СКД на шляху до IoT:

від електронних замків до хмарних рішень

Людина завжди намагалася захистити те, що їй було важливо: свій дім, господарські споруди і свою територію, винайшовши для цього дерев'яні механічні засоби запирання. Найдавнішим знайденим зразкам яких було приблизно 6000 років. З появою металу з'явилися металеві механічні замки та ключі, які на багато століть стали стандартом. Лише у другій половині 20-го століття було винайдено електронні замки , які в сукупності з фізичними та електронними засобами керування проходом та проїздом в сучасному світі стали називатися системою контролювання/контролю доступу.

Абетка систем контролювання доступу

Сучасні системи контролювання доступу (надалі — СКД) — це складні електронні системи, до складу яких входять фізичні та технічні засоби, апаратне та програмне забезпечення. Технічно грамотне проєктування та впровадження СКД вимагає від системних інтеграторів відповідних знань, кваліфікації та сертифікації, а ефективне використання та експлуатація СКД — знань та навичок від замовників. Тому спочатку приділимо увагу типовим помилкам та міфам, які притаманні українському ринку СКД.

Не магнітні, а безконтактні картки СКД

«Магнітні картки», — кажуть і навіть пишуть в інструкціях 70% замовників та користувачів систем контролювання доступу. На жаль, це типова помилка, яку треба виправити. Суто магнітних карт в системах контролювання доступу ніколи не було ☺. Але чому замовники досі кажуть «магнітні»? Для цього треба трошки згадати історію розвитку банківських систем та галузі систем доступу.

Рис. 1. Механічний замок VingCard

Рис. 2. Електронний замок VingCard для карт з магнітною стрічкою

Першу банківську пластикову картку випустила/ввела в обіг (дані відрізняються) американська компанія American Express у 1957 році. Особливістю цих карт з пластику стала наявність магнітної смужки (magnetic stripe), у створенні якої важливу роль відіграла американська компанія IBM. Нововведення було покликане убезпечити дані клієнтів, оскільки раніше використовувані перфорація та штрих-коди застаріли. У 1958 році Bank of America почав випускати банківські пластикові карти для своїх клієнтів, що викликало попит, і в середині 60-х років платіжними картками користувалися вже не тільки по всій Америці, але і в інших країнах. Bank of America почав пропонувати іншим банкам користуватись своєю системою, яка у 1976 році отримала назву Visa і стала першою міжнародною платіжною системою. В 1966 році банки-конкуренти Bank of America об'єдналися і створили Interbank Card Association (ICA), яка в кінці 70-х років змінила назву на MasterCard.

У 1975 році норвежець Тор Сьорнес (Tor Sørnes) винайшов перший механічний замок, якій відчинявся пластиковою карткою з отворами (**рис. 1**). Замок отримав назву VingCard, і через декілька років компанія з такою самою назвою стала постачати ці замки до готелів, тому що за рахунок комбінації отворів у пластикових картках готелі могли вирішити задачу безпеки готельних номерів.

В 1992–93 роках компанія VingCard випустила на ринок електронний готельний замок, який відчинявся картами з магнітною стрічкою (**рис. 2**). Ринок готельних СКД виявився таким перспективним, що у VingCard швидко з'явився конкурент — Onity, іспанська компанія зі штаб-квартирою в США, яка разом з VingCard стала на довгі роки готельним стандартом. Електронні замки обох компаній виявилися настільки надійними, що навіть зараз, подорожуючи мережами відомих готелів, досі можна зустріти в номерах їхні замки для карт з магнітною стрічкою.

В Україну банківські пластикові картки з магнітною смужкою/стрічкою прийшли в 1995–1996 роках разом з міжнародними платіжними системами. З розвитком банківської сфери виник шалений попит на впровадження систем контролювання доступу серед банківських та фінансових установ. Типовим завданням для системних інтеграторів у середині 2000-х років було забезпечення доступу клієнтів банків у нічний час до зони банкоматів саме за допомогою зчитувачів банківських карт з магнітною стрічкою та відповідних зчитувачів (**рис. 3**).

Рис. 3. Банківська картка з магнітною стрічкою та зчитувач СКД

Українська банківська сфера еволюціонувала від пластикових карт з магнітною стрічкою в 90-х, контактних пластикових карт підвищеної надійності з вбудованим чіпом/мікросхемою (chip card) в 2000-х до безконтактних (contactless) пластикових карт з вбудованим чіпом у 2010-х. З розвитком смартфонів від 2017 року стали звичними безконтактні NFC-платежі за допомогою Apple Pay/ Google Pay та мобільних телефонів.

Паралельно з розвитком банківських технологій в 90-ті роки в Україні та на всьому пострадянському просторі також відбувалися колосальні зміни у процесах доступу людей до робочих місць: паперові журнали, механічні турнікети та механічні замки з ключами активно замінювалися на західні електронні СКД з новим типом безконтактних

proximity-карток та proximity-зчитувачів (**рис. 4**), які працювали за технологією радіочастотної ідентифікації (RFID). Proximity-картки виготовлялися з пластику і містили всередині пасивну антену та мікропроцесор (чіп). Proximity-зчитувачі постійно випромінювали сигнал низької потужності в певному радіодіапазоні. Коли картка опинялася на певній відстані від зчитувача, спрацьовувала її антена, живила мікропроцесор, і він передав свій унікальний код на зчитувач.

Рис. 4. Безконтактна/proximity картка та зчитувач СКД

Отже, будь ласка, шановні замовники, інтегратори та користувачі систем безпеки, вживаймо коректну професійну термінологію: безконтактні чи proximity-картки системи контролювання доступу, а не магнітні картки.

Не пікалка, а ідентифікатор СКД

Кожен системний інтегратор хоч раз у своєму професійному житті чув від приватного чи навіть корпоративного замовника: «Мені треба домофон з пікалкою». Насправді мова йшла про домофон із вбудованим зчитувачем ідентифікаторів СКД.

Термін «домофон» на позначення пристрою, що містить мікрофон та динамік, є локальним і виник як похідна від двох англійських термінів: intercom та door phone. Коли кажуть «домофон», то за замовчуванням мають на увазі «аудіодомофон» та можливість голосового спілкування, а коли очікують можливості візуального контролю + голосового спілкування, то кажуть «відеодомофон». Домофони стали зручним засобом дистанційного відкриття дверей для відвідувачів та проходу людей, які мають на це право, завдяки вбудованому зчитувачу. Найбільшої популярності у домофонній сфері за кордоном в 90-ті роки набули інтеркоми з вбудованим зчитувачем типу Touch Memory iButtons (стандарт, що його розробила та вивела на ринок американська компанія Dallas Semiconductor), які інженери СКД швидко назвали «таблетка» (**рис. 5а**). Згодом виробники домофонів також перейшли на безконтактні proximity-брелоки (**рис. 5б**).

В Україні домофони почали масово з'являтися на ринку у 2000-х роках. Спочатку в офісах як аудіо та відео засіб спілкування з відвідувачами, потім в банках та на інших об'єктах. Фахівці добре пам'ятають перші іноземні відеодомофони південнокорейських компаній Commax та Kocom. Пізніше домофони стали масовим явищем та з'явилися на вхідних дверях звичайних будинків. Наймасовішими та найпопулярними до приходу на ринок китайських виробників були російські домофони Vizit.

Аби було зрозуміло, що двері відчинені, в домофон вбудували відповідні звукові та світлові сигнали. Звичайні користувачі поєднали форму брелока СКД зі звуковим ефектом, і утворилася ця дивна назва — «пікалка» ☺.

Не російський СКУД, а український СКД

Державний стандарт України ДСТУ 4000–2000 «Системи тривожної сигналізації охоронні теле(відео) системи і системи контролювання доступу. Терміни та визначення» ще у 2001 році визначив український термін «***система контролювання доступу***» (скорочено — СКД). Термін СКУД (системи контроля и управления доступом) визначений російськими стандартами та стандартами країн СНД, тому, якщо на сайті чи у документах українського інтегратора ви бачите термін СКУД, — це пряма ознака непрофесіоналізму і незнання державних стандартів.

До ДСТУ 4000–2000 додалися ДСТУ EN 50133–2-1:2012, ДСТУ IEC 60839–11–1:2017 та ціла низка стандартів ДСТУ IEC «Системи тривожної сигналізації та електронні системи безпеки. Електронні системи контролювання доступу». Корпоративні замовники, які мають СКД чи планують її встановити, повинні обов'язково ознайомитися з українськими стандартами, а системні інтегратори, що проєктують та встановлюють системи – мають їх знати та виконувати.

а) Контактний Touch Memory брелок СКД

б) Безконтактний proximity-брелок СКД

Рис. 5. Брелоки СКД

Чи дійсно всі СКД однакові?

Кожний замовник сприймає простоту/складність СКД крізь призму свого особистого досвіду. Згадаймо, що саме відноситься до сучасних систем контролювання доступу:
- прості автономні рішення на декілька точок доступу (хвіртка, будинок тощо);
- домофонні багатоквартирні системи;
- готельні СКД;
- СКД для фітнес-клубів, зон відпочинку та курортів;
- СКД для паркінгів та стоянок;
- пропускні пункти на платних автомобільних дорогах;
- СКД, які забезпечують доступ в офіси, житлові комплекси, державні структури, підприємства тощо;
- СКД об'єктів підвищеної важливості, які мають у своєму складі системи фізичного захисту: аеропорти, атомні станції, державний кордон і т.п.

Якщо замовник має досвід експлуатації СКД невеликого офісу, котеджу чи власного будинку — це дуже простий рівень, який не дасть розуміння цінності та функціональності СКД. Коли замовник має досвід експлуатації СКД великого об'єкта — наприклад підприємства, — його рівень буде вищім, і він обов'язково звертатиме увагу на облік робочого часу та звіти. Якщо замовник — гірськолижний курорт чи аквапарк, то СКД йому потрібна як засіб забезпечення оплати за послуги та доступ людей у відповідні зони.

В СКД немає другорядних складових, адже всі елементи пов'язані між собою, тому що СКД побудована на керуванні фізичними діями людей за допомогою певних логічних процесів. Зчитувачі завжди працюють в парі з ідентифікаторами СКД, а рівень, складність та функціональність будь-якої СКД визначається технічними характеристиками контролерів, сумісним з ними програмним забезпеченням та обраними замовниками технологіями СКД.

Найкращий спосіб для замовників отримати користь, максимум функцій від існуючої чи майбутньої СКД та запобігти витоку даних — це підняти свій рівень знань.

Технології СКД: від старих до нових та безпечних

Коли інженери винайшли пластикові карти з магнітною стрічкою та почали використовувати їх в СКД — це було дуже круто, але з часом виявилося, що контактні картки не дуже зручні та надійні. У 80-х роках американський інженер німецького походження Джон Річард Віганд відкрив фізичне явище, при якому запресовані у пластик металеві смужки, виконані зі спеціального феромагнітного сплаву, при піднесенні до відповідного зчитувача створювали сплески індукційного струму, які можна було перетворити на двійковий код, тобто фактично було відкрито ефект безконтактної передачі цифрового коду. Стандартом індустрії став однойменний інтерфейс Wiegand, який виник як розвиток технологій Віганда. Інтерфейс ***Wiegand*** — це принцип підключення дротів між зчитувачами та контролерами, він призначений для передачі на контролери СКД унікальних кодів карток або PIN-кодів, набраних на клавіатурах.

З часом та статистикою зламів СКД з'ясувалось, що критичними проблемами інтерфейсу Wiegand є відсутність контролю цілісності кабелю між зчитувачем та контролером, відсутність автентифікації, шифрування та контролю цілісності даних. На практиці це означає, що якщо зловмисник відкриє будь-який зовнішній чи внутрішній зчитувач та фізично підключить зовнішній пристрій зчитування даних до кабелю, який йде на контролер — то він отримає всі дані зчитаних ідентифікаторів СКД, після чого зможе відкрити ці двері за допомогою зчитаних даних навіть з мобільного застосунку.

OSDP (Open Supervised Device Protocol) — це новий галузевий стандарт СКД підключення зчитувачів до контролерів, який забезпечує шифрування та автентифікацію. Він був створений в 2011 році Асоціацією індустрії безпеки (SIA) на заміну Wiegand. Усі ключові виробники СКД підтримують саме його.

У ті ж 80-ті роки багато компаній працювали над створенням бездротових стандартів та протоколів. Вклад у RFID-технології зробила швейцарська компанія EM Microelectronic зі штаб-квартирою у місті Марин. Вона вважається засновником формату пасивних, напівактивних та активних RFID-міток/карт EM Marin, які працюють на частоті 125 кГц. ***EM Marin*** — це найпопулярніший формат ідентифікаторів СКД.

Процес виробництва самих ідентифікаторів EM Marin був розділений: великі високотехнологічні компанії випускали чіпи (оригінальний мав назву EM4100), інші численні виробники купували чіпи та виготовляли готові ідентифікатори (картки чи брелоки), саме тому вартість ідентифікаторів EM Marin низька. Картки/брелоки EM Marin за замовчуванням є пасивними, і це обумовлює невеликий радіус їх використання: максимум до 10 см. Користувачі карток EM Marin часто фізично прикладають їх до зчитувача, інакше вони не спрацювують (особливо на турнікетах). Товсті пасивні картки EM Marin мають трошки більший радіус дії — до 15 см. Для контрольованого проїзду транспорту використовували зчитувачі великого розміру та активні картки EM Marin (всередині картки була літієва батарейка, яка забезпечувала живлення чіпу), які забезпечували збільшену дальність передачі коду від 50 см до 2 метрів.

Нагадаємо, що ідентифікатори працюють в парі зі зчитувачами, тож ідентифікатори формату EM Marin розуміють зчитувачі формату EM Marin, яких на ринку сотні. З-поміж усіх різноманітних виробників карт та зчитувачів EM Marin, які були присутні на українському ринку з 2000-х років, для важливих об'єктів обирали американську компанію HID Global. HID пропонував професійні зчитувачі серії Prox, тонкі картки ISO Prox II та товсті Prox Card II, мітки Prox Tag, брелоки ProxKey та активні мітки для автомобілів. Серед українських виробників зчитувачів СКД лідерську позицію тримала компанія Integrated Technical Vision Ltd (будь ласка, не плутайте з російською ITV, яка займається відеоспостереженням) — зараз вона працює під брендом U-Prox.

Але, окрім широких можливостей, формат EM Marin мав обмеження на кількість номерів карт, що призводило до того, що номери карт/брелоків у світі періодично повторюються. **Критичною проблемою формату EM Marin є незахищеність від копіювання.** На товстих картках EM Marin номер, який передається в СКД під час зчитування, нанесений прямо на корпусі. Достатньо просто сфотографувати карту, щоб зробити її клон і отримати всі права доступу. Для того, щоб скопіювати тонку картку, достатньо мати відповідний програматор (є у кожного інсталятора домофонів) та пусту картку. Квартирні грабіжники, на жаль, так і роблять: достатньо проїхати з вами впритул у транспорті/попити поруч каву та відстежити ваш будинок, і у зловмисників вже є копія брелока від вашого багатоквартирного домофону.

Проблему легкого клонування ідентифікаторів EM Marin вирішив новий формат ***MIFARE***, який у 1994 році створила австрійська компанія Mikron (Mifare= MIkron FARE Collection System) на базі стандарту ISO/IEC 14443 Type-A з частотою в 13,56 МГц. Сьогодні MIFARE — це торгова марка, якою володіє нідерландська компанія NXP Semiconductors. Замовникам та інтеграторам буде корисним дізнатися більше про MIFARE на їхньому сайті *www.mifare.net*, адже це найпопулярніший стандарт RFID у світі.

Переваги ідентифікаторів MIFARE — наявність внутрішньої енергонезалежної пам'яті, можливість перезапису інформації та криптозахист. Першим поколінням були картки сімейства ***MIFARE Classic***: Mifare Classic 1k та Mifare Classic 4k. Їхній криптозахист виявився недосконалим, і були факти задокументованої компрометації карт, тому сімейства Mifare Plus посилили криптозахистом стандарту AES. Функціонал зробив MIFARE привабливим не лише в СКД, а і в мікроплатіжних системах. І це навіть створило нові послуги та покращило індустрію розваг та відпочинку, наприклад:

- вологостійкі браслети MIFARE дозволяють відкривати персональні шафи у фітнес-клубі чи аквапарках та «сплачувати» товари з браслета;
- пластикові ski passes з MIFARE дозволяють користуватися послугами гірськолижних курортів;
- паперові носії з MIFARE використовуються як квитки на концерти;
- пластикові картки лояльності з MIFARE дозволяють накопичувати бонуси;
- паперові чи пластикові теги (мітки) з MIFARE використовують для сплати за проїзд по платних дорогах, для оплати паркінгу тощо.

Існують ще сімейства ідентифікаторів MIFARE Ultralight та SmartMX, але найбільш широке практичне визнання та втілення для проєктів ***Smart Cities*** отримало сімейство ***MIFARE DESFire*** з криптозахистом на базі стандартів AES/DES як засіб для оплати проїзду у громадському транспорту у деяких великих містах, наприклад у Лондоні.

Карти формату MIFARE ще називають smart cards, тому що сімейства карт MIFARE можуть взаємодіяти з технологією NFC (мобільні телефони, смарт-годинники, тощо). Саме цю ідею підхопила компанія HID Global, яка в 2014 році створила та вивела на ринок технологію мобільного доступу (HID Mobile Access), і авторизовані користувачі могли використовувати свої мобільні телефони як картку СКД. Функція Tap (прикладання мобільного телефона) була створена для зручного проходу людини, а функція Twist and Go (повернути телефон перед зчитувачем) була зручною для парковок, шлагбаумів, воріт тощо. За даними HID, завдяки цій технології деякі великі компанії повністю позбулися пластикових карт і при цьому зберегли високий рівень безпеки та повне і швидке керування правами доступу. Наразі технологію мобільного доступу пропонують все більше виробників СКД.

Архітектура СКД та (улюблена замовниками) інтеграція з СВН

СКД — це дуже фізична система і для замовників вона завжди вартувала кілометри кабелів, а інтегратори мали складне підключення кабелів та шлейфів (інженери використовували сленг «розключка»). Класичною архітектурою СКД була ієрархічна централізована архітектура на базі інтерфейсу RS-485. З розвитком мікроелектроніки та мережевих технологій контролери нового покоління стали мережевими пристроями з форм-факторами для встановлення на DIN-рейки, а системи — розподіленими (**рис. 6**).

Мережеві контролери стали більш «самостійними» та почали зберігати на борту досить велику базу даних. Кожен з них здатен взяти на себе роль майстера-контролера. Також контролери можуть комунікувати один з одним без участі сервера СКД, а програмування здійснюється з web-інтерфейсу контролера, що дуже зручно для пусконалагодження. Це дійсно класний функціонал для невеликих та середніх систем.

Всім відомо, що замовник може обрати контролери одного виробника, а зчитувачі іншого, і все буде працювати, якщо їхні формати сумісні: Wiegand-зчитувачі з Wiegand-контролерами чи OSDP-зчитувачі з OSDP-контролерами. Але для того, щоб ваша система не була просто системою з «пікалками», треба спочатку визначати/обирати її функції. За функції СКД відповідає програмне забезпечення СКД (новий термін access control management software), яке керує контролерами. Тож ПЗ СКД та контролери мають бути повністю сумісними. Саме тому побудова СКД великих та критично важливих об'єктів потребує наступного підходу:

- аналіз необхідних функцій ПЗ СКД, потенційних загроз, зручності користування та обслуговування;
- вибір стандарту ідентифікаторів як рівня безпеки (EM Marin, MIFARE, тощо);
- аналіз потенційних вендорів-виробників СКД під задачі об'єкта;
- вибір вендора ПЗ СКД та контролерів;
- вибір вендора зчитувачів та ідентифікаторів;
- вибір вендорів виконавчих елементів (турнікетів, шлагбаумів, замків тощо);
- вибір вендорів аксесуарів (кнопки виходу, довідники, тощо);
- проєктування системи для визначення оптимальної архітектури, кількості обладнання та специфікації;
- бюджетування запроєктованої СКД;
- тендер та реалізація.

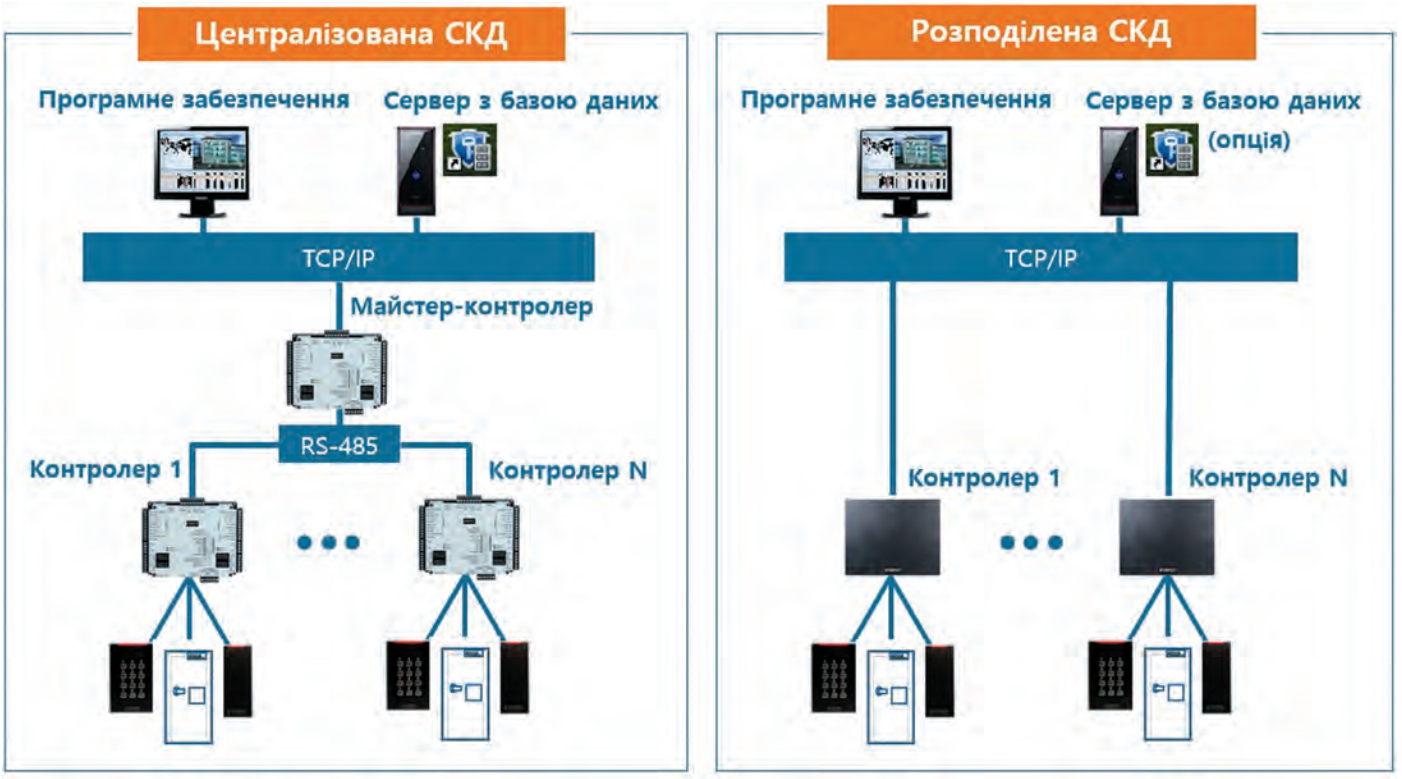

Рис. 6. Архітектура СКД

Не можна будувати СКД як завгодно на бюджетних рішеннях, а потім вимагати від інтегратора «додати» в існуючу СКД функції типу обліку робочого часу, бюро перепусток, обходу території охоронцем (guard tour), заборони повторного проходу (antipassback) тощо. Так не працює.

Аналогічно не можна будувати будь-яку СВН на якихось камерах та NVR, купити якусь СКД, а потім поставити задачу інтегратору «Ми хочемо отримати інтегровану систему безпеки». Інтегратор може зробити інтеграцію, але для цього треба розібратися з протоколами виробників СВН та СКД, зрозуміти, чи можливий обмін даними та як саме це зробити, написати окреме програмне забезпечення. Але до цього зазвичай не доходить, бо замовник не хоче інвестувати додаткові гроші у те, що має. На цьому, як кажуть програмісти, «вихід із циклу»: інтегратор змарнував свій час, а замовник зіпсував собі настрій.

Якщо замовник хоче отримати дійсно інтегровану систему безпеки, у нього є два конструктивні шляхи (**рис. 7**):

- обрати одного вендора СВН, який має в портфелі також СКД і пропонує закінчене, повністю готове, інтегроване рішення;
- обрати спочатку програмну платформу для ІСБ (зазвичай це VMS-системи), подивитися, які виробники СКД вже інтегровані та як саме; або обрати вендора СКД, який має можливості для інтеграції і закласти бюджет на саму інтеграцію.

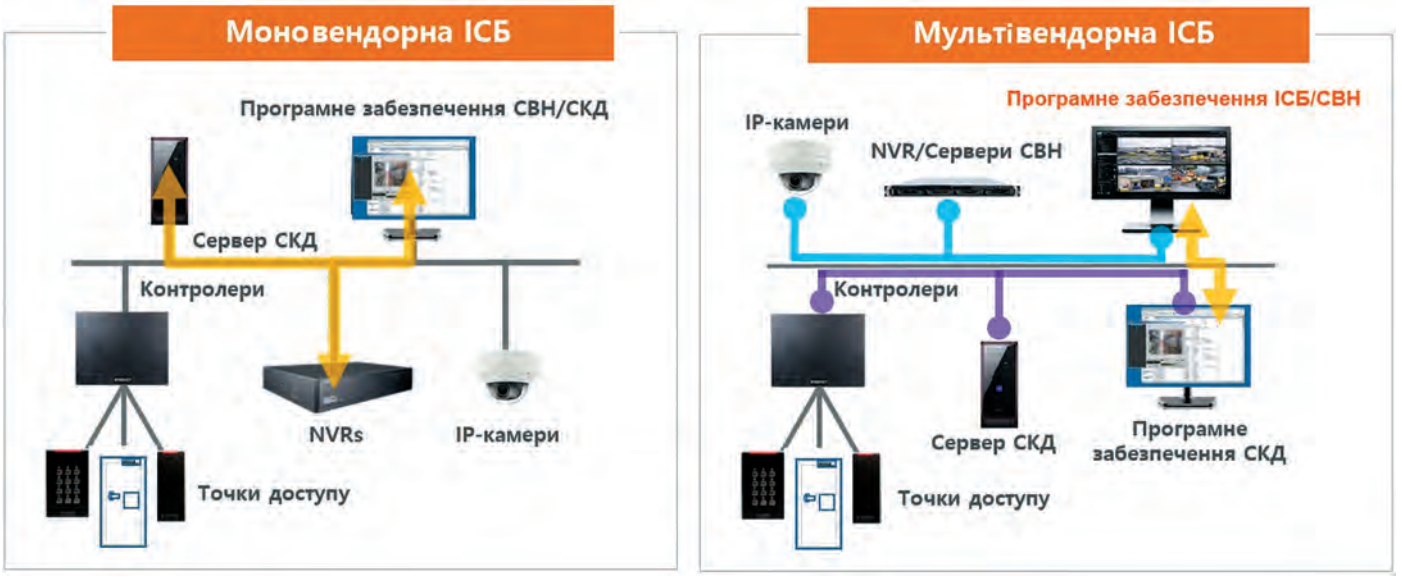

Рис. 7. Інтегровані системи безпеки (ІСБ)

В моновендорному рішенні зазвичай все зручно та прекрасно (один виробник, повна сумісність, один дистриб'ютор, спеціальні проєктні умови тощо), окрім можливого обмеження щодо функцій. Треба чітко усвідомити, що СКД для виробників СВН — це маркетинговий додаток для збільшення портфелю проєктів і продажів, зазвичай навіть не свій, а якийсь OEM. Тому не буде виробник СВН вкладати кошти та час, щоб додавати функції у продану вам СКД. Прошивки на камерах буде оновлювати, а СКД майже ні.

Мультивендорні рішення з професійними СКД дадуть замовнику все, що він забажає, але треба інвестувати час у аналіз, проєктування та більший бюджет. На великих і відповідальних проєктах — воно того варте.

Гравці світового та українського ринку СКД

Це найскладніше питання, адже не існує єдиного джерела статистики щодо виробників СКД. В деяких рейтингах виробники СКД потрапляють у розділ програмного забезпечення, а деякі виробники є у складі рейтингів виробників замків.

Апроксимовано світова картина СКД виглядає так: перше місце за обсягами продажів посідає шведська група компаній Assa Abloy, до складу якої входять відомий всім HID Global, вищезгаданий VingCard, добре відомий українському ринку виробник електромеханічних замків Effeff, виробники замків Mottura та Mul-t-lock і ще десятки інших компаній. Помітними та традиційними гравцями світового ринку виробників СКД є Honeywell Security (США), Johnson Controls (Ірландія), Dormakaba (Швейцарія), Nedap (Нідерланди), Bosch (Німеччина). Відносно новими гравцями СКД є майже всі вендори відеоспостереження, які додали СКД у свій портфель в останні 5–7 років: Axis Comminications (Швеція), Avigilon (Канада), Hanwha Vision (Корея) та інші. В мережевих зіркових готелях в бренд-буках присутні VingCard, Onity та Salto (Іспанія). Серед виробників надійних турнікетів користуються повагою Kaba (Швейцарія) та Gunnebo (Швеція). Серед виробників шлагбаумів виділяються Automatic Systems (Бельгія), CAME (Італія) та інші.

З 2015 року на ринок систем контролю доступу досить агресивно вийшли багаточисленні китайські виробники: Hikvision, Dahua, ZKTeco та інші. Щойно вони привчили замовників купувати дешеві системи відеоспостереження з кібервразливостями, схоже, настав час українським компаніям швидко та безпроблемно для хакерів «ділитися» базами даних користувачів та їхніми персональними даними.

Досить популярними були та залишаються українські виробники СКД: вищезгаданий U-Prox, Stop-Net (Card Systems) та продукція (переважно турнікети) компанії TISO.

Український ринок традиційно дуже цікавив російських виробників СКД, варто їх пам'ятати та оминати: Bolid, PERCo, Parsec, IronLogic, RusGuard, SIGUR, APACS 3000, Gate. Оскільки вони суто російські, а всі російські розробники є абсолютно підконтрольними силовим структурам, то порада українським замовникам – міняти системи якомога швидше, щоб запобігти витоку даних.

Оскільки, окрім компанії Bosch, в Україні немає представництв потужних гравців СКД, на українському ринку часто ставали популярними та відомими бренди, якими активно займалися дистриб'ютори: Apollo (США), Inner Range (Австралія), Suprema (Корея) та інші.

Обирати за ціною та дизайном можна тільки самі зчитувачі та ідентифікатори СКД, а справжню цінність системи можна отримати лише обравши корисні функції та можливості. Тому кожну СКД перед покупкою обов'язково треба перевіряти на пілотному проєкті за допомогою відповідних звітів. Для існуючих систем буде дуже корисним проведення відповідного аудиту.

Тенденції СКД

Кардинальні зміни у галузі контролю доступу почалися з появою OSDP-протоколу, адже він забезпечує контроль за цілісністю даних. Мережеві контролери, по суті, стали мережевими IoT-пристроями, а безпечний зв'язок між контролером та зчитувачами по OSDP може означати, що зчитувачі також стануть з часом мережевими чи навіть бездротовими. Всього п'ять років тому ідея бездротової охоронної сигналізації викликала у фахівців посмішку, а сьогодні українська компанія Ajax є новою зіркою бездротових охоронних систем не лише в Україні. Отже цілком логічно, що безпечні технології передачі даних рано чи пізно замінять кілометри кабелів для СКД.

Ключовою тенденцією світового ринку СКД є пропозиція виробників щодо cloud-based СКД. І це відверто поки що про маркетинг. Адже контролери, турнікети, ліфти та шлагбауми поки що фізичні, і в хмару їх не перенесеш. Максимум, що можна зберігати в хмарі (велике питання — в якій, і це точно не повинна були публічна хмара), — це базу даних з серверу контролю доступу чи резервні бази даних мережевих контролерів. Досвід роботи державних структур та різних бізнесів в екстремальних умовах 2022—2023 років спонукав українських IT-фахівців вирішувати ці питання комплексно, а не лише для СКД.

Нові вимоги безпеки та дистанції між людьми через пандемію коронавірусу дав більше місця біометричним технологіям та технологіям мобільного доступу на основі Bluetooth та NFC, які вже змінили досвід багатьох користувачів та замовників СКД.

Оскільки українські фахівці компетентні у використанні мікропроцесорної техніки та контролерів, а також у створенні якісного програмного забезпечення та інтеграцій, хотілося б бачити більш активний розвиток галузі систем контролю доступу саме українських виробників. Сподіваємося, що так воно і буде і через декілька років вийде нова стаття з оглядом нових українських технологій та брендів, які підкорили світ.

Альона ШВЕЦОВА,
незалежний експерт з систем безпеки, cctvmadonna