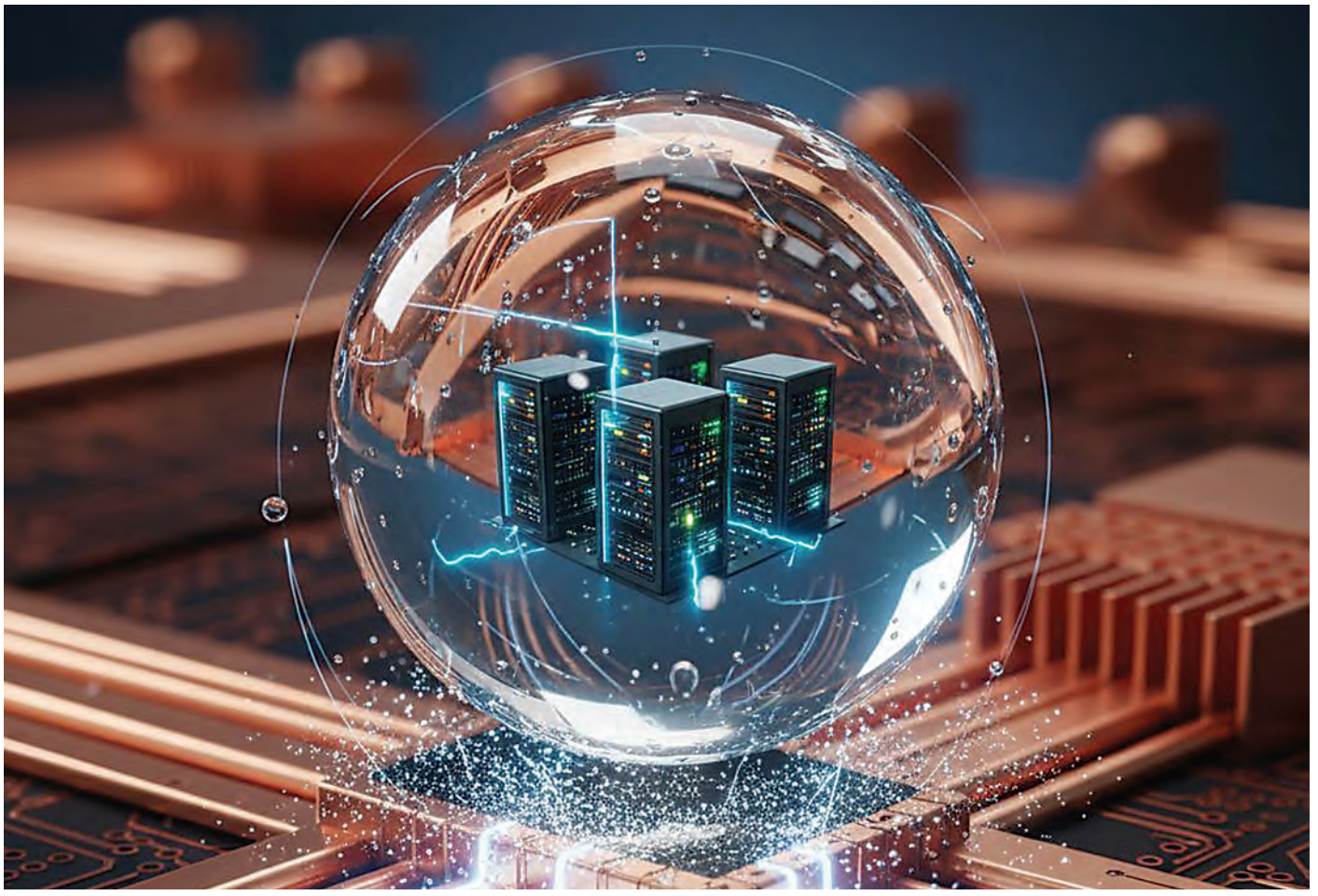
NVR vs відеосервер:

технологічний вибір, що формує майбутнє систем безпеки



На перший погляд здається, що відповідь очевидна: вибір диктує бюджет. Та чи справді все так просто? Подивімося, чим обертається цей вибір через 2–3 роки.

Ілюзія простого вибору

NVR (Network Video Recorder) завжди коштує дешевше, ніж відеосервер. Керуючись логікою «дешевше — значить краще для бюджету», замовники мали б завжди обирати тільки NVR. Проте значна частина свідомо купує для своїх проєктів відеосервери. Чому так?

Практика показує: NVR і відеосервер — це не просто різні типи обладнання. Це різні підходи до побудови відеоспостереження, різна філософія роботи з відеоданими, масштабування, інтеграції та управління життєвим циклом системи відеоспостереження та інших систем безпеки.

Цей вибір починає проявляти свої справжні можливості або обмеження в процесі експлуатації: під час розбору інцидентів і протидії кібератакам, контролю належного виконання службових обов'язків, підключення додаткових камер, додавання відеоаналітики та інтеграції з іншими системами безпеки.

В процесі експлуатації питання «Що було дешевше на тендері?» поступається іншому: «Що було закладено в основу системи?» та новою задачею від керівництва: «Як впровадити AI-стратегію на існуючій системі?».

NVR: комфорт із коробки та його межі

NVR десятиліттями залишалися і залишаються «золотим стандартом» для об'єктів малого та середнього бізнесу. Аптеки, невеликі магазини, кафе, ресторани, школи, склади, АЗС і приватні власники віддають перевагу NVR як доступному засобу збереження відеоархіву.

Цей принцип роботи NVR був успадкований з часів аналогового відеоспостереження. Тоді система будувалася в буквальному сенсі навколо DVR (Digital Video Recorder) — окремого пристрою, який приймав аналогові відеосигнали, оцифровував їх, записував на диски, а аналогове зображення камер виводив на монітор охорони. Це була повністю закрита, локальна система, орієнтована на функцію відеоспостереження в режимі реального часу. Архітектура системи на DVR передбачала невелику кількість камер та обмежене число користувачів. Функції системи відеоспостереження повністю залежали від можливостей DVR, а розвиток не розглядався як необхідність.

З появою IP-камер коаксіальні кабелі замінилися мережевими, а DVR еволюціонував у NVR. Проте зміни торкнулися переважно способу підключення камер, а не філософії роботи системи відеоспостереження. NVR зберіг ту саму модель: окремий пристрій для обробки та запису відео з жорстко визначеним набором функцій, обмежень і сценаріїв.

Саме тому більшість NVR і сьогодні сприймаються як самодостатні «коробкові» рішення, орієнтовані на швидке розгортання та базові задачі відеоспостереження (**рис. 1**).

Рис. 1. «Коробкові» рішення на базі NVR

Для інтегратора NVR — це ідеальний продукт для швидкого проєкту та джерело прибутку без зайвих турбот. NVR постачаються з попередньо встановленою безкоштовною операційною системою Linux і переважно з вбудованим PoE-комутатором. NVR легко проєктувати, легко продавати та легко встановлювати. Якщо у замовника виникає потреба хоча б в одній додатковій камері, то інтегратор залюбки продасть йому новий NVR і диски до нього.

Закрита логіка. NVR — готовий продукт із закритою логікою, де апаратна частина, програмне забезпечення й логіка роботи жорстко пов'язані між собою і заздалегідь запропоновані виробником. Якщо через два роки замовник вирішить замінити свої старі 2Мп-камери на нові 4K-моделі зі штучним інтелектом, то архітектура NVR не дасть зробити апгрейд, і йому потрібно буде замінити існуючий NVR на нову модель.

Vendor lock-in. Виробники IP-камер пропонують власні NVR-и разом з IP-камерами, адже їхня головна мета — збільшити дохід від продажів обладнання в кожен свій проєкт. IP-камери інших виробників сумісні з сторонніми NVR-ами через протоколи RTSP чи ONVIF, але NVR-и найкраще працюють і підтримують функції зі своїми рідними IP-камерами. Виробники NVR-ів навмисно не інтегрують відеоаналітику з IP-камер інших виробників чи не інтегрують свої NVR-и із сторонніми VMS (Video Management Software), щоб замовник став заручником обраного бренду камер, англійською це має назву vendor lock-in.

Ризики втрати відеоданих. Пропуск кадрів, сцена без потрібної деталізації, відсутність чи пошкодження відеоархіву є неприємними, але не бізнес-критичними для таких замовників.

Питання кібербезпеки. Виробники NVR-ів намагаються заспокоїти замовників, що «закрита архітектура робить пристрій менш вразливим до типових вірусів, що атакують Windows-системи», проте забувають сказати, що NVR-и (особливо китайських виробників) часто стають мішенню для DDoS-атак, які перетворюють NVR-и на керовані хакерами мережеві пристрої. Відомі випадки, коли хакнуті NVR-и допомагали атакувати IT-системи банків, телекомунікаційних та державних компаній, завдаючи серйозних фінансових збитків.

NVR — розумний вибір для проєктів, де кількість камер і завдання системи відеоспостереження не змінюватимуться протягом наступних 2—3 років.

Проте для замовників, де системи відеоспостереження починають «рости» або змінювати свої завдання з часом, існуючі NVR-и та програмне забезпечення від виробників IP-камер створюють великі проблеми та обмеження. Саме в таких сценаріях стає очевидно: проблема не в кількості камер, а в тому, що система відеоспостереження проєктувалася як набір пристроїв, а не як платформа.

Відеосервер: платформа та складова IT-інфраструктури

Дані з систем відеоспостереження державних проєктів, об'єктів критичної інфраструктури, промислових об'єктів, телекомунікаційних компаній, банків, національних музеїв та інших об'єктів належать до чутливої інформації, адже це важливі візуальні відомості про графік роботи компаній, працівників та відвідувачів, процеси та процедури. Для таких об'єктів відеоінформація — це не просто відеоархів. Вона є відеодоказом, який може бути ключем до виявлення обставин інцидентів та причетних до них осіб або засобом попередження можливих інцидентів.

Безпеку таких відеоданих, як і будь-яких інших критичних даних, може бути порушено через несанкціонований доступ до відеоінформації, мережі або пристроїв систем відеоспостереження унаслідок кібератак, зовнішніх та внутрішніх загроз. Тому захист відеоданих для таких об'єктів має ґрунтуватися на IT-стратегіях і процесах, які допомагають запобігти загрозам, зокрема пошкодженню, порушенню безпеки та втрати важливої інформації.

Відеосервер в парі з VMS — це програмно-апаратна платформа для системи відеоспостереження, своєрідний ***«центр обробки відеоданих безпеки»***, який при правильному плануванні та проєктуванні є однією із складових захищеної та керованої IT-інфраструктури об'єкта (**рис. 2**).

Функціональність. Функціональні можливості VMS разом з продуктивністю відеосерверів визначають функціональні можливості та сценарії роботи системи відеоспостереження, комплексних чи інтегрованих систем безпеки. Замовник може обрати різні моделі IP-камер чи IoT-пристроїв від різних виробників, які інтегровані в VMS. Це дозволяє отримати найкращий функціонал та на 100% вирішити задачі безпеки.

Інтеграції. VMS є програмним ядром сучасних систем безпеки, яке здатне підтримати інтеграцію з іншими системами. Відеосервер може бути базою відеоданих суто для системи відеоспостереження, а може — ядром інтегрованої системи безпеки, підтримуючи IP-камери, IoT-пристрої, VMS, відеоаналітику, біометрію, системи контролю доступу, охорони периметру, охоронної сигналізації, інженерні системи тощо. Готові чи кастомні інтеграції дозволяють замовникам будувати складні сценарії систем безпеки без залежності від одного виробника обладнання, тобто без vendor lock-in.

Масштабованість. Один відеосервер під керуванням сучасної VMS може обробляти та записувати до 500 камер, що відчутно підвищує керованість та спрощує адміністрування систем середнього (300—500 камер) та великого розміру (1000+ камер). Збільшення кількості камер, додавання камер більшої роздільної здатності, потреба в нових сценаріях, додавання нових користувачів не потребують заміни всієї системи. Масштабування системи відеоспостереження відбувається шляхом розрахунку вартості додаткових каналів, обчислювальних ресурсів для відео, а також додаткових програмних модулів. Збільшення глибини зберігання відеоданих з 30 до 60 днів не потребує заміни відеосервера, це питання розрахунків та вибору оптимальної системи зберігання даних (DAS/SAN/NAS).

Свобода вибору та керованість. Відеосервер може бути фізичним або віртуальним, розміщеним у серверній, в датацентрі, гібридному середовищі чи в хмарі. Відеосервер підтримує сучасні IT-стандарти та корпоративні політики: ActiveDirectory, централізоване керування доступом, логування подій та регулярні оновлення. Це не гарантує абсолютного захисту, але дає замовнику можливість вибору та найкращий спосіб керувати своїми відеоданими, що дозволяє керувати ризиками на рівні всієї організації, а не окремого пристрою.

Централізація та ієрархічна архітектура. Тільки повністю нові об'єкти (аеропорти, готелі тощо) потребують одночасної закупівлі сотень камер та інфраструктури.

Рис. 2. Програмно-апаратна платформа для системи відеоспостереження

Більшість замовників ростуть разом зі своїм бізнесом та роблять модернізацію застарілих систем відеоспостереження поетапно: спочатку ядро (головний офіс) і поступово підключення до нього всіх активів. VMS разом з відеосерверами мають забезпечити безшовну інфраструктуру та доступ операторів до всіх камер через єдиний клієнтський інтерфейс. Наприклад: «7 днів записуємо відео в філії, а потім зберігаємо ще 30 днів в центрі. Оператору філії необхідно надати права перегляду камер філії, а оператору центру моніторингу — на перегляд та експорт всіх камер». Такої гнучкої архітектури потребують безпечні міста, державні підприємства з єдиним центром керування (національна поліція, державна прикордонна служба, державна митна служба тощо), банки, логістичні компанії, промислові холдинги тощо.

Надійність. Серверна архітектура має апаратні RAID-контролери, що витримують одночасний вихід з ладу двох і більше дисків без зупинки запису. Щоб забезпечити відмовостійкість для відеосерверів запису та керування, створюють кластери, які забезпечують резервування типу hot— чи cold-failover. Якщо один сервер «падає», інший автоматично підхоплює його камери. Це дозволяє не втратити хвилини відео, вартість яких може коштувати мільйони.

Відеоаналітика та AI (докладніше в статті «VLM-відеоаналітика — новий тренд на ринку відеоспостереження», «МтБ» №№4—5/2025). Сучасні професійні VMS на серверах не просто записують відео: за рахунок інтеграції з новими AI-камерами різних виробників вони одночасно створюють метадані з атрибутами (тип, колір, класифікація об'єктів). Це дозволяє оператору VMS здійснювати майже миттєвий пошук за потрібними критеріями (чоловік в синій куртці, білий легковий автомобіль тощо), а вартість такої відеоаналітики безкоштовна для замовника, адже не потребує окремих відеосерверів. Якщо ж у замовників немає можливості замінити існуючі IP-камери, але є потреба у відеоаналітиці, то професійні VMS пропонують або «рідні» модулі відеоаналітики (менш популярний варіант через обмежену кількість модулів аналітики), або ж інтегровані модулі від сторонніх виробників (найбільш поширений варіант). Таким чином замовники можуть обрати найкращого виробника відеоаналітики для своїх задач, а інтегратори прорахують обчислювальну потужність та оптимальну архітектуру (CPU/GPU) відеосерверів для відеоаналітики. Наприклад, національна поліція зазвичай тестує до 3—5 виробників модулів розпізнавання номерів одночасно, щоб обрати найкраще рішення, але всі обрані виробники мають бути інтегрованими в VMS задля централізованого керування на рівні країни. Такий підхід відкриває нові можливості і для локальних стартапів — розробників певної категорії відеоаналітики. Ці розробники можуть створити свій алгоритм/модуль відеоаналітики та інтегрувати його у відомі VMS, що відкриє для них як місцевий ринок замовників, так і міжнародний.

Кібербезпека. При правильній побудові корпоративних політик безпеки відеосервери системи відеоспостереження та інтегрованої системи безпеки є складовою IT-інфраструктури. Це означає використання корпоративних механізмів аутентифікації, регулярну зміну паролів, контроль операторів та адміністраторів, контроль зовнішніх та внутрішніх ризиків. Лише в такому разі система відеоспостереження перестає бути «сліпою зоною» для служби інформаційної безпеки та не стане несподіваним джерелом кібератаки, яка здатна паралізувати роботу всіх інформаційних систем (це особливо критично для державних замовників).

Відеосервер — це не «дорожча альтернатива NVR», а інший клас рішень, орієнтований на довгострокову експлуатацію, підвищені вимоги та складні сценарії використання. Відеосервер — це не тільки компонент системи відеоспостереження, це основа для подальшого розвитку комплексної чи інтегрованої системи безпеки об'єкта.

Що має рахувати замовник, але чого не покаже жоден тендер

Вибір між NVR-ми і відеосерверами майже завжди починається з початкових інвестицій (CAPEX).

З цієї точки зору NVR виглядає беззаперечним фінансовим фаворитом: готовий пристрій з попередньо встановленою безкоштовною операційною системою, безкоштовним програмним забезпеченням для відео та вбудованим PoE-комутатором. Відеосервери вимагають більшого бюджету: серверне обладнання, ліцензійна операційна система, професійне VMS. Для багатьох замовників, особливо в межах тендерних процедур, нижча ціна стає вирішальним аргументом, адже її простіше обґрунтувати керівництву, яке помилково сприймає CAPEX на відеоспостереження як незворотні витрати.

Проте економіка систем відеоспостереження не обмежується початковими витратами: кожна придбана система має свою сукупну вартість володіння (TCO, total cost of ownership), яка і визначає справжню ціну безпеки.

В процесі експлуатації різниця між NVR-ми та відеосерверами стає більш помітною. OPEX (операційні витрати) відеосервера є прогнозованими й керованими. Замовник розуміє, за що він платить, які ризики знижує і які можливості отримує в майбутньому. Архітектура зберігає цілісність, єдину логіку управління та централізований контроль безпеки.

У випадку з NVR витрати на розвиток просто не враховуються, OPEX виникає в процесі експлуатації як вимушений апгрейд або повна заміна обладнання у відповідь на нові вимоги бізнесу. Додавання нових об'єктів, збільшення глибини архіву та (найбільш критичне) впровадження відеоаналітики показує: OPEX такого апгрейду NVR буде вищим за CAPEX.

Порівняння TCO NVR-рів та серверів показує, що ключовим економічним фактором є не початкова ціна, а вартість адаптації системи до майбутніх змін (див. **таблицю**).

Табл. NVR vs відеосервер

Критерій	Linux-based NVR	Відеосервер з VMS
Життєвий цикл	2—4 роки (заміна)	4—6 років (апгрейд)
Резервування	Базове чи відсутнє	Професійне (RAID, Cluster)
Кібербезпека	Entry-level	Професійна, згідно зі стандартами
Інтеграція	Vendor lock-in	Безмежна (API/SDK)
ML-відеоаналітика	Vendor lock-in	Будь-які IP-камери та інтегроване програмне забезпечення. Будь-які інтегровані AI-камери
DL-відеоаналітика	Vendor lock-in: окремі дорогі моделі IP-камер	
AI-відеоаналітика	Vendor lock-in: тільки нові дорогі AI-камери	
CAPEX	Низький	Середній чи високий
OPEX	Прихований	Чіткий та передбачуваний
Відповідність стандартам	Базова (IP, електромагнітна сумісність тощо)	Максимальна (включно з ISO, NIS2, GDPR)

Коли «дешево» стає «дорого»

Розгляньмо декілька прикладів, коли до замовників приходить усвідомлення, що їхня система відеоспостереження проєктувалася як набір пристроїв, а не як платформа чи центр керування безпекою.

Банк має головний офіс, двадцять філій по всій країні, 1000 IP-камер, 40 NVR і програмне забезпечення від виробника камер. Керівництво ставить задачу: забезпечити контроль за касовими операціями та банкоматами, підрахунок клієнтів у чергах перед касами, впровадити двофакторну автентифікацію в сховищі згідно з PCI DSS та підвищити якість обслуговування клієнтів менеджерами банку.

Як служба безпеки буде вирішувати ці задачі, враховуючи, що наявні IP-камери та ПЗ не підтримують відеоаналітику, а відеоспостереження не інтегровано з встановленою на об'єкті системою контролю доступу?

Промисловий об'єкт має підрозділи, які контролюють охорону території, промислові процеси та охорону праці. У кожного з підрозділів свої окремі системи відеоспостереження, підрозділ контролю за промисловими процесами має відеосервер з VMS, інші — окремі системи на NVR. Керівництво ставить задачу: забезпечити зниження смертності людей на виробництві, нарахування заробітної плати по факту кількості відпрацьованих годин з обов'язковим візуальним підтвердженням відвідування людиною робочого місця, а також запобігання крадіжкам під час вивозу готової продукції. Який підрозділ отримає від керівництва бюджет на вирішення цих задач, а в разі успішного впровадження — премії?

Обласний центр відзвітував у ЗМІ про впровадження системи відеоспостереження на базі штучного інтелекту. На фото, що поширювалось у пабліках, шість відеомоніторів з дрібними зображеннями з камер (по 32 камери на один монітор) без результатів роботи відеоаналітики. Замість чотирьох камер на моніторах чорні плями (це означає, що відеосигнал відсутній). Як можна оцінити таку роботу інтегратора? На чому побудована ця система: на NVR чи на серверах з VMS, враховуючи інформацію про «камери з функцією розпізнавання облич та транспортних засобів»? Чи захищена ця система від кібератак? Які результати і яким чином отримає поліція сусідніх областей? Чи зможе національна поліція відстежити шлях автомобіля чи людини по всій країні та на кордонах?

Об'єкт культурної спадщини. Недавній зухвалий грабунок у Луврі в Парижі наочно продемонстрував, яку фінансову та культурну цінність мають об'єкти, що перебувають під відеонаглядом. У жовтні 2025 року з музею було викрадено королівські коштовності з приблизною вартістю €88 млн, перш ніж служба безпеки встигла відреагувати.

Чи була на об'єкті система відеоспостереження? Чи була вона ефективною? Чи була вона інтегрована з системою охоронної сигналізації? Чи знала служба безпеки про стан справ? Чи подавалися бюджети на модернізацію відеоспостереження, враховуючи, що за рік Лувр отримував біля €198 млн за рахунок відвідувачів?

Аналізуючи відкриті публікації, можна з впевненістю сказати, що злодії абсолютно точно розуміли стан та можливості системи відеоспостереження.

Як думаєте ви: в Луврі були NVR-и чи відеосервери з VMS?

Архітектура, яка визначає майбутнє системи

Вибір між NVR і відеосервером — це не вибір між «дешево» і «дорого». Це вибір між короткостроковою зручністю та довгостроковою керованістю.

NVR-и залишаються ефективним рішенням для простих, статичних та відокремлених систем відеоспостереження. Проте у проєктах, де відеодані стають частиною бізнес-процесів, відеодоказами, потребують кіберзахисту та впровадження AI-стратегій, NVR-и стають обмеженням та створюють ризики.

Відеосервери з професійними VMS дозволяють побудувати інший клас рішень — надійний, безпечний і керований. Саме такий підхід дозволяє системам безпеки розвиватися разом з організацією, а не стримувати її розвиток.

Через 2—3 роки після запуску проєкту питання «що було дешевше на тендері» втрачає значення. Натомість вирішальним стає інше: чи готова ваша система до майбутнього.

Альона ШВЕЦОВА,
незалежний експерт з систем безпеки,
cctvmadonna