Від тактильної безпеки до нейронної мережі підприємства

**Безпека має бути невидимою.
Доступ — безшовним.
Інтелект — абсолютним.**

Індустрія систем контролю доступу та фізичної безпеки активно розвивається вже понад чверть століття. За ці роки біометричні термінали та зчитувачі стали в рази точнішими, швидшими і захищенішими, проте принципова архітектурна логіка більшості рішень тривалий час залишалася незмінною: суб'єкт підходить до точки проходу, пред'являє ідентифікатор, а система реагує в бінарному режимі — **«Так»** або **«Ні»**. Ця стаття про те, чому ця логіка вичерпала себе — і яка архітектура приходить їй на зміну.

Еволюція апаратних засобів безпеки: анатомія архітектурного глухого кута

Протягом останніх десятиліть індустрія фізичної безпеки пройшла через кілька масштабних хвиль технологічної еволюції (**табл. 1**). Якщо перші комерційні впровадження біометричних алгоритмів розпізнавання відбитків пальців тривалий час залишалися нішевими рішеннями, то згодом галузь здійснила якісний стрибок — від класичних Wiegand-карток до передових систем 2D/3D-розпізнавання обличчя, а також від локальних аналогових контролерів до мережевих IP-терміналів із захищеним протоколом OSDP. Але фундаментальна операційна логіка залишилась незмінною.

Кожне покоління робило один крок: покращувало точність або зручність верифікації в конкретній точці входу. Але жодне не змінило фундаментального обмеження, яке ми називаємо **тактильною безпекою**.

За останню чверть століття індустрія фізичної безпеки пройшла колосальний шлях еволюції: на ринку з'явилися тисячі моделей високотехнологічних пристроїв, було впроваджено технології розпізнавання обличчя найвищого класу (Tier-1) та стандартизовано захищені протоколи передачі даних, такі як OSDP із шифруванням AES-128/256. Апаратний прогрес був реальним і значним. Проте у 2026 році, коли кіберзагрози стали гібридними, а сучасні атаки дедалі частіше поєднують фізичне проникнення з цифровим зламом, будь-який ізольований термінал — яким би точним і захищеним він не був сам по собі — залишається вразливою ланкою в загальному контурі інформаційної безпеки корпорації.

Таблиця 1. Розвиток технологій фізичного контролю доступу

Покоління	Технологія	Роки	Принципова межа
Перше	Картки Wiegand / PIN-коди	1990-і	Повна відсутність верифікації особи
Друге	Біометрія — відтиск пальця, геометрія руки	2000–2010	Ізольований сенсор без контексту
Третє	Розпізнавання обличчя (2D/3D)	2010–2020	Одна модальність, статична логіка
Четверте	Мультимодальна біометрія + OSDP	2020–2025	Дані залишаються у «силосах»

ТАКТИЛЬНА БЕЗПЕКА — ВИЗНАЧЕННЯ

Тактильна безпека – модель фізичного контролю доступу, в якій система активується виключно в момент контакту суб'єкта зі зчитувачем або терміналом. До цього моменту об'єкт «сліпий» – він не знає, хто наближається, з яким наміром і в якому контексті.

Головна вразливість: реактивність. Система реагує на подію, але не прогнозує її.

Для прихованого проникнення більше не потрібно підробляти картку або підробляти відтиск. Достатньо скомпрометувати людину з легітимним доступом — і жоден термінал, що перевіряє лише ідентичність, не відрізнить лояльного співробітника від скомпрометованого.

Інформаційні силоси: чому існуючі дані не рятують

На кожному сучасному Enterprise-об'єкті щодня генеруються терабайти даних безпеки. Відеоаналітика периметра, журнали СКУД, система обліку робочого часу (T&A), логи мережевої активності, VMS і система управління відвідувачами, — кожна з цих систем накопичує масиви даних, з яких можна зробити висновки про аномалії. Але вони не спілкуються одна з одною.

Ізоляція даних — не технічна проблема конкретного вендора. Це архітектурна проблема цілої індустрії, яка еволюціонувала через додавання нових систем поряд зі старими, а не замість них. Вирішення цієї проблеми потребує не нового термінала, а нової архітектурної парадигми.

Multimodal Fusion: руйнування силосів через єдину сесію довіри

Щоб подолати критичний бар'єр ізольованих систем, сучасна IT-архітектура безпеки переходить до впровадження патерну **Multimodal Fusion** (мультимодального злиття даних). У межах цієї концепції замість класичного очікування ізольованої транзакції від конкретного зчитувача (наприклад, прикладання картки до термінала СКУД) система починає збирати розрізнені телеметричні потоки в єдину наскрізну сесію «контекстної довіри».

Замість очікування транзакції від конкретного зчитувача, система розгортає три шари верифікації.

Дистанційний шар (просторовий ШІ): на далеких підступах — парковка, прилегла територія — оглядові камери під управлінням нейромереж аналізують силует, ходу (gait recognition) та вектор руху суб'єкта. Ідентифікація починається за 30–50 метрів до точки входу.

Контекстний шар (мережева телеметрія): система зіставляє відеопотік із непрямими ознаками присутності — BLE/NFC-сигналами смартфона, логами авторизації у внутрішній Wi-Fi мережі підприємства, статусом цифрової перепустки у VMS.

Еталонний шар (апаратний Trust Anchor): коли суб'єкт досягає фізичної межі зони доступу, термінал (Suprema або аналог) проводить локальне сканування за <0.2 с, генерує криптографічно захищений біометричний хеш і передає його до ШІ-ядра як юридично значуще підтвердження особи.

У цій схемі роль термінала кардинально змінюється. Він перестає бути ізольованим контролером-автоматом. Тепер це — **високоточний еталонний сенсор** в архітектурі більшого ШІ-контуру. Його завдання — не «відкрити двері», а надати фінальне, апаратно-підтверджене підтвердження ідентичності для системи, яка вже сформувала контекстну картину суб'єкта.

Таблиця 2. Бінарна модель Dynamic Risk Scoring: Invisible Security vs Посилена верифікація

Invisible Security Risk Score = 0	Посилена верифікація Risk Score > порогу
Співробітник рухається звичним маршрутом. Двері відчиняються за метр. Турнікет — у режимі вільного шлюзу. Бар'єри зникають	Аномальна поведінка, нетиповий час, відсутність у корпмережі. Шлюз вимагає еталонної біометрії. Пріоритетний потік — на IT-безпеку

Цифровий двійник підприємства та Dynamic Risk Scoring

В основі архітектурного контенту майбутнього лежить модель активного Digital Twin (цифрового двійника) підприємства. Це не 3D-візуалізація будівлі — це математична Decision System, що працює в режимі реального часу і безперервно оновлює два профілі (**табл. 2**).

- **Профіль простору:** базова поведінкова матриця об'єкта — типові потоки людей, завантаження зон у різний час доби, стандартні сценарії руху транспорту, патерни доступу по відділах.
- **Динамічний профіль суб'єкта:** параметр Risk Scoring, який розраховується постійно. Замість жорстко прописаних правил If-Then система управляє доступом на основі рівня довіри, що обчислюється в реальному часі з урахуванням десятків параметрів одночасно.

1. Сценарій «Норма»: Invisible Security

Співробітник R&D-департаменту рухається своїм звичним маршрутом у звичайний час. Його Risk Score дорівнює нулю: gait recognition підтвердив особу на підході, смартфон зареєстрований у корпоративній мережі Wi-Fi, цифрова перепустка активна. Розсувні двері

АНАЛОГІЯ: ЗЕРНОВІ СИЛОСИ

У промисловості силос – це герметична, висока і абсолютно ізольована башта для зберігання зерна. Зерно в одному силосі ніяк не контактує з вмістом сусіднього.

В IT-архітектурі Enterprise-об'єктів безпека влаштована достоту так само. Камери пишуть гігабайти у свою «башту». Біометричні термінали СКУД зберігають логи у своїй. Мережева служба безпеки веде моніторинг у третій. Кожна система може бути ультрасучасною – але без спільного контексту ШІ-ядро не може приймати інтелектуальних рішень.

Результат: загальна картина об'єкта залишається фрагментарною навіть при наявності всіх даних.

відкриваються за метр до його наближення, турнікети переходять у режим вільного шлюзу. Бар'єри зникають — безпека стає невидимою.

2. Сценарій «Аномалія»: посилена верифікація

Той самий співробітник з'являється о 2:15 ночі і прямує до серверної кімнати. Смартфон не зареєстровано у Wi-Fi. Хода відрізняється від еталонного патерну. RiskScore перевищує поріг — система непомітно для оточуючих переходить у режим посиленої верифікації: шлюз вимагає еталонного розпізнавання обличчя на терміналі, суміжні камери IT-безпеки отримують пріоритетний потік. Все це — без залучення охорони до моменту фактичного підтвердження загрози.

Нейронна мережа підприємства: новий рівень архітектури

Multimodal Fusion і Dynamic Risk Scoring — це важливі інструментальні компоненти. Проте за ними стоїть більш фундаментальний архітектурний концепт, який принципово змінює логіку побудови сучасних систем фізичної безпеки.

Ми називаємо її **нейронною мережею підприємства** (Enterprise Neural Fabric).

Класичний підхід: кожна система безпеки — це ізольований інтелект. Камера вирішує, чи є в кадрі людина. Термінал — чи збігається відбиток пальця. Контролер — чи відкривати двері. Це набір паралельних, незалежних рішень.

ЕФЕКТИВНІСТЬ: BLACKWELLVS ПОПЕРЕДНЄ ПОКОЛІННЯ (H100)

×30 – прискорення інференсу складних MoE-моделей (рівень GPT-3, 1.8 трлн параметрів)

×25 – зниження енергоспоживання на одиницю ШІ-потужності

×2 – вища пропускна здатність при FP4 vs. FP8 при вдвічі меншому об'ємі пам'яті

130 ТБ/с – внутрішня пропускна здатність NVLink Fabric стійки GB200 NVL72 (72 GPU як один)

1.44 Ексафлопс FP4 – пікова обчислювальна потужність однієї стійки

Нейронна мережа підприємства — це єдиний когнітивний контур, де кожна точка збору даних є не кінцевим пристроєм прийняття рішень, а нейроном у загальній мережі. Жодна точка не вирішує самостійно. Рішення приймається ядром на основі синтезу всіх доступних сигналів.

Компоненти нейронної мережі підприємства

- **Сенсорний шар (нейрони-входи):** біометричні термінали, IP-камери, LiDAR, BLE/NFC-маяки, датчики вібрації, мережеві логи, ANPR-системи на в'їзді.
- **Шар агрегації (аксони):** потоки даних уніфікуються через HAL (Hardware Abstraction Layer) — єдиний протокол для обладнання всіх вендорів.
- **Когнітивне ядро (SDS Core):** Policy Engine + Multimodal Fusion + Risk Scoring + Digital Twin. Обробка та синтез усіх сигналів у реальному часі.
- **Виконавчий шар (ефектори):** турнікети, шлагбауми, IP-замки, оповіщення Security Operations Center, алерти в Telegram/SIEM.
- **Шар навчання (зворотній зв'язок):** кожна зафіксована аномалія та підтверджений інцидент коригує поведінкові патерни. Система стає точнішою з кожним тижнем роботи.

Ключова властивість нейронної мережі підприємства — вона отримує цифрові образи: персони, пристрою, транспортного засобу, події. Не набір записів у базі даних, а живий, динамічний профіль, що безперервно оновлюється в реальному часі.

Саме це робить перехід якісним, а не кількісним. Мова не про «більше камер» або «точнішу біометрію». Йдеться про принципово іншу модель: від реагування на події — до управління простором через безперервне розуміння контексту.

Обчислювальний базис: чому NVIDIA Blackwell — і чому зараз

Ідея мультимодального злиття та нейронної мережі підприємства не є новою. Дослідники пропонували схожі концепції ще в 2010-х. Але до 2025–2026 років їх реалізація в масштабі реального Enterprise-об'єкта була технічно нездійсненна.

Таблиця 3. Архітектура Blackwell в інфраструктурі Enterprise-безпеки та критичних ШІ-обчислень

Технологія Blackwell	Ефект для Enterprise-безпеки
HBM3e — до 8 ТБ/с на GPU	Утримання терабайтних баз біометричних векторів і цифрових двійників у надшвидкій пам'яті. Нуль звернень до повільних сховищ — нульова затримка на прохідних заводів, аеропортів, офісних кампусів
Формат FP4 (Tensor Cores 5-го пок.)	Прискорення інференсу важких мультимодальних нейромереж (LLM/VLM) у 2.5–5 разів проти архітектури Hopper при радикальному зниженні енергоспоживання. Трансформерні моделі, що розуміють контекст відеопотоку
Фабрика NVLink 5-го пок. — 130 ТБ/с на стійку	Внутрішня «тканина» стійки GB200 NVL72 об'єднує 72 GPU в єдиний вичислювальний домен. Усі 72 GPU бачать спільний пул пам'яті — ШІ-ядро безпеки масштабується лінійно без вузьких місць
RT-ядра 4-го пок.	Апаратний Spatial Intelligence — зіставлення LiDAR/радар із цифровим двійником об'єкта в реальному часі. Точні 3D-координати об'єктів без постобробки на CPU
Confidential Computing	Апаратно-ізольовані анклави пам'яті: навіть за root-доступу до ОС — компрометація біометричних шаблонів фізично неможлива. Критично для відповідності GDPR / ISO 27001
Multi-Instance GPU (MIG)	Жорстка ізоляція: контури реального часу (відеоаналітика, СКУД) та фонова бізнес-аналітика — на одному сервері, з гарантованим QoS кожному
Рідинне охолодження DLC — 120–140 кВт на стійку	Трансформація серверного СКУД у корпоративний ШІ-мікродатацентр. Та ж споживана потужність виробляє у 30 разів більше II-обчислень, ніж кластер H100

Рис. NVIDIA DGX GB200 NVL72

Спроба реалізувати Multimodal Fusion на CPU або GPU попередніх поколінь натикається на одну й ту саму стіну: обробка 200+ відеопотоків у реальному часі, паралельний інференс десятків нейромережевих моделей, зіставлення тисяч цифрових профілів із затримкою менш ніж 100 мс — це потребує обчислювальної щільності, яка стала комерційно доступною лише з приходом архітектури NVIDIA Blackwell (**табл. 3**).

Важливо: для розгортання SDS Core на більшості Enterprise-об'єктів не потрібна повна стійка GB200 NVL72 (рис.). Реальні конфігурації стартують від окремих серверів HGX B200 або периферійних рішень на базі NVIDIA IGX Orin. Архітектура Blackwell масштабується від Edge-вузла на периметрі об'єкта до централізованого ШІ-хабу корпоративного кампусу.

Апаратна безпека та Confidential Computing

Впровадження ШІ-архітектури порушує критично важливе питання: якщо система збирає та аналізує стільки персональних даних, як захистити самі ці дані? Компрометація бази біометричних шаблонів — це катастрофа, оскільки, на відміну від пароля, відтиск пальця не можна змінити. Сучасний стек технологій вирішує цю проблему на двох незалежних рівнях.

На стороні сенсора: фотографії облич та відтиски пальців знищуються відразу після сканування на пристрої. У мережу передається виключно незворотний математичний хеш. Передача здійснюється по захищеному протоколу OSDP із шифруванням AES-128/256, що повністю виключає атаку типу Man-in-the-Middle.

На стороні обчислювального ядра (NVIDIA Blackwell): підтримка технології Confidential Computing гарантує, що обробка біометричних даних та робота ШІ-моделей відбуваються в апаратно ізольованих анклавах пам'яті (TEE — Trusted Execution Environment). Навіть за умови компрометації операційної системи на рівні root — дані в анклаві залишаються недоступними для зловмисника.

Комбінація цих двох механізмів дозволяє підприємству відповідати вимогам GDPR (стаття 25 — Privacy by Design), ISO 27001 та галузевих регуляторних стандартів без компромісів між безпекою та функціональністю системи.

Нова метрика для CISO та CTO: від Cost Center до стратегічного активу

Фізична безпека Enterprise-об'єктів перестала бути зоною відповідальності виключно адміністративно-господарського відділу. У 2026 році це повноцінна частина IT-ландшафту та ІБ-стратегії корпорації.

Компанія Suprema за 26 років довела, що апаратна еволюція реальна: від примітивних зчитувачів до біометрії Tier-1 з апаратним шифруванням. Але наступний крок — не черговий апаратний цикл. Це архітектурний перехід, після якого сама роль фізичної безпеки в підприємстві змінюється кардинально.

Три зсуви, які відбуваються прямо зараз

- **Від реакції до прогнозу:** система не фіксує порушення після факту — вона розраховує Risk Score і попереджає до того, як станеться інцидент.
- **Від ізольованих пристроїв до нейронної мережі:** кожна камера, термінал, датчик стає нейроном єдиного когнітивного контуру підприємства.
- **Від контролю точок входу до управління простором:** нова архітектурна оперує безперервним потоком цифрових образів персон, пристроїв, транспорту та подій у реальному часі.

Інтеграція передових біометричних сенсорів та інтелектуального програмного забезпечення у програмно-визначене ШІ-ядро на базі NVIDIA Blackwell переводить систему безпеки з категорії витратних сервісів (Cost Center) до категорії драйверів ефективності бізнесу.

У результаті підприємство отримує не просто надійний замок чи ізольований пункт пропуску. Формується цілісна інтелектуальна екосистема, яка мінімізує людський фактор, гарантує безперервність бізнес-процесів і створює безпечне, безшовне цифрове середовище — у якому безпека є невидимою саме тому, що вона абсолютна.

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