Системи безпеки — вже не просто сигналізація та відео, а нова IT-реальність

Про те, як відкрита архітектура, уніфікована IT-інфраструктура, аналітика та інтеграція змінюють сучасні системи безпеки — і що це дає бізнесу, розповідає Андрій Кондрашов, генеральний директор компанії Space IT.

Традиційно системи безпеки сприймають як набір спеціалізованих інженерних рішень: охоронну сигналізацію, системи контролю доступу, відеоспостереження, охорону периметра та інші системи, кожна з яких виконує окреме завдання.

Але чи відповідає таке уявлення сучасним технологіям і підходам до побудови систем безпеки?

Сьогодні відбувається фундаментальна зміна самої їхньої архітектури.

Від окремих систем до єдиної IT-інфраструктури

Камера відеоспостереження, контролер СКУД, домофон, датчик або інший пристрій безпеки стає звичайним мережевим пристроєм, підключеним до єдиної IP-інфраструктури підприємства.

Ethernet, IP, VLAN, PoE, QoS, маршрутизація, резервування, моніторинг і кібербезпека стають не додатковими можливостями, а складовими сучасної архітектури безпеки.

Пристрій → Ethernet → IP → VLAN → PoE → єдина керована мережа.

Це означає, що системи безпеки дедалі менше є окремою інженерною інфраструктурою і дедалі більше — спеціалізованим сегментом загальної IT-інфраструктури підприємства.

Ядро системи — вже не прилад, а обчислювальна інфраструктура

Змінилося не лише мережеве середовище. Змінилося саме обчислювальне ядро системи.

Якщо традиційна система була побудована на принципі:
пристрій → контролер → пульт → оператор,
то сучасна архітектура виглядає інакше:
серверна інфраструктура → віртуалізація → кластер → GPU → аналітика → дані → сервіси → інтеграція.

У великих проєктах системи безпеки можуть використовувати віртуалізовані сервери, кластеризацію, розподілені системи зберігання та обробки даних, GPU-прискорювачі для відеоаналітики та спеціалізовані обчислювальні ресурси для завдань штучного інтелекту.

Таким чином, інтегрована система безпеки стає повноцінною обчислювальною платформою.

Дані стають основним ресурсом

Сучасна камера вже не просто передає відеосигнал — вона генерує структуровані дані.

Сучасна відеоаналітика дозволяє детектувати об'єкти — людину, транспорт, тварину, предмет, обличчя, номерний знак, пожежу, чергу тощо; визначати атрибути об'єктів — колір, тип, напрямок руху та інші характеристики; а також додатково виконувати розпізнавання облич, номерних знаків та інших об'єктів.

При цьому аналітичні модулі можуть працювати безпосередньо на камері, на серверній платформі VMS-системи або на окремій AI-платформі.

Система перетворює дані на події, події — на рішення, а рішення — на автоматизовані дії.

Саме тут система безпеки виходить за межі суто охоронних функцій і починає брати участь в автоматизації технологічних та бізнес-процесів.

Наприклад, розпізнаний номерний знак або обличчя може стати підставою не лише для фіксації події, а й для автоматичного контролю доступу, реєстрації в'їзду, передачі даних до системи обліку, тарифікації або запуску іншого технологічного сценарію.

Відкрита архітектура стає ключовою вимогою

Сучасна система безпеки не повинна бути закритим набором обладнання одного виробника. Вона має бути відкритою платформою, здатною взаємодіяти з іншими системами.

API та SDK дають можливість інтегрувати функціональність на рівні виробника, системного інтегратора та самого замовника. Система безпеки може взаємодіяти з ERP, BMS, SCADA, SIEM, PSIM, Microsoft Active Directory та іншими корпоративними або державними IT-системами та реєстрами.

Провідні виробники — Milestone, Genetec, Inner Range, Network Optix, Incoresoft, Suprema, Axis, Hanwha та інші — розвивають інструменти інтеграції, які дозволяють створювати не лише системи виявлення подій, а й платформи для автоматизації процесів.

І тут є сенс зупинитися детальніше.

Наприклад, розпізнаний номерний знак або обличчя з додатковими атрибутами, трансформовані в дані та передані за допомогою API/SDK до іншої системи, можуть стати основою для автоматизації процесів у різних сферах:

- **у державному секторі** — для ідентифікації та перевірки визначених критеріїв: розшук, заборгованість, перевищення швидкості. Відповідно формується автоматизований процес реагування, що мінімізує людський фактор і скорочує час прийняття рішення щодо зупинки, переслідування тощо;
- **у корпоративному секторі** — для ідентифікації працівників і відвідувачів, обліку робочого часу, автоматизації їхнього доступу, а також в'їзду/виїзду транспортних засобів за визначеними правилами;
- **у секторі комерційної нерухомості та ритейлу —** для роботи з великими потоками відвідувачів: їхньої ідентифікації, підрахунку та перевірки за визначеними критеріями, зокрема виявлення осіб із чорних списків; автоматизації роботи інженерних систем будівлі, зокрема керування ліфтовим обладнанням залежно від прав доступу, часу та поточного навантаження; автоматизації в'їзду/виїзду гостьового автотранспорту, а також його тарифікації.

Інший приклад — виявлення задимленості в кадрі та зміни температури за допомогою біспектральних комплексів відеофіксації. У поєднанні із сучасною відеоаналітикою та відкритою архітектурою це дозволяє не лише отримати дані про подію — дим чи пожежу, а й визначити координати, побудувати маршрут та запустити інші реакції щодо її ліквідації: направити визначену пожежну команду за певним маршрутом, запустити безпілотний літальний апарат для відеофіксації ситуації на місці події та допомогти у прийнятті управлінських рішень.

Передача подій додатково із систем безпеки до SIEM та PSIM дозволяє не лише централізовано збирати, структурувати й зберігати інформацію, а й відображати її у вигляді наочних дашбордів та аналітичних звітів. Об'єднання подій із різних систем — відеоспостереження, СКУД, охоронної сигналізації, периметрових датчиків, IT-інфраструктури, BMS та SCADA — дає можливість встановлювати взаємозв'язки між подіями, визначати їхню послідовність і виявляти причинно-наслідкові сценарії.

Наприклад: система захисту периметра фіксує подію → СКУД показує відсутність легального проходу → охоронна сигналізація фіксує рух у критичних зонах → BMS інформує про непрацездатність ліфтів → IT-monitoring фіксує перехід серверної на безперебійне живлення. SIEM/PSIM об'єднує ці події в один інцидент проникнення та формує відповідний сценарій реагування.

У результаті окремі події перетворюються на цілісну картину, на основі якої система може автоматично сформувати реакцію або передати інформацію оператору для прийняття рішення.

Таким чином, SIEM та PSIM дозволяють перейти від простого реагування на окремі тривоги до управління комплексними подіями та інцидентами. Система вже не просто повідомляє, що «щось сталося», а допомагає визначити, що саме сталося, як розвивалася подія, які системи та об'єкти задіяні і яку реакцію необхідно виконати.

У результаті змінюється сама цінність системи безпеки: вона має не лише виявляти загрози, а й допомагати приймати рішення, автоматизувати процеси, економити ресурси та підвищувати ефективність підприємства.

Безпека стає частиною IT-екосистеми

Технологічно сучасні системи безпеки давно вийшли за межі класичної сигналізації, контролю доступу та відеоспостереження.

Сьогодні недостатньо просто підібрати камери, контролери та сервери. Необхідно спроєктувати єдину архітектуру — від мережевої інфраструктури та обчислювальних ресурсів до аналітики, зберігання даних, інформаційної безпеки та інтеграції з корпоративними системами.

Саме такий підхід ми застосовуємо у своїх проєктах: розглядаємо системи безпеки не як набір розрізнених технічних засобів, а як єдину IT-систему, інтегровану в інфраструктуру та бізнес-процеси замовника.

Адже сучасна система безпеки повинна не лише захищати бізнес — вона має допомагати йому працювати ефективніше.