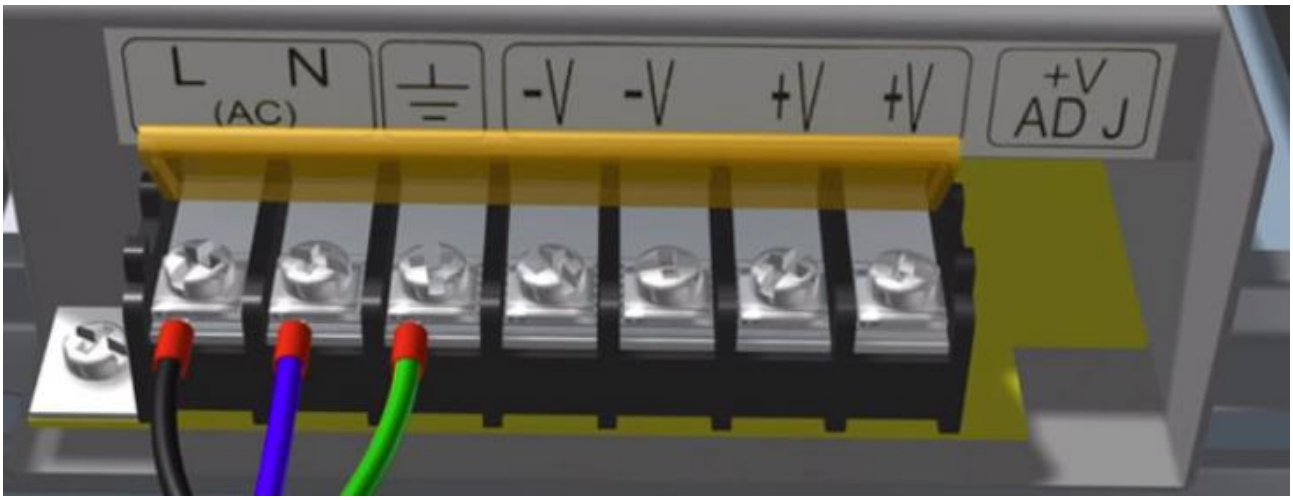


Рисунок 6.9 – Підключення ДБЖ до блоку живлення

Особливої різниці у фазуванні або полярності куди підключати нуль і фазу тут немає. Далі подається живлення на відеокамери (рис. 6.10).

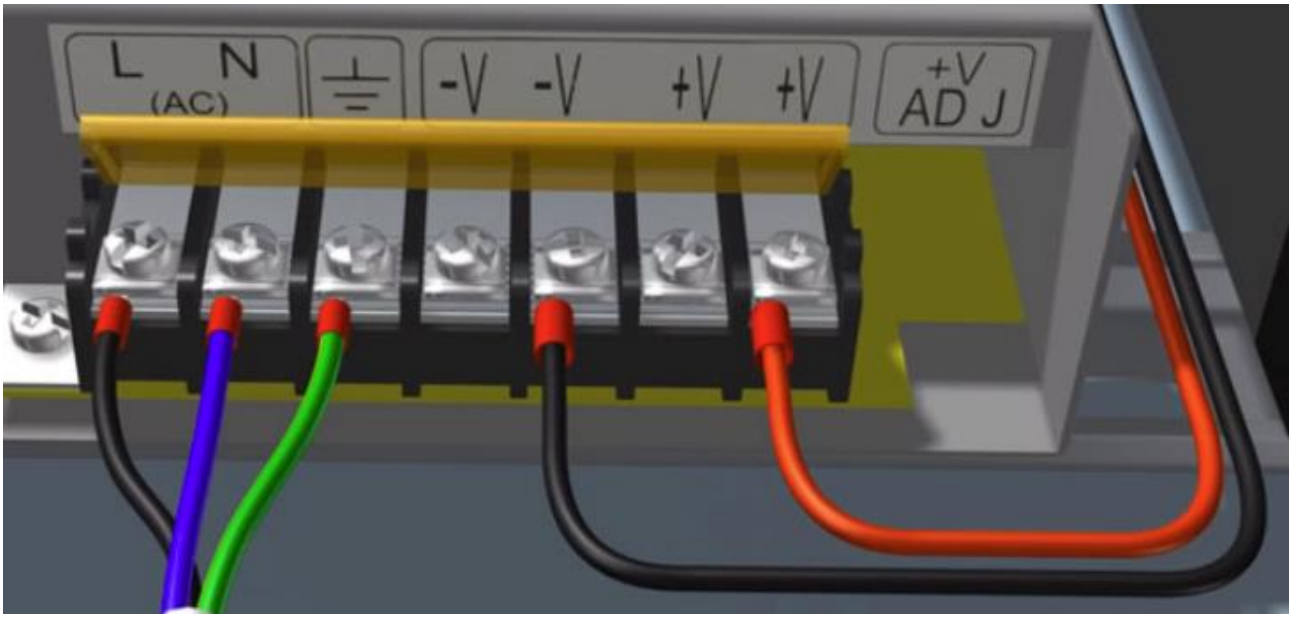


Рисунок 6.10 – Подача 12 В від блока живлення до камери

При нестачі вихідних клем 12 В на блоці живлення, найкраще скористатися спеціальними клемними колодками, кількість яких має відповідати кількості камер і мати промарковані контакти як «+V» і «-V» (рис. 6.11).

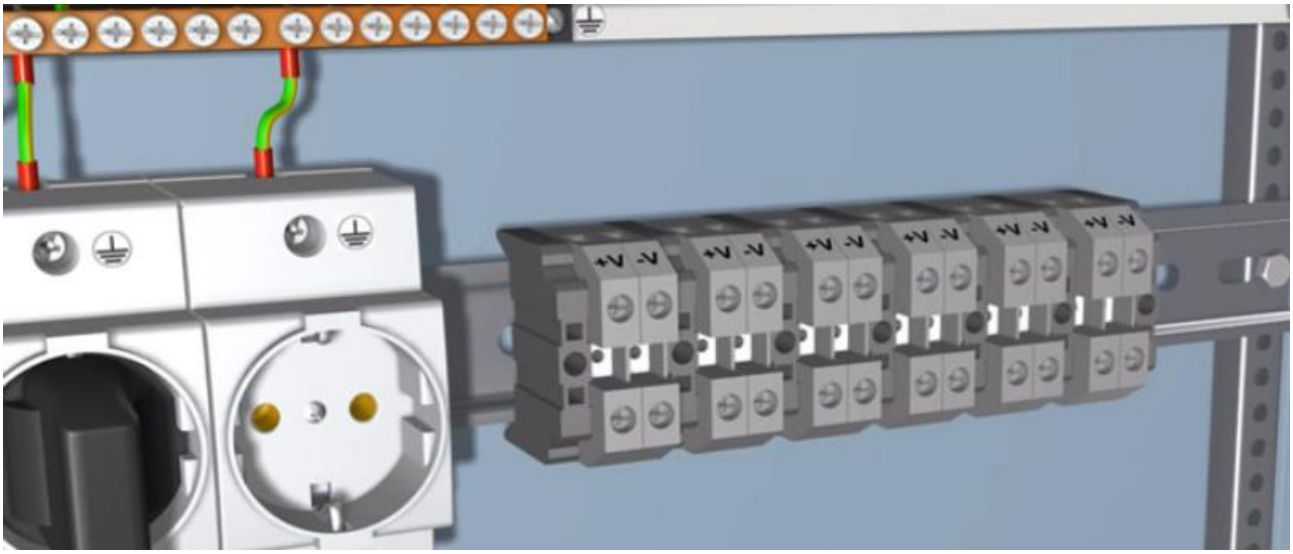


Рисунок 6.11 – Встановлення клемних колодок на DIM рейку шафи

Потім, проводами марки ПуГВ потрібно підключити вихідні клеми 12В «+V» і «-V» з блоку живлення, з відповідними роз’ємами першої клемної колодки (рис. 6.12).

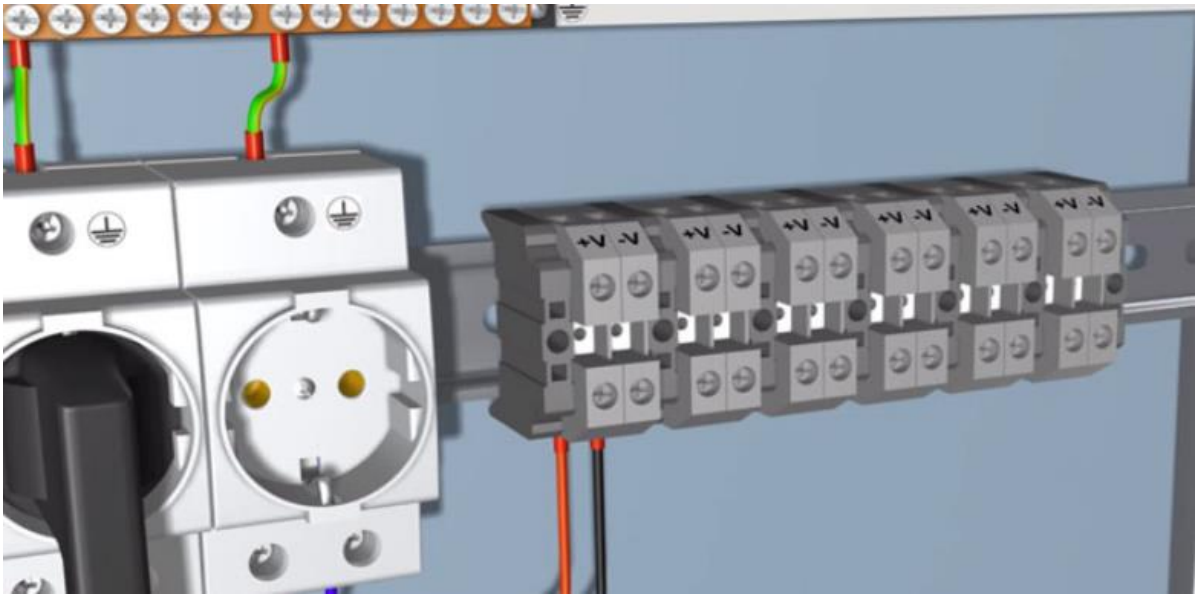


Рисунок 6.12 – Подача живлення на клемні колодки

Для плюсового проводу краще використовувати жили червоного кольору, для мінусового – чорного. На решту клем живляться подають перемичками відповідного кольору (рис. 6.13).

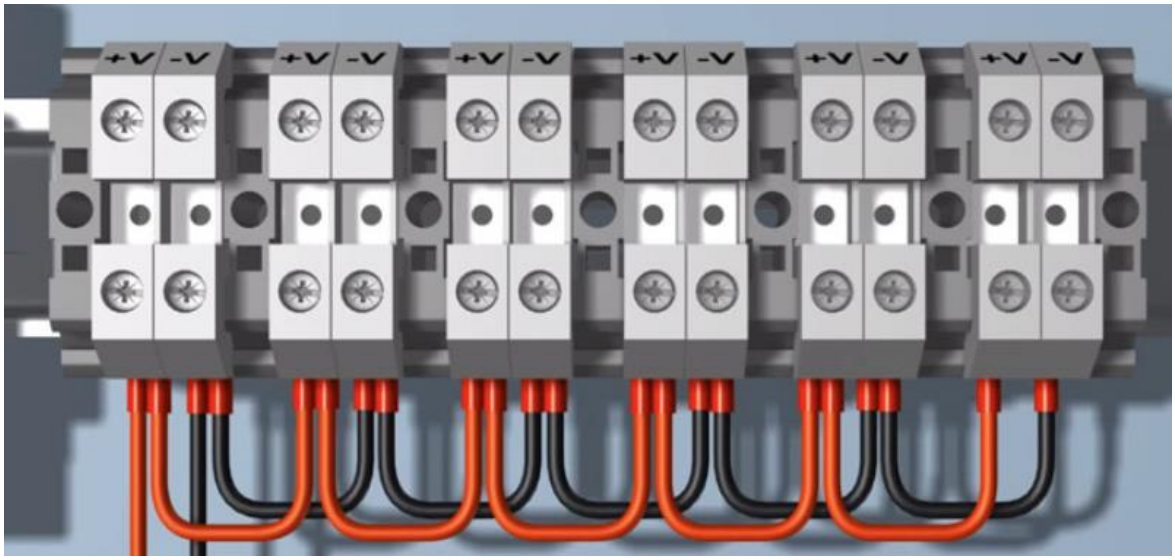


Рисунок 6.13 – Розведення живлення 12 В між клемними колодками

Далі потрібно прокласти кабель, наприклад, марки КВК-П до кожної відеокамери, або до того місця, де планується їх розмістити. Прокладати його в приміщенні можна як в пластиковому каналі, так і просто поверх стін.

На вулиці при бажанні кабель можна захистити у гофрі (рис. 6.14), але не обов’язково.

Рисунок 6.14 – Прокладання гофри до монтажної коробки

Далі з кабелю потрібно зняти верхній шар ізоляції, приблизно на 8-9 см і зачистити дві жили живлення і обпресовувати їх наконечниками НШВ (рис. 6.15).

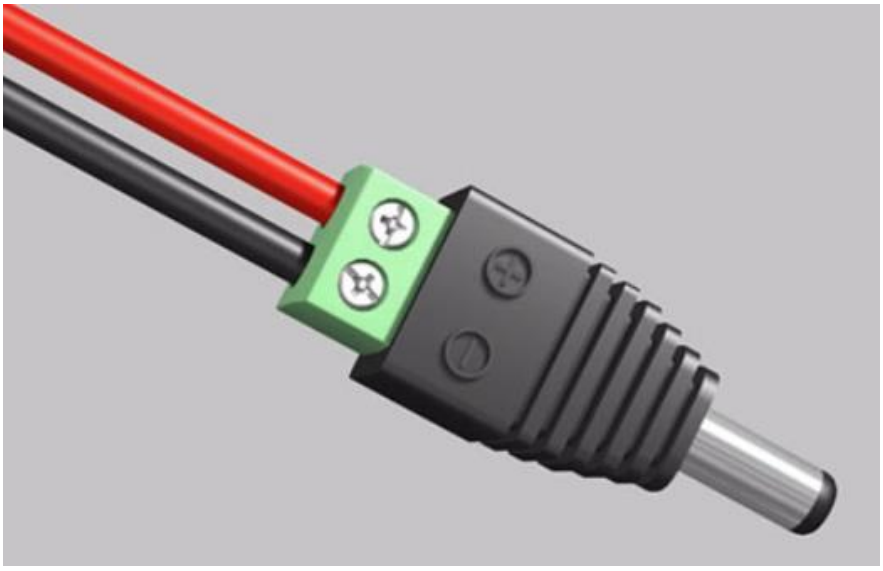


Рисунок 6.15 – Підключення наконечника НШВ

Після цього потрібно зняти ізоляцію з коаксіального кабелю.

Зовнішню оплітку з міді необхідно змістити назад, щоб жоден волосок не торкався контакту з центральною жилою. Далі потрібно оголити центральну жилу на 3-4 мм і змонтувати в BNC-F роз’ємі (рис. 6.16).

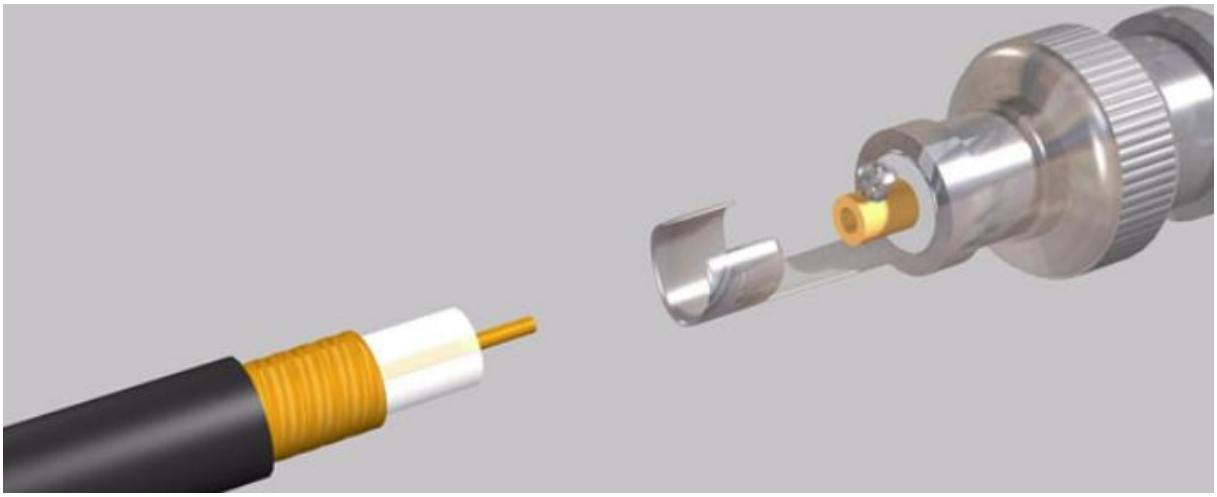


Рисунок 6.16 – Підключення коаксіального кабелю до BNC-F роз’єму

Далі потрібно встановити на стіну саму відеокамеру, а провід від неї запустити в розподільчу коробку і з’єднати з ввідними роз’ємами та закрити кришку.

Для запобігання попадання вологи всередину необхідно використовувати коробку з герметичними кабельними вводами з боків (рис. 6.17).

Аналогічно виконується підключення всіх інших відеокамер на стінах будинку. До кожної з них доведеться тягнути окремий кабель КВК-П.

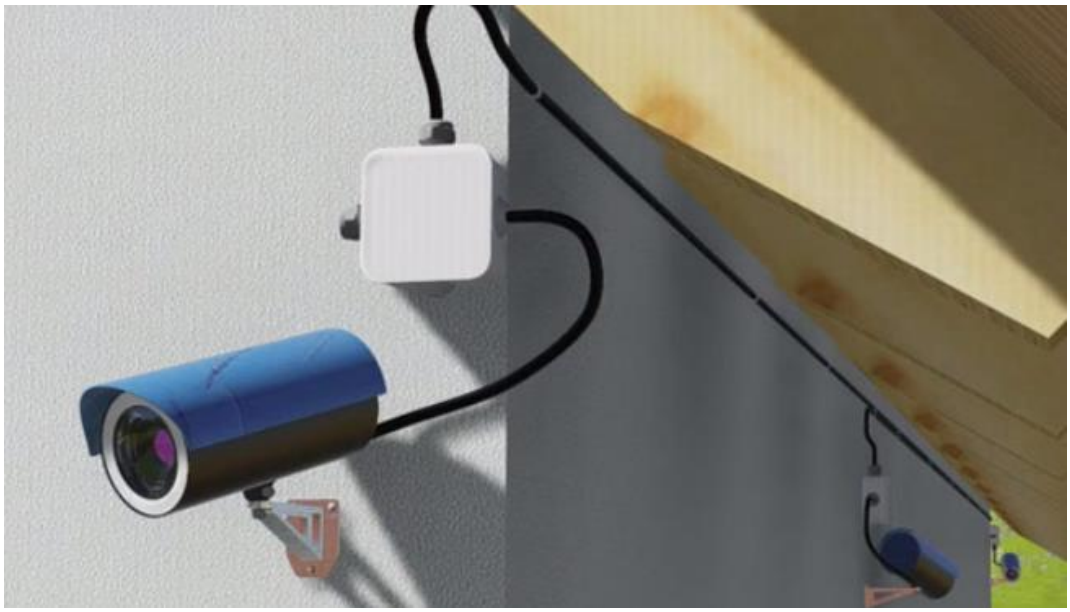


Рисунок 6.17 – Приклад коробку застосування монтажної коробки з герметичними кабельними вводами з боків

Далі всі кабелі відеоспостереження потрібно розвести в слабкострумовій шафі. Для початку доцільно підключити сам відеореєстратор через джерело безперебійного живлення.

Потім потрібно зачистити протилежні кінці кабелю КВК-П, заведені в шафу від відеокамер, аналогічним чином як показувалося вище. При цьому

жили живлення (червоний з чорним) під’єднати на відповідні клемні колодки «+ V» і «-V» (рис. 6.18).

Кінець коаксіального кабелю, з встановленим роз’ємом BNC-F, заводиться у вільне гніздо відеореєстратора з написом Video In відповідного каналу. Далі те ж саме потрібно проробити з рештою відеокамер.

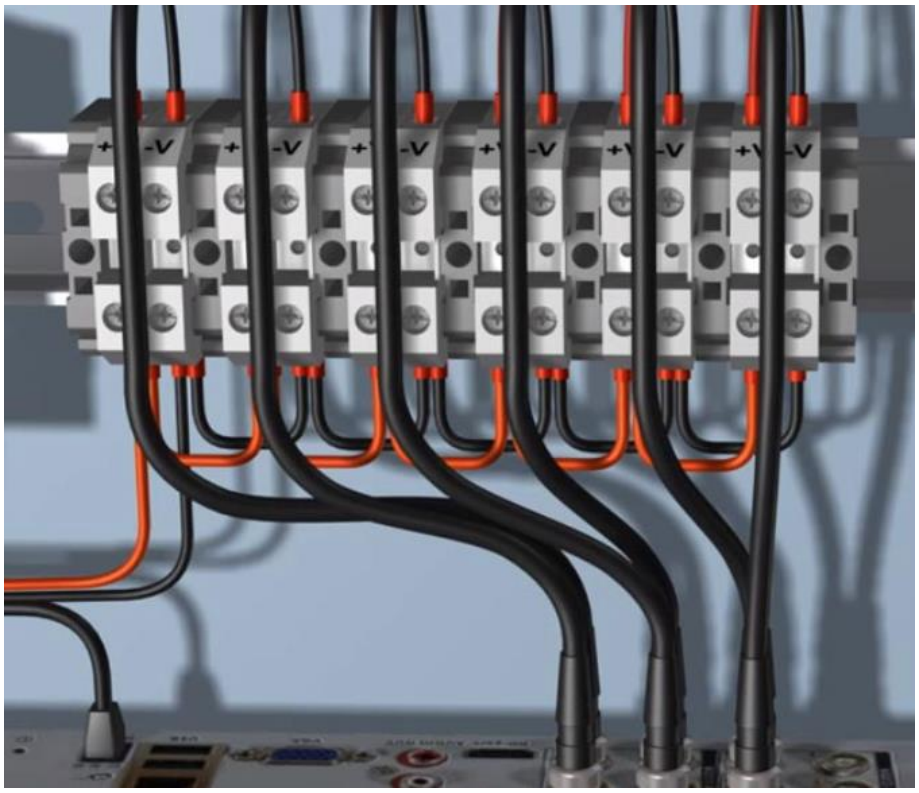


Рисунок 6.18 – розведення живлення по контактних колодках

Долі потрібно налаштувати систему, підключивши монітор до реєстратора через VGA або HDMI роз’єми.

Щоб використовувати монітор для інших цілей, можна в HDMI роз’єм включити комп’ютер, а в VGA – камери. Тоді шляхом зміни режимів відображення легко отримати перемикання картинки з різних джерел.

Все програмне забезпечення для налаштування відеоспостереження має йти в комплекті з відеореєстратором.

Для монтажу і встановлення IP камер, крім матеріалів зазначених вище, знадобляться дещо інші комплектуючі: 4-х парний кабель UTP замість КВК-П, IP камери з функцією PoE для вуличного виконання, мережевий реєстратор, PoE комутатор, роз’єми RJ-45.

Всі компоненти мають бути сумісні між собой. Монтаж силової частини слабкострумового щита з автоматичним вимикачем, розетками та розрядником здійснюється аналогічно вищевикладеному (рис. 6.19).

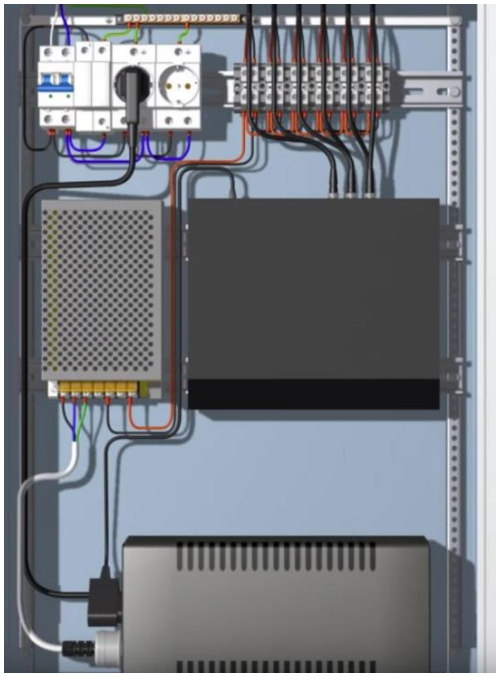


Рисунок 6.19 – Приклад укомплектованої шафи аналогового відеоспостереження

Відмінності є в підключеннях відеореєстратора і кабелів. По-перше, закріпити на din-рейці блоки живлення PoE комутатора і мережевого реєстратора. Їх вилки підключати тільки через ДБЖ (рис. 6.20).

Рисунок 6.20 – Приклад встановлення на din-рейці блоки живлення PoE комутатора і мережевого реєстратора

Далі в гофрі прокладають кабель UTP Cat5E від слабкострумової шафи до місць встановлення IP камер.

Біля камер встановлюють розподільчі коробки. Зачищення ізоляції та обпресування кабелю в RJ-45 розглядалося раніше.

У розподільчу коробку має бути заведено два кабелі – від IP камери і кабель з шафи (рис. 6.21). Там їх і з’єднують між собою.

Рисунок 6.21 – Приклад введення у розподільчу коробку кабелів від IP-камери і кабель з шафи

Потрібно пам’ятати, що при використанні PoE технології, передача живлення йде через виту пару. Підключати другий провід від камери не потрібно.

Аналогічно підключають усі інші камери.

Тепер потрібно зробити розведення проводів в шафі відеоспостереження під’єднати їх до PoE комутатора та з’єднати відеореєстратор з комутатором (рис. 6.22).

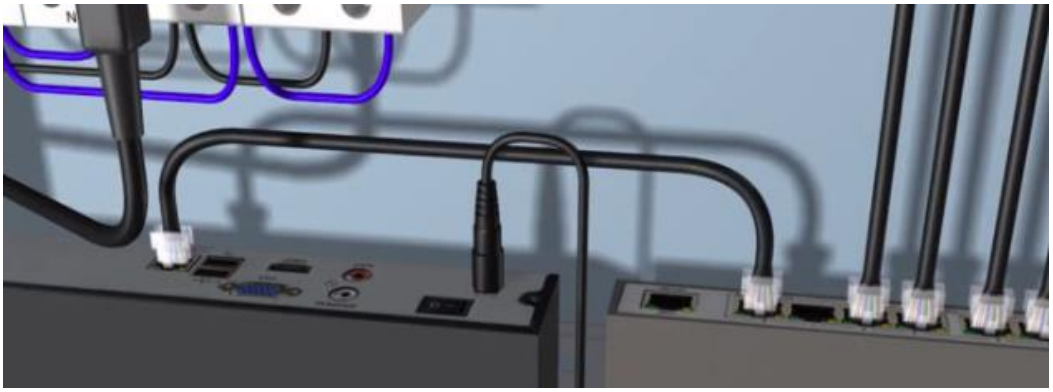


Рисунок 6.22 – Приклад розведення проводів в шафі до PoE комутатора та з’єднання відеореєстратора з комутатором

На завершення здійснити налаштування відеокамер, а також їх підключення до роутера і монітора. Роутер з’єднують з відеореєстратором через патчкорд, а монітор за допомогою HDMI кабелю (рис. 6.23).

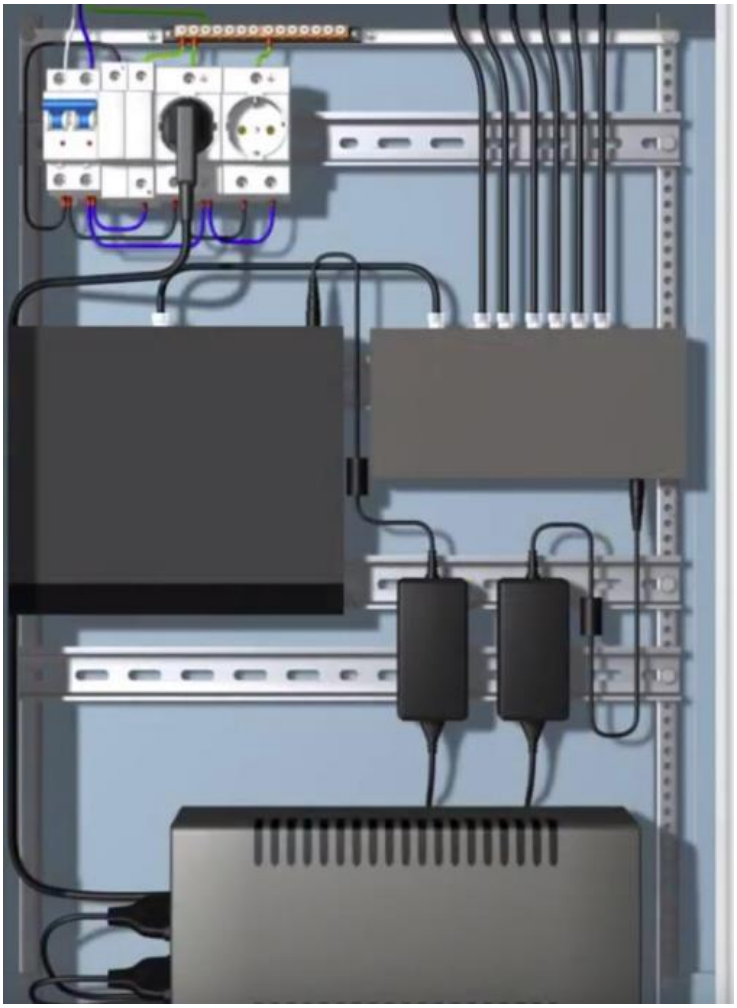


Рисунок 6.23 – Приклад укомплектованої шафи IP-відеоспостереження

По завершенню монтажу потрібно здійснити відповідні налаштування системи.

PoE технологія живлення та її стандарти. Технологія Power over Ethernet (PoE) являє собою фундаментальну парадигму в проектуванні сучасних мережевих інфраструктур, що забезпечує одночасну передачу високошвидкісних даних та електричної енергії постійного струму (DC) через єдину кабельну систему на базі мідної витої пари, таку як Cat5e, Cat6 або кабелі вищих категорій. Основна концепція цієї технології полягає в радикальному спрощенні топології підключення кінцевих пристроїв шляхом усунення необхідності прокладання паралельних електричних ліній для живлення. Ця інновація не лише оптимізує капітальні витрати на створення інфраструктури, але й значно розширює можливості розміщення обладнання в локаціях, де доступ до традиційних розеток змінного струму є обмеженим або неможливим.

На фізичному рівні технологія працює за принципом інжекції низьковольтного постійного струму в кабелі Ethernet без порушення цілісності трафіку.

Оскільки стандарти Ethernet є ізольованими мережами, кожна вита пара всередині кабелю підключається до спеціалізованого імпульсного трансформатора даних на обох кінцях лінії зв'язку. Устаткування, що подає

живлення, вводить напругу постійного струму через центральні відводи цих трансформаторів. Суть цього інженерного рішення полягає в тому, що сигнал даних у мережах Ethernet передається як диференціальний сигнал (різниця потенціалів між двома провідниками однієї пари), тоді як електричне живлення подається як синфазний сигнал, де струм тече паралельно по обох провідниках пари в одному напрямку. Завдяки такій фізичній розв'язці, постійний струм не створює магнітних перешкод у трансформаторі для диференціального сигналу, гарантуючи абсолютну чистоту високошвидкісного трафіку.

Для розуміння розгортання PoE необхідно розглянути класифікацію обладнання та топологічні моделі побудови мережі. Будь-яка екосистема PoE базується на взаємодії двох фундаментальних типів пристроїв: Power Sourcing Equipment (PSE – джерело живлення) та Powered Devices (PD – пристрій споживання).

PSE – це активне мережеве обладнання, функціональним призначенням якого є генерація, управління та інжекція електричної енергії постійного струму в кабельну інфраструктуру Ethernet. PSE виконує роль інтегратора: він об'єднує потоки даних зі стандартизованим електричним живленням перед їх спільною відправкою до мережевого вузла. До категорії PSE відносяться мережеві комутатори з вбудованою підтримкою PoE, спеціалізовані маршрутизатори, автономні інжектори живлення, а також промислові медіаконвертери. Здатність конкретного PSE постачати енергію визначається його внутрішнім блоком живлення та відповідністю конкретному стандарту (802.3af, 802.3at або 802.3bt), що диктує максимальну потужність, доступну на один порт.

PD – це кінцевий мережевий пристрій, який використовує технологію PoE для отримання і даних, і електричного струму через один і той самий роз'єм Ethernet (зазвичай RJ45). PD не має власного незалежного підключення до електромережі і повністю покладається на енергію, яку постачає PSE. Номенклатура пристроїв PD надзвичайно широка і постійно зростає з появою нових стандартів. Вона включає IP-камери спостереження (від базових до складних PTZ-моделей), бездротові точки доступу тощо.

Методологія постачання живлення від PSE до PD може бути реалізована через дві основні топологічні конфігурації, вибір яких залежить від існуючої інфраструктури та вимог проекту.

У конфігурації Endspan (кінцевий проліт) функцію PSE виконує сам мережевий комутатор, оснащений портами PoE. Комутатор знаходиться на кінці кабельного прольоту і безпосередньо генерує як дані, так і живлення. Це найбільш інтегрований підхід до побудови мережі, оскільки він дозволяє системним адміністраторам централізовано управляти живленням (наприклад, дистанційно перезавантажувати пристрої шляхом відключення живлення на порту) через інтерфейс управління комутатором. Ця топологія є стандартом де-факто для нових інсталяцій та масштабних проектів модернізації.

Топологія Midspan (проміжний проліт) застосовується у сценаріях, коли існуючий мережевий комутатор виконує лише передачу даних і не підтримує технологію PoE, але його заміна є економічно недоцільною. У цьому випадку

між комутатором та кінцевим пристроєм встановлюється проміжний пристрій – PoE-інжектор. Інжектор отримує чистий сигнал даних від комутатора, додає до нього електричну напругу і передає комбінований сигнал далі до PD. Це ідеальне рішення для додавання одиничних PoE-пристроїв (наприклад, однієї нової камери чи точки доступу) до існуючої традиційної мережі.

Окремим випадком топології є використання медіаконвертерів, таких як Perle S-1110HP, які поєднують функції перетворення середовища передачі (від оптоволокна до міді) з потужним PoE інжектором. Оптичний кабель не проводить електричний струм, тому він використовується для передачі даних на великі відстані, а медіаконвертер, розміщений безпосередньо біля кінцевого обладнання, інжектує живлення в короткий сегмент мідного кабелю, поєднуючи переваги обох технологій.

PoE джерела діляться на класи з потужністю від 4 до 60 ват на порт.

Структура стандартного мережевого кабелю типу вита пара передбачає наявність чотирьох пар мідних провідників, підключених до восьми контактів конектора RJ45. Механіка розподілу живлення по цих парах залежить від швидкості мережі (10/100 Мбіт/с проти 1000 Мбіт/с) та стандарту PoE. Існує два основні режими інжекції, які визначають, які саме контакти використовуються для передачі постійного струму: Режим A (Alternative A або Mode A) та Режим B (Alternative B або Mode B).

У мережах Fast Ethernet (10Base-T та 100Base-TX) для передачі даних традиційно використовуються лише дві з чотирьох пар провідників. Інші дві пари залишаються вільними або «запасними».

У цьому режимі A (Mode A) електрична енергія інжектується безпосередньо в ті самі дві виті пари, по яких передаються пакети даних. З точки зору розпіновки, це означає, що напруга подається на контакти 1, 2, 3 та 6. Цей режим живлення дозволяє максимально ефективно використовувати існуючі провідники і є типовим для PoE-комутаторів.

Режим B (Mode B) використовує для передачі енергії ті самі вільні, або запасні, пари, які не задіяні у передачі даних у 100-мегабітних мережах. Позитивна напруга зазвичай прикладається до контактів 4 і 5, а негативна напруга – до контактів 7 і 8. Режим B використовується зовнішніми PoE-інжекторами. Пристрої, що живляться від напруги 24 В, майже завжди використовують Режим B.

Ситуація стає дещо іншою при переході на гігабітні мережі, де для передачі даних використовуються всі чотири виті пари одночасно для досягнення високої пропускної здатності. В таких мережах концепція «вільних пар» зникає. Тому, незалежно від того, чи працює PSE в режимі A, чи в B, електричний струм завжди накладається поверх високочастотного сигналу даних за допомогою методу фантомного живлення через трансформатори.

Основою сумісності та стрімкого поширення технології є послідовна еволюція стандартів, що розробляються комітетом IEEE 802.3. Кожен новий етап розвитку відображався у вигляді нових розділів до базового стандарту, послідовно збільшуючи обсяги переданої енергії для задоволення потреб нових

поколінь кінцевого обладнання. Усі стандартизовані пристрої інтероперабельні між собою.

Стандарт IEEE 802.3af (PoE / Type 1) також відомий як базовий PoE або Type 1, був офіційно прийнятий у 2003 році. Він заклав основи передачі енергії по двох витих парах кабелю. Згідно зі специфікаціями даного стандарту, джерело PSE здатне видавати до 15,40 Вт потужності на порт. Проте, враховуючи природні втрати на опір у кабелі довжиною до 100 метрів, стандарт гарантує доставку мінімум 12,95 Вт безпосередньо на роз'єм кінцевого пристрою PD. Цей стандарт використовується для живлення датчиків присутності, простих систем контролю доступу та базових статичних камер відеоспостереження, які не вимагають високих енергозатрат.

Поява стандарту IEEE 802.3at (PoE+/Type 2) у 2009 році пояснюється зростаючими потребами у продуктивності мережевого обладнання. Максимальна потужність, що генерується PSE, була підвищена майже вдвічі – до 30,0 Вт. На кінці кабельної лінії PD гарантовано отримує до 25,5 Вт. Стандарт вимагає використання кабельних систем Cat 5 або вище, чий опір не перевищує 12,5 Ом на лінію. Він оптимально підходить для складних керованих PTZ-камер (Pan, Tilt, Zoom) з моторними приводами та бездротових точок доступу стандарту 802.11n/ac, які вимагають значно більших енергоресурсів для живлення багатоантенних радіомодулів.

Затверджений у 2018 році стандарт IEEE 802.3bt (PoE++/4PPoE/Hi-PoE) здійснив революцію в індустрії, збільшивши доступну потужність майже втричі. Головна архітектурна зміна полягала в обов'язковому використанні всіх чотирьох витих пар кабелю Ethernet для передачі енергії. Це стандарт дозволяє PSE видавати до 60 Вт потужності, гарантуючи при цьому до 51 Вт безпосередньо для PD після врахування втрат у кабелі. Це ідеально підходить для високопродуктивних бездротових точок доступу Wi-Fi 6/7 та складних систем контролю доступу з біометричними сканерами.

Зведена інформація по стандартам PoE подано в таблиці 6.1.

Таблиця 6.1 – Характеристика стандартів PoE

Стандарт IEEE	Тип PoE	Назва	Класи	Макс. потужність від PSE (Вт)	Доступна потужність на PD (Вт)	Використані пари	Типове застосування
802.3af	Type 1	PoE	0-3	15,40	12,95	2 пари	Датчики, статичні IP-камери
802.3at	Type 2	PoE+	4	30,00	25,50	2 пари	PTZ-камери, бездротові точки доступу 802.11n/ac
802.3bt	Type 3	PoE++ / 4PPoE	5, 6	60,00	51,00	4 пари	AP Wi-Fi 6, масиви мікрофонів, AV-обладнання
802.3bt	Type 4	PoE++ / 4PPoE	7, 8	90,00	71,30	4 пари	Розумне освітлення, інтерактивні дисплеї, ноутбуки

Основним інженерним принципом цієї технології є гарантування абсолютної зворотної сумісності всіх поколінь обладнання PoE. Це означає, що модернізація центральних комутаторів не вимагає негайної заміни тисяч кінцевих пристроїв.

Сучасний PSE (наприклад, комутатор 802.3bt/Type 4) без будь-яких проблем розпізнає найстарішу IP-камеру стандарту 802.3af (Type 1), коректно класифікує її як пристрій Класу 0 або 3, і подасть їй необхідні 15,4 Вт по двох витих парах, ігноруючи додаткові можливості. Системному адміністратору не потрібно виконувати жодних додаткових конфігурацій; процес повністю автоматизований.

Значно складнішим є сценарій, коли до існуючої застарілої інфраструктури (наприклад, комутатора PoE 802.3af з лімітом 15,4 Вт) підключають сучасний пристрій високої потужності (наприклад, Wi-Fi 6 точку доступу 802.3at, яка потребує 30 Вт). У такій ситуації під час апаратного узгодження точка доступу повідомить свій Клас 4. Комутатор зрозуміє, що він не здатен задовольнити цей запит. У цьому випадку спрацьовує механізм зниження потужності. PSE повідомляє PD про свою обмеженість, виділяючи йому лише доступні 15,4 Вт. Далі поведінка PD залежить від його внутрішнього мікропрограмного забезпечення. Деякі пристрої (як-от моторизовані PTZ-камери) можуть взагалі відмовитися включатися, блимаючи індикатором помилки, оскільки їм фізично не вистачає струму для старту моторів. Більш інтелектуальні пристрої (наприклад, сучасні Wi-Fi точки доступу) перейдуть у режим обмеженої функціональності – вони успішно завантажаться на потужності 15,4 Вт, але програмно відключать ресурсомісткі компоненти (наприклад, вимкнуть радіомодуль 5 ГГц або деактивують USB-порти), продовжуючи надавати базовий сервіс в очікуванні модернізації інфраструктури.

Потрібно пам’ятати, що живлення камер по PoE незважаючи на зручність і перспективність має певне обмеження. Довжина кабелю, який транслює відеопотік без суттєвих втрат і напруга живлення від комутатора до камери відеоспостереження, не повинна перевищувати 100 метрів (92 м). Цей поріг можна подолати декількома способами: застосуванням PoE репітерів (повторювачів), або використанням конвертерів VDSL2.

Розрахунок потужності та вибір кабелів. Проектування CCTV вийшло за межі простого вибору камер та реєстраторів. Сьогодні цей процес являє собою складну інженерну задачу, де центральне місце займає розрахунок енергетичного бюджету та топологія кабельних мереж. Надійність передачі відеосигналу та стабільність живлення є факторами, оскільки найменша деградація сигналу або просідання напруги може призвести до втрати важливих кадрів, некоректної роботи інтелектуальних модулів аналітики або повного виходу обладнання з ладу в екстремальних умовах.

Першим етапом будь-якого професійного проектування є детальний аудит споживання енергії всіма елементами системи. Камери

відеоспостереження, як основні споживачі, мають нерівномірний графік навантаження, що зумовлено їх динамічною роботою.

Енергоспоживання камер варіюється залежно від їхнього призначення, роздільної здатності та наявності механічних елементів. Статичні камери, як правило, демонструють базове споживання, яке забезпечує роботу сенсора та процесора обробки сигналу. Проте поява камер високої роздільної здатності (4K та вище) внесла корективи в енергетичні розрахунки, оскільки такі пристрої потребують значних обчислювальних потужностей для стиснення відеопотоку в реальному часі (табл. 6.2).

Основним чинником зростання потужності є перехід у нічний режим. Активація інфрачервоних світлодіодів може подвоїти або навіть потроїти споживання енергії. У камерах з великою дальністю підсвічування (до 100-300 метрів) використовуються потужні лазерні або матричні діоди, які створюють значне теплове навантаження, що іноді потребує активації внутрішнього кулера для охолодження сенсора.

PTZ-камери є найбільш енергоємними компонентами через наявність двигунів панорамування, нахилу та масштабування. Під час ініціалізації або виконання туру патрулювання споживання досягає пікових значень. Крім того, в умовах суворого клімату внутрішні термостати активують тени при зниженні температури нижче певного рівня (наприклад, +6°C), що забезпечує стабільну роботу механізмів та запобігає запотіванню об’єктива. Ввімкнення підігріву може додати до енергобюджету камери від 15 до 40 Вт залежно від моделі.

Таблиця 6.2 – Енергоспоживання відеокамер в різних режимах

Тип камери та її функціональні особливості	Споживання вдень (Вт)	Споживання вночі (ІЧ увімк.) (Вт)	Пікове навантаження (Вт)
Аналогова камера (стандартна роздільна здатність)	3-5	7-10	12
IP-камера початкового рівня (2 Мп)	5-8	10-12	15
Професійна 4K IP-камера з AI-аналітикою	10-15	15-22	25
PTZ-камера (поворотно-похила)	12-15	25-35	40-60
Спеціалізована PTZ-камера з обігрівом та потужною ІЧ	30-40	60-85	90-120

Відеореєстратори (NVR або DVR) споживають енергію не лише для роботи центрального процесора, а й для живлення встановлених жорстких дисків. Один диск корпоративного рівня споживає в середньому 5-7 Вт у режимі запису, проте його пусковий струм під час розкручування шпинделя може досягати 15-20 Вт.

Загальний енергетичний бюджет системи розраховується як сума всіх номінальних потужностей з обов’язковим додаванням 20-30% резерву для компенсації втрат у кабелях та забезпечення стабільної роботи при пікових навантаженнях.

Вибір кабелю є вирішальним фактором, що визначає якість зображення та довговічність системи. Кожен тип провідника має свої електричні

характеристики, які необхідно зіставляти з відстанню та потужністю обладнання.

Однією з головних проблем при проектуванні ліній живлення 12 В DC є падіння напруги на значних відстанях. Камери відеоспостереження вкрай чутливі до вольтажу – зниження напруги до 10,5-10,8 В може призвести до мерехтіння зображення, відключення ІЧ-підсвічування або повної відмови пристрою. Для розрахунку падіння напруги використовується закон Ома у формі для постійного струму. Важливо враховувати, що струм проходить шлях від джерела до камери і назад, тому опір розраховується для подвоєної довжини лінії. Падіння напруги можна визначити як:

$$V_{cn} = \frac{2LI\rho}{A}, \tag{6.2}$$

де L – відстань до камери (м), I – струм споживання (А), ρ – питомий опір провідника (0.0175 Ом*мм²/м для міді), А – поперечний переріз жили (мм²). Використання цієї формули дозволяє точно підібрати переріз кабелю для забезпечення допустимого відхилення напруги не більше 10%.

Перехід на систему живлення 24 В AC дозволяє значно збільшити дистанцію передачі енергії. Оскільки напруга вища, струм для передачі тієї ж потужності менший, що пропорційно зменшує втрати у вольтах. Крім того, допустиме падіння напруги для змінного струму часто становить до 20%, що робить такі системи більш стійкими на великих об’єктах.

Ринок насичений кабелями з обмідненого алюмінію (CCA), які на 30-50% дешевші за мідні. Проте алюміній має вищий опір, меншу механічну міцність та схильність до окислення. Для систем живлення та PoE використання CCA є неприпустимим на відстанях понад 30 метрів, оскільки це призводить до значного перегріву кабелю та нестабільної роботи обладнання.

Для вибору ДБЖ та акумуляторних батарей необхідно знати сумарну потужність навантаження та бажаний час автономної роботи. Формула розрахунку ємності акумулятора виглядає наступним чином:

$$C = \frac{PT}{V\eta}, \tag{6.3}$$

де P – загальна потужність (Вт), T – час роботи (год), V – напруга акумулятора (зазвичай 12В), η – ККД інвертора (приймається за 0,8-0,85).

Слід враховувати, що акумулятори втрачають ємність при низьких температурах та з часом (деградація пластин). Тому рекомендується обирати ємність з 20-30% запасом. Крім того, при використанні свинцево-кислотних АКБ (AGM/GEL), не варто розряджати їх нижче 30% залишку, щоб не допустити незворотних хімічних процесів.

Зовнішні камери є ідеальною мішенню для грозових розрядів. Пряме влучання блискавки трапляється рідко, але вторинні наведення –

електромагнітні імпульси, що виникають у кабелях при розряді поблизу – знищують порти обладнання щосезону.

Ефективна система захисту включає:

– модулі блискавкозахисту (встановлюються на обох кінцях довгих ліній (біля камери та біля комутатора). Вони відводять надлишковий потенціал на шину заземлення);

– заземлення (опір контуру заземлення для систем відеоспостереження повинен бути не більше 4 Ом);

– розв'язка (для найбільш відповідальних ділянок використовується гальванічна розв'язка або перехід на оптичне волокно, яке фізично не може проводити електричний розряд блискавки).

Типові проблеми живлення відеокамер та шляхи їх вирішення. Забезпечення стабільного та якісного електроживлення є фундаментальним аспектом проектування, монтажу та подальшої експлуатації систем відеоспостереження будь-якого масштабу. Статистика сервісних центрів та досвід провідних інженерних компаній свідчать про те, що понад сімдесят відсотків усіх несправностей у комплексах безпеки прямо чи опосередковано пов'язані з порушеннями в енергетичному ланцюзі. Проблеми можуть варіюватися від повної відсутності сигналу через вихід з ладу блоку живлення до тонких артефактів зображення, спричинених електромагнітними завадами або земляними петлями. Сучасна архітектура систем відеоспостереження вимагає від фахівця не лише базових знань електротехніки, а й глибокого розуміння специфіки передачі потужності через Ethernet (PoE), особливостей функціонування імпульсних джерел живлення та хімічних процесів у накопичувальних елементах систем безперебійного живлення.

Системний підхід до діагностики передбачає поділ проблем на кілька ієрархічних рівнів: технічні помилки на етапі проектування, фізичні пошкодження компонентів та експлуатаційні фактори. Однією з найбільш очевидних причин непрацездатності відеокамери є повна відсутність енергії, що може бути наслідком розрядженого джерела безперебійного живлення, аварії в загальній електромережі або спрацювання запобіжників. Проте існують і більш складні випадки, коли блок живлення формально працює (індикатори світяться), але не видає необхідну силу струму для запуску апаратної частини пристрою або роботи жорстких дисків у відеореєстраторі.

Постійні перезавантаження системи, «зависання» інтерфейсу та уривчаста трансляція відео часто свідчать про те, що обладнання працює на межі своїх енергетичних можливостей. Зокрема, відеореєстратори можуть циклічно перезавантажуватися через несправність власного адаптера живлення (зазвичай 12 В, 3-5 А), який з часом втрачає здатність стабілізувати напругу під навантаженням. Окрім того, фізичні чинники, такі як удари, акти вандалізму, перегрів або тривала робота при екстремально низьких температурах, призводять до деградації ізоляції та мікротріщин у друкованих платах, що стає причиною коротких замикань або плаваючих контактів.

Експлуатація камер у зовнішніх умовах вносить додатковий рівень ризику. Герметичність корпусу є важливим параметром – проникнення вологи всередину викликає корозію конекторів, що не лише погіршує якість передачі сигналу, а й може призвести до повного виходу обладнання з ладу через коротке замикання. Зимовий період характеризується ризиком появи льоду, який при розширенні здатний руйнувати структуру захисного шару провідників та корпусів. Важливо розуміти, що блоки живлення, особливо ті, що встановлені у вуличних боксах, піддаються значному тепловому стресу. Високі температури прискорюють висихання електролітичних конденсаторів, що веде до зростання амплітуди пульсацій на виході та нестабільності роботи цифрових процесорів камери.

Активація інфрачервоного (ІЧ) підсвічування є моментом істини для будь-якої системи живлення. Вдень камера споживає мінімальну кількість енергії (зазвичай 3-5 Вт), необхідну для роботи сенсора та процесора. Вночі, коли вмикається блок ІЧ-світлодіодів, споживання зростає вдвічі, а то й втричі.

Якщо блок живлення або лінія передачі розраховані без запасу, виникає характерний «ефект нічного перезавантаження». Камера працює нормально до настання сутінків, потім датчик освітленості подає сигнал на ввімкнення ІЧ-модуля, струм різко зростає, напруга на довгій лінії падає нижче критичної межі, і камера перезавантажується. Після перезавантаження камера знову намагається увімкнути нічний режим, і цикл повторюється нескінченно.

Окрім проблем із живленням, нічна зйомка може страждати від зовнішніх факторів:

– мерехтіння зображення (може бути спричинене раптовою зміною освітлення (фари авто, вуличні ліхтарі), що змушує камеру постійно перемикатися між режимами «день» і «ніч»);

– артефакти від часток у повітрі (пил, сніг або краплі дощу відбивають ІЧ-промені назад у лінзу, що створює ефект «шуму» і змушує процесор працювати на вищих потужностях, що також підвищує енергоспоживання);

– несправність ІЧ-фільтра (механічний перемикач може заклинити через низьку напругу, що призведе до некоректної передачі кольорів удень або повної відсутності картинки вночі).

Для вирішення цих проблем рекомендується використовувати блоки живлення з запасом потужності не менше 30% від максимального споживання системи. В окремих випадках доцільно вимикати вбудоване підсвічування через веб-інтерфейс та встановлювати автономні ІЧ-прожектори з власним джерелом живлення.

Більшість систем відеоспостереження сьогодні базуються на імпульсних блоках живлення. Їхніми перевагами є високий ККД (до 98%), здатність працювати в широкому діапазоні вхідної напруги (від 100 до 240 В) та компактні розміри. Проте вони є джерелом високочастотних завад. Якісні моделі використовують багатоступеневі вихідні фільтри для згладжування пульсацій, що критично для стабільної роботи цифрових сенсорів.

При виникненні проблем у роботі системи інженер повинен слідувати чіткому протоколу для швидкої локалізації причини.

Крок 1 – візуальний та апаратний контроль індикації. Перевірка наявності світлової індикації на блоці живлення, комутаторі та самій камері. Більшість IP-камер мають приховані світлодіоди біля порту RJ-45, які сигналізують про наявність живлення та активність мережевого обміну.

Крок 2 – вимірювання напруги під навантаженням. Використання мультиметра для вимірювання напруги на клемній колодці камери. Важливо робити це саме в момент роботи пристрою (найкраще – імітуючи нічний режим, закривши об'єктив рукою для активації ІЧ-підсвічування). Напруга без навантаження може бути в межах норми, але різко падати при включенні додаткових вузлів.

Крок 3 – перевірка кабельної траси та з'єднань. Огляд роз'ємів на наявність окислення. Перевірка цілісності оболонки кабелю. У випадку з PoE – тестування кабелю мережевим тестером для виявлення обривів або перехрещень жил. Максимальна довжина Ethernet-кабелю без підсилювачів не повинна перевищувати 100 метрів.

Крок 4 – метод виключення компонентів. Підключення камери через короткий заводський патч-корд безпосередньо до перевіреного джерела живлення або PoE-порту. Якщо камера запускається – проблема в лінії. Якщо ні — проблема в апаратній частині самої камери або в програмному забезпеченні (наприклад, помилка прошивки або конфлікт IP-адрес).

Крок 5 – діагностика відеореєстратора та накопичувачів. Якщо система «гальмує» або відео йде уривками, причиною часто є не камера, а жорсткий диск, якому не вистачає струму для стабільного обертання шпинделя або зчитування даних. Рекомендується тимчасово відключити HDD і перевірити роботу системи без нього.

Контрольні питання:

1. Які основні переваги та недоліки імпульсних джерел живлення порівняно з класичними трансформаторними блоками?
2. Для чого в системах живлення відеоспостереження рекомендується використовувати коефіцієнт запасу потужності не менше 30%?
3. Поясніть різницю між фізичними одиницями вимірювання «юніт» (U) та стандартною шириною 19 дюймів у монтажних шафах.
4. Які компоненти забезпечують активну терморегуляцію всередині кліматичної шафи та для чого вони потрібні?
5. Назвіть основне призначення блискавкорозрядника (ПЗІП) у слабкострумовій шафі та опишіть принцип його підключення.
6. У чому полягає фізична суть передачі живлення по PoE: як струм передається через кабель Ethernet, не заважаючи передачі даних?
7. Порівняйте топології живлення Endspan та Midspan: у яких випадках доцільно використовувати кожну з них?

8. Які функціональні режими відеокамери (наприклад, ІЧ-підсвічування чи підігрів) найбільше впливають на пікове енергоспоживання?

9. Як розрахувати необхідну ємність акумулятора для забезпечення автономної роботи системи відеоспостереження?

10. Опишіть причини та механізм виникнення «ефекту нічного перезавантаження» відеокамери.

Література: [2].

Тема 7. Пристрої зберігання та обробки відео

План:

Призначення та особливості застосування відеореєстраторів типу NVR, DVR, HVR, CarDVR та XVR. Кодеки стиснення даних. Жорсткі диски для систем відеоспостереження: типи, об’єм, надійність. Типовий функціонал реєстраторів і його налаштування.

Призначення та особливості застосування відеореєстраторів типу NVR, DVR, HVR, CarDVR та XVR. Еволюція систем відеоспостереження за останні два десятиліття трансформувала галузь безпеки з пасивного моніторингу в інтелектуальну екосистему прогнозування та аналізу інцидентів. В основі цієї трансформації лежить розвиток технологій запису та обробки відеосигналу, де перехід від аналогових до цифрових і мережевих архітектур визначив нові стандарти ефективності. Сучасний ринок пропонує розгалужену класифікацію відеореєстраторів, кожен з яких оптимізований під конкретні інфраструктурні умови, бюджетні обмеження та вимоги до глибини аналітики. Розуміння технічних нюансів таких пристроїв, як DVR, NVR, HVR, XVR та CarDVR, є важливим для системних інтеграторів та фахівців з безпеки, оскільки вибір архітектури реєстратора визначає не лише якість поточного моніторингу, але й життєздатність всієї системи в довгостроковій перспективі. Вибір конкретного типу залежить від того, які камери планується використовувати (аналогові чи цифрові) та в яких умовах вони працюватимуть.

Відеореєстратор – це пристрій, призначений для запису, тривалого зберігання з подальшим відтворенням будь-якого фрагмента відеозапису.

Цифрові відеореєстратори DVR представляють собою технологію, яка дозволила перевести традиційне аналогове відеоспостереження в цифровий формат зберігання. Основний принцип роботи DVR полягає в централізованій обробці сигналу безпосередньо в корпусі реєстратора. Аналогові камери формують зображення та передають його у вигляді електричного сигналу через коаксіальний кабель. Після надходження сигналу на вхідні роз’єми BNC, вбудований у DVR аналогово-цифровий перетворювач виконує дискретизацію та квантування сигналу, перетворюючи його на цифровий потік, який згодом стискається та записується на жорсткий диск (рис. 7.1).

Така архітектура передбачає, що камери є відносно простими пристроями, які не мають власних обчислювальних потужностей для кодування відео. Це робить аналогові камери дешевшими порівняно з мережевими аналогами, що є вагомим фактором для бюджетних інсталяцій. Однак централізація обробки створює значне навантаження на процесор реєстратора, особливо при збільшенні кількості каналів або роздільної здатності.

Сучасні DVR пройшли шлях від роздільної здатності CIF та D1 до підтримки стандартів високої чіткості, таких як AHD, HD-TVI та HD-CVI. Ці технології дозволили передавати відео роздільною здатністю 1080p і навіть 4K по традиційному коаксіальному кабелю на значні відстані, що вдихнуло нове життя в застарілу інфраструктуру.

Рисунок 7.1 – Відеореєстратор DVR

Їх використовують в бюджетних системах спостереження для невеликих об’єктів захисту (магазини, приватні будинки тощо).

Їм характерне просте налаштування: підключив кабель – з’явилося зображення.

Своєрідним різновидом DVR реєстратора є PC-based DVR – це відеореєстратор у вигляді плати відеозахоплення на базі ПК (рис. 7.2).

Рисунок 7.2 – Плата PC-based DVR

Плата PC-based встановлюється на материнську плату комп’ютера.

Незважаючи на прогрес, DVR системи мають вроджені обмеження. По-перше, використання коаксіального кабелю вимагає окремих ліній живлення для кожної камери, що збільшує обсяг монтажних робіт. По-друге, аналоговий

сигнал схильний до електромагнітних перешкод, що може призводити до появи шумів та спотворень на зображенні при великій довжині кабельних ліній. По-третє, масштабованість DVR обмежена кількістю фізичних портів на задній панелі пристрою, а додавання навіть однієї камери понад ліміт вимагає заміни всього реєстратора або встановлення додаткового пристрою.

Мережеві відеореєстратори NVR (рис. 7.3) представляють собою наступний етап еволюції, де обробка відеосигналу децентралізована. На відміну від DVR, реєстратор типу NVR не має вбудованих аналогово-цифрового перетворювача. Замість цього, функцію кодування та стиснення відео виконує сама IP-камера. Камера перетворює світловий потік на цифровий сигнал, стискає його (наприклад, за допомогою кодека H.265) і передає готовий пакет даних через локальну мережу LAN до NVR.

NVR виконує роль спеціалізованого сервера, який приймає цифрові потоки, зберігає їх на дискових масивах і забезпечує інтерфейс для перегляду та аналізу. Така архітектура дозволяє системі бути надзвичайно гнучкою – камери можуть розташовуватися в будь-якій точці мережі, а передача даних може здійснюватися через мідну виту пару, оптоволокно або бездротові канали Wi-Fi.

Головною перевагою NVR є підтримка надвисокої роздільної здатності. Оскільки реєстратор не витрачає ресурси на оцифрування, він може обробляти потоки 4K (8MP), 12MP і навіть 32MP, що практично недоступно для традиційних аналогових систем. Крім того, IP-системи забезпечують значно вищу якість зображення завдяки відсутності подвійного перетворення сигналу (з аналогу в цифру і навпаки), що мінімізує втрати деталей кадру.

Ще одним важливим елементом NVR є використання технології PoE. Це дозволяє передавати і дані, і електроживлення по одному кабелю Cat5e або Cat6, що радикально спрощує інсталяцію та знижує витрати на кабельну інфраструктуру.

Рисунок 7.3 – Відеореєстратор NVR

Однак залежність від мережі є одночасно і слабким місцем NVR. Пропускна здатність мережі стає вразливим ресурсом – при великій кількості камер з високою роздільною здатністю мережа може перевантажуватися, що призводить до затримок або втрати кадрів. Для вирішення цієї проблеми професійні NVR використовують окремі мережеві інтерфейси для камер та клієнтського доступу, а також підтримують протоколи багаторівневого керування потоками.

У перехідний період, коли об'єкти вже оснащені аналоговою інфраструктурою, але потребують поступового впровадження IP-технологій, на ринок вийшли гібридні пристрої. Гібридний відеореєстратор HVR, або HDVR, поєднує в собі функції DVR та NVR. Він має фізичні входи BNC для аналогових камер та мережевий порт для підключення IP-камер.

Традиційні HVR зазвичай мали жорсткі обмеження щодо розподілу каналів (наприклад, тільки 8 аналогових + 8 IP). Подальшим розвитком цієї ідеї став XVR (eXtended Video Recorder) реєстратор. XVR є найбільш універсальним пристроєм у сучасній індустрії відеоспостереження, оскільки він підтримує одночасну роботу з п'ятьма основними форматами відеосигналу: HD-CVI, HD-TVI, AHD, CVBS (аналог) та IP.

Ключовою особливістю XVR є функція автоматичного розпізнавання сигналу. Реєстратор самостійно ідентифікує тип підключеної аналогової камери, що усуває необхідність ручного налаштування кожного каналу. Більш того, XVR дозволяють гнучко змінювати конфігурацію: користувач може відключити аналоговий вхід і отримати замість нього додатковий IP-канал.

Цей тип реєстраторів ідеально підходить для проектів модернізації. Наприклад, на об'єкті можна залишити старі аналогові камери для загального огляду території, але додати кілька 4K IP-камер для ідентифікації облич на вході, використовуючи один і той самий XVR для керування всією системою. Це забезпечує максимальний захист інвестицій, дозволяючи оновлювати систему поетапно.

Автомобільні відеореєстратори CarDVR виділяються в окрему категорію через специфіку середовища експлуатації. На відміну від стаціонарних систем, CarDVR повинні працювати в умовах постійної вібрації, широкого температурного діапазону та нестабільного живлення. Їхнє основне призначення – фіксація дорожньої обстановки для вирішення спірних ситуацій при ДТП, моніторинг поведінки водія та безпека вантажів.

Кожен тип відеокамер краще використовувати тільки зі своїм типом відеореєстраторів. Незважаючи на існуючі стандарти (ONVIF і PSIA) для інтеграції обладнання різних виробників часто виникають проблемні ситуації.

Відеореєстратори будь-яких типів мають цілу лінійку моделей, яка підрозділяється за кількістю каналів, до яких підключають відеокамери.

Загальноприйнятим вважається лінійка, що складається з 4-х, 8-й і 16-ти канальних реєстраторів. У лінійках NVR можуть зустрічатися моделі, які мають до 32-х вхідних відеоканалів.

Відеореєстратори всіх типів крім відео дозволяють записувати і звуковий канал з відеокамери. Кількість входів може змінюватися в залежно від моделі.

Для збільшення тривалості запису відеореєстратора в корпус можна встановити один або кілька жорстких дисків. Професійні моделі мають порт e-Sata для підключення зовнішніх масивів (HDD), що дозволяє значно збільшити глибину архіву.

Для захисту від втрати або псування записаних даних в професійних реєстраторах використовують резервне копіювання інформації, використовуючи технології RAID 0 або RAID 1.

RAID 0 (striping – «чергування») – дисковий масив з двох або більше жорстких дисків без резервування. Інформація розбивається на блоки даних фіксованої довжини і записується на кілька дисків по черзі. Таким чином, ймовірність втрати інформації через відмову одного диска зменшується майже в два рази.

RAID 1 (mirroring – «віддзеркалення») – масив з двох або більше дисків, є повними копіями один одного. Імовірність втрати інформації через відмови відразу двох дисків дорівнює добутку ймовірностей відмови кожного диска.

Відеореєстратори будь-яких типів мають подібний зовнішній вигляд.

На передню панель зазвичай виносяться світлодіодні індикатори підключення реєстратора до мережі живлення, контролю роботи жорсткого диска і локальної мережі, а також індикатор тривоги.

Для зручності користувачів на передню панель може бути винесено USB роз’єм для підключення комп’ютерної мишки.

Основні елементи, розташовані на задній панелі DVR відеореєстратора і їх призначення наведені на рисунку 7.4.

Для об’єднання великої кількості відеореєстраторів в єдину систему відеоспостереження використовують програмне забезпечення CMS. Це ПЗ присутнє в комплекті поставки до відеореєстраторів.

Кожен порт комутатора підключається до порту мережі відеореєстратора, а один з портів комутатора підключається до комп’ютера, на якому встановлено програмне забезпечення CMS. За допомогою цього ПЗ можна оперативно переглядати інформацію з відеокамер, аналізувати інформацію, збережену на жорстких дисках.

Мережеві NVR відеореєстратори відрізняються тим, що у них роз’єми для підключення відеокамер можуть бути як відсутні так і присутні. Останній варіант передбачає вмонтований у середину реєстратора мережевого комутатора (рис. 7.5).

Всі відеокамери підключаються до NVR відеореєстраторів через комутатори, які об’єднують всю відеоінформацію в один потік. Цей потік надходить по кабелю UTP в мережевий порт відеореєстратора.

Одним з найбільш значущих аспектів сучасних реєстраторів є можливість віддаленого доступу. Традиційні методи, такі як прокидання портів та використання DDNS, поступово витісняються більш безпечними та простими в налаштуванні P2P-технологіями.

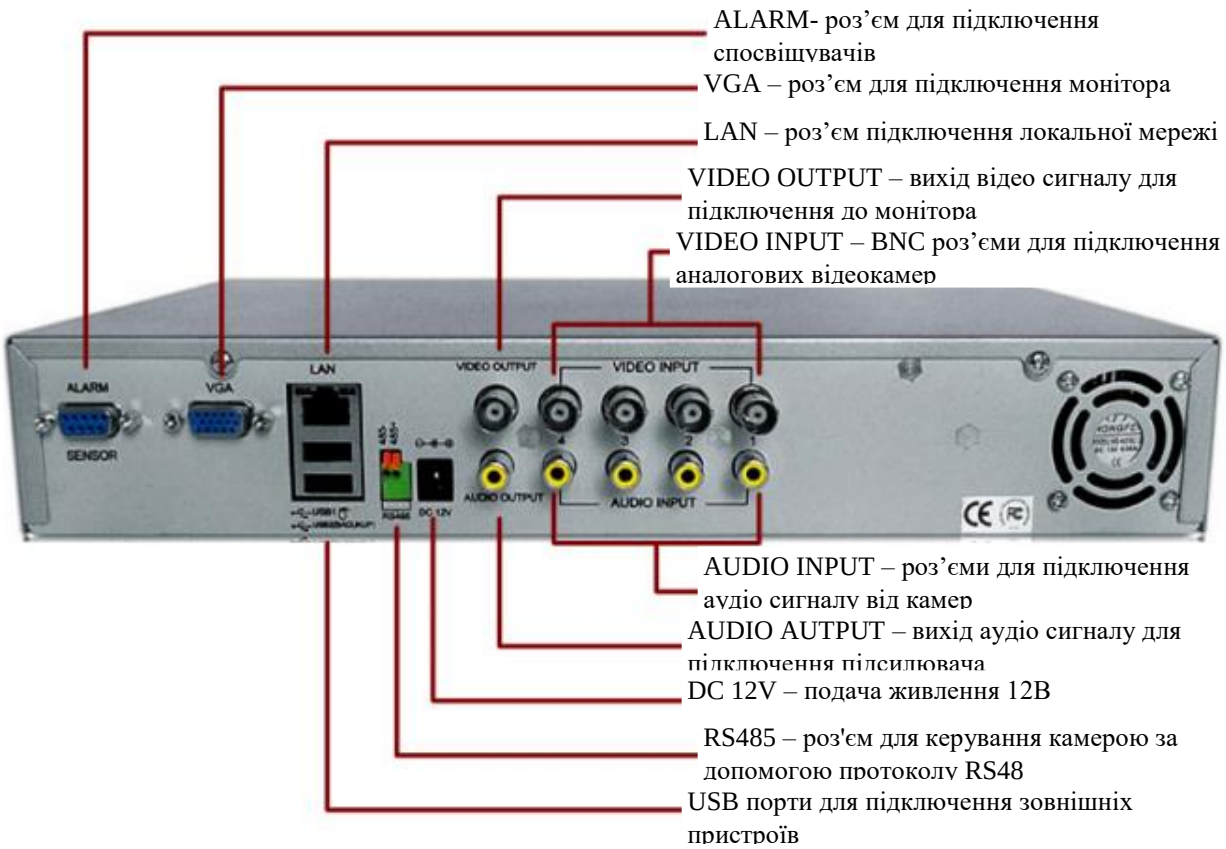


Рисунок 7.4 – Призначення елементів задньої панелі DVR відеореєстратора

Рисунок 7.5 – Задня панель NVR відеореєстратора з роз’ємом для підключення до мережевого комутатора

Методи віддаленого доступу є наступні: P2P (Peer-to-Peer), Port Forwarding та VPN (Virtual Private Network).

Перший метод P2P пристрій реєструється на хмарному сервері виробника за унікальним ID. Користувач підключається до хмари, яка виступає посередником для встановлення прямого зашифрованого з’єднання зі смартфоном або ПК. Це не потребує відкриття портів на роутері, що значно підвищує рівень безпеки.

Другий метод Port Forwarding потребує ручного відкриття портів на маршрутизаторі та наявності статичної білої IP-адреси. Цей метод створює прямий шлях із зовнішнього інтернету до реєстратора, що робить систему вразливою до атак типу «brute force» та сканування портів.

Метод VPN є найбільш безпечним для корпоративного сектора. Реєстратор знаходиться всередині приватної мережі, і доступ до нього можливий лише через зашифрований тунель. Це виключає пряму видимість пристрою в глобальній мережі.

Сьогодення показує, що питання кібербезпеки стає дедалі гострішим. NVR-системи, будучи повноцінними мережевими вузлами, потребують регулярного оновлення прошивок, використання складних паролів та двофакторної автентифікації для запобігання несанкціонованому доступу до конфіденційного відеоматеріалу.

Сучасні відеореєстратори, особливо типу NVR та AI NVR, перетворилися на потужні аналітичні платформи. Завдяки використанню графічних процесорів та спеціалізованих нейронних процесорів, реєстратори здатні виконувати складні завдання в реальному часі.

Ключовим функціями AI-аналітики реєстраторів є: розпізнавання обличь та атрибутів, захист периметра, розпізнавання номерних знаків транспортних засобів тощо.

Можливість створення баз даних обличь, пошук за статтю, віком, наявністю окулярів або маски дозволяє автоматизувати контроль доступу та розслідування інцидентів.

Функція виявлення перетину віртуальної лінії або вторгнення в зону з інтелектуальною фільтрацією об’єктів дозволяє системі ігнорувати рух листя, дощ або тварин, реагуючи лише на людей або транспортні засоби, що знижує кількість помилкових тривог на 90%.

Функція розпізнавання номерних знаків (LPR/ANPR) дозволяє автоматично зчитувати номери для керування шлагбаумами або ведення логів відвідування парковок.

Тенденції 2025 року вказують на зростаючу роль Edge AI – технології, де первинний аналіз виконується камерою, а реєстратор здійснює фінальну агрегацію даних та забезпечує взаємодію з іншими системами безпеки, такими як контроль доступу та пожежна сигналізація.

Вибір типу реєстратора безпосередньо впливає на сукупну вартість системи відеоспостереження. Хоча DVR та XVR системи мають нижчу початкову вартість обладнання, витрати на монтаж складних кабельних мереж можуть нівелювати цю різницю.

Для великих підприємств з розвиненою IT-інфраструктурою NVR є безальтернативним вибором завдяки можливості централізованого керування тисячами камер через VMS-платформи. Для малого бізнесу або приватних домогосподарств, де вже прокладено коаксіальний кабель, найбільш раціональним є вибір XVR, який дозволяє отримати доступ до сучасних функцій без капітальної перебудови мережі.

Таким чином, сучасний спектр технологій відеореєстрації демонструє чіткий поділ на масовий сегмент (XVR) та професійний мережевий сегмент (NVR). DVR в його класичному розумінні практично зник, поступившись місцем універсальним XVR-платформам, які підтримують цифрові стандарти високої чіткості. CarDVR продовжують розвиватися як автономні пристрої інтелектуальної допомоги водієві, інтегруючи функції ADAS та хмарне резервне копіювання критичних моментів.

У найближчій перспективі спостерігатиметься подальша конвергенцію локальних реєстраторів із хмарними сервісами. Це дозволить створювати гібридні сховища, де найбільш важливі метадані та короткі ролики подій зберігаються в хмарі для миттєвого доступу, а повний архів високої роздільної здатності знаходиться на локальних дисках реєстратора. Інтеграція алгоритмів глибокого навчання та великих мовних моделей для пошуку по відео змінить саму парадигму роботи оператора, перетворивши його з пасивного спостерігача на куратора інтелектуальної системи безпеки. Таким чином, вибір відеореєстратора сьогодні – це не просто купівля пристрою для запису, а рішення, що визначає здатність організації швидко реагувати на загрози та ефективно використовувати накопичені дані для оптимізації бізнес-процесів.

Кодеки стиснення даних. Кодек – це частина програмного забезпечення, яке може використовувати обладнання для «кодування» відеофайлів під час їх створення, а також для «декодування» того ж типу відео для відтворення. Фактично, слово «кодек» – це просто комбінація слів «код» та «декодувати». Необроблені відеодані без стиснення можуть займати дуже багато місця. Це особливо актуально для контенту з високою роздільною здатністю або контенту з надвисокою роздільною здатністю, наприклад 1080p та 4K відповідно.

Зі збільшенням роздільної здатності камер до 4K і вище, навантаження на підсистему зберігання даних зросло експоненціально. Це зумовило перехід від застарілого стандарту H.264 до високоефективного кодування відео H.265 (HEVC).

Деякий час, та навіть зараз, H264 був фантастичним методом стиснення і до цієї пори залишається популярним використовуваним кодеком. Це пов’язано з тим, що H264 пропонує вражаюче стиснення з мінімальною втратою якості та не дуже сильно навантажує систему кодування. Переважна більшість обладнання може з лімітованими зусиллями кодувати відеодані з використанням як програмних, так і апаратних версій H264. Фактично, більшість камер відеоспостереження донедавна та, отже, переважна більшість систем відеоспостереження, які були встановлені багато років тому, використовують кодек H264. Для стиснення до 2 мегапікселів це було і залишається нормальним по більшості стандартів.

Однак по мірі того, що середня якість відеоконтенту стає все вище і вище в роздільній здатності, так як кількість пікселів в зображенні має величезний вплив на розмір файлу, то постала потреба у рішенні, що перевершує за потужністю стиснення H264. З огляду на це з’явився новий кодек стиснення H265. Він може зменшити розмір файлу приблизно на 64% при роздільній

здатності 4К та на 57% при роздільній здатності 1080р, ніж його аналог H264. Однак це відбувається за рахунок більшої обчислювальної потужності.

Перевага H.265 полягає в здатності динамічно змінювати розмір блоків кодування, що дозволяє передавати складні сцени з меншою кількістю артефактів та при значно нижчому бітрейті. Впровадження фірмових надбудов, таких як H.265+ або Smart Codec, дозволяє реєстраторам аналізувати статичні фони та передавати лише зміни в рухомих об'єктах. Це може зменшити обсяг займаного місця на жорсткому диску до 70-90% у порівнянні зі стандартним H.264, що є важливо для великих архівів.

У відеореєстраторах можна керувати цифровим потоком, використовуючи режими VBR і CBR.

На перший погляд все просто: в камері є заводські налаштування відеопотоків, відштовхуючись від яких проектувальник розраховує проект, інсталятор цей проект виконує.

Складнощі починаються відразу ж: якого саме розміру потік видає камера «з коробки»? Чи достатньо його щоб забезпечити прийнятну якість зображення? Що значить «змінний», як він змінюється і коли?

CBR (скорочення від «constant bit rate», в перекладі – «постійний потік даних», він же «сібіер», він же «констант біт Рейт», він же «постійний бітрейт») – означає, що камера видає сталий відеопотік, що не залежить від інших параметрів (може коливатися в межах ± 10%). Ця величина визначається в налаштуваннях камери. За замовчуванням різні виробники для різних лінійок камер обмежують потік для CBR в районі 2-х, 3-х, 4-х Мбіт/с.

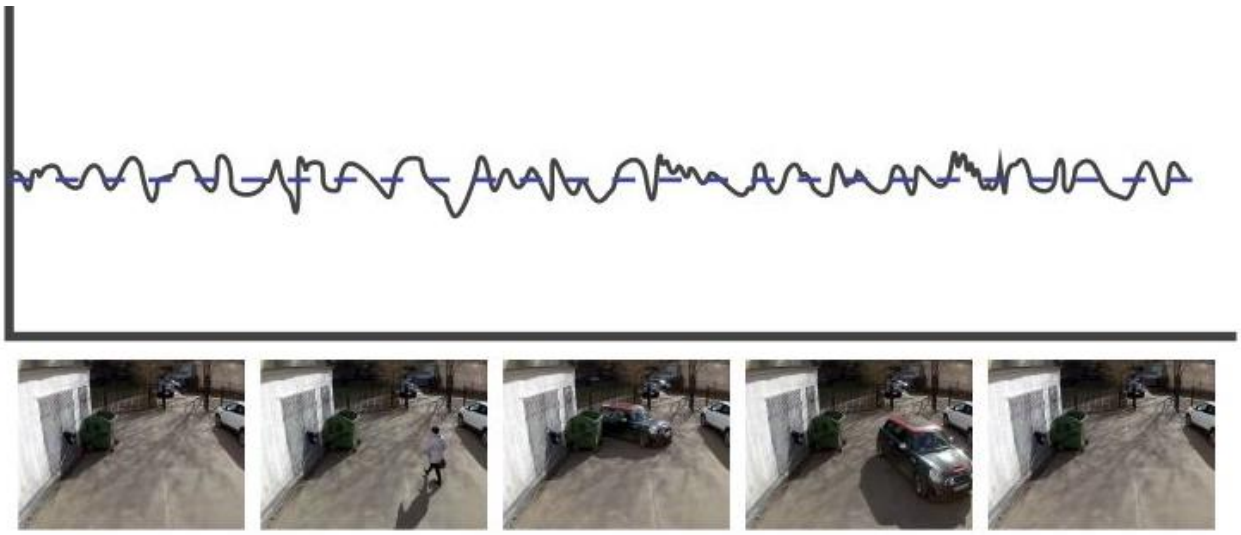


Рисунок 7.6 – Відеопотік при кодуванні в CBR

Очевидно зручний тим, що під нього легко порахувати необхідний дисковий простір і підібрати комутатори. Потрібно розуміти, що 10 к/с із середнім розміром кадру в 100 КБ і 25 к/с із середнім розміром 40 Кбайт в результаті дають один і той же потік. Який варіант більше влаштує? Менша швидкість з кращою якостю чи середня якість «живого відео»? Щоб отримати відповіді, потрібно звернути увагу на пов'язану з режимом CBR опцію завдання

користувачем пріоритету (Priority). В результаті отримаємо такі сценарії роботи:

– пріоритет швидкості (speed або rate):

У цьому випадку при ускладненні картинки (пройшли люди, проїхав автомобіль, з'явилися перешкоди або шуми через зниження освітленості) камера буде намагатися зберігати задану швидкість і при досягненні потоком заданої величини – збільшувати ступінь стиснення зображення з одночасним погіршенням якості. Погіршення може виявитися досить серйозним, аж до грубих артефактів і повної нерозбірливості картинки.

– пріоритет якості (quality):

Тепер при ускладненні картинки камера буде прагнути зберігати задану якість зображення, а кількість кадрів за секунду при цьому може зменшуватися (щоб не вийти за заданий розмір CBR). Візуально нагадує роботу аналогової камери в режимі накопичення кадрів. Очевидний мінус – ризик пропустити щось важливе через зниження FPS.

– пріоритет однаковий (none):

Означає, що однаково важливі як швидкість, так і якість – і тоді при досягненні заданого порогу передачі даних будуть погіршуватися обидва параметри.

Як видно, доводиться йти на жертви. Чи не йти? А якщо поставити великий розмір потоку? Надмірна. З запасом. Скажімо, поставити відразу 10 Мбіт/с. Але наслідком буде невиправдано велика вартість мережевого обладнання (лінії зв'язку, високопродуктивні комутатори) і висока вартість відеосерверів з великими дисковими сховищами.

Отже, режим CBR знижує максимальне навантаження на мережу, але не знижує навантаження на ЦП відеосервера, тому що кількість необхідних для роботи відеоаналітики опорних кадрів не змінюється. Налаштування опорних кадрів і налаштування CBR/VBR в камерах не залежать один від одного.

VBR (означає «variable bit rate», в перекладі – «змінний потік даних», він же «вібіер», він же «варіейбл біт Рейт») – інший підхід до формування вихідного потоку. Працює так: в меню камери задається конкретне значення якості зображення (ступінь стиснення), після чого потік генерується «як є», розміром пропорційно складності зображення. Гарна освітленість, малий рух, нерухома камера – і вихідний потік не перевищує мегабіт-другий. Якщо ж ситуація почне змінюватися (пішли люди, поїхали машини, замиготіли ліхтарі або навіть шум підріс через зниження освітленості) – відеопотік збільшиться пропорційно, без «різання» швидкості або якості (рис. 7.7). Однак, тут інші складності: VBR за визначенням за розміром річ змінна і теоретично необмежена (залежить тільки від продуктивності «начинки» камери). Якщо камера є керованою (PTZ), то при повороті або масштабування потік зростає в рази або навіть на порядки. Можливі сумні наслідки:

– перевантаження мережевих з'єднань і/або комутаторів, що тягне застигання картинки, пропуски кадрів і т.п.;

– перевантаження відеосерверов (аж до зависань) через що дані можуть залишитися незаписані, а відеоаналітіка - взагалі перестати працювати;

– система все-таки справляється, але глибина архіву зменшується.

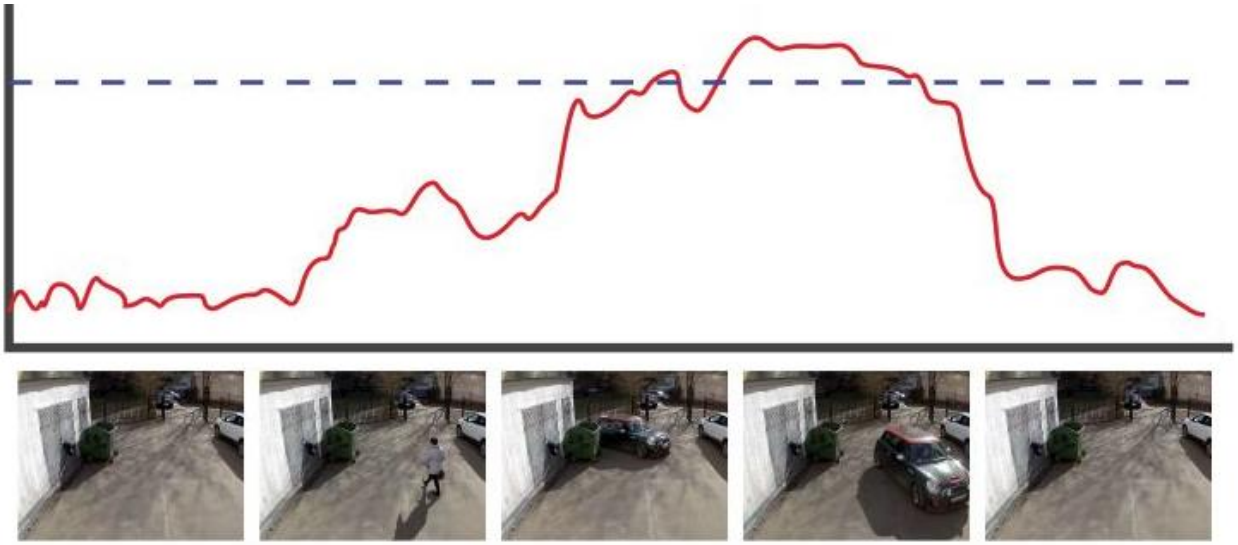


Рисунок 7.6 – Відеопотік при кодуванні в VBR

Щоб уникнути значних перевантажень багато виробників наділили VBR налаштуванням, що обмежує максимальний розмір потоку (коротко кажучи, «обмеження зверху»). Це дасть гарантію, що потік не зросте вище певної величини і саме від цієї величини треба буде виходити при розрахунку трафіку. Розраховувати ж архіви слід виходячи із середнього значення потоку. Конкретну максимальну і середню величину можна визначити або калькуляторами виробників камер, що імітують спостереження обстановки, або досвідченим шляхом.

Отже, CBR доцільно використовувати при необхідності укластися в твердо задану і при тому невисоку пропускну здатність лінії зв’язку (коли перевантажувати канал не можна ні в якому разі). Крім того, CBR підходить для спостереження за статичними об’єктами (наприклад, приміщення, яке однаково освітлене днем-вночі-влітку-взимку з однією і тією ж ситуацією в полі зору камери).

VBR з можливістю обмеження «зверху» (варіанти типу Zipstream) - рекомендовано для задач спостереження, не прив’язаних жорстко до пропускної здатності IP-каналів. Дозволяє отримати якісне зображення з заданим темпом, незалежно від умов експлуатації.

Жорсткі диски для систем відеоспостереження: типи, об’єм, надійність. Еволюція систем безпеки від аналогових замкнутих контурів до інтелектуальних мереж відеоаналітики змінила вимоги до інфраструктури зберігання даних. У сучасному середовищі жорсткий диск перестав бути просто периферійним пристроєм – він є вузлом, від якого залежить цілісність доказової бази та стабільність роботи всієї системи безпеки. Системи відеоспостереження працюють у режимі безперервного запису, що створює навантаження, з яким

стандартні накопичувачі для персональних комп'ютерів не здатні впоратися в довгостроковій перспективі.

Фундаментальна відмінність між жорстким диском для відеоспостереження та стандартним накопичувачем полягає в їхньому призначенні та конструктивній витривалості. Десктопні диски розроблялися для сценаріїв використання, де активна робота триває приблизно 8 годин на добу, а навантаження розподілене між читанням та записом даних. Натомість системи відеоспостереження вимагають безперервної експлуатації в режимі 24/7, де частка операцій запису досягає 90-95% від загального робочого циклу.

У сучасних мережевих відеореєстраторах NVR, що містять 8, 16 або більше дискових відсіків, накопичувачі стикаються з проблемою обертальної вібрації. Кожен працюючий диск створює мікроколивання, які передаються через раму пристрою на сусідні накопичувачі. Для боротьби з цим явищем професійні серії дисків оснащуються спеціальними RV-датчиками (датчиками обертальної вібрації).

Ці датчики, що представляють собою високочутливі акселерометри, що фіксують зовнішні коливання і передають сигнал системі керування актуатором голівок. Система миттєво вносить корективи в положення голівки, компенсуючи вібрацію та запобігаючи помилкам позиціонування. Накопичувачі без RV-датчиків у багатодискових кошиках демонструють стрімке падіння продуктивності, оскільки голівки постійно збиваються з вузьких доріжок даних, що змушує диск виконувати повторні операції пошуку.

Механічна конструкція спеціалізованих дисків враховує ці особливості. У десктопних моделях шпиндель зазвичай фіксується лише з одного боку, що допустимо для короткочасних навантажень. Проте в професійних серіях для відеоспостереження, таких як WD Purple, Seagate SkyHawk або Toshiba S300, шпиндель фіксується з обох боків корпусу. Таке рішення дозволяє зменшити радіальний відгук дискового пакета на 50%, що важливо для мінімізації помилок запису в умовах постійної вібрації. Окрім цього, спеціалізовані диски використовують потужніші магніти голосової котушки та міцніші демпферні пластини для позиціонування голівок, що забезпечує швидше прискорення та точніше фокусування на доріжці даних навіть при інтенсивних вібраційних впливах.

На світовому та українському ринках домінують три ключові виробники: Western Digital, Seagate та Toshiba. Кожен із них пропонує ієрархічну структуру продуктів, розділену на базові рішення для малих систем та професійні моделі для корпоративних середовищ з підтримкою штучного інтелекту.

WD Purple є однією з найбільш впізнаваних лінійок у галузі безпеки. Ключовою технологією тут є AllFrame 4K, яка оптимізує керування кеш-пам'яттю для зменшення втрат кадрів та покращення відтворення архіву.

WD Purple розраховані на навантаження до 180 ТБ/рік. Ці диски зазвичай мають швидкість обертання шпинделя 5400 або 5640 об/хв, що сприяє меншому енергоспоживанню та тепловиділенню, що є важливим для компактних реєстраторів без активного охолодження.

WD Purple Pro призначені для передових систем з використанням штучного інтелекту. Вони підтримують до 64 камер високої чіткості одночасно з 32 додатковими потоками для AI-аналітики. Ці моделі працюють на швидкості 7200 об/хв та мають ліміт навантаження до 550 ТБ/рік.

Seagate фокусується на інтелектуальному моніторингу та сервісах відновлення. Прошивка ImagePerfect розроблена для забезпечення плавного запису без пропущених кадрів у системах з високою інтенсивністю потоків.

Seagate SkyHawk підтримує до 64 камер і робоче навантаження 180 ТБ/рік. Однією з головних переваг є включення плану Rescue Data Recovery Services, який дозволяє відновити дані в лабораторії Seagate у разі фізичного пошкодження диска.

Накопичувачі Seagate SkyHawk AI оптимізовані для роботи в NVR з підтримкою штучного інтелекту. Вони витримують екстремальні навантаження до 550 ТБ/рік і демонструють на 15% вищу швидкість запису порівняно зі стандартними моделями (до 250 МБ/с).

У свою чергу Toshiba пропонує надійні рішення, які часто мають краще співвідношення ціни та продуктивності.

Накопичувач Toshiba S300 використовує технологію SMR (Shingled Magnetic Recording) у деяких моделях для збільшення щільності запису, що підходить для послідовного відеопотоку, але вимагає уваги при інтенсивному перезаписі.

Накопичувач Toshiba S300 Pro використовує виключно CMR (Conventional Magnetic Recording) і має швидкість обертання 7200 об/хв. Нове покоління цих дисків отримало збільшений буфер до 512 МБ, що забезпечує швидкість передачі даних до 281 МБ/с, випереджаючи конкурентів у певних тестових сценаріях.

Вибір об’єму жорсткого диска залежить від трьох основних факторів: роздільної здатності камер, частоти кадрів (FPS) та обраного кодека стиснення. Окрім цього, важливу роль відіграє режим запису – постійний або за детекцією руху.

Сучасні системи відеоспостереження переходять на стандарт H.265 та його вдосконалені версії, такі як H.265+. Кодек H.265 дозволяє скоротити обсяг даних на 40-50% порівняно з H.264 при збереженні аналогічної якості зображення. Технологія H.265+ йде ще далі, аналізуючи фонові елементи сцени і стискаючи їх інтенсивніше, що в статичних сценах може дати економію до 70-80%.

Для розрахунку загальної потреби дискового простору у спрощеному вигляді використовується формула:

$$V = \frac{B \times T \times N}{8 \times 1024} \qquad (7/1)$$

де V – необхідний об’єм у ТБ; B – бітрейт однієї камери в Мбіт/с; T – час зберігання в секундах; N – кількість камер.

Практичний приклад: для системи з 16 камер 4MP при 15 FPS з використанням H.265, де необхідний архів за 30 днів, розрахунок покаже потребу у приблизно 19-20 ТБ чистого простору. Враховуючи особливості форматування дисків та необхідність запасу, рекомендується встановлювати накопичувачі загальною ємністю 24 ТБ (наприклад, три диски по 8 ТБ).

Повна формула визначення об'єму жорсткого диску матиме наступний вигляд:

$$V = \frac{T\sum_{i=1}^{m}(b_i n_i t_i)3600}{8192} \tag{7.2}$$

де T – тривалість зберігання архіву, дн (визначається замовником); b_i – бітрейт i-ї камери, Mbit/c; n_i – кількість камер з i-м бітрейтом, шт; t_i – час запису i-ю камери протягом доби, год; 3600 – кількість секунд в годині; 8192 – кількість мегабіт в гігабайті (1 Кбайт = 1024 байт, 1 Мбайт = 1024 Кбайт, 1 Гбайт = 1024 Мбайт, 1 байт = 8 біт).

Надійність жорсткого диска визначається показниками MTBF (Mean Time Between Failures) або MTTF (Mean Time To Failure) та AFR (Annualized Failure Rate). Для сучасних дисків відеоспостереження MTBF зазвичай становить від 1 до 2,5 мільйонів годин. Однак важливо розуміти, що ці цифри є статистичними: MTTF у 1 мільйон годин означає, що при популяції в 1000 дисків один виходитиме з ладу кожні 1000 годин (приблизно кожні 42 дні).

Температура є головним чинником, що впливає на тривалість життя механічного накопичувача. Виробники вказують робочий діапазон до 65-70°C, проте оптимальною для тривалої експлуатації є температура близько 40°C.

Згідно з дослідженнями Toshiba, кожні 5°C підвищення температури понад 40°C збільшують річний рівень відмов (AFR) на 30%.

Постійна робота при температурі 55°C подвоює ймовірність виходу диска з ладу порівняно з роботою при 40°C.

Високі температури призводять до деградації мастила в підшипниках та мікроскопічних деформацій пластин, що зрештою викликає контакт голівки з поверхнею.

Хоча традиційні жорсткі диски HDD залишаються основним засобом зберігання через низьку ціну за терабайт, галузь починає трансформуватися. З впровадженням камер роздільної здатності 8K та необхідністю миттєвого пошуку в архівах за допомогою штучного інтелекту, швидкості інтерфейсу SATA (6 Гбіт/с) стає недостатньо.

З'являються рішення на базі NVMe, такі як Seagate SkyHawk NVMe (серія QM), що забезпечують швидкість до 3500 МБ/с. Це в 14 разів швидше за найкращі HDD. Очікується, що в найближчі 5 років системи будуть будуватися за гібридним принципом: NVMe SSD для оперативного аналізу та метаданих AI, а традиційні ємні HDD – для глибокого архівного зберігання. Також зростає роль Edge Storage – використання microSD карт промислового класу

безпосередньо в камерах для резервного запису у разі втрати зв'язку з сервером.

Вибір накопичувача для системи відеоспостереження – це рішення, яке безпосередньо впливає на надійність усієї системи безпеки. Аналіз підтверджує, що економія на купівлі десктопного диска замість спеціалізованого є ілюзорною – підвищений знос механіки та невідповідність прошивки призведуть до виходу диска з ладу протягом перших 6-12 місяців експлуатації.

Ключові рекомендації:

– слід обирати спеціалізовані серії (Purple, SkyHawk, S300) для роботи 24/7;

– для систем з 8 і більше дисками обов'язково використовуйте моделі з датчиками обертальної вібрації (RV);

– використовуйте сучасні кодеки (H.265 або H.265+) для оптимізації витрат на сховище;

– забезпечувати належне охолодження (температура всередині реєстратора не повинна перевищувати 45°C для досягнення заявленого MTBF);

– враховуйте робоче навантаження (для систем з AI-аналітикою використовуйте диски класу Pro/AI з лімітом 550 ТБ/рік).

Професійний підхід до вибору накопичувача гарантує, що в критичний момент необхідний відеозапис буде доступний і цілісний, що є першочерговим завданням будь-якої системи відеоспостереження.

Типовий функціонал реєстраторів і його налаштування. Типовий функціонал реєстраторів у системах відеоспостереження (DVR / NVR) включає такі основні можливості.

1. Запис відео:

– безперервний запис – 24/7;

– запис за розкладом (у визначені години/дні);

– запис за подією (при виявленні руху або тривоги);

– передзапис/постзапис (кілька секунд до та після події.

Налаштування здійснюють наступні: вибір режиму запису для кожного каналу, встановлення якості (роздільна здатність, бітрейт), частота кадрів (FPS), кодек стиснення (H.264, H.265).

2. Підтримка камер:

– аналогові (для DVR);

– IP-камери (для NVR);

– підтримка ONVIF;

– керування PTZ-камерами (поворот, нахил, зум).

Налаштування здійснюють наступні: додавання камер вручну або автоматичний пошук, вказання IP-адреси, логіна, пароля, налаштування зон огляду та пресетів PTZ.

3. Детекція руху:

– виявлення руху в кадрі;

– налаштування зон детекції;

– регулювання чутливості.

Налаштування здійснюють наступні: виділення області мишкою, становлення рівня чутливості, прив’язка до запису або сповіщення.

4. Архів і відтворення:

– пошук по даті/часу;

– пошук по подіях;

– експорт фрагментів (USB, мережа).

Налаштування здійснюють наступні: вибір формату експорту (AVI, MP4), встановлення періоду збереження, перезапис при заповненні диска.

5. Мережеві функції:

– віддалений доступ через браузер або мобільний додаток;

– P2P-підключення;

– підтримка DDNS.

Налаштування здійснюють наступні: призначення статичної IP-адреси, налаштування портів, сканування QR-коду для мобільного додатку.

6. Керування користувачами:

– створення облікових записів;

– рівні доступу (адміністратор, оператор, гість);

– журнал подій.

Налаштування здійснюють наступні: встановлення складного пароля, обмеження доступу до окремих камер, увімкнення двофакторної автентифікації (якщо підтримується).

7. Зберігання даних:

– підтримка HDD/SSD;

– RAID (у професійних моделях);

– SMART-моніторинг дисків;

Налаштування здійснюють наступні: форматування диска, увімкнення автоматичного перезапису, налаштування сповіщень про помилки диска.

8. Тривожні входи/виходи:

– підключення датчиків (руху, відкриття дверей);

– сирени або світлові сигнали.

Налаштування: призначення дії на тривогу, затримка спрацювання, повідомлення на e-mail або телефон.

Основні рекомендації з налаштування наступні:

– змінити стандартний пароль одразу після встановлення;

– оновити прошивку реєстратора;

– налаштувати запис за рухом для економії місця;

– встановити резервне копіювання важливих фрагментів;

– перевірити доступ із зовні (мобільний додаток).

Контрольні питання:

1. У чому полягає принципова різниця в архітектурі та процесі обробки сигналу між відеореєстраторами типів DVR та NVR?
2. Які формати відеосигналу здатні автоматично розпізнавати та підтримувати сучасні реєстратори типу XVR?
3. Охарактеризуйте переваги та недоліки використання PC-based DVR порівняно зі спеціалізованими автономними реєстраторами.
4. Для вирішення яких специфічних завдань призначені реєстратори типу CarDVR та в яких умовах вони мають стабільно працювати?
5. Порівняйте технології RAID 0 та RAID 1: як кожна з них впливає на надійність зберігання даних та швидкість роботи системи?
6. Які існують методи віддаленого доступу до відеореєстратора і який із них вважається найбільш безпечним для корпоративного сектора?
7. Назвіть ключові функції AI-аналітики, які реалізуються в сучасних реєстраторах (наприклад, AI NVR), та поясніть їхню користь для оператора.
8. Порівняйте ефективність кодеків H.264 та H.265: за рахунок чого H.265 дозволяє суттєво економити дисковий простір?
9. У чому полягає різниця між режимами керування цифровим потоком CBR та VBR і як вибір режиму впливає на планування об’єму архіву?
10. Які сценарії роботи виникають при встановленні пріоритету «швидкість» (speed) або «якість» (quality) у режимі CBR при ускладненні сцени спостереження?

Література: [1-4].

Тема 8. Передумови до проектування системи відеоспостереження

План:

Типи оперативних завдань відеоспостереження та їх особливості. Умовні графічні зображення типового обладнання. Методи вибору відеокамер і об’єктивів. Загальні вимоги до встановлення відеокамер.

Типи оперативних завдань відеоспостереження та їх особливості. Одним з основних параметрів, який враховується при виборі камери відеоспостереження є ступінь деталізації зображення, яка регламентується відповідними стандартами. Залежить вона від чіткості відображення об’єкта спостереження на моніторі та визначається завданнями, що стоять перед системою.

Основні завдання, що ставлять перед системою відеоспостереження, за ступенем деталізації зображення виділяють: моніторинг, детектування, огляд, розпізнання, ідентифікація тощо.

Під час вирішення оперативних завдань користуються критеріями світових стандартів.

На вибір обладнання для вирішення кожного з означених завдань впливають такі фактори як відстань до об’єкта, умови спостереження (погодні, час доби, умови освітленості).

Крім того, слід враховувати, що, наприклад, ідентифікація знайомої (для спостерігача) людини досягається простіше ніж незнайомої. Фіксація і розпізнання дій теж може вимагати різної деталізації.

Одна справа – зафіксувати, що людина взяла якийсь предмет (розпізнання дії), і якщо потрібно конкретно визначити, що це за предмет - слід враховувати його розміри, ідентифікаційні ознаки (завдання ідентифікації).

Таким чином, постановка задач перед системою відеоспостереження індивідуальна для кожного конкретного випадку, вимагає передбачливості при оцінці можливого розвитку подій.

Традиційно в аналогових системах відеоспостереження вимоги до розв’язання поставленого завдання формулюють виходячи з того, яку частину кадру по вертикалі повинен займати об’єкт спостереження, що реалізується на основі Британського стандарту охоронних систем 2009 року (рис. 8.1). Для різних цілей потрібна різна величина об’єкта в кадрі (табл. 8.1).

Наприклад, для виявлення людини в кадрі може бути досить, щоб його зростання становило 10% вертикального розміру. У той же час для розпізнавання (ідентифікації) людини може знадобитися, щоб його зріст становив 50% вертикалі кадру, а для ретельної ідентифікації - до 120% і більше.

З появою цифрових камер почали застосовувати нові способи встановлення відповідності експлуатаційним вимогам. Процентні співвідношення стосовно цифрових камер не використовують, а вимоги до роздільної здатності вказують в пікселях (замість ТВЛ) і користуються альтернативним параметром – «щільність пікселів», або кількість пікселів зображення на 1 м на відстані спостереження за об’єктом.

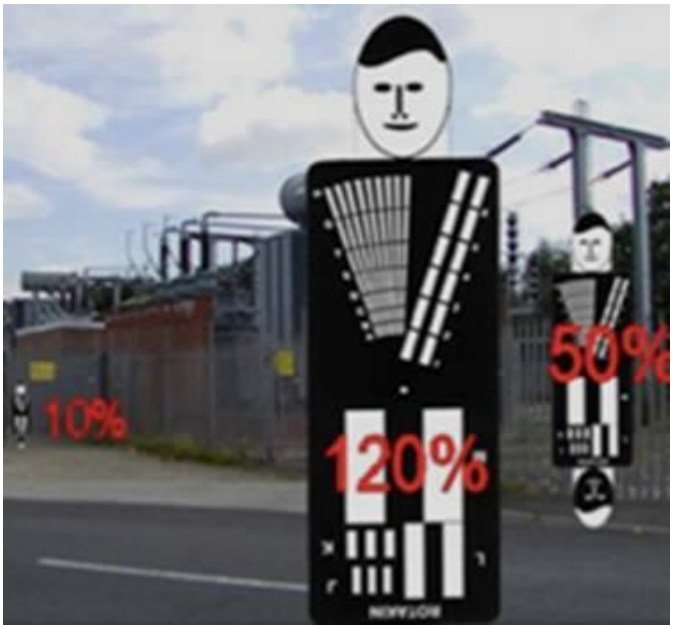


Рисунок 8.1 – Відображення тестового манекену на 10%, 50% і 120% від висоти зображення

Таблиця 8.1 – Критерії вирішення поставленого завдання до аналогового відеоспостереження

№ п/п	Вид активності	Задачі і можливості	Висота відображення в кадрі від загальної його висоти, %
1	Моніторинг	моніторинг і контроль натовпу	5%
2	Детектування	гарантоване виявлення людини в кадрі	10%
3	Спостереження	визначення характерних особливостей людини, наприклад одягу	25%
4	Розпізнавання	розпізнавання знайомих оператору людей	50%
5	Ідентифікація	якість, достатня для ідентифікації людини	100%
6	Інспектування	можливість 100% ідентифікації, яка виключає сумнів	400%

Таким чином, у багатопіксельних камерах відеоспостереження роздільна здатність характеризується загальною кількістю пікселів на площу матриці.

Роздільна здатність IP-камер визначається як добуток кількості пікселів по горизонталі і вертикалі матриці. Для того, щоб окремо визначити роздільну здатність по горизонталі і вертикалі слід врахувати співвідношення сторін матриці. Так для матриці формату 4:3 кількість пікселів за висотою визначається $n_в$ як:

$$n_в = 0{,}75 n_м \tag{8.1}$$

де 0,75 – коефіцієнт, який враховує співвідношення сторін матриці; $n_м$ – загальна кількість пікселів матриці, шт.

Кількість пікселів матриці за шириною визначається як:

$$n_ш = \sqrt{\frac{n_м}{0{,}75}} \tag{8.2}$$

Якщо відомий розмір поля зору і кількість пікселів за шириною матриці (табл. 8.2), то роздільна здатність зображення $n_з$ визначається як відношення кількість пікселів до поля зору:

$$n_з = \frac{n_ш}{A} \tag{8.3}$$

де A – розмір поля зору, м.

Таблиця 8.2 – Характеристики матриць типових відеокамер

Тип камери	Загальна кількість пікселів, $n_м$ шт	Кількість пікселів за висотою, $n_в$ шт	Кількість пікселів за шириною, $n_ш$ шт
HD 720	921.600	720	1280
1.3 MPix	1.310.720	1024	1280
HD 1080	2.073.600	1080	1920
2 MPix	1.920.000	1200	1600
3 MPix	3.145.728	1536	2048
5 MPix	4.915.200	1920	2560

Фокусна відстань ‘, залежно від типу поставленого завдання і відстані до об’єкта, визначається як:

$$f = \frac{Lhn_з}{n_ш} \tag{8.4}$$

де L – відстань до об’єкта, мм; h – ширина матриці, мм.

Таблиця 8.3 – Критерії вирішення поставленого завдання відповідно європейського стандарту EN 50 132-7

№ п/п	Вид активності	Задачі і можливості	Кількість пікселів на 1 м поля зору, $n_з$ шт
1	Моніторинг	моніторинг і контроль натовпу	12
2	Детектування	гарантоване виявлення людини в кадрі	25
3	Спостереження	визначення характерних особливостей людини, наприклад одягу	62
4	Розпізнавання	розпізнавання знайомих оператору людей	125
5	Ідентифікація	якість, достатня для ідентифікації людини та номерів транспортних засобів	250
6	Інспектування	можливість 100% ідентифікації, яка виключає сумнів	1000

Для інших об’єктів застосовуються інші критерії. Наприклад, для читання номерних знаків висота букв повинна складати приблизно 15 пікселів (що відповідає приблизно 200 пікселям/м).

Практично це означає, що проектувальник і замовник повинні визначитися з метою встановлення кожної камери (розпізнавання людей, ідентифікація, детектування, спостереження). І при підборі зони огляду камери слід розрахувати, при яких параметрах камери і об’єктиву в зоні огляду камери буде достатня щільність пікселів для обраної для камери завдання.

Проектувальнику треба знайти золоту середину між більшою щільністю пікселів, що дозволяє побачити більше деталей при меншому куті огляду, і більшою шириною зони огляду камери при більшому куті огляду, що дозволяє зменшити число камер в проекті.

У багатьох випадках, щоб забезпечити виконання завдань розпізнавання або ідентифікації людей, проектувальнику потрібно буде вибирати об’єктиви з великою фокусною відстанню або камери з більшою роздільною здатністю або міняти місце і висоту установки камери.

Якщо відеозаписи з камер передбачається використовувати в якості судових доказів, при виборі роздільної здатності необхідно також враховувати законодавчі та нормативні вимоги.

Умовні графічні зображення типового обладнання. На кресленнях планів проектів систем відеоспостереження відеокамера і сектор спостереження повинні бути представлені в такий спосіб:

– відеокамери на поверховому плані позначаються в місцях їх встановлення у вигляді умовних позначень (УГП) та орієнтують в потрібному напрямку (рис. 8.2);

– сектори спостереження представляють в двох проекціях (горизонтальній та вертикальній);

– знесення від камери повинна містити інформацію про номер камери, висоту її встановлення на вертикальній проекції і номер камери і фокусну відстань ‘ на горизонтальній проекції;

– сектори спостереження оформляються у вигляді проекції на землю кута спостереження камери, на якому наносяться зони ідентифікації, розпізнавання і виявлення (рис. 8.3).

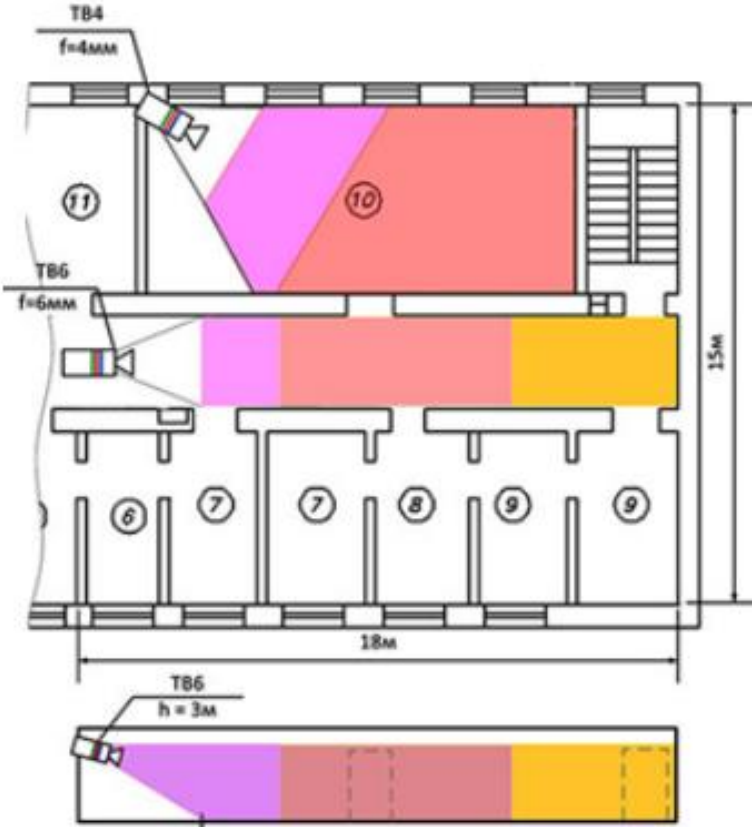


Рисунок 8.2 – Приклад використання УГП відеокамер на плані

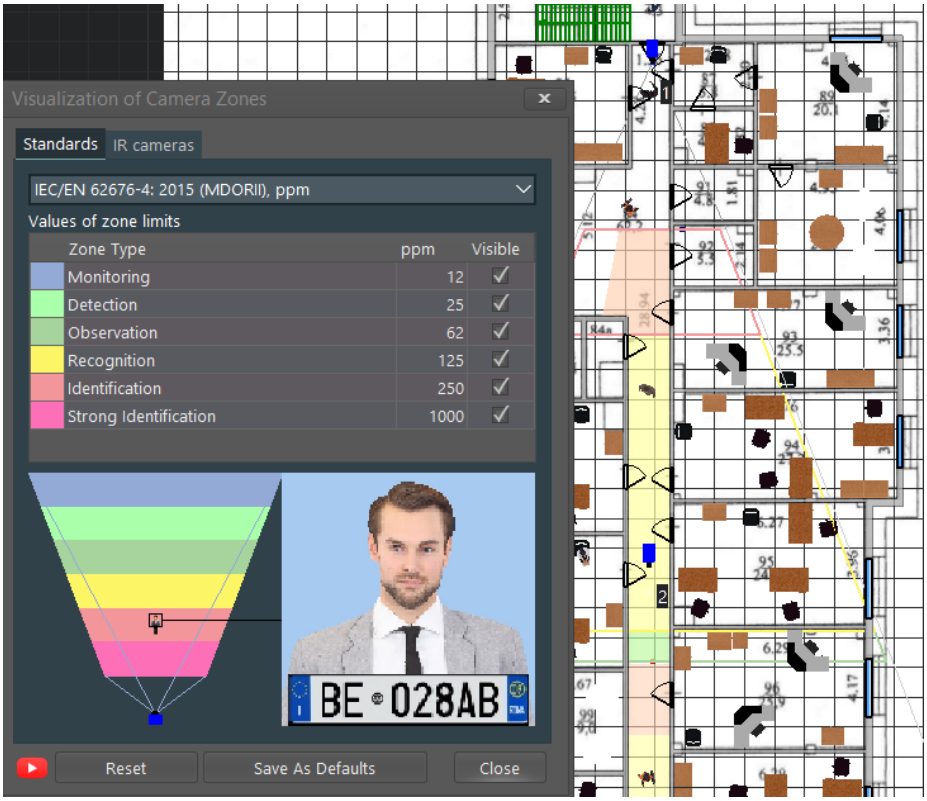


Рисунок 8.3 – Відображення камери та секторів спостереження на кресленнях

При виготовленні креслень на паперових носіях у ручний спосіб замість кольорової заливки різні зони виділяють відповідним штрихуванням.

На планах можна використовувати позначення відеокамер, які подано на рисунку 8.4.

Відеокамера Відеокамера в гермобоксі Поворотна відеокамера

Рисунок 8.4 – Умовні графічні позначення камер на кресленнях планів

Методи вибору відеокамер і об'єктивів. Процес вибору відеообладнання перетворився з простого порівняння технічних характеристик на складну дисципліну. Основою для прийняття рішення є розуміння того, як фізичні параметри обладнання впливають на фінальний візуальний ряд і яким чином вони корелюють із виробничими завданнями.

Вибір відеокамер і об'єктивів ґрунтується на визначенні мети спостереження, тобто поставленої оперативної задачі, умов освітлення та розміру об'єкта. Основні критерії: роздільна здатність, фокусна відстань, тип ‘ (фіксований/варіофокальний) і розмір сенсора.

Для того, щоб вибір камери та ‘ не був випадковим, професіонали використовують стандарт EN 62676-4, відомий як методологія DORI (Detection,

Observation, Recognition, Identification). Ця система визначає відстані, на яких камера з певними параметрами може виконувати конкретні завдання безпеки, виходячи з щільності пікселів на метр.

Для практичного розрахунку ідентифікації незнайомої людини часто використовується емпіричне правило: відстань ідентифікації дорівнює половині фокусної відстані ‘ (у метрах), тоді як розпізнавання знайомої особи можливе на відстані, що приблизно дорівнює фокусній відстані.

Вибір відеокамер та об’єктивів не є статичним процесом; він вимагає балансу між технічними можливостями, бюджетом та конкретними завданнями безпеки. Для загального огляду територій, наприклад, у Луцьку оптимальним вибором будуть IP-камери роздільною здатністю 4 Мп з об’єктивом 2,8 мм та технологією Smart Hybrid Light. Для ідентифікації на в’їздах необхідно використовувати вузькокутні об’єктиви (6 мм і більше) та камери з апаратним WDR 120dB.При проектуванні важливо спиратися на перевірених виробників та локальних постачальників, які надають офіційну гарантію та підтримку в Україні. Правильно підібрані компоненти – це не лише «картинка», а й гарантія того, що в критичний момент система виконає свою головну функцію – надасть неспростовні докази та допоможе запобігти інциденту.

Загальні вимоги до встановлення відеокамер. Сучасний стан розвитку технологій безпеки в Україні характеризується переходом від локальних засобів візуального контролю до інтегрованих інтелектуальних систем відеомоніторингу. Цей процес вимагає від фахівців не лише глибоких інженерних знань, а й ґрунтовного розуміння нормативно-правової бази, що регулює питання приватності, захисту персональних даних та технічної надійності. Встановлення відеокамер сьогодні не є виключно технічним актом – це складний процес, що поєднує конституційні гарантії людини, вимоги цивільного та трудового законодавства, а також суворі галузеві стандарти серії ДСТУ EN 62676. Аналіз поточної ситуації вказує на те, що системний підхід до монтажу відеообладнання є єдиним шляхом забезпечення як фізичної безпеки об’єктів, так і юридичної чистоти отриманих доказів.

В основі будь-якої діяльності із застосуванням технічних засобів фіксації в Україні лежить Конституція України. Стаття 32 Основного Закону чітко встановлює, що ніхто не може піддаватися втручанню в його особисте та сімейне життя, а збирання, зберігання та використання конфіденційної інформації про особу без її згоди не допускається. Оскільки зображення людини, що дозволяє її ідентифікувати, прямо відноситься до категорії персональних даних, будь-який процес встановлення відеокамер автоматично потрапляє під дію законодавства про захист персональних даних.

Цивільний кодекс України, зокрема стаття 307, виступає основним регулятором відносин у сфері зйомки фізичних осіб. Загальне правило вимагає отримання згоди особи на її знімання на відео- чи кіноплівку. Однак законодавець впровадив критично важливу норму – презумпцію згоди. Згідно з нею, згода особи на зйомку припускається, якщо вона проводиться відкрито в місцях публічного характеру: на вулицях, зборах, мітингах або конференціях.

Розуміння цієї норми є фундаментальним для монтажних організацій, адже воно визначає вимоги до відкритості встановлення камер та обов’язковості інформування.

Другий рівень правового регулювання забезпечується Законом України «Про захист персональних даних». Відеозапис, що дозволяє прямо (за рисами обличчя) або опосередковано (за майна, поведінки) ідентифікувати особу, розглядається як обробка персональних даних. Це накладає на власника системи (контролера) обов'язок забезпечити цільове використання даних, обмежити доступ до них та визначити чіткі терміни зберігання. Законопроект № 8153, який готується до впровадження, посилює ці вимоги, вводячи принцип «останнього засобу» (субсидіарності), згідно з яким відеокамери повинні встановлюватися лише тоді, коли безпекові цілі неможливо досягти іншими шляхами.

На робочих місцях відеоспостереження виконує подвійну функцію: забезпечення безпеки майна та контроль за дотриманням трудової дисципліни. Однак без належного оформлення таке спостереження є незаконним і може призвести до судових позовів працівників щодо втручання в особисте життя. Стаття 29 Кодексу законів про працю України зобов’язує роботодавця інформувати працівників про всі умови праці.

Процедура легального встановлення камер на підприємстві включає наступні кроки, які мають бути задокументовані:

– прийняття Наказу про організацію відеоспостереження (у документі має бути чітко прописана мета (наприклад, «запобігання розкраданню ТМЦ» або «забезпечення безпеки персоналу»), а не абстрактний контроль);

– внесення змін до Правил внутрішнього трудового розпорядку (це легітимізує відеозйомку як частину трудового процесу);

– розробка Положення про захист персональних даних (у ньому визначається порядок доступу до архіву, особи, відповідальні за його збереження, та процедура знищення записів);

– персональне інформування (хоча пряма «згода» працівника часто є дискусійною через нерівність сторін, підпис про ознайомлення з Положенням є важливим).

Заборона встановлення камер у зонах приватності є абсолютною. Розміщення технічних засобів у туалетах, душових, роздягальнях чи кімнатах для куріння є грубим порушенням, що тягне за собою кримінальну відповідальність за незаконне використання спецзасобів. Крім того, не рекомендується встановлювати камери в кабінетах, де працює одна людина (за винятком кас), оскільки це створює надмірний психологічний тиск, що суперечить принципам гідності праці.

Встановлення відеокамер у багатоквартирних будинках (ОСББ) регулюється нормами цивільного права щодо розпорядження спільним майном. Оскільки під’їзди, холи, ліфти та прибудинкова територія є власністю всіх мешканців, рішення про монтаж системи не може прийматися правлінням одноосібно.

Згідно із Законом «Про особливості здійснення права власності у багатоквартирному будинку», для встановлення камер необхідно отримати згоду власників, площа квартир яких становить понад 75% загальної площі будинку. Таке рішення оформлюється протоколом загальних зборів. Важливо, що при досягненні цього порогу меншість (ті, хто проти) зобов'язана підкоритися волі більшості та прийняти режим відеоспостереження як належне.

Приватне встановлення камери окремим мешканцем над власними дверима є правомірним лише в тому випадку, якщо об'єктив не фіксує внутрішню обстановку сусідніх квартир при відкритті дверей.

Відповідність технічних параметрів системи національним стандартам є гарантією її експлуатаційної придатності. Стандарт ДСТУ EN 62676-4:2017 «Правила застосування» визначає методику вибору камер, місць їх встановлення та параметрів якості зображення.

Якість монтажу кабельних мереж прямо впливає на надійність системи та захищеність від наводок. Згідно з ПУЕ (Правила улаштування електроустановок), усі лінії зв'язку мають бути захищені від механічних пошкоджень та впливу зовнішнього середовища.

Для зовнішнього монтажу критично важливим є ступінь захисту оболонки камери. В умовах України рекомендованим є рівень IP66 або IP67, що гарантує захист від сильних струменів води та пилу. Також при роботі в зимовий період камери повинні мати вбудований обігрів або працювати в широкому температурному діапазоні (від -30°C до +50°C).

Місце зберігання відеозаписів (серверна або ЦОД) має бути захищене від фізичного доступу сторонніх осіб та забезпечувати оптимальні умови для роботи накопичувачів даних.

Важливою вимогою є обмеження доступу до відеореєстраторів. Всі входи в серверну мають контролюватися СКУД, а в самому приміщенні повинна стояти окрема камера, що фіксує дії адміністраторів. Кабельні вводи в серверну обов'язково заповнюються вогнестійкими проходками, що запобігають поширенню полум'я та диму.

З початком 2026 року в Україні набули чинності оновлені правила безпеки в освітніх закладах, затверджені наказом МВС. Ці норми перетворюють відеоспостереження з факультативного заходу на обов'язковий стандарт безпеки.

Згідно з новими вимогами:

– обов'язковість встановлення (школи мають бути обладнані камерами в коридорах, на входах та на прилеглій території);

– термін зберігання (відеозаписи мають зберігатися не менше 30 діб);

– зони заборони (категорично заборонено ставити камери в туалетах, роздягальнях, душових, а також у кабінетах психологів та медичних кабінетах, де очікується високий рівень приватності);

– доступ батьків (омбудсмен наголошує, що вільний онлайн-доступ батьків до камер у класах є неприпустимим, оскільки це порушує приватність

інших дітей. Доступ може бути наданий лише до конкретного фрагмента запису у разі інциденту (бійки, травмування тощо)).

Важливо, що функції моніторингу не можуть виконувати педагоги; для цього мають залучатися професійні охоронці або представники поліції охорони. На входах до шкіл також передбачено встановлення металодетекторів, що інтегруються в загальну систему безпеки.

Юридична легітимність зйомки прямо залежить від якості інформування суб'єктів даних. Стаття 307 ЦК України вимагає «відкритості» зйомки, що найкраще реалізується через встановлення попереджувальних знаків.

Згідно з ДСТУ 7313:2013 та міжнародними рекомендаціями, сучасна табличка повинна бути не просто наклейкою, а джерелом інформації.

Таким чином, процес встановлення відеокамер в Україні в 2026 році – це комплексна інженерно-правова задача. Якість системи визначається не мегапікселями, а відповідністю операційним вимогам замовника та законодавчим обмеженням.

Для забезпечення максимальної ефективності та легітимності рекомендується: проводити оцінку впливу на захист даних перед початком проектування, особливо якщо планується використання функцій аналітики, суворо дотримуватися стандартів ДСТУ EN 62676 при виборі висот та кутів встановлення для гарантування потрібного рівня деталізації, забезпечувати фізичну та пожежну безпеку серверної інфраструктури згідно з ДБН, оскільки втрата архіву нівелює сенс існування системи, юридично оформлювати систему через локальні акти (накази, положення) та належне інформування суб'єктів через «розумні» таблички.

Відеоспостереження стає невід'ємною частиною цифрового суспільства України, і лише професійний підхід до його монтажу дозволить зберегти баланс між суспільною безпекою та невід'ємним правом людини на приватність.

Контрольні питання:

1. Назвіть основні типи оперативних завдань відеоспостереження за ступенем деталізації зображення (від найменшого до найбільшого).
2. Яку мінімальну висоту в кадрі (у відсотках) повинен займати об'єкт для виконання завдання «розпізнавання» згідно з Британським стандартом?
3. Поясніть сутність параметра «щільність пікселів» та в яких одиницях він вимірюється для цифрових камер.
4. Скільки пікселів на 1 метр поля зору необхідно забезпечити для виконання завдання «ідентифікація» згідно з європейським стандартом EN 50 132-7?
5. Яка щільність пікселів рекомендується для надійного читання номерних знаків транспортних засобів?
6. У чому полягає «золота середина» для проектувальника при виборі між щільністю пікселів та шириною зони огляду?
7. Яку інформацію повинні містити винесення (текстові позначення) від відеокамер на горизонтальній та вертикальній проекціях креслення?

8. Опишіть методологію DORI: що означає кожна літера в цій абревіатурі?

9. Яке емпіричне правило використовується для розрахунку відстані ідентифікації незнайомої людини на основі фокусної відстані об’єктива?

10. Які законодавчі та нормативні вимоги необхідно враховувати, якщо відеозаписи планується використовувати як судові докази?

Література: [12-24].

Тема 9. Етапи створення проекту системи відеоспостереження

План:

Розробка технічного завдання. Визначення кількості, місць і способів встановлення відеокамер та їх технічних характеристик. Вибір режимів відображення відеоінформації. Вибір режимів зберігання відеоінформації. Структурний синтез системи. Обґрунтування каналів передачі інформації. Вибір параметрів і конкретного типу обладнання системи. Моделювання роботи CCTV. Створення проекту. Оцінка ефективності системи. Представлення та затвердження замовником робочого проекту.

Розробка технічного завдання (ТЗ). Проект CCTV починається із складання технічного завдання. Для створення завдання на проектування CCTV необхідно визначити цілі, які необхідно вирішити. Важливо чітко сформулювати – що у кінцевому підсумку необхідно отримати та які оперативні завдання вирішити. При детальному розгляді багато поставлених завдань необхідно вирішувати у комплексі. Наприклад, виникла задача «запобігання несанкціонованого проникнення сторонніх осіб на територію». Тільки засобами системи відеоконтролю її вирішити не можна. Необхідний комплексний підхід: огорожа території, охоронна сигналізація та система відеоспостереження по периметру.

До основних етапів розробки CCTV можна віднести:

1) аналіз об’єкту захисту з визначенням контрольованих зон, об’єктів спостереження (люди, транспорт, предмети, безпілотні літальні апарати тощо), основних вимог до проектованої системи і умов її роботи (кліматичних, освітленості тощо);

2) вибір кількості, місць встановлення і орієнтації відеокамер, кутів огляду і роздільної здатності;

3) вибір режимів відображення відеоінформації;

4) вибір режимів зберігання відеоінформації;

5) структурний синтез системи;

6) вибір каналів передачі інформації;

7) вибір параметрів і конкретного типу обладнання системи;

8) оцінку ефективності системи.

Перш за все слід усвідомити загальну «концепцію» контролю та відеоспостереження, які потрібні споживачеві: чи буде вестись постійний моніторинг камерами і 24-х годинна робота персоналу безпеки, або планується робота в автоматичному режимі (зазвичай з постійним записом), або передбачається поєднання обох варіантів спостереження. Як тільки виконавець зрозуміє, чого хоче замовник, було б добре роз'яснити йому, чого можна домогтися за допомогою пропонованого обладнання. Працювати з невеликими і простими системами досить легко, але як тільки вони збільшуються до 10 камер і більш (деякі з яких можуть бути встановлені на поворотних пристроях), декількох моніторів (відеостіна), більше одного місця відеоспостереження, декількох датчиків тривоги і цифрових відеореєстраторів – завдання набагато ускладниться.

Існує також багато змінних, які необхідно враховувати при розробці системи відеонагляду. Що трапиться, якщо одночасно спрацюють декілька датчиків тривоги? Який монітор повинен показувати «тривожні» відеокамери? Чи буде записуватися зображення за сигналом тривоги, якщо відеореєстратор в цей час відтворює запис? Який рівень пріоритету для кожного оператора? І так далі.

Перша зустріч із замовником відбувається на етапі розробки ТЗ на проект. На цьому етапі замовник повинен:

1) вказати об'єкти, які потрібно обладнати CCTV (периметр території, прохідна, автостоянка, виробничі приміщення тощо);

2) визначитися з місцем, куди буде зведено всю інформацію з відеокамер;

3) визначити режим роботи CCTV: за участю операторів чи автономно;

4) взаємодія з існуючими системами безпеки;

5) побажання бренда виробника продукції CCTV;

6) знати детально вимоги до особливо відповідальних місці об'єкта з точки зору концепції безпеки.

Нижче наведені питання, які потрібно задати замовнику до початку розробки системи і до або під час обстеження місця встановлення.

1. Яка основна задача проектованої CCTV (стримуюча чи прихованого спостереження)?

Якщо це стримуюча зловмисників система, то необхідно так спланувати розміщення камер і моніторів, щоб вони були видні публіці. Якщо система призначається для прихованого відеоспостереження, то необхідно приділити особливу увагу типу і розмірам телекамери, її маскування, прихованості проводки і аналогічних проблем, а також з'ясуванню передбачуваних термінів її встановлення.

2. Хто буде оператором?

Якщо планується 24-х годинна робота охорони, реакція системи на сигнал тривоги повинна бути іншою, ніж в автоматичному режимі або при роботі в частково автоматичному режимі.

3. Це буде чорно-біла або кольорова відеосистема?

Від цього буде залежати вартість системи і її чутливість. Отже, необхідно вивчити освітленість в зоні установки системи. Кольорове зображення дасть велику інформацію про деталі спостережуваних об'єктів, але якщо передбачається спостереження при дуже низькому рівні освітленості або при інфрачервоному освітленні, то немає інших варіантів, крім використання чорно-білих камер (якщо тільки замовник не згоден оплатити, наявні на ринку камери, які перемикаються з кольорового на чорно-білий режим).

4. Скільки телекамер буде використовуватися?

Для невеликої системи достатньо відеореєстратора з можливістю віддаленого доступу, для більшої системи швидше за все знадобиться матричний її поділ із застосуванням комутаторів.

5. Скільки камер буде з фіксованим встановленням і об'єктивом з постійною фокусною відстанню і скільки поворотних камер і скільки з варіооб'єктивами?

Між цими видами камер існує велика цінова різниця.

6. Скільки буде потрібно моніторів і пультів управління?

Для невеликої системи логічно запропонувати один монітор і один пульт управління, але як тільки збільшується кількість операторів і/або одночасно переглядаються каналів і керованих телекамер, спланувати практичну та ефективну систему стає важче. В цьому випадку для планування розташування обладнання і з'єднань необхідне обстеження диспетчерської (приміщення охорони).

7. Чи система використовуватися для моніторингу в реальному режимі часу (що вимагає негайної реакції на тривоги), або буде здійснюватися запис відеосигналу подальшого перегляду і перевірки?

Відповідь на це питання визначає обсяг місця для збереження інформації – глибини архіву.

Наступне, що необхідно зробити – це провести обстеження об'єкта в місці розміщення CCTV.

Цей етап процедури розробки CCTV включає в себе:

– визначення кількості і конфігурації зон, контрольованих засобами CCTV;

– формулювання завдань, що вирішуються системою по кожній зоні;

– оцінку умов роботи елементів системи, в першу чергу телекамер (освітленості, перешкод, кліматичних умов і т.п.).

На основі аналізу особливостей об'єкта, режиму і умов його функціонування, способів реалізації загроз на початковому етапі розробки телевізійної системи необхідно визначити три основні групи зон:

1) пріоритетного спостереження;

2) бажаного контролю засобами спостереження;

3) заборонених для спостереження.

Перша група – зони, які повинні обов'язково контролюватися засобами CCTV для забезпечення необхідного рівня безпеки. Наприклад, прохідна для входу і в'їзду на підприємство.

Друга – це зони, для яких немає жорсткої необхідності спостереження, і рішення про їх контролі може прийматися на підставі інших міркувань. Наприклад, якщо в системі буде використовуватися 16-канальний відеореєстратор, а телекамер, контролюючих першу групу зон, тільки 14, то у такому випадку незначне збільшення вартості системи за рахунок двох додаткових телекамер дозволить контролювати дві додаткові зони або найбільш важливі зони декількома додатковими камерами.

До третьої групи відносяться зони, з тієї чи іншої причини заборонені для спостереження, такі як клавіатури для набору пароля, вікна видачі грошових купюр банкоматів, ділянки приватних територій або вікна житлових будинків (принаймі, без згоди їх власників) або інші, які торкають приватне життя людей або інші питання забезпечення безпеки (наприклад, інформаційної), і т.п.

Таким чином, треба визначити положення і розміри зон спостереження та їх пріоритетність або порядок за важливістю з точки зору необхідності і умов організації телевізійного спостереження.

Надалі кількість цих зон, їх розміри і особливості контролю можуть коригуватися і остаточно визначатимуться в сукупності з вартісними і іншими обмеженнями, наприклад на кількість камер в системі.

Також на основі аналізу об’єкта необхідно оцінити умови освітленості контрольованої зони. А саме наявність, кількість, параметри джерел освітлення і їх розташування щодо зони спостереження. При цьому обов’язково слід врахувати можливі зміни в процесі експлуатації протягом доби і в різні пори року. Сонце постійно змінює своє положення протягом доби і пори року і може ховатися за хмарами, отже, будуть суттєво змінюватися умови освітленості. Інший приклад: потужний прожектор для освітлення території включається в темну пору доби і вимикається в світлу і знаходиться в фіксованому положенні. Тому освітленість, створювану ним, легко врахувати. Однак фари проїжджаючих автомашин в темну пору доби різко змінюють освітленість і, більш того, можуть створювати зустрічне засвічення, при цьому ще й змінюють своє положення.

Все це істотно впливатиме як на вибір місць установки камер, так і на вибір обладнання (його функціональних характеристик).

На основі даних аналізу об’єкта по кожній зоні, що вимагає організації спостереження для виявлення загроз, слід мати чітке формулювання завдань, що вирішуються CCTV.

Одна з поширених помилок, яку допускають починаючі користувачі і розробники CCTV, пов’язана з бажанням забезпечити спостереження за об’єктом мінімальною кількістю камер з максимальним розміром контрольованих зон. Це пояснюється фінансовими обмеженнями. А це, як наслідок, тягне збільшення кутів огляду. У свою чергу збільшення кута огляду камери призводить до відповідного збільшення розмірів контрольованої зони, таким чином згадане завдання, на перший погляд, вирішується. Але при цьому часто забувають, що роздільна здатність камери обмежена, і збільшення кута огляду, наприклад, в 3 рази, з 30 до 90 градусів, призведе до збільшення

лінійних розмірів контрольованої зони теж майже в 3 рази. А це означає, що для відображення об'єкта одного і того ж лінійного розміру на одній і тій відстані буде використовуватися в 3 рази менша кількість пікселів матриці. Отже, якість зображення істотно погіршиться, можливість розрізняти дрібні деталі буде втрачена.

Загальний план контрольованого об'єкта вирішує задачі виявлення, спостереження або моніторингу (відстеження об'єкта спостереження після його виявлення) і оцінки загальної ситуації в контрольованій зоні. При цьому ставиться завдання загального огляду та оцінки ситуації в цілому, без дрібних деталей. Наприклад, спостереження за територією, що прилягає до входу в банк, або за ситуацією в вестибюлі метро (виникнення скупчення людей, що може призвести до тисняви). В такому випадку необхідно виявити появу нових об'єктів спостереження і (або) відстежувати ситуацію в зоні спостереження – переміщення деяких об'єктів (машин, людей і т.д.). Можливість оцінити деталі не тільки дрібних (номер автомашини, обличчя людини і т.п.), але часто і більших (марку автомашини, наявність предметів в руках людей) зазвичай відсутня.

Визначення кількості, місць і способів встановлення відеокамер та їх технічних характеристик. Визначення необхідної кількості камер не може бути довільним процесом; воно базується на аналізі вразливостей об'єкта та геометричних характеристиках обраної оптики. Загальна стратегія передбачає поділ території на зони різного пріоритету: зовнішній периметр, підходи до будівель, вхідні групи та внутрішні приміщення.

Після початкового обговорення проекту із замовником, переконавшись, що виконавець добре усвідомлює те, що йому потрібно – він повинен обстежити місце встановлення системи. Зазвичай збирають наступну інформацію:

– потрібний тип камер: чорно-білі або кольорові, фіксовані або поворотні, роздільна здатність тощо;

– достатні характеристики об'єктивів: кути огляду, діапазон фокусних відстаней для варіооб'єктивів (12,5-75 мм, 8-80 мм і так далі).

– захист камери: тип кожухів (стандартні, вологозахищені, купольні, антивандальнітощо), тип кріплення;

– освітленість: рівні, джерела світла, східний/західний напрям огляду. Чітко потрібно усвідомити положення сонця в різні дні року, влітку і взимку. Це має велике значення для загальної якості зображення;

– приймальну апаратуру: місце знаходження/розміщення, площа приміщення охорони, фізичний простір і пульт керування;

– монітори: роздільна здатність, розмір, місце знаходження, кріплення і так далі;

– електропостачання: тип, потужність (із запасом). Чи є необхідність в безперебійному електроживленні? (У цьому випадку споживана потужність у Вт);

Замовнику потрібно представити схему даної зони та надати пропозиції по розміщенню камер. Необхідно драти до уваги точку зору фахівця з монтажу, наскільки це можливо. Незначні зміни в розташуванні камер не вплинуть на їх роботу, але можуть полегшити працю монтувальника, заощадити час і, в кінцевому рахунку, кошти.

Щоб отримати якісне зображення – потрібно пам'ятати золоте правило: уникати потрапляння в об'єктив камери прямих сонячних променів.

На схемі доцільно нанести назви зон, в яких замовник хоче (або пропонується) встановити камери. Нанесіть також назви зон, які будуть проглядатися, оскільки вони будуть потрібні у документації як опорні точки.

Проектування системи, як і будь-яка розробка всього нового, це форма творчості.

При розробці систем користуються різними методиками.

Завжди розробку системи потрібно починати із складання схеми загального вигляду системи, якою вона має бути. На схему наносять розміщення обладнання: монітори, камери, кожухи, з'єднувальні кабелі, блоки живлення і так далі. Складаючи схему, ви побачите фізичні з'єднання і всі необхідні складові. Потрібно не забути про такі дрібниці, як кронштейни, типи кабелю, довжина кабелю і так далі. Складання навіть грубого ручного нарису приведе до деяких коректив або удосконалень.

Склавши остаточний варіант схеми можна побачити, що потрібно для системи, і тоді можна приступати до складання списку пропонованого обладнання. Потім доцільно перейти до етапу підбору комбінацій камера/об'єктив.

Переконайтеся, що вони будуть відповідати кожуху або куполу, які припускається використовувати. Це ще один шанс переглянути буклет технічних характеристик постачальника. Не забудьте врахувати деякі прості речі, які, однак, можуть створити труднощі при установці, такі як простір за телекамерою для коаксіального кабелю (пам'ятаєте, що завжди добре мати в запасі як мінімум 50 мм для BNC-роз'єму), переміщення об'єктива при фокусуванні може істотно допомогти при підготовці варіооб'єктивів при фокусуванні на ближні об'єкти і т.д.

Наступний етап – розрахунок вартості: витрати на обладнання, податок з обороту і мито, витрати на монтаж, розмір прибутку і найважливіше (особливо для замовника) – загальна вартість.

Не забудьте включити сюди витрати на приймально-здавальні випробування, хоча багато хто не включають їх в цю суму і розраховують витрати на випробувальний період і введення системи в експлуатацію окремо. Це питання практики, оскільки витрати на приймально-здавальний період будуть значно варіюватися і цей період може виявитися довше або коротше планованого. В цілому практика показує, що приймально-здавальний період завжди в три рази довше запланованого. Крім того, до витрат на приймально-здавальні випробування повинно бути включено час на навчання операторів системи відеоспостереження.

Після виконання вищезгаданого потрібно зробити остаточну і точнішу схему запропонованої вами системи. Вона може бути виконана від руки, але в даний час більшість проектувальників цих систем використовують для цього комп'ютери і спеціалізовані програми або CAD. Ці засоби дозволяють легше і швидше скласти схему, а сама схема буде виглядати набагато професійніше.

Ручний розрахунок калькуляції необхідно оформити письмово у формі комерційної пропозиції, що містить також пояснення принципів роботи відеосистеми і досягаються нею результати. Важливо, щоб пропозиція була складена лаконічно, просто і точно, оскільки читати комерційні пропозиції будуть і працівники, що не володіють технічними знаннями – відповідальні за закупівлю, бухгалтери і так далі.

Часто для забезпечення точності розрахунків використовуються програми складання великоформатних таблиць, що дає ще один шанс перевірити список обладнання і переконатися в тому, що нічого не втрачено.

Для стандартного прямокутного будинку площею 150-200 $м^2$ на ділянці приблизно 6 соток, галузеві стандарти рекомендують встановлення мінімум 6 камер. Ця цифра виведена з необхідності покриття критичних точок без створення «сліпих зон».

Розподіл камер зазвичай виглядає наступним чином:

– чотири камери по периметру будівлі (по одній на кожен фасад), що забезпечує круговий огляд підходів;

– одна камера на головний вхід до будинку для ідентифікації відвідувачів;

– одна камера на в'їзну групу (ворота та хвіртку) для контролю доступу на територію.

У разі наявності додаткових споруд на ділянці, таких як гараж, баня чи гостьовий будинок, до проекту рекомендується додавати по одній камері на кожен об'єкт. При використанні ширококутних об'єктивів (кут огляду 120°-160°) кількість одиниць обладнання може бути оптимізована, проте це часто йде всупереч вимогам до деталізації на великих відстанях.

Правильний вибір місця встановлення камери безпосередньо впливає на якість аналітики та можливість ідентифікації обличь. Основною помилкою при монтажі є встановлення камер на занадто великій висоті без врахування кута нахилу.

Досвід експлуатації систем відеоспостереження дозволяє сформулювати наступні рекомендації висоти монтажу:

– для внутрішніх офісних чи житлових приміщень 2,5-3 метри від рівня підлоги;

– для зовнішнього периметрального спостереження 3-4 метри від землі;

– для зон ідентифікації (над дверима, турнікетами) 2-2,5 метри.

Встановлення камери вище 4 метрів для ідентифікації обличь є неефективним, оскільки кут нахилу об'єктива стає занадто гострим. У такому разі на відео фіксуватимуться лише верхівки голів або головні убори людей, що

робить розпізнавання рис обличчя неможливим. Для ідентифікації особи камера повинна бути спрямована під кутом не більше 30° до горизонталі.

При плануванні місць встановлення необхідно враховувати архітектурні перешкоди (колони, виступи, дерева), які створюють зони неоглядності. Для забезпечення безперервності спостереження на периметрах використовується принцип зустрічного огляду – кожна ділянка повинна переглядатися мінімум двома камерами з різних точок. Також рекомендується забезпечувати перекриття зон огляду сусідніх камер на 10-15%, що гарантує відсутність «дірок» у системі безпеки.

В довгих коридорах найефективнішою схемою є діагональне розміщення камер у протилежних кутах. Це дозволяє не тільки повністю охопити простір, але й захистити самі камери – кожна з них знаходиться у полі зору іншої, що запобігає несанкціонованому демонтажу чи вандалізму.

Встановлення камер для автоматичного розпізнавання номерних знаків вимагає значно суворішого дотримання геометричних параметрів, ніж загальне спостереження. Алгоритми розпізнавання чутливі до нахилу номера в кадрі та кута між оптичною віссю камери та траєкторією руху автомобіля.

Для досягнення високої точності розпізнавання необхідно дотримуватися наступних параметрів:

– вертикальний кут нахилу до дороги повинен становити від 15° до 30° (хоча деякі камери дозволяють роботу при кутах до 45°, це суттєво підвищує ризик того, що номер буде прихований капотом чи іншими елементами кузова, особливо на вантажних автомобілях);

– горизонтальний кут (кут відхилення від прямої лінії руху) не повинен перевищувати 25°, в ідеалі – до 10°. Нахил самого номерного знаку відносно горизонту в кадрі не повинен перевищувати 5°.

Висота монтажу для LPR-камер зазвичай становить близько 1-2 метрів для в’їздів на парковки або 4-6 метрів для магістральних доріг. Головна вимога – камера має бути встановлена мінімум на 1 метр вище рівня фар автомобіля, щоб уникнути засліплення матриці прямим світлом у нічний час.

Вибір способу встановлення залежить від матеріалу поверхонь та умов експлуатації. Надійне кріплення не тільки запобігає падінню обладнання, але й мінімізує вібрації, які можуть негативно впливати на роботу відеоаналітики.

Залежно від місця встановлення використовуються різні типи кронштейнів: настінні, стельові, кутові або для кріплення на стовп. При вуличному монтажі критично важливим є використання монтажних коробок, які забезпечують герметичність з’єднань кабелів.

Купольні камери відрізняються компактністю та високим ступенем вандалозахисту (стандарт IK10).

Циліндричні камери легше спрямовувати на конкретну ціль, вони часто мають потужнішу ІЧ-підсвітку.

Поворотні PTZ-моделі призначені для активного моніторингу великих територій, де оператор може керувати напрямком огляду та збільшенням.

Особливу увагу слід приділити температурному режиму. Надійні вуличні камери повинні мати температурний діапазон роботи від -30°C до +60°C та герметичність корпусу не нижче стандарту IP66/IP67.

Встановлення камер на стовпах забезпечує панорамний огляд та захист від вандалізму за рахунок висоти. При монтажі на бетонні або металеві опори категорично не рекомендується свердлити конструкцію, оскільки це може призвести до її поступового руйнування під дією корозії чи погодних умов.

Замість свердління використовуються спеціальні кронштейни з кріпленням на бандажну стрічку або сталеві хомути. Це забезпечує жорстку фіксацію без пошкодження цілісності опори. При використанні стовпів, що належать електромережам, необхідно обов'язково отримувати дозвіл від власника балансоутримувача, щоб уникнути ризику ураження струмом або демонтажу обладнання сервісними службами.

Вибір режимів відображення відеоінформації. Ефективність функціонування будь-якої системи візуального контролю безпосередньо залежить від того, наскільки вдало обрано режими відображення відеоінформації, оскільки саме на етапі візуалізації відбувається передача даних від технічної підсистеми до оператора. Вибір режиму відображення не є статичним рішенням; це динамічний процес, що враховує технічні характеристики сенсорів, архітектуру мережі, специфіку об'єкта охорони та психофізіологічні обмеження людини, яка здійснює моніторинг.

Одним із найважливіших технологічних рішень у сучасних системах відеоспостереження є використання дуального або багатопотокового кодування. Ця технологія була впроваджена для вирішення фундаментальної суперечності між необхідністю високої якості локального архіву та плавністю відображення при віддаленому доступі через мережі з обмеженою пропускною здатністю.

Основний потік призначений для локального запису на жорсткі диски реєстратора в максимальній якості. Він забезпечує найвищу роздільну здатність та частоту кадрів, що є важливим для подальшого експертного аналізу подій та ідентифікації осіб. У режимі живого перегляду основний потік зазвичай активується лише тоді, коли оператор розгортає певну камеру на повний екран.

Додатковий потік має значно меншу роздільну здатність та бітрейт. Він використовується для мультиекранного відображення (сітки 2x2, 3x3, 4x4 тощо) та віддаленого моніторингу через мобільні додатки або веб-клієнти. Використання субпотоку дозволяє уникнути таких проблем, як «завмирання» зображення або затримки в передачі сигналу, що часто виникають при спробі одночасної трансляції десятків потоків високої чіткості.

Вибір режиму відображення нерозривно пов'язаний з алгоритмами стиснення відео. Стандарт H.265 є поточним мейнстрімом, оскільки він дозволяє економити до 50% смуги пропускання та обсягу зберігання порівняно з H.264, зберігаючи при цьому візуальну цілісність зображення. При виборі режиму відображення важливо враховувати потужність станції моніторингу,

оскільки декодування багатьох потоків H.265 вимагає значних ресурсів графічного процесора.

У сучасних системах безпеки вибір режиму відображення часто виходить за межі стандартного прямокутного кадру. Використання камер зі специфічною оптикою вимагає складних програмних маніпуляцій для приведення зображення до вигляду, придатного для аналізу людиною.

Одним із найбільш ефективних режимів є Auto-popup, коли при спрацюванні детектора (наприклад, перетин лінії або вхід у зону) вікно відповідної камери автоматично виводиться на центральний монітор пріоритетного перегляду. Це дозволяє оператору миттєво зосередитися на потенційній загрозі, не переглядаючи десятки статичних кадрів.

Режим Focus Mode використовує AI для автоматичного керування PTZ-камерою: при виявленні руху система самостійно наближає об'єкт, утримує його в центрі кадру та супроводжує його переміщення між зонами. Такий підхід мінімізує потребу в ручному керуванні джойстиком, яке часто супроводжується затримками до 2 секунд.

Вибір режимів зберігання відеоінформації. Процес проектування та експлуатації систем відеоспостереження стикається з безпрецедентним викликом – стрімким зростанням обсягів даних, що генеруються камерами надвисокої роздільної здатності, на фоні необхідності забезпечення миттєвого доступу до архіву та інтелектуального аналізу подій. Вибір режимів зберігання відеоінформації на відеореєстраторі перетворився на комплексну інженерну задачу, яка визначає економічну ефективність, надійність та функціональність усієї системи безпеки.

Ефективність зберігання відео починається з алгоритмів компресії, які дозволяють трансформувати сирий візуальний потік у компактні цифрові пакети без втрати важливих деталей. Перехід від застарілих стандартів, таких як MJPEG, до сучасних H.264 та H.265, став етапом у розвитку галузі, дозволивши зменшити вимоги до обсягу сховища приблизно на 50% при збереженні ідентичної якості зображення.

Вибір режиму запису є ключовим інструментом адміністратора системи для балансування між глибиною архіву та його інформативністю. Сучасні реєстратори пропонують декілька основних стратегій, які можуть комбінуватися в межах одного пристрою або навіть окремого каналу.

Постійний запис є найбільш традиційним методом, за якого реєстратор фіксує відеопотік 24 години на добу незалежно від наявності руху в кадрі. Цей режим гарантує відсутність прогалин у часі та дозволяє відновити контекст подій, що передували інциденту. Проте він є найбільш витратним з точки зору дискового простору, особливо при використанні камер з високою частотою кадрів (FPS).

Запис за розкладом дозволяє оптимізувати ресурси сховища, активуючи фіксацію відео лише у визначені години, наприклад, у робочий час підприємства або під час нічної зміни охорони. Це ефективно для об'єктів з

чітким операційним графіком, але несе ризик пропуску подій у позапланові періоди.

Запис за детекцією руху радикально змінює підхід до формування архіву. Реєстратор починає запис лише тоді, коли алгоритм виявляє зміни в піксельній структурі кадру. У зонах з низькою інтенсивністю руху, таких як запасні виходи або серверні кімнати, цей режим може скоротити використання дисків на 90%. Однак традиційна детекція руху вразлива до хибних тривог, викликаних тваринами, снігом або зміною освітлення, що призводить до «засмічення» архіву непотрібними фрагментами.

Технології інтелектуального аналізу (AcuSense, WizSense) виводять детекцію на новий рівень. Замість простого руху, реєстратор реагує на конкретні типи об’єктів – людей або транспортні засоби. Це дозволяє не тільки економити місце, але й створювати архів, який легко фільтрувати при проведенні розслідувань. Застосування таких методів у 2025 році дозволяє підвищити точність спрацювання до 95% і вище.

Гібридний режим запису заслуговує на особливу увагу. У цьому сценарії реєстратор постійно записує відео з низькою частотою кадрів (наприклад, 1-2 FPS), а при виявленні руху або тривоги миттєво перемикається на максимальну якість (25-30 FPS). Це забезпечує безперервність архіву при значній економії ресурсів сховища.

Сучасний ринок пропонує три основні моделі архівації: локальну (на реєстраторі), хмарну (VSaaS) та гібридну. Вибір моделі безпосередньо залежить від бюджету та вимог до безпеки даних.

Локальне зберігання передбачає одноразову інвестицію в обладнання. Користувач має повний фізичний контроль над даними, що важливо для об’єктів з високими вимогами до конфіденційності. Локальні системи не залежать від якості інтернет-з’єднання для здійснення запису, що робить їх надійними в умовах нестабільної мережі. Головний недолік – ризик викрадення або знищення реєстратора разом із архівом під час інциденту. Також обслуговування дисків та оновлення ПЗ лягає на плечі власника.

Хмарні сервіси працюють за моделлю підписки (OPEX). Відео передається на віддалені сервери провайдера, що гарантує збереження доказів навіть при повному знищенні об’єкта. Користувач отримує доступ до відео з будь-якої точки світу без налаштування складних мережевих протоколів. Проте хмарне зберігання залежить від вихідної швидкості інтернету. Система з 16 камер 4MP може споживати до 64 Mbps каналу, що вимагає дорогого корпоративного підключення. За 5 років сукупна вартість хмарної підписки для 16 камер може у 5-7 разів перевищувати вартість локальної системи.

Найбільш прогресивним підходом у 2025-2026 роках є гібридне зберігання. Основний архів записується на локальний NVR, а критичні події (тривоги, обличчя, номери авто) миттєво дублюються у хмару. Це забезпечує надійність, швидкий доступ у локальній мережі та захист від фізичного знищення даних при помірних витратах.

Можна сформулювати алгоритм вибору режимів зберігання відеоінформації:

– якщо мета – загальна охорона периметра, достатньо запису за детекцією руху об’єктів типу «людина» з глибиною архіву 7-14 днів. Якщо йдеться про моніторинг касових операцій або технологічних процесів, необхідний постійний запис з максимальною частотою кадрів та архівом від 30 днів;

– для статичних сцен (склади, паркінги) критично важливо активувати H.265+ або Zipstream. Це дозволить подовжити термін життя жорстких дисків за рахунок зменшення інтенсивності запису;

– найкращою практикою є комбінація локального запису високої якості та хмарного зберігання тривожних подій. Це захищає від крадіжки реєстратора та дозволяє оперативно отримувати сповіщення на смартфон;

– після налаштування системи необхідно провести реальний тест глибини архіву. Коефіцієнти активності руху часто виявляються вищими за розрахункові через вуличний шум або рослинність, що може скоротити очікуваний термін зберігання.

Сучасні технології відеореєстрації дозволяють побудувати надзвичайно ефективну систему зберігання, яка не просто накопичує терабайти даних, а стає інтелектуальним активом бізнесу, забезпечуючи безпеку та надаючи цінні інструменти для аналізу подій у реальному часі.

Структурний синтез системи. Структурний синтез системи відеоспостереження є етапом інженерного проектування, що полягає у формуванні оптимальної топології, визначенні складу обладнання та встановленні логічних зв’язків між компонентами для досягнення заданих показників ефективності. Цей процес охоплює не лише вибір апаратних засобів, а й розробку математичних моделей, які враховують пропускну здатність мереж, параметри обробки даних на периферії та відповідність нормативним вимогам національних і міжнародних стандартів.

Структурний синтез, який також називають топологічним синтезом, зосереджується на визначенні кількості вузлів, типів з’єднань та патернів комунікації, що відрізняє його від параметричного синтезу, де встановлюються конкретні характеристики, такі як фокусна відстань об’єктива чи роздільна здатність сенсора. В основі проектування лежить тріада: ціль визначає необхідні функції, які, у свою чергу, диктують вибір структури. Цей підхід дозволяє уникнути надлишковості ресурсів при забезпеченні максимальної ймовірності виконання оперативного завдання.

У процесі синтезу виділяють три основні стадії: макропроектування, безпосередній структурно-параметричний синтез та адаптивне структурне налаштування в процесі експлуатації. На етапі макропроектування проводиться аналіз об’єкта та визначення зон ризику, що стає фундаментом для всієї подальшої архітектури. Структурний синтез забезпечує відповідність побудованої моделі її призначенню через локалізацію функціональних інваріантів – блоків, які залишаються незмінними незалежно від зовнішніх умов.

Сучасні методи синтезу все частіше використовують алгебраїчні методи апроксимації, проективну геометрію та сингулярний розклад матриць для точного визначення просторових координат камер. Це дозволяє мінімізувати кількість «мертвих зон» та дублювання ракурсів, що є важливим для великих промислових чи міських об'єктів.

Математичним фундаментом для опису структури системи відеоспостереження є теорія графів. Система представляється як впорядкована пара G =(V, E), де V – множина вершин (відеокамери, сервери, комутатори), а E – множина ребер (кабельні лінії, бездротові канали зв'язку). Таке представлення дозволяє застосовувати потужний апарат алгоритмів для оптимізації потоків даних та оцінки надійності системи.

Для аналізу мереж відеоспостереження використовують матриці суміжності або списки суміжності. Оскільки мережі зазвичай є розрідженими, використання списків суміжності є більш ефективним з точки зору обчислювальних ресурсів при пошуку найкоротших шляхів передачі трафіку. Вершини в таких графах можуть бути зваженими, відображаючи обчислювальну потужність вузла, а ребра – відображаючи пропускну здатність або затримку каналу.

Застосування теорії графів у синтезі систем дозволяє вирішувати наступні завдання:

– оптимізація маршрутизації (використання алгоритмів Дейкстри або Флойда-Уоршелла для мінімізації затримок при передачі відеопотоків високої чіткості в реальному часі);

– аналіз вразливості (ідентифікація критичних вузлів, вихід з ладу яких призведе до втрати зв'язку з цілими сегментами системи);

– синтез структури (використання генеративних фреймворків, таких як GraphGen, які за допомогою LSTM-мереж здатні моделювати оптимальні конфігурації на основі послідовностей DFS-кодів).

При проектуванні масштабних систем, таких як «Безпечне місто», виникає проблема масштабованості. Для її вирішення застосовується стратегія семплювання підграфів за допомогою випадкових блукань з перезапусками, що дозволяє обробляти графи з мільйонами вузлів, зберігаючи локальну зв'язність та структурну цілісність.

Одним із центральних завдань структурного синтезу є оптимальне розміщення камер для забезпечення максимального покриття цільової території при мінімальних витратах. Ця задача є NP-складною і часто формулюється як задача про «галерею мистецтв».

Процес вибору позицій для камер базується на кількох математичних моделях:

– MCLP (Maximal Coverage Location Problem): максимізація загальної площі спостереження за умови обмеженої кількості сенсорів;

– BCLP (Backup Coverage Location Problem): забезпечення дублюючого покриття для критично важливих зон, що підвищує стійкість системи до фізичних пошкоджень окремих камер;

– аналізі просторового синтаксису (Space Syntax): використання метрик зв'язності та інтеграції простору для виявлення найбільш завантажених маршрутів, де ймовірність виникнення інцидентів є найвищою.

Ефективність розміщення оцінюється за щільністю пікселів на об'єкті, що визначає можливість виконання конкретних аналітичних оперативних завдань.

Перехід до IP-відеоспостереження перетворив систему на спеціалізовану мережу передачі даних, де пропускна здатність є головним обмежуючим ресурсом.

Сучасний структурний синтез відходить від суворо централізованих моделей на користь розподілених обчислень. Це дозволяє вирішити проблему «вузького місця» в каналах зв'язку та забезпечити швидку реакцію на події.

Розміщення алгоритмів штучного інтелекту безпосередньо в камерах (Edge AI) радикально змінює профіль системи. Обробка візуальних даних на місці виникнення дозволяє приймати рішення менш ніж за 100 мілісекунд. Це важливо для систем безпеки, де кожна секунда затримки може мати наслідки. Використання спеціалізованих ARM-процесорів забезпечує неймовірну енергоефективність – споживання енергії на один висновок може бути в 10 000 разів нижчим, ніж при обробці в хмарі.

Структурний синтез систем відеоспостереження охоронного призначення в Україні має чітко відповідати національним стандартам, гармонізованим з міжнародними вимогами IEC та ISO.

Основу нормативної бази складає серія ДСТУ IEC 62676 «Системи відеоспостереження охоронного призначення»:

– ДСТУ IEC 62676-1-1:2017: загальні вимоги до систем, що визначають їх структуру та функціональний склад;

– ДСТУ IEC 62676-1-2:2017: експлуатаційні вимоги до передавання відео, що гарантують цілісність та якість потоку в мережі;

– ДСТУ EN IEC 62676-5:2019: характеристики даних та якості зображення, що дозволяє об'єктивно оцінювати ефективність синтезованої системи.

Крім галузевих стандартів, проектування має враховувати загальноінженерні нормативи, такі як ДСТУ ISO/IEC/IEEE 15288:2016 щодо процесів життєвого циклу систем та ДСТУ ISO/IEC/IEEE 29148:2015 щодо розроблення вимог. Це забезпечує системність підходу – від формування технічного завдання до виведення системи з експлуатації.

Топологія інформаційної мережі створюється на основі інформації про трьох її складових:

– величина максимального потоку, який створений всіма відеокамерами системи відеоспостереження;

– величина максимального потоку, який здатна передавати мережа (пропускна здатність);

– величина максимального потоку на один порт, який здатне забезпечити мережеве обладнання.

Проектування мережі системи IP відеоспостереження потрібно починати із визначення максимальних інформаційних потоків, створюваних усіма відеокамерами системи.

Результуюче значення потоку від кожної камери залежить від її роздільної здатності, від використовуваних кодеків стиснення, обраної частоти кадрів, інтенсивності руху в полі зору камери.

Крім зображення камера може транслювати і звук, що не суттєво, але, тим не менш, збільшує загальний трафік.

Знаходження сумарного значення максимальних інформаційних потоків на початковому етапі проектування дозволяє:

– визначити кількість інформаційних підмереж, за допомогою яких можна доставити весь обсяг відео та аудіо інформації від камер до сервера (серверів);

– розробити структуру і склад інформаційної підмережі.

Рекомендації з вибору архітектури мережі наступні:

1) для створення системи IP відеоспостереження рекомендується створення окремої ізольованої мережі. Найбільш широко використовуваною технологією є технологія Езернет і спеціалізований стандарт IEEE 802.3.2;

2) при роботі мережі Езернет використовується топологія «зірка», в якій кожен вузол (пристрій) з'єднаний в мережі з іншим вузлом за допомогою активного мережного обладнання;

3) якщо в мережі мало пристроїв (камер, реєстраторів, клієнтських машин), але вони розподілені на великій площі, то рекомендується використовувати комутатор, розташований приблизно посередині між пристроями;

4) якщо використовується мережа середніх розмірів з одним або двома центральними серверами запису, то в цьому випадку всі пристрої об'єднуються через один або кілька багатопортових комутаторів, об'єднаних через центральний високопродуктивний комутатор, до якого підключені сервера запису, керуючий сервер і клієнтські машини;

5) якщо використовується мережа середніх розмірів, що має розподілену структуру серверів запису, то пристрої підключаються до декількох комутаторів, при цьому до кожного комутатора підключений сервер запису. Мережа може ділитися на кілька VLAN;

6) якщо велика мережа розташована в одній будівлі, то в основному, рекомендації ті ж, що і в попередньому випадку. Найчастіше використовують топологію типу «зірка». Відмінність – продуктивність комутаторів і пропускна здатність каналів зв'язку;

7) якщо велика мережа розташована в декількох будівлях, то тут всі шляхи ведуть до центрального керуючого сервера, який приєднаний до центрального маршрутизатора або комутатора 3го рівня. Всі потоки з серверів запису, розташованих у зовнішніх мережах і розподілених VLAN, управляються через маршрутизатор.

Обґрунтування каналів передачі інформації. Вибір конкретного типу каналу – будь то традиційний коаксіальний кабель, сучасна структурована кабельна мережа на базі витої пари, волоконно-оптична лінія зв'язку чи бездротові технології нового покоління (Wi-Fi 6, 5G) – залежить від широкого спектра чинників, включаючи топологію об'єкта, вимоги до смуги пропускання, рівень електромагнітних завад та бюджетні обмеження.

Дротові системи залишаються еталоном стабільності в професійному сегменті завдяки відсутності впливу радіозавад та гарантованій смузі пропускання для кожного пристрою. Їхня еволюція пройшла шлях від простих коаксіальних ліній до складних оптичних магістралей.

У сучасних умовах коаксіальні кабелі використовуються переважно в системах форматів HD-TVI, HD-CVI та AHD. Ці технології дозволяють передавати сигнал роздільною здатністю до 4K на відстані до 500 метрів без використання проміжних підсилювачів.

Мережеві кабелі на основі витої пари є стандартом для IP-відеоспостереження. Головною перевагою є підтримка технології PoE, що дозволяє передавати і дані, і електроживлення по одному кабелю. Це не тільки знижує витрати на кабельні лінії, але й дозволяє централізовано керувати живленням камер через керовані комутатори, що підвищує живучість системи при збоях в електромережі.

Згідно з міжнародним стандартом ISO/IEC 11801, вибір категорії кабелю визначає максимальну швидкість та дальність передачі даних. Для сучасних систем відеоспостереження, особливо з використанням камер високої роздільної здатності (5-8 Мп), важливим є вибір кабелю відповідної категорії.

Найбільш популярним видом середовища передачі даних на невеликі відстані (до 100 м) визнана неекранована вита пара (UTP), яка включена практично в усі сучасні стандарти і технології локальних мереж забезпечуючи пропускну здатність до 100 Мбіт/с.

Екранована вита пара (STP/FTP категорії 6) дозволяє збільшити пропускну здатність до 1000 Мбіт/с.

Оптоволоконний кабель широко застосовується як для побудови локальних зв'язків, так і для побудови магістралей глобальних мереж. Оптоволоконний кабель може забезпечити дуже високу пропускну здатність каналу (до декількох Тбит/с) і передачу на значні відстані до декількох десятків кілометрів без проміжного посилення сигналу.

Рекомендації з проектування мереж:

1) кабель вибирається однаковим на всю мережу (найчастіше використовується вита пара 5 (5e) і 6 категорії);

2) на довгих ділянках мережі рекомендується використовувати екранований кабель – це зменшує можливість втрати пакетів;

3) мкомутаторами Gigabit Ethernet рекомендується використовувати оптоволоконне з'єднання;

4) у деяких випадках слід розглядати можливість бездротових мереж (тут слід особливу увагу приділяти безпеці);

5) рекомендується використовувати обладнання, по можливості, від одного відомого виробника;

6) вибирати обладнання потрібно по співвідношенню ціна/якість;

7) продуктивність кумутуючого обладнання повинна бути вище продуктивності машин для обробки потоків даних;

8) облік масштабованості: залишати в резерв 10% портів і до 30% пропускної здатності;

9) ядро мережі, проміжні комутатори, сервери запису управління повинні бути об'єднані за резервними лініями зв'язку, ключове комунікаційне обладнання також резервується;

10) резервування даних на дублюючий сервер через комутатори з відзеркаленням портів.

Таким чином, обґрунтування каналів передачі інформації системи відеоспостереження є комплексним процесом, де технічні характеристики середовища повинні відповідати операційним завданням системи. Дротові рішення на базі витої пари та оптоволокна залишаються основою для професійних стаціонарних об'єктів завдяки своїй стабільності, безпеці та високій пропускній здатності. Бездротові технології, такі як Wi-Fi 6 та 5G, стрімко скорочують розрив у продуктивності, пропонуючи гнучкість та швидкість розгортання, проте вони вимагають більш ретельного підходу до кіберзахисту та керування радіоефіром.

Використання сучасних стандартів компресії (H.265+) та протоколів безпеки (TLS 1.3, WPA3) дозволяє оптимізувати навантаження на мережу та захистити приватність даних. Правильний вибір каналу передачі інформації на етапі проектування дозволяє суттєво знизити сукупну вартість володіння системою та забезпечити її актуальність протягом багатьох років експлуатації. В кінцевому рахунку, надійність системи відеоспостереження визначається не роздільною здатністю камер, а здатністю каналів зв'язку гарантовано та безпечно доставити кожен кадр від об'єктива до оператора.

Вибір параметрів і конкретного типу обладнання системи. Станом на 2026 рік індустрія відеоспостереження зазнала фундаментальної трансформації, перейшовши від пасивного фіксування подій до проактивного інтелектуального моніторингу в реальному часі. Вибір архітектури системи є першим і найбільш важливим етапом проектування, що визначає майбутню гнучкість, вартість експлуатації та здатність системи до масштабування. Основна дилема вибору між цифровими (IP) та аналоговими (AHD, HD-CVI, HD-TVI) системами залишається актуальною, проте акценти суттєво змістилися у бік інтелектуальної інтеграції та мережевої незалежності.

Аналогові системи високої чіткості, попри свою консервативність, продовжують утримувати значну частку ринку завдяки впровадженню стандартів 4K та ColorHunter в аналоговому середовищі. Основним аргументом на користь аналогового сигналу у 2026 році залишається відсутність затримок, що важливо для оперативного керування поворотними камерами (PTZ) у закритих контурах спостереження. Проте технологічні обмеження аналогового

сигналу стають очевидними при спробі впровадження складних аналітичних функцій. Встановлено, що реєстратори, які підтримують AHD-сигнал з роздільною здатністю понад 1080p (2 Мп), стають менш поширеними, оскільки ринок зміщується в бік IP-рішень для високої деталізації. Більше того, аналоговий сигнал є незахищеним від перехоплення через відсутність шифрування, що створює ризики в системах з підвищеними вимогами до конфіденційності.

Цифрові IP-системи у 2026 році пропонують безпрецедентний рівень деталізації та аналітичних можливостей. Використання мережевої інфраструктури дозволяє передавати відео, аудіо та живлення по одному кабелю, що радикально спрощує монтаж у великих будівлях. Однак цифрова архітектура вносить власні виклики: затримка сигналу може досягати 2-3 секунд, а система залежить від пропускної здатності мережі.

Вибір типу системи часто обумовлений наявною інфраструктурою. На об'єктах, де вже прокладено коаксіальний кабель, модернізація за допомогою HD-CVI або HD-TVI є економічно вигідною, забезпечуючи якість 5-8 Мп без перекладання мереж. Проте для нових проектів, особливо в корпоративному та державному секторах, IP-технології є єдиним шляхом для впровадження розпізнавання обличь, аналізу трафіку та автоматизації сценаріїв безпеки.

Роздільна здатність камери визначає не лише кількість точок на екрані, а й можливість програмного наближення (цифрового зуму) без втрати важливих деталей:

– 2 Мп (1920x1080) використовується для загального моніторингу приміщень, де не потрібна ідентифікація дрібних деталей. Це базовий стандарт для бюджетних систем;

– 4-5 Мп забезпечує достатню деталізацію для розпізнавання обличь на відстані до 10-15 метрів та ідентифікації номерних знаків;

– 8 Мп (4K) та вище використовується на відкритих просторах, парковках та логістичних центрах. Дозволяє охопити велику територію однією камерою з можливістю детального аналізу окремих зон.

У свою чергу фокусна відстань об'єктива визначає геометрію зони спостереження. Інсталятори використовують чітку диференціацію за цілями спостереження (табл 9.1).

Таблиця 9.1 – Рекомендовані значення фокусної відстані та кута огляду для різних сценаріїв використання

Фокусна відстань, мм	Кут огляду	Типовий сценарій використання
2,1-2,4	110-130°	Панорамний огляд малих кімнат, ліфтів
2,8	95-110°	Загальний огляд вулиці, офісу, коридору
3,6-4,0	75-85°	Спостереження за касовими зонами, входами
6,0-12,0	25-50°	Вузькі проходи, периметр, ідентифікація об'єктів
5-125 (PTZ)	Варіативний	Активне стеження на великих дистанціях

Важливо розуміти ефект «дистанційної ідентифікації». Об'єктив 2,8 мм ідеально підходить для фіксації факту події на площі 50-70 квадратних метрів, але для розпізнавання обличчя невідомої особи на відстані понад 8 метрів

краще використовувати об’єктив 4 мм або 6 мм. Останнім часом широкого розповсюдження набули варифокальні об’єктиви з моторизованим керуванням, які дозволяють змінювати кут огляду віддалено через інтерфейс реєстратора, адаптуючи систему до змінних умов об’єкта.

Для прийняття фінального рішення щодо конфігурації системи необхідно пройти через певні етапи аналізу.

При визначенні цілей спостереження необхідно чітко розмежувати зони об’єкта за рівнем необхідної деталізації:

– зонам загального моніторингу (двір, паркан, коридор) рекомендовано камери 4 Мп з об’єктивом 2,8 мм та функцією виявлення людей/авто;

– зонам ідентифікації (вхідні двері, хвіртка, каса) рекомендовано камери 5-8 Мп з об’єктивом 4 мм або 6 мм з підтримкою WDR 120dB для компенсації контрового світла від сонця;

– зонам підвищеного ризику (периметр складу, стоянка авто) рекомендовано камери з активним стримуванням (сирена, світло) та потужним нічним баченням (ColorVu/ColorHunter).

Моделювання роботи CCTV. Моделювання роботи систем відеоспостереження – це не лише процес розміщення камер на плані об’єкта, а складний інженерний аналіз, що поєднує в собі оптичну фізику, теорію передачі даних, розрахунок мережевих потужностей та прогнозування ефективності алгоритмів штучного інтелекту. У 2024-2025 роках цей напрям зазнав фундаментальних змін через оновлення міжнародних стандартів, зокрема перехід від концепції DORI до OODPCVS, та через стрімку інтеграцію систем безпеки в єдині державні та муніципальні цифрові платформи.

Центральним елементом моделювання є визначення того, що саме оператор або алгоритм зможе «побачити» на отриманому зображенні. Донедавна галузевим стандартом була модель DORI, закріплена в IEC 62676-4:2014. Проте з розвитком технологій 4K, 8K та нейромережевого аналізу, стара модель перестала повноцінно задовольняти потреби експертів, що призвело до появи стандарту IEC 62676-4:2025.

Стандарт IEC/EN 62676-4:2025 (OODPCVS) офіційно затверджений та набрав чинності 9 жовтня 2025 року. Цей стандарт встановлює більш реалістичні мінімальні щільності пікселів для об’єктів різних розмірів, враховуючи можливості та обмеження сучасних цифрових IP-камер, такі як стиснення та шум.

У попередній версії стандарту, для області ідентифікації визначалася кількість пікселів на метр або пікселів на фут, чого не завжди було достатньо для ідентифікації людей, особливо в умовах слабкого освітлення або коли зображення розмите через рух цільових об’єктів.

З цієї причини замість 250 пікселів на метр тепер рекомендується 500 пікселів на метр. Назви зон також тепер нові (рис. 9.1). Тож замість зони ідентифікації нова зона 500 пікселів на метр називається зоною перевірки.

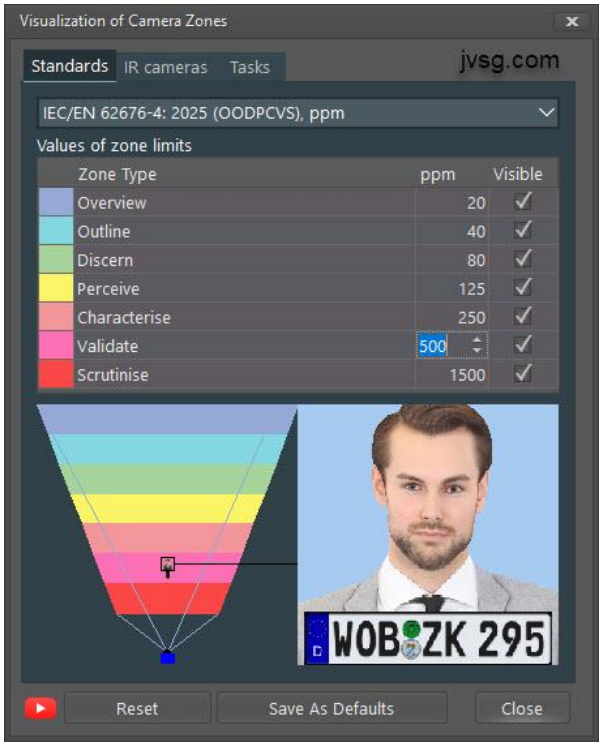


Рисунок 9.1 – Візуалізація зон камери на основі IEC 64676-4:2025 в IP Video System Design Tool 2025

Ці зміни вказують на зростання вимог до роздільної здатності сенсорів та фокусної відстані об'єктивів. При моделюванні зони Scrutinise (криміналістична ідентифікація) на відстані 20 метрів стандартна камера Full HD вже не здатна забезпечити необхідні 1500 px/m, що змушує проектувальників переходити на камери 8MP (4K) та довгофокусну оптику.

Моделювання базується на геометрії та тригонометрії. Головним завданням є розрахунок горизонтального (HFOV) та вертикального (VFOV) кутів огляду. Кут огляду розраховується за формулою:

$$\alpha = 2\arctan\frac{h}{2f}, \tag{9.1}$$

де h – фізичний розмір сенсора (мм), а f – фокусна відстань об'єктива (мм).

Другим параметром є щільність пікселів на метр PPM, яка визначається як відношення горизонтальної роздільної здатності сенсора R_h до ширини поля зору W на певній відстані D:

$$\text{PPM} = \frac{R_h}{W} = \frac{R_h}{2D\tan\frac{\alpha}{2}}. \tag{9.2}$$

Ці розрахунки дозволяють ще до етапу закупівлі обладнання визначити, чи зможе обрана модель камери забезпечити ідентифікацію на вході в будівлю або розпізнавання номерів на парковці.

Проектування сучасної IP-системи відеоспостереження також неможливе без точного моделювання навантаження на локальну мережу та розрахунку об’єму дискових масивів. Відеопотік – це динамічні дані, об’єм яких змінюється залежно від інтенсивності руху в кадрі, складності сцени та обраного кодека.

Однією з найбільш недооцінених частин проектування є вплив зовнішніх факторів на роботу сенсора. Атмосферні явища, такі як туман, дощ та сніг, розсіюють світло, що призводить до значного зниження контрастності та неможливості ідентифікації об’єктів навіть при високій роздільній здатності.

У складних симуляціях враховується параметр видимості. Доведено, що при видимості менше 1 км туман стає головним фактором згасання сигналу, перевищуючи вплив диму або опадів. Моделювання дозволяє підібрати довжину хвилі ІЧ-підсвітки (850 нм проти 940 нм) для кращого проникнення крізь атмосферні перешкоди.

Якість нічного відео залежить не лише від ІЧ-підсвітки, а й від фізичних параметрів сенсора. При моделюванні апаратної частини камери враховується розмір пікселя: сенсор з пікселем 2,8 мкм здатний зібрати вдвічі більше фотонів, ніж сенсор 1,4 мкм, що важливо для систем без додаткового освітлення.

Моделювання ІЧ підсвічування включає розрахунок кута випромінювання (який має відповідати куту огляду об’єктива) та потужності. ПЗ VideoCAD дозволяє візуалізувати зони пересвіту та зони недостатнього освітлення, де ідентифікація стає неможливою через високий рівень цифрового шуму.

Сучасний ринок ПЗ для моделювання CCTV пропонує інструменти різного рівня складності – від простих онлайн-калькуляторів до складних BIM-орієнтованих систем.

IP Video System Design Tool (JVSG) – це інструмент, який є «золотою серединою» для системних інтеграторів. Він дозволяє створювати реалістичні 3D-моделі об’єктів, враховуючи висоту встановлення камер, кути нахилу та фізичні перешкоди. Він має величезну базу даних реальних камер, можливість імпорту Google Maps та планів у PDF/AutoCAD, дозволяє візуалізувати зони DORI/OODPCVS у кольорі, що допомагає замовнику зрозуміти реальні можливості системи до її монтажу.

VideoCAD Professional є більш потужний інструмент для наукового аналізу та складних проектів. VideoCAD дозволяє моделювати не лише геометричні параметри, а й складні фізичні процеси, такі як дисторсія об’єктива та спектральна чутливість сенсора. Так, функція «Території» дозволяє формалізувати ТЗ, розмічаючи зони з різними вимогами (наприклад, «Тут потрібна ідентифікація, а тут – лише детекція руху») та отримувати точний числовий звіт відповідності проекту цим вимогам. Підтримка формату COLLADA для SketchUp та AutoCAD дозволяє інтегрувати зони огляду камер у загальнобудівельні 3D-моделі.

Для великих інфраструктурних об’єктів проектування ведеться безпосередньо в середовищі Autodesk Revit. Виробники, такі як Axis та Motorola (Pelco), випустили спеціалізовані плагіни. Ці додатки дозволяють обирати камери безпосередньо з BIM-каталогу з усіма метаданими, перевіряти наявність «сліпих зон», спричинених інженерними комунікаціями будівлі (вентиляція, освітлення), автоматично оновлювати 3D-види при переміщенні камери на плані.

Моделювання системи повинно враховувати не лише технічні, а й етичні та юридичні межі. Камери не повинні бути спрямовані в місця, де очікується приватність (вбиральні, роздягальні). Встановлення попереджувальних табличок про ведення відеоспостереження є обов’язковою вимогою чинного законодавства.

Створення проекту. Сучасна еволюція систем технічної безпеки демонструє перехід від простих засобів фіксації зображення до складних інтелектуальних екосистем, що інтегрують штучний інтелект, глибоке навчання та високоефективні алгоритми обробки даних. Створення проекту системи відеоспостереження в сучасних умовах України вимагає не лише глибоких інженерних знань, а й прискіпливого дотримання динамічного законодавства, врахування вимог національних стандартів та стратегічного планування ресурсів для довготривалої експлуатації. Процес проектування охоплює широкий спектр етапів – від передпроектного обстеження та формування технічного завдання до розрахунку ємності сховищ та вибору оптимальної мережевої архітектури.

У контексті воєнного стану в Україні виникають додаткові обмеження та дозволи. Наприклад, використання відеореєстраторів водіями не заборонено жодним чинним законом, проте існують рекомендації та військові накази щодо обмеження зйомки стратегічних об’єктів, переміщення військової техніки та роботи ППО. Освітні заклади при впровадженні систем безпеки повинні орієнтуватися на «найкращі інтереси дитини», оскільки публікація зображень дітей у мережі може нести ризики фізичної безпеки та кібербулінгу.

Технічна частина проекту повинна базуватися на державних будівельних нормах (ДБН) та національних стандартах (ДСТУ), які визначають обов’язковість та правила встановлення систем безпеки. ДБН В.2.2-9:2018 «Громадські будинки і споруди» вводить вимогу обов’язкового облаштування громадських будівель сучасними системами охоронної сигналізації та відеоспостереження, ставлячи безпеку людини пріоритетом номер один.

Для різних типів об’єктів діють специфічні норми:

– заклади освіти: ДБН В.2.2-3:2018 «Будинки і споруди. Заклади освіти» передбачає обов’язкове проектування заходів безпеки, включаючи моніторинг приміщень та прилеглої території;

– дошкільні заклади: ДБН В.2.2-4:2018 регламентує вимоги до будівель садків, де відеоспостереження стає частиною загальної системи захисту та контролю доступу.

Методологічною основою для інженерів є стандарт ДСТУ EN 50132-7:2014 «Системи відеоспостереження охоронного призначення. Частина 7. Правила застосування» (хоча він і замінений на ДСТУ EN 62676-4:2017, основні принципи залишаються релевантними). Цей стандарт визначає життєвий цикл системи, починаючи з етапу визначення експлуатаційних вимог.

Процес створення проекту згідно з ДСТУ EN 50132-7:2014 та ДСТУ EN 62676-4:2017 включає декілька критичних фаз:

– визначення цілей спостереження (на цьому етапі встановлюється рівень деталізації, необхідний для кожної зони – детекція (виявлення об'єкта), розпізнавання (визначення знайомої особи) або ідентифікація (отримання доказів, достатніх для суду));

– передпроектне обстеження (аналіз середовища, топології мережі, конфігурації апаратних засобів та архітектури об'єкта);

– формування технічного завдання (документування оперативних вимог, вибір обладнання, визначення характеристик відео та параметрів зберігання);

– складання проектної документації (включає розробку схем розміщення камер, кабельних трас, специфікацій обладнання та розрахунків енергоспоживання);

– тестовий план та пусконаладка (визначення методики перевірки системи на відповідність ТЗ за допомогою тестових мішеней та протоколів якості зображення).

В умовах України, де питання безпеки є важливими, якісно спроектована система відеоспостереження стає не просто засобом фіксації подій, а проактивним інструментом захисту життя, майна та бізнес-інтересів. Використання сучасних стандартів, таких як ДБН та ДСТУ EN, гарантує, що інвестиції у безпеку будуть ефективними та виправданими.

Оцінка ефективності системи. Сучасна парадигма безпеки розглядає системи відеоспостереження не просто як засіб пасивної фіксації подій, а як інтелектуальний інструмент підтримки прийняття рішень. Ефективність такої системи визначається її здатністю трансформувати візуальний потік у релевантні дані, що мають операційну або доказову цінність. В умовах стрімкого технологічного прогресу оцінка ефективності перейшла від суб'єктивного сприйняття якості зображення до суворого кількісного аналізу метрик, що охоплюють технічні, алгоритмічні та економічні аспекти.

Історично оцінка базувалася на роздільній здатності камер, однак сьогодні такий підхід визнається фрагментарним. Комплексна ефективність розглядається як функція від імовірності виявлення загрози, точності ідентифікації об'єктів та операційної швидкості реакції на інциденти. Це потребує інтеграції технічного аудиту інфраструктури, оцінки надійності алгоритмів штучного інтелекту та аналізу повної вартості володіння. На системному рівні ефективність системи забезпечується через трикомпонентну стратегію: структурно-механічні заходи, електронні рішення та організаційні процедури.

Ефективність відеосистеми залежить від здатності мережевої та серверної інфраструктури обробляти відеопотоки без втрати пакетів та деградації якості. Основними параметрами оцінки тут виступають роздільна здатність, частота кадрів та ефективність алгоритмів компресії.

Для підтримки високої ефективності в сучасних IP-системах рекомендується використання гігабітних мереж, де реальна корисна пропускна здатність становить близько 500 Мбіт/с, що дозволяє уникнути мережевих затримок та «фрізів» відео. Важливо також враховувати резервування пропускної здатності (20–30%) для віддаленого перегляду та майбутнього масштабування системи.

Інтеграція нейромережевих алгоритмів змінила підхід до моніторингу, дозволяючи автоматизувати виявлення аномалій та класифікацію об’єктів. Оцінка ефективності таких систем базується на метриках точності, запозичених із галузі машинного навчання.

Надійність аналітичних функцій (наприклад, детекції вторгнення або розпізнавання обличь) оцінюється через чотири стани: справжнє спрацювання (TP), хибне спрацювання (FP), пропуск події (FN) та правильне ігнорування (TN). Ефективність алгоритму визначається балансом між чутливістю та стійкістю до завад.

У системах безпеки здатність системи виявити всі реальні загрози має бути максимальною, оскільки пропуск події (FN) може мати катастрофічні наслідки. Низька точність частки правильних ідентифікацій серед усіх спрацювань призводить до великої кількості хибних тривог, що спричиняє «втому оператора».

Ефективність системи відеоспостереження не може бути оцінена у відриві від фінансових витрат на її впровадження та підтримку протягом усього життєвого циклу.

Загальні витрати на побудову та функціонування системи включають не лише початкову вартість обладнання, а й приховані витрати, які можуть становити до 40-60% від загального бюджету за 5 років експлуатації. Сюди ж входять: електроенергія, охолодження серверних, ліцензії на програмне забезпечення, хмарне зберігання, витрати на обслуговування та втрати внаслідок простою системи.

Найбільш ефективною є та система відеоспостереження, яка інтегрована в загальну стратегію безпеки об’єкта, має чітко визначені цілі для кожної зони огляду та забезпечує позитивну модель окупності за рахунок мінімізації ризиків та оптимізації бізнес-процесів.

Представлення та затвердження замовником робочого проекту. Робочий проект системи відеоспостереження, який подається на затвердження замовнику, повинен бути вичерпним і цілісним. Він складається з декількох ключових блоків, кожен з яких несе специфічне смислове навантаження. Пояснювальна записка є інтелектуальним ядром проекту, де розкривається концепція безпеки, обґрунтовується вибір конкретних моделей обладнання та наводяться результати складних інженерних розрахунків.

Графічна частина проекту повинна відображати просторову архітектуру системи. Це не просто точки на плані, а деталізовані сектори огляду камер, де враховуються сліпі зони, висота встановлення та кути нахилу. Згідно з правилами ДСТУ Б А.2.4-4:2009, креслення мають виконуватися в масштабах, що дозволяють чітко ідентифікувати траси прокладки кабелів та місця монтажу обладнання. Особливо важливою є розробка структурних схем, які демонструють логіку взаємодії між камерами, комутаторами та центральним сервером, а також схеми підключення, що деталізують розпінування роз'ємів та маркування проводів.

Специфікація обладнання та матеріалів у складі РП є основою для подальших закупівель. Вона повинна містити не лише назви моделей, а й детальні технічні характеристики, що дозволяють замовнику переконатися у відповідності обраних рішень технічному завданню. У специфікації враховуються всі дрібниці – від об'єктивів та кронштейнів до кріпильних елементів та маркувальних бирок.

Кошторисна частина проекту є найбільш чутливою для замовника. Вона включає локальні кошториси, відомості ресурсів та об'єктні кошториси, складені згідно з чинними ціновими нормами. Для об'єктів, що фінансуються з бюджету, кошторисна документація повинна проходити сувору перевірку на відповідність ринковим цінам, що часто стає предметом зауважень під час експертизи.

Одним із найскладніших аспектів представлення проекту замовнику є пояснення того, чому обрано саме ці камери з такою роздільною здатністю та об'єктивами. Тут професійна спільнота спирається на міжнародний стандарт IEC 62676-4, адаптований в Україні як ДСТУ EN 62676-4:2014.

Момент представлення робочого проекту замовнику – це складний акт комунікації, де проектувальник виступає не лише як інженер, а й як консультант з безпеки. Важливо структурувати зустріч таким чином, щоб замовник пройшов шлях від розуміння глобальної концепції до деталей реалізації.

Типовою помилкою є фокусування лише на технічних характеристиках камер. Натомість, представлення має базуватися на цінності: як ця система вирішує конкретні болі замовника (крадіжки, контроль персоналу, безпека відвідувачів). Коли виникає зауваження «це занадто дорого», проектувальник повинен використовувати алгоритм приєднання та аргументації:

– визнання важливості бюджету для клієнта;

– роз'яснення структури вартості (наприклад, вартість спеціалізованих дисків для відеоспостереження порівняно зі звичайними комп'ютерними дисками);

– демонстрація ризиків відмови від певних рішень (наприклад, відсутність ідентифікації на критичних вузлах зробить систему неефективною для правоохоронних органів).

Також важливо враховувати «економію на масштабі». Дешевша система сьогодні може вимагати величезних витрат на ремонт та обслуговування завтра.

Професійно розроблений проект мінімізує аварійні ситуації та загрози життю і здоров'ю людей, що є головним пріоритетом будь-якої інвестиції в безпеку.

Для багатьох об'єктів в Україні етап представлення проекту замовнику завершується не підписом, а направленням документації на державну або приватну експертизу. Згідно з ДСТУ 8907:2019, експертиза є обов'язковою для об'єктів класів наслідків СС2 та СС3, а також для проектів, що фінансуються з державного бюджету (якщо вартість перевищує 300 тис. грн).

Метою експертизи є незалежна перевірка якості проектних рішень на відповідність вимогам законодавства, будівельних норм та правил пожежної безпеки. Експерти оцінюють не лише технічну частину, а й кошторисну дисципліну. Виявлення помилок на цьому етапі дозволяє запобігти дорогим витратам на етапі будівництва та експлуатації. За результатами видається експертний звіт, який може бути позитивним або містити зауваження, які проектувальник зобов'язаний усунути в найкоротші терміни.

Затвердження робочого проекту замовником не означає припинення роботи проектувальника. На етапі реалізації вкрай важливим є здійснення авторського нагляду, щоб переконатися, що монтаж виконується в повній відповідності до затверджених креслень. Автор проекту контролює відповідність обладнання специфікаціям та правильність виконання кабельних трас, що є гарантією надійної роботи системи в майбутньому.

Контрольні питання:

1. З чого починається процес проектування системи CCTV і яка головна мета розробки технічного завдання (ТЗ)?
2. Чому для вирішення складних завдань, таких як «запобігання проникненню», необхідний комплексний підхід, а не лише встановлення камер?
3. Які ключові чинники аналізуються на етапі обстеження об'єкта захисту?
4. Яким чином визначається необхідна кількість та місця встановлення відеокамер у проекті?
5. Що включає в себе вибір режимів відображення та зберігання відеоінформації?
6. У чому полягає суть «структурного синтезу» системи відеоспостереження?
7. Які параметри та критерії є визначальними при виборі конкретних типів обладнання для системи?
8. Для чого проводиться моделювання роботи системи CCTV перед її фінальною реалізацією?
9. Згідно з якими критеріями та стандартами проводиться оцінка ефективності спроектованої системи?
10. У яких випадках в Україні є обов'язковим проведення державної або приватної експертизи проектної документації?

Література: [25-28].

Тема 10. Інсталяція системи та здача замовнику

План:

Інсталяція відеокамер. Комплектування поста оператора. Прокладання та монтаж кабельних трас і комутаційного обладнання. Запуск і випробування системи на стійкість. Здача системи замовнику.

Інсталяція відеокамер. Процес інсталяції систем відеоспостереження у сучасному технічному середовищі вимагає розуміння відмінностей між доступними технологіями передавання сигналу. Вибір архітектури системи – чи то цифрової IP-мережі, чи то аналогової системи високої чіткості – визначає не лише методологію монтажу, а й майбутню масштабованість та надійність комплексу безпеки.

Ефективність системи відеоспостереження визначається не стільки кількістю камер, скільки стратегічною точністю їх розміщення відповідно до оперативних задач. Основною метою планування є повне перекриття важливих зон та виключення так званих «сліпих» зон, де зловмисник може пересуватися непоміченим.

Висота встановлення камери має бути збалансована між охопленням території та здатністю до розпізнавання обличь:

– рівень очей на висоті 1,7-2,0 м вважається еталонною висотою для ідентифікації осіб. Камера, встановлена на цьому рівні, фіксує обличчя відвідувача без перспективних спотворень, що важливо для подальшої експертизи записів;

– середня висота 2,5-3,0 м є оптимальним варіантом для зовнішнього спостереження. Це забезпечує широкий огляд території та одночасно захищає пристрій від вандалізму, оскільки до нього важко дістатися без використання драбини;

– стельовий монтаж на висоті понад 3,0 м використовується у великих складських приміщеннях або на відкритих майданчиках для моніторингу загальної логістики, проте ідентифікація окремих осіб при такому розміщенні значно ускладнюється через гострий кут зйомки (вид «зверху»).

У випадках, коли камеру неможливо змонтувати на безпечній висоті, обов’язковим є використання антивандальних корпусів, оснащених датчиками удару та розкриття.

При виборі ракурсу зйомки інсталятор повинен враховувати динаміку освітлення протягом доби. Пряме сонячне світло або потужні штучні ліхтарі, спрямовані безпосередньо в об’єктив, «засліплюють» камеру, перетворюючи зображення на сукупність відблисків.

Камери слід спрямовувати трохи вниз, уникаючи лінії горизонту з прямим сонцем.

Не рекомендується монтувати камери безпосередньо на вікнах або за склом через виникнення перешкод від відбитого інфрачервоного підсвічування вночі.

Важливо переконатися, що в зоні огляду немає об’єктів, що можуть загороджувати видимість: гілок дерев, бігбордів чи елементів конструкції даху.

Професійне встановлення системи відеоспостереження вимагає специфічного набору інструментів та розхідних матеріалів, склад яких варіюється залежно від обраного типу системи та умов середовища.

Для фізичного монтажу кронштейнів та прокладання кабельних ліній необхідні:

– перфоратор зі спеціальними бурами для цегли та бетону;

– дриль для свердління отворів під кріплення в дереві або металі;

– набір викруток, плоскогубці та кусачки для роботи з дротами;

– спеціалізований кримпер (обтискні кліщі) для конекторів RJ-45 та стрипер для зняття ізоляції;

– цифровий мультиметр та тестер кабельних ліній для перевірки цілісності трас та коректності живлення.

Якість кабельної продукції безпосередньо впливає на довговічність системи. Для IP-відеоспостереження використовується вита пара категорій Cat5e або Cat6, переважно з мідними жилами. Використання обмідненого алюмінію є небажаним через високий опір, що може призвести до падіння напруги в системах PoE та перегріву кабелю.

Для зовнішнього монтажу обов’язковим є використання:

– гофрованих труб або пластикових коробів для захисту кабелю від механічних пошкоджень та УФ-випромінювання;

– герметичних монтажних коробок (ступінь захисту IP66/IP67) для приховування роз’ємів та блоків живлення;

– силіконового герметика для заповнення отворів у стінах після прокладання кабелю, що запобігає потраплянню вологи та шкідників всередину приміщення.

Вулична інсталяція висуває підвищені вимоги до герметичності та стійкості конструкцій. Атмосферні опади та конденсат є головними ворогами електроніки.

Найвразливішою частиною системи є місце з’єднання камери з магістральним кабелем. Навіть мікроскопічна кількість вологи з часом викликає електрохімічну корозію контактів RJ-45, що призводить до мережевих збоїв або повної втрати сигналу. Усі конектори повинні бути заховані всередину монтажної коробки. Якщо камера постачається з герметичними ковпачками для роз’ємів, їх використання є обов’язковим.

Для додаткового захисту від вологи всередині корпусу камери або монтажної коробки рекомендується розміщувати пакетики з адсорбентом (силікагелем), які вбиратимуть зайву вологу.

При монтажі на фасадні системи (наприклад, сайдинг) свердління повинно проводитися максимально обережно, щоб не деформувати панелі. Після протягування кабелю отвір має бути ретельно загерметизований. Важливим інженерним прийомом є створення так званої «петлі для стоку» – невеликого вигину кабелю перед входом у стіну або коробку, щоб дощова вода

стікала в найнижчій точці петлі, а не затікала безпосередньо в роз'єм або отвір у фасаді.

Для забезпечення стабільності зображення камери мають монтуватися на жорсткі опори, що не піддаються вібраціям від вітру. У разі використання Wi-Fi антен на вулиці, вони повинні бути надійно заземлені та захищені від грозових розрядів.

Алгоритм підключення через PoE наступний. Базова схема з'єднання компонентів IP-системи включає наступні ланки:

кожна камера підключається кабелем вита пара до PoE-комутатора;

– PoE-комутатор виконує роль концентратора, що живить камери та об'єднує їх у локальну мережу. Він своєю чергою підключається до вільного порту головного маршрутизатора;

– маршрутизатор (роутер) забезпечує зв'язок між усіма пристроями в мережі та надає вихід в Інтернет для віддаленого перегляду.

– NVR відеореєстратор також підключається до роутера або безпосередньо до PoE-портів на задній панелі реєстратора, якщо такі передбачені конструкцією.

Така топологія «зірка» забезпечує максимальну стабільність: вихід з ладу однієї камери не впливає на роботу інших. Для систем, де кількість камер перевищує 8, рекомендується використовувати декілька комутаторів або професійні стійкові рішення.

Фізичне встановлення є лише половиною справи. Наступний етап – програмна активація та налаштування параметрів безпеки.

Сучасні камери постачаються в «неактивному» стані з міркувань безпеки. Для їх запуску використовується утиліта SADP (для Hikvision) або аналогічні інструменти інших виробників.

Утиліта сканує локальну мережу та знаходить усі підключені пристрої.

Користувач повинен задати складний пароль адміністратора. Це перший і найважливіший крок захисту від несанкціонованого доступу.

Рекомендується призначати кожній камері статичну IP-адресу, щоб уникнути конфліктів у мережі та забезпечити стабільний зв'язок з реєстратором після перезавантаження обладнання.

Налаштування детектора руху дозволяє суттєво зекономити дисковий простір та час на пошук потрібного фрагмента в архіві.

В інтерфейсі камери необхідно позначити лише ті області, де поява руху є важливою (наприклад, двері або вікна), виключаючи зони з листям дерев чи інтенсивним трафіком на задньому плані.

Регулювання рівня чутливості допомагає відсікти дрібні завади, такі як сніг чи комахи.

Увімкнення метаданих дозволяє візуально підсвічувати зони руху в режимі перегляду, що спрощує моніторинг оператором.

Функція запису за кілька секунд до фактичного спрацювання детектора гарантує, що початок події не буде втрачено через інерційність системи.

Дотримання наведених технічних регламентів дозволяє створити систему, яка не просто фіксує події, а реально працює як інструмент стримування правопорушень та надійне джерело доказової бази. Інтеграція штучного інтелекту для розпізнавання обличь та номерних знаків стає наступним логічним етапом розвитку, який вимагатиме ще вищої якості монтажу та оптичної підготовки об'єктів.

Комплектування поста оператора. Процес комплектування поста оператора вимагає глибокої інтеграції технічних засобів обробки даних, ергономічних рішень для підтримки працездатності персоналу та суворого дотримання нормативно-правової бази. Ефективність моніторингового центру визначається не лише роздільною здатністю камер, а й тим, наскільки раціонально організовано робочий простір, як забезпечено безперебійність живлення та який рівень комфорту надано оператору для мінімізації помилок, спричинених втомою.

Основою будь-якого поста відеоспостереження є спеціалізована обчислювальна станція. На відміну від стандартних офісних ПК, комп'ютер оператора повинен забезпечувати безперервне декодування десятків відеопотоків високої чіткості в режимі реального часу, що вимагає специфічної архітектури апаратного забезпечення. Технічні вимоги до таких систем базуються на показниках надійності, де середній наробіток між відмовами має становити щонайменше 13 000 годин.

Критичним компонентом робочої станції є графічна карта. Згідно з державними стандартами та технічними вимогами до систем безпеки, відеокарта повинна відповідати класифікації G3 або вище. Це означає, що розрядність буфера кадру має перевищувати 128 біт, що дозволяє ефективно обробляти потоки з великою кількістю кадрів за секунду без затримок у виведенні зображення на монітори. Для систем, що використовують інтелектуальну відеоаналітику на стороні клієнта, вимоги зростають до рівнів G5-G7, де графічний процесор бере на себе частину обчислень з розпізнавання образів.

Системна пам'ять комп'ютера оператора повинна бути не лише достатньою за об'ємом (мінімум 4 ГБ, але рекомендовано від 16 ГБ для сучасних VMS), а й володіти механізмами корекції помилок. Використання цієї пам'яті мінімізує ризик критичних збоїв системи (синій екран), які можуть бути фатальними в моменти інцидентів, коли безперервність спостереження є пріоритетом.

Оперативне керування сучасними роботизованими камерами (PTZ) неможливе за допомогою лише клавіатури та миші. Професійне облаштування поста передбачає використання спеціалізованих IP-пультів з багатокоординатними джойстиками. Пристрої типу Hikvision DS-1100KI пропонують 3-осьові джойстики, які дозволяють одночасно контролювати поворот, нахил та наближення (zoom) об'єктива, що важливо при супроводі об'єкта, який швидко рухається.

Такі пульти часто обладнуються сенсорними екранами для швидкого вибору камер або пресетів, а також мають інтерфейси RS-485 та RS-232 для прямого керування застарілим аналоговим обладнанням або інтеграції в складні системи автоматизації. Використання пультів знижує когнітивне навантаження на оператора, дозволяючи йому фокусуватися на моніторі, а не на пошуку кнопок у програмному інтерфейсі.

Ефективність оператора відеоспостереження різко падає після двох годин безперервної роботи, якщо його робоче місце не відповідає ергономічним нормам. В Україні ці параметри жорстко регулюються стандартами ДСТУ 7951:2015 «Крісло оператора» та ДСТУ 7299:2013 щодо взаємного розташування елементів робочого місця.

Згідно з ДСТУ 7951:2015, робоче крісло повинно забезпечувати «фізіологічно раціональну позу», яка мінімізує статичне напруження м’язів та запобігає застійним явищам у судинах. Хребет повинен зберігати свої природні вигини, а кут нахилу тазу має бути близьким до положення стоячи (40-45°). Це досягається через складну систему регулювань, де крок зміни лінійних розмірів становить 15-20 мм, а кутових становить 2-5°.

Особливо важливим є дотримання кутів згинання кінцівок – руки в ліктьових суглобах мають бути під кутом 70-90°, а ноги в колінних та гомілковостопних суглобах – 95-135°. Для забезпечення останнього параметра робоче місце обов’язково обладнується підставкою для ніг шириною не менше 300 мм та глибиною 400 мм, що дозволяє змінювати кут нахилу до 20°.

Розташування моніторів визначає рівень зорової втоми. Відстань від очей оператора до екрана має бути в межах 500-700 мм, а лінія погляду в розслабленому стані повинна бути на 35° нижче горизонталі. Це дозволяє охоплювати максимальну кількість інформації без напруження шийних м’язів.

Важливим аспектом є яскравість та контрастність зображення. Яскравість екрана повинна бути не менше 100 кд/м², а відношення яскравості екрана до оточуючих його поверхонь у робочій зоні не повинно перевищувати 3:1. Порушення цього балансу призводить до швидкої адаптаційної втоми кришталика ока. Крім того, екрани повинні мати антивідблискове покриття, щоб уникнути паразитного засвічення від штучного або природного освітлення.

Організація поста оператора в приміщенні з поганою вентиляцією або надмірним шумом знецінює будь-які інвестиції в дороге обладнання. Моніторингові центри вимагають прецизійного контролю мікроклімату, оскільки велика кількість працюючої електроніки постійно виділяє тепло.

Для приміщень, де ведеться спостереження, встановлено норми штучного освітлення: загальне освітлення має становити 400 лк, а комбіноване (з підсвіткою безпосередньо робочої зони) – до 1500 лк. Природне світло повинно падати збоку, переважно зліва, при цьому робочі місця мають бути розташовані не ближче ніж за 3 метри від вікон. Це мінімізує прямі сонячні відблиски, які можуть «засліпити» оператора при перегляді темних нічних сцен з відеокамер.

Температурний режим у межах 19-25 °С є важливим не лише для людини, а й для стабільної роботи активного мережевого обладнання, що знаходиться на

посту. Надмірний шум від серверних вентиляторів або систем охолодження (понад 60 дБ) призводить до підвищення витрат енергії організмом оператора на 17%, що спричиняє розвиток зорової втоми та зниження відчуття кольору. Тому рекомендується виносити основне серверне обладнання за межі зони постійного перебування оператора, використовуючи KVM-подовжувачі для дистанційного керування.

Надійність поста відеоспостереження залежить від фізичного та логічного захисту ліній зв'язку. У великих об'єктах, таких як бізнес-центри або промислові підприємства, відстань від камер та серверів до робочого місця оператора може перевищувати 100 метрів.

KVM-подовжувачі (Keyboard, Video, Mouse) дозволяють розташувати гучні та тепловиділяючі сервери в окремих серверних кімнатах, залишаючи на столі оператора лише монітори та маніпулятори. Сучасні цифрові подовжувачі, наприклад моделі брендів Aten та Lenkeng, забезпечують передачу 4K-відео без затримок на відстань до 70-120 метрів по витій парі CAT6 або навіть через IP-мережу.

Використання KVM-рішень з підтримкою протоколу HDCP гарантує апаратне шифрування цифрового сигналу, що унеможливлює перехоплення відеопотоку безпосередньо з кабелю. Крім того, професійні подовжувачі забезпечують електромагнітну сумісність та мінімізують ризики наведень, що важливо для чіткої ідентифікації об'єктів на відео.

Система живлення поста повинна розраховуватися з урахуванням пускових струмів та необхідного запасу потужності в 20-30%. Для сервера з блоком живлення PFC потужністю 600 Вт, розрахункова ємність ДБЖ повинна бути не менше 800 ВА.

Мінімальний час автономної роботи повинен становити 5-10 хвилин, що достатньо для коректного збереження метаданих та завершення сесій запису. Проте для автономних постів охорони рекомендується розраховувати АКБ на 2-8 годин роботи.

У приміщеннях з великою концентрацією дорогої електроніки використання водяних або пінних систем пожежогасіння є неприпустимим, оскільки вони призводять до незворотного пошкодження обладнання навіть при невеликому загорянні.

Стандарт ДСТУ 4466-1:2008 регламентує використання систем газового пожежогасіння. Такі системи використовують інертні гази або інгібітори (наприклад, HFC 23, HFC 125 або суміші типу IG-541), які швидко знижують концентрацію кисню в зоні горіння або охолоджують її на молекулярному рівні, не завдаючи шкоди платам та накопичувачам. Час випуску вогнегасної речовини зазвичай становить до 10 секунд, що дозволяє локалізувати пожежу на стадії задимлення. Важливо, щоб приміщення поста було обладнане системою аварійного вимкнення вентиляції та затримкою пуску газу для евакуації персоналу.

Прокладання та монтаж кабельних трас і комутаційного обладнання. Надійність передачі сигналу, довговічність обладнання та якість отримуваного

зображення безпосередньо залежать від дотримання технологічних регламентів під час проектування та монтажу кабельних трас.

Проектування електроживлення для обладнання спостереження має відповідати нормам ДБН В.2.5-23:2010, які поширюються на житлові, адміністративні та побутові будинки. Важливою вимогою є використання систем заземлення TN-S або TN-C-S для забезпечення електробезпеки та мінімізації електромагнітних завад.

Для об'єктів з умовною висотою понад 73,5 метра застосовуються спеціальні вимоги ДБН В.2.2-24, а блискавкозахист споруд регламентується ДСТУ Б В.2.5-38. Такий багатошаровий підхід до нормування гарантує, що кабельна інфраструктура відеоспостереження буде захищена від перенапруг, пожеж та механічних руйнува.

Спосіб прокладання визначається умовами експлуатації, архітектурними особливостями об'єкта та вимогами до механічного захисту.

Для відкритого прокладання всередині будівель найчастіше використовують пластикові кабель-канали (короби). Вони дозволяють швидко монтувати трасу, приховувати дроти та забезпечувати естетичний вигляд приміщень. Для промислових об'єктів або зон за підвісною стелею застосовуються металеві кабельні лотки (відкриті конструкції у вигляді жолобів) або короби (закриті конструкції). Лотки забезпечують кращу вентиляцію, що запобігає перегріву кабелів, тоді як короби забезпечують кращий захист від вологи та пилу.

У приховано монтажі (у штробах стін) кабель обов'язково затягується в гофровану трубу. Це захищає ізоляцію від пошкоджень під час будівельних робіт та дозволяє в майбутньому замінити кабель без руйнування стін.

При прокладанні кабелю між будівлями або по території об'єкта використовують підземний спосіб або повітряні лінії. Підземний монтаж є найбільш надійним, оскільки захищає трасу від атмосферних впливів та вандалізму.

Алгоритм підземного прокладання згідно з нормативами:

– розмітка траси та викопування траншеї глибиною не менше 70 см;

– видалення з траншеї каміння та предметів, що можуть пошкодити кабель;

– засипка піщаної подушки товщиною 10 см;

– затягування кабелю в захисний канал (ПНД-трубу) або використання броньованого кабелю (серії ВБбШв);

– вільне укладання кабелю в траншею (без натягу).

– засипка другого шару піску (10 см) та шару ґрунту (15 см);

– укладання сигнальної металевої стрічки над кабелем;

– повна засипка та перевірка цілісності ізоляції мегомметром.

Для повітряних ліній використовують кабелі з несучим тросом, що запобігає розривам при сильному вітрі або обледенінні.

Обладнання (відеореєстратори NVR, сервери, блоки живлення, ДБЖ) монтується у стандартні 19-дюймові стійки. Важливими елементами є патч-

панелі, на які заводяться всі кабелі від камер. Використання патч-кордів для з'єднання панелей з комутаторами дозволяє швидко змінювати конфігурацію мережі та проводити діагностику.

Приміщення серверної має бути сухим, провітрюваним та мати обмежений доступ. Обов'язковим є встановлення джерел безперебійного живлення (ДБЖ), які підтримують роботу системи під час короткочасних збоїв у мережі електропостачання та захищають жорсткі диски реєстраторів від пошкоджень.

Для стабільної роботи системи, особливо її вуличних компонентів, критично важливим є правильне заземлення та грозозахист. Навіть якщо блискавка влучає не безпосередньо в камеру, а поруч, індуковані перенапруги можуть вивести з ладу всю систему.

Захист має бути багатоступеневим і включати ПЗІП для ліній живлення та сигнальних ліній:

– захист Ethernet (PoE) – грозозахисні пристрої з роз'ємами RJ45 встановлюються між камерою та комутатором;

– захист аналогового сигналу – розрядники BNC або TVS-діоди монтуються перед відеореєстратором;

– захист живлення – обмежувачі напруги встановлюються у головному розподільчому щиті.

Згідно з ДСТУ EN 62305, опір заземлення для систем захисту не повинен перевищувати 10 Ом. Всі металеві корпуси реєстраторів та шаф мають бути підключені до шини PE.

Поширеною помилкою є підключення екрана витої пари або коаксіального кабелю до заземлення з обох сторін. Це створює «петлю заземлення», через яку по екрану протікають вирівнюючі струми, що викликають сильні відеоперешкоди та можуть пошкодити порти обладнання. Правильним рішенням є заземлення екрана лише в одній точці – зазвичай з боку комутаційної шафи. При монтажі на вулиці рекомендується використовувати діелектричні кронштейни для ізоляції камер від металевих опор будівель.

Для забезпечення керованості системи та швидкого усунення несправностей кожен елемент мережі має бути промаркований. Стандарт ANSI/TIA-606-B встановлює правила ідентифікації кабелів, портів та стійок.

Кожен ідентифікатор має бути унікальним та відповідати записам у базі даних (кабельному журналі). Наприклад, маркування 1A.AD02-40:02 означає:1A – 1-й поверх, приміщення A, AD02 – координати стійки в приміщенні, 40 – позиція патч-панелі (в юнітах від підлоги), а 02 – конкретний порт на панелі.

Кабелі повинні маркуватися з обох кінців надійно закріпленими етикетками. Використання QR-кодів на етикетках дозволяє персоналу миттєво отримати повну інформацію про лінію (тип кабелю, довжина, дата монтажу) за допомогою мобільного пристрою.

Стандарт рекомендує використовувати кольорові ковпачки або кабелі для візуального розділення функціональних зон: жовтий – системи безпеки, сигналізація, відеоспостереження; блакитний – горизонтальна підсистема (робочі місця); білий – перший рівень магістралі; пурпуровий – загальне мережеве обладнання (сервери, принтери).

Запуск і випробування системи на стійкість. Після завершення монтажу проводиться комплексне тестування мережі. Для витої пари це включає перевірку схеми розводки жил, вимірювання довжини лінії, затухання сигналу та перехресних наводок на відповідність стандартам ISO 11801 або TIA-568. Результати тестування оформлюються у вигляді звітів кабельного аналізатора.

Виконавча документація є обов'язковою для передачі замовнику і включає: схеми фактичного розміщення камер та трас, кабельний журнал із зазначенням маркування кожної лінії, протоколи вимірювання опору заземлення та ізоляції, специфікації встановленого обладнання та результати тестування ліній, логіни/паролі доступу та інструкції з експлуатації.

Ці документи є важливими для подальшої модернізації та обслуговування системи системними адміністраторами.

Процес запуску системи – це багатоетапна інженерна процедура, що починається з глибокого аналізу технічного завдання та завершується валідацією всіх підсистем під повним навантаженням. Дане дослідження детально розглядає методологію розгортання та випробування систем на стійкість, базуючись на міжнародних стандартах серії IEC 62676 та практичному досвіді експлуатації в специфічних кліматичних зонах.

Одним із найбільш ефективних методів попереднього випробування архітектури є програмне моделювання. Використання інструментів, таких як Cisco Packet Tracer, дозволяє створити віртуальну копію локальної мережі, підключити віртуальні камери та сервери, а також протестувати логіку маршрутизації та обробки даних ще до закупівлі обладнання. Це допомагає уникнути помилок у проектуванні IP-адресації та виявити потенційні вузькі місця в топології мережі.

Запуск системи починається з фізичного монтажу та первинної перевірки цілісності обладнання. Особлива увага приділяється відсутності механічних пошкоджень об'єктивів, сенсорів та роз'ємів, а також перевірці кабельних ліній на предмет заломів або оголених ділянок.

Процес активації сучасних IP-камер, зокрема виробництва Hikvision, передбачає обов'язкове встановлення надійного пароля адміністратора, що є першим кроком до кіберстійкості. Налаштування мережевих параметрів включає присвоєння статичних IP-адрес або резервування адрес на DHCP-сервері для запобігання конфліктам у мережі, що є поширеною причиною виходу камер із режиму онлайн.

Конфігурація серверів запису або NVR передбачає встановлення спеціалізованого програмного забезпечення, налаштування прав доступу користувачів та розкладу запису. Важливо ввімкнути сервіси хмарного

моніторингу, такі як Hik-Connect, для отримання сповіщень про стан системи в реальному часі. Для великих об'єктів налаштовується ієрархія прав, де оператори мають доступ лише до перегляду, а адміністратори – до зміни системних налаштувань, що мінімізує вплив людського фактору на стабільність системи.

Стійкість системи до зовнішніх впливів регламентується міжнародними стандартами, які класифікують рівень захисту оболонки від проникнення пилу, вологи та механічних ударів.

Мережева стабільність є важливою для запобігання втраті кадрів та забезпечення реального часу спостереження. Стрес-тестування мережі (Network Stress Testing) дозволяє оцінити поведінку інфраструктури під екстремальним навантаженням, імітуючи сплески трафіку або насичення каналів.

На відміну від стандартного тестування навантаження, стрес-тест спрямований на навмисне доведення мережі до стану відмови для виявлення «точок розлому». Основними параметрами для моніторингу є:

– пропускна здатність (Throughput) – максимальний об'єм даних, який мережа може передати без затримок;

– затримка (Latency) – час проходження пакету (для відеоспостереження затримка понад 100 мс може зробити PTZ-керування неможливим);

– джитер (Jitter) – коливання затримки, що призводять до розсипання зображення на артефакти;

– bufferbloat – стан, коли надмірна буферизація в мережевих пристроях призводить до величезних затримок при передачі потокового відео.

Для проведення випробувань рекомендується використовувати iPerf3 для генерації великих об'ємів UDP-трафіку, що імітує роботу десятків камер у високій роздільній здатності. Сценарій тестування повинен включати поступове нарощування навантаження від 50% до 90% від номінальної ємності каналу. Особливо важливо тестувати завантаження та вивантаження окремо, оскільки багато провайдерів та обладнання мають асиметричну продуктивність.

Система відеоспостереження втрачає свою цінність, якщо вона припиняє роботу в момент відключення електроенергії – саме тоді, коли ризик здійснення правопорушень є найвищим. Стійкість живлення забезпечується використанням джерел безперебійного живлення (ДБЖ) та схем резервування.

Типи ДБЖ та їх застосування є наступні:

– резервні (Offline) – найдешевший варіант, підходить для домашніх систем. Має час перемикання до 10-20 мс, що може бути критичним для деяких серверів;

– лінійно-інтерактивні – оснащені стабілізатором напруги (AVR), що дозволяє підтримувати стабільну напругу без переходу на батареї при незначних відхиленнях у мережі;

– онлайн (Online/Double Conversion) має найвищий рівень захисту. Постійне перетворення енергії гарантує ідеальну синусоїду та нульовий час перемикання, що є обов'язковим для великих серверних станцій.

Випробування на стійкість живлення включає «failover-тест» – фізичне від'єднання ДБЖ від мережі та фіксацію часу роботи під реальним навантаженням. Важливо переконатися, що при досягненні критично низького рівня заряду сервер встигає коректно завершити запис та закрити базу даних для запобігання корупції файлової системи.

Завершальним етапом запуску є підписання акту введення в експлуатацію на основі чек-листа випробувань. Це включає перевірку кутів огляду, якості ідентифікації осіб (згідно з критеріями пікселів на метр), стабільності нічного бачення та коректності роботи тривожних входів/виходів. Важливо задокументувати всі параметри системи – від серійних номерів камер до схеми прокладки кабелів та конфігурації RAID-масиву.

Детальний аналіз методології запуску та випробування систем відеоспостереження дозволяє стверджувати, що стійкість є не характеристикою окремих компонентів, а результатом злагодженої роботи всієї інфраструктури. Кожна підсистема – від фізичного кронштейна до криптографічного ключа – має бути протестована в умовах, що максимально наближені до критичних.

По-перше, виявлено, що найбільш недооціненим фактором відмови є деградація RAID-масивів великої ємності під час відновлення. Перехід на RAID 6 або використання розподілених об'єктних сховищ стає необхідністю для сучасних систем з роздільною здатністю 4K та вище. По-друге, кліматична адаптація, розглянута на прикладі Луцька, доводить, що стандартних характеристик IP66 часто недостатньо для тривалої експлуатації в умовах високої вологості; необхідні активні системи вентиляції та підігріву. По-третє, мережева стійкість вимагає не просто широкої пропускної здатності, а інтелектуального керування трафіком для пріоритезації відеопотоків над фоновими процесами.

Завершальним інструментом забезпечення стійкості має стати впровадження автоматизованого моніторингу станів системи, що дозволяє виявляти перші ознаки деградації дисків, перегріву процесорів або падіння напруги в ДБЖ ще до того, як це призведе до зупинки спостереження. Тільки через поєднання суворого дотримання нормативних вимог ДСТУ та агресивного стрес-тестування можна гарантувати, що система відеоспостереження виконає свою функцію в критичний момент інциденту.

Здача системи замовнику. Процес здачі системи відеоспостереження замовнику є завершальною, але найбільш відповідальною стадією реалізації безпекового проекту. Вона інтегрує в собі технічну верифікацію обладнання, юридичне оформлення прав власності та відповідальності, а також запуск механізмів довгострокової експлуатаційної підтримки. У сучасному українському правовому та технічному полі цей процес перестав бути суто формальним підписанням актів, перетворившись на складну процедуру підтвердження відповідності державним стандартам, нормам кібербезпеки та вимогам щодо захисту персональних даних. Ефективна здача об'єкта гарантує замовнику не лише фізичну наявність камер, а й легітимність отриманих

доказів у разі правопорушень, стабільність роботи мережевої інфраструктури та зрозумілий алгоритм дій для обслуговуючого персоналу.

Передача системи відеоспостереження неможлива без формування повного пакету виконавчої документації. Цей масив документів слугує «біографією» системи, фіксуючи фактично виконані роботи, використані матеріали та налаштування програмного середовища. Відповідно до ДСТУ 2230-93 та загальних галузевих практик, документація повинна забезпечувати можливість відновлення системи у разі критичного збою або модернізації іншим підрядником.

Основним юридичним документом є акт приймання-передачі виконаних робіт. У структурі такого акта обов’язково відображаються перелік облікових одиниць обладнання, їх вартість (відновна та залишкова), а також результати проведених обстежень та випробувань. Важливо, що разом з об’єктом передається вся технічна документація, перелік якої фіксується в самому акті або додатках до нього.

Експлуатаційна документація, що ведеться під час технічного обслуговування, має включати:

– акт первинного обстеження складається при прийнятті системи на обслуговування, де фіксується поточний стан обладнання та виявлені дефекти;

– акт технічного повторного огляду, це такий документ, що складається не рідше одного разу на 5 років для оцінки морального та фізичного зносу системи;

– журнали реєстрації робіт необхідні для систематичного обліку планового сервісу та непередбачених ремонтів.

Кожен компонент системи повинен супроводжуватися гарантійним талоном від виробника або постачальника. Обов’язковими реквізитами в такому талоні є модель виробу, серійний номер, дата продажу та тривалість гарантійного терміну. Для безкоштовного обслуговування замовник зобов'язаний зберігати талон та дотримуватися правил експлуатації, зазначених у супровідних документах. Будь-яке порушення цілісності гарантійних пломб або механічні пошкодження, спричинені діями третіх осіб, анулюють зобов'язання виконавця. Окрім того, при оформленні документів на повернення або заміну товару необхідно вказувати ідентифікаційний код суб’єкта господарювання, його адресу та номер накладної.

Етап пусконалагодження завершується комплексним тестуванням, результати якого заносяться до протоколів і є підставою для підписання фінальних актів. Згідно з методологіями розробки та впровадження систем, тестування має бути мінімальним за кількістю тест-кейсів, але достатнім для підтвердження функціональності.

Тестування системи відеоспостереження поділяється на кілька ключових напрямків:

– об’ємне тестування – перевірка здатності системи обробляти та зберігати великі масиви відеоданих протягом заданого періоду часу. Це

дозволяє переконатися, що обчислювальна потужність сервера та ємність дискового масиву відповідають проектним розрахункам;

– стрес-тестування – оцінка стабільності роботи при пікових навантаженнях, наприклад, при одночасному зверненні кількох віддалених клієнтів або спрацюванні великої кількості тривожних сповіщень;

– тестування швидкості відновлення – моделювання ситуацій раптового зникнення живлення або розриву мережевого з'єднання з метою перевірки часу, необхідного системі для повернення у штатний режим роботи.

Важливим аспектом є верифікація реакції програми на зовнішні переривання та коректність відображення на різних пристроях (монітори операторів, мобільні клієнти). Кожен тест-кейс повинен мати унікальний ідентифікатор, короткий зміст, перелік передумов (налаштування середовища) та очікуваний результат.

Одним із фінальних кроків здачі системи є підготовка оперативного персоналу. Без належних навичок використання ПЗ навіть найдорожча система буде неефективною. Виконавець зобов’язаний надати технічну допомогу замовникові у питаннях експлуатації, що включає проведення інструктажу та складання інструкцій.

Контрольні питання:

1. Які існують еталонні висоти для встановлення відеокамер залежно від оперативної задачі (ідентифікація осіб чи загальний огляд території)?
2. Які переваги та недоліки має встановлення камер на значній висоті (понад 4 метри)?
3. Які вимоги висуваються до робочого місця оператора (поста спостереження) щодо ергономіки та освітлення?
4. Чому не рекомендується використовувати побутові телевізори замість спеціалізованих моніторів у професійних системах відеоспостереження?
5. Яких правил слід дотримуватися при прокладанні кабельних трас поруч із силовими лініями електропередач для мінімізації наводок?
6. Яке призначення «дрип-петлі» при монтажі кабелю та до яких наслідків може призвести її відсутність?
7. У чому полягає суть об’ємного тестування системи перед її здачею в експлуатацію?
8. Які параметри перевіряються під час стрес-тестування та моделювання швидкості відновлення системи?
9. Яку інформацію повинен містити «журнал подій» та чому важливо забезпечити його захист від редагування?
10. Які документи та навички повинен отримати персонал замовника під час фінального етапу здачі системи?

Література: [29].

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Сайт: SCRIBD. Технічні засоби систем відеоспостереження. URL: https://www.scribd.com/document/705265266/ (дата звернення 02.06.25р.).
2. Damjanovski V. CCTV: From Light to Pixels. 3rd Edition. Butterworth–Heinemann. URL: https://pdf-up.com/download/cctv-third-edition-from-light-to-pixels-4951969 (дата звернення 02.06.25р.).
3. Сайт: Deps. Побудова та технічна експлуатація систем відеоспостереження URL: https://deps.ua/ua/training/catalog/cctv/67108.html (дата звернення 02.06.25р.).
4. Чернявський С. С., Вознюк А. А., Грібов М. Л., Нєбитов А. А., Гвоздюк В. В. Основи візуального спостереження: практичний посібник. Київ: Норма права, 2024. 112 с.
5. Системи відеоспостереження. URL: https://expert112.com.ua/videonablyudenie/index_ua.html (дата звернення 02.06.25р.).
6. Відеонагляд. Як це працює? Як побудувати ефективну систему відеонагляду дома, офіса? URL: https://imperia.org.ua/article/videonaglyad-yak-ce-pracyue-yak-pobuduvati-efektivnu-sistemu-videonaglyadu-doma-ofisa (дата звернення 02.06.25р.).
7. Інтелектуальні системи відеоспостереження. URL: https://alarm.lviv.ua/blog/intelektualni-systemy-videosposterezhennia (дата звернення 02.06.25р.).
8. ШІ у камерах Ajax: Як одна технологія змінює підхід до відеоспостереження. URL: https://ajax.systems/ua/blog/ai-in-ajax-video-surveillance/ (дата звернення 02.06.25р.).
9. Як підключити відеоспостереження до системи Ajax. URL: https://ajax.systems/ua/how-to-connect-camera-to-ajax/ (дата звернення 02.06.25р.).
10. Встановлення відеоспостереження в транспорті. URL: https://alliancesafety.com.ua/uk/blog-ukr/vstanovlennya-videosposterezhennya-v-transporti/ (дата звернення 02.06.25р.).
11. Камера відеоспостереження Green Vision. Інструкція користувача. URL: https://logicfox.info/manuals/GV/site/IPC_user_manual.pdf (дата звернення 02.06.25р.).
12. BS 7958:2009 CCTV management and operation code of practice. URL: https://infostore.saiglobal.com/en-us/Standards/BS-7958-2009-2009-263522_SAIG_BSI_BSI_609599/ (дата звернення 02.06.25р.).
13. BS EN 62676-4:2015 Video surveillance systems for use in security applications. Application guidelines. URL: https://www.thenbs.com/PublicationIndex/documents/details?Pub=BSI&DocID=311425.
14. BS 7958:2015 Closed circuit television (CCTV) – management and operation – code of practice. URL: https://www.thenbs.com/PublicationIndex/documents/details?Pub=BSI&DoID=312704. (дата звернення 02.06.25р.).

15. BS 8418:2015 CCTV Systems for Installers. URL: https://www.riscauthority.co.uk//index.cfm?originalUrl=free-document-library/RISCAuthority-Library_detail.bs-8418-2015-installation-and-remote-monitoring-of-detector-activated-cctv-systems-code-of-practice.html&_tkn=FD45BCF0%2D18D2%2D4EC8%2DB8DDA7701FEA1C54. (дата звернення 02.06.25р.).

16. NTCIP 1205. Object Definitions for Closed Circuit Television (CCTV) Camera Control. URL: https://www.standards.its.dot.gov/Factsheets/Factsheet/83 (дата звернення 02.06.25р.).

17. I.S. 199:1987, Alarm systems – CCTV surveillance for use in security applications. URL: https://www.nsai.ie/certification/product-certification/security-systems/ (дата звернення 02.06.25р.).

18. AS 4806.2 – 2006 Closed Circuit Television (CCTV): Application Guidelines. URL: https://www.techstreet.com/standards/as-4806-2-2006?product_id=2068183 (дата звернення 02.06.25р.).

19. EN 50132-7:2012. Alarm systems - CCTV surveillance systems for use in security applications - Part 7: Application guidelines. URL: https://www.slideshare.net/malvvv/en-501327 (дата звернення 02.06.25р.).

20. ДСТУ EN IEC 62676-5:2019 Системи відеоспостереження охоронного призначення. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=83148 (дата звернення 02.06.25р.).

21. Критерії вирішення оперативних задач світових стандартів інформаційних систем CCTV / Терлецький Т. В., Ткачук А. А., Кайдик О. Л., Цебрук В. Р. // Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». Луцьк: Луцький НТУ, 2020. №41. С. 218-227.

22. Шляхи визначення граничної доцільності застосування стандартних критеріїв вирішення оперативних задач інформаційними системами CCTV / Цебрук В. Р., Терлецький Т. В., Кайдик О. Л. // Приладобудування та метрологія: сучасні проблеми, тенденції розвитку : матеріали Всеукраїнської науково-практичної конференції (29-30 жовтня 2020 р.): збірник тез. Луцьк, ВНЗ Луцький НТУ, 2020. 104 с. С. 91-92.

23. Терлецький Т. В., Кайдик О. Л., Пташенчук В. В. Реалізація інформаційної технології в проектуванні CCTV / Технічна творчість: Збірник наукових праць. / Укл.: Скиба М. Є., Поліщук О. С., Романець Т. П. Хмельницький: ХНУ, 2021. № 4 С. 53-54.

24. Терлецький Т. В., Кайдик О. Л., Пташенчук В. В. Гранична доцільність застосування стандартних критеріїв вирішення оперативних задач CCTV / The IV International Science Conference «Prospects and achievements in applied and basic sciences», February 9-12, 2021, Budapest, Hungary. pp. 690-694.

25. Сайт: Правозахисна організація «Фрірайтс». Системи відеоспостереження. URL: https://umdpl.info/programs/systemy-videosposterezhennya/ (дата звернення 02.06.25р.).

26. Відеоспостереження в публічних місцях: основи захисту персональних даних (посібник для органів місцевого самоврядування) / В. К. Батчаєв, У. С. Шадська. Київ: Компринт. 98 с. URL: https://umdpl.info/wp-

content/uploads/2021/09/POSIBNYK_videosposterezhennya_u_publichnyx_miscyax.pdf (дата звернення 02.06.25р.).

27. Технічне завдання на проектування, побудову (створення) і впровадження відомчої системи IP- відеоспостереження на міському полігоні твердих побутових відходів. URL: https://zt-rada.gov.ua/files/upload/sitefiles/_29.pdf (дата звернення 02.06.25р.).

28. Сайт: Siluette. Курс: Проектування систем відеоспостереження. URL: https://siluette.com.ua/uk/product/sstv/?srsltid=AfmBOooSNuoMN_sGjh7i0fJ1ACTpyjyT70s1NnY926JNGqL22-FXGcm0 (дата звернення 02.06.25р.).

29. Самостійний монтаж системи відеоспостереження на роботі і вдома. URL: https://topguard.ua/ua/korysne/419-montazh-systemy-videosposterezhennya (дата звернення 02.06.25р.).

С 75 **Системи відеоспостереження**: Конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп'ютерна інженерія» галузі знань Інформаційні технології спеціальності Комп'ютерна інженерія денної та заочної форм навчання. Терлецький Т. В., Кайдик О. Л.. Луцьк: ЛНТУ, 2026. 209 с.

Комп'ютерний набір та верстка: Т. В. Терлецький.

Підп. до друку "__" _____ _ 2026 р.
Формат 60х84/16. Папір офс. Гарн. Таймс.
Ум. друк. арк. ___. Обл. – вид. арк. ___
Тираж ___ прим. Зам. ____.

Відділ іміджу і промоцій
Луцького національного технічного університету
43018 м. Луцьк, вул. Львівська, 75
Друк – ВІП ЛНТУ