Фізична безпека 2026: від обладнання до платформи подій



Десять мегатрендів SIA і що вони означають для українського ринку СКД

Наприкінці 2025 року Security Industry Association (SIA) опублікувала щорічний звіт Security Megatrends 2026 — десять сил, які визначатимуть розвиток галузі безпеки найближчими роками. Головний висновок звіту: найбільшим чинником змін став штучний інтелект, який додає новий рівень трансформації в індустрію, що досі трималася на обладнанні та класичному програмному забезпеченні. Розгляньмо кожен із десяти трендів — і те, як він виглядає з погляду розробника систем контролю доступу в Україні.

Конкуренція в галузі поступово переміщується від характеристик камер, контролерів і зчитувачів до програмного забезпечення, інтеграції даних та ШІ (**рис. 1**). Системи контролю та управління доступом (СКД), відеоспостереження й охоронна сигналізація вже не можуть розвиватися як ізольовані рішення: замовник очікує від них не лише реєстрації подій, а й аналізу ситуацій, оцінки ризиків та автоматизованого реагування.

Перелік мегатрендів SIA сформовано за результатами опитувань і фокус-груп керівників галузі під час конференції Securing New Ground 2025. Нижче кожен розділ відповідає одному тренду; оригінальна назва SIA наведена під заголовком.

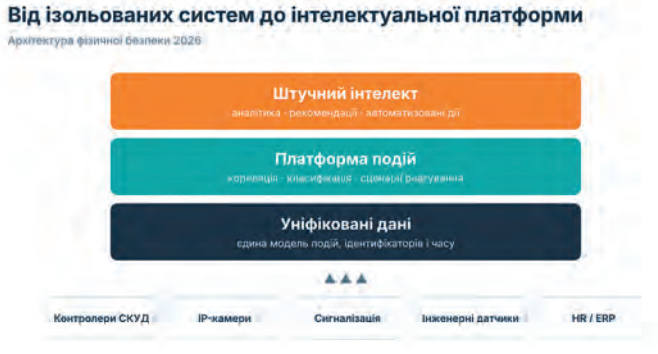


Рис. 1. Від ізольованих систем до платформи: дані, події, ШІ

1. Програмне забезпечення стає основою конкурентної переваги

SIA: Software Eats the World. Will AI Eat Software?
Тривалий час виробники конкурували характеристиками обладнання: роздільною здатністю камер, швидкодією контролерів, типами біометрії, кількістю точок доступу. Сьогодні вирішальним стає програмна платформа, яка об'єднує обладнання, забезпечує інтеграцію та визначає можливості системи.

Новий імпульс цьому дає генеративний та агентний ШІ. Традиційне ПЗ виконує заздалегідь запрограмовані функції, а ШІ-агент отримує завдання природною мовою, звертається до різних джерел даних, аналізує результати й виконує послідовність операцій. Замість ручного формування звіту оператор може попросити систему проаналізувати всі відмови в доступі за місяць, визначити проблемні об'єкти та підготувати аналітичний документ (**рис. 2**).

Програмне забезпечення перетворюється з набору функцій на інструмент управління процесами.

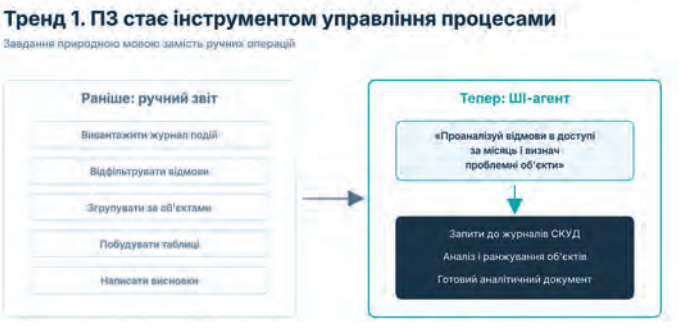


Рис. 2. Ручний звіт і завдання для ШІ-агента

2. Обладнання стає джерелом даних

SIA: The Security Hardware Layer Is Reinvented.
Камери, контролери та датчики залишаються фізичною

основою систем безпеки, але критерій їхньої цінності змінюється. Важливо не лише те, що пристрій уміє, а й те, яку інформацію він передає центральній платформі.

Сучасна камера передає відео разом із результатами розпізнавання об'єктів і даними про рух. Контролер доступу повідомляє не тільки про успішний прохід, а й про недійсні ідентифікатори, примусове відкриття дверей, порушення графіків, зміну конфігурації та втрату зв'язку (**рис. 3**).

Тому на перший план виходять відкриті API, документовані протоколи та повнота журналів подій. Пристрій, який повідомляє лише мінімум про свій стан, обмежує аналітику; обладнання, що генерує повні структуровані дані, стає повноцінним елементом інтелектуальної інфраструктури.



Рис. 3. Типи подій, які має передавати контролер доступу

3. Фізична безпека зливається з IT-інфраструктурою

SIA: Security Solutions Lose Their Boundaries. Межі між фізичною безпекою, IT та операційними системами підприємства зникають. СКД взаємодіє з HR та ERP, відеоспостереження — з інженерними датчиками, системи моніторингу — з корпоративними платформами управління.

Приклад із центру обробки даних: сигнал про зростання температури в зоні зіставляється з відео цієї зони, журналом доступу технічного персоналу та станом інженерного обладнання. Оцінюється не окрема тривога, а ситуація загалом (**рис. 4**).

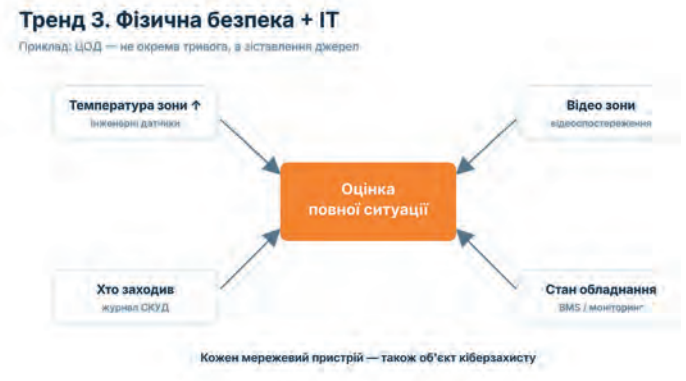


Рис. 4. Зіставлення джерел даних у ЦОД

Водночас зростає роль кібербезпеки. Контролер доступу чи IP-камера — це мережеві пристрої з власним ПЗ, обліковими записами та каналами адміністрування; їх компрометація загрожує всій корпоративній мережі. Тому фізичну та кібербезпеку слід розглядати як складові єдиної системи захисту.

4. Замість продажу обладнання — вимірювана цінність

SIA: The Value Chain Replaces the Channel Model. Традиційний ринок працював ланцюжком «виробник — дистриб'ютор — інтегратор — замовник», і винагороджувалися насамперед транзакції. SIA пропонує замінити цю модель ланцюгом цінності, у центрі якого — результат для замовника: рівень безпеки, керованість ризиків та операційний ефект.

Підприємству важливо не те, скільки камер встановлено, а наскільки ефективно працює система. Ключовими показниками стають час виявлення інциденту, швидкість реагування, кількість хибних тривог, доступність системи та витрати на її обслуговування (**рис. 5**). Інтегратори й розробники мають пропонувати рішення, ефективність яких можна виміряти.

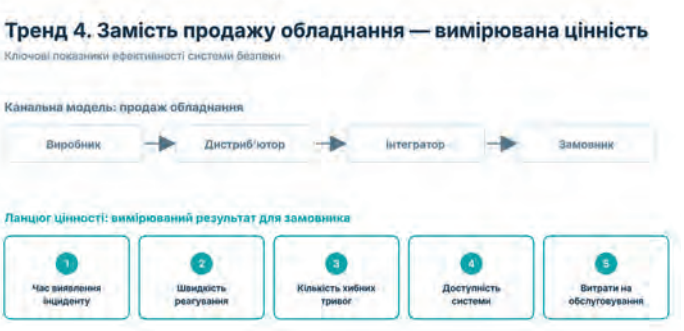


Рис. 5. Від канальної моделі до вимірюваних показників

5. Від автоматизації операцій до автономних процесів

SIA: Posthuman Automation of Security. SIA відзначає, що галузь дедалі охочіше надає ШІ повноваження в конкретних операційних сценаріях. Система, яка раніше лише реєструвала події, може самостійно аналізувати ситуацію та виконувати дозволені дії (**рис. 6**). У разі спроби несанкціонованого доступу вона здатна:

- отримати подію від контролера та оцінити її критичність;
- відкрити відео з камери відповідної зони;
- перевірити інші події в цій зоні та зіставити їх із правилами доступу;
- повідомити відповідального оператора;
- запустити затверджений сценарій реагування;
- сформувати картку інциденту.

ШІ-агенти можуть також регулярно перевіряти обладнання, аналізувати журнали подій і створювати завдання технічному персоналу.

Автономність не означає відмови від людського контролю. Критичні операції мають виконуватися в межах встановлених повноважень, із журналюванням і можливістю підтвердження оператором.



Рис. 6. Автономний сценарій реагування з контролем людини

6. Комплексні платформи та підхід «одного бренду»

SIA: End-to-End Solutions and One-Logo Approaches. Виробники розширюють екосистеми, поєднуючи СКД, відеоспостереження, сигналізацію та аналітику в єдиному програмному середовищі. Для малого й середнього бізнесу це зручно: менше інтеграцій, простіше адміністрування, одна точка підтримки.

Зворотний бік — залежність від одного виробника. Обмежені API, специфічні протоколи та закрита архітектура ускладнюють модернізацію чи заміну окремих компонентів. Довгострокову перспективу матимуть платформи, що поєднують переваги комплексного рішення з можливістю підключати обладнання інших виробників (**рис. 7**).



Рис. 7. Екосистема одного виробника та відкрита платформа

7. Уніфікація починається з даних

SIA: The Unification of the Security Experience Layer. Історично кожна система безпеки мала власні базу даних, журнал подій та інтерфейс. Навіть якщо відео, СКД і сигналізація виведені на один монітор, це ще не єдина інформаційна система. Справжня інтеграція починається на рівні даних і потребує:

- єдиної класифікації подій;
- узгоджених ідентифікаторів користувачів і пристроїв;
- стандартизованих часових міток;
- нормалізації повідомлень різних виробників;
- кореляції подій із різних джерел.

Наприклад, повідомлення про примусове відкриття дверей від трьох різних виробників платформа має трактувати як одну категорію загрози (**рис. 8**). Це дає змогу будувати універсальні правила реагування та аналітику незалежно від конкретного обладнання.

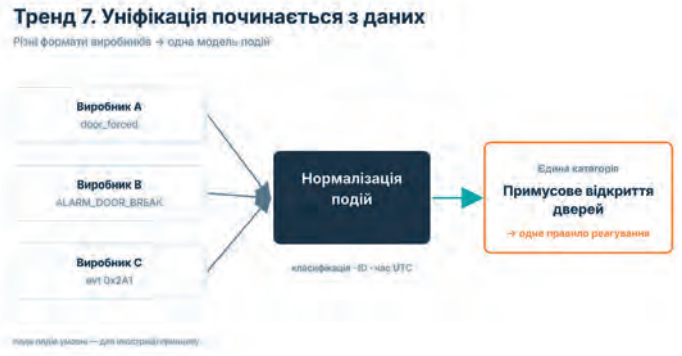


Рис. 8. Нормалізація подій різних виробників

8. Центри моніторингу переходять до управління інцидентами

SIA: SOCS and Monitoring Will Be Disrupted and Automated. Класичний центр моніторингу будувався навколо операторів, які стежать за відеостіною та обробляють потік тривог. Зі зростанням кількості камер і датчиків ця модель втрачає ефективність.

ШІ автоматично аналізує потоки подій, визначає пріоритети та передає оператору лише ситуації, що потребують уваги. Наступний крок — автоматизоване реагування: увімкнення освітлення, звукові попередження, блокування маршрутів доступу, виклик патруля, формування звітів. Оператор зосереджується на складних інцидентах і контролі автоматизованих процесів (**рис. 9**).

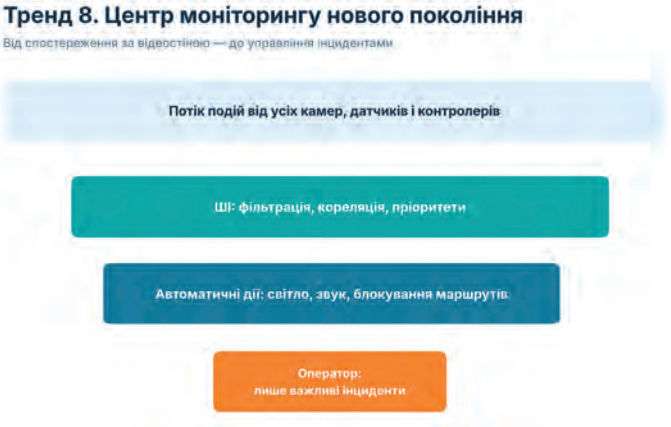


Рис. 9. Багаторівнева обробка подій у центрі моніторингу

9. Безпека має довести свою економічну цінність

SIA: Correcting the Systemic Undervaluation of Security. SIA говорить про системну недооцінку безпеки: підприємства традиційно сприймають її як

вимушену статтю витрат. Проте сучасні системи створюють і операційну цінність.

Дані СКД дозволяють аналізувати присутність персоналу, використання приміщень і дотримання робочих графіків; відеоаналітика допомагає оцінювати потоки відвідувачів і завантаженість зон. Ефективність системи вимірюється не лише кількістю попереджених інцидентів, а й скороченням операційних витрат, часу реагування та підвищенням прозорості бізнес-процесів. У галузі для цього вживають поняття Return on Security — віддачі від інвестицій у безпеку (**рис. 10**).

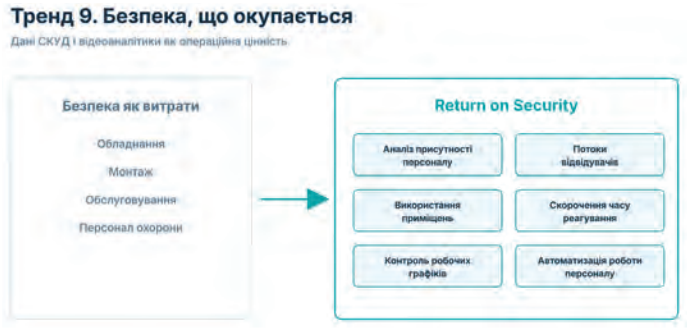


Рис. 10. Безпека як джерело операційної цінності

10. Цикли оновлення обладнання скорочуються

SIA: Security Technology Refresh Cycles Accelerate. Модель, за якої обладнання працює 10–15 років без суттєвого оновлення, відходить у минуле. Причини — кіберзагрози, нові технології, вимоги до інтеграції та розвиток ШІ-аналітики. Застарілі пристрої можуть не підтримувати сучасне шифрування, захищені API та централізований моніторинг, що створює ризики для всієї інфраструктури.

Модернізація не обов'язково означає повну заміну. Завдяки відкритій архітектурі можна зберегти працездатні контролери й камери, оновивши серверну частину, ПЗ та аналітичні модулі. Це дозволяє підприємствам модернізувати систему поетапно, без великих разових капітальних витрат (**рис. 11**).



Рис. 11. Повна заміна і поетапна модернізація

Український контекст

Для українських підприємств глобальні тренди накладаються на воєнні реалії. Система безпеки має зберігати працездатність під час відключень електроенергії, тому контролери повинні автономно ухвалювати рішення про доступ і буферизувати події до відновлення зв'язку з сервером. Сценарії реагування доповнюються інтеграцією з сигналами повітряної тривоги — наприклад, автоматичним розблокуванням шляхів до укриттів. А мережеві камери та контролери стали реальною ціллю кібератак, що робить вимоги **тренду 3** не теоретичними, а нагальними.

Висновки

Усі десять трендів мають спільну основу — перехід від ізольованих систем до інтелектуальної платформи управління подіями та процесами. На нашу думку, нову архітектуру фізичної безпеки визначатимуть три складові (**рис. 12**).

Дані. Обладнання різних виробників має передавати інформацію у стандартизованому, придатному для аналізу форматі.

Платформа подій. Об'єднує інформацію з різних систем, класифікує події, виявляє взаємозв'язки та забезпечує централізовану логіку реагування.

Штучний інтелект. Перетворює накопичені дані на аналітику, рекомендації та автоматизовані операції.



Рис. 12. Три складові нової архітектури фізичної безпеки

Для українського ринку це відкриває можливість будувати сучасні інтелектуальні системи на базі вже встановленого обладнання, поступово розширюючи функціональність без повної заміни інфраструктури.

Головна зміна 2026 року: фізична безпека перестає бути системою контролю обладнання і стає платформою управління подіями, ризиками та операційними процесами підприємства.



Андрій РОГОВ,
директор ПП «Конус»
andrey.rogov@gmail.com