Кайдик О. Л., Терлецький Т. В., Угрин Д. І., Кондіус І. С.

СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Кайдик О. Л., Терлецький Т. В., Угрин Д. І, Кондіус І. С.

СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

НАВЧАЛЬНИЙ ПОСІБНИК

Луцьк – 2026

УДК 681.52:004.056
С34

Рекомендовано до друку рішенням кафедри комп'ютерної інженеріх та охоронних систем (протокол № __ від __ травня 2026 р.) та Вченою радою Луцького національного технічного університету (протокол № __ від __ травня 2026 р.)

Авторський колектив:

Кайдик Олег Леонтійович – кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки Луцький національний технічний університет.

Терлецький Тарас Володимирович – кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки Луцький національний технічний університет.

Угрн Дмитро Ілліч – доктор технічних наук, професор кафедри комп'ютерної інженерії Чернівецького національного університету імені Юрія Федьковича.

Кондіус Інна Степанівна – кандидат економічних наук, доцент кафедри кафедри комп'ютерної інженерії та безпеки Луцький національний технічний університет.

Рецензенти:

Грабовський Олег Вікторович – кандидат технічних наук, доцент, декан факультету метрології, автоматизації та електроніки Державного університету інтелектуальних технологій і зв'язку (м. Одеса).

Вовна Олександр Володимирович – доктор технічних наук, професор, професор кафедри програмних систем і технологій Київського національного університету імені Тараса Шевченка (м. Київ).

Клеха Олександр Васильович – СЕО ТОВ «СП-Луцьк» (м. Луцьк).

С34 Кайдик О. Л., Терлецький Т. В., Угрин Д. І., Кондіус І. С. **Системи контрою та управління доступом** : навч. посіб. для студентів технічних спеціальностей. Луцьк : ЛНТУ, 2026. 240 с.

У навчальному підручнику викладено теоретичні та практичні основи функціонування сучасних систем керування контролем доступу. Видання охоплює повний спектр знань: від еволюції систем безпеки та нормативно-правової бази обробки персональних даних до складних математичних моделей топології зон доступу. Особливу увагу приділено фізиці процесів ідентифікації, аналізу мережевих протоколів та архітектурних рішень, включаючи хмарні сервіси та інтеграцію СКУД у загальні системи управління будівлями. Розглянуто інноваційні напрямки розвитку галузі та методологію управління ІТ-проєктами у сфері безпеки.

Підручник розрахований на здобувачів вищої освіти технічних спеціальностей та інженерів із проєктування систем безпеки, які прагнуть опанувати сучасний технологічний стек і методику практичної реалізації СКУД.

ЗМІСТ

ВСТУП

У сучасному світі, де межа між цифровим та фізичним просторами поступово зникає, безпека трансформується з простого замкнення дверей у складну інтелектуальну екосистему. Фундаментальну роль у цьому процесі відіграють системи контролю та управління доступом (СКУД). Насьогодні це не просто сукупність технічних засобів для блокування проходу, а комплексна платформа, яка об'єднує у собі методи прикладної фізики, математичне моделювання, цифрову ідентифікацію та стратегії управління ІТ-проєктами. Актуальність цього курсу зумовлена стрімкою еволюцією галузі: від класичних механічних бар'єрів до систем на базі Інтернету речей (IoT), біометрії та штучного інтелекту (ШІ).

Для глибокого розуміння принципів функціонування СКУД недостатньо лише знати специфікацію обладнання. Фахівець повинен розуміти топологію систем та володіти математичним апаратом для опису зон доступу й рівнів їх ієрархії. Графові моделі санкціонованих переходів – це фундамент для розроблення алгоритмів, які дозволяють мінімізувати логічні помилки та вразливості системи. Такий підхід перетворює фізичний об'єкт на чітко структуровану модель, де кожне переміщення суб'єкта є прогнозованим та верифікованим.

Технічна реалізація сучасних СКУД неможлива без глибокого знання інтерфейсів та мережевих протоколів. Аналіз вразливостей застарілих рішень на фоні переваг сучасних захищених протоколів, перехід до Ethernet-архітектур та впровадження технології Power over Ethernet (PoE) відкривають безпрецедентні можливості для масштабування систем у межах корпоративної мережевої інфраструктури.

Сучасний етап розвитку галузі нерозривно пов'язаний із впровадженням ШІ, що, окрім нових функцій, несе у собі й специфічні ризики кібератак. Саме тому проєктування СКУД сьогодні розглядається не просто як вузьке інженерне завдання, а як повноцінний ІТ-проєкт, що потребує комплексного підходу до захисту даних та системної стійкості.

Цей підручник покликаний сформувати у майбутніх фахівців системне інженерне мислення. Синергія глибоких технічних знань та управлінських компетенцій дозволить їм не лише впроваджувати готові рішення, а й створювати безпечне середовище, де технології працюють на благо суспільства, гарантуючи захищеність, приватність та ефективність бізнес-процесів. Отримані знання стануть надійним фундаментом для професійного розвитку в динамічній галузі технічних засобів безпеки та системного інтегрування.

РОЗДІЛ 1. Концептуальні основи та нормативна база

1.1 Еволюція систем безпеки: від механіки до IoT

Прагнення до безпеки є одним із найдавніших і найбільш фундаментальних інстинктів людства, що пройшов шлях від біологічного виживання до складних технологічних екосистем. У найдавніші часи концепція захисту базувалася виключно на фізичному просторі та використанні ландшафту. Первісні громади обирали для поселення печери, скелясті виступи або густі лісові масиви, які створювали природні перешкоди для хижаків та ворожих племен. Такий підхід до безпеки був суто пасивним і залежав від географічної удачі.

З настанням аграрної революції, коли люди почали накопичувати ресурси та осідати на постійних місцях, виникла потреба в активному перетворенні середовища. Поселення почали обносити дерев'яними частоколами, а згодом – масивними кам'яними мурами. Безпека в цей період стала синонімом фортифікації.

Проте справжня еволюція систем безпеки почалася тоді, коли людина винайшла спосіб індивідуалізації доступу до майна. Перші механічні засоби захисту – замки – з'явилися приблизно 4000-6000 років тому в Месопотамії та Стародавньому Єгипті [38]. Ці примітивні пристрої були виготовлені з дерева і працювали за принципом штифтового засува (рис. 1.1). Конструкція складалася з дерев'яного поста, закріпленого на дверях, і горизонтального засува, який входив у цей пост. Всередині були вільні штифти, які опускалися під власною вагою і блокували засув. Щоб відімкнути двері, використовувався великий дерев'яний ключ із виступами, які піднімали штифти на потрібну висоту, звільняючи шлях для руху засува. Незважаючи на свою простоту та громіздкість, цей винахід заклав основу для всіх майбутніх штифтових механізмів, які ми використовуємо до сьогодні.

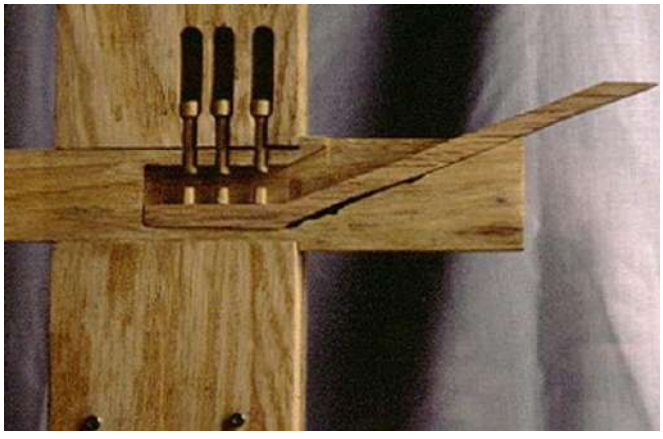


Рисунок 1.1 – Давній єгипетський замок [51]

Римляни зробили наступний крок, замінивши дерево металом – переважно залізом для замків і бронзою для ключів. Це дозволило зменшити розміри пристроїв і підвищити їхню стійкість до злому. Римські інженери винайшли «захищені» замки, у яких всередині знаходилися фігурні перешкоди. Ключ повинен був мати відповідні прорізи, щоб обійти ці перешкоди та повернути засув. Це зробило замок не лише засобом захисту, а й символом статусу – заможні римляни носили ключі як перстні на пальцях, демонструючи оточуючим свою владу та наявність цінностей, які варто охороняти. У Середньовіччі ковальство стало мистецтвом, і замки перетворилися на складні витвори з безліччю прихованих механізмів, але фундаментальний принцип захисту залишався незмінним протягом тисячоліть.

XVIII та XIX століття стали періодом радикальних змін у розвитку безпекових систем, спричинених швидкою урбанізацією та необхідністю захисту фабричних ресурсів. У 1778 році Роберт Баррон запатентував важільний замок подвійної дії, а у 1784 році Джозеф Брама створив замок з надзвичайно високим рівнем секретності, який залишався незламним понад 60 років, поки його не відкрив американець Альфред Гоббс під час виставки у Лондоні.

Проте справжній тріумф сучасної механічної безпеки відбувся в США. Лінус Єйл-старший у 1848 році, натхненний давньоєгипетськими кресленнями, запатентував штифтовий замок, а його син, Лінус Єйл-молодший, у 1861 році вдосконалив конструкцію, створивши сучасний циліндровий замок з пласким ключем із зубцями. Ця розробка стала промисловим стандартом завдяки зручності, надійності та можливості масового виробництва. Промислова революція також принесла перші комбіновані (кодові) замки, що усували потребу у фізичному ключі, та перші механічні засоби сповіщення, такі як «Ross' Patent Mechanical Burglar and Fire Alarm» 1872 року, який працював на основі натягу дротів.

До середини XIX століття людство все ще покладалося на механічні перепони та звукові сигнали тварин – гусей, собак або встановлених біля входу дзвонів. Справжній технологічний розрив стався 21 червня 1853 року, коли Огастус Рассел Поуп, винахідник із Сомервіля, штат Массачусетс, запатентував першу в світі електромагнітну систему сигналізації [52].

Пристрій Поупа був революційним у своєму мінімалізмі та ефективності. Він використовував паралельне електричне коло, підключене до дверей та вікон. При несанкціонованому відкритті коло замикалося, і електричний струм змушував вібрувати електромагніт, який приводив у дію молоточок, що бив по латунному дзвону. Унікальною особливістю системи було те, що тривожний дзвін не припинявся, навіть якщо зловмисник швидко зачиняв вікно або двері

назад. Попри геніальність винаходу, Поуп не зміг його масштабувати, і у 1857 році продав патент Едвіну Холмсу.

Холмс виявився майстерним бізнесменом. Розуміючи, що в Бостоні злочинність була низькою, він переніс компанію до Нью-Йорка – міста, де, за його словами, «мешкали всі зломщики країни». Щоб подолати страх і скептицизм людей перед електрикою, Холмс використовував агресивний маркетинг. Він публікував у пресі списки відомих клієнтів, які вже встановили його систему, перетворюючи безпеку на престижний продукт. У 1877 році його син, Едвін Т. Холмс, створив першу мережу сигналізацій, підключених до центральної станції моніторингу, використавши для цього нічні телефонні лінії, які вдень служили для звичайного зв'язку [54]. Ця колаборація з Александром Гемом Беллом заклала фундамент для всієї індустрії віддаленого охоронного моніторингу.

Паралельно з Холмсом, у 1875 році Едвард Калаган розробив систему «викличних коробок», яка дозволяла власникам будинків викликати допомогу, надсилаючи сигнал до центрального пункту, розділеного на дистрикти [55]. У разі тривоги з центру виїжджав кур'єр, щоб перевірити ситуацію. Це була перша ітерація послуг фізичного реагування на сигнали тривоги. На початку XX століття системи безпеки продовжували розвиватися – після Першої світової війни з'явилася практика залучення людей, які за плату проходили вулицями вночі та перевіряли, чи зачинені двері будинків клієнтів. Проте справжній технологічний стрибок відбувся після Другої світової війни.

Контроль доступу є однією з найбільш динамічних галузей безпеки. Якщо протягом тисячоліть основою був фізичний ключ, то за останні 50 років ця сфера пройшла три фундаментальні трансформації [50].

У 1970-х та 1980-х роках домінуючою технологією стали карти з магнітною смугою. Вони дозволили організаціям відмовитися від громіздких зв'язок ключів і впровадити базовий аудит подій – тепер можна було знати, хто і коли увійшов у приміщення. Проте дані на смузі були статичними та незашифрованими, що робило їх легкими для клонування за допомогою дешевих пристроїв.

На зміну їм у 1990-х прийшли проксі-карти, що використовували RFID-технологію. Це був перший крок до безконтактності: карту достатньо було піднести до зчитувача на відстань кількох сантиметрів. Це зменшило зношення обладнання, але безпека залишалася вразливою через відсутність шифрування сигналу. Лише у 2000-х з'явилися смарт-карти другого покоління (наприклад, MIFARE, iCLASS), які запровадили взаємну автентифікацію між картою та зчитувачем, де кожен сеанс зв'язку був унікальним і зашифрованим.

Сьогодні ми переживаємо етап «Mobile First». Смартфон витісняє пластикові картки завдяки технологіям Bluetooth Low Energy (BLE) та NFC. Мобільні облікові дані надають переваги, які раніше були неможливими:

– двофакторна автентифікація (для відкриття дверей потрібно не лише мати телефон, а й розблокувати його за допомогою біометрії типу FaceID або відбиток пальця);

– дистанційне керування (адміністратор надісилає «ключ» через хмару новому співробітнику або гостю за секунду, а також миттєво відкликає його);

– екологічність (відмова від мільйонів пластикових карток позитивно впливає на довкілля).

Поняття Інтернету речей (IoT – Internet of Things) почало формуватися ще у 1980-х роках, коли студенти Університету Карнегі-Меллон підключили автомат із Coca-Cola до мережі, щоб дистанційно перевіряти наявність та температуру напоїв. Проте як самостійна ідея безпеки IoT оформився лише у 2008-2009 роках, коли кількість підключених пристроїв перевищила чисельність населення планети.

У сучасній архітектурі безпеки IoT виконує роль нервової системи. Замість ізольованих систем ми маємо «Security as a Utility» – інтегроване середовище, де камери, замки, датчики якості повітря та системи освітлення спілкуються між собою через хмару. Це дозволяє реалізувати складні сценарії автоматизації, наприклад, при виявленні витоку газу система не лише вмикає сирену, а й автоматично розблоковує двері для евакуації, вмикає вентиляцію та надсилає відео з місця події на смартфон власника.

Проте масове підключення пристроїв створило нові вектори загроз. Історія ботнету Mirai 2016 року стала суворим нагадуванням про вразливість IoT. Зловмисники використали мільйони веб-камер та роутерів із заводськими паролями для створення армії «зомбі-пристроїв». Цей ботнет здійснив DDoS-атаку потужністю 1 Тбіт/с на сервіс Dyn, що призвело до відключення Twitter, Netflix та Reddit по всьому світу. Це спричинило зміну підходу до розробки пристроїв – тепер безпека закладається на етапі проектування, включаючи обов’язкову зміну паролів та шифрування трафіку.

Якщо IoT – це нервова система, то Штучний інтелект (ШІ) – мозок сучасної безпеки. Традиційні системи були реактивними. Вони спрацьовували за фактом події. Системи на базі ШІ стають предиктивними (прогностичними).

Сучасна відеоаналітика більше не потребує оператора, який втомлюється через 20 хвилин спостереження за моніторами. Алгоритми глибокого навчання здатні самостійно класифікувати об’єкти. Наприклад, система може ігнорувати рух гілок дерев або собак, але миттєво зреагувати на появу людини в забороненій зоні. Більше того, з’явився концепт «Адаптивного ШІ», який

вивчає норми поведінки для конкретного об’єкта. Якщо вантажівка розвантажується о 10:00 ранку – це норма; якщо та сама вантажівка з’являється о 02:00 ночі – система розцінює це як аномалію.

Окремим фронтом розвитку є біометрія. У 2025 році акцент змістився з контактних методів на пасивні, зокрема аналіз ходи. Кожна людина має унікальний динамічний профіль руху, який надзвичайно важко підробити або приховати, навіть якщо обличчя закрите маскою або окулярами. Системи розпізнавання ходи можуть ідентифікувати підозрілу особу на відстані до 100 метрів за допомогою звичайних камер спостереження, що робить їх незамінними у боротьбі з тероризмом та серійними злочинами.

Сучасна індустрія відходить від ізольованих рішень (VMS, Access Control) до інтегрованих платформ управління інформацією – PSIM (Physical Security Information Management) та CSIM (Converged Security and Information Management). Ці системи об’єднують дані не лише від камер та замків, а й із соціальних мереж, метеорологічних служб та IT-інфраструктури. Це створює «цифровий двійник» об’єкта, де оператор бачить ситуацію в 3D-просторі в реальному часі.

Головним трендом наступного десятиліття стане поглиблення конвергенції фізичної та кібербезпеки. Вже сьогодні неможливо гарантувати фізичну безпеку банку, якщо його камери спостереження вразливі для хакерів. Концепція Zero Trust (нульової довіри) поступово переходить із корпоративних мереж у сферу фізичної безпеки, де кожен пристрій повинен постійно підтверджувати свою автентичність, а права доступу надаються лише на мінімально необхідному рівні.

Пройдена еволюція систем безпеки від дерев’яних засувів Стародавнього Єгипту до автономних дронів із ШІ-аналітикою демонструє не лише технологічний прогрес, а й зміну філософії захисту. Ми перейшли від пасивних бар’єрів до активних сигналізацій, а тепер – до інтелектуальних систем, які здатні передбачати загрози до їх виникнення. Безпека майбутнього – це не високий паркан, а невидима, але всюдисуща мережа інтелектуальних сенсорів, що забезпечує захист, не заважаючи життю та роботі людини. Ключовим викликом у цій новій реальності залишатиметься баланс між тотальним спостереженням заради безпеки та збереженням приватності особистості.

1.2 Термінологія СКУД

Процес формування єдиного термінологічного та нормативного простору в галузі електронних систем контролювання доступу пройшов тривалий шлях від локальних відомчих інструкцій до глобальних міжнародних стандартів. В основі сучасної української нормативної бази лежить принцип гармонізації з

європейськими (EN) та міжнародними (IEC) стандартами, що забезпечує високу якість безпекових рішень та їхню сумісність на технічному рівні. Ключовим документом у цій сфері є ДСТУ EN 60839-11-1:2014 «Системи тривожної сигналізації та електронні системи безпеки. Частина 11-1. Електронні системи контролювання доступу. Вимоги до системи та її складників» [97], який є ідентичним перекладом європейського стандарту EN 60839-11-1:2013.

Перехід від попереднього покоління стандартів, зокрема серії EN 50133 [92], до нової лінійки IEC/EN 60839 став відповіддю на стрімкий розвиток інформаційних технологій та цифровізацію фізичної безпеки. Старий стандарт EN 50133-1:1996, який тривалий час був базовим для європейського ринку, поступово втратив актуальність через обмеженість у питаннях мережевої безпеки, біометрії та інтеграції з іншими системами управління будівлями. Нова редакція 60839-11-1 запровадила більш гнучку класифікацію систем, деталізувала вимоги до компонентів та розширила термінологічну базу, що дозволило фахівцям оперувати універсальними поняттями незалежно від країни виробника обладнання.

На сьогодні цей стандарт є чинним і обов’язковим для використання під час проектування систем безпеки на об’єктах державної власності та критичної інфраструктури, а також стає де-факто стандартом для приватного сектору.

Сучасна структура стандартів серії 60839 охоплює широкий спектр аспектів функціонування СКУД – від загальних вимог до системи та її компонентів (Частина 11-1) до настанов з експлуатації (Частина 11-2 [98]) та специфічних протоколів взаємодії, таких як OSDP (Частина 11-5 [26]) або веб-сервіси (Частини 11-31 [99], 11-32 [104], 11-33 [103]). Така диференціація дозволяє створювати складні ієрархічні системи, що поєднують у собі надійність фізичних бар’єрів та гнучкість хмарних технологій управління.

Термінологічна точність є основою будь-якої інженерної дисципліни. У сфері СКУД неправильне тлумачення понять може призвести до серйозних помилок при виборі обладнання або налаштуванні логіки доступу. Стандарт ДСТУ EN 60839-11-1 у розділі 3 фіксує визначення, які є обов’язковими для професійної комунікації.

В загальному випадку, СКУД являє собою елемент або підсистему безпеки об’єкта й сама виконує додаткові функції із забезпечення безпеки. В роботі СКУД приймає участь, перш за все, об’єкт чи/або суб’єкт, який претендує на право доступу до ресурсів, які розташовано у певній зоні.

Із загальної точки зору суб’єкт виступає у якості конкретної особи (зазвичай людини), як носія будь-яких властивостей. Щодо об’єкта, то це філософська категорія, яка виражає те, що протидіє суб’єкту по відношенню до його діяльності.

На практиці об’єкту або суб’єкту необхідно отримати чи/або надати доступ до певної, контрольованої, зони. Доступ – переміщення суб’єкта чи/або об’єкта в деякій зоні для отримання можливості взаємодії з певним матеріальним або інформаційним ресурсом.

Суб’єкт доступу (СД) або об’єкт доступу (ОД) – особа (жива істота), предмет або фізичний процес, які претендують на право доступу до контрольованої зони.

Центральним поняттям архітектури системи є «Точка доступу» (Access Point). Згідно з визначенням, це сукупність обладнання, розташованого біля входу або виходу, де здійснюється контроль доступу. Важливо розуміти, що точка доступу – це не лише фізичний отвір у стіні, а складний функціональний вузол, що включає перепону (двері, турнікет, шлагбаум), зчитувач, виконавчий пристрій (замок чи привід), датчик стану перепони та засоби оповіщення. Кожен із цих елементів взаємодіє з інтерфейсом точки доступу (контролером), який приймає рішення на основі отриманих даних.

Зона – це ділянка контрольованого об’єкта (територія контрольованого об’єкта або його частина; приміщення або група приміщень в контрольованій будівлі; доступні для використання канали зв’язку, зони на носіях інформації або самі носії тощо).

Зазвичай доступ суб’єкта чи/або об’єкта контролюється й управляється СКУД. Для вирішення завдань пов’язаних із контролем та управлінням доступу система виконує ряд певних процедур.

Контроль та управління доступом (КУД) – ідентифікація, автентифікація, контроль санкціонованості й управління доступом до контрольованої зони.

Розуміння різниці між ідентифікацією, автентифікацією та авторизацією є важливим для проектування систем з високим рівнем безпеки.

Ідентифікація – це процедура розпізнавання суб’єкта/об’єкта за властивими лише йому або деяким носіям ідентифікаційним ознакам.

Автентифікація – це процедура перевірки права власності на володіння суб’єктом/об’єктом наданої ним ідентифікаційної ознаки (ІО), яка збережена/відтворена на відповідному носії або ідентифікаторі.

Авторизація – визначення того, куди особі дозволено зайти і в який час.

Верифікація – порівняння ідентичності двох різних суб’єктів доступу.

Процедура ідентифікації, як правило, складається із наступних етапів:

– виявлення та зчитування ідентифікаційної ознаки;

– порівняння виявленої ідентифікаційної ознаки з еталонними ознаками, які розміщено у базі даних;

– прийняття рішення про права доступу.

Для того щоб у точці доступу можна було розпізнати та ідентифікувати СД, останній повинен володіти рядом ідентифікаційних ознак.

Ідентифікаційний ознака – набір характеристик та параметрів, які містять інформацію, яка є достатню для вирішення завдань із ідентифікації та автентифікації.

Наступним важливим терміном є «Ідентифікатор» (Credential). Стандарт визначає його як дані, що зберігаються фізично або віртуально, або фізичну характеристику особи, які використовуються системою для ідентифікації чи автентифікації. Це широке визначення охоплює всі можливі носії інформації – від класичних RFID-карток до мобільних NFC-токенів та біометричних шаблонів. Класифікація ідентифікаторів базується на трьох принципах: «те, що особа має», «те, що особа знає» та «те, чим особа є».

Таким чином, ідентифікатор – носій ідентифікаційної ознаки. На практиці це може бути як суб’єкт, так і об’єкт, визначені характеристики/параметри якого є його характерними ознаками, за якими й здійснюється ідентифікація або автентифікація.

Зазначимо, що ідентифікатором (носієм ідентифікаційних ознак) може виступати як сам СД чи ОД, так і спеціальний предмет, на якому тим або іншим чином нанесено чи/або відтворено ідентифікаційні ознаки (рис. 1.2).

Рисунок 1.2 – Ідентифікатори

Дійсний (недійсний) ідентифікатор – ідентифікатор із наявною ІО, який допускає (не допускає) переміщення СД через визначену точку доступу (ТД) у певний часовий і календарний періоди.

Як уже було зазначено ідентифікатором може бути як сам суб’єкт/об’єкт доступу, так і окремі додаткові предмети (наприклад, людина ідентифікує себе

за відбитком пальця, тобто, вона сама є носієм ІО, або ж вона володіє деяким предметом на який нанесено ідентифікаційні ознаки).

Система контролю та управління доступом являє собою сукупність методів і засобів контролю й управління доступом, які функціонують та взаємодіють за певними правилами. Іншими словами, це сукупність всіх технічних, програмних, організаційних та інших методів і засобів, які необхідні для виконання завдання контролю й управління доступом суб'єкта чи/або об'єкта до визначеної зони.

Контрольовані зони доступ, зазвичай, володіють різними властивостями, які напряму пов'язані із застосуванням процедур КУД, характером функціонування системи та можливістю доступу того чи іншого суб'єкта чи/або об'єкта.

Зона контрольованого доступу (ЗКД) – зона, доступ до якої контролюється СКУД.

Зона санкціонованого (дозволеного) доступу (ЗСД) – зона, доступ до якої суб'єкту чи/або об'єкту дозволено тільки у встановлені часові та календарні інтервали. Термін «зона санкціонованого доступу» можна застосовувати лише для конкретного суб'єкта/об'єкту доступу.

Щодо зони несанкціонованого (недозволеного) доступу (ЗНД), то вона являє собою таку зону доступ до якої встановленому суб'єкту чи/або об'єкту заборонений у заздалегідь встановлений часові та календарні інтервали (наприклад, доступ до суб'єкта/об'єкта до приміщення в неробочий час або у вихідні чи святкові дні; одна і та ж зона може бути як ЗСД, так і ЗНД для кокретновзятого суб'єкта/об'єкта в залежності від часу і дати).

Окремим випадком ЗНД може бути зона недозволеного доступу, доступ об'єкта/суб'єкта до якої заборонено назавжди.

Зона вільного (неконтрольованого) доступу (ЗВД) – зона, доступ до якої не обмежується.

Зона обмеженого за часом доступу (ЗОЧД) – зона, доступ до якої обмежується тільки тимчасовими і календарними інтервалами (наприклад, доступ до торгових приміщень для покупців обмежено лише робочими годинами, у той час, коли для продавців такі тимчасові рамки розширено).

Зона обмеженого доступу об'єктів (ЗОДО) – зона, доступ до якої обмежують правилами заборони переміщення визначених об'єктів чи предметів (наприклад, доступ в торгові приміщення самообслуговування обмежено (заборонено) для покупців з великими сумками; доступ в літак заборонено пасажирам із зброєю або предметами, що становлять небезпеку для пасажирів).

Санкціонований (несанкціонований) доступ – доступ, який не порушує (порушує) правила управління доступом. Іншими словами доступ

окремовзятого суб’єкта/об’єкта до зони за наявності (відсутності) відповідного рівня доступу.

Розмежування доступу – дозвіл переміщення за одними маршрутами та заборона переміщення за іншими.

Однією з найбільш вагомих інновацій ДСТУ EN 60839-11-1 є впровадження ієрархічної системи оцінки захищеності СКУД, що поділяється на чотири рівні (Grade 1-4), які визначають можливість того або іншого суб’єкта/об’єкта переміщуватись через точки доступу (табл. 1.1). Ця класифікація дозволяє замовникам вибирати обладнання та архітектурні рішення, що відповідають реальним ризикам та профілю потенційного порушника.

Таблиця 1.1 – Характеристика рівнів доступу СКУД [23]

Рівень (Grade)	Профіль порушника	Основні технічні вимоги	Типове застосування
Grade 1	Випадковий порушник, мінімальні знання	Базова ідентифікація, відсутність вимог до шифрування зв’язку	Малі офіси, житлові будинки
Grade 2	Порушник з обмеженими знаннями та інструментами	Контроль розкриття корпусів (тампери), базовий моніторинг зв’язку	Роздрібна торгівля, комерційні об’єкти
Grade 3	Досвідчений порушник, знайомий з принципами роботи СКУД	Обов’язкове шифрування каналів, детекція спроб підбору паролів, висока надійність	Банки, великі промислові підприємства
Grade 4	Професійний порушник, спеціальне обладнання та методи саботажу	Багатофакторна автентифікація, повний криптозахист всіх ліній, стійкість до інтелектуальних атак	Державні установи, військові об’єкти, АЕС

Виділяють дві основні складові рівня доступу: просторову (маршрути переміщення) і тимчасову (тимчасові й календарні інтервали).

Рівень доступу (РД) – це сукупність дозволених точок доступу та відповідних для них дозволених тимчасових і календарних інтервалів.

Рівень доступу характеризує права суб’єкта чи/або об’єкта доступу відносно переміщення їх через точки доступу в різні зони контрольованого об’єкта. Тобто термін «рівень доступу» встановлює, куди (до чого) і коли буде дозволено доступ окремо взятого СД/ОД.

Рівень 1 (Grade 1) орієнтований на об’єкти з низьким ризиком, де порушник має мінімальні знання про систему та використовує прості підручні засоби. Такі системи зазвичай використовують нешифровані картки та мають мінімальний самозахист компонентів. На противагу цьому, Рівень 4 (Grade 4) розроблений для об’єктів критичної інфраструктури, де очікується напад професійно підготовлених осіб із глибокими технічними знаннями та спеціальним інструментарієм.

Система Grade 4, наприклад Roger RACS 5, повинна забезпечувати не лише фізичну стійкість бар’єрів, а й повну цифрову безпеку – шифрування комунікацій між зчитувачем та контролером за протоколом OSDP (AES-128), контроль цілісності ліній зв’язку та негайне реагування на будь-які спроби втручання в роботу пристроїв. Це передбачає використання антимаскування зчитувачів та складних алгоритмів детекції підроблених біометричних ознак.

Варто зауважити, що рівень доступу включає у себе:

– перелік дозволених зон контрольованого доступу;
– допустимі часові та календарні інтервали доступу до цих зон;
– сукупність дозволених точок доступу до цих зон.

Системний аналіз термінології та стандартів СКУД дозволяє стверджувати, що галузь остаточно відійшла від концепції «замка та ключа» на користь інтелектуальних систем управління ризиками. ДСТУ EN 60839-11-1 виступає не лише як регуляторний документ, а як комплексний інженерний фреймворк, що гарантує надійність захисту об’єктів.

1.3 Правові засади обробки персональних та біометричних даних

Сучасна епоха характеризується безпрецедентним зростанням обсягів інформації, що генерується, обробляється та зберігається в цифровому середовищі. Персональні дані перетворилися з елементу приватності на ключовий економічний актив, що зумовило необхідність створення жорстких та адаптивних правових рамок для їх захисту. У центрі цього процесу стоїть конфлікт між технологічним прогресом, що вимагає дедалі більшої кількості даних для машинного навчання та ідентифікації, та фундаментальними правами людини на недоторканність приватного життя. Аналіз правових засад обробки персональних та біометричних даних вимагає комплексного підходу, що поєднує вивчення європейського стандарту, втіленого в загальному регламенті про захист даних (GDPR), та поточної динаміки реформування українського законодавства, яке прагне до повної гармонізації з нормами ЄС [34].

Концепція захисту персональних даних пройшла тривалий шлях від загальних принципів поваги до приватного життя, закладених у Конвенції про захист прав людини і основоположних свобод, до спеціалізованих регламентів.

Ключовим моментом став 1981 рік, коли була прийнята Конвенція Ради Європи №108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Саме цей документ заклав фундамент для сучасного українського Закону «Про захист персональних даних», прийнятого у 2010 році. Проте технологічний вибух початку XXI століття продемонстрував недостатність Директиви 95/46/ЄС, що призвело до розробки та прийняття у 2016 році GDPR [15], який набув чинності 25 травня 2018 року.

Філософія GDPR базується на принципі інформаційного самовизначення – ідеї про те, що індивід повинен мати повний контроль над своєю цифровою тінню [1]. В Україні цей підхід наразі впроваджується через масштабну реформу, ключовими елементами якої є законопроєкти №8153 та №6177. Ця реформа є не лише вимогою Угоди про асоціацію з ЄС, а й стратегічною необхідністю для забезпечення сумісності українських цифрових систем із глобальним ринком.

Принципи обробки персональних даних є не просто деклараціями, а прямо діючими правилами, порушення яких тягне за собою найсуворіші санкції за GDPR та новим українським законопроєктом [47]. Ці принципи створюють рамку, в якій будь-яка обробка має бути виправданою та безпечною.

Персональні дані повинні оброблятися на законних підставах, у спосіб, що є справедливим стосовно суб'єкта даних. Прозорість вимагає, щоб будь-яка інформація щодо обробки була легкодоступною та викладеною простою мовою. У поточному українському законі цей принцип реалізується через обов'язок інформувати суб'єкта про володільця, склад даних та мету їх збору в момент збору або протягом 30 днів після нього.

Дані мають збиратися для чітко визначених, явних і легітимних цілей. Використання даних для мети, що є несумісною з початковою, заборонено, крім випадків отримання нової згоди. Наприклад, якщо банк збирає біометричні дані для ідентифікації клієнта при вході в мобільний додаток, він не може без додаткової згоди використовувати ці ж дані для аналізу емоційного стану клієнта з метою маркетингу.

Збиратися та оброблятися має лише той обсяг даних, який є строго необхідним для досягнення мети. Надмірний збір інформації є порушенням. Це особливо актуально для біометрії, де часто достатньо зберегти цифровий шаблон замість повноцінного зображення обличчя чи відбитка пальця.

Володільці зобов'язані забезпечувати актуальність даних та видаляти їх, як тільки мета обробки досягнута. У контексті 2026 року та впровадження хмарних рішень, це вимагає від компаній наявності чітких політик автоматичного видалення застарілих записів.

Для законності будь-якої дії з даними необхідно спиратися на одну з вичерпних підстав, визначених у статті 6 GDPR або статті 11 Закону України «Про захист персональних даних» [119].

Згода залишається найбільш розповсюдженою підставою в Україні, проте GDPR висуває до неї значно жорсткіші вимоги – вона має бути вільною, конкретною, інформованою та однозначною. Це означає відсутність «попередньо проставлених галочок» та можливість відкликати згоду так само легко, як вона була надана. У трудових відносинах згода часто вважається недійсною через дисбаланс сил між працівником та роботодавцем, що змушує компанії шукати інші підстави.

Обробка є законною, якщо вона необхідна для виконання договору, стороною якого є суб'єкт (наприклад, доставка товару), або якщо закон прямо вимагає від контролера певних дій (наприклад, звітність перед податковою).

Біометричні дані – це персональні дані, отримані в результаті спеціального технічного опрацювання фізичних, фізіологічних або поведінкових характеристик особи, що дозволяють здійснити її унікальну ідентифікацію. Згідно зі статтею 9 GDPR, обробка таких даних для цілей унікальної ідентифікації за загальним правилом заборонена, якщо не виконується одна зі спеціальних умов.

Важливо розрізняти два типи процесів, оскільки вони створюють різні рівні ризику для прав людини.

Ідентифікація (1:N) – пошук відповідності біометричного зразка особи серед великої бази даних (наприклад, камери з розпізнаванням обличь на вулицях міст). Це створює високі ризики масового стеження та дискримінації.

Верифікація (1:1) – порівняння зразка, наданого особою, з її власним шаблоном для підтвердження особи (наприклад, Face-ID на смартфоні або відбиток пальця для входу в офіс). Такий метод вважається менш інвазивним, особливо якщо шаблон зберігається локально на пристрої користувача.

Реформа захисту даних в Україні призвела до появи законопроєкту №8153 [120], який докорінно змінює правила гри. Основна його мета – привести національне право у повну відповідність до GDPR.

Таким чином, біометричні дані залишаються найбільш ризикованою зоною. Їх обробка вимагає найвищого рівня технічної підготовки та юридичної обґрунтованості. Компанії, що використовують біометрію, повинні відійти від централізованих баз даних на користь локального зберігання шаблонів та застосування надійного шифрування.

Контрольні запитання

1. Дайте визначення терміну «Доступ».

2. Для яких об’єктів використання стандарту ДСТУ EN 60839-11-1:2014 є обов’язковим на сьогодні?

3. З яких етапів складається процедура ідентифікації?

4. З яких основних складових формується «Рівень доступу» для конкретного суб’єкта?

5. На основі якого принципу базується сучасна нормативна база у сфері систем контролювання доступу?

6. На чому базувалась революційна суть електромагнітної сигналізації Огастуса Рассела Поупа?

7. Назвіть критерії «ідеальної» згоди за стандартами GDPR.

8. Назвіть основний етичний виклик та який філософський конфлікт залишається актуальним у розвитку систем безпеки майбутнього?

9. Опишіть ієрархічну систему оцінки захищеності СКУД.

10. Охарактеризуйте типи зон доступу.

11. У чому полягає різниця між «реактивними» системами минулого та «предиктивними» системами на базі ШІ?

12. У чому полягає різниця між ідентифікацією та верифікацією?

13. У чому полягає різниця між суб’єктом та об’єктом доступу?

14. У чому полягає філософія «інформаційного самовизначення»?

15. Чим відрізняються смарт-карти від звичайних проксі-карт?

16. Що означає принцип «мінімізації даних» для обробки в біометрії?

17. Що таке «Ідентифікатор»? На яких принципах базується їх класифікація?

18. Що таке «Точка доступу» та з яких функціональних елементів вона складається?

19. Як вдосконалювалась конструкція замків?

20. Як римляни змінили соціальний статус ключа?

21. Яка різниця між наступними критичноважливими процедурами: ідентифікацією, автентифікацією та авторизацією.

22. Який принцип роботи було закладено в основу роботи давньоєгипетського дерев’яного замка?

23. Яким чином було організовано першу мережу централізованого моніторингу?

24. Які відомі підходи до безпеки формувались у первісних громадах та від чого вони залежали?

25. Які переваги притаманні «Mobile First» у системах контролю доступу у порівнянні із пластиковими картками?

26. Які технічні заходи допомагають компаніям правильно зберігати та шифрувати біометричні дані?

РОЗДІЛ 2. Топологія та математичні моделі СКУД

2.1 Класи СКУД, структура зон доступу та рівні вкладення

За технічними характеристиками та функціональними можливостями СКУД умовно поділяють на чотири класи (табл. 2.1).

Таблиця 2.1 – Класифікація СКУД [121]

Клас системи	Ступінь захисту від НДС	Функції	Застосування
1	*2*	*3*	*4*
1	Недостатня	Однорівневі СКУД малої місткості, які працюють в автономному режимі та здатні забезпечити: – допуск до зони контролю усіх осіб, які володіють відповідним ідентифікатором; – вбудовану світлову/звукову індикацію режимів роботи; – управління пристроями загородження (функція замка)	На об’єктах, де необхідним є лише обмеження доступу сторонніх осіб
2	Середня	Однорівневі та багаторівневі СКУД малої й середньої місткості, які працюють в автономному або мережевих режимах та здатні забезпечити: – обмеження доступу для конкретної особи або групи осіб до контрольованої зони за датою та тимчасовими інтервалами відповідно до наявних у них ідентифікаторів; – автоматичну реєстрацію подій у власному буфері пам’яті та видачу тривожних сповіщень (під час несанкціонованого проникнення, невірний набір коду або взломі огороджувального пристрою чи його елементів) на зовнішні оповіщувачі або внутрішній пост охорони; – автоматичне керування пристроями загородження (відкривання чи/або закривання)	Усе те, що і для СКУД 1-го класу. А також на об’єктах, де необхідно вести облік та контроль присутності співробітників в дозволеній зоні. У якості доповнення до наявних на об’єкті систем охорони і захисту

Кінець таблиці 2.1

1	2	3	4
3	Висока	Однорівневі та багаторівневі СКУД середньої місткості, які працюють в мережевому режимі й забезпечують: – функції СКУД 2-го класу; – контроль переміщень осіб та майна в контрольованих зонах (об'єкті); – ведення табельного обліку і баз даних за кожним СД; – ведення безперервного автоматичного контролю справності складових частин системи; – інтеграцію з системами і засобами охоронно-пожежної сигналізації (ОПС) й телевізійної системи відеонагляду (ТСВ) на релейному рівні	Те ж, що й для СКУД 2-го класу. На об'єктах, де необхідно вести табельний облік та контроль переміщення співробітників по об'єкту. Для спільної роботи із системами ОПС та ТСВ
4	Дуже висока	Багаторівневі СКУД середньої та великої місткості, які працюють в мережевому режимі та забезпечують: – функції СКУД 3-го класу; – інтеграцію з системами і засобами ОПС, ТСВ та іншими системами безпеки й управління на програмному рівні; – автоматичне керування пристроями загородження під час пожежі та інших надзвичайних ситуацій	Те ж, що й для СКУД 3-го класу

В залежності від особливостей об'єкта, конфігурації СКУД, фірми виробника набір функцій кожного класу може змінюватися й доповнюватись функціями з інших класів [87].

До СКУД 1-го класу відносять малофункціональні системи малої місткості, які здатні працювати в автономному режимі. Такі системи застосовують у тих випадках, коли замовнику необхідно забезпечити контрольований доступ співробітників і відвідувачів, у яких наявні відповідні ідентифікатори. При цьому не ставиться завдання контролю часу доступу й виходу з приміщення, реєстрація проходів й передача даних на центральний комп'ютер. Робота СКУД не контролюється. Зазвичай адміністратор (особа, яка

відповідає за пропускний режим) володіє майстер-картою (ноутбук), за допомогою якої він може вносити (виключати) з бази даних системи ідентифікатори співробітників та відвідувачів та зчитувати інформацію з буфера системи.

Автономна система складається з контролера, який конструктивно об'єднано із зчитувачем, та виконавчого елемента. В більшості випадків такій системі властиве використання магнітних карт та електронних ключів «Touch Memory». Залежно від типу контролера або замка кількість СД в списку бази даних системи може досягати від 60 до 2800 чоловік. До складу автономної системи входить також й резервне живлення та механічний ключ для аварійного відкривання замка.

СКУД 2-го класу також відносять до малофункціональних систем, але для них характерною є можливість розширення або включення їх, чи складових частин системи, до загальної лінії зв'язку (мережевий режим). Таким системам притаманні уже ряд додаткових функцій.

На об'єктах, які обладнано засобами і системами охоронно-пожежної сигналізації (ОПС), СКУД 2-го класу зазвичай застосовують у якості самостійних систем й переважно розглядають з точки зору засобу підсилення режиму забезпечення безпеки об'єкта.

СКУД 3-го і 4-го класів прийнято називати мережевими, оскільки контролери у них об'єднано в локальну мережу, яка працює в режимі реального часу, під час якого відбувається їх безперервний діалог із периферійними пристроями. Слід пам'ятати, що системи цих класів – великі та багаторівневі системи, які розраховано на велику кількість користувачів (більше 1500 осіб), а отже потребують більш складних електронних ідентифікаторів (Proxmity, Wiegand-картки, біометричний контроль тощо).

На релейному рівні, в переважній своїй більшості, системи 3-го класу інтегруються із системами ОПС та телевізійними системами відеонагляду (ТСВ). При цьому, релейний рівень передбачає у собі наявність додаткового модуля (додаткових входів/виходів) в контролері до якого можуть бути підключені як охоронні чи/або пожежні сповіщувачі, так і виходи для керування телекамерами або іншими пристроями. Така інтеграція застосовується лише для малих об'єктів де кількість взаємодій між системами невелика, і всі вони можуть бути враховані в процесі проектування системи безпеки. На практиці цей рівень інтеграції вважають простим, універсальним й досить надійним.

Системи 4-го класу – це багаторівневі системи великої ємності. Відмінними рисами великих систем прийнято вважати як наявність розвиненого програмного забезпечення, яке дозволяє реалізовувати велику

кількість функціональних можливостей, так і високу ступінь інтеграції на програмному (системному) рівні з іншими системами охорони та безпеки.

Програмний рівень передбачає об'єднання різних систем на основі єдиної програмно-апаратної платформи, якій притаманний єдиний комунікаційний протокол та загальна БД.

На практиці, під час побудови мережевих СКУД використовують чотири рівня мережевої взаємодії [129]:

– перший рівень – комп'ютерна мережа типу клієнт/сервер на основі Ethernet з протоколом обміну TCP/IP;

– другий рівень – зв'язок між контролерами та комп'ютерами підсистем через інтерфейс RS 232, USB з дальністю зв'язку до 15 м;

– третій рівень – зв'язок між контролерами та зчитувальними пристроями через інтерфейс RS 485, RS-422 тощо;

– четвертий рівень – рівень сповіщувачів ОПС й ланцюгів керування (нестандартні спеціалізовані інтерфейси та протоколи обміну інформацією).

В інтегрованих системах охорони та інтегрованих системах безпеки та управління системами життєзабезпечення

Для вирішення сформованих вище завдань система контролю та управління доступом повинна включати в себе три основні елементи:

– пристрій зчитування ідентифікаційних ознак (зчитувач);

– пристрій аналізу ідентифікаційних ознак та прийняття рішення (контролер);

– пристрій управління доступом.

Зазвичай пристрій управління доступом включає у себе:

– пристрій перешкоджуючий (загороджувальний) керований (двері, турнікет та схожі за принципом роботи пристрої й устаткування);

– виконавчий пристрій для управління станом загороджувальнийх пристроїв (електромагнітний замок, болард, шлагбаум тощо);

– елементи контролю стану загороджувальних пристроїв (магнітно-герконовий давач тощо);

– елементи неконтрольованого управління станом загороджувальних пристроїв.

На практиці СКУД має забезпечувати виконання наступних функцій [21]:

– відкривання ППК під час зчитування ідентифікаційної ознаки, доступ за якою дозволено в передбачену зону доступу протягом заданого часового інтервалу або за командою оператора СКУД;

– заборона відкривання ППК під час зчитування ідентифікаційної ознаки, доступ за якою не дозволено до передбаченої заздалегідь зони доступу в певний часовий інтервал;

– санкціонована зміна (додавання, видалення) ідентифікаційних ознак в ПУ і зв'язок їх з зонами доступу (приміщеннями) й тимчасовими інтервалами доступу;

– захист від несанкціонованого доступу до програмних засобів ПУ для зміни (додавання, видалення) ідентифікаційних ознак;

– захист технічних і програмних засобів від несанкціонованого доступу до елементів управління, встановлення режимів і до інформації;

– збереження налаштувань та БД ідентифікаційних ознак під час відключення електроживлення, ручного, напівавтоматичного або автоматичного відкривання ППК для проходу за аварійних ситуацій, пожеж, технічних несправностях відповідно до правил встановленого режиму та протипожежної безпеки;

– автоматичне закриття ППК під час відсутності факту проходу через певний час після зчитування дозволеної ідентифікаційної ознаки;

– видача сигналу тривоги (або блокування ППК на певний час) під час спроби підбору ідентифікаційних ознак;

– реєстрація та протоколювання поточних і тривожних подій;

– автономна робота зчитувача з ППК в кожній точці доступу під час відмови зв'язку із ПУ.

Узагальнена структура СКУД (рис. 2.1) реалізується, в переважній більшості, для усіх технічних (електронних, механічних тощо) або автоматизованих систем із використанням людини, як елемента загальної системи КУД.

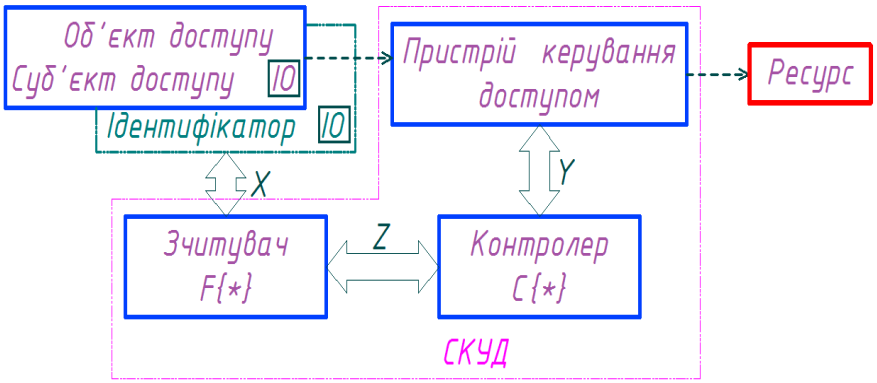


Рисунок 2.1 – Узагальнена структурна схема СКУД [110]

Найбільш вживана СКУД – це механічний замок, який володіє усіма необхідними елементи СКУД. Людина (суб'єкт) володіє ключем (ідентифікатором), який є фізичною носієм ідентифікаційної ознаки. При цьому сама ІО – це форма ключа. Механізм замка – зчитувач та пристрій прийняття рішення (контролер). Засувка й фіксатор – виконавчі пристрої, які приводяться

в дію під час відповідності форми ключа (тобто ІО) параметрами механізму (зразок ІО) і дозволяють відкрити двері.

Інший приклад – охоронець на КПП. СД пред'являє йому пропуск із різними ідентифікаційними ознаками – форма, колір або розмір пропуску, фотографія, прізвище, спеціальні знаки, які дозволяють доступ до різних підрозділів, зон тощо. Охоронець візуально оцінює (зчитує) пропуск на відповідність із встановленим зразком, про який йому заздалегідь відомо (процедура ідентифікації). Після цього порівнює фотографію із реальною особою (автентифікація). В кінці, коли порівнювальні параметри збігаються розблоковує ППК (доступ дозволений).

Перелічені вище процедури виконують й сучасні автоматизовані СКУД. Усі або частина процедур (ідентифікація й автентифікація; перевірка санкціонування доступу; управління виконавчими пристроями управління доступом; протоколювання подій) автоматизуються. Таким чином, частково або повністю виключається людський фактор – одне із найбільш слабших ланок системи безпеки.

Отримані базові знання про СКУД дозволяють сформувати, у загальному вигляді, алгоритм функціонування СКУД.

Відомо, що для виконання процедур ідентифікування та автентифікації СД/ОД він або ідентифікатор повинен володіти ідентифікаційною ознакою або ознаками, кожна з яких характеризується набором параметрів або функцій. У функціональній схемі (рис. 2.1) М ідентифікаційних ознак xkm суб'єкта або об'єкта (ідентифікатора), які володіють К параметрами, визначаються у загальному матрицею Х. Елемент матриці x_{km} являє собою k-й параметр (функцію) m-ої ознаки.

Зчитувач СКУД перетворює інформаційні ознаки xkm з носіями певної фізичної природи в сигнали z_{km}, які будуть придатні для подальшого оброблення контролером.

Алгоритм перетворення визначається арифметичним оператором F:

$$Z=F\{X\}. \qquad (2.1)$$

Контролер, у загальному випадку, порівнює ознаки Z з усіма зразками Z_{eo}, які зберігаються в БД системи, тим самим визначаючи порядковий номер «і» ОД/СД або фіксуючи відсутність його еталонної ознаки Z_{eo}, відповідно до наданої Z.

На підставі результатів порівняння (фактично за знайденим значенням «і»), тобто інформації про рівень доступу і-го СД/ОД, який зберігається в базі даних, контролер формує матрицю P_i вихідних сигналів:

$$P_i = C\{Z, Z_{eo}\}|_{i=1, \ldots, I}. \quad (2.2)$$

До складу цих сигналів входять й сигнали, які управляють виконавчими пристроями. Виконавчі пристрої розблоковують (під час санкціонованого доступу) загороджувальні пристрої, забезпечуючи, тим самим, доступ до контрольованої зони. Рівень доступу визначає дозволені зони та тимчасові й календарні інтервали доступу (коли, куди і до чого дозволено доступ). Для детермінованої системи, якою є СКУД, це визначає реакцію системи, тобто, процедуру функціонування загороджувальних пристроїв, які у свою чергу, приводяться в дію виконавчими пристроями.

Як бачимо, основні особливості СКУД залежать, насамперед, від характеристик об'єкта, на якому здійснюється контроль та управління доступом. Серед особливостей об'єкта, основними його особливостями, виступає структура (топологія) й режим функціонування зон контрольованого доступу (маршрути переміщення, тимчасовий та календарний графік, потенційні можливості несанкціонованих дій).

З точки зору СКУД, найбільшу вагу мають особливості точок контролю доступу, як основного осередку будь-якої системи КУД. У свою чергу, точка доступу повинна обов'язково містити усі основні елементи СКУД. Зважаючи на склад її технічних засобів і принципів побудови можна зробити висновок, що це саме те від чого залежить характеристики системи.

Еволюція СКУД у межах сучасної парадигми безпеки демонструє перехід від простих механічних бар'єрів до складних інтелектуальних екосистем, що інтегрують фізичні, інформаційні та технічні аспекти захисту об'єктів. СКУД на сьогодні є не лише інструментом обмеження переміщень, а фундаментальним складником глобальної безпеки, що включає національну, економічну, інформаційну та фізичну компоненти. Проектування таких систем вимагає розуміння структури зон доступу та логіки їх вкладення, оскільки саме ці параметри визначають здатність системи ефективно протидіяти несанкціонованим проникненням, забезпечувати облік робочого часу та підтримувати високий рівень безпеки в критичних точках об'єкта.

Зонування об'єкта в СКУД – це процес поділу фізичного простору на логічно та фізично відокремлені області, для кожної з яких визначаються специфічні правила доступу, методи ідентифікації та рівні безпеки. Зона доступу не є просто геометричним простором; це динамічний об'єкт у пам'яті системи, що характеризується певним статусом перебування користувачів та набором пов'язаних виконавчих пристроїв. На великих промислових та комерційних об'єктах структура СКУД безпосередньо залежить від характеру

діяльності та внутрішніх регламентів безпеки, де прості рішення поступаються місцем багаторівневим охоронним централям.

Центральним елементом будь-якої структури зон є точка доступу Точки доступу класифікуються за напрямком контролю: односторонні, де вхід здійснюється за зчитувачем, а вихід – за кнопкою, та двосторонні, що забезпечують повний контроль переміщень в обох напрямках. Саме двосторонні точки доступу є базисом для формування ієрархічних структур, оскільки лише вони дозволяють системі однозначно фіксувати факт перетину межі зони та змінювати статус користувача з «зовні» на «всередині».

Проектування та експлуатація зон доступу в Україні базуються на чіткому дотриманні державних стандартів, які гармонізовані з міжнародними нормами. Ключовим документом є ДСТУ EN 60839-11-1:2014, який встановлює вимоги до електронних систем контролювання доступу та їх складників. Цей стандарт визначає рівні розпізнавання об’єктів та вимоги до цілісності інформації, що є важливим для систем з глибокою вкладеністю зон.

Проста (одиночна) зона. Структуру простої зони z_j контрольованого доступу до однієї точки доступу d_i, яка належить цій зоні, подано на рисунку 2.2.

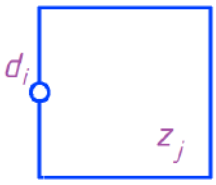


Рисунок 2.2 – Проста зона

На схемах, зазвичай, точку доступу позначають колом, при цьому акцентують на тому, що вона містить усі необхідні для вирішення завдання КУД елементи (зчитувач, контролер, пристрій управління доступом). Така зона має як мінімум одну ТД. Форма зони, в загальному випадку, може бути довільною. Окрім цього, слід пам’ятати, що зона доступу може включати у себе декілька приміщень із загальним режимом функціонування, що є однією зоною.

Взаємопов’язані зони. У пов’язаних зонах переміщення в одну із зон контрольованого доступу можливо через інші зони контрольованого доступу. Взаємопов’язані зони z_1 та z_2 (рис. 2.3) мають, принаймні, одну спільну ТД d_2, яка належить обом пов’язаним між собою зонам. Через неї здійснюється переміщення з однієї ЗКД z_1 в іншу, пов’язану з нею зону z_2. Контроль та управління доступом у кожну із зон може відбуватися як через ТД, які знаходяться по периметру взаємопов’язаних зон d_1 та $<d_3$, так і через загальні ТД d_2, тобто через ті точки доступу, які належать цій зоні або зонам.

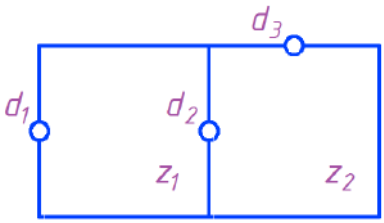


Рисунок 2.3 – Взаємопов’язані зони

Групи взаємопов’язаних зон. На практиці для декількох взаємопов’язаних зон існують різні окремі випадки:

– послідовнопов’язані зони (рис. 2.4), коли доступ в кожну зону здійснюється з однієї і тієї ж загальної зони (z_1 і z_2);

– паралельнопов’язані зони (рис. 2.5), коли доступ в кожну наступну зону (z_2, z_3 і z_4) здійснюється із попередньої зони (z_1);

– довільнопов’язані зони, які є комбінацією попередніх випадків.

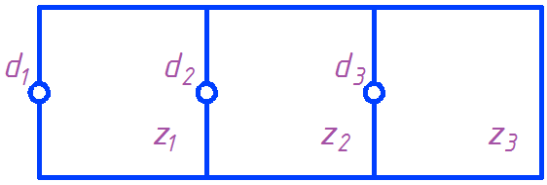


Рисунок 2.4 – Послідовнопов’язані зони

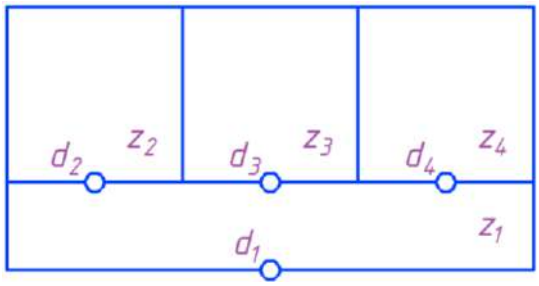


Рисунок 2.5 – Паралельнопов’язані зони

Під час вибору рівнів доступу для взаємопов’язаних зон слід пам’ятати, що для них притаманні деякі особливості.

Ієрархія зон доступу будується на принципі послідовного обмеження прав у міру просування вглиб об’єкта. Рівень вкладення визначає кількість бар’єрів, які необхідно подолати користувачеві для досягнення цільової зони. У великих розподілених системах, таких як Hikvision HikCentral, ієрархія груп персоналу може налічувати до 10 рівнів, що дозволяє детально структурувати доступ для компаній з тисячами співробітників.

Вкладеними називають зони, коли одна або група зон контрольованого доступу знаходяться всередині іншої ЗКД (рис. 2.6). Вкладені зони можуть бути як простими, так і взаємопов’язаними.

Типовим прикладом цієї структури є територія (z_1) на якій розташовано деякі об'єкти (z_2, z_3, z_4). Зауважимо, що ця структура та її схемне подання відображають лише взаємозв'язок зон, а не їх просторове розташування.

Так, на рисунку 2.6 дві групи вкладених зон можуть бути різними поверхами однієї і тієї ж будівлі, а зовнішній периметр виступає як у якості периметра території, так і межами однієї будівлі. В останньому випадку зона z_1 може бути загальним приміщенням (хол, сходи тощо).

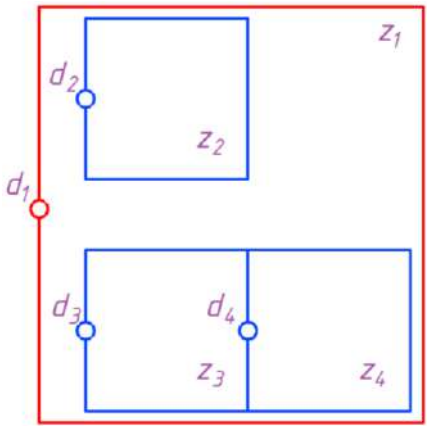


Рисунок 2.6 – Вкладені зони

Провівши аналіз розглянутої структури зон, можна виділити два типи:

– зовнішні зони контрольованого доступу – зони, доступ до котрих можливий із зон вільного доступу;

– внутрішні зони контрольованого доступу – зони, доступ до яких можливий лише з інших зон контрольованого доступу.

Оперуючи наведеною термінологією доцільно ввести ще один термін – рівень вкладення зон, або рівень доступу зон. У тому випадку, коли за нульовий рівень взяти зони вільного доступу, тоді:

– зовнішні зони матимуть перший рівень (доступ до них можливий лише через ЗСД, а отже, необхідно пройти один етап контролю доступу – одну ТД);

– внутрішні зони, які межують із зовнішніми, тобто мають загальні ТД із зовнішніми зонами, матимуть другий рівень (щоб потрапити в них, необхідно пройти як мінімум дві точки доступу);

– третій рівень матимуть зони, доступ до яких можливий лише через дві згадані вище зони (тобто необхідно подолати мінімум три ТД).

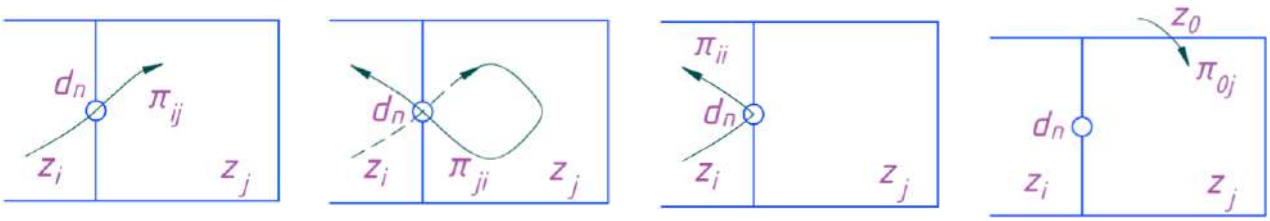
Дана теорія добре сприймається за прикладом наведеним на рисунку 2.6, на якому зона z_1 має перший рівень, z_2 та z_3 – другий, а z_4 – третій. Таким чином, поняття рівня вкладення зон або рівня доступу зон характеризує необхідні вимоги, які висуваються до рівня доступу суб'єкта в ці зони. Як

бачимо чим вищим є рівень доступу зони, тим вищим повинен бути рівень доступу суб'єкта.

З функціональної точки зору, кінцевою метою системи є контроль та управління доступом в ЗКД, тобто контролювання й управління доступом суб'єкта у ній, а також отримання інформації у якій саме зоні він знаходиться із протоколюванням подій. Очевидно, що інформацію для виконання описаних процедур доцільно отримувати лише в ТД.

Для подальшого сприйняття матеріалу необхідно оперувати терміном «перехід/переміщення» з однієї зони доступу (контрольованої чи/або вільної) в іншу. Такий перехід із зони z_i в зону z_j прийнято позначати через π_{ij} (при цьому нульовий індекс означає зону вільного доступу).

На рисунку 2.7 подано різні варіанти переміщення суб'єкта доступу через точку доступу [58].



а) б) в) г)

Рисунок 2.7 – Можливі варіанти руху суб'єкта доступу

В першому випадку (рис. 2.7, а) СД переміщається із зони z_i в зону контрольованого доступу z_j через точку доступу d_n.

Далі (рис. 2.7, б) він може переміщуватись всередині зони z_j та вийти з неї назад через ту ж саму ТД. Таким чином, переходи з різним порядком індексів відрізняються напрямком переміщення.

Для різних виконань СКУД можливими є ще два випадки. У першому (рис. 2.7, в) СД пройшовши ідентифікацію, залишився в тій же самій зоні z_i. Такий перехід позначають π_{ii}. У другому випадку (рис. 2.7, г) СД потрапляє несанкціоновано до зони контрольованого доступу, тим самим оминаючи ТД. Цей перехід позначають π_{0j}.

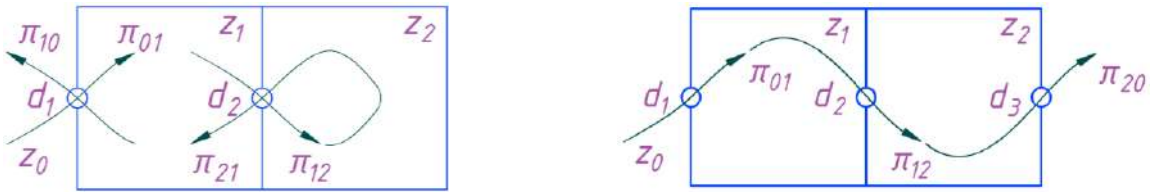
Більш складні випадки переміщення СД в заємопов'язаних зонах можна спостерігати на рисунку 2.8.

Таким чином, перехід πij означає наступне:

– за умови коли $i \neq 0$, $j \neq 0$ – переміщення СД з i-ої зони контрольованого доступу в j-ту;

– за умови коли $i = 0$, $j \neq 0$ – переміщення СД із зони вільного доступу в j-ту зону контрольованого доступу;

– за умови коли i = j – повернення в ту ж саму зону доступу (контрольовану або вільну) із ідентифікацією в ТД без переміщення через цю ж точку доступу.



а) б)

Рисунок 2.8 – Маршрути руху суб’єкта доступу

Переходи π_{ij} та π_{ji} з різним порядком проходження індексів відрізняються напрямком переміщення (порядком проходження ТД).

Далі необхідно оперувати терміном «маршруту суб’єкта доступу». Отже, маршрут СД – це кінцева послідовність переходів, виконаних ним.

Послідовність переходів, яка подана на рисунку 2.8, а, для двох послідовнопов’язаних зон можна записана наступним чином:

$$\pi_{01}, \pi_{12}, \pi_{21}, \pi_{10}. \qquad (2.3)$$

Зони, з яких починається та якими закінчується маршрут, прийнято називати кінцевими. Решта – це внутрішні.

Наведена послідовність переходів (2.3) визначає замкнутий маршрут руху СД. При цьому замкнутість означає повернення в ту ж саму вихідну зону доступу.

Замкнутий маршрут починається і закінчується в одній і тій же зоні доступу. В іншому випадку маршрут прийнято називати відкритим.

Повний маршрут починається та закінчується на зовнішніх кінцевих зонах вільного доступу й включає у себе усі переходи, які відбуваються в зонах контрольованого доступу на об’єкті.

Повний замкнутий маршрут починається та закінчується в одній і тій же зовнішній кінцевий зоні вільного доступу, тобто в окремому випадку повного маршруту кінцеві зоною доступу є зовнішні зонами вільного доступу.

Маршрут може бути й квазізамкненим, коли СД переміщується в контрольовану зону із зони вільного доступу через одну точку доступу, а виходить із ЗСД через іншу зовнішню ТД (рис. 2.8, б). іншими словами вхід та вихід із ЗКД відбуваються в область поза контрольованим об’єктом через різні точки доступу. Такий квазізамкнений маршрут можна записати як:

$$\pi_{01}, \pi_{12}, \pi_{20}. \qquad (2.4)$$

Усі ці переходи прийнято вважати коректними (санкціонованими) переходи, оскільки переміщення СД здійснюється за конструктивно-призначеним для цього елементами конструкції об'єкта.

На практиці часто зустрічаються й некоректні (несанкціоновані) переходи – переміщення за не призначеним для цього елементам конструкції об'єкта, в тому числі й з порушенням цілісності конструкцій, тобто, оминаючи ТД.

Коректний (санкціонований) маршрут являє собою послідовність коректних переходів. Враховуючи загальну точку зору, коректний маршрут СД повинен бути безперервним: суб'єкт повинен пройти усі послідовнопов'язані зони сформованого маршруту.

Наприклад, повний замкнутий маршрут $\pi_{01}\rightarrow\pi_{12}\rightarrow\pi_{21}\rightarrow\pi_{10}$ (рис. 2.8, а) є безперервним. Однак, маршрут $\pi_{01}\rightarrow\pi_{12}\rightarrow\pi_{10}$ навпаки, не буде таким, оскільки СД, перебуваючи в другій із двох послідовних зон контрольованого доступу,

виявився в першій, без повернення в зону z_1 з z_2, тобто відсутній перехід π_{21}.

З огляду на це, доцільно навести деякі принципи функціонування СКУД, які випливають із наведених вище особливостей:

1. Санкціоновані дії – будь-які дії в СКУД повинні бути підтверджені відповідним рівнем доступу.

2. Здійсненність – коректне переміщення СД повинно проводитися тільки за конструктивно-призначеними, для цього, елементами об'єкта.

3. Безперервність – санкціоноване переміщення через ТД має відбуватись лише з послідовним проходженням поспіль усіх взаємопов'язаних зон та відповідних, які належать цим зонам, точок доступу без жодного їх нехтування на цьому маршруті (в заданому часовому інтервалі).

4. Неповторюваність – проходження однієї і тієї ж ТД не може бути виконано двічі поспіль в одному і тому ж напрямку без проходження інших точок доступу або цієї ТД в зворотному напрямку.

Варто зауважити, що перші три принципи є обов'язковими для усіх типів СКУД. Виконання четвертого не контролюють для спрощених системах. Однак це призводить до зниження надійності СКУД.

Для кращої уяви про основні елементи системи, які впливають на режим функціонування ТД необхідно ввести певні графічні позначення. На подальших схемах j-й зчитувач будемо позначати прямокутником, а кнопку m управління виходом k – квадратом з колом всередині (рис. 2.9).

При цьому пам'ятаємо, що виконавчий та загороджувальний пристрої входять до складу ТД (d_i), яка позначається колом.

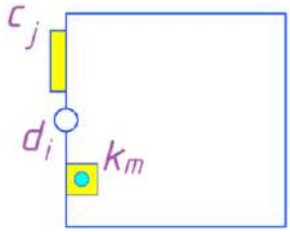


Рисунок 2.9 – Позначення елементів обладнання точки доступу

У залежності від структури та складу використаних для організації ТД технічних засобів, остання може мати різну конфігурацію, від якої істотно залежатимуть їх режими функціонування.

Точки доступу, в залежності від їх особливостей прийнято класифікувати наступним чином:

1. За розташуванням на контрольованому об’єкті:

– зовнішні, через які здійснюється переміщення із зон вільного доступу в зони контрольованого доступу або вихід із ЗКД в ЗСД;

– внутрішні, під час проходження яких суб’єкт доступу не залишає меж зони контрольованого або обмеженого за часом доступу.

2. За характером взаємодії точок доступу одна з одною:

– пов’язані (ТД, алгоритм роботи яких залежить від алгоритму роботи інших);

– непов’язані (ТД, які функціонують незалежно від інших).

3. За напрямком переміщення:

– однонаправлені (рух через ТД здійснюється лише в одному напрямку);

– ненаправленні (рух через ТД здійснюється за обома напрямками).

4. За способом контролю напрямку переміщення:

– з одностороннім контролем доступу (контроль доступу (ідентифікація та управління доступом) здійснюється тільки в одному напрямку (під час переміщення СД/ОД у зворотньому напрямку здійснюється лише управління доступом (без контролю), причому безпосередньо самим суб’єктом доступу);

– з двостороннім контролем доступу (під час руху СД/ОД у будь-якому з напрямків відбувається повний цикл процедур КУД: ідентифікація (автентифікація), перевірка санкціонованості та управління доступом (при цьому управління доступом здійснюється самою системою КУД, а не СД)).

В випадку точки доступу з одностороннім контролем система контролює переміщення суб’єкта доступу лише в одному напрямку. Переміщення у зворотному напрямку система не відслідковує. Наприклад, в неавтоматизованій системі для проходу в контрольовану зону необхідно надати (пред’явити) перепустку (ідентифікатор), а для виходу цього не треба. В автоматизованій

системі – СД надає свій ідентифікатор, СКУД перевіряє рівень доступу і подає команду на пристрій управління доступом. Під час переміщення суб'єкта доступу у зворотному напрямку він або рухається за маршрутом, який не обладнано загороджувальними пристроями управління доступом, або керує ними без надання ідентифікатора.

Як бачимо, під час санкціонованого доступу дозвіл на вхід у контрольовану зону після ідентифікації СД/ОД надається лише СКУД. У той час, коли для виходу з неї (прохід у зворотньому напрямку) достатньо натиснути кнопку виходу, щоб розблокувати замок дверей або пройти через турнікет з фіксованим напрямком обертання (прохід лише одному напрямку), тобто здійснюється неконтрольований вихід. Приклад такої системи наведено на рисунках 2.10 та 2.11.

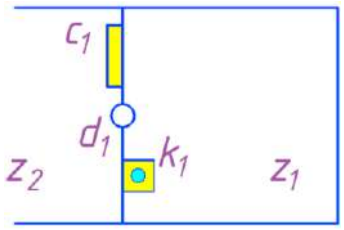


Рисунок 2.10 – Точка доступу з одностороннім контролем

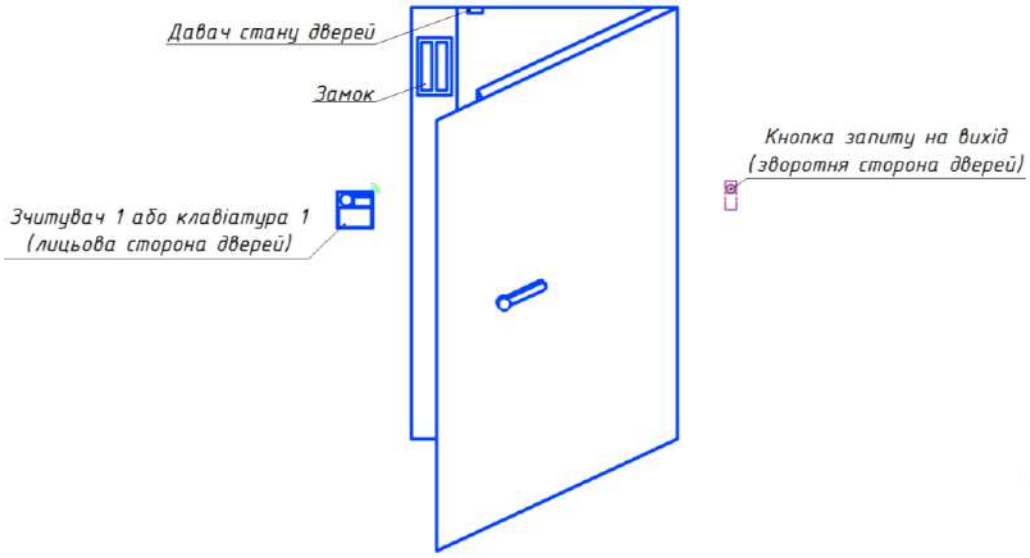


Рисунок 2.11 – Технічні засоби точки доступу з одностороннім контролем

Для контрольованого проходу необхідно надати дійсний ідентифікатор, а для виходу – лише натиснути кнопку виходу. З точки зору наповнення ТД технічними засобами, то вона повинна бути обладнана одним зчитувачем сх на вході. На виході монтується елемент неконтрольованого управління загороджувальним пристроєм (наприклад, кнопка управління дверима або турнікетом).

Розглянутий випадок є досить поширеним варіантом побудови ТД, який використовуються для багатьох систем. Перевагою цього варіанту є простіша, у технічному плані, система. З функціональної точки зору вона використовується у тому випадку, коли необхідно обмежити лише вхід на контрольований об'єкт.

При цьому, для цього випадку контролю притаманні наступні недоліків:

– не відомо, де знаходиться СД/ОД (в контрольованій зоні z_1 або поза нею, в зоні z_2 (причина – вихід не контролюється, і система не може фіксувати факт виходу суб'єкта, який отримав доступ в контрольовану зону));

– внаслідок неконтрольованого виходу виникає можливість використання одного і того ж ідентифікатора для багаторазового повторного проходу через цю точку доступу (СД/ОД проходить до контрольованої зони (санкціоновано), потім передає ідентифікатор іншому, і він також (але уже несанкціоновано) проходить на цю ж територію, використовуючи один і той же ідентифікатор).

Варто зауважити, що другий недолік притаманний лише для СКУД, у яких не застосовується автентифікація – перевірка права володіння СД ідентифікатора.

У свою чергу, точки доступу із двостороннім контролем переміщення дозволяють усунути наведені вище недоліки, зокрема фіксувати факти спроб проходу за одним й тим самим ідентифікатором без попереднього виходу із ЗКД.

На практиці відомо про наступні типи схем із двостороннім контролем проходу:

1. Точка доступу, у якій контролюється й фіксується тільки факт проходу, без визначення напрямку. Тобто використовується, один і той же зчитувач для контролю й управління проходом в обох напрямках. В цьому випадку пройти в прямому, та в зворотному напрямку може лише власник ідентифікатора. Оскільки, в такій схемі, застосовується тільки один зчитувач для визначення напрямку руху, то, формально, ведеться облік кількості проходів суб'єкта з певним ідентифікатором. Напрямок проходу може фіксуватися за порядком проходження точки доступу (наприклад, непарні проходи відповідають одному напрямку (вхід в контрольовану зону), а парні – другому напрямку (виходу)).

Зауважимо, що така система, за рядом причин, рідко використовується на практиці:

– втрата дійсного напрямку під час дворазового (поспіль) пред'явлення ідентифікатора, якщо вхід не відбувся за яких-небудь причин (в друге пред'явлений ідентифікатор сприймається як вихід, хоча СД/ОД або не був в контрольованій зоні реально, або тільки но увійшов у неї);

– відсутність, у ряді випадків, технічної можливості використання одного і того ж зчитувача для входу і виходу.

2. Точка доступу, у якій контролюється й фіксується напрямок переміщення. Для цього зазвичай використовують окремі зчитувачі для контролю і управління дверима під час проходження з різних сторін (рис. 2.12 та 2.13).

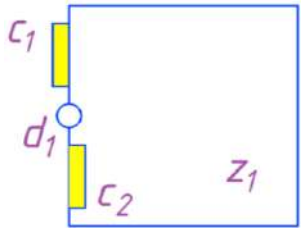


Рисунок 2.12 – Точка доступу з двостороннім контролем

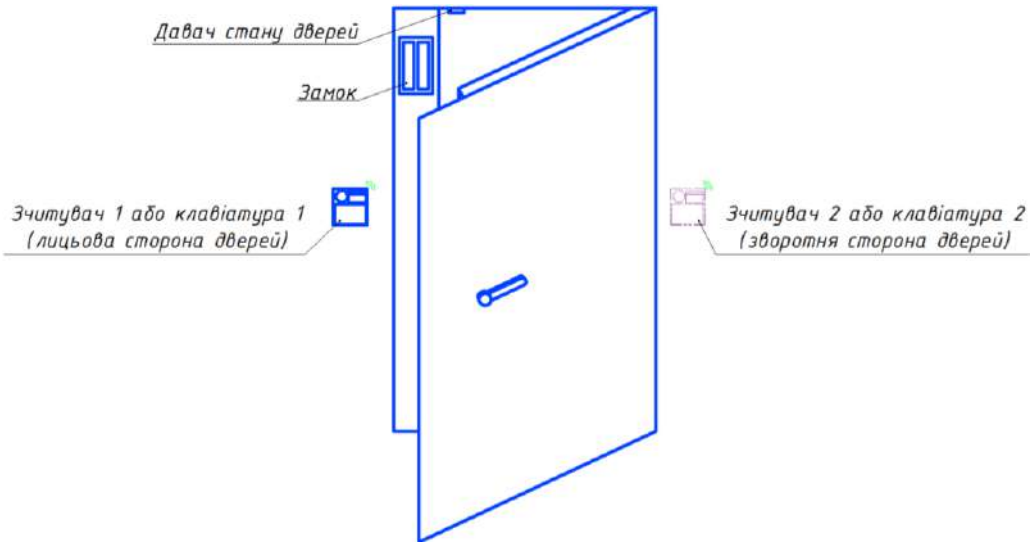


Рисунок 2. 13 – Технічні засоби точки доступу з двостороннім контролем

Для цього випадку притаманною є можливість усунення згаданих вище недоліків за рахунок фіксації всіх переходів через ТД.

Для контрольованого двостороннього проходу дійсний ідентифікатор пред’являється як при переміщенні із зони вільного доступу в ЗКД, так і при зворотному русі. Наприклад, ідентифікатор надається як для входу в контрольовану зону, так і для виходу з неї. Більш того, зробити це необхідно використовуючи окремі зчитувачі. Цей випадок дозволяє здійснювати контроль місця розташування СД/ОД, оскільки напрямок, в якому він рухається, точно визначається за зчитувачем до якого пред’явлено ідентифікатор. Окрім контролю місцезнаходження СД/ОД є можливість реєстрації спроб повторного проходу (в заданий часовий інтервал) як несанкціонованої дії, забороняючи, при цьому, прохід.

Тепер розглянемо пов’язані точки доступу. Точку доступу із двостороннім контролем можна розглядати як дві пов’язані між собою ТД, які володіють спільними пристроями керування доступом. Окрім цього, під час використання алгоритму заборони повторного проходу алгоритми їх функціонування також пов’язані, тобто це дві технічно й алгоритмічно пов’язані точки доступу (як правило обслуговуються вони одним контролером).

Прикладом пов’язаних точок доступу є наступна схема (рис. 2.14).

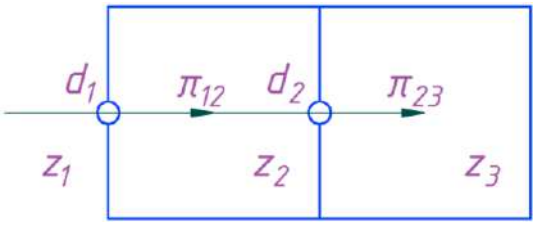


Рисунок 2.14 – Пов’язані точки доступу з направленим переміщенням

Як уже зазначалось, в загальному випадку переходи (або їх частина) можуть бути односпрямованим, тобто дозволене переміщення може здійснюватися лише в одному напрямку. Особливістю цієї схеми є те, що переходи π_{12} і π_{23} є послідовно односпрямованим, тобто вони можуть бути виконані тільки послідовно, один за іншим з рухом в одному напрямку.

Практичним прикладом такої схеми може бути переміщення в ЗКД z_3 через спеціальну зону або спеціальний загороджувальний пристрій z_2. Тут спочатку відкриються перші двері (точка доступу d_1), СД/ОД переміщується до тамбура (зона z_2) із зони z_1. Після чого перші двері закриваються, і лише тоді можна відкрити другі двері (точка доступу d_2) для проходу в зону z_3. Такий режим використовують, перш за все, з двох основних причин. По-перше, для контролю (огляду) СД/ОД в закритій зоні (наприклад, митниця, атомна енергетика тощо). По-друге, для виключення прориву через одиночну ТД в зону контрольованого доступу групи СД/ОД слідом за суб’єктом, який має дійсний ідентифікатор, після розблокування замків дверей. Тактика такого доступу називається шлюз.

Категорії доступу зони характеризують важливість або значимість зони контрольованого доступу для послідовно пов’язаних зон. Для санкціонованого доступу в ЗКД вищої категорії суб’єкту доступу необхідно володіти більш високим рівнем доступу. Наочно це можна продемонстровано на прикладі послідовно пов’язаних зон (рис. 2.4). Для доступу в кожну наступну зону СД необхідно володіти більш високим рівнем доступу. Відповідно до визначення, рівень доступу – це сукупність дозволених ТД і відповідних їм дозволених тимчасових й календарних інтервалів. Цю сукупність можна записати так:

$$P_i(d_1, d_2, ..., d_n, \Delta t_1, \Delta t_2, \Delta t_m, \Delta T_1, \Delta T_2, \Delta T_l). \quad (2.5)$$

Цей вираз включає згадані сукупності точок доступу d_n, дозволених тимчасових Δt_m і календарних ΔT_l інтервалів. В окремому випадку такі змінні, як тимчасові й календарні інтервали, можуть бути відсутніми, тобто мінімальний набір змінних – це сукупність дозволених точок доступу:

$$P_i(d_1, d_2, ..., dn). \quad (2.6)$$

Повертаючись до поняття категорії доступу зони, можна говорити, що цей термін визначає необхідний для доступу набір параметрів рівня доступу суб'єкта, який наведено у виразі (2.5).

Так, для схеми об'єкта, який наведено на рисунку 2.4, можливими є три суб'єкта доступу з відповідними рівнями:

$$P_1(d_1), P_2(d_1, d_2) \text{ та } P_3(d_1, d_2, d_3). \quad (2.7)$$

Першому дозволений прохід в першу зону контрольованого доступу, другому – в першу і другу, третьому – в будь-яку.

Аналогічно визначаються зони дозволеного доступу для випадку паралельно пов'язаних зон (рис. 2.5). Аналізуючи їх, можна сформулювати ще один принцип, яким повинні задовольняти алгоритми СКУД для послідовно-пов'язаних зон – монотонність.

Монотонність в СКУД базується на тому, що:

– категорія доступу кожної наступної із послідовно пов'язаних зон повинна бути вищою за попередню (в іншому випадку, коли категорія доступу нижча, то тоді немає необхідності в ТД, а зони можуть бути об'єднаними);

– суб'єкт доступу, який має і-й рівень доступу (що дозволяє переміщуватись через j-ту точку доступу), повинен мати і (і-1)-й рівень доступу (для $i > 1$).

Прикладом, який ілюструє першу частину, може бути схема на рисунку 2.4. У тому випадку, коли категорії доступу зон z_2 і z_3 однакові, то ці зони можуть бути об'єднані в одну. Те ж саме можна сказати про схему, яка наведена на рисунку 2.5 для будь-якої з пар зон, в які входять z_1 і одна з паралельних зон. Якщо категорія будь-якої пари зон збігається, то вони також можуть бути об'єднаними. Інший приклад (рис. 2.6) – зони, для яких повинні виконуватися сформульовані принципи це z_1, z_3, z_4. Винятком є той випадок, коли наявними будуть не менше двох зовнішніх точок доступу.

Прикладом коректнопризначених рівнів доступу, які будуть відповідати принципам монотонності можуть бути рівні доступу, які наведено у виразі (2.7). Прикладом некоректного рівня є запис $P_3(d_1, d_3)$ – тут дозволена третя ТД, але заборонена друга.

2.2 Графові та математичні моделі санкціонованих переходів

Трансформація сучасних архітектур безпеки в умовах цифровізації фізичних просторів вимагає переходу від статичних переліків прав доступу до динамічних реляційних моделей [109]. СКУД еволюціонували від простих механізмів автентифікації за ідентифікаторами до складних екосистем, де рішення про санкціонування переходу приймається на основі багатовимірного аналізу зв'язків між суб'єктами, об'єктами, часовими контекстами та фізичною топологією об'єкта. Графові моделі – фундаментом цієї еволюції, пропонуючи математичний апарат для опису складних ієрархій, транзитивних прав доступу та виявлення прихованих вразливостей у ланцюгах авторизації [27].

Традиційні підходи до управління доступом, такі як дискреційне (DAC) та мандатне (MAC) управління, тривалий час домінували в індустрії безпеки, проте їхня обмеженість стала очевидною при масштабуванні до рівнів сучасних підприємств. Впровадження рольового управління доступом (RBAC) у 1990-х роках стало значним кроком вперед, дозволивши групувати дозволи за функціональними обов'язками [111]. Проте RBAC стикається з феноменом «рольового вибуху», коли для специфічних комбінацій прав у великих організаціях доводиться створювати тисячі унікальних ролей, що робить адміністрування практично неможливим.

Графова парадигма вирішує ці проблеми, розглядаючи безпеку як мережу взаємопов'язаних сутностей. У графових моделях управління доступом (GBAC [24]) або реляційних моделях (ReBAC [66]) доступ визначається не статичним призначенням, а наявністю шляху в графі відносин. Це дозволяє моделювати організацію як семантичний граф, де вузли представляють людей, підрозділи, активи та фізичні зони, а ребра – типи зв'язків, такі як «керівник», «учасник проекту», «власник ресурсу» або «знаходиться в межах».

Застосування теорії графів у СКУД дозволяє використовувати метрики центральності для ідентифікації критичних вузлів інфраструктури, що є життєво важливим для запобігання несанкціонованим переходам та мінімізації наслідків компрометації окремих елементів [5].

2.2.1 Множини точок та зон доступу

У нашому випадку сукупність точок доступу d усієї СКУД може бути визначена множиною D, якій належать ці точки доступу $d \in D$. Зазвичай специфіка об'єктів (особливо середньої і великої місткості за кількістю

контрольованих зон) така, що об’єкт має декілька структурних підрозділів (цехи, корпуси тощо) яким притаманні різні категорії доступу до кожного з них. Отже, з урахуванням специфіки функціональних особливостей об’єкта СКУД володіє декількома підсистемами, які відрізняються категоріями доступу зон і, відповідно, різними рівнями доступу СД [25]. В загальному випадку множина D у свою чергу поділяється на I-підмножин Di до складу яких входять елементи di. Підмножини $D_i \subset D$ (i=1, ..., I) є власними підмножинами множини D.

Підмножини точок доступу D_i можуть як перетинатись, так і не перетинатись. Це залежить від того, чи мають згадані структурні підрозділи загальні зони доступу і, відповідно, загальні точки доступу. Враховуючи це можна записати такий вираз:

$$(D_1 \cup D_2 \cup ... \cup D_I)=D. \quad (2.8)$$

Слід врахувати, що для підмножин ТД, які не перетинаються $z_i \in Zj$, i=j; $z_i \notin Z_j$, $i \neq j$.

Вищеописаний математичний апарат доцільно подати на прикладах об’єктів зі пов’язаними зонами доступу, які наведено на рисунках 2.4 та 2.5. Відповідні підмножини D_1, D_2 і D_3 точок доступу d_i подано на рисунках 2.15 і 2.16.

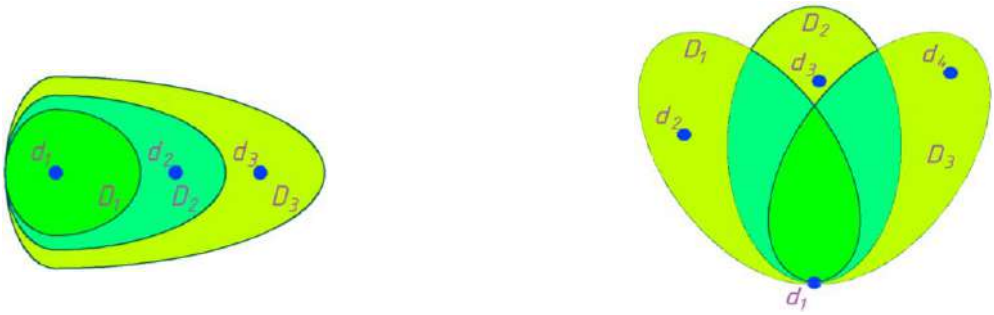
Аналогічно сукупність зон доступу z всій СКУД може бути визначена множиною Z, якій належать ці точки доступу $z \in Z$. З огляду на згадану вище специфіку об’єктів (кілька структурних підрозділів з різними категоріями доступу зон), множина Z розділяється на J підмножин Z_j з елементами z_j. Підмножини $Z_i \subset Z$, j=1, ..., J є власними підмножинами множини Z. Як і підмножини точок доступу, підмножини Z_j можуть бути як пересічними, так і непересічними, тобто $(Z_1 \cup Z_2 \cup ... \cup Z_J)=Z$. При цьому для непересічних підмножин $z_i \in Z_j$, $i = j$; $z_i \notin Z_j$, $i \neq j$. Проілюструємо вищесказане на прикладах об’єктів зі пов’язаними зонами доступу, наведеними на рисунках 2.15 та 2.16. Відповідні підмножини D_1, D_2, D_3 точок доступу Di показані на рисунку 2.15, а та 2.15, б, як діаграми Ейлера-Венна з різними зонами контрасту.

Для об’єкта, випадок якого подано на рисунку 2.4, підмножини D включатимуть (рис. 2.15, а) такі точки доступу:

$$(d_1) \in D_1; (d_1, d_2) \in D_2; (d_1, d_2, d_3) \in D_3. \quad (2.9)$$

Відповідно, для об’єкта (рис. 2.5) підмножини D_i можуть бути записані (рис. 2.15, б) у вигляді:

$$(d_1, d_2) \in D_1; (d_1, d_3) \in D_2; (d_1, d_4) \in D_3. \quad (2.10)$$



а) б)

Рисунок 2.15 – Підмножини точок доступу
а) – послідовно пов’язані зони; б) – паралельно пов’язані зони

З огляду на склад підмножин D_i, неважко зробити висновок, що вони перетинаються.

В обох прикладах підмножини D мають загальну точку доступу d_i, яка відповідає області перетину цих підмножин: $d_1(D_1 \cap D_2 \cap D_3)$.

Зрозуміло, що для загального випадку може бути притаманним й інший склад підмножин D_r. Для прикладу, на рисунку 2.16 підмножина D_2 включає в себе три точки доступу $(d_1, d_3, d_4) \in D_2$.

Аналогічне подання може бути використано й для підмножин Z_j зон.

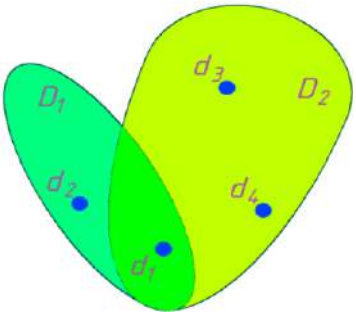


Рисунок 2.16 – Підмножина точок доступу

2.2.2 Подання СКУД у вигляді графа

В системі СКУД суб’єкт доступу може переміщатися з однієї зони в іншу через точки доступу. Таку систему можна подати за допомогою теорії графів. Переходи (переміщення) рій суб’єкта доступу можна трактувати як гілки графа. Якщо говорити про вершини графа, то тут можливі два підходи. Вони засновані на тому, що вибирається в якості вершин графа – зона або точка доступу.

Врахуємо, що система контролю доступу фіксує лише факт реєстрації в ТД. Однак, необхідно пам’ятати й те, що факт проходу через точку доступу може не реєструватися.

Тому в загальному випадку в системі КУД під час реєстрації суб'єкта доступу в ТД виникає невизначеність, в якій зоні реально знаходиться СД – з якої або в яку він переміщався. За факт можна прийняти лише те, що суб'єкт зареєструвався в і-й точці доступу. Отже, можна говорити про доцільність вибору ТД в якості вершин графа. Інший підхід, який використовує зони у якості вершин графа, також використовується на практиці.

Розглянемо граф (рис. 2.17), вершини якого будуть відповідати точкам доступу D_i, а ребра – переходам p_m між цими ТД. Іншими словами, перехід p_m можна уявити як ребро графа pm, яке з'єднує дві кінцеві вершини d_i та d_j графа точки доступу $p_m=(d_i, d_j)$. При цьому, сукупність можливих коректних переходів p_m, m=1, ..., M становить множину P.

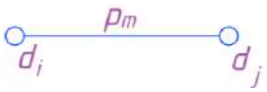


Рисунок 2.17 – Вершини та гілки графа

Таким чином, ребро визначає коректний перехід між двома точками доступу, тобто можливість санкціонованого переміщення СД в системі. Некоректні переходи повинні контролюватися іншими засобами комплексної системи безпеки, наприклад охоронною сигналізацією або відеоспостереженням. Тоді граф буде визначатися відповідними множинами точок доступу і коректних переходів між ними G=(D, P).

Якщо два ребра графа (переходу) мають загальну кінцеву вершину (точку доступу), то їх називають суміжними. Ребра з однаковими кінцевими вершинами – паралельними. У СКУД це відповідає наявності декількох шляхів переміщення між одними і тими ж точками доступу. Якщо в СКУД немає декількох шляхів переміщення між двома ТД, то граф називається простим.

Маршрут СД в графі G=(D, P) являє собою кінцеву послідовність точок доступу, які чергуються і переходів між ними d_0, p_1, d_l, p_2, ..., d_{n-1}, p_n, d_n, при цьому d_{n-1} та d_n є кінцевими вершинами ребра p_n.

Маршрут прийнято вважати відкритим, якщо його кінцеві вершини різні, в іншому випадку – замкнутий. У тому випадку коли він розпочинається і закінчується в різних зовнішніх точках доступу, то квазізамкненим.

З точки зору СКУД граф може бути:

– неорієнтованим або ненаправленим, якщо ТД допускає коректні переміщення в будь-якому напрямку;

– орієнтованим або спрямованим, якщо переміщення через ТД допускається лише в одному напрямку;

– змішаним.

Граф прийнято називати пленарним, у тому випадку, якщо його можна накреслити на площині таким чином, що його ребра перетинаються тільки у вершинах. Слід пам’ятати, що основна частина СКУД може бути представлена пленарними графами.

Порядок графа визначається кількістю вершин, тобто точок доступу (або кількістю елементів множини D). На рисунку 2.18 наведено приклад графа для об’єкта, який подано на рисунку 2.5. Вихідна зона вільного доступу позначена як нульова точка доступу.

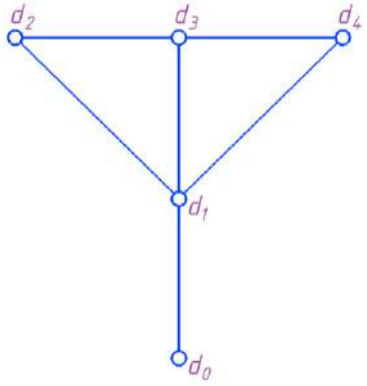


Рисунок 2.18 – Граф СКУД з паралельно пов’язаними зонами

Розглянемо, деякий об’єкт, який має два поверхи, план якого подано на рисунку 2.19.

У лівій частині будівлі розташований головний вхід із зони вільного доступу, контрольований точкою доступу d_1. У правій – аварійний (пожежний) вихід (точка доступу d_{11}). Двері пожежного виходу, закриті в штатній ситуації, розблоковуються під час спрацювання системи пожежної сигналізації, забезпечуючи вільний вихід для усіх суб’єктів системи.

На першому поверсі розташовані кабінети керівників $КР_1$ і $КР_2$. Доступ до них здійснюється з коридору $К_1$ через приймальню П. Контроль доступу до приймальні й кабінети реалізується відповідно точками доступу d_2, d_3 і d_4. З коридору $К_1$ доступний прохід до кімнати переговорів КП через ТД d_5.

На другому поверсі розташовано комерційний відділ. Для контролю проходу в коридор встановлено точку доступу d_6. Доступ в робочі кабінети відділу $Р_1$, $Р_2$ контрольованого (в межах відділу) доступу (d_7, d_8) і не контрольованого $Р_3$ здійснюється з коридору $К_2$. При цьому, доступ в кабінет $Р_3$ вільний з коридору $К_2$ (в тому числі і для осіб, які мають доступ до кімнат $Р_1$ та $Р_2$).

Як з коридору $К_1$, так і $К_2$ в аварійній (пожежної) ситуації можливо вийти через відповідні точки доступу d_9 і d_{10}, які стають автоматично доступними в надзвичайній ситуації.

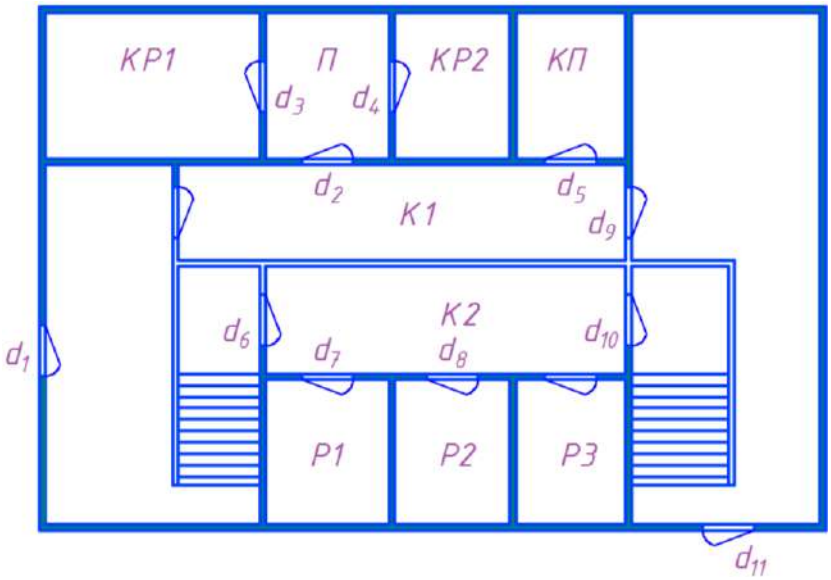


Рисунок 2.19 – План контрольованого об’єкта [110]

Для розглянутого прикладу притаманні три підсистеми КУД. Дві контролюють перший і другий поверхи. Третя – аварійна, контролює пожежні виходи (в правій частині будівлі).

Взаємозв’язок точок доступу, в загальному вигляді, може бути представлений графом, гілки якого визначають можливі шляхи переміщення суб’єктів через точки доступу (тобто можливі коректні маршрути проходження системи КУД). На рисунку 2.20 представлено планарний граф, цього об’єкту, який визначає взаємозв’язок множини ТД.

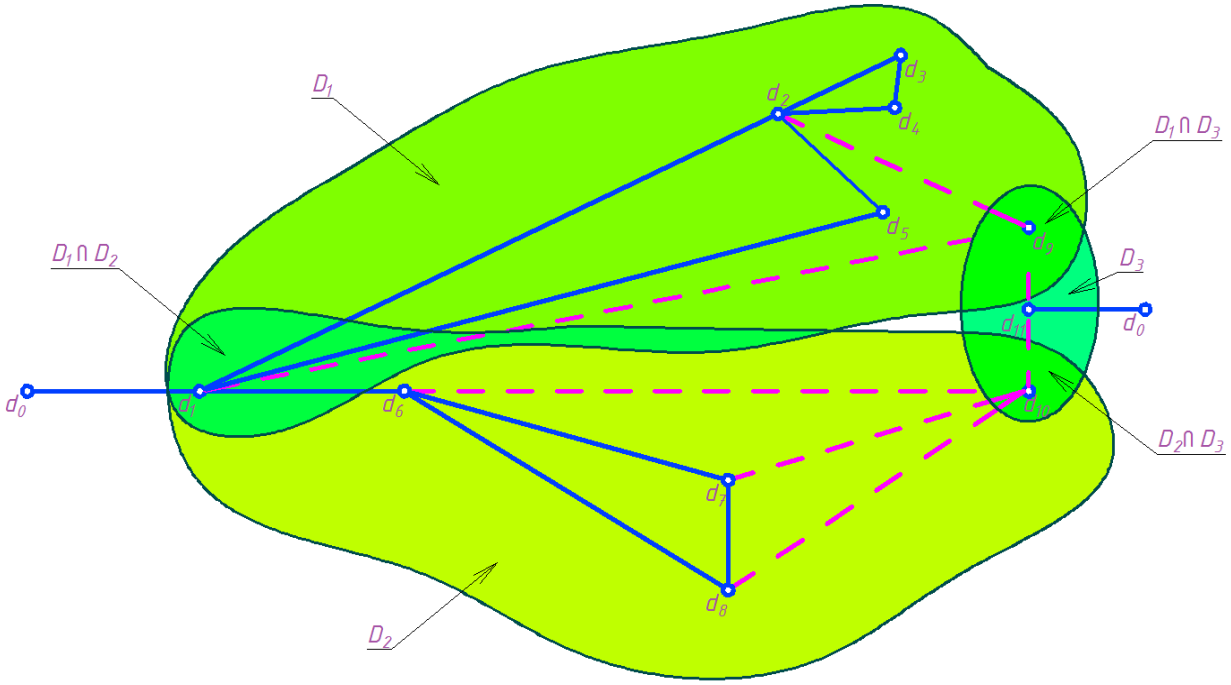


Рисунок 2.20 – Граф, який визначає взаємозв’язок точок доступу [110]

На графі діаграмами Ейлера-Венна різним відтінками показано взаємозв'язок підмножин D_i (підсистем) множини точок доступу D розглянутої СКУД. У даному прикладі маємо три пересічних підмножини точок доступу.

Перетин першого D_1 і другого D_2 визначає головний вхід як загальну точку доступу d_1.

Таким чином, точка доступу d_1 належить як підмножині D_1, так і D_2, тобто:

$$d_1 \in (D_1 \cap D_2). \quad (2.11)$$

Окрім цього, перетинаються й підмножини D_1 і D_3 аварійної підсистеми, а також D_2 і D_3:

$$d_9 \in (D_1 \cap D_3);\ d_{10} \in (D_2 \cap D_3). \quad (2.12)$$

Відповідність рисунку 2.19 до 2.20 пояснюється накладанням відтінків відповідних діаграм Ейлера-Венна на графі і приміщень на плані об'єкта. Ребра графа з кінцевими вершинами d_9, d_{10} та d_{11}, тобто переходи, які використовуються лише в аварійній ситуації, позначені пунктиром. Розглянутий граф – це неорієнтований планарний граф 11-го порядку.

2.2.3 Моделювання графів атак та вразливостей

Моделювання графів атак та вразливостей для СКУД дозволяє візуалізувати та математично обґрунтувати ризики несанкціонованого проникнення. Оскільки СКУД поєднує фізичну безпеку та IT-інфраструктуру (контролери, сервери, БД), графові моделі стають незамінними для пошуку «найслабшої ланки».

Графи атак представляють собою спеціалізований інструментарій (табл. 2.2), де вузли відповідають станам системи або вразливостям, а ребра – можливим діям порушника для переходу між станами. Автоматизація генерації графів атак звільняє адміністраторів від трудомісткої ручної роботи та дозволяє виявляти багатоступеневі сценарії вторгнення, які неможливо помітити при аналізі окремих компонентів. Залежності між вразливостями моделюються як ієрархічні зв'язки – задоволення однієї умови (наприклад, отримання доступу до сервісного тамбура) є пререквізитом для експлуатації наступної вразливості.

Для строгої верифікації безпеки СКУД застосовуються структури Кріпке, які дозволяють описати систему як множину станів та переходів. Формально граф атак AG визначається наступним набором чинників:

$$AG=(S, s_0, \Sigma, R, V, W), \quad (2.13)$$

де S – скінченна множина станів системи та зловмисника;

s_0 – початковий стан (наприклад, зловмисник поза межами об’єкта);

Σ – набір міток атак (наприклад, експлуатація CVE-xxxx);

R – відношення переходів;

V – функція маркування станів атомарними пропозиціями;

W – підмножина цільових станів зловмисника.

Таблиця 2.2 – Характеристика графу атак та вразливостей

Метрика графа	Застосування в СКУД	Значення для безпеки
Щільність графа	Оцінка надмірності прав доступу	Висока щільність вказує на потенційне порушення принципу найменших привілеїв
Центральність вузла	Визначення ключових точок ідентифікації	Допомагає оптимізувати розміщення постів охорони та камер
Коефіцієнт кластеризації	Виявлення груп користувачів з ідентичними ролями	Спрощує впровадження рольового управління доступом
Досяжність	Перевірка відсутності шляхів до критичних зон для певних груп	Основа для доведення безпеки системи

СКУД характеризується асинхронністю та паралелізмом – декілька зчитувачів можуть обробляти запити одночасно, а зловмисник може виконувати паралельні атаки на різні компоненти інфраструктури. Мережі Петрі забезпечують вищу експресивність для цих сценаріїв порівняно з деревами атак. Позиції у мережі Петрі моделюють передумови (наявність підключення до підмережі контролерів), а переходи – власне, виконання атаки.

Ієрархічний підхід до побудови мереж Петрі дозволяє створювати масштабні моделі критичних інфраструктур, де окремі підмережі описують логіку роботи зчитувачів, серверів управління та засобів мережевого захисту [67]. Це важливо для великих об’єктів, де кількість вузлів у графі атак може сягати тисяч, що робить ручний аналіз неможливим.

Для перетворення графа атак з візуальної схеми на інструмент прийняття рішень необхідно інтегрувати кількісні параметри [7]. Найбільш вживаним методом є використання метрик CVSS для розрахунку ймовірності успіху кожного кроку атаки.

2.2.4 Математична модель процесу ідентифікації

За наведеною на рисунку 2.1 структурною схемою СКУД формалізуємо процеси зчитування та обробки інформації, які у ній відбуваються. Ідентифікаційні ознаки m-го СД/ОД визначаються в загальному матрицею X

параметрів ІО або функцій, які їх характеризують. Нехай М – кількість інформаційних ознак, а К – максимальна кількість параметрів однієї з ознак. Тоді матриця отримає наступний вигляд:

$$X = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{K1} \\ x_{12} & \dots & \dots & x_{K2} \\ \dots & x_{km} & \dots & \dots \\ x_{1M} & \dots & \dots & x_{KM} \end{bmatrix}. \qquad (2.14)$$

Елемент x_{km} являє собою k-й параметр (функцію) m-ої ознаки. Кількість параметрів різних ІО може бути різною, тобто частина елементів матриці X може бути рівною нулю. Зчитувач СКУД перетворює інформаційні ознаки x_{km} з фізичними носіями в сигнал z_{km}, який буде придатним для подальшої обробки контролером. Алгоритм перетворення визначається оператором F з виразу (2.1), де

$$Z = \begin{bmatrix} z_{11} & z_{12} & \dots & z_{K1} \\ z_{12} & \dots & \dots & z_{K2} \\ \dots & z_{km} & \dots & \dots \\ z_{1M} & \dots & \dots & z_{KM} \end{bmatrix}. \qquad (2.16)$$

В окремому випадку для однієї ІО матриця Z буде являти собою матрицю-рядок. Наприклад, для числового пароля з шести цифр 052830 відповідні елементи єдиного рядка матриці Z будуть збігатися з цифрами введеного пароля Z=[052830].

Зауважимо, що в загальному випадку критерії порівняння можуть бути різними для різних ІО одного і того ж СД/ОД.

Контролер проводить порівняння за певним алгоритмом матриці Z з еталонними Z_{i0} (i – порядковий номер суб'єкта доступу i=1, ..., I; 0 – кількість суб'єктів доступу), які зберігаються в БД. Критерій порівняння позначаємо оператором C, який повинен враховувати можливі допуски ΔZ на зміну значень параметрів ІО, які схильні до випадкових змін в силу об'єктивних чи суб'єктивних обставин (наявність шумів впливу перешкод, тимчасові зміни ідентифікаційних ознак). У загальному випадку контролер порівнює матрицю Z з усіма зразками Z_{i0} по черзі, тим самим визначаючи номер і суб'єкт доступу,

який володіє цим ідентифікатором, або фіксує відсутність еталона Z_{i0}, відповідно пред'явленому Z. Критерії порівняння можуть бути різними для різних інформаційних ознак одного і того ж СД/ОД.

На підставі результатів порівняння (за знайденим значенням і) та інформації про рівень доступу і-го СД/ОД, які зберігається в базі даних, контролер формує матрицю P_i вихідних сигналів за витразом (2.2):.

До складу цих сигналів, перш за все, входять сигнали, які управляють виконавчими пристроями.

Рівень доступу СД визначає дозволені зони доступу, а також тимчасові та календарні інтервали доступу (тобто коли, куди, до чого дозволено доступ). Для детермінованої системи, якою є СКУД, це визначає реакцію системи на дії СД. Тобто процедуру функціонування загороджувальних пристроїв, які у свою чергу приводяться в дію виконавчими пристроями.

З огляду на, те що більшість сучасних СКУД використовують цифрову обробку, на виході зчитувача отримують матрицю Z, елементи якої будуть являти собою цифри в тій або іншій системі числення. В цьому випадку алгоритм порівняння С, для багатьох випадків, спрощується та зводиться до порівняння елементів матриць Z і Z_{eo}, метою якої є виявлення співпадіння з еталонною. Або необхідно визначити значення і, за якого буде виконуватись умова:

$$Z-Z_{eo}=0. \qquad (2.18)$$

Однак, в загальному випадку це залишиться багатоальтернативною перевіркою гіпотез виявлення, оцінки параметрів або розпізнавання образів.

Контрольні запитання

1. На які класи, за технічними характеристиками та ступенем захисту від небажаного доступу, прийнято поділяти СКУД?
2. Опишіть рівні мережевої взаємодії, які використовують під час побудови мережевих СКУД.
3. Поясніть сутність базових принципів функціонування СКУД.
4. У чому полягає відмінність між точками доступу з одностороннім та двостороннім контролем?
5. У чому полягає головна відмінність СКУД 4-го класу в контексті програмного забезпечення та управління в надзвичайних ситуаціях?
6. У чому полягає принцип «монотонності» в СКУД?
7. Чим відрізняється СКУД 2-го класу від 1-го в плані реєстрації подій та режимів роботи?

8. Чому мережі Петрі, під час моделювання сучасних СКУД, прийнято вважати більш ефективнішими за дерева атак?

9. Чому традиційні моделі стають неефективними під час масштабування на рівні сучасних великих підприємств?

10. Що являє собою «маршрут суб’єкта доступу»?

11. Що являє собою «рольовий вибух»? В контексті якої моделі управління доступом він виникає?

12. Що являє собою планарний граф та чому його вважають основою для опису фізичної топології СКУД?

13. Що являє собою пристрій управління доступом?

14. Як визначається рівень вкладення зони у порівнянні із зоною вільного доступу?

15. Як математично можна виразити «рівень доступу» суб'єкта та які параметри він включає у себе?

16. Як теорія графів допомагає виявляти критичні вузли інфраструктури безпеки?

17. Яка різниця між «простою», «взаємопов’язаною» та «вкладеною» зонами доступу?

18. Яка різниця між відкритим, замкнутим та квазізамкнутим маршрутами суб'єкта доступу?

19. Яким чином можна інтегрувати метрики CVSS у графові моделі атак для прийняття управлінських рішень?

20. Які основні елементи повинна включати у себе СКУД для вирішення завдань контролю доступу?

21. Які основні задачі СКУД вирішує тактика доступу за типом «шлюз»?

22. Які типи графів, залежно від напрямку дозволеного руху через точки доступу, використовуються в СКУД?

23. Яку роль відіграють діаграми Ейлера-Венна в описі підмножин точок доступу та зон?

РОЗДІЛ 3. Фізика процесів та технології ідентифікації

3.1 Основні методи та типи ідентифікації

Як із практичної точки зору реалізації, так й з позиції захищеності від основних загроз несанкціонованих дій в загальній групі носіїв ідентифікаційних ознак прийнято виділяти: копіювання, примус, крадіжка носія, втрата або передача його іншій особі (останні загрози дуже реальні та дозволяють, у ряді випадків, достатньо просто, несанкціоновано, подолати СКУД).

Отже, для ідентифікування слід використовувати [68]:

– матеріальний носій, предмет (ключ, картка, радіобрелок, номерний знак автомобіля), який у загальному випадку не пов’язаний безпосередньо із суб’єктом доступу, на який нанесено ідентифікаційні ознаки;

– знання суб’єкта (наприклад, буквено-цифровий пароль, який є ідентифікаційною ознакою);

– суб’єкт або об’єкт доступу – його характерні й, за можливістю, унікальні індивідуальні особливості (відбиток пальців, долоні, вен сітківки ока для людини тощо), які можуть бути інформаційними ознаками.

Коли мова йде про контроль доступу суб’єктів, то використовують наступні принципово різних методи, які засновано на тому, що:

– користувач має;
– користувач запам’ятовує;
– характеризує його як особистість.

До ідентифікаторів, які використовують перший метод, зазвичай відносять карти доступу з різними фізичними принципами запису інформації (ідентифікаційних ознак), брелки, пропуски тощо.

В якості запам’ятовування користувач, найбільш широко, використовує різні літери та цифри (пароль), які набирають на клавіатурі СКУД.

Для останнього методу характерним є дві групи біометричних ознак. Перша – квазістатичні ознаки, які мало змінюються у часі (наприклад, форма обличчя, відбитки пальців або долоні тощо). Друга – квазідинамічні ознаки, які напряму залежать від часових змін (форма і динаміка нанесення підпису, спектральний склад мови, тип ходи, параметри пульсу тощо).

3.1.1 Імітаційна стійкість та криптозахист СКУД

Розглянемо можливість несанкціонованих дій з носіями ІО, які можуть зашкоджувати роботі СКУД. Такі дії, зазвичай, полягають у спостереженні, маніпулюванні, копіюванні, примушуванні, пошкодженні.

Відповідно до чинних нормативних документів визначення цих термінів варто розуміти в наступному контексті:

– спостереження – це дії, які виконуються з пристроями контролю і управління доступом без прямого доступу до них, їх метою є отримання дійсного коду;

– знімання інформації – цей термін має більш ширше значення оскільки мова іде не лише про спостереженням за набором коду на клавіатурі, але й знімання інформації (наприклад, за радіоканалом для безконтактних карт, які працюють за таким же принципом дії);

– маніпулювання – це дія, яка виконується із пристроями контролю доступу без їх руйнування, її метою є отримання чинного коду або приведення у відкритий стан загороджувального пристрою;

– маніпулювання – це дія, яка включає у себе роботу над програмним забезпеченням;

– копіювання – це дія, яка виконується з ідентифікаторами, її метою є отримання копії ідентифікатора з дійсним кодом;

– примушування – насильні дії над суб'єктом, який має право доступу, з метою несанкціонованого проникнення через керовані загороджувальні пристрої (при цьому пристрої контролю й керування доступом функціонують нормально);

– пошкодження – руйнівний вплив ідентифікатора як без використання відповідних інструментів, так і за їх допомогою.

Варто зауважити, що в нормативних документах немає жодної згадки про небезпечний, з точки зору подолання СКУД, вид несанкціонованого доступу, як крадіжка ідентифікатора.

3.1.2 Захищеність ідентифікатора

Під захищеністю ідентифікатора необхідно розуміти прихованість його використання, стійкість до несанкціонованих дій, складність знімання інформації про ідентифікаційні ознаки та їх параметри й використання цієї інформації або самого ідентифікатора для несанкціонованих дій в СКУД.

Аналіз захищеності та вразливості різних носіїв ІО від несанкціонованого доступу дозволяє зробити висновок, що для будь-яких способів реалізації вище згаданих методів найбільш небезпечним є примус, тобто насильницькі дії над суб'єктом, яка має право доступу [134].

Матеріальний носій можна втратити, викрасти або передати іншій особі. Таким чином, з точки зору несанкціонованого заволодіння та використання носія цього типу СКУД не сильно захищені. Окрім крадіжки, для деяких способів реалізації першого методу, становить небезпеку й копіювання носія ІО. Для методу, який використовує пам'ять користувача, найбільш небезпечним є знімання інформації, зокрема за візуальним каналом. Також, практично неконтрольованою є передача пароля власником іншій особі. Ще одним небезпечним чинником є маніпулювання (наприклад, підбір пароля за відсутності захисту від цього).

Найбільшої захищеності досягають під час використання біометрії.

На практиці доцільно подавати й шляхи покращення захищеності засобів, які базуються на різних методах ідентифікації, відносно різних загроз. В таблиці 3.1 подано порівняння існуючих методів за стійкістю до різних видів несанкціонованих дій.

Як бачимо, деякі позиції таблиці містять діапазон змін, оскільки ступінь захищеності буде залежати від обраного технічного способу реалізації методу та його параметрів.

Таблиця 3.1 – Порівняння методів захисту СКУД за стійкістю інформаційних ознак до різних видів несанкціонованих дій

Основа методу ідентифікації	Захищеність від НСД						Можливість автентифікації
	Викрадання	Знімання інформації	Маніпулю-вання	Копіюван-ня	Примус	Пошкод-ження	
Те, що користувач має	Н	В	В	Н…В	Н	Н…В	Н
Те, що користувач знає	В	Н	…С…В	В	Н	Н…В	Н
Те, що характери-зує користувача	В	В	В	П…В	Н	Н…В	В
Примітка: Н – низька; С – середня; П – підвищена; В – висока.							

3.1.3 Класифікація ідентифікаторів

Ідентифікатори, зазвичай, класифікують за рядом ознак, які пов’язані, перш за все, зі способом технічної реалізації та безпосередньо залежать від принципу їх роботи [130].

До числа таких ознак можна віднести:

1. За способом взаємодії ідентифікатора та зчитувача:
   – безконтактні (дистанційної дії);
   – контактні (із безпосередньою взаємодією).
2. За технологією нанесення/зчитування або передачі/приймання інформації (фізичним принципом дії):
   – магнітні;
   – оптичні;
   – радіочастотні;
   – штрих-коди;
   – проксіміті-технологія;
   – смарт-технологія;
   – технологія Віганда (Wiegand);
   – механічне кодування;
   – тач-меморі (touch-memory);
   – біометричний (квазістатичний і квазідинамічний);
   – кодонабірні способи.

Оскільки найбільш важливою ознакою прийнято вважати фізичний принцип дії, від якого багато в чому залежать експлуатаційні характеристики як

ідентифікатора, так і зчитувача, то в подальшому за основу необхідно використовувати фізичний принцип дії. Однак, слід пам’ятати, що це не виключає, а навпаки вимагає враховувати як метод ідентифікації, так і спосіб його технічної реалізації під час вибору ідентифікатора для СКУД.

3.2 Магнітне кодування та ефект Віганда

У 1975 році американцем Джоном Вігандом (John R. Wiegand) було відкрито ефект швидкої зміни магнітних полів за допомогою спеціально оброблених феромагнітних дротиків малого діаметра та їх реєстрацію [19]. Конструкція чутливого елемента запатентована, а для формування сигналів вимагає усього лише декілька простих елементів – пару постійних магнітів з котушкою котушку індуктивності, яка розташовується між магнітами, уздовж яких переміщуються відрізки дрота Віганда.

На початку вісімдесятих років стали випускати карти і зчитувачі, засновані на Wiegand-ефекті. Джон Віганд і Мілтон Велінський розробили метод пасивного кодування, який кардинально відрізнявся від популярних тоді карток з магнітною смугою [61]. Приклад такої карти наведено на рисунку 3.1.

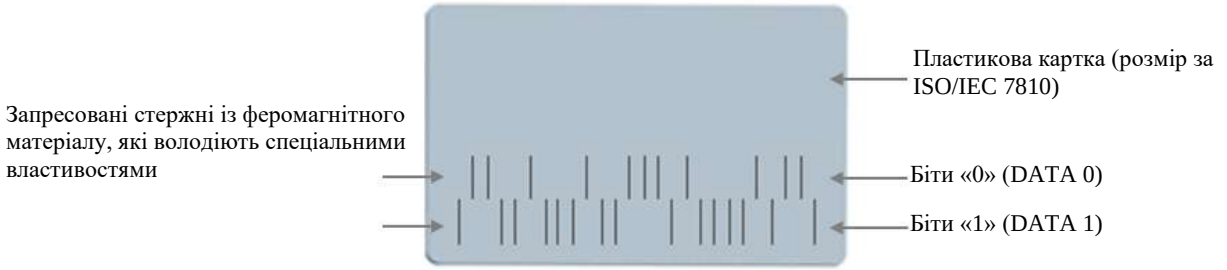


Рисунок 3.1 – Карта Віганда [110]

У встановленому місці пластикової карти товщиною 0,76 мм запресовано два ряди відрізків дротиків Wiegand. Слід зауважити, що у зчитувачі передбачено чутливі елементи для кожного з рядів.

Кількість відрізків та відстань між ними визначають ідентифікаційний код картки. На практиці прийнято використовувати 26-бітові коди, які й визначають кількість відрізків дротиків в карті [9]. Її інформаційна ємність визначає 67108864 можливих комбінацій та зводить до мінімуму ймовірність формування двох карт із однаковим номером (теоретично ймовірність менша за 2×10-8). Враховуючи вищесказане, можна зробити висновок про те, що картки Віганда слід віднести до карт з рівнем підвищеної стійкості до несанкціонованих дій (не менше 107).

3.2.1 Ефект Wiegand

Дротики Віганда виготовляють із холоднообробленого феромагнітного

дроту на основі сплаву кобальту, заліза та ванадію, діаметр яких не перевищує 0,2 мм. Процес холодної обробки складається із великої кількості етапів скручування та розкручування дроту в напруженому стані. Така обробка дозволяє отримати максимальну деформацію в поверхневому шарі дроту. Як наслідок, магнітні властивості дротика будуть змінюватись за відношенням від відстані до центру. Така процедура призводить до того, що у дротиках Віганда формується магнітомяка серцевина (стержень), якій притаманна оболонка із високою коерцитивної силою. Під час взаємодії з дротом Вігандат зовнішнього поздовжнього магнітного поля достатньої напруженості магнітне поле стержня перемикає свою полярність, формуючи Wiegand-імпульс.

Петля гістерезису дротика Віганда складається із великої кількості дискретних переходів, які формуються під час перемикань полярності стержня та оболонки. Ці переходи відомі як ефект Баркґаузена, суть якого полягає у тому, що феромагнетики, перебуваючи в магнітному полі, напруженість якого змінюється безперервним чином, змінюють свою намагніченість дискретно. Швидкість цієї зміни настільки висока, що в котушці, намотаній навколо дроту, індукується значний імпульс напруги. Згідно з законом Фарадея, напруга пропорційна швидкості зміни магнітного поля:

$$V \infty (d\Phi/dt). \qquad (3.1)$$

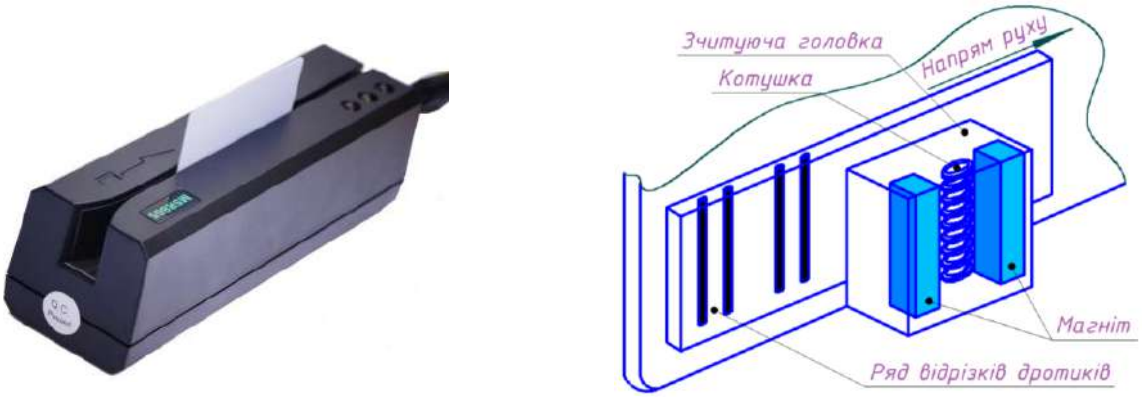
Завдяки надзвичайно високому значенню dt у дроті Віганда, вихідна напруга може бути на кілька порядків вищою, ніж у аналогічних котушках з невігандівським осердям. Це дозволяє створювати пасивні датчики, які генерують електричний сигнал без зовнішнього живлення.

Однією з найбільш цінних характеристик ефекту Wiegand є незалежність параметрів імпульсу від швидкості зміни зовнішнього поля. На відміну від класичної електромагнітної індукції, де напруга падає при сповільненні руху магніту, дріт Віганда генерує ідентичний за амплітудою та тривалістю імпульс незалежно від того, наскільки швидко або повільно змінюється полярність. Це дозволяє зчитувати дані навіть при надзвичайно повільному проведенні картки через зчитувач.

Енергія одного імпульсу, що виникає при переполюсовці 15-міліметрового відрізка дроту, становить приблизно 200 наноджоулів. Цього обсягу достатньо для активації малопотужних електронних схем, що відкриває широкі можливості для систем збору енергії.

Існує два способи формування Wiegand-ефекту – симетричне і асиметричне магнітні перемикання. За симетричного перемикання для намагнічування й активізації Wiegand-дроту використовують магнітні поля

однакової напруженості й протилежної полярності. Ці поля формуються, наприклад, постійними магнітами, які встановлено в стаціонарній голівці зчитувача (рис. 3.2, б). При цьому Wiegand-дротики переміщаються відносно неї.



а) б)

Рисунок 3.2 – Кардрідер [110]
а) – загальний вигляд зчитувача; б) – будова зчитувача

На початку насичуюче магнітне поле першого магніту однієї полярності орієнтує полярності стержня та оболонки в одному напрямку (етап А, рис. 3.3). За ходом переміщення дротиків до наступного магніту протилежної полярності змінюється полярність прикладеного до них поля. Під час наближення до другого магніту напруженість знову прикладеного зовнішнього поля збільшується. Це призводить до того, що спочатку переключається полярність стержня (етап Б, рис. 3.3) та генерується імпульс напруги в котушці зчитувача. Потім, за подальшого збільшення напруженості поля (в міру наближення до другого магніту), перемикається полярність оболонки, генеруючи імпульси напруги менші за розміром. Амплітуда цього імпульсу значно менша за попередню (на порядок і більше). В результаті магнітне поле другого магніту повністю насичує Wiegand-дротика.

За асиметричного режиму перемикання дротик Віганда намагнічується і активізується магнітними полями протилежної полярності та різної інтенсивності. Насичуючи магнітне поле першого, більш потужного магніту однієї полярності орієнтує полярність стержня й оболонки в одному напрямку. Після чого поле іншого магніту протилежної полярності, але уже меншої напруженості перемикає полярність стержня (але не оболонки) і тим самим формує імпульс напруги меншої амплітуди в котушці зчитувача. Після цього насичуюче поле відновлює попередню полярність, одночасно перемикаючи полярність намагніченості стержня, формуючи імпульс більшої амплітуди. Слід

зауважити, що через простоту підбору постійних магнітів, в більшості випадків, користуються режимом симетричного перемикання.

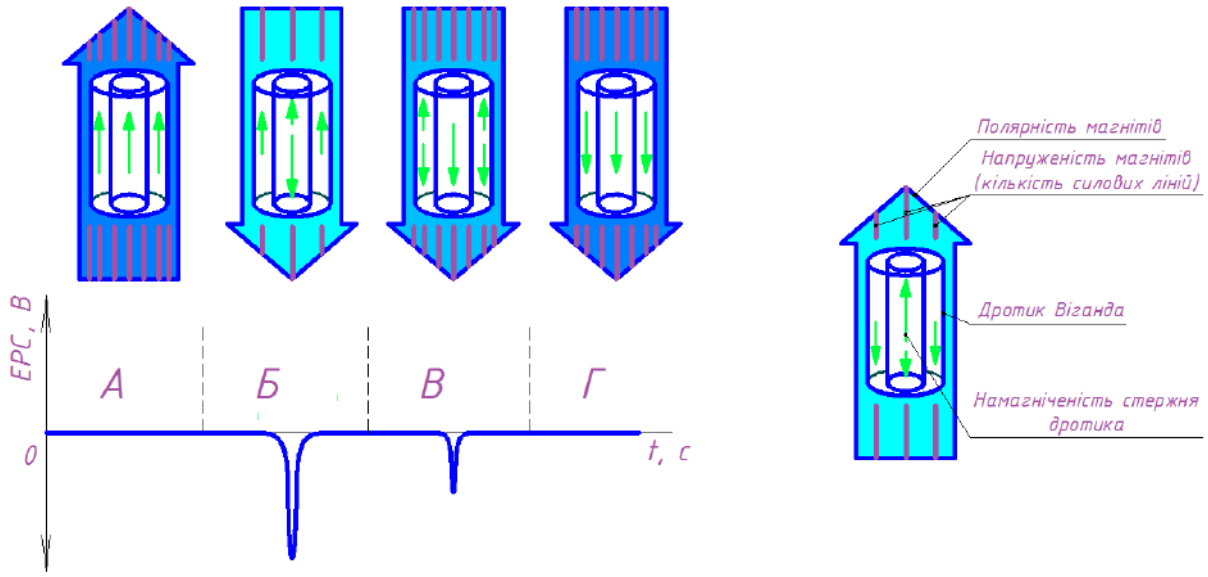


Рисунок 3.3 – Процес формування сигналів [110]

Під час магнітного перемикання Wiegand-дротика в котушці зчитувача наводиться ЕРС індукції тривалістю близько 10 мкс (рис. 3.4). Амплітуда ЕРС індукції котушки знаходиться в межах від 2 до 8 В залежно від конструкції головки зчитувача та опору навантаження. При цьому, амплітуда ЕРС індукції не залежить від напруженості (якщо його значення більше напруженості насичення) і полярності поздовжнього магнітного поля. Зазор між головкою зчитувача і дротиками Віганда, зазвичай, не перевищує 1,3 мм.

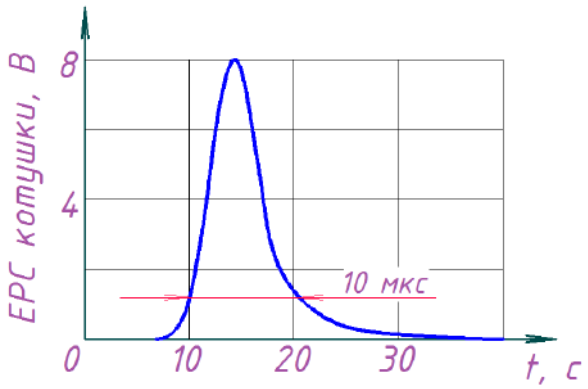


Рисунок 3.4 – Імпульс ЕРС котушки зчитувача

На практиці зустрічаються різні варіанти виконання зчитувачів. Окрім розглянутого, зустрічаються й такі варіанти конструкції зчитувачів де використовується одна зчитуюча головка для обох рядів відрізків дротиків (з одним магнітом і котушкою на кожен ряд) та одним загальним насичуючим

магнітом, який розташовують поблизу головки з протилежною полярністю відносно магнітів головки. Загальний магніт встановлюють так, щоб можна було поляризувати усі відрізки дротиків відносно їх проходження перед головкою.

3.2.2 Області застосування

На основі Wiegand-ефекту, окрім СКУД, працюють деякі типи лічильників витрат газів, рідин, давачів швидкості, вимірювачів положення тощо (в тому числі давачі, які використовують в системах управління машинами та механізмами).

Wiegand-ефект спостерігається при температурі від -80 до +260°С. Діапазон робочих температур конкретного типу пристрою визначається властивостями застосованих у ньому елементів й не залежить від властивостей Wiegand-дротиків.

За відповідної конструкції головки та розташуванні котушки відносно магнітів можна додатково контролювати напрям переміщення дротиків Віганда шляхом аналізу полярності Wiegand-імпульсів.

До переваг пристроїв, які працюють на основі Wiegand-ефекту можна віднести:

– відсутність зовнішнього джерела живлення та двохпровідникове підключення зчитуючої головки;

– спосіб зчитування, який виключає механічне зношування деталей зчитуючої головки;

– високу надійність, яка обумовлена простотою конструкцій карт Віганда та зчитувачів;

– високу стійкість карт Віганда до зовнішніх впливів (у тому числі електричних та магнітних);

– неможливість підроблення карт поза заводських умов (недоступність інформації про технологію виготовлення дроту й використання матеріалів та послідовність розташування відрізків Wiegand-дроту).

Незважаючи на свою монументальність, технологія Wiegand сьогодні вважається однією з вразливих ланок у системі фізичної безпеки об’єкта. Основна проблема полягає в тому, що стандарт розроблявся в епоху, коли питання кібербезпеки та шифрування не були пріоритетними для локальних дротових систем.

Основні недоліки протоколу наступні:

– відсутність шифрування (дані по лініях DATA0 та DATA1 передаються у вигляді простого тексту і будь-який пристрій, підключений до дротів, може «прослухати» номер картки);

– одностороння комунікація (зчитувач лише відправляє дані, а контролер не може відправити команду назад чи перевірити стан зчитувача, а це робить систему «сліпою» до маніпуляцій);

– відсутність автентифікації пристрою (контролер приймає будь-які імпульси на своїх входах як валідні дані від зчитувача, а це дозволяє легко імітувати роботу зчитувача стороннім пристроєм);

– сприйнятливість до фізичного втручання (якщо зчитувач встановлено на зовнішній стіні будівлі, зловмисник може демонтувати його, отримавши доступ до дротиків).

3.2.3 Характеристики інтерфейсу

За великої кількості виробників ідентифікаторів та зчитувачів, які використовують різні фізичні принципи дії, важливим залишається питання сумісності цих пристроїв.

Оскільки, переважна більшість СКУД використовувала Wiegand-зчитувачі, то інтерфейс для передачі даних від зчитувача до контролера (Wiegand-інтерфейс) став «де-факто» стандартом серед виробників контролерів. На сьогоднішній день практично усі сучасні контролери та зчитувачі, в тому числі магнітних і proximity-карт, підтримують інтерфейс Wiegand.

Інтерфейс визначає сумісність різних пристроїв за електричними параметрами й формат представлення даних. Він використовує дві сигнальні лінії, по одній з яких передаються імпульси, які відповідають «0» двійкового коду даних, а по іншій – «1». Зчитувач містить схему, яка перетворює електричні параметри інтерфейсу та формат представлення даних від елемента, який зчитує (магнітна головка зчитувача, схема безконтактного зчитування тощо) у відповідні параметри Wiegand-інтерфейсу.

Для узгодження швидкості надходження інформації від зчитувального елемента із швидкістю приймання інформації контролером використовують буфер. Швидкість, з якою дані передаються на контролер є фіксованою та не залежить від швидкості пред’явлення карти й швидкодії електронної схеми зчитувача.

У нормальному стані на обох сигнальних лініях інтерфейсу утримується потенціал +5 В (відносно загального дротика). Під час передачі біта даних сигнальна лінія з’єднується із загальним дротиком (потенціал 0 В). Рівні сигналів відповідають логічним рівням транзисторно-транзисторної логіки (ТТЛ). Типова тривалість імпульсу 20 … 100 мкс, а інтервалу між імпульсами 0,2 … 200 мкс (значення тривалості можуть відрізнятися в залежності від виробників зчитувачів).

Пакети даних від різних карт відокремлюються одна від одної часовими інтервалами (близько 500 мкс). На рисунку 3.5 показано часову діаграму на

виході зчитувача під час передачі двійкового числа «01101». Кожен імпульс відповідає зміні логічних рівнів напруги з +5 до 0 В.

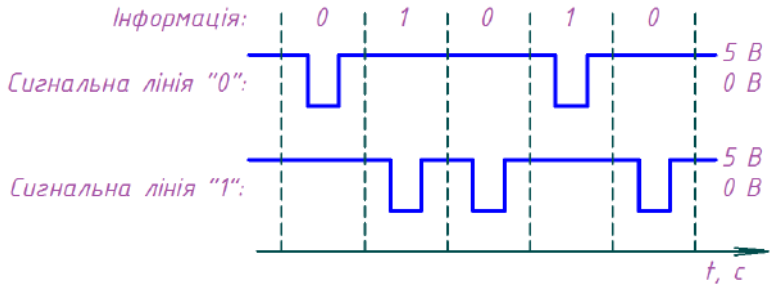


Рисунок 3.5 – Часова діаграма імпульсів на виході зчитувача

Формат представлення даних визначається загальним числом записаних на карті біт інформації і їх розподілом за групами (полями) даних. Один із найбільш поширених є 26-бітний Wiegand-інтерфейс. Відповідно, до цьому на карту записують 26-біт інформації. 26-бітний формат Wiegand-карт був розроблений досить давно. На сьогодні він є найбільш популярним та підтримується переважною більшістю контролерів різних фірм-виробників.

Цей формат (26-біт) є відкритим, тобто будь-яка компанія може замовити у виробника карти із будь-яким системним кодом та номером. У зв’язку з цим існує потенційна можливість дублювання номера карт та несанкціонованого доступу на об’єкт. Для унеможливлення повторення номерів карт багато виробників карт та зчитувачів розробили свої власні формати, які містять більшу кількість біт даних. Виробники таких карт можуть практично гарантувати, що кожна карта має унікальний номер.

Для прикладу, компанія HID є одним із провідних виробників безконтактних карт та зчитувачів пропонує такі стандартні формати карт, які будуть сумісними із усіма типами зчитувачів:

– 26-розрядний формат;
– 37-розрядний формат HID;
– формат Corporate 1000 (35 біт);
– формат Long (до 84 біт).

Окрім системного коду, номера карти та бітів контролю парності, на карту може бути записано й номер випуску карти.

3.2.4 Магнітні карти

Магнітна карта являє собою пластикову карту стандартних розмірів із нанесеною на неї магнітною полосою (смугою). На магнітній полосі можуть перебувати від однієї до трьох доріжок запису (рис. 3.6, б), причому положення доріжок, їх ширина і глибина запису регламентуються ANSI та ISO.

Доріжка 1 використовується для запису й зберігання цифрової та літерної інформації. Вона застосовується у тому випадку, коли на карті необхідно зберегти інформацію про ім’я та прізвище її власника. Стандарт на запис даних на неї було розроблено IATA (International Air Transportation Association), яка використовувала пластикові карти для бронювання авіаквитків. У банківських картках на цій доріжці зберігають ім’я та прізвище власника, номер карти й термін її дії. Дані записуються із щільністю запису 210 біт на дюйм, кожен символ кодується 7 бітами. Всього на неї можна записати до 79 символів.

а) б)

Рисунок 3.6 – Пластикова карта з магнітною стрічкою [110]
а) – інформація про карту; б) – розташування доріжок на магнітній стрічці

Формат запису на доріжку 2 стандартизований ABA (American Banking Association) та передбачає запис цифрових даних із щільністю 75 BPI. На доріжці розміщують до 39 символів, для кодування кожного використовується 5 біт. У банківських картах на цій доріжці зберігаються номер карти та термін її дії.

Доріжка 3 використовується вкрай рідко, в основному для інформації, яка пов’язана із постійним перезаписом інформації на карті. Цифрові дані довжиною до 107 біт записуються із щільністю 210 BPI (5 біт на символ). Стандарт ANSI визначає формат запису інформації на доріжку.

Для прикладу розглянемо запис на доріжку 2. На початку смуги знаходиться послідовність з нулів, яка використовується для калібрування зчитувача. Перше значення «1» є першим бітом даних. Цей перший біт входить в стартову мітку (преамбулу), яка являє собою шістнадцяткове значення «B» (послідовність біт «1011»). За цією міткою йде інформаційна частина, яка може мати довжину до 37 десяткових знаків. Кожен символ складається із 4 біт даних та одного біта контролю непарності в межах символу. Після інформаційної частини йде завершальна мітка, яка являє собою шістнадцятизначне «F» (послідовність біт «1111»). Завершує кодову посилку біт контролю парності.

Приклад запису інформації на магнітній стрічці. Нехай послідовність двійкових символів, записаних на карті, містить 10 десяткових знаків:

11010010000001010011011011100111100010000001011100100111111100001.

Кожен символ кодується 5 бітами, з яких 4 є інформаційними, а п’ятий служить для контролю парності:

1101 0010 0000 0101 0011 0110 1110 0111 1000 1000 0001 0111 0010 0111 1111 00001.

Після поділу кодової посилки на блоки по 5 біт здійснюється перетворення інформації в десятковий формат. З кожного блоку видаляється біт контролю парності «П», а перші 4 біта переставляються в зворотному порядку (рис. 3.7).

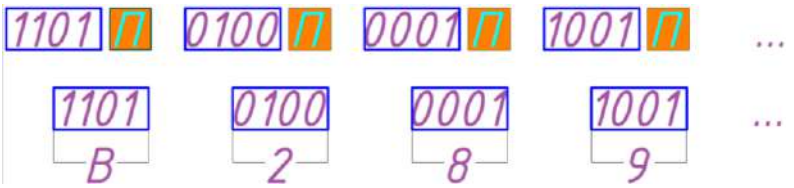


Рисунок 3.7 – Перетворення даних

Отримані блоки перетворюються в десяткову форму.

Запис інформації на магнітну смугу здійснюється за допомогою пристрою запису магнітних карт, який має магнітну головку. Ця головка складається із сердечника з обмоткою. В осерді є зазор шириною 0,1 … 10 мкм. Під час протікання через обмотку струму запису в області зазору виникає магнітне поле розсіювання, яке впливає на прилеглу до головки область робочого шару магнітної полоси карти. Поле запису, через певні проміжки часу, змінює свій напрямок на протилежний. В результаті, під дією поля розсіювання магнітної головки, відбуваються намагнічування й перемагнічування окремих ділянок рухомого магнітного носія. Під час періодичної зміні напрямку поля запису в робочому шарі носія виникає ланцюжок ділянок, які чергуються із протилежним напрямком намагніченості, які зіштовхуються один з одним однойменними полюсами. Ширина кожної ділянки, за щільності запису 75 біт на дюйм, становить 0,338 мм. Якщо, в межах однієї ділянки, напрямок намагніченості змінюється один раз, то це відповідає бінарному «0», а якщо два рази – «1». На рисунку 3.8 подано розподіл поляризації магнітного поля на доріжці, що відповідає двійковому рядку «000101010».

Основні переваги пристроїв ідентифікації на картах із магнітною смугою:

– невисока вартість карт;

– можливість зміни коду на карті під час її експлуатації за допомогою пристрою запису.

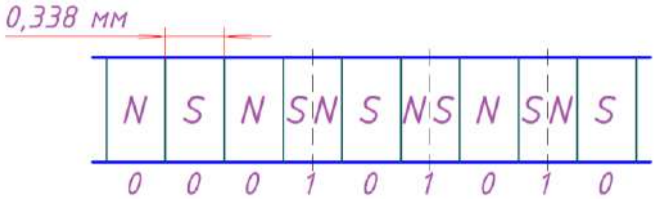


Рисунок 3.8 – Поляризація магнітного поля на доріжці

Основні недоліки:

– невисока захищеність карт від підробки;

– контактний спосіб зчитування, який не завжди є зручним;

– невисока пропускна здатність зчитувачів;

– магнітні головки з часом засмічуються та зміщуються;

– картки вимагають дбайливого зберігання, оскільки магнітна смуга на карті чутлива до впливу електромагнітних полів та механічних пошкоджень.

Використання карт із магнітною смугою в сучасних СКУД може бути доцільним у тому випадку, коли необхідно забезпечити мінімальну вартість карт (автоматизовані парковки, перепустки в метро тощо). В інших випадках, через розглянуті вище недоліки, карти із магнітною смугою використовуються вкрай рідко. Щодо вартість зчитувачів карт із магнітною смугою, то на даний час вони не дорожчі за прості моделі зчитувачів proximity-карт.

3.3 RFID-технології в СКУД

У сучасних СКУД радіочастотна технологія ідентифікації набуває більш ширшого поширення завдяки своїм можливостям та перевагам [53]. Ще одним терміном, який часто застосовують на практиці, є проксіміті (proximity). У різних першоджерелах зустрічаються й інші назви – безконтактна або дистанційна технологія. Слід пам’ятати, що всі вони недостатньо повно відображають фізичний принцип, який використано в цих системах (наприклад, технологію ідентифікації СД за райдужною оболонкою ока також можна віднести до безконтактної або дистанційної, так як її зчитування відбувається на певній відстані).

Термін «радіочастотний принцип ідентифікації» є найбільш правильним, оскільки він відображає фізичний принцип, який використовується у цих системах (дані від ідентифікатора на зчитувач передаються за радіочастотним каналом) та відповідає загальному класу систем RFID (Radio Frequency Identification).

На практиці, найбільш широко, оперують термінами радіочастотна технологія ідентифікації та проксіміті-технологія.

3.3.1 Принцип роботи зчитувача та ідентифікатора

Як і в інших системах ідентифікування, які використовують матеріальний

носій ідентифікаційної ознаки, система радіочастотної ідентифікації включає у себе зчитувач та ідентифікатор. В ідентифікаторі (карта, брелок або мітка) знаходиться мікросхема із фіксованим або програмно змінюваним кодом, котушка індуктивності й конденсатор, які представляють собою резонансний коливальний контур (рис. 3.8).

Рисунок 3.8 – Будова карти радіочастотної ідентифікації [110]

Індуктивність, у залежності від використовуваного діапазону частот, може виконуватися у вигляді котушки або друкованих провідників. Частота, на якій працює система, визначає більшість її експлуатаційних характеристик – від дистанції зчитування до здатності сигналу долати фізичні перешкоди. У глобальній практиці СКУД виділяють три основні технологічні пласти, кожен з яких займає власну нішу залежно від вимог до безпеки та функціональності.

Низькочастотний діапазон, що охоплює частоти від 125 до 134,2 кГц, історично став першим стандартом для безконтактних карт доступу. Фізика цього діапазону базується на індуктивному зв’язку в ближньому полі. Довжина хвилі λ при частоті 125 кГц становить приблизно 2400 метрів, що означає, що передача даних відбувається виключно за рахунок магнітної індукції між котушками антени зчитувача та карти. Це забезпечує унікальну стійкість до навколишнього середовища – низькочастотні сигнали практично не поглинаються водою та людським тілом і здатні проходити крізь тонкі шари металу, що робить їх ідеальними для ідентифікації тварин (підшкірні чіпи) або роботи в умовах високої вологості. Однак обмеженням цієї технологій є низька швидкість передачі даних та мала дистанція зчитування, яка зазвичай не перевищує 10 … 20 сантиметрів для стандартних пасивних карт.

Високочастотний діапазон, що працює на чітко визначеній частоті 13,56 МГц, сьогодні є домінуючим у системах, де безпека є пріоритетом. Як і попередня технологія, цей діапазон використовує індуктивний зв’язок, але значно вища частота дозволяє передавати складні криптографічні пакети даних на швидкостях до 848 кбіт/с. Стандарти ISO 14443 та ISO 15693 визначають два підкласи цих систем – «близькі» з дистанцією до 10 см та «околичні» з

дистанцією до 1,5 метра [110]. Основною перевагою цієї технології є можливість реалізації дворівневої взаємної автентифікації та використання смартфонів з підтримкою NFC як повноцінних ідентифікаторів.

Ультрависокочастотний діапазон, що працює в межах 860 … 960 МГц, використовує принципово інший фізичний механізм – зворотне розсіювання електромагнітної хвилі у далекому полі. Тут антени зчитувача та тега працюють як повноцінні випромінювачі. Це дозволяє досягати вражаючої дистанції зчитування до 12 … 15 метрів для пасивних міток. У СКУД дана технологія незамінна для автоматизації паркінгів та складських комплексів, де ідентифікація має відбуватися без зупинки об’єкта. Проте висока частота робить систему чутливою до екранування металом та поглинання сигналу рідинами.

Загалом, котушку індуктивності прийнято називати антеною, хоча в згаданих діапазонах частот вона не є такою (для того щоб переконатися у цьому, необхідно порівняти її розміри із робочою довжиною хвилі).

Коли ідентифікатор з’являється поблизу зчитувача, два контури (ідентифікатора та зчитувача) стають індуктивнопов’язаними. Контур зчитувача прийнято розглядати як первинний, а ідентифікатора – як вторинний. Індуктивний зв’язок котушок призводить до появи взаємної індуктивності. Отже, поява в магнітному полі первинного контуру котушки індуктивності вторинного призводить до зміни параметрів первинного контуру зчитувача, які можуть реєструватися. Таким чином, змінюючи параметри вторинного контуру (здійснюючи переналаштування або шунтування вторинного контуру) можна організувати інформаційний обмін між зчитувачем та ідентифікатором.

Для зміни параметрів вторинного контуру ідентифікатора (модуляція) використовують спеціальну мікросхему, яка комутує вторинний контур відповідно до запрограмованого в її пам’яті коду. Зазвичай, такій мікросхемі (рис. 3.9) притаманні: ланцюг синхронізації; енергонезалежна пам’ять (зберігання коду ідентифікатора); випрямляч та стабілізатор напруги із буферним конденсатором; схема модуляції, яка змінює параметри контуру; детектор команд в носіях із двостороннім обміном інформацією.

Зчитувач являє собою мікропроцесорний пристрій, який містить первинний коливальний контур та електронну схему, яка й дозволяє детектувати сигнал, що модулюється кодом карти. Використаний частотний діапазон істотно впливає на характеристики системи.

У діапазонах довгих і коротких хвиль, в умовах двохстороннього обміну інформацією, між зчитувачем та ідентифікатором використовується індуктивний (трансформаторний) зв’язок (рис. 3.10). Це і є основною відмінністю фізичного принципу проксіміті-технології від приймально-

передавальних радіоканальних пристроїв. Ідентифікатор не є передавачем, а лише модулює амплітуду несучої частоти зчитувача відповідно до запрограмованого в його пам'яті коду.

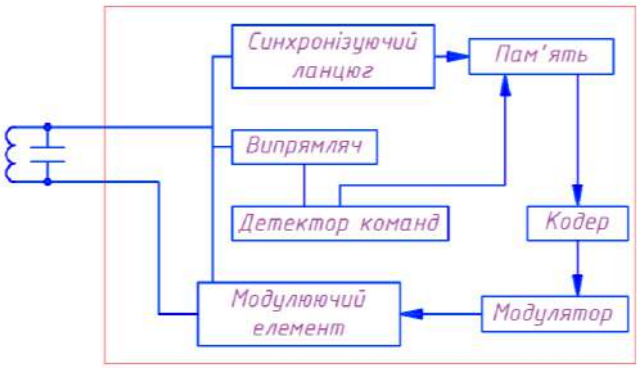


Рисунок 3.9 – Функціональна схема безконтактного ідентифікатора

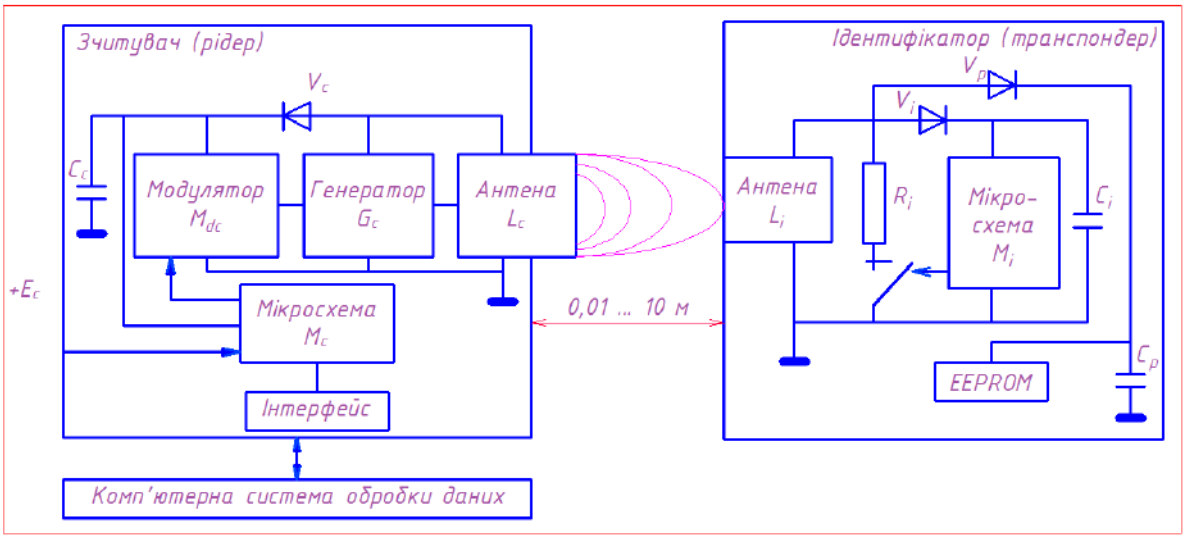


Рисунок 3.10 – Функціональна схема радіочастотного пристрою ідентифікації

У діапазоні надвисоких частот (НВЧ) для обміну інформацією між зчитувачем й ідентифікатором використовують радіоканал.

Типовий сеанс зв'язку між зчитувачем та картою складається з етапів:

1. Пристрій зчитування формує коливання несучої частоти, при цьому контролює безперервно наявність модуляції в сигналі (модуляція сигналу буде свідчати про виявлення карти в зоні дії зчитувача (рис. 3.11)).

2. Карта потрапляє в поле зчитувача (після накопичення енергії, яка буде достатньою для роботи мікросхеми та синхронізації, розпочинається управління транзистором, який буде шунтувати контур).

3. Шунтування контуру здійснюється відповідно до інформаційного коду, який записано в пам'яті мікросхеми картки, що призводить до зміни напруги несучого коливання в контурі зчитувача.

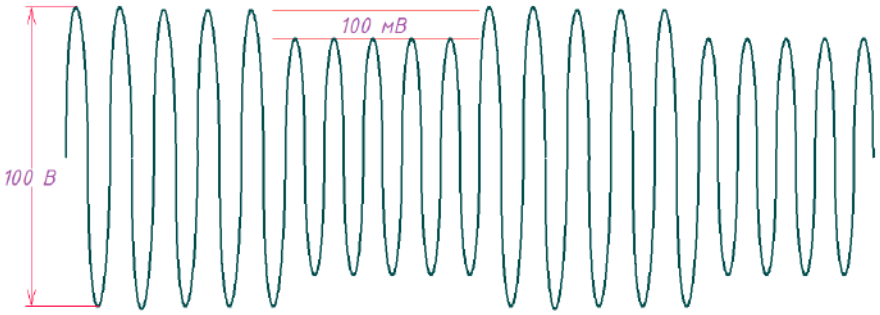


Рисунок 3.11 – Амплітудно-модульований сигнал

3.3.2 Кодування інформації в системах радіочастотної ідентифікації

Вибір способу кодування впливає на можливість виявлення та виправлення помилок під час приймання, займаної сигналом смуги частот, можливості синхронізації, вартості реалізації та інші параметри системи.

На практиці відомо про багато способів кодування, однак в системах радіочастотної ідентифікації найпоширенішими стали (рис. 3.12):

1. Прямий код. Для даного випадку найпростішого дворівневого коду нулю відповідає низький рівень сигналу, а одиниці – високий. Інформаційні переходи співпадають з границею біт. Цей код позначають як NZR (Non Return to Zero), тобто кодування «без повернення до нуля». Перевагою цього способу кодування є його простота: двійковий код повідомлення не потрібно піддавати додатковим перетворенням. Однак він не забезпечує синхронізації, що є його найбільшим його недоліком.

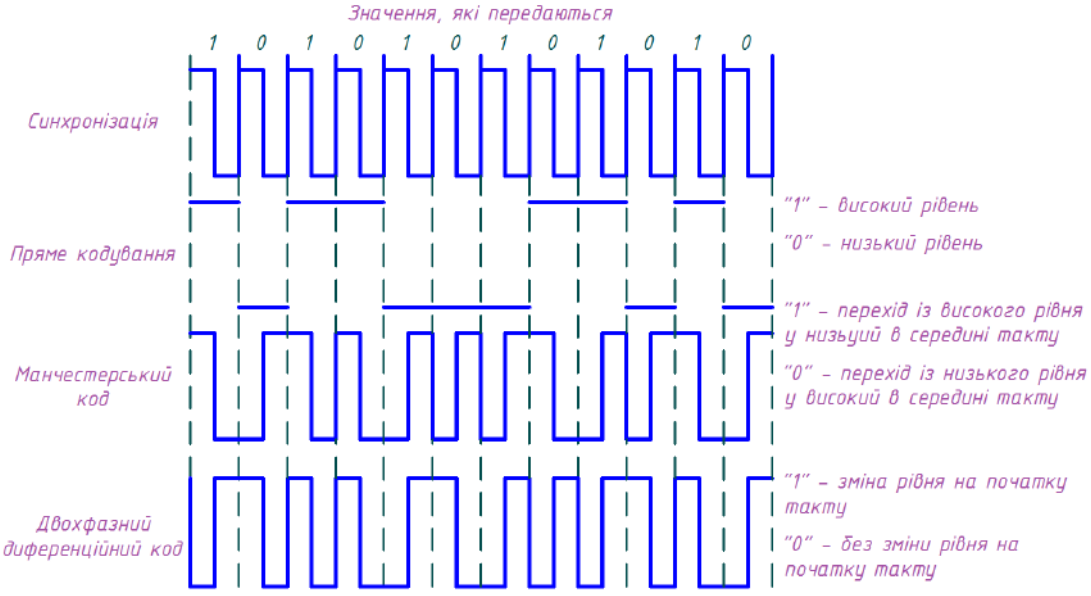


Рисунок 3.12 – Способи кодування даних [110]

2. Диференціальний двохфазний код. Існує декілька різновидів способу кодування, який використовує цей код, але у загальному випадку зміна рівня

сигналу відбувається кожен такт синхронізації, причому логічні значення «0» і «1» розрізняються за переходами напруги у середині такту синхронізації. Оскільки переходи здійснюються кожен такт незалежно від значення біта («0» або «1»), цей метод використовують лише для синхронізації зчитувача з потоком переданих даних (самосинхронізований код). Слід зауважити, що він дозволяє виявляти помилки.

3. Манчестерський код це різновид диференціального двохфазного способу кодування. Його прийнято вважати самосинхронізуючим кодом. Одиниця відповідає переходу сигналу з високого рівня в низький, нуль – зворотній перехід. Особливістю манчестерського коду прийнято вважати відсутність у сигналі постійної складової під час передачі довгої послідовності одиниць або нулів.

У зоні дії зчитувача, у деяких системах радіочастотної ідентифікації, можливим може бути наявність одночасно декілька ідентифікаторів. В цьому випадку виникає конфлікт – спроба модуляції несучого сигналу зчитувача двома ідентифікаторами одночасно. Для коректного зчитування інформації з усіх ідентифікаторів прийнято використовувати спеціальні алгоритми (тимчасовий розподіл сигналів від різних ідентифікаторів), які дозволяють йому запобігти. Варто пам’ятати, що завдання буде ускладнюватись, коли необхідно не тільки зчитувати, але й записувати дані на ідентифікатори.

3.3.3 Чинники, які впливають на дальність зчитування

Ознайомившись із особливостями функціонування зчитувачів та ідентифікаторів, можливим є формулювання чинників, які впливають на дальність зчитування системи радіочастотної ідентифікації із пасивними ідентифікаторами:

1. Робоча частота та конструкція антени зчитувача.
2. Якість контуру антени зчитувача.
3. Взаємна орієнтація антен зчитувача та ідентифікатора у просторі.
4. Величина струму та напруги в котушці зчитувача.
5. Чутливість приймача зчитувача.
6. Алгоритм кодування/декодування даних та використаний спосіб модуляції сигналу.
7. Довжина кодову (кількість біт в коді ідентифікатора).
8. Навколишні умови (наявність розташованих близько металевих предметів, електромагнітних перешкод, тощо).

3.4 Смарт-технології та мобільна ідентифікація

Станом на 2026 рік мобільна ідентифікація, що базується на технологіях NFC (Near Field Communication) та BLE (Bluetooth Low Energy), стала

домінуючим стандартом для нових інсталяцій та масштабних проектів модернізації [10]. Цей зсув зумовлений не лише прагненням до зручності користувачів, а й фундаментальною потребою у вищому рівні безпеки, який неможливо забезпечити за допомогою статичних пластикових карток. Сучасний смартфон у контексті СКУД розглядається не просто як заміна токена, а як інтелектуальний вузол, здатний виконувати складні криптографічні операції, підтримувати багатофакторну автентифікацію (MFA) та забезпечувати безперервний зв'язок із хмарними платформами управління.

Вибір між NFC та BLE більше не розглядається як альтернатива «або-або» [41]. Сучасна архітектура СКУД базується на гібридному використанні обох протоколів, що дозволяє задовольнити найширший спектр експлуатаційних вимог – від суворого режиму на критичних об'єктах до комфортного доступу «вільні руки» в офісах класу А.

NFC функціонує на частоті 13,56 МГц, використовуючи принцип магнітної індукції для передачі даних на надкороткі відстані, зазвичай до 4 см. Ця технологія є прямим спадкоємцем стандартів високочастотного RFID, зокрема ISO/IEC 14443 [28, 105] та ISO/IEC 15693 [29], що забезпечує їй високий рівень сумісності з існуючою інфраструктурою смарт-карт. Основна цінність NFC у системах безпеки полягає у фізичному обмеженні радіусу дії. Мала дистанція зчитування вимагає від користувача свідомого його піднесення майже впритул до зчитувача. Це нівелює ризики випадкового спрацювання або дистанційного перехоплення сигналу в натовпі, що робить NFC ідеальним вибором для точок доступу з високими вимогами до підтвердження наміру користувача.

Особливістю NFC є підтримка трьох режимів роботи – емуляції картки, зчитування/запису та рівний-рівному (P2P). Для СКУД важливим є режим емуляції картки, який дозволяє смартфону імітувати поведінку безконтактної смарт-картки. Завдяки HCE (Host Card Emulation) на платформі Android розробники отримали можливість програмно керувати процесом ідентифікації, хоча найбільш захищені рішення все ще покладаються на апаратний SE (Secure Element).

У свою чергу, BLE, що працює в діапазоні 2,4 ГГц, радикально відрізняється від NFC за своїми фізичними характеристиками. Використовуючи поширення радіохвиль, BLE забезпечує стабільний зв'язок на відстані до 10, 30 або навіть 100 метрів, залежно від умов середовища та налаштувань обладнання. Така дальність дозволяє реалізувати сценарії, які раніше були недоступні для RFID-систем, зокрема автоматичне відчинення дверей під час наближення користувача або керування шлагбаумами без необхідності відчиняти вікно автомобіля.

Механізм роботи BLE у СКУД базується на регулярному випромінюванні рекламних пакетів смартфоном або зчитувачем. Коли пристрій потрапляє в зону дії, ініціюється процес встановлення зв’язку, який у сучасних реалізаціях BLE 5.0+ займає лічені секунди. Важливою перевагою BLE є його здатність передавати великі обсяги даних із високою швидкістю (до 2 Мбіт/с), що корисно для оновлення прошивок зчитувачів або передачі складних сертифікатів безпеки.

Таким чином, безконтактні смарт-карти поєднують у собі переваги безконтактних proximity- та смарт-карт [8]. Запис та зчитування інформації з мікросхеми (чіпа) картки здійснюється безконтактним способом, та за змістом нагадує роботу proximity-карту. Так, як і proximity-карти, безконтактні смарт-карти є пасивними пристроями, тобто не мають вбудованого джерела живлення. Живлення мікросхеми карти під час обміну інформацією із зчитувачем відбувається за допомогою змінного електромагнітного поля, яке генерується кард-рідером (рис. 3.13).

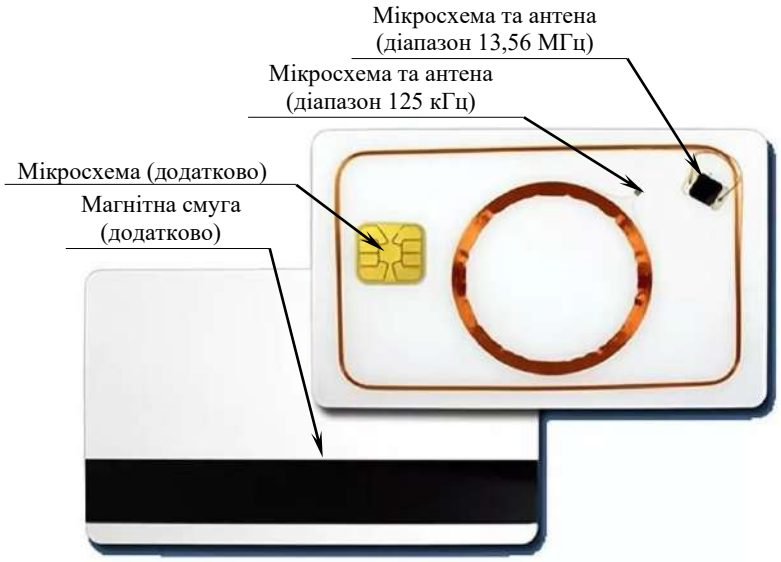


Рисунок 3.13 – Комбінована безконтактна смарт-карта [110]

На початку безконтактні смарт-карти розроблялись для використання в платіжних системах (наприклад, оплата проїзду в транспорті, метро тощо), пізніше, набули широкого вжитку і в СКУД. На сьогодні найбільш широко використовуються карти стандартів MIFARE (Philips Electronics) та iCIass (HID).

Робоча частота зчитувачів MIFARE становить 13,65 МГц, при цьому максимальна дальність зчитування – близько 10 см. Швидкість обміну даними між картою і зчитувачем – 106 кбіт/с. Фізичний принцип обміну інформацією із зчитувачем аналогічний proximity-картам, які використовують діапазон частот

13,56 МГц. Основна відмінність від них полягає в обсязі пам’яті карти, способі зберігання інформації та організації сеансу зв’язку із зчитувачем. Карта може переміщуватись у полі дії антени зчитувача без переривання сеансу обміну даними.

Впровадження смарт-технологій у СКУД приносить вимірювані фінансові переваги, які стають очевидними вже в перший рік експлуатації. Традиційні витрати на пластикові картки є лише «верхівкою айсберга».

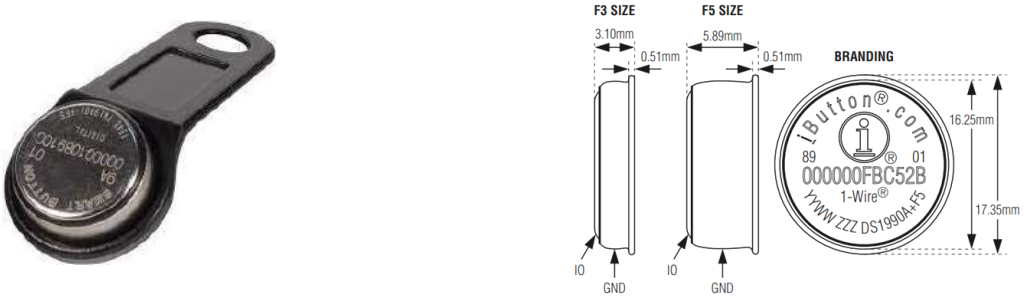
Випуск захищеної смарт-картки формату MIFARE DESFire EV3 обходиться компанії значно дорожче, ніж мобільна ліцензія. Крім того, фізичні картки постійно губляться, ламаються або забуваються. Мобільна перепустка завжди зі співробітником. Статистика вказує, що люди помічають втрату смартфона протягом 15 хвилин, тоді як втрата картки може залишатися непоміченою годинами або днями, створюючи загрозу безпеці.

Час, витрачений на друк та видачу карток, особливо у великих компаніях з високою плинністю кадрів або великою кількістю підрядників, є значним операційним тягарем. Використання мобільного доступу з дистанційною видачею облікових даних дозволяє HR-відділу або службі безпеки видати перепустку ще до того, як новий співробітник прийде в офіс у свій перший робочий день. Якщо доступ через BLE економить хоча б 10 секунд на кожному вході/виході для 100 співробітників, це сумарно дає близько 8 годин збереженого робочого часу на місяць.

У 2026 році корпоративна соціальна відповідальність стала важливим фактором вибору технологій. Традиційні перепустки виготовляються з ПВХ – пластику, який важко переробляється і створює значне екологічне навантаження. Мобільний доступ повністю усуває потребу у пластикових картках та батарейках для активних брелоків, що ідеально вписується у стратегії сталого розвитку сучасних корпорацій. Дослідження, проведені в університетських кампусах, показують, що перехід на мобільні ідентифікатори покращує загальну продуктивність системи на 80% та значно знижує вуглецевий слід підрозділів безпеки.

3.4.1 Електронні таблетки

Електронні таблетки (touch memory) набули досить широкого поширення завдяки своїй простоті (а отже, дешевизні) та надійності, стійкості до механічних впливів [79]. Вперше даного роду ідентифікатори були розроблені компанією Dallas Semiconductor. Конструктивно електронна таблетка (рис. 3.14) являє собою металевий корпус циліндричної форми. Одна частина – торцева – відокремлена від основної частини корпусу ізолятором. Таким чином, є дві ізольовані струмопровідні частини, що утворюють пару з сигнальної і загальної лінії.



а) б)

Рисунок 3.14 – Електронний ідентифікатор типу «Touch memory» [110]
а) – вигляд загальний; б) – технічні параметри

Зчитувач (рис. 3.15), зазвичай містить гніздо, яке відповідає розмірам електронної таблетки. При цьому сама таблетка та гніздо зчитувача повинні мати таку форму, яка практично виключає коротке замикання.

Сама таблетка зазвичай кріпиться на тримачі (рис. 3.15, а), що дозволяє спростити процес користування (зручніше тримати в руці) та її кріплення.

В середині корпусу ключа touch memory розташовується електронна частина схеми, яка, залежно від модифікації, включати в себе такі елементи:

– постійний запам’ятовуючий пристрій (ПЗП), дані в який записуються під час виготовлення та не можуть бути змінені у ході експлуатації;

– енергонезалежний перепрограмовуваний запам’ятовуючий пристрій (ППЗП);

– буферна пам’ять для захисту від можливого порушення контакту під час процесу запису/зчитування;

– інтерфейс для приймання та передачі інформації з функцією контролю цілісності даних;

– схема синхронізації та годинник;

– вбудоване джерело живлення для ППЗП.

а) б) в)

Рисунок 3.15 – Зчитувач ключів [110]
а) – Dallas CZ-3-S; б) – AURES Dallas; в) – TMR-900 DALLAS

Як уже говорилось вище, залежно від типу пристрою, частина таких елементів може бути відсутньою, наприклад ППЗУ або схема синхронізації та

годинник. Об’єм ПЗП зазвичай становить від 64 біт до десятків кілобіт.

Жорстких вимог до габаритів таких пристроїв не висувають, тому й істотних технологічних складнощів із реалізацією відповідної схемотехніки практично немає.

Живлення електронної частини відбувається від зчитувача під час контакту. З цього стає зрозумілим, що основне вбудоване джерело живлення, яке б знаходилось в самому ідентифікаторі, є необов’язковим. Однак, слід пам’ятати про можливість нестабільного контакту під час роботи (цим й обумовлена наявність буферної пам’яті ідентифікатора з ППЗП). Слід пам’ятати, що запам’ятовуючі пристрої повинні володіти захистом від несанкціонованого доступу (зазвичай це реалізують за допомогою ключів).

Оскільки для живлення та обміну інформацією використовується два контакти необхідно розділяти постійний (живлення) та змінний (інформація) струми, що досить просто реалізується технічно. Наприклад, амплітудною модуляцією струму споживання. Таким чином, живлення, прийом та передача даних здійснюється за однією парою провідників.

Передача або прийом інформації здійснюється за напівдуплексним режимом. Взаємодію організовано за принципом «ведений-ведучий», тут головним вважають зчитувач.

Металевий корпус, а отже, їх висока механічна міцність, та відсутність джерела живлення обумовлюють широке застосування таких ідентифікаторів на практиці (в масових системах – домофонна система ідентифікації тощо).

3.4.2 Смарт-карти

Контактні смарт-карти, так само як і електронні таблетки, набули досить широкого застосування. Конструктивно такий ідентифікатор (рис. 3.16) виконаний у вигляді пластикової карти, на якій закріплена мікросхема з декількома (зазвичай 6 … 8) контактами (рис. 3.17).

Контактна смарт-карта є пасивним пристроєм, який не має вбудованого джерела живлення. Відмінність від електронного ідентифікатора типу «Touch memory» полягає, перш за все, у наявності декількох контактів, до дозволяє живити мікросхему, передавати дані та приймати їх за розподіленими каналами [131]. Враховуючи це, можна відмітити зростання швидкодії обміну та спрощення інтерфейсної частини ідентифікатора.

Розглянуті ідентифікатори дозволяють достатньо просто реалізувати не тільки двосторонній обмін інформацією, але й перезапис даних (наприклад, списування з рахунку грошових коштів у міру їх витрачення) [122].

Основною технологічною вимогою, яка стосується розміру мікросхеми, прийнято вважати її плоскість та товщину, яка не на багато повинна перевищувати товщину пластикової карти. Окрім того, на практиці, висувають

більш жорсткі вимоги до матеріалу покриття контактів. Щодо зчитувача, то до його складу повинна входити група ковзаючих контактів, які відповідали б розташуванню контактів на карті.

а) б)

Рисунок 3.16 – Контактна смарт-карта [110]
а) – без контактного чіпа; б) – з контактним чіпом

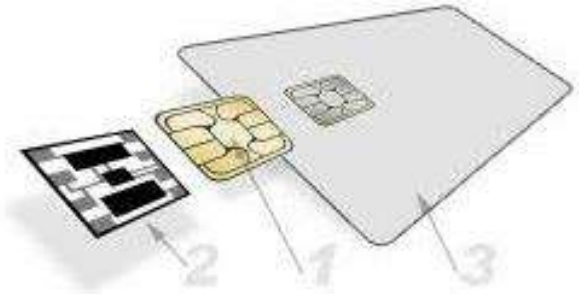


Рисунок 3.17 – Будова контактної смарт-карти [110]
1) – контактна область (6 або 8 контактів квадратної або овальної форми, позиції яких виконано за ISO 7816); 2) – контактний чіп (мікропроцесор карти); 3) – пластикова основа

До типових різновидів смарт-карт, які визначаються, насамперед, функціональними можливостями та структурою пам’яті карти слід віднести:

– карти із фіксованою інформацією, до яких входять лише тільки ПЗП, дані у якому не можуть змінюватися під час експлуатації;

– карти із інформацією, яка перезаписується, до яких входять не лише ПЗП, але й перепрограмовуючу пам’ять, інформація у якій може змінюватися під час їх експлуатації;

– мікропроцесорні карти із широкими можливостями.

Необхідно пам’ятати, що для будь-якого випадку, варто забезпечити відповідні заходи щодо захисту інформації від несанкціонованого доступу, копіювання або модифікації. При цьому засоби захисту можуть бути різними – від системи ключів до використання складних спеціальних криптографічних алгоритмів. іАж до блокування або самознищення інформації. Рівень захисту залежить від умов конкретного завдання.

Контактні смарт-карти набули широкого поширення як ідентифікатори для оплати телефонних розмов в автоматах, на транспорті і для інших застосувань.

3.5 Штрихове та матричне кодування

Трансформація сучасних СКУД у бік цифрової мобільності та безконтактних технологій зумовила ренесанс візуальних методів ідентифікації. Штрихове та матричне кодування, що раніше сприймалося як допоміжний інструмент логістики, сьогодні інтегрується у складні безпекові архітектури як повноцінна альтернатива або доповнення до радіочастотної ідентифікації (RFID) та ближнього бездротового зв’язку (NFC). Перехід від фізичних карток до візуальних токенів, що відображаються на екранах смартфонів, відкриває нові можливості для масштабування систем, зниження капітальних витрат та впровадження динамічних механізмів автентифікації, які раніше були доступні лише у високобюджетних рішеннях.

Розвиток засобів автоматичної ідентифікації та збору даних призвів до формування двох фундаментальних категорій візуальних ідентифікаторів – одновимірних (1D) лінійних штрих-кодів та двовимірних (2D) матричних кодів [2]. Лінійні штрих-коди, що десятиліттями були основою роздрібної торгівлі, кодують дані лише в горизонтальному вимірі, використовуючи послідовність ліній та пробілів різної ширини. Їхня ємність обмежена кількома десятками символів, а для зчитування потрібна орієнтація сканера відносно коду. Натомість матричні коди, такі як QR-коди та Data Matrix, використовують двовимірну сітку контрастних осередків, що дозволяє зберігати значно більші обсяги інформації та забезпечує всеспрямоване зчитування (360°).

Матричний код Data Matrix, винайдений у 1994 році компанією International Data Matrix, Inc. (I.D. Matrix), є одним із найбільш надійних форматів для промислових СКУД та систем відстеження активів. Його архітектура базується на сітці чорно-білих осередків, оточених спеціальним шаблоном пошуку у формі латинської літери «L», що складається з двох суцільних суміжних меж. Ця структура дозволяє камері сканера миттєво визначити орієнтацію та масштаб коду незалежно від кута нахилу пристрою.

Однією з ключових переваг Data Matrix є висока щільність запису [48].

Цей формат дозволяє створювати ідентифікатори розміром всього 10×10 пікселів, що значно менше за мінімальні вимоги до QR-кодів. Завдяки компактності Data Matrix став стандартом для маркування малогабаритних компонентів в автомобільній, аерокосмічній та медичній галузях. У контексті СКУД Data Matrix часто використовується для маркування обладнання, ключів та внутрішніх ідентифікаторів, які повинні залишатися зчитуваними навіть при значних фізичних пошкодженнях або забрудненні. Максимальна ємність коду становить 2335 буквено-цифрових символів, що регулюється стандартом ISO/IEC 16022 [30].

QR-коди, розроблені корпорацією Denso Wave у 1994 році, стали домінуючим форматом у клієнтських додатках СКУД та системах мобільного доступу. На відміну від Data Matrix, QR-код використовує три ідентичні квадратні структури («очі») у верхньому лівому, верхньому правому та нижньому лівому кутах як шаблон пошуку. Це дозволяє смартфонам та спеціалізованим сканерам миттєво захоплювати код навіть у складних умовах освітлення.

QR-коди мають вражаючу інформаційну місткість – до 7089 цифрових або 4296 буквено-цифрових символів, що значно перевищує можливості більшості конкурентів. У сучасних СКУД такий обсяг даних використовується для вбудовування зашифрованих цифрових підписів, URL-адрес для веб-автентифікації або складних метаданих користувача. Стандарт ISO/IEC 18004 [47] визначає параметри QR-кодів, включаючи налаштовуваний рівень корекції помилок за алгоритмом Ріда-Соломона.

Рівні корекції помилок у QR-кодах дозволяють відновити дані навіть при втраті від 7% (рівень L) до 30% (рівень H) поверхні коду. Це важливо для СКУД, де ідентифікатор може бути пошкоджений або відображений на екрані з подряпинами чи відблисками.

Штрихові коди досить широко використовують під час ідентифікації СД.

Штриховий код являє собою групу смуг різної ширини (рис. 3.18), які наносять на поверхню ідентифікатора.

Інформаційним параметром в штриховому коді виступає співвідношення ширини темних смуг (штрихів) по відношенню до ширини світлих смуг (пропуски між штрихами), що відповідає широтно-імпульсній модуляції. Кожну цифру кодують визначеною кількістю штрихів та пропусків. Відведене для такої цифри коду місце прийнято називати знаком, який і є основною одиницею інформації в штриховому коді. Зазвичай, усі знаки мають однакову ширину й складаються з елементарних модулів, тому ширина штрихів і пропусків завжди кратна елементарному модулю. Елементарний модуль – це самий вузький елемент (штрих або пропуск).

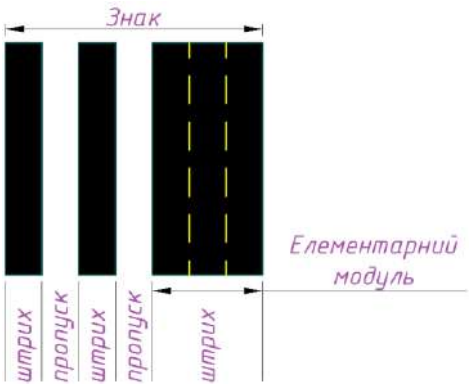
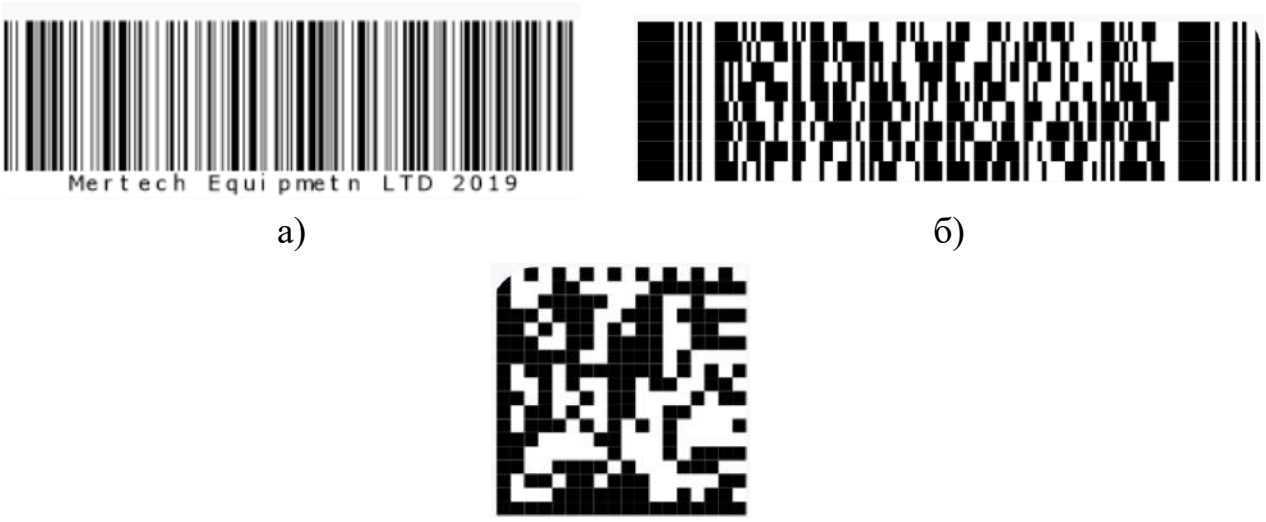


Рисунок 3.18 – Знак штрихового коду [110]

Існують різні способи кодування інформації, які називають штрих-кодовим кодуванням. На практиці, прийнято розрізняти одноплощинні (лінійні) та двохплощинні штрих-коди (рис. 3.19).



а) б)

в)

Рисунок 3.19 – Приклади штрих-кодів [110]
а) – одноплощинний (Code 128); б) – двохплощинний (PDF-417);
в) – двохплощинний (Data Matrix)

Одноплощинними (лінійними) називають штрих-коди, які читаються в одному напрямку (за горизонталлю поперек штрихів). Найбільш поширеними системами лінійного кодування прийнято вважати: EAN, UPC, Code 39, Code 128, Codabar, Interleaved 2 of 5. Така система дозволяє кодувати невеликий об’єм інформації (до 20 … 30 символів, зазвичай цифр).

У свою чергу, двохплощинними називають штрих-коди, які розроблено для кодування великого обсягу інформації (до декількох тисяч символів).

Двохплощинний код зчитується за допомогою спеціального сканера й дозволяє швидко та безпомилково заносити великий обсяг інформації.

Декодування такого коду здійснюється у двох площинах (як за горизонталлю, так й за вертикаллю). До двохплощинних систем кодування відносять наступні штрих-коди: PDF417 Aztec, Data Matrix тощо.

Використання штрихових кодів є найбільш дешевою технологією ідентифікації. У сучасних системах контролю доступу штриховий код використовують переважно в поєднанні з іншими способами ідентифікації (наприклад, на пластиковій картці із штрих-кодом може бути розташоване фото СД).

Зчитування коду здійснюється за допомогою оптичного способу у видимому або інфрачервоному діапазоні хвиль. Зчитувач містить джерело світла, фотодетектор та пристрій оброблення сигналу (рис. 3.20).

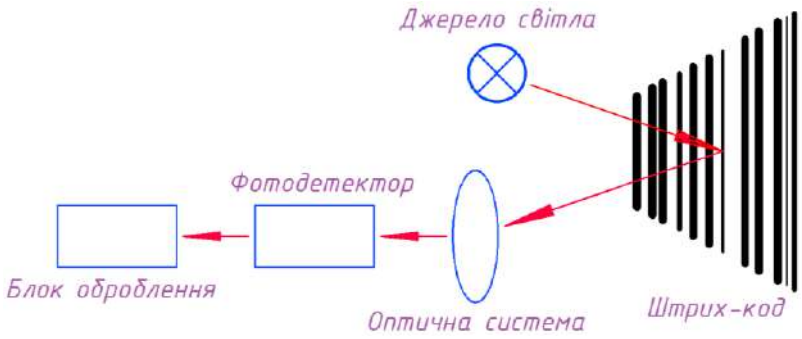


Рисунок 3.20 – Будова зчитувача штрих-коду

Джерело світла випромінює, на штриховий код, світловий потік із певною довжиною хвилі. Відбите світло відбивається назад та фокусується на фотодетекторі. Останній перетворює оптичну інформацію в електричний сигнал, який обробляється й перетворюється у формат, який буде зручним для передачі в пристрій обробки (контролер) для прийняття рішення.

Як уже зазначалось, на практиці існують різні типи штрихових кодів, кожен із яких розроблено для певної області застосування. У свою чергу для них притаманні свої переваги та особливості. Окремі із штрихових кодів мають високу щільність запису інформації, що дозволяє розмістити на обмеженій ділянці великий обсяг даних. Також відомо про коди, які дозволяють перевіряти зчитану інформацію (забезпечують контролювання помилок під час зчитування). Деякі із штрих-кодів дозволяють записувати як цифрову, так й текстову інформацію.

Найбільш часто, в СКУД, використовують штрихові коди Interleaved 2 of 5 та Code 39. Перший з них дозволяє кодувати тільки цифрову інформацію, а другий – цифрову та літерну.

Для подолання головного недоліку візуальних ідентифікаторів – легкості копіювання – у сучасних СКУД застосовується концепція динамічних QR-

кодів. Ця технологія базується на використанні одноразових паролів, що змінюються у реальному часі.

Основою безпечного мобільного доступу є алгоритм Time-Based One-Time Password (TOTP), який поєднує спільний секретний ключ та поточну мітку часу для генерації унікального коду. Процес функціонування такої системи в СКУД (наприклад, у рішеннях ZKTeco Atlas ZKey) включає наступні етапи: реєстрацію, генерацію та верифікацію.

Під час першого налаштування сервер СКУД генерує унікальний секретний ключ для кожного користувача. Цей ключ передається у мобільний додаток у зашифрованому вигляді або через одноразове сканування адміністративного QR-коду.

Під час синхронізації додаток на смартфоні та контролер доступу використовують системний час як змінний параметр. Важливо, щоб часові пояси та годинники обох пристроїв були синхронізовані, інакше згенерований код буде невалідним.

Кожні 30 секунд додаток автоматично генерує новий 6-значний код за допомогою алгоритму HMAC-SHA1. Цей код вбудовується у графічну структуру QR-коду, який відображається на екрані смартфона.

При верифікації, коли користувач підносить смартфон до пристрою зчитування, зчитувач декодує QR-код, витягує TOTP і передає його контролеру. Контролер самостійно розраховує очікуваний код для даного користувача в цей конкретний момент часу. Якщо значення збігаються, доступ надається.

Перевагою систем на базі TOTP є можливість генерації кодів без підключення смартфона до мережі Інтернет. Оскільки алгоритм базується на часі та локально збереженому ключі, користувач може відкрити двері навіть у підземному паркінгу або в умовах відсутності зв’язку. Більше того, розробники СКУД впроваджують захист від скріншотів у мобільних додатках, що робить неможливим пересилання динамічного коду третім особам. Код стає недійсним майже миттєво після використання або після закінчення 30-секундного вікна.

3.5.1 Код Interleaved 2 of 5

Цей код (відомий також з іншою інтерпретацією USSITF2/5, ITF або 1-2/5) вважається безперервним штрих-кодом змінної довжини та дозволяє кодувати цифри від 0 до 9. Його відносять до кодів із високою щільністю запису, що дозволяє записувати до 18 цифр на дюйм при ширині елементарного модуля 0,19 мм. Висока щільність досягається за рахунок виключення пропусків, які поділяють сусідні знаки (рис. 3.21).

Код Interleaved використовують в багатьох областях для кодування цифрових даних. Він є стандартними міжнародними кодом маркування тари та упаковки. Код Interleaved широко застосовується в автоматизованих системах

для ідентифікації предметів складування, багажу в аеропортах, нумерації авіаційних квитків, ідентифікації поштових відправлень тощо. Він належить до сімейства кодів «2 з 5» (2 of 5) і має п’ять елементів у знакові, два з яких є широкими. Особливість коду Interleaved – представлення пар цифр у знаках штрихового коду за допомогою п’яти штрихів і п’яти проміжків (від цього пішла назва коду – Interleaved («перемежовані»)). При цьому використовується чергування цифр: на непарних позиціях (відлік зліва направо) знаки зображують штрихами, а на парних – пропусками (рис. 3.22).

а) б) в)

Рисунок 3.21 – Приклади штрихового коду сімейства 2 of 5 [110]
а) – Interleaved; б) – Industrial та в) – Matrix

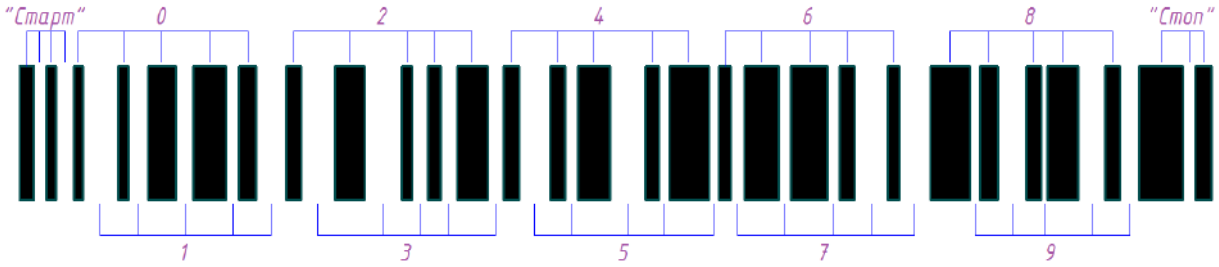


Рисунок 3.22 – Структура штрихового коду Interleaved

Під час кодування даних із непарною кількістю знаків попереду записується «0». У двійковому зображенні широкий штрих або широкий проміжок ідентичний «1», вузький штрих або вузький проміжок – «0». Співвідношення ширини широкого та вузького елементів складає не менше 2,5:1.

Знак «Старт» складається із двох вузьких штрихів та двох вузьких пропусків. Знак «Стоп» складається з одного широкого штриха, одного вузького пропуску й одного вузького штриха.

Для підвищення надійності зчитування, в коді Interleaved, використовують контрольний знак. Контрольний знак розташовується безпосередньо після інформаційних знаків перед знаком «Стоп». Якщо додавання контрольного знаку робить кількість знаків у кодованих даних непарним, то попереду кодового рядка, безпосередньо після знаку «Старт», додають «0».

3.5.2 Код Code 39

Штриховий код Code 39 є кодом змінної довжини та дозволяє відобразити 43 символи (рис. 3.23), серед них цифри, 26 літер англійського алфавіту та 7 службових символів. Цей код може бути розширеним для кодування усіх 128 символів ASCII шляхом подвоєння числа знаків, які припадають на один символ.

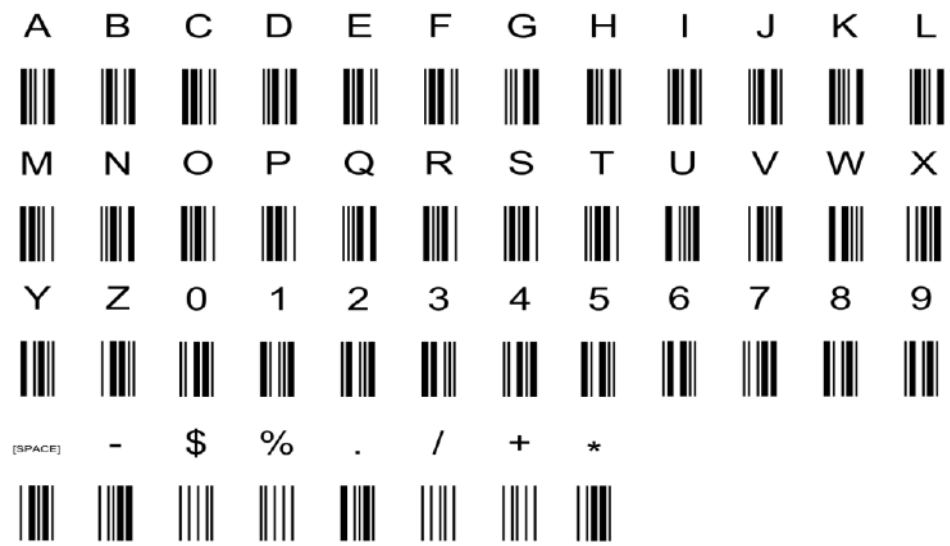
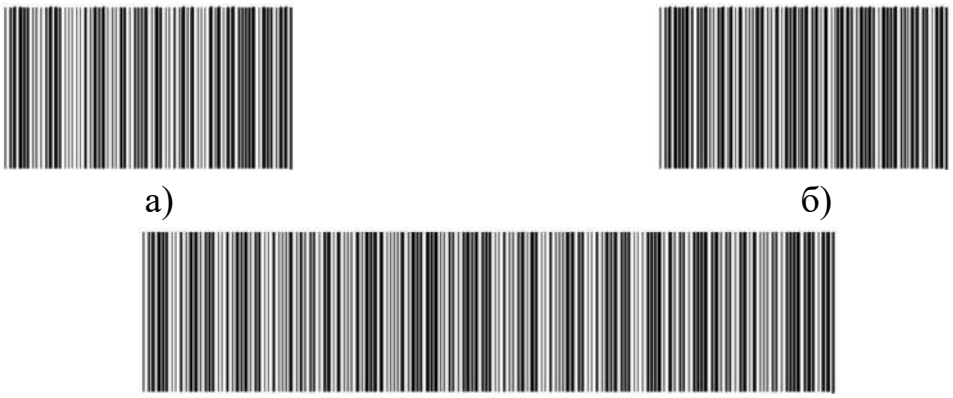


Рисунок 3.23 – Відображення символів у штриховому коді Code 39 [110]

Іноді, цей код називають «Code 3 of 9». Його назва пов’язана із структурою зображення знаків «3 з 9» (рис. 3.24), де три елементи знаку (два штриха і один пропуск) з дев’яти є широкими, а решта шість – вузькими. Кожен символ починається й закінчується темним штрихом, складається із п’яти темних та чотирьох світлих штрихів. Відношення ширини вузького і широкого штриха може становити від 2,2:1 до 3:1.



а) б)

в)

Рисунок 3.24 – Приклади штрихового коду сімейства 3 of 9 [110]
а) – code 39; б) – FAST REPORT та в) – code 39 extended

Перевагою цього коду є його дуже висока ймовірність зчитування, яка може бути збільшена додаванням в символ контрольного знаку. Ймовірність помилки зчитування становить не більше $3{,}33\times10^{-7}$.

3.5.3 Двохплощинний штрих-код Aztec

Цей код, із високою щільністю запису, відноситься до двохплощинних, оскільки його зчитування та декодування здійснюється у двох площинах. Він дозволяє кодувати до 3750 символів повного набору ASCII-символів (256 байт). Штрих-код являє собою квадратну матрицю з концентричними квадратами в центрі, які призначені для визначення позиції коду відносно зчитувального пристрою. Дані у вигляді чорних і білих модулів (елементарних квадратів чорного або білого кольору) розміщуються на різній відстані від центра за периметром опорних квадратів (рис. 3.25).

Такий спосіб розміщення модулів дозволяє кодувати різний обсяг даних, та є пропорційним розміру матриці. Окрім цього, можуть й використовуватись різні способи виявлення та корекції помилок на основі кодів Ріда-Соломона. Параметрами для штрих-коду Aztec є розміри елементарного модуля та спосіб виявлення й корекції помилок. Мінімальні розміри штрих-коду складають 15×15 модулів (що дозволяє кодувати 12 ASCII-символів із 40% надлишку), максимальні – 151×151 (до 3750 символів із 25% надлишку).

а) б) в)

Рисунок 3.25 – Приклади штрихового коду сімейства Aztec [110]
а) – Full Aztec; б) – Compact Aztec та в) – Aztec Rune

Вибір конкретного типу штрих-коду залежить від багатьох чинників: обсягу та складу записуваних даних, необхідної надійності зчитування, допустимих розмірів штрих-коду, вартості зчитуючих пристроїв.

До переваг штрихових кодів слід віднести:

– низьку вартість ідентифікатора та пристроїв для друку;

– можливість запису на ідентифікатор цифрової та літерної інформації різної довжини.

Основним недоліком штрихового коду є слабкий захист від копіювання або підробки. Штрих-код може бути скопійованим за допомогою

копіювального апарату або іншого оптичного пристрою зчитування. У деяких системах друку штрих-код закривається плівкою, непрозорою для видимого світла, але достатньо прозорою в інфрачервоному діапазоні.

Слід пам’ятати, що усі параметри штрихових кодів стандартизовані (ширина ліній, відстань між ними, кількість ліній, які кодують один символ тощо), тому формування або відтворення штрихового коду із необхідними даними не являє жодної складності. Аналогами штрих-кодів в даний час є голографічні етикетки (марки) для захисту товарів.

3.5.4 Апаратне забезпечення зчитування штрихового та матричного кодування

Ефективність СКУД з використанням штрихового та матричного кодування безпосередньо залежить від характеристик зчитувальних пристроїв. На відміну від побутових веб-камер, професійні сканери для СКУД повинні забезпечувати миттєве розпізнавання кодів у широкому діапазоні умов.

Сучасні зчитувачі (наприклад, серія QR600 від ZKTeco або STid Architect) використовують монохромні CMOS-сенсори з високою роздільною здатністю (наприклад, 1280×960 пікселів). Використання монохромних сенсорів замість кольорових дозволяє досягти кращої контрастності та чіткості меж модулів коду, що важливо для швидкого декодування. Оптична система зчитувача зазвичай має широкий кут огляду – близько 50˚ по горизонталі, що забезпечує комфортне сканування без необхідності точного позиціонування смартфона.

Важливим параметром є також «імунітет» до навколишнього освітлення. Професійні модулі здатні працювати при інтенсивності світла від 0 до 100000 люкс, що дозволяє встановлювати їх на вулиці під прямими сонячними променями. Для роботи в повній темряві зчитувачі оснащуються вбудованим підсвічуванням (білим або інфрачервоним) та цілевказівними променями, які допомагають користувачеві зорієнтувати пристрій.

Використання протоколів OSDP (Open Supervised Device Protocol) замість Wiegand дозволяє забезпечити шифрування каналу зв’язку між зчитувачем та контролером, що додає ще один рівень захисту до системи.

Однією з найбільших технічних проблем СКУД на базі матричних кодів є фізика взаємодії сканера з екраном смартфона. Більшість сканерів, розроблених для паперових носіїв, демонструють незадовільні результати під час роботи з підсвіченими дисплеями.

Екрани смартфонів зазвичай мають глянцеве покриття, яке створює дзеркальні відблиски. Коли зчитувач спрямовує власне підсвічування на екран, світло відбивається прямо в сенсор, створюючи «сліпу пляму», яка приховує частину коду. Для вирішення цієї проблеми необхідно тримати смартфон під кутом 15 … 20˚ до площини сканера, що дозволяє відхилити відбитий промінь.

Окрім цього, сучасні OLED та LCD дисплеї мають власну поляризацію та частоту оновлення (60 … 120 Гц). Невідповідність між частотою оновлення екрана та частотою кадрів CMOS-сенсора сканера може призводити до появи ефекту мерехтіння або муарових візерунків на цифровому зображенні. Це змушує алгоритми розпізнавання витрачати більше часу на обробку, що знижує пропускну здатність точки доступу.

Користувачі часто намагаються встановити максимальну яскравість екрана для кращого зчитування, але це може бути контрпродуктивним. Надмірна яскравість «розмиває» межі чорних модулів на білому тлі, що особливо критично для щільних кодів Data Matrix. Найбільш стабільні результати демонструють скріншоти кодів, оскільки вони виключають випадкове масштабування або оновлення сторінки додатком у момент сканування.

Незважаючи на домінування мобільного доступу, фізичні перепустки з надрукованими кодами залишаються актуальними для разових відвідувачів та ідентифікації персоналу на об’єктах з обмеженим використанням смартфонів.

Незважаючи на технологічну досконаліть, СКУД на базі штрихового та матричного кодування стикаються зі специфічними загрозами безпеки.

Контрольні запитання

1. Дайте визначення терміну «захищеність ідентифікатора».
2. Дайте визначення терміну «маніпулювання» у контексті СКУД.
3. З яких основних компонентів складається пасивний ідентифікатор?
4. За якими ознаками класифікують ідентифікатори СКУД?
5. Назвіть основні недоліки протоколу Wiegand, які роблять його вразливим у сучасних системах безпеки.
6. Назвіть основну конструктивну відмінність між контактною смарт-картою та електронною таблеткою.
7. Назвіть п’ять чинників, які впливають на дальність зчитування пасивного ідентифікатора.
8. Назвіть типи контактних смарт-карток враховуючи структуру їх пам'яті та функціональні можливості.
9. Назвіть, з точки зору безпеки, основні переваги та недоліки використання технології штрихового кодування у порівнянні з RFID/NFC-технологіями?
10. У чому полягає головна перевага низькочастотного діапазону?
11. У чому полягає основна вразливість методу ідентифікації, яка базується на знаннях суб'єкта?
12. У чому полягає основна технічна різниця між NFC та BLE?

13. У чому полягає особливість будови дротика Віганда?

14. У чому полягає різниця між квазістатичними та квазідинамічними біометричними ознаками?

15. У чому полягає, з точки зору способу кодування даних та напрямку зчитування, принципова різниця між одновимірними та двовимірними кодами?

16. Чим відрізняється симетричне магнітне перемикання від асиметричного під час формування Wiegand-ефекту?

17. Чим відрізняються коди сімейства «2 з 5» від Code 39?

18. Чому використання смартфонів, з точки зору ідентифікатора, вважають безпечнішим за використання статичних пластикових карток?

19. Чому дані з карти Віганда можна зчитувати навіть за дуже повільного її руху через зчитувач?

20. Чому професійні зчитувачі СКУД використовують монохромні CMOS-сенсори під час розпізнавання кодів?

21. Чому термін «радіочастотний принцип ідентифікації» вважається більш коректним у порівнянні із «безконтактною» або «дистанційною» технологією?

22. Як відбувається інформаційний обмін між зчитувачем та картою на фізичному рівні?

23. Як саме передаються логічні «0» та «1» через Wiegand-інтерфейс?

24. Яке фізичне явище пояснює дискретну зміну намагніченості феромагнетика під час безперервної зміни напруженості зовнішнього поля?

25. Який вид несанкціонованого доступу є найбільш небезпечним для будь-якого методу ідентифікації?

26. Який тип карт має вищий рівень захисту від підробки та чому?

27. Який фізичний механізм передачі даних використовується в ультрависокочастотному діапазоні?

28. Яким чином забезпечується живлення мікросхеми у безконтактних смарт-картах та електронних таблетках?

29. Які доріжки притаманні стандартній магнітній карті та для чого вони призначені?

30. Які ключові конструктивні особливості шаблонів пошуку дозволяють сканерам розрізняти коди Data Matrix та QR-коди?

31. Які основні (технологічні) діапазони частот виокремлюють у глобальній практиці СКУД?

32. Які основні методи ідентифікації суб’єктів доступу використовуються в СКУД?

33. Які режими роботи підтримує технологія NFC? Який з них є ключовим для СКУД?

РОЗДІЛ 4. Біометричні системи

Біометричний метод контролю доступу є одним із небагатьох напрямків ідентифікації, який зазнав, на сьогодні, стрімкого розвитку. Цей метод засновано на використанні характерних та унікальних фізіологічних особливостей або поведінкових характеристик людини, за допомогою яких здійснюється ідентифікація її особистості. З поміж основних переваг цього методу варто відмітити високий ступінь ймовірності одночасного вирішення завдань, які пов'язані із її ідентифікацією та автентифікацією.

На практиці широко застосовують дві групи систем, які використовують біометричний метод ідентифікації.

До першої групи прийнято входять біометричні системи, які аналізують статичні характеристики СД (папілярний візерунок пальців, геометрія долоні, райдужна оболонка ока тощо). Ці ідентифікаційні ознаки є постійними фізичними характеристиками людини та зазнають вкрай слабких змін у часі – тому вони отримали назву «квазістатичні».

До другої групи належать біометричні системи, які аналізують динамічні ідентифікаційні ознаки людини під час виконання нею певних дій (динаміка відтворення підпису, параметри мови, клавіатурний почерк тощо). Ці ознаки знаходяться під постійним впливом як виконуваних дій (контрольованих, керованих), так і психологічних чинників, які є менш керованими – їх називали «квазідинамічними». Тут варто пам'ятати, що ці характеристики можуть змінитись у часі, а отже зареєстрований біометричний зразок необхідно піддавати періодичному оновленню.

Враховуючи усі переваги біометричного методу ідентифікації не потрібно забувати про етичну сторону цього питання, адже СД не завжди готові, щоб їх відбитки пальців або інші фізіологічні характеристики були зафіксовані системою. Ще одним важливий моментом є те, що перед аналізом обраних біометричних ІО людини, необхідно впевнитися, що пред'явлені характеристики дійсно належать живій істоті.

У тому випадку коли система не дозволяє, із досить високим ступенем достовірності, встановити, що надані для ідентифікації біометричні ознаки відповідають живій істоті, то не варто забувати про існування потенційних загроз для СКУД.

4.1 Передумови біометричної ідентифікації

Під час запису біометричних ознак в пам'ять системи необхідно переконатись у достовірності опрацьованої нею інформації для подальшої успішної ідентифікації СД [108]. При цьому занесені еталонні біометричні ознаки мають містити достатню кількість інформації для можливості

порівняння їх із зчитуваними для прийняття рішення з необхідною ймовірністю. Наприклад, під час ідентифікації за відбитками пальців необхідно переконатися, що еталонний відбиток не був «змазаний» та містить достатню кількість характерних деталей (завитків, пересічний папілярних ліній), які дозволяють однозначно ідентифікувати користувача. У тому випадку коли еталонний відбиток (образ) не володіє необхідною кількістю характеристик, то система має запропонувати СД повторно його занесення або завести новий зразок (наприклад, інший палець).

Якщо зчитаний еталонний відбиток відповідає зазначеним вимогам, то тоді відбувається його перетворення у форму, яка є зручною для пошуку в базі даних з подальшим його порівнянням. Як правило, зчитаний образ містить велику кількість надлишкової інформації, якою нехтує система під час ідентифікації СД. У тому випадку коли не використовується перетворення та стиснення образу, розмір пам’яті, яка необхідна для зберігання усіх відбитків, може бути занадто великою, а час пошуку необхідного образу в БД занадто тривалим.

Слід зауважити, що процес занесення біометричних образів в пам’ять системи повинен складається із наступних етапів:

– пошук та зчитування біометричних ознак;

– перевірка відповідності пред’явлених біометричних ознак (БО) живій особі;

– перевірка достовірності зчитаної еталонної інформації для успішної ідентифікації СД;

– перетворення зчитаного образу у форму, яка є зручною для подальшої роботи та зберігання (формування еталону ідентифікаційних ознак);

– занесення еталонного образу в пам’ять системи.

На практиці, гіпотези дозволяють розглянути, які ж саме події можуть мати місце під час ухвалення рішення системою біометричної ідентифікації (СБІ). Їх є дві:

– пред’явлений біометричний ідентифікатор (БІ) належить уповноваженому користувачу;

– пред’явлений БІ не належить уповноваженому користувачу.

Отже, в системі біометричної ідентифікації здійснюється прийняття рішень про дозвіл або заборону доступу (табл. 4.1).

Імовірність дозволу доступу піж час надання діючого ідентифікатора характеризує ймовірність правильного вирішення доступу ($Р_{пд}$). Заборона доступу, під час пред’явлення діючого ідентифікатора, називається помилковою відмовою у доступі, та характеризується ймовірністю $Р_{хд}$ варто зазначити, що ці події й утворюють повну групу, тобто:

$$P_{пд}+P_{хд}=1. \quad (4.1)$$

Таблиця 4.1 – Матриця рішень системи біометричної ідентифікації

Гіпотеза	Рішення системи ідентифікації	
	Дозвіл на доступ	Заборона у доступі
Надано дійсний ідентифікатор	Правильний дозвіл на доступ ($P_{пд}$)	Хибний дозвіл на доступ($P_{хд}$)
Надано не дійсний ідентифікатор	Несанкціонований доступ ($P_{нд}$)	Санкціонований відмова у доступі ($P_{сд}$)

Відповідно й імовірність дозволу на доступ під час пред'явлення недіючого ідентифікатора називається ймовірністю несанкціонованого доступу ($P_{нд}$), а імовірність заборони доступу під час надання недіючого ідентифікатора – ймовірністю правильної відмови у доступі ($P_{сд}$). Так як і для попереднього випадку, ці події здатні сформувати повну групу подій:

$$P_{нд}+P_{сд}=1. \quad (4.2)$$

На практиці прийнято виражати ймовірність $P_{нд}$ через FAR (False Acceptance Rate) або FMR (False Match Rate), а $P_{хд}$ – через FRR (False Rejection Rate) або FNMR (False Non-Match Rate). Помилкову відмову у доступі та несанкціонований дозвіл на доступ називають помилками першого і другого роду відповідно.

Очевидно, що для будь-якої системі вкрай бажаною є якнайменше значення ймовірностей $P_{нд}$ і $P_{хд}$, хоча ця умова є суперечливою. Зрозумілим стає те, що під час зниження ймовірності несанкціонованого доступу збільшується ймовірність відмови у доступі чинному СД системи, і навпаки, зниження ймовірності відмов у доступі уповноваженим користувачам СБІ неминуче призводить до збільшення ймовірності несанкціонованого доступу.

Деякі біометричні системи дозволяють налаштовувати згадані вище характеристики, що задовольняє вирішенню поставлених задач. Так у системах, де необхідно отримати високу пропускну здатність, доцільно знизити $P_{хд}$, що дозволить уникнути затримок під час проходу СД. На об'єктах із підвищеною категорією надійності, яка не вимагає високої пропускної здатності, необхідно зменшити $P_{нд}$ (у цьому випадку система буде потребувати декілька спроб читання біометричних характеристик СД для його достовірної ідентифікації).

Ще однією характеристикою, яка використовується у системах біометричної ідентифікації є ймовірність відмови системи у реєстрації користувача ($P_{вр}$). під час занесення еталонного зразка ідентифікаційних

характеристик користувача можливою є така ситуація, коли отриманої від нього біометричної інформації виявляється недостатньо для його подальшої однозначної ідентифікації (така ситуація може виникнути, у тому випадку коли відбиток пальця містить мало характерних елементів, які використовуються для порівняння відбитків між собою, або палець був пошкоджений або забруднений). Така характеристика виражається через параметр FTE (Failure To Enroll Rate).

4.2 Квазістатична біометрія

Сучасна епоха цифрової трансформації докорінно змінила підходи до забезпечення безпеки та автентифікації особистості. Перехід від традиційних методів, заснованих на володінні матеріальними об'єктами або знанні секретних кодів, до систем, що базуються на невід'ємних фізіологічних характеристиках людини, став черговим етапом розвитку глобальної інфраструктури безпеки [73]. Статична біометрія, яка аналізує фіксовані анатомічні параметри – такі як відбитки пальців, геометрія обличчя та унікальні структури ока – на сьогоднішній день є найбільш розповсюдженим і довіреним класом технологій ідентифікації. На відміну від динамічної або поведінкової біометрії, що вивчає патерни дій, статичні методи зосереджені на морфологічних ознаках, які залишаються стабільними протягом десятиліть, що забезпечує високу точність та довгострокову надійність.

Ринок безконтактних біометричних рішень демонструє стрімке зростання, зумовлене потребою в гігієнічних та швидких методах взаємодії, особливо в умовах постпандемічного світу. Прогнозується, що обсяг цього ринку зросте з 26,72 мільярдів доларів США у 2025 році до вражаючих 77,46 мільярдів доларів до 2031 року, демонструючи середньорічний темп зростання на рівні 19,43%. Ця динаміка підкреслює стратегічну важливість розуміння технологічних нюансів, що лежать в основі біометричних систем, оскільки вони інтегруються в критичні сектори економіки – від банківської справи та охорони здоров'я до прикордонного контролю та національної безпеки [12].

4.2.1 Ідентифікація за відбитком пальця

Шкіра людини складається із двох шарів, при цьому нижній шар формує велику кількість виступів. На основній частині шкіри виступи розташовуються хаотично, а тому за ними тяжко стежити. На окремих ділянках шкіри кінцівок виступи впорядковані строго у лінії (гребені), які формують унікальні папілярні візерунки. Ідентифікація СД на основі папілярних малюнків пальців рук вперше було запропоновано Г. Фулдсом (H. Faulds) та В. Гершелем (W. Herschel) у 1880 році на сьогодні цей метод ідентифікації є широко відомим й поширеним.

Системи ідентифікації, які працюють на основі відбитків пальців (також

відомі як дактилоскопічні) набули найбільшого поширення серед біометричних систем завдяки зручності користування, невеликих габаритів зчитувальних пристроїв, швидкості ідентифікації та порівняно невисокій вартості [135].

Структурну схему такої системи подано на рисунку 4.1.

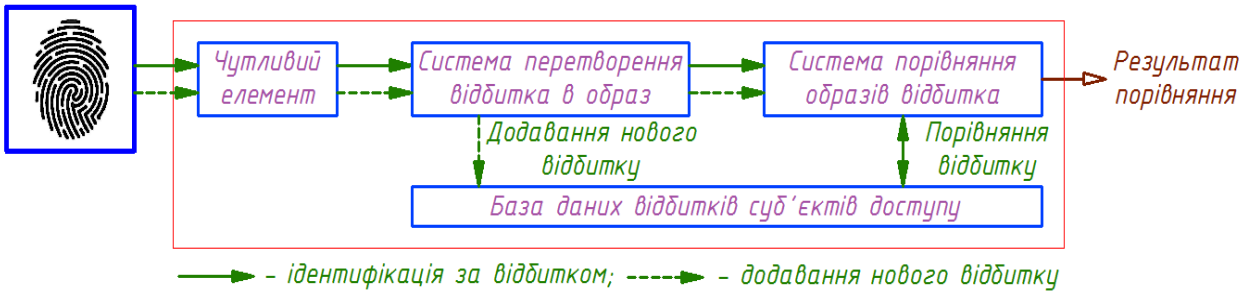


Рисунок 4.1 – Структурна схема зчитувача відбитка пальців [110]

За допомогою чутливого елемента зчитувач знімає папілярний малюнок з пальця СД. Типова роздільна здатність, яку мають сучасні зчитувальні елементи, становить близько 500 точок на дюйм, що відповідає розмірам елементарного чутливого елемента 50×50 мкм (це значення рекомендованим для інтегрованих автоматизованих систем ідентифікації за відбитками пальців). Ширина папілярних виступів становить близько 450 мкм, тому теоретично, достатньо було б мати роздільну здатність чутливого елемента на рівні 112 точок на дюйм (елементарний чутливий елемент 225×225 мкм), однак для повної реалізації усіх можливостей алгоритмів порівняння цієї роздільної здатності недостатньо. Нормативними документами рекомендованим є сканування папілярного малюнка із 256 градаціями сірого на кожен елемент. Однак, за реальних умов достатньо й 64 градацій сірого. При цьому слід пам’ятати, що кожна точка кодується 6 бітами.

На практиці відомими є такі системи, які використовують бінарне квантування зображень відбитків. Початковий відбиток зчитується із роздільною здатністю 500 точок/дюйм та 256 градаціями сірого, займає порівняно великий об’єм пам’яті (наприклад, для зображення розміром 2×3 см, яке містить близько 400×600 елементів вимагає для збереження 240 кбайт пам’яті). Очевидним є те, що зберігання таких об’ємів інформації призведе до значного подорожчання пристрою, а пошук та порівняння зображень такого розміру будуть займати багато часу й вимагати більших обчислювальних ресурсів.

Окрім цього, вкрай небажаним, з точки зору конфіденційності, є збереження відбитків у початковому вигляді. Зазвичай користувачам подобається анонімність, вони не хочуть, щоб відбитки пальців, без їх згоди,

передавались правоохоронним органам або просто були викрадені зловмисниками. Враховуючи це виробники використовують спеціальні методи обробки та зберігання отриманих даних, які не дозволяють відновити початковий відбиток СД.

Для стиснення вихідного зображення зазвичай користуються Вейвлет-перетвореннями. Коефіцієнт стиснення підбирається таким чином, щоб можна було б уникнути втрати інформації, яка необхідна для успішної ідентифікації. На практиці, його максимальне значення становить 10. Після стиснення розмір зображення може сягати десятків кілобайт. Об’єм інформації про відбиток пальця можна істотно зменшити, якщо застосувати класифікацію характерних типів папілярних малюнків та виокремити на його відбитку характерні ознаки, які являють собою початки (закінчення) папілярних ліній або їх злиття (розгалуження). На папілярних малюнках прийнято виділяти декілька типів характерних елементів (рис. 4.2): дуга (arch), петля (loop), виток (whorl), перетин, з’єднання та розгалуження ліній, закінчення ліній, острівці й дельти.

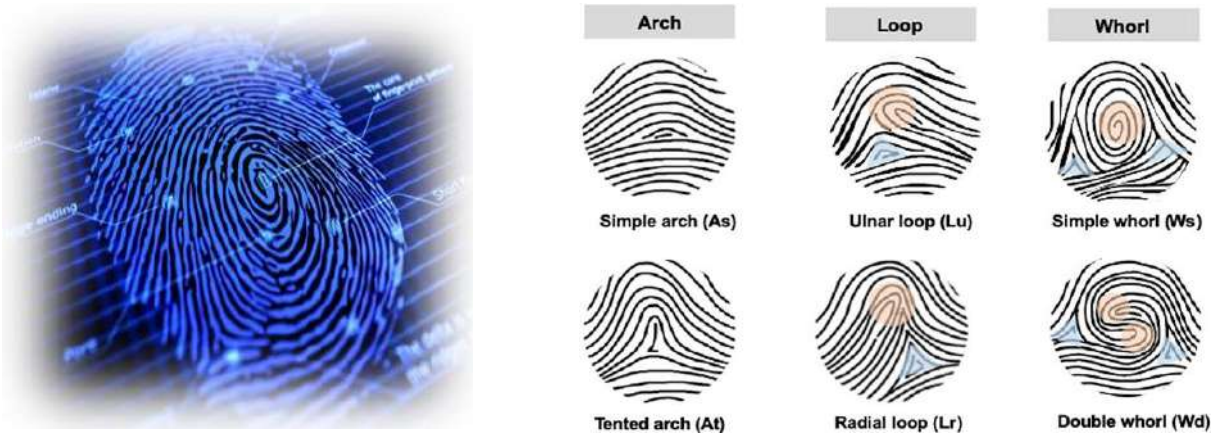


Рисунок 4.2 – Характерні особливості відбитка пальця [110]

Сучасні алгоритми обробки з’єднують характерні точки зображення векторами та описують їх властивості і взаємне розташування. При цьому використовуються відносні відстані між характерними точками зображення, що дозволяє зробити процес порівняння відбитків інваріантним до розташування пальця відносно зчитувача. Зазвичай у відбитку виділяється близько 30 … 40 характерних точок, що й дозволяє створити зразок відбитка розміром від 40 байт до 1 кбайта. Зауважимо, що за таким зразком неможливо відновити початковий відбиток, проте можна порівнювати відбитки один з одним.

Ідентифікація СД здійснюється шляхом порівняння образу пред’явленого відбитка користувача із еталонними зразками, які зберігаються в БД зчитувача [75]. При цьому можливими є два алгоритми роботи:

1. Порівняння образу зчитаного відбитка із усіма наявними зразками, які

збережено в пам’яті зчитувача. Якщо такий зразок не знайдено, то системою приймається рішення про відмову у доступі.

Перевагою цього алгоритму є можливість роботи тільки з відбитком пальця без використання додаткових ідентифікаторів.

2. Порівняння образу зчитаного відбитка із одним конкретним зразком, який збережено у пам’яті зчитувача. В цьому випадку біометричний зчитувач до аналізу образу відбитка пальця повинен містити інформацію про те, який користувач буде надавати палець для ідентифікації (зазвичай це досягається за рахунок поєднання зчитувача відбитка пальця з кодовим пристроєм або кардридером).

Під час ідентифікації СД системою за другим алгоритмом роботи кожному користувачеві присвоюють унікальний пароль або видається картка. СД вводить пароль або пред’являє карту, після чого прикладає палець до зчитувального пристрою. Зчитувач на основі введеного пароля або номера карти вибирає із БД зразок того відбитка, який відповідає цьому користувачу, та на його основі здійснює порівняння. Для цього алгоритму притаманні наступні переваги:

– можливість одночасного використання різних методів ідентифікації;

– більш висока швидкодія (у порівнянні із першим алгоритмом, оскільки здійснюється порівняння зчитаного образу тільки з одним еталонним, а не перебір всіх зразків);

– можливість зберігання у БД інформації про велику кількість СД.

На практиці відомими є декілька технологій зчитування відбитків пальців. Перша та найбільш поширена заснована на використанні оптичної системи (рис. 4.3): призми та декількох лінз із вбудованим джерелом світла.

Світло, яке потрапляє на призму, відбивається від поверхні де розташовується палець СД, та виходить через іншу сторону призми, потрапляючи на оптичний давач (монохромна камера на основі ПЗС-матриці), де й формується зображення. Перевагою такого способу зчитування відбитка пальців є її, порівняно невисока, вартість реалізації. До недоліків відносять залежність коефіцієнта відображення від параметрів шкіри (сухість і забрудненість) та забруднення сканера (місця контакту пальця з призмою).

Незважаючи на свою популярність, оптичні сенсори стикаються з проблемою «латентних відбитків», коли залишки жиру від попередніх користувачів можуть створювати перешкоди для нових сканувань. Крім того, оскільки ці системи фіксують лише двовимірне зображення поверхні, вони теоретично більш вразливі до атак із використанням високоякісних фотографій або роздрукованих муляжів, якщо не застосовуються додаткові методи перевірки життєвості.

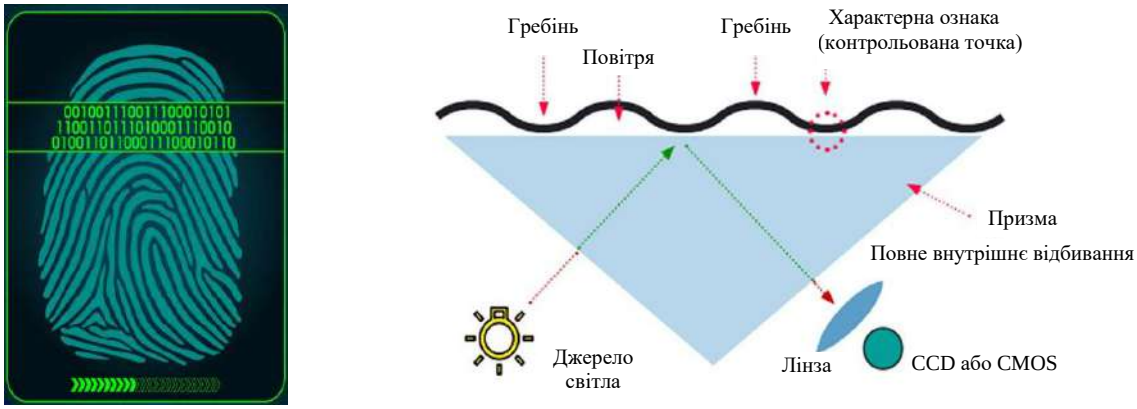


Рисунок 4.3 – Функціональна схема оптичного зчитувача відбитка пальця [110]

Інший спосіб засновано на вимірюванні різниці електричних потенціалів між гребенями та впадинами на шкірі пальця СД із використанням напівпровідникової пластини. Палець у зчитувачі виступає у якості однієї із пластин конденсатора (рис. 4.4). Іншою пластиною конденсатора слугує напівпровідникова поверхня чутливого елемента, яка містить кілька десятків тисяч конденсаторних пластин із щільністю зчитування 500 елементів/дюйм. В результаті цього отримують зображення гребенів та впадин шкіри на пальці.

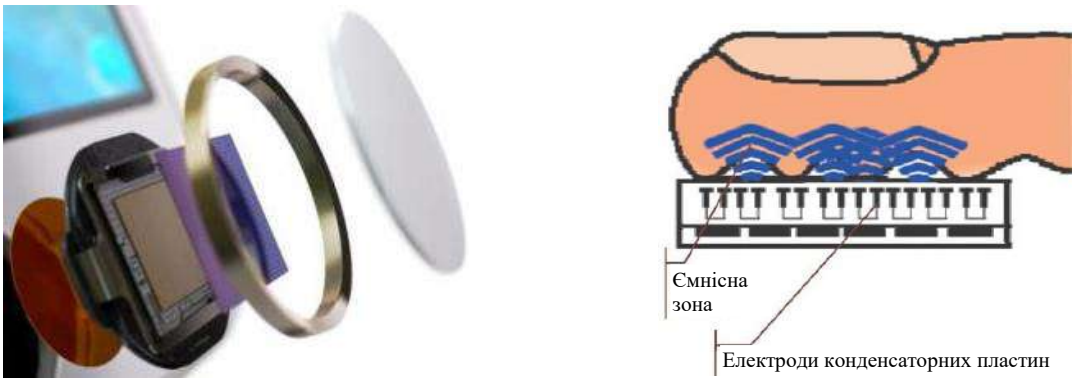


Рисунок 4.4 – Напівпровідниковий зчитувач відбитка пальця [110]

У даному випадку жировий баланс шкіри та ступінь її чистоти не відіграють такої істотної ролі, як в попередньому випадку. Якщо говорити про недоліки цього методу, то напівпровідниковий чутливий елемент потребує експлуатування в герметичній оболонці, а додаткові покриття зменшують чутливість системи. Окрім того на якість зображення впливає й сильне зовнішнє електромагнітне поле та підвищена вологість.

Існують також напівпровідникові чутливі елементи, які дозволяють фіксувати різницю температур між гребенями та западинами шкіри на пальці. Перевагою цієї технології є висока стійкість до електромагнітних перешкод, забруднень, вологості.

На сьогодні відомо ще про один, інноваційний, метод реалізації зчитувальної системи на основі електрооптичний полімер (система TactileSense). Цей матеріал дозволяє отримати оптичне зображення відбитка пальця із високою роздільною здатністю, після чого переводиться в цифровий формат та обробляється. При цьому такий метод є нечутливим до стану шкіри та ступеня її забруднення (у тому числі хімічного), а зчитуючому пристрою притаманні достатньо малі розміри.

Додатковою функцією цих сканерів є встановлення приналежності пальця до живої людини. Даний ефект досягається за рахунок аналізу електропровідності шкіри та її температури.

Найбільш технологічно досконалий підхід до дактилоскопії є ультразвуковий метод. Він базується на принципі ехолокації. Сканер випромінює високочастотні звукові імпульси, які відбиваються від пальця. Оскільки акустичний імпеданс гребенів шкіри та повітря в борознах суттєво різниться, сенсор фіксує час повернення ехо-сигналу та будує тривимірну модель папілярного візерунка.

Ключовою перевагою ультразвуку є його здатність проникати крізь верхні шари епідермісу, зчитуючи структуру дермального шару шкіри. Це робить технологію стійкою до поверхневих пошкоджень, таких як порізи або потертості, а також дозволяє ігнорувати забруднення (воду, масло, пил), які часто стають критичними для оптичних або ємнісних аналогів. Ультразвукові сенсори можуть бути розміщені під склом дисплея, що сприяє розвитку безрамкових дизайнів мобільних пристроїв, зберігаючи при цьому найвищий рівень безпеки за рахунок аналізу 3D-геометрії.

4.2.2 Райдужна оболонка ока

Ідентифікація за характеристиками ока вважається найбільш безпечним і точним методом статичної біометрії. Хоча райдужна оболонка і сітківка часто згадуються разом, вони представляють абсолютно різні технологічні підходи.

Райдужна оболонка ока людини (РО) – це мембрана, яка оточує зіницю (зазвичай, її діаметр не перевищує 11 мм). Характерною особливістю райдужної оболонки ока є її неповторний малюнок, який практично не змінний після досягнення людиною одного року. Унікальність такого малюнка обумовлена генотипом особистості (при чому, суттєві відмінності малюнка РО спостерігають навіть у близнюків). Варто акцентувати увагу на тому, що ймовірність того, що існує дві райдужні оболонки ока людини із однаковим малюнком становить 10^{-72} [132].

Малюнок РО містить велику кількість дрібних елементів, за якими можна ідентифікувати СД, та є стабільним і найбільш захищеним органом протягом усього його життя.

Системи ідентифікації людини за райдужною оболонкою ока вважається однією із найбільш надійних біометричних технологій. Імовірність винекнення помилки під час допуску суб'єкта у систему становить 0,000001 за ймовірності відмови в доступі уповноваженому користувачу 0,02.

Система ідентифікації використовує відеокамеру, що зчитує малюнок райдужної оболонки ока. Сучасні зчитувачі дозволяють робити це з відстані від 10 сантиметрів до одного метра, що забезпечує високу пропускну здатність у таких місцях, як аеропорти. При цьому наявність у людини окулярів або контактних лінз не впливає якість зчитаного зображення.

Для найпростішої системи автентифікації необхідно мати чорно-білу телевізійну камери та плату вводу відеозображення у комп'ютер. Підсвічування ока варто здійснювати декількома малопотужними світлодіодами, які випромінюють інфрачервоне випромінювання в діапазоні від 700 до 900 нм. Наведення камери здійснюється за рахунок системи дзеркал, а фокусування – об'єктивом із трансфокатором (для деяких моделей зчитувачів наведення камери відбувається автоматично під час наближення СД на відстань ближче півметра). Після наведення камери зчитувач аналізує зображення та виділяє в ньому зовнішню межу райдужної оболонки, зрачкову область і центр зіниці (рис. 4.5). Після чого визначається область райдужної оболонки, яка й використовується для подальшого аналізу (виключаються області, які закриті повіками, тіньові та відбиті області).

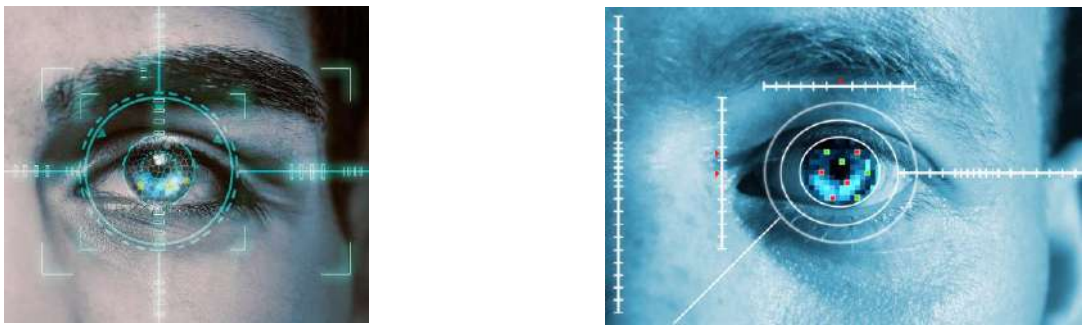


Рисунок 4.5 – Область зчитування райдужної оболонки ока [110]

Для сучасних зчитувачів притаманні високі характеристики розпізнавання, які досягаються навіть з аналізу менше 40% поверхні РО. Уся отримана інформація обробляється у полярній системі координат.

Отримане оптимізоване зображення перетворюється у цифровий зразок ідентифікаційних ознак (зазвичай, це займає декілька сотень байт пам'яті зчитувача). Під час порівнянні зчитаного образу з еталонним зразком із наявної БД зчитувача відбувається обчислення відстані Хеммінга, яка характеризує ступінь відмінності між двома образами. Кожен з 2048 біт образу, який

отримано під час зчитування, попарно порівнюється із бітом образу із пам’яті пристрою, а отримане значення обчислюється логічним оператором, який виключає «АБО».

Наприклад, якщо перший біт відсканованого образу дорівнює «1», а перший біт образу з пам’яті «0», то це означає, що збігу немає – як результат заносять «1». І навпаки, якщо є збіг, то як результат заносять «0». Далі порівнюються другі біти образів, потім треті тощо. У наявних, на сьогодні, системах порівняння усіх 2048 пар біт відбувається досить рідко, оскільки райдужна оболонка ока людини не повністю доступна для сканування.

Після порівняння усіх доступних пар біт кількість отриманих розбіжностей ділиться на загальне число порівнянь. Отримане значення й називають відстанню Хеммінга.

Для прикладу, розглянемо такий випадок коли під час порівняння 2048 пар біт було знайдено 204 розбіжності (рис. 4.6), тоді відстань Хеммінга обчислюється як 204:2048≈0,1. Це говорить про те, що два образи, які порівнюються між собою, відрізняються на 10%.

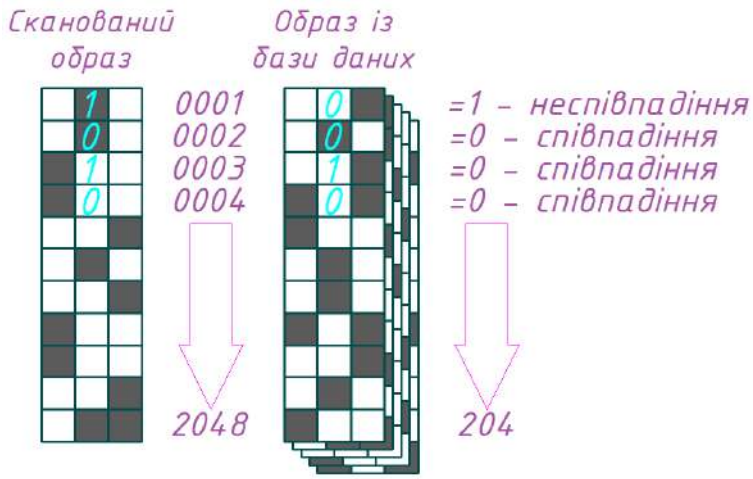


Рисунок 4.6 – Обчислення відстані Хеммінга [110]

Логічний оператор, який виключає операцію «АБО», прийнято реалізовувати хоча б на 32-розрядному процесорі, який дозволяє достатньо швидко виконати, за одну машинну операцію, дію для двох цілих десяткових чисел із діапазону від 0 до 4294967295 (на процесорі частотою 300 МГц за одну секунду виконується порівняння приблизно 100000 малюнків РО ока людини).

На підставі експериментальних даних, за наявної вибірки порівнянь образів райдужних оболонок (не менше 10^6), будують гістограми щільності ймовірностей, за якими оцінюють ступінь відповідності відсканованого для ідентифікації образу та еталонного зразка, який є наявним у базі даних пристрою.

4.3 Квазідинамічна біометрія

Концепція квазідинамічної біометрії полягає у тому, що категорії біометричних ознак базуються на вимірюванні фізіологічних та поведінкових процесів, які демонструють високу повторюваність у часі, проте за своєю фізичною природою є динамічними. На відміну від статичних дескрипторів, таких як відбиток пальця або малюнок сітківки, квазідинамічні параметри, зокрема хода, голос та клавіатурний почерк, дозволяють реалізувати концепцію «прозорого» доступу, де автентифікація відбувається пасивно, не вимагаючи від суб'єкта спеціальних маніпуляцій або зупинок. Таким чином, основною специфічною особливістю ідентифікації та автентифікації СД на основі квазідінамічних біометричних ознак є можливість істотної зміни цих ідентифікаційних ознак у часі. Ці зміни можуть бути пов'язані із великою кількістю зовнішніх чинників, які безпосередньо впливають на людину, а також його фізіологічних особливостей (фізичний стан, настрій тощо).

4.3.1 Аналіз підпису та клавіатурного почерку

Підпис людини давно використовувався для встановлення її особистості. Роботи із автоматизації цього процесу вказують на те, що для досягнення необхідної надійності ідентифікації необхідно враховувати не тільки саму форму підпису але й динаміку руху пера та ступінь його натискання. Лише це дозволятиме ідентифікувати СД із високою надійністю [80].

Навчитися підписуватися схожим підписом не так вже й складно. Однак відтворити цей підпис із тією ж динамікою дуже складно (рис. 4.7).

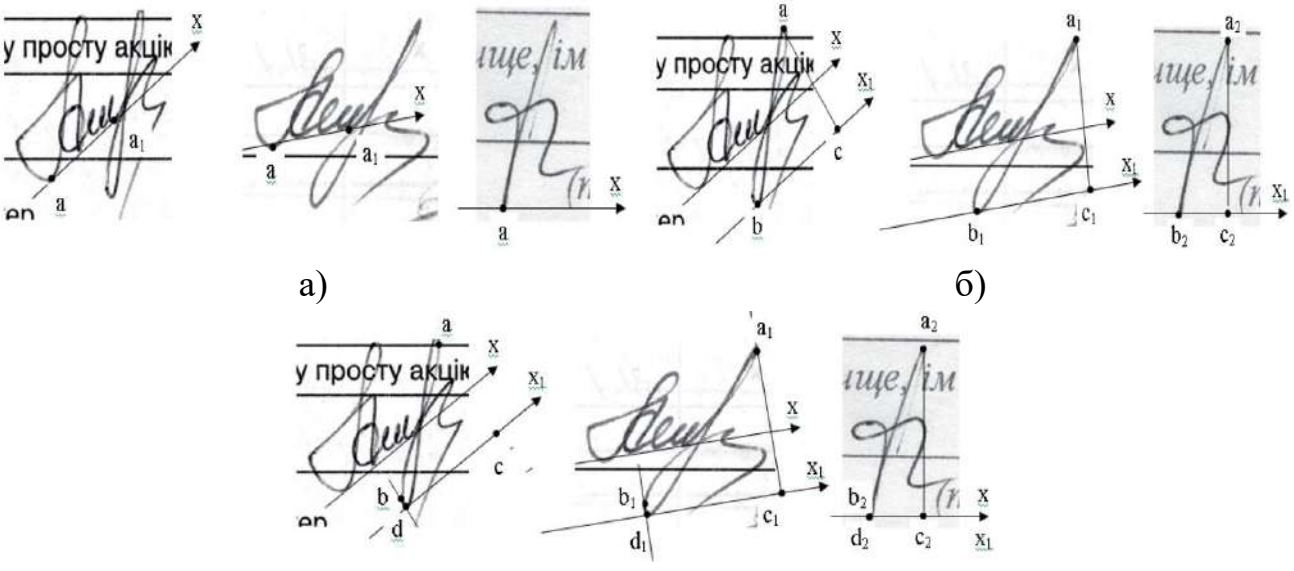


Рисунок 4.7 – Ідентифікаційна ознака за підписом [110]
а) – визначення лінії підпису; б) – визначення протяжності рухів за вертикаллю;
в) – визначення протяжності рухів за горизонталлю

Очевидним є й те, що ідентифікація на основі підпису не може знайти широкого застосування в СКУД у зв'язку із низькою її пропускною здатністю. Такі системи зазвичай застосовуються у банківських додатках.

Клавіатурний почерк (Keystroke Dynamics) – це найбільш доступна форма поведінкової біометрії, яка вимірює унікальні ритми та часові інтервали під час друку. Вона стає ключовою в стратегіях Zero Trust, оскільки дозволяє підтверджувати ідентичність користувача безперервно, поки він працює за комп'ютером [71].

Клавіатурний почерк базується на ідеї «fist» (кулака) – терміну, що пішов від операторів телеграфу часів Другої світової війни, які могли впізнавати один одного за характерним ритмом передачі коду Морзе. У сучасних системах аналізуються наступні параметри: час утримування, час польоту, затримка, тиск та кут.

Час утримання – час від натискання клавіші до її відпускання.

Час польоту – час між відпусканням однієї клавіші та натисканням наступної.

Затримка – загальний час між послідовними натисканнями (key-down to key-down).

Тиск та кут (на мобільних пристроях) – додаткові вектори даних, що знімаються з сенсорних екранів та акселерометрів.

Паттерни друку є нейрофізіологічно обумовленими та стабільними, як і рукописний підпис. Проте вони можуть змінюватися під впливом втоми, стресу, травм або зміни типу клавіатури. Для компенсації цих факторів системи використовують адаптивне навчання, яке постійно оновлює біометричний шаблон користувача на основі його останніх дій.

4.3.2 Голосова ідентифікація

Голосова автентифікація стала важливим компонентом СКУД для віддаленого доступу, банківських операцій та управління розумними будівлями. Привабливість даного методу полягає у зручності застосування. Основною складністю, яка пов'язаною з ним, це досягнення необхідної точності ідентифікації. Спектральний склад мови (рис. 4.8) визначається не тільки фізіологічними та поведінковими чинниками, але й наявністю можливих перешкод – оточуючим шумом.

Не варто забувати й про низьку захищеність цього способу ідентифікації від знімання інформації за акустичним каналом (можливий запис ідентифікатора з подальшим його відтворенням для несанкціонованого подолання СКУД).

На сьогодні голосова ідентифікація застосовується для управління доступом в приміщеннях із низькими та середніми вимогами, які висуваються

до їх безпеки [76]. Ідентифікація за голосом залишається зручним, але, в той же час, не надійним способом ідентифікації СД.

Рисунок 4.8 – Ідентифікаційна ознака за голосом [110]

4.3.4 Ідентифікація за ходою

Цей напрямок пов’язаний, перш за все, із автоматизованим виявленням конкретних осіб серед інших СД (для пошуку злочинців, які перебувають у розшуку тощо) [127].

Прикладом може бути система CCTV (Closed-Circuit Television) для розпізнавання СД за ходою, як досить широко застосовується у сфері антитерористичної діяльності (рис. 4.9).

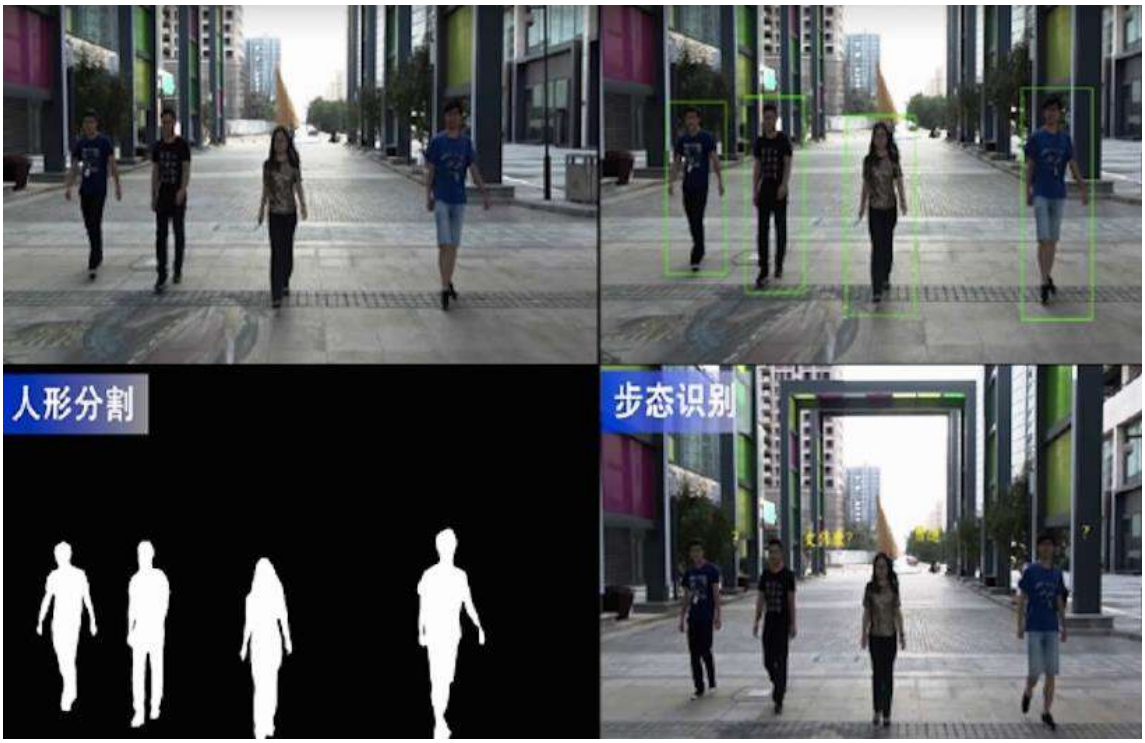


Рисунок 4.9 – Фрагменти програмного забезпечення CCTV для пошуку зловмисників за ходою [110]

Дана технологія ідентифікування заснована на унікальній ознаці – стиль ходи СД.

Основним методом розпізнавання ходи залишається аналіз силуетів, отриманих шляхом фонового віднімання з відеопотоку. Центральною концепцією тут є енергетичне зображення ходи (GEI – Gait Energy Image), яке представляє собою просторово-часову стиснуту характеристику циклу кроку суб'єкта.

Математично GEI визначається як усереднене значення вирівняних бінарних силуетів за один або декілька циклів ходи:

$$G(x,y)=\frac{1}{N}\sum_{t-1}^{N}B_t(x,y), \tag{4.3}$$

де $B_t(x, y)$ – бінарне зображення силуету в момент часу t;

N – кількість кадрів у циклі.

Яскравість пікселів у GEI відображає ймовірність перебування частин тіла в даній точці простору: статичні частини (голова, тулуб) мають максимальну інтенсивність, тоді як кінцівки, що рухаються, створюють розмиті зони з низькою інтенсивністю. Це дозволяє системі одночасно аналізувати як антропометричні дані (зріст, пропорції), так і динаміку руху (амплітуда кроку, махи руками).Для підвищення точності в умовах зміни одягу або носіння сумок використовуються модифікації, такі як Ентропійне зображення ходи (GEnI).

Оцінка ефективності такої системи базується на правильному розпізнаванні індивідуальних характеристик та параметрів тіла людини (рис. 4.10) та знаходиться у межах від 80 до 90%. До складнощів використання таких систем слід віднести труднощі, які пов'язані із розпізнаванні СД, яким притаманна чітка хода.

Інноваційними проєктами, які знаходяться у стадії розробки, прийнято вважати розпізнавання СД за контуром на відстані до 150 м (оціночна ймовірність правильної ідентифікації не менше 90%) та трьохмірне стеження за рухами тіла СД.

4.4 Перспективні напрямки біометричних систем ідентифікації

Еволюція СКУД протягом останніх десятиліть демонструє стрімкий перехід від традиційних методів ідентифікації, заснованих на володінні об'єктом (картки, ключі) або знанні інформації (паролі, ПІН-коди), до використання біометричних характеристик суб'єкта доступу. У цьому контексті технологія розпізнавання малюнку вен долоні позиціонується як одна з найбільш прогресивних та надійних модальностей, що поєднує в собі високий рівень безпеки, гігієнічність та стабільність ідентифікатора протягом усього

життя людини [13]. На відміну від поверхневих біометричних ознак, таких як відбитки пальців або риси обличчя, венозна сітка прихована всередині тіла, що робить її практично неможливою для фальсифікації, крадіжки або випадкового пошкодження зовнішніми факторами.

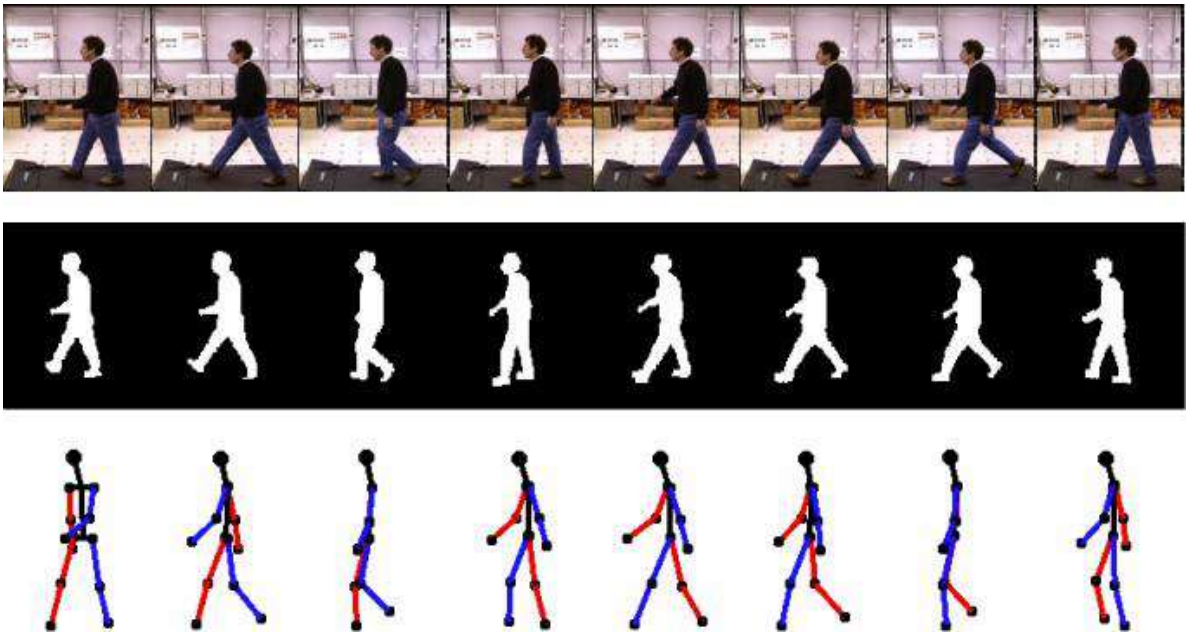


Рисунок 4.10 – Розкадровка відеозапису, яка фіксує різні фази циклу кроку

Фундаментальний принцип роботи систем розпізнавання вен долоні ґрунтується на спектроскопічних властивостях людської крові та тканин. Ключовим елементом ідентифікації є дезоксигенований гемоглобін – білок, що міститься в еритроцитах і вже віддав кисень тканинам організму, повертаючись до серця через венозну систему.

Така система використовує ближнє інфрачервоне світло, яке безпечно проникає крізь шкірний покрив. Гемоглобін у венах має унікальну здатність поглинати це випромінювання на певних довжинах хвиль, зокрема близько $7{,}6\times10^{-4}$ мм. Коли інфрачервоне світло від сканера спрямовується на долоню людини, вени, що містять дезоксигенований гемоглобін, інтенсивно поглинають промені, тоді як навколишні тканини їх розсіюють або відбивають. В результаті на чутливому сенсорі камери формується зображення, де вени виглядають як чіткий візерунок темних ліній на світлому фоні [46].

Цей малюнок є надзвичайно складним і містить величезну кількість інформації, включаючи товщину судин, їх розгалуження, кути перетину та загальну топологію судинного дерева. Вважається, що венозна структура формується під час пренатального розвитку та залишається практично незмінною протягом усього життя, що забезпечує довгострокову стабільність ідентифікаційного шаблону.

Процес ідентифікації проходить кілька важливих етапів обробки даних, що забезпечує точність і швидкість роботи системи: захоплення зображення, сегментація та виділення області інтересу, покращення якості та фільтрація, екстракція ознак, кодування та шифрування.

Одним із нових напрямків автентифікації СД є використання його індивідуальних особливостей генетичного коду. На сьогодні методи аналізу генетичного коду застосовують лише в криміналістиці, так як вони порівняно дорогі та не дозволяють отримувати результат у реальному масштабі часу. Варто зауважити, що вартість технології експрес-аналізу біологічних матеріалів та час їх аналізу знижуються достатньо швидко. Цілком можливо, що методи ідентифікації особи за генетичним кодом уже скоро стануть комерційними технологіями.

Наступним кроком в еволюції СКУД стане інтеграція алгоритмів глибокого навчання. Це дозволить покращити розпізнавання вен у людей з порушенням кровообігу, виявляти спроби спуфінгу (використання підроблених рук) завдяки аналізу мікро-пульсацій судин, реалізувати концепцію Palm-as-a-Service, де ідентифікація відбувається у хмарі через безпечне API, дозволяючи використовувати одну реєстрацію долоні для доступу до офісу, оплати в магазині та проходу в метро. Також ведуться розробки мультимодальних систем, які одночасно аналізуватимуть вени долоні та відбиток долоні. Поєднання внутрішніх та зовнішніх ознак дозволить знизити FAR до значень, які раніше вважалися недосяжними (<0,000001%).

В цілому, коли мова іде про біометричну ідентифікацію СД, необхідно пам’ятати й про етичні аспекти (дотримання конфіденційності), які тісно пов’язані із завданнями контролю доступу та безпеки.

Контрольні запитання

1. На чому засновано біометричний метод ідентифікації та в чому його основна перевага?
2. Навіщо біометричний образ піддають перетворенню перед збереженням у базі даних?
3. Назвіть мінімальну (рекомендовану) роздільну здатність сканування відбитка пальця.
4. Назвіть основні етапи процесу занесення біометричного образу в пам'ять системи.
5. Назвіть переваги ультразвукового методу зчитування відбитків над оптичним або ємнісним?
6. У чому полягає основна відмінність квазідинамічних ознак від статичних дескрипторів?

7. У чому різниця між статичною та динамічною біометрією?

8. У якій сфері діяльності найбільш поширеною є ідентифікації за ходою людини?

9. Чому голосова ідентифікація вважається зручним, але ненадійним способом доступу до об'єктів з високими вимогами до безпеки?

10. Чому системи, які базуються на використанні динамічних ознак, потребують періодичного оновлення еталонного зразка?

11. Чому у СКУД не зберігаються відбитки пальців у їх початковому (графічному) вигляді?

12. Чому, під час ідентифікації суб’єкта доступу за підписом, недостатньо аналізувати лише його форму?

13. Що впливає на коректну роботу алгоритмів порівняння?

14. Що означає термін «fist» в контексті клавіатурного почерку?

15. Що являє собою «енергетичне зображення ходи» і як воно формується?

16. Що являють собою мультимодальні системи і якої точності вони здатні досягнути?

17. Що являють собою помилки першого та другого роду в біометричних системах?

18. Як змінювались підходи до ідентифікації в СКУД?

19. Як пов'язані між собою ймовірності помилок FAR та FRR під час налаштування біометричних систем?

20. Яка різниця між «квазістатичними» та «квазідинамічними» біометричними ознаками?

21. Який математичний показник використовують для визначення ступеня відмінності між відсканованим образом ока та еталоном у базі даних?

22. Який чинник забезпечує унікальність малюнка райдужної оболонки ока?

23. Які аспекти слід враховувати під час впровадженні біометричної ідентифікації?

24. Які вимоги висуваються до еталонного відбитка пальця під час його реєстрації в системі?

25. Які дозволяють суттєво змінювати квазідинамічні ідентифікаційні ознаки людини?

26. Які основні параметри прийнято аналізувати в сучасних системах клавіатурного почерку?

27. Які характерні типи папілярних малюнків або мінуцій прийнято виділяти на відбитку пальця для формування цифрового шаблону?

РОЗДІЛ 5. Інтерфейси та мережеві протоколи СКУД

5.1 Класичний Wiegand-інтерфейс та його вразливості

Інтерфейс Wiegand, який виник як побічний продукт інновацій у матеріалознавстві 1970-х років, перетворився на стандарт для зв'язку між зчитувачами ідентифікаторів та контрольними панелями в СКУД [65]. Його повсюдне поширення зумовлене унікальним поєднанням низької вартості впровадження, здатності передавати сигнали на великі відстані та широкої сумісності між обладнанням різних виробників. Однак архітектура Wiegand, розроблена в епоху до появи масового хакерського інструментарію, позбавлена будь-яких вбудованих механізмів шифрування, автентифікації або контролю цілісності, що робить її вразливою до перехоплення, підміни даних та атак повтору.

Розуміння вразливостей інтерфейсу Wiegand неможливе без розуміння вивчення його фізичної основи, що викладено у 3 розділі даного посібника.

З появою технологій RFID на частотах 125 кГц та 13,56 МГц, фізичні карти Wiegand поступово вийшли з ужитку, але назва «Wiegand» закріпилася за електричним інтерфейсом, що з'єднує зчитувач і контролер. Більшість сучасних зчитувачів, незалежно від того, як вони отримують дані від карти (через Bluetooth, NFC або біометрію), перетворюють фінальний ідентифікатор у стандартний двійковий потік Wiegand для забезпечення сумісності з застарілими контрольними панелями. Цей факт створює парадоксальну ситуацію в безпеці – сучасні зашифровані смарт-карти часто компрометуються саме на етапі передачі даних від зчитувача до панелі через незахищений Wiegand-канал.

Інтерфейс Wiegand використовує трьохпровідну схему підключення, яка забезпечує асинхронну передачу даних за допомогою імпульсів низької напруги. Спрощена архітектура робить його легким у впровадженні, але водночас полегшує завдання зловмисникам, оскільки всі сигнали є передбачуваними та немодульованими.

Протокол Wiegand не має жорстко визначеної довжини кадру, що дозволяє передавати повідомлення будь-якої розрядності [59]. Однак для сумісності з існуючим обладнанням галузь виробила кілька стандартних форматів, кожен з яких має свої особливості кодування.

Будь-який сигнал, що проходить по провідниках Wiegand, є «голим» ідентифікатором користувача. Це означає, що зловмиснику не потрібно зламувати складні алгоритми шифрування карти (наприклад, DESFire EV3), якщо він може просто «підслухати» вже розшифровані зчитувачем дані на шляху до контролера.

Wiegand – це протокол типу «передав і забув». Зчитувач лише надсилає дані, а контролер лише слухає. У цієї схеми є кілька критичних наслідків для безпеки:

– неможливість автентифікації пристрою (контролер не знає, хто саме надіслав ідентифікатор, чи це легітимний зчитувач чи хакерський пристрій, підключений до лінії);

– відсутність контролю стану (якщо зловмисник відключить зчитувач, контролер не помітить цього до моменту, поки хтось не спробує скористатися дверима і вони не спрацюють);

– відсутність оновлень (оскільки зв'язок односторонній, неможливо дистанційно оновити прошивку зчитувача або змінити його налаштування через кабель передачі даних.

Більшість зчитувачів встановлюються на зовнішній, незахищеній стороні дверей. Для доступу до проводів зловмиснику часто достатньо відкрутити один гвинт кришки або витягнути зчитувач зі стіни. Оскільки дроти Wiegand зазвичай не мають активного моніторингу цілісності, коротке замикання або розрив лінії не завжди викликають негайну тривогу в системі. Навіть якщо кабелі прокладені в кабель-каналах, вони часто проходять через розподільчі коробки в коридорах або над підвісними стелями, які легко відкриваються.

Завдяки простоті протоколу, атаки на Wiegand стали доступними навіть для людей без глибоких знань в електроніці. Ринок пропонує готові пристрої, які дозволяють виконувати складні маніпуляції за лічені секунди.

З точки зору вектору атак та інструментаріїв зловмисників то вони можуть бути наступними.

Сніфінг та перехоплення – це пасивна атака, при якій пристрій-перехоплювач підключається паралельно до ліній DATA0 та DATA1. Пристрій фіксує всі імпульси й зберігає їх у внутрішній пам'яті. Зловмисник може встановити такий пристрій всередині зчитувача («імплант») і повернутися за ним через кілька днів, отримавши базу даних ідентифікаторів усіх співробітників компанії. Останні моделі сніферів мають вбудований Wi-Fi або Bluetooth, що дозволяє отримувати дані дистанційно, навіть не виймаючи пристрій зі стіни.

Атаки повтору – найбільш ефективний метод обходу СКУД. Зловмисник перехоплює сигнал легітимної карти (наприклад, директора або охоронця) і згодом відтворює ту саму послідовність електричних імпульсів на лінії. Оскільки для контролера цей сигнал ідентичний сигналу від рідного зчитувача, двері відчиняються без будь-яких затримок. Цей метод працює навіть проти найсучасніших біометричних систем, якщо вони підключені до контролера

через Wiegand (перехоплюється не відбиток пальця, а двійковий код, у який цей відбиток перетворюється після успішної автентифікації).

Спеціалізоване обладнання таке як ESPKey та BLEKey є звичним в колах спеціалістів з тестування на проникнення та хакерів [35].

BLEKey – пристрій розміром з монету в 25 центів. Він розташовується на провідниках зчитувача (рис. 5.1) і керується через Bluetooth. Його встановлення займає менше хвилини. Він може зберігати тисячі карт і дозволяє відкривати двері через мобільний додаток одним натисканням кнопки.

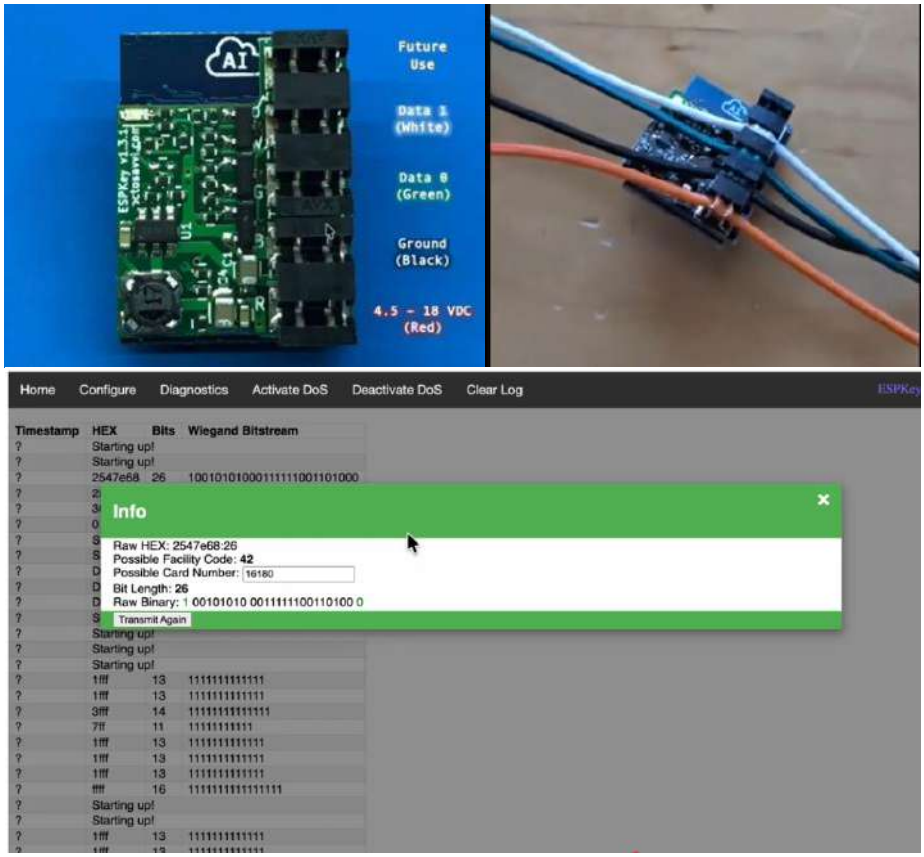


Рисунок 5.1 – Модуль BLEKey та вікно зчитування даних карти

ESPKey (ESP RFID Tool) побудований на базі чіпа ESP8266 (рис. 5.2). Цей пристрій створює Wi-Fi точку доступу з веб-інтерфейсом. Він дозволяє не тільки збирати дані, але й виконувати атаки типу «людина посередині» (MitM), підміняючи біти в реальному часі або блокуючи передачу даних (DoS) [20].

The Tick – це наступна еволюція подібних засобів, що підтримує не тільки Wiegand, а й інтерфейси Clock&Data та RS-485. Пристрій має вбудований конвертер напруги, що дозволяє йому працювати в системах від 5 В до 24 В без додаткового живлення.

Крім втручання в дроти, Wiegand-системи вразливі до дистанційного скімінгу. Якщо система використовує 125 кГц карти (наприклад, EM-Marine або

HID Prox), дані в ефірі передаються так само незашифровано, як і по лінії Wiegand. Зловмисник з потужною антеною (наприклад, «Tastic RFID Thief») може прочитати карту з відстані до одного метра, просто пройшовши поруч. Отриманий номер потім програмується на чисту карту-болванку або вводиться безпосередньо в лінію через ESPKey.

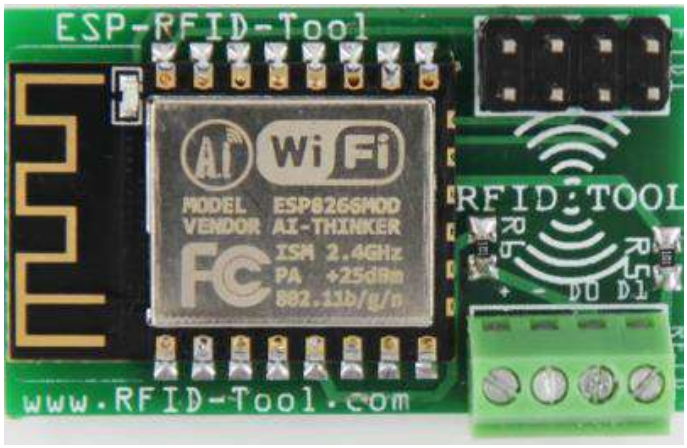


Рисунок 5.2 – Модуль ESP RFID Tool

Хоча Wiegand є вразливим, існують інженерні рішення, які дозволяють значно підвищити поріг входу для зловмисника, не вимагаючи негайної повної заміни всієї інфраструктури.

Фізичний захист та посилення конструкції є першим ешелоном захисту, що унеможливлює швидкий доступ до проводів. Їх реалізація може бути наступною:

– використання броньованих кабельних трас (всі проводи від зчитувача до контролера повинні проходити всередині жорстких сталевих кабельних трас);

– захищені кріплення (використання гвинтів з нестандартними шліцами та прихований монтаж зчитувачів);

– герметизація електроніки (встановлення зчитувачів, плати яких повністю залиті епоксидним компаундом, що робить неможливим підключення до внутрішніх контактів без руйнування пристрою);

– використання паяних з’єднань (замість знімних клемників на задній панелі зчитувача краще використовувати припаяні кабельні виводи, причому місце їх з’єднання з магістральним кабелем повинно знаходитися всередині будівлі, а не безпосередньо за зчитувачем).

Доцільно реалізовувати активний моніторинг цілісності лінії, а оскільки Wiegand не має вбудованої діагностики, її потрібно реалізувати зовнішніми засобами. Наприклад, дріт тампера повинен бути підключений до окремої зони

контролера, яка налаштована на цілодобовий моніторинг. Будь-яка спроба зняти зчитувач повинна миттєво активувати тривогу, блокувати двері та сповіщати пост охорони. Також можна встановлювати резистори на кінці лінії, що дозволить контролеру вимірювати опір ланцюга. Цей захід допомагає виявити коротке замикання (спробу обійти тампер) або розрив лінії (спробу підключити імплант).

Деякі зчитувачі мають додаткову лінію, яка активується тільки в момент піднесення карти. Це дозволяє контролеру ігнорувати будь-які імпульси на лініях DATA, якщо сигнал «Card Present» не був активований, що дещо ускладнює деякі типи автоматизованих атак повтору.

Перехід на багатофакторну ідентифікацію покращить рівень захисту. Навіть якщо зловмисник перехопить код карти, він не зможе увійти, якщо система вимагає додатковий фактор. Комбінація «Карта + PIN-код» значно підвищує рівень безпеки. Проте варто пам’ятати, що в багатьох зчитувачах натискання кнопок на клавіатурі також передається по тій самій лінії Wiegand у вигляді 4-бітних або 8-бітних повідомлень, які також можуть бути перехоплені сніфером. Біометрична автентифікація є найбільш надійним додатковим фактором, за умови, що фінальне рішення приймається на стороні контролера, а не зчитувача.

Єдиним надійним і довгостроковим рішенням для усунення вразливостей Wiegand є повна відмова від нього на користь протоколу OSDP (Open Supervised Device Protocol), розробленого асоціацією SIA.

5.2 Протокол OSDP

Еволюція СКУД протягом останнього десятиліття призвела до переходу від застарілих, вразливих інтерфейсів до інтелектуальних, захищених протоколів. Основним індикатором цих змін став протокол OSDP [44], який на сьогоднішній день є галузевим стандартом, що забезпечує не лише надійне шифрування, а й глибоку взаємодію між обладнанням різних виробників. Розроблений як відповідь на недоліки протоколу Wiegand, OSDP трансформував архітектуру безпеки на рівні дверей, перетворивши зчитувач із пасивного пристрою передачі даних на активний вузол інтелектуальної мережі.

До появи OSDP у 2008 році галузь СКУД покладалася на протокол Wiegand. З розвитком кіберзагроз стало очевидно, що передача ідентифікаційних даних у відкритому вигляді є неприпустимим ризиком, що й зумовило необхідність появи OSDP.

В основі OSDP лежить фізичний рівень RS-485, який забезпечує надійну передачу даних у складних промислових та комерційних середовищах [49]. Вибір RS-485 не був випадковим; цей інтерфейс використовує диференційну

передачу сигналів, що робить його надзвичайно стійким до електромагнітних завад та шумів, які часто виникають поблизу силових ліній або електродвигунів.

Функціонування RS-485 базується на передачі сигналу через пару провідників, де логічний стан визначається різницею потенціалів між ними. Згідно зі специфікаціями, для логічної одиниці напруга на терміналі A має бути нижчою за напругу на терміналі B, а для логічного нуля – навпаки. Такий підхід дозволяє приймачу ефективно нівелювати синфазні завади, які однаково впливають на обидва дроти витої пари.

Для забезпечення цілісності сигналу на довгих дистанціях важливим є використання термінуючих резисторів номіналом 120 Ом на обох кінцях шини. Відсутність термінації призводить до відбиття сигналу, що викликає спотворення даних та нестабільність зв'язку. Крім того, стандарт рекомендує використання витої пари, оскільки крок скрутки провідників безпосередньо впливає на здатність кабелю пригнічувати зовнішні наведення.

Однією з ключових архітектурних переваг OSDP над Wiegand є підтримка топології multi-drop (багатоточкове підключення) [64]. Це дозволяє підключати кілька периферійних пристроїв, таких як зчитувачі карток, клавіатури або біометричні сканери, до однієї пари дротів, що йдуть до контролера.

Стандартна реалізація RS-485 у контексті OSDP зазвичай підтримує до 32 пристроїв на одній лінії, хоча теоретична межа адресації в протоколі становить 127 унікальних адрес (від 0×00 до 0×7E). Така структура спрощує монтаж – замість того, щоб тягнути окремий 12-жильний кабель від кожного зчитувача до панелі («зірка»), інсталятор може прокласти одну шину через усі двері, використовуючи лише 4 жили (2 для даних та 2 для живлення). Це призводить до суттєвої економії на матеріалах та трудовитратах, особливо у великих офісних центрах або промислових об'єктах.

Протокол OSDP побудований на моделі опитування «запит-відповідь», де контролер завжди виступає ініціатором обміну. Кожне повідомлення має чіткий формат, що дозволяє пристроям на шині ідентифікувати пакети, призначені саме їм, та ігнорувати транзитний трафік.

Типовий пакет даних OSDP складається з наступних полів, розташованих у строгому порядку [42]:

1. SOM (Start of Message) – завжди має значення 0×53. Це маркер початку фрейму, який сповіщає всі пристрої на шині про початок нової транзакції.

2. ADDR (Address) – фізична адреса периферійного пристрою. Значення 0x7F використовується для широкомовних повідомлень, на які пристрої не дають відповіді.

3. LEN_LSB та LEN_MSB – два байти, що визначають загальну довжину пакету (включаючи SOM та контрольний код). Використання формату little-endian (молодший байт попереду) є стандартним для протоколу.

4. CTRL (Control Byte) – важливе поле, що містить метадані про пакет:

– біти 0-1 (SQN) – номер послідовності повідомлення (0-3), що дозволяє виявляти дублікати або пропущені пакети;

– біт 2 (CKSUM/CRC) визначає метод перевірки цілісності (0 для 8-бітного Checksum, 1 для 16-бітного CRC);

– біт 3 (SCB) – мітка наявності блоку керування безпекою (Security Control Block).

5. SCB (Security Control Block) – присутній лише в режимі Secure Channel. Містить інформацію про довжину блоку безпеки та тип криптографічної операції.

6. CMND/REPLY – однобайтний код, що вказує на тип команди (від контролера) або відповіді (від пристрою).

7. DATA – тіло повідомлення, довжина якого залежить від типу команди. Тут передаються коди карток, біометричні шаблони або команди на зміну кольору LED.

8. CRC/Checksum – завершальне поле для верифікації цілісності даних. У сучасних системах використання 16-бітного CRC є обов'язковим через вищу надійність детекції помилок порівняно зі звичайною контрольною сумою.

OSDP є асинхронним протоколом, де пристрій має повернути відповідь протягом 200 мс після отримання запиту. Якщо периферійний пристрій не може негайно виконати дію (наприклад, зчитування великого обсягу даних зі смарт-картки), він надсилає код osdp_BUSY. Це запобігає «зависанню» шини та дозволяє контролеру перейти до опитування наступного пристрою в ланцюгу. Повторний запит даних здійснюється через команду osdp_POLL, яка є основним інструментом підтримки зв'язку в системі.

Головною перевагою OSDP v2 є режим Secure Channel, який забезпечує конфіденційність, цілісність та автентифікацію повідомлень. В основі цього режиму лежить алгоритм AES з довжиною ключа 128 біт, що відповідає вимогам федеральних стандартів безпеки США для захисту критично важливої інформації.

Безпека OSDP базується на багаторівневій структурі ключів, що мінімізує ризики компрометації системи в разі фізичного доступу до одного з пристроїв:

– SCBK-D (Default Secure Channel Base Key) – заводський ключ (0×303132333435363738393A3B3C3D3E3F), визначений специфікацією SIA. Він призначений виключно для початкового узгодження при першому підключенні пристрою;

– SCBK (Secure Channel Base Key) – унікальний майстер-ключ для конкретного зчитувача або об’єкта. Він може бути згенерований випадковим чином контролером та переданий пристрою в режимі інсталяції, або введений вручну;

– сесійні ключі S-ENC та S-MAC – тимчасові ключі, що діють лише протягом однієї сесії зв’язку. S-ENC використовується безпосередньо для шифрування корисного навантаження, а S-MAC – для генерації кодів автентифікації повідомлень, що гарантує захист від модифікації даних.

Встановлення захищеного каналу – це складний чотирьохстадійний процес взаємної перевірки автентичності:

– запит виклику (osdp_CHLNG) – контролер надсилає периферійному пристрою 8-байтне випадкове число (RND.A);

– криптограма клієнта (osdp_CCRYPT) – пристрій відповідає власним випадковим числом (RND.B) та ідентифікатором пристрою, зашифрованим за допомогою SCBK. На основі цих даних обидві сторони незалежно вираховують сесійні ключі;

– криптограма сервера (osdp_SCRYPT) – контролер надсилає відповідну криптограму, доводячи пристрою, що він володіє правильним SCBK. Це забезпечує взаємну автентифікацію, запобігаючи підключенню підроблених контролерів до зчитувачів;

– початковий MAC (osdp_RMAC_I) – пристрій підтверджує успішне завершення процедури та встановлює вектор ініціалізації для подальшого ланцюжка повідомлень.

Важливою деталлю є те, що метадані пакету (адреса, довжина) залишаються у відкритому вигляді, тоді як лише поле DATA шифрується. Проте кожне повідомлення супроводжується MAC-кодом, який базується на вмісті попереднього пакету. Це створює безперервний криптографічний ланцюг, що робить атаку типу «перехоплення та повтор» неможливою, оскільки будь-яке втручання або пропуск пакету призведе до розсинхронізації MAC.

Однією з найбільш революційних особливостей OSDP є можливість двостороннього обміну інформацією, що перетворює зчитувач на керований мережевий вузол. У системах Wiegand зв’язок був суто одностороннім – від зчитувача до панелі. Контролер не міг перевірити стан зчитувача, поки той не надішле код картки.

У режимі OSDP контролер постійно (декілька разів на секунду) надсилає команду osdp_POLL кожному пристрою на шині. Якщо зчитувач не відповідає, система негайно генерує тривогу «Device Offline». Це дозволяє виявити

саботаж (наприклад, перерізання кабелю) миттєво, а не тоді, коли користувач намагається прикласти картку і не отримує реакції.

Завдяки двосторонньому каналу, адміністратори можуть змінювати логіку роботи зчитувачів без фізичного доступу до них. Контролер може надсилати команди:

– osdp_LED (керування кольором, яскравістю та режимом миготіння світлодіода) дозволяє реалізувати складні сценарії візуального зворотного зв'язку (наприклад, миготливий червоний при тривозі або синій при переході в режим очікування);

– osdp_BUZ (керування звуковим сигналом для підтвердження дій або сповіщення про помилки);

– osdp_TEXT (виведення текстових повідомлень на вбудований LCD-дисплей зчитувача, що значно підвищує зручність для користувачів).

Найбільш вагомою функцією в сучасних умовах є дистанційне оновлення прошивок (osdp_FILETRANSFER). OSDP v2.2 вдосконалив цей механізм, дозволяючи передавати великі набори даних частинами. Це дозволяє централізовано оновлювати програмне забезпечення сотень зчитувачів на об'єкті для усунення вразливостей або додавання підтримки нових типів карток, що раніше вимагало демонтажу та ручного перепрошивання кожного пристрою.

Незважаючи на те, що OSDP на порядки безпечніший за Wiegand, він не є магічним рішенням, яке автоматично захищає від усіх загроз. Дослідження безпеки виявили ряд вразливостей, пов'язаних переважно з неправильною конфігурацією.

Режим інсталяції дозволяє новому зчитувачу отримати майстер-ключ SCBK від контролера. Якщо цей режим залишається активним після завершення робіт, зловмисник може підключити свій пристрій до шини, імітувати «новий зчитувач» і запросити ключ у контролера. Після отримання SCBK він може розшифрувати весь трафік. Таким чином, даний режим необхідно вимикати на контролері відразу після завершення налаштування пристроїв.

Використання заводського ключа (SCBK-D) перетворює шифрування на формальність. Будь-який хакерський пристрій, знаючи цей публічно доступний ключ, зможе розшифрувати дані. Таким чином, потрібно використовувати унікальні ключі для кожного об'єкта. Найкращою практикою є автоматична генерація випадкових ключів контролером під час першої ініціалізації.

Деякі контролери дозволяють зчитувачам працювати в незашифрованому режимі («Basic»), якщо шифроване з'єднання не вдалося встановити. Зловмисник може навмисно створювати перешкоди для шифрованих пакетів,

змушуючи систему перейти на відкритий текст. Вирішити це питання можна налаштувавши параметр «Secure Channel Required» на рівні контролера. У такому режимі контролер повністю відмовляється приймати будь-які дані від зчитувача, якщо не встановлено захищений сеанс AES.

Оскільки світ безпеки все більше інтегрується з IT-мережами, OSDP розширює свої межі за межі RS-485. Робоча група SIA OSDP активно працює над стандартизацією передачі OSDP-пакетів через IP-мережі (TCP/UDP).

Це відкриває нові можливості, але й приносить нові виклики. Для захисту даних в IP-середовищі передбачається використання протоколу TLS v1.3 [57]. TLS v1.3 забезпечує значно вищий рівень безпеки завдяки механізму Perfect Forward Secrecy – навіть якщо зловмисник колись дізнається довгостроковий приватний ключ сервера, він все одно не зможе розшифрувати дані, перехоплені раніше. Це робить OSDP over IP ідеальним рішенням для хмарних систем контролю доступу, де зчитувачі підключаються безпосередньо до інтернету.

5.3 Ethernet, PoE та бездротові мережі у СКУД

Сучасна архітектура безпеки базується на фундаменті інформаційних технологій, де Ethernet, живлення через мережу (Power over Ethernet, PoE) та бездротові протоколи зв’язку визначають не лише ефективність експлуатації, а й загальний рівень захищеності об’єкта [6]. Перехід до IP-орієнтованих систем дозволив інтегрувати контроль доступу в загальну IT-інфраструктуру підприємства, забезпечуючи гнучкість управління, детальну аналітику та безпрецедентні можливості для масштабування.

Вибір між традиційними послідовними інтерфейсами та сучасними мережевими технологіями залишається ключовим архітектурним рішенням. Незважаючи на появу нових протоколів, RS-485 продовжує використовуватися завдяки своїй надійності та низькій вартості, проте Ethernet поступово витісняє його в проектах, де потрібна висока швидкість передачі даних та інтеграція з корпоративними мережами [63].

Ethernet як технологія локальних мереж LAN базується на використанні витої пари та забезпечує з’єднання типу «точка-точка», що фізично реалізується через топологію «зірка» з використанням мережевих комутаторів. RS-485, навпаки, є стандартом лише фізичного рівня, який використовує диференційну передачу сигналів по збалансованій парі дротів у топології «шина».

Однією з фундаментальних переваг Ethernet є використання ізолюючих трансформаторів на обох кінцях лінії зв’язку. Це забезпечує гальванічну розв’язку, що кардинально знижує вплив спільних мод перешкод та захищає обладнання від коливань потенціалів землі. У промислових середовищах, де

присутні значні електромагнітні завади, Ethernet з кодуванням 4B5B та MLT-3 демонструє високу стійкість, передаючи більше біт у меншій частотній смузі порівняно з бінарними сигналами RS-485.

Технічні обмеження довжини кабелю для Ethernet (стандартні 100 метрів) часто сприймаються як недолік порівняно з 1200 метрами для RS-485. Проте на практиці мережа Ethernet легше масштабується за допомогою оптичних ліній та медіаконвертерів, що дозволяє передавати дані на відстані понад 40 км. RS-485 вимагає ретельного узгодження імпедансу для запобігання відбиттю сигналів, що стає особливо критичним при підвищенні швидкості передачі даних.

У контексті СКУД важливою характеристикою є детермінованість зв'язку [16]. Технологія RS-485 зазвичай використовує топологію Master/Slave, де центральний контролер опитує кожен периферійний пристрій, що виключає колізії, але створює затримки при великій кількості вузлів. Ethernet у класичному розумінні не має вбудованих методів уникнення колізій, проте сучасні комутовані мережі працюють у режимі Full Duplex, що фактично усуває проблему колізій на фізичному рівні. Для завдань, що потребують гарантованого часу відгуку в мікросекундному діапазоні, Ethernet адаптується через технології TSN (Time-Sensitive Networking), що робить його придатним навіть для найбільш критичних систем контролю доступу.

Впровадження технології PoE стало одним із найбільш значущих каталізаторів розвитку IP-СКУД. Можливість передачі постійного струму разом із даними по одному кабелю UTP спрощує монтаж, зменшує витрати на кабельну продукцію та дозволяє централізувати систему безперебійного живлення.

Розвиток стандартів PoE IEEE 802.3 відображає зростаючі потреби кінцевих пристроїв у потужності [45]. Якщо перші IP-зчитувачі задовольнялися потужністю до 13 Вт, то сучасні мультибіометричні термінали та контролери на кілька дверей вимагають набагато більших енергетичних ресурсів.

Стандарт IEEE 802.3bt запровадив концепцію використання всіх чотирьох пар кабелю для передачі живлення (4PPoE), що дозволило подолати поріг у 30 Вт. Важливою особливістю 802.3bt є функція «Autoclass», яка дозволяє джерелу живлення вимірювати реальне споживання пристрою та динамічно перерозподіляти бюджет потужності між портами, що значно підвищує енергоефективність системи.

При проектуванні СКУД на базі PoE необхідно враховувати сумарне споживання всіх компонентів точки проходу – контролера, зчитувачів, датчиків стану дверей та виконавчих механізмів (замків). Бюджет потужності комутатора є кінцевим ресурсом, і його перевищення призводить до нестабільної роботи або відмови системи.

Важливо розрізняти номінальну потужність та клас PoE. Якщо пристрій підтримує Class 0, комутатор зарезервує для нього 15,4 Вт, навіть якщо реальне споживання становить 5 Вт. Це може призвести до штучного вичерпання бюджету потужності при наявності вільних ватів у блоці живлення комутатора.

Взаємодія між мережевою інфраструктурою та фізичними замикаючими пристроями є найбільш критичною точкою при проектуванні живлення. Електронні замки мають специфічні профілі енергоспоживання, які суттєво відрізняються від типових IT-пристроїв.

Електромагнітні замки працюють за принципом постійного споживання енергії для утримання дверей у зачиненому стані. Це означає, що вони створюють постійне базове навантаження на бюджет PoE. Електромеханічні замки та защіпки часто працюють у режимі Fail-Secure, де енергія потрібна лише для відмикання. Однак соленоїдні пристрої в момент активації створюють значні стрибки струму (до 1,5 А), що може спричинити просідання напруги та перезавантаження IP-контролера, якщо бюджет порту PoE не має достатнього запасу.

Для інтеграції в бюджет PoE всі значення струму повинні бути переведені у вати за наступним виразом:

$$P=U\times I. \qquad (5.1)$$

Наприклад, електрозамок на 12 В з піковим струмом 0,7 А споживає 8,4 Вт. При використанні контролера, що живить замок зі свого внутрішнього перетворювача, необхідно додавати ККД цього перетворювача та власне споживання контролера (зазвичай 3 … 7 Вт).

Усереднені показники споживання для проектування:

- контролер на одні двері зі зчитувачем: 5 … 10 Вт;
- електромагнітний замок (стандартний): 3 … 6 Вт;
- біометричний термінал з розпізнаванням обличчя: 12 … 25 Вт.

Бездротові рішення стають незамінними при реставрації історичних будівель, в офісах зі скляними перегородками або при необхідності швидкого розгортання СКУД без капітальних монтажних робіт.

Вибір бездротового протоколу визначає баланс між швидкістю передачі даних, дальністю зв’язку та автономністю роботи від батарей.

Технологія Bluetooth – основна технологія для мобільних ідентифікаторів. Bluetooth працює на коротких відстанях (до 10 … 30 метрів) і характеризується надзвичайно низьким енергоспоживанням, що дозволяє замкам працювати до року на одному комплекті батарей. Завдяки підтримці в кожному сучасному

смартфоні, Bluetooth став стандартом для «hands-free» доступу та цифрових гаманців (Apple Wallet, Google Wallet).

Для прямого підключення замків до існуючої корпоративної мережі використовується Wi-Fi. Перевагою є висока швидкість та відсутність потреби в додаткових хабах. Проте Wi-Fi є енергоємним протоколом – замки в активному режимі швидко виснажують батареї (термін служби 2 … 6 місяців), тому вони частіше використовуються в режимі періодичного «пробудження» або вимагають проводового живлення.

Протоколи Zigbee та Thread, побудовані на стандарті IEEE 802.15.4, призначені для створення самоорганізованих комірчастих мереж (mesh). Zigbee є ідеальним для великих об’єктів, де кожен замок може передавати сигнал наступному, збільшуючи дальність покриття без встановлення потужних роутерів. Новий стандарт Matter базується на Thread та забезпечує уніфіковану взаємодію пристроїв різних виробників, що є майбутнім для корпоративної автоматизації.

Для професійних СКУД розроблені пропрієтарні та відкриті екосистеми, що базуються також на стандарті 802.15.4, але мають глибшу інтеграцію з софтом безпеки.

Технологія ASSA ABLOY Aperio дозволяє об’єднати бездротові замки з онлайн-системами контролю доступу. Aperio-хаби підключаються до контролерів по шині RS-485 або через IP-мережу та підтримують до 64 замків кожен. Зв’язок між хабом та замком захищений шифруванням AES-128, а час відгуку дозволяє приймати рішення про доступ на центральному сервері в реальному часі.

Аналогічна до попередньої екосистема Salto Sallis інтегрована з багатьма світовими виробниками ПЗ (наприклад, Honeywell Pro-Watch). Sallis-вузли забезпечують зв’язок на відстані до 15 метрів від замка, передаючи події про стан дверей, злам або низький заряд батареї безпосередньо в інтерфейс моніторингу.

З переходом СКУД на рейки IT-мереж, вони успадкували всі вразливості та загрози цифрового світу. Контролер доступу на базі Linux, підключений до корпоративної мережі, може стати вектором атаки на всю організацію, якщо не дотримані правила мережевої гігієни.

Таким чином, інтеграція Ethernet, PoE та бездротових мереж у СКУД перетворила їх із простих електронних замків на високотехнологічні мережеві вузли. Використання Ethernet забезпечує необхідну швидкість та масштабованість, тоді як PoE пропонує гнучкість у проектуванні систем живлення та централізацію резервування. Проте перехід до IP-технологій вимагає суворого дотримання стандартів кібербезпеки, включаючи сегментацію

мереж через VLAN та використання захищених протоколів OSDP. Бездротові технології, такі як BLE та Zigbee, доповнюють проводову інфраструктуру, забезпечуючи мобільність користувачів та економічну вигоду при інсталяції в складних умовах. Майбутнє галузі визначатиметься хмарними сервісами та інтелектуальною аналітикою, що зробить СКУД невід'ємною частиною сучасного цифрового бізнесу.

Контрольні запитання

1. Назвіть основні недоліки протоколу Wiegand.
2. Назвіть основні переваги та недоліки використання Wi-Fi для підключення бездротових пристроїв СКУД у порівнянні з Bluetooth.
3. Опишіть структуру типового пакету даних OSDP.
4. Поясніть різницю між ключами SCBK-D, SCBK, S-ENC або S-MAC.
5. У чому полягає особливість технологій типу Aperio або Sallis під час інтегрування бездротових пристроїв СКУД у професійні онлайн-системи?
6. У чому полягає різниця між стандартами Ethernet та RS-485?
7. Чому атаку «повторення» вважають ефективною проти сучасних біометричних систем?
8. Чому багатофакторна ідентифікація не завжди є гарантованим захистом від перехоплення даних сніфером?
9. Чому інтерфейс Wiegand став галузевим стандартом в СКУД?
10. Чому топологія Master/Slave у RS-485 може спричиняти затримки за великої кількості вузлів у СКУД?
11. Яка причина розробки та впровадження протоколу OSDP?
12. Який протокол вважають єдиною надійною альтернативою Wiegand та чому?
13. Яким чином вирішується проблема обмеження довжини кабелю для Ethernet у великих проектах?
14. Яким чином протокол OSDP дозволяє захистити СКУД від атак типу «перехоплення та повтор»?
15. Яким чином реалізація «активного моніторингу цілісності лінії» допомагає виявити втручання в роботу інтерфейсу, який за замовчуванням не містить у собі засобів самодіагностування?
16. Які критичні наслідки для безпеки має протокол за схемою «передав і забув»?
17. Які методи фізичного захисту та підключення зчитувача допоможуть суттєво ускладнити доступ зловмисник до ліній передачі даних?
18. Які переваги, в промислових умовах застосування СКУД, має інтерфейс RS-485?

19. Які помилки в конфігурації OSDP можуть зробити систему вразливою для зловмисників?

20. Які ризики можуть появитись під час переходу СКУД на IP-орієнтовану архітектуру?

21. Яку роль виконують зчитувачі у системі СКУД під час переходу системи на протокол OSDP?

РОЗДІЛ 6. Виконавчі та загороджувальні керовані пристрої

Виконавчі пристрої, в основному, визначають рівень та якість виконання функції затримання та чинять істотний вплив на швидкодію системи й вартість СКУД в цілому. У зв'язку з цим, до питань вибору та застосування виконавчих пристроїв, необхідно підходити досить уважно. Усі виконавчі пристрої, за ступенем їх застосування, можна розділити на три основні класи:

– призначені для організації доступу в приміщеннях;

– призначені для організації доступу на пішохідних контрольно-пропускних пунктах (КПП);

– призначені для організації доступу на транспортних КПП.

У свою чергу, загороджувальні керовані пристрої (ЗКП) – пристрої, які забезпечують фізичне перешкоджання доступу суб'єктів та об'єктів доступу та обладнано виконавчими пристроями для управління їх станом (двері, ворота, турнікети, шлюзи, прохідні кабіни). Виконавчі пристрої (ВП) є найбільш важливими компонентами загороджувальних керованих пристроїв СКУД, оскільки саме це обладнання реалізує активну частину управління доступом в зону захисту, яка охороняється та/або приміщення за командою пристроїв керування.

Класифікація ЗКП подана на рисунку 6.1.

На практиці ЗКП прийнято класифікувати за наступними ознаками:

– за видом перекривання проєму: з частковим перекриттям (турнікети, шлагбауми); з повним перекриттям (суцільні двері, ворота); з блокуванням суб'єкта/об'єкта доступу в проємі (шлюзи, кабіни прохідні);

– за способом керування: з ручним керуванням; з напівавтоматичним керуванням; з автоматичним керуванням.

6.1 Загальні технічні вимоги, які висуваються до ЗКП

Загороджувальні керовані пристрої СКУД повинні виготовлятися відповідно до чинних вимог, стандартів та інших нормативних документів на них [124]. Стосовно цих пристроїв необхідно передбачати проведення регламентних технічних робіт із їх обслуговування, а самі вони повинні забезпечувати можливість як цілодобової, так і позмінної роботи.

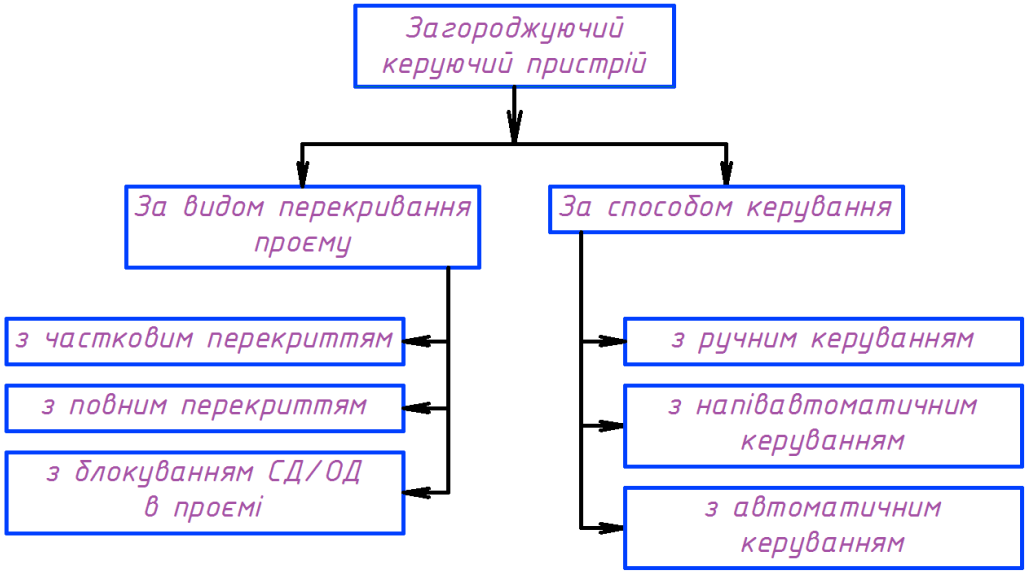


Рисунок 6.1 – Класифікація загороджувальних керованих пристроїв

Дані пристрої повинні володіти відповідним ступенем надійності, конструктивною, інформаційною й експлуатаційною сумісністю. Параметри та вимоги, які визначають сумісність засобів КУД (залежать від призначення та умов застосування конкретного типу засобу або системи) зазвичай зазначаються в нормативних документах на них.

6.1.1 Вимоги, які висуваються до функціональних характеристик ЗКП

Загороджувальні керовані пристрої повинні забезпечувати:

– повне або часткове перекриття проєму для проходу;
– ручне, напівавтоматичне або автоматичне управління;
– блокування ЗКП суб’єкта або об’єкта доступу в проємі для проходу.

ЗКП, які перебувають у режимі чергування можуть знаходитись як в нормально відкритому, так і нормально закритому стані.

ЗКП із частковим перекриттям проєму для проходу за необхідності можуть бути обладнані засобами сигналізації, які будуть спрацьовувати під час обходу загороджувального пристрою (рис. 6.2).

В нормативних документах або технічних умовах на конкретний тип ЗКП, який використовують на прохідних або в інших місцях із великими потоками СД, обов’язково встановлюються показники його пропускної здатності.

Загороджувальні керовані пристрої, які знаходяться в закритому стані повинні забезпечити фізичну перешкоду переміщенню СД, транспорту та інших об’єктів в (або з) приміщення, будівлю, зону або на територію та приведення в роботу виконавчого пристрою під час подачі на нього керуючого сигналу від пристрою управління. При цьому параметри керуючого сигналу

повинні бути вказані в стандартах або нормативних документах на ЗКП конкретного типу.

Рисунок 6.2 – Варіанти обходу загороджувального пристрою [110]

На практиці нормально закриті ЗКП прийнято обладнувати засобами звукової сигналізації, яка вмикається під час їх відкриття або за відсутності проходу протягом встановленого часу. Зустрічаються також й системи, які обладнані засобами повернення у закритий стан. ЗКП за необхідності можуть містити захист від проходу через них одночасно двох або більше осіб.

У випадку зникнення електроживлення, виникнення пожежі або інших стихійних лих в ЗКП, на конструктивному рівні, передбачають механічне аварійне відкривання. Аварійна система відкривання повинна бути захищеною від можливості використання її для несанкціонованого проникнення. Умисне пошкодження зовнішніх електричних ланцюгів та елементів блокування не повинно призводити до відкривання ЗКП.

З метою захисту нормального функціонування ЗКП необхідно передбачити заходи щодо захисту зовнішніх електричних ланцюгів від можливості подачі на них високої напруги. У такому випадку ЗКП можуть бути обладнані додатковими засоби спеціального контролю.

Вимоги, які висуваються до ЗКП, до складу яких входять засоби спеціального контролю, встановлюються в нормативних документах на пристрої конкретного типу.

6.1.2 Вимоги, які висуваються до електромагнітної сумісності ЗКП

Засоби та системи КУД залежно від стійкості до впливу електромагнітних перешкод (за стандартами серій ДСТУ EN 50130 [91] та ДСТУ EN 61000 [100]) повинні відповідати таким ступеням жорсткості:

– перший або другий ступінь – за нормальної стійкості;
– третій ступінь – за підвищеної стійкості;
– четвертий або п’ятий ступінь – за високої стійкості.

Вимоги, які висуваються до стійкості штучно створюваним електромагнітним перешкодам висуваються до тих пристроїв, які володіють

ступенем жорсткості не нижче другого, і повинні бути зазначені в технічних умовах на засоби та системи КУД конкретного типу.

Рівень допустимих радіоперешкод під час роботи засобів та систем контролю й управління доступом повинен відповідати ДСТУ EN 55014-1:2019 «Електромагнітна сумісність. Вимоги до побутових електроприладів, електричних інструментів та аналогічної апаратури. Частина 1. Емісія завад» [93] та ДСТУ EN IEC 55014-2:2022 «Електромагнітна сумісність. Вимоги до побутових електроприладів, електроінструментів та аналогічних виробів. Частина 2. Несприйнятливість до завад» [101].

6.1.3 Вимоги, які висуваються до стійкості ЗКП на несанкціоновані дії

Вимоги, які висуваються до стійкості ЗКП на несанкціоновані дії (НСД) встановлено в ДСТУ EN 60839-11-1:2014. «Системи тривожної сигналізації. Системи контролювання доступу для застосування в охоронних цілях. Частина 1. Системні вимоги» [97] та інших нормативних документах на засоби та системи КУД конкретного типу.

Вимоги щодо стійкості до НСД руйнівного типу поширюються також й на ЗКП та включають:

– стійкість до взламування – здатність конструкції протистояти руйнівному впливу без використання інструментів, а також за допомогою ручних та інших типів інструментів;

– кулестійкість – здатність конструкції протистояти наскрізному пробиванню кулями та відсутність при цьому небезпечних для людини вторинних вражаючих елементів;

– стійкість до вибуху – здатність конструкції протистояти руйнівній дії вибухових речовин.

Для ЗКП підвищеної та високої стійкості, на практиці, додатково встановлюють 5 класів показників стійкості (табл. 6.1).

Стійкість до руйнівних впливів, зазвичай, встановлюють для засобів із підвищеним та високим рівнями стійкості. Нормальна стійкість забезпечується механічною міцністю конструкції без оцінювання за показниками стійкості. Підвищену стійкість прийнято визначати за показниками стійкості до взламування одиночними ударами та/або набором інструментів. Високу стійкість визначають за показниками стійкості до взламування, кулестійкості та/або вибуху. При цьому, вимоги, які висуваються до кулестійкості застосовують лише для тих ЗКП, які здатні повністю перекрити проєм проходу.

Вимоги для засобів КУД, які висуваються до стійкості на НСД під час неруйнівного впливу, встановлюються за функціональним призначенням ЗКП та обов’язково включають у себе стійкість до взламування як ЗКП, так і виконавчих пристроїв.

Таблиця 6.1 – Класи ЗКП за показниками стійкості

Показний стійкості	Клас стійкості ЗКП				
	1	2	3	4	5
Захищеність від взламування одиночними ударами	+	+	+	+	+
Захищеність від взламування набором інструментів	–	–	–	–	–
Кулестійкість	–	–	–	±	±
Стійкість до вибуху	–	–	–	±	±

Примітка. Умовний знак «+» означає наявність вимоги та обов'язкової її перевірки. Знак «–» – відсутність вимоги. Знак «±» – можливість виконання ЗКП як стійкими, так і нестійкими до цього виду впливу

Зауважимо, що системи та засоби КУД високої стійкості підлягають обов'язковій сертифікації за вимогами захисту від несанкціонованого доступу до інформації.

6.1.4 Вимоги, які висуваються до надійності ЗКП

Основні показники надійності зазвичай наводять в нормативних документах або технічних умовах на засоби та системи КУД конкретного типу. Відповідно до ДСТУ 2860-94 «Надійність техніки. Терміни та визначення» [83] та ДСТУ 2861-94 «Надійність техніки. Аналіз надійності. Основні положення» [84] до таких показників слід віднести:

– показник безвідмовності – середнє напрацювання на відмову, год;

– показник ремонтопридатності – середній час відновлення працездатного стану, год;

– показник довговічності – середній термін служби, років.

Безвідмовність – властивість об'єкта безперервно зберігати працездатний стан протягом деякого часу або напрацювання.

Середнє напрацювання на відмову (напрацювання на відмову) – відношення сумарного напрацювання об'єкта, який відновлюється, до математичного сподівання числа його відмов протягом цього ж напрацювання.

Ремонтопридатність – властивість об'єкта, яка полягає у пристосованості до підтримання й відновлення працездатного стану шляхом технічного обслуговування та ремонту.

Середній час відновлення – математичне сподівання часу відновлення працездатного стану об'єкта після відмови.

Довговічність – властивість об'єкта зберігати працездатний стан до настання граничного стану за встановленої системи технічного обслуговування та ремонту.

Середній термін служби – математичне сподівання терміну служби.

Під час встановлення показників надійності необхідно зазначати критерії

відмови. Відмова – подія, яка полягає в порушенні працездатного стану об’єкта. Критерій відмови – ознака або сукупність ознак порушення працездатного стану об’єкта, які встановлено в нормативно-технічній або конструкторській (проєктній) документації.

Показники надійності засобів КУД встановлюють виходячи із необхідності забезпечення надійності системи в цілому. Зауважимо, що на вимогу замовника у технічних умовах на конкретні засоби й системи контролю та керування доступом можна встановлювати додатково й інші вимоги щодо їх надійності.

6.1.5 Вимоги, які висуваються до стійкості ЗКП на вплив зовнішніх чинників

Вимоги, які висуваються до стійкості ЗКП зі сторони впливу кліматичних чинників встановлюються у нормативних документах на засоби та СКУД конкретного типу відповідно до кліматичного виконання і категорії виробів за ДСТУ 8280:2015 «Вироби електротехнічні. Методи випробовування на тривкість до дії зовнішніх кліматичних чинників» [89].

Захисні кожухи засобів КУД у разі необхідності захисту від зовнішніх впливів повинні відповідати ступеню захисту за ДСТУ EN 60529:2018 «Ступені захисту, забезпечувані кожухами (Код IP)» [96].

Вимоги, які висуваються до стійкості в частині впливу механічних чинників необхідно встановлювати із нормативних документах на такі засоби та системи КУД із акцентуванням уваги на їх тип та необхідну групу умов експлуатації за ДСТУ 8280:2015 «Вироби електротехнічні. Методи випробовування на тривкість до дії зовнішніх кліматичних чинників» [89] та ступеня жорсткості виробів за ДСТУ EN 60068-2-57:2022 «Випробування на вплив навколишнього середовища. Частина 2-57. Випробування. Випробування Ff. Вібрація. Історія та метод синусоїдації» [95].

6.1.6 Вимоги, які висуваються до електричного живлення ЗКП

Так як і у вимогах, які висуваються до основних компонентів СКУД для загороджувальних керованих пристроях основою для електричного живлення засобів та систем КУД є мережа змінного струму з номінальною напругою 220 В, з частотою 50 Гц. При цьому ЗКП мають зберігати свою працездатні за допустимих відхилень напруги мережі електричного живлення від -15 до +10% від її номінального значення та частоти 50±1 Гц.

Електроживлення окремих засобів та систем КУД допускається здійснювати й від джерел з іншими параметрами вихідних напруг. При цьому, у разі зникнення напруги основного джерела живлення, в них необхідно передбачити резервне електроживлення. В якості резервного джерела живлення допускається використовувати резервну мережу змінного струму або джерело

живлення постійного струму (номінальну напругу резервного джерела живлення постійного струму обирають із ряду 12 В, 24 В). Перехід на резервне живлення має відбуватися автоматично без порушення встановлених режимів роботи та функціонального стану засобів й системи КУД.

У випадку зникнення, в мережі живлення, напруги резервне джерело живлення повинне забезпечити виконання основних функцій системи на час не менше 0,5 год для систем першого та другого класу та не менше 1 год для систем третього класу. За умови використання таких ЗКП, які вимагають для свого керування значних потужностей приводних механізмів (приводи воріт, шлюзи тощо) рекомендовано не застосовувати резервування електроживлення за допомогою акумуляторних батарей, але тоді їх необхідно обладнати аварійними механічними засобами відкривання.

Під час використання, у якості джерела резервного живлення, акумуляторних батарей слід передбачити відповідний пристрій для їх автоматичного зарядження.

6.1.7 Вимоги, які висуваються до безпеки ЗКП

Засоби та системи контролю й управління доступом повинні відповідати вимогам безпеки за ДСТУ 7237:2011 «Система стандартів безпеки праці. Електробезпека. Загальні вимоги та номенклатура видів захисту» [88], ДСТУ EN 60065:2019 «Аудіо-, відео- та аналогічна електронна апаратура. Вимоги щодо безпеки» [94] та ДСТУ 3135.0-95 «Безпека побутових та аналогічних електричних приладів. Загальні вимоги» [85].

Матеріали та комплектуючі, які використовуються під час виготовлення засобів і систем КУД, повинні мати гігієнічний паспорт або сертифікат.

Монтаж та експлуатація засобів і систем контролю й управління доступом повинні відповідати чинним вимогам безпеки: законодавчими та нормативно-правовими актами України про охорону праці; правилами охорони праці для відповідних видів робіт, галузей та типів устаткування та національними стандартами, які встановлюють вимоги безпеки до конкретного виробничого устаткування чи робочих процесів.

Засоби та системи КУД повинні відповідати чинним вимогам пожежної безпеки за ДСТУ 8828:2019 «Пожежна безпека. Загальні положення» [90].

Електричний опір ізоляції засобів та систем КУД між ланцюгами мережевого живлення та корпусом, а також між ланцюгами мережевого живлення та вхідними/вихідними ланцюгами повинен бути не менше значень, які наведено у таблиці 6.2

Електрична міцність ізоляції засобів і систем контролю й керування доступом між колами мережевого живлення та корпусом, а також між колами

мережевого живлення та вхідними/вихідними колами повинна відповідати вимогам чинних нормативних документів.

Таблиця 6.2 – Необхідні значення опору ізоляції

Критичні умови експлуатації	Опір ізоляції, не менше МОм
Нормальні	20,0
За найбільшого значення робочої температури	5,0
За найбільшого значення відносної вологості	1,0

Опір ізоляції та електрична міцність засобів і систем КУД, які призначені для побутового та аналогічного загального застосування, повинні відповідати вимогам ДСТУ EN 60065:2019 «Аудіо-, відео- та аналогічна електронна апаратура. Вимоги щодо безпеки» та ДСТУ 3135.0-95 «Безпека побутових та аналогічних електричних приладів. Загальні вимоги».

Для засобів контролю та керування доступом, які працюють за напруги живлення не вище +12 В змінного струму та +36 В постійного струму, нормативним документом рекомендовано не наводити значення електричної міцності ізоляції та її опору. В інших випадках значення опору ізоляції та електрична міцність ізоляції обов’язково зазначаються в технічних умовах на ці засоби та системи КУД.

Рівні випромінювання засобів контролю та керування доступом повинні відповідати вимогам безпеки, які встановлено Державними санітарними нормами та правилами при роботі з джерелами електромагнітних полів.

Засоби і системи контролю й керування доступом, призначені для експлуатації в зонах із вибухонебезпечним середовищем та повинні відповідати вимогам ДСТУ EN IEC 60079-0:2019 «Вибухонебезпечні середовища. Частина 0. Устаткування. Загальні вимоги» [102] або іншим нормативним документам, які регламентують вимоги до виробів, які експлуатуються у вибухонебезпечних середовищах.

6.1.8 Вимоги, які висуваються до конструкції ЗКП

Габаритні розміри засобів контролю й управління доступом, їх окремих функціональних та конструктивних пристроїв і блоків повинні забезпечувати легке транспортування ЗКП через типові проєми в будівлях, а складання, встановлення та монтаж – на місці їх експлуатації.

Конструкція засобів контролю й управління доступом має формуватися за модульним та блочно-агрегатним принципом і забезпечувати:

– взаємозамінність змінних однотипних складових частин;

– зручність технічного обслуговування, експлуатації та ремонтопридатність;

– унеможливлення несанкціонованого доступу до елементів керування параметрами;

– доступ до усіх елементів, вузлів і блоків, що потребують регулювання або заміни під час експлуатації.

Конструкційні та електроізоляційні матеріали, покриття та комплектувальні вироби повинні забезпечувати:

– механічну міцність;

– необхідну надійність;

– стійкість до несанкціонованих дій за категоріями та класами стійкості;

– безпечну роботу в заданих умовах експлуатації.

6.1.9 Вимоги, які висуваються до маркування ЗКП

Маркування засобів та систем контролю та управління доступом необхідно здійснювати за ДСТУ EN 50131-1:2014 «Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 1. Загальні вимоги» [9] та містити:

– товарний знак та (або) інші реквізити підприємства-виробника;

– умовне позначення;

– серійний номер;

– дату виготовлення;

– знак сертифікату відповідності (за його наявності).

В супровідній документації на ЗКП має бути вказано: номер сертифіката або реквізити висновку (за їх наявності); фірмовий знак та (або) інші реквізити організації, яка здійснювала сертифікаційні чи експертні випробування.

6.2 Виконавчі пристрої для контролю суб'єкта доступу у приміщенні

До виконавчих пристроїв, які здійснюють контроль СД до приміщення відносять засоби, які забезпечують кероване відкриття/закриття дверей. Такими пристроями прийнято вважати електричні замки різних типів та доводчики, у тому числі й різні електричні або механічні приводи.

Доводчик дверей (рис. 6.3) прийнято вважати тим необхідним елементом, який автоматично здійснює їх закривання після кожного проходу. Для того щоб доводчик надійно виконував свою основну функцію (закривав двері та оберігав замок від механічних ударів), під час його вибору, необхідно враховувати наступні параметри: маса і тип дверей, частота спрацьовувань, необхідна швидкість закривання.

З метою блокування дверей, за відсутності проходів через них, та можливості автоматичного їх відмикання, у випадку наявності проходу через

них, доцільно застосовувати електричні керовані замки (рис. 6.4) і защіпки (рис. 6.5), які на практиці поділяють на електромеханічні і електромагнітні.

а) б)

Рисунок 6.3 – Монтаж доводчика дверей [110]
а) – на дверях; б) – на дверній коробці

а) б)

Рисунок 6.4 – Електричні керовані замки [110]
а) – електромеханічний; б) – електромагнітний

Рисунок 6.5 – Електрозащіпки [110]

Основна відмінність цих засобів полягає у тому, що в електромеханічних замках, в основному, застосовують ті ж принципи, що й в звичайному механічному замку, тільки управління ригелем може здійснюватися як механічно (використовуючи ключ), так і з використанням електрики.

В електромагнітному замку утримання дверей здійснюється за рахунок створюваного магнітного поля між сталевою пластиною (якорем) та електричним магнітом (замком).

Важливим, для оцінки правильності застосування того чи іншого замкового пристрою (ЗП) є те, що під час відключення живлення електромеханічні замки, як правило, залишаються в закритому стані, у той час як електромагнітні – навпаки, відкриті. Враховуючи цю особливість, електромагнітні замки найчастіше монтують на дверях, які виконують функції аварійних виходів (для екстреної евакуації людей).

Під час вибору ЗП необхідно враховувати й особливості подачі сигналу управління та/або живлення. Так, для управління електромеханічним замком, як правило, кабель прокладають в полотні дверей або на їх внутрішній поверхні. Для цього випадку характерним є використання спеціальні кабелепроводів або контактних груп провідників для подачі живлення від коробки дверей до замка. Зауважимо, що деякі виробники електромеханічних замків, для подачі живлення використовують запірну планку. Підведення живлення та сигнальних ланцюгів до електромагнітних замків та електромеханічних защіпок здійснюється лише шляхом прокладання кабелю у дверній коробці та не вимагає втручання в полотно дверей.

Окремо варто згадати про автоматичні розсувні двері, які монтуються у спеціально підготовленому дверному проємі. В таких ЗП уся механічна частина приводу, зазвичай, розміщується у верхній частині конструкції дверей. Автоматичні розсувні двері є, по суті, достатньо складним пристроєм, який характеризується встановленою швидкістю відкриття/закриття, ресурсними показниками, типом полотна, формою, шириною дверного проєму, наявністю додаткових сервісних функцій.

Під час вибору замка необхідно враховувати наступні його особливості: матеріал, з якого виготовлено замок; стійкість замка до взламування; кліматичні умови експлуатації; параметри керуючого сигналу та необхідного джерела живлення; наявність органів аварійного розблокування; сумісність за рівнем напруги живлення та керуючих сигналів з контролерами СКУД тощо. Зауважимо, що найбільш важливими параметрами, які характеризують будь-які ЗП (в основному електромеханічний) є його функціональні та технічні (ресурсні) показники.

На сьогодні деякі виробники освоїли випуск замків із більш розвиненими сервісними функціями, що дозволяє відстежувати стан ригеля ВП.

6.3 Виконавчі пристрої для контролю суб'єкта доступу на КПП

Під час вибору виконавчих пристроїв для контролю СД на КПП необхідно чітко усвідомити те коло завдань, які замовник хоче вирішити за рахунок застосування цього виду обладнання.

Розглянемо основні завдання, які необхідно вирішити замовнику. У тому

випадку, коли необхідно розділити потік СД та мати інформацію про час і напрямок проходу тієї чи іншої особи, іншими словами вирішити завдання контролю робочого часу (табельний обліку), найбільш ефективним є використання напівзростових турнікетів.

Напівзростові турнікети (рис. 6.6) бувають як нормальнозакритими, так і нормальновідкритими. Різниця між ними полягає у тому, що перший тип турнікетів завжди заблокований та знаходиться в режимі очікування. У разі отримання дозволу на прохід його пропускний пристрій (ПП) розблоковує загороджувальний пристрій, а після проходу через нього ПП знову блокує турнікет. В свою чергу, в залежності від типу загороджуючих пристроїв даний вид турнікетів можна розділити на триподи та роторні.

а) б)

Рисунок 6.6 – Напівзростовий турнікет [110]
а) – нормальнозакритий; б) – нормальновідкритий

У турнікетах-триподах (рис. 6.7) функцію загороджувального пристрою виконують три штанги, які розташовано на спеціальній головці під кутом 120 градусів один по відношенню до одного, при цьому одна із штанг, яка знаходиться в режимі очікування, розташовується в горизонтальному положенні, створюючи, тим самим, бар’єр, який заважає вільному проходу СД. З метою виключення пролазування під штангою турнікета або перелазування над нею деякі виробники встановлюють додатковий засіб виявлення, який контролює зону проходу під або над нею.

Роторний турнікет (рис. 6.8) – це турнікет із вертикально розташованою віссю, на якій закріплено три або чотири лопаті, які утворюють перегородки для запобігання несанкціонованому проходу.

Роторні турнікети, у порівнянні із триподами, виключають можливість несанкціонованого їх подолання шляхом пролазування під горизонтально розташованою лопаттю. Для цього у них застосовується або суцільне заповнення перекриваючої області (ударостійке скло, пластик тощо) або горизонтально монтується декілька штанг.

Рисунок 6.7 – Турнікет-трипод електромеханічний [110]

а) б)

Рисунок 6.8 – Роторний турнікет [110]
а) – з трьома лопатями; б) – з чотирма лопатями

Зазвичай нормальновідкриті турнікети, які використовуються в метро (рис. 6.9), дещо відрізняються своїм конструктивним виконанням від загальноприйнятого. Такий вид турнікетів залишає зону проходу завжди відкритою. Під час несанкціонованого проходу із стійок турнікета висуваються спеціальні загороджувальні пристрої.

Нормальновідкриті турнікети мають, як правило, більш високу пропускну здатність та надійність, а також володіють кращими ресурсними показниками, у порівнянні із нормальнозакритими турнікетами. Іншою перевагою нормально-відкритого турнікета є його постійна готовність до евакуації людей. У турнікетах-триподах для реалізації аварійного проходу використовують спеціальний механізм «антипаніка», який забезпечує складання загороджувальної стійки під час прикладання навантаження у певному напрямку.

З огляду на той факт, що турнікети не є серйозною перешкодою для

зловмисника, виробники пропонують більш досконалі пристрої для забезпечення посилених вимог із організації пропускного режиму на КПП. Тут мова іде про застосування повнозростових турнікети та шлюзових пропускних пристроїв.

Рисунок 6.9 – Нормальновідкритий турнікет, який використовується в метро

Повнозростові турнікети (рис. 6.10) являють собою виконавчий пристрій на повний зріст людини, який містить трьох- або чотирьохлопатеву вертушку розташовану на його вертикальній осі для запобігання несанкціонованому проходу.

Рисунок 6.10 – Повнозростовий турнікет [110]

У вихідному положенні двері заблоковано спеціальним електромеханічним ригелем. Після надання особистого ідентифікатора та отримання дозволу на прохід блокування із ригеля знімається, а СД проходить

далі, штовхаючи двері від себе. Після проходу двері знову блокуються системою. Слід пам'ятати, що подолання цього типу турнікетів є більш проблематичним, у порівнянні із напівзростовими, однак досвідчений зловмисник достатньо вільно може подолати і його.

В ідеальному випадку пропускні пристрої СКУД повинні забезпечувати реалізацію принципу шлюзування, тобто здійснювати почергове відкривання дверей тамбура із реалізацією обов'язкової фази тимчасового блокування в зоні контролю будь-якого СД. У даному випадку забезпечується максимальний рівень вимог, які висуваються до управління доступом.

Принцип шлюзування із застосуванням ваговимірювального пристрою дозволяє практично повністю виключити прохід по одному пропуску двох та більше осіб й забезпечити надійне затримання несанкціонованих осіб.

Повнозростові пропускні пристрої шлюзового типу зазвичай виконують у вигляді пропускних кабін (рис. 6.11, а та б), які оснащені двома дверима: одні – на територію без охорони, другі – на територію, яка охороняється. Між замкненими дверима і стінками такого пристрою формується зона контролю, у якій знаходиться СД під час його ідентифікації. У випадку виявлення причин, які вимагають затримання, СД залишається заблокованим в контрольованій зоні.

Повнозростові трьохлопатеві турнікети блокуючого типу (рис. 6.11, в) забезпечують створення зони контролю та реалізують принцип шлюзування СД під час кожного циклу повороту ротора на 120 градусів. Однак ці пристрої є менш зручні в користуванні та мають гірші характеристики у порівнянні із пропускними кабінами.

Зауважимо, що на ринку пропускних пристрої шлюзового типу широко представлені й інтегровані системи, які забезпечують додатково до виконання основної функції – управління доступом – реалізацію завдань із виявлення зброї, вибухових речовин та радіоактивних матеріалів.

Під час вибору типу пропускного пристрою необхідно звернути увагу на:

– основну функцію доступу (від її правильної оцінки багато в чому залежить вартість обладнання);

– пропускну здатність (від неї залежить кількість пристроїв, які необхідно придбати);

– коефіцієнт використання площі залу КПП;

– габаритні розміри проходу, масу пристрою, ймовірність проносу предметів із певними габаритними розмірами.

Шлюзовий тамбур – це система, яка складається із двох дверей та керується електронікою, що дозволяє відкривати одну із дверей тільки в тому випадку, коли друга закрита.

а)

б)

в)

Рисунок 6.11 – Повнозростові пропускні пристрої шлюзового типу [110]
а) та б) – пропускні кабіни (тамбур-шлюзи); в) – трьохлопатевий турнікет

До характерних особливостей шлюзових тамбурів слід віднести:

– різна ширина проходу;

– система зважування, яка дозволяє виявити предмет, залишений в тамбурі та обмежити кількість людей, які проходять через кабіну;

– система захисту від нещасних випадків;

– можливість роботи кабіни як в ручному, так і в автоматичному режимі;

– двосторонній зв’язок (СД-охорона);

– цифровий металодетектор;

– детектор вибухових речовин;
– синтезатор мовних повідомлень;
– виносний пульт ручного управління шлюзовою кабіною;
– логічний блок керування дверима;
– режим аварійного виходу;
– гарантоване живлення (вбудований акумулятор великої ємності дозволяє не порушувати роботу системи навіть у разі тривалого відключення електричного живлення).

Контрольні запитання

1. На які групи поділяють електричні керовані замки?
2. На які класи, за ступенем застосування, зазвичай поділяють виконавчі пристрої?
3. На які характеристики звертають увагу під час вибору типу пропускного пристрою?
4. У чому полягає «принцип шлюзування» та які його переваги в СКУД?
5. У чому полягає різниця в управлінні ригелем між звичайним механічним та електромеханічним замком?
6. У чому полягає різниця у роботі між нормальнозакритими та нормальновідкритими турнікетами?
7. У яких станах можуть перебувати ЗКП, які знаходяться в режимі чергування?
8. Чому повнозростові турнікети вважаються надійнішими за напівзростові?
9. Що повинні включати у себе вимоги щодо стійкості ЗКП до несанкціонованих дій руйнівного типу?
10. Що являє собою механізм «антипаніка» у турнікетах-триподах та у яких ситуаціях його застосовують?
11. Як класифікують загороджувальні керовані пристрої?
12. Який чинник необхідно врахувати замовнику перш ніж обирати конкретний тип виконавчого пристрою для КПП?
13. Яким чином здійснюється утримання дверей в електромагнітних замках?
14. Які види напівзростових турнікетів прийнято розрізняти на практиці?
15. Які додаткові функції безпеки інтегровано в сучасних шлюзових кабінах?
16. Які критерії, з точки зору забезпечення надійної експлуатації, прийнято враховувати під час вибору замкового пристрою?

17. Які основні функціональні можливості повинні забезпечувати ЗКП?

18. Які показники прийнято відносити до основних характеристик надійності ЗКП?

19. Які пристрої прийнято відносити до виконавчих засобів, які забезпечують кероване відкриття/закриття дверей?

20. Яку основну функцію виконує дверний доводчик та чому він вважається необхідним елементом СКУД?

РОЗДІЛ 7. Системна архітектура та інтегрування

7.1 Централізовані, розподілені та хмарні архітектури

Сучасний підхід до фізичної безпеки розглядає СКУД не просто як інструмент для обмеження несанкціонованого проникнення, але як комплексну платформу для оптимізації бізнес-процесів, управління ресурсами компанії, обліку робочого часу та інтеграції з екосистемами розумних будівель. Зростаюча складність сучасних комерційних об’єктів вимагає від архітектури фізичної безпеки високої відмовостійкості, еластичного масштабування та здатності протистояти як фізичним, так і кібернетичним загрозам.

Фундаментальний вибір архітектури системи – централізованої, розподіленої або хмарної – визначає не лише технічні характеристики розгортання, але й стратегічні бізнес-показники, такі як сукупна вартість володіння, швидкість впровадження інновацій та здатність до адаптації в умовах мінливого регуляторного середовища [133]. Історично індустрія спиралася на централізовані моделі, які функціонували за принципом суворої ієрархії, де єдиний сервер приймав усі рішення щодо доступу. Однак, з розвитком мікросервісної архітектури, технологій контейнеризації та хмарних обчислень, розробники отримали можливість створювати розподілені системи, які працюють як колаборативні мережі незалежних вузлів [78].

Незалежно від обраної макроархітектури, будь-яка система контролю доступу функціонує завдяки синергійній взаємодії п’яти ключових компонентів, які забезпечують безперервний цикл ідентифікації, автентифікації та авторизації [36]. Розуміння ролі кожного компонента є важливим для усвідомлення того, як дані переміщуються в межах мережі та де саме відбувається обробка логіки безпеки.

Першим елементом є ідентифікатор або облікові дані, які слугують носієм унікального коду користувача. Технології ідентифікації еволюціонували від простих карток зі штрих-кодом та кодових клавіатур до безконтактних радіочастотних карток формату Proximity, які містять чіп та малопотужний передавач. Сучасний етап розвитку характеризується переходом до віртуальних

мобільних ідентифікаторів, що використовують протоколи NFC, BLE та динамічні QR-коди, що значно спрощує процес онбордингу працівників та управління гостьовим доступом.

Другим компонентом є периферійні пристрої на межі мережі – зчитувачі. Їхня єдина функція полягає у генеруванні електромагнітного поля для живлення пасивних карток, захопленні ідентифікаційного коду та передачі його на контролер за допомогою стандартизованих комунікаційних протоколів.

Третім і найважливішим апаратним елементом є контролер доступу. Це апаратна панель, яка виступає мозком локальної точки проходу. Контролер отримує необроблені дані від зчитувача, проводить їх валідацію та зіставляє з правилами доступу. Контролери керують четвертим компонентом – виконавчими пристроями (електромеханічними замками, автоматичними воротами, шлагбаумами або турнікетами), надсилаючи електричний імпульс на замикання або розмикання реле.

П’ятим компонентом є програмне забезпечення для управління, яке формує політики безпеки, зберігає історію подій та забезпечує інтерфейс адміністратора. Процес взаємодії цих компонентів відображається у стандартизованому логічному потоці.

У цьому процесі ключова архітектурна відмінність між різними моделями СКУД полягає в тому, де саме фізично розміщена база даних для автентифікації та авторизації, і який вузол бере на себе обчислювальне навантаження під час прийняття рішення.

Централізована архітектура базується на обчислювальній моделі, в якій єдиний центральний сервер або авторитарний хост бере на себе управління всіма процесами обробки даних, зберігання інформації та безпосереднього прийняття рішень для всіх підключених периферійних клієнтів (рис. 7.1). У такій реалізації контролери, встановлені біля точок проходу, діють як пасивні ретранслятори сигналів. Отримавши код ідентифікатора від зчитувача, такий контролер не проводить жодного аналізу, а відразу пакетує дані та відправляє їх через локальну мережу або послідовну шину до центрального сервера. Сервер зіставляє отриманий код з глобальною базою даних, перевіряє права доступу і відсилає зворотну команду контролеру на активацію реле замка.

Головною перевагою такої архітектури є її виняткова простота в реалізації та управлінні. Оскільки всі політики безпеки, розклади доступу та конфігурації зберігаються в одному місці, адміністратори мають єдину точку контролю, що нівелює будь-які проблеми з розсинхронізацією даних. Консистентність даних у централізованій системі є природною, оскільки не існує проблеми паралельного оновлення записів на різних пристроях, що є типовим головним болем для розподілених середовищ. Крім того, централізація

інфраструктури дозволяє впроваджувати надзвичайно жорсткі заходи захисту периметра та спрощує проведення аудитів на відповідність нормативним вимогам, адже вся чутлива інформація локалізована в одному фізично та логічно захищеному серверному приміщенні. З фінансової точки зору, для невеликих об’єктів цей підхід може бути дуже рентабельним, оскільки периферійне обладнання (контролери) не потребує дорогих мікропроцесорів та великих модулів пам’яті.

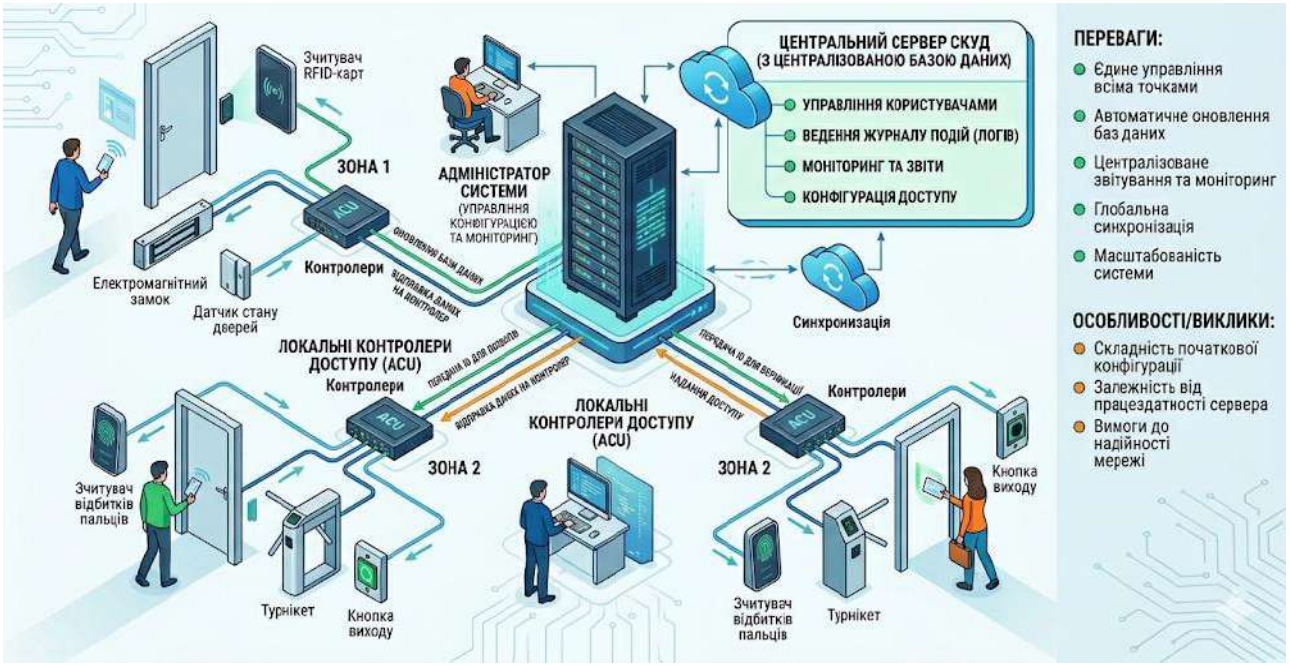


Рисунок 7.1 – Топологія централізованої архітектури СКУД

Незважаючи на простоту, централізована модель страждає від вразливостей, які роблять її вкрай неефективною для середніх та великих підприємств. Фундаментальним недоліком є наявність єдиної точки відмови. Якщо центральний сервер «падає» через апаратний збій, або якщо виникає пошкодження мережевого комутатора, що з’єднує серверну з рештою будівлі, вся система контролю доступу повністю паралізується. У такій ситуації контролери не здатні самостійно приймати рішення, і об’єкт залишається або заблокованим, що створює ризики для безпеки персоналу в екстрених ситуаціях, або відкритим настіж, що повністю руйнує безпековий периметр підприємства.

Ще одним суттєвим обмеженням є проблема масштабованості та продуктивності. Централізована архітектура масштабується переважно вертикально – шляхом нарощування обчислювальної потужності самого сервера. При збільшенні кількості зчитувачів та користувачів обсяг транзакцій стрімко зростає. Під час пікових навантажень (наприклад, на прохідній

великого заводу о 8:00 ранку) тисячі запитів одночасно надходять до сервера. Це призводить до виникнення мережевих затримок та деградації продуктивності системи. Користувачі змушені стояти біля турнікетів у очікуванні, поки сервер обробить їхні запити через перевантажений канал зв'язку.

Для подолання вразливостей централізованих систем інженерна думка розробила модель «розподіленого інтелекту», в якій повноваження щодо прийняття рішень децентралізуються і переносяться на межу мережі (Edge). У цій реалізації використовуються інтелектуальні контролери, оснащені власними мікропроцесорами та незалежною енергонезалежною пам'яттю (рис. 7.2).

Рисунок 7.2 – Топологія розподіленого інтелекту з резервуванням

Розподілена архітектура передбачає, що сервер управління виступає скоріше координатором, а не диктатором. Його основна роль зводиться до формування політик, зберігання глобальної історії подій та реплікації бази даних користувачів на локальні контролери. Під час нормальної роботи контролер отримує ідентифікаційні дані від зчитувача і самостійно здійснює пошук у своїй локальній базі даних. Знайшовши збіг та перевіривши розклад доступу, мікропроцесор контролера приймає рішення та відкриває замок, паралельно відправляючи асинхронне повідомлення про подію на центральний сервер для ведення звітності.

Головною перевагою розподіленого підходу є унікальна відмовостійкість. Система проектується з розрахунком на те, що комунікація з сервером може перерватися в будь-який момент. У разі втрати зв'язку контролери продовжують функціонувати в автономному режимі, повністю зберігаючи всі

основні функції управління. Вони використовують закешовані ідентифікаційні ознаки для дозволу чи заборони проходу, спираючись на останні отримані розклади. При цьому всі транзакції (події проходу, тривоги, спроби доступу незареєстрованих осіб) записуються у внутрішню пам’ять контролера і буферизуються до моменту відновлення мережевого підключення, після чого відбувається автоматична пакетна синхронізація журналів з центральною базою.

Іншою перевагою є можливість прямої комунікації між самими контролерами без участі центрального сервера – так званий Peer-to-Peer (P2P) зв’язок. Це дозволяє реалізувати складні алгоритми глобального контролю, такі як Global Anti-passback (захист від повторного проходу). Якщо співробітник зайшов через двері, підключені до «Контролера А», цей контролер миттєво сповіщає «Контролер Б» (який керує виходом на іншому кінці будівлі), що даний співробітник зараз перебуває всередині периметра. Такий рівень взаємодії забезпечує горизонтальне масштабування системи, де додавання нових вузлів не перевантажує центральний процесор і підвищує загальну продуктивність.

Слабким місцем розподілених систем є висока складність управління та забезпечення консистентності даних. На відміну від централізованої моделі, тут дані реплікуються на десятки або сотні вузлів. Процес підтримки ідентичності баз даних на всіх контролерах є серйозним інженерним викликом, адже транзакції оновлення можуть ініціюватися одночасно.

У теорії розподілених баз даних застосовується концепція «узгодженості в кінцевому рахунку». Це означає, що після внесення змін (наприклад, звільнення співробітника та відкликання його прав адміністратором), може пройти певний короткий час (затримка поширення), перш ніж ця інформація оновиться на всіх без винятку периферійних контролерах. Для запобігання конфліктам при паралельному записі (наприклад, коли два адміністратори намагаються змінити права доступу одного користувача одночасно), системи часто використовують протоколи узгодження, такі як двофазне блокування (2PL – Two-Phase Locking). Алгоритм 2PL гарантує, що транзакція отримує блокування на дані під час «фази зростання» і не відпускає їх до завершення всіх операцій, після чого переходить у «фазу звуження», звільняючи ресурси. Це запобігає ситуаціям, коли локальні бази даних опиняються у пошкодженому стані через перехресні оновлення. Крім того, розподілені СКУД повинні вирішувати проблеми гетерогенності, коли в мережі знаходяться різні покоління обладнання з різними обсягами пам’яті, що вимагає розробки інтелектуальних протоколів диференційної синхронізації.

Останнє десятиліття ознаменувалося масовим переходом корпоративного програмного забезпечення в хмарні середовища. Індустрія фізичної безпеки не стала винятком, породивши концепцію «Контроль доступу як послуга» (Access Control as a Service, ACaaS). Хмарна архітектура (рис. 7.3) усуває потребу в розгортанні локальних серверів, переносячи весь обчислювальний центр управління у віртуалізовані дата-центри постачальників послуг (таких як AWS, Microsoft Azure або Google Cloud).

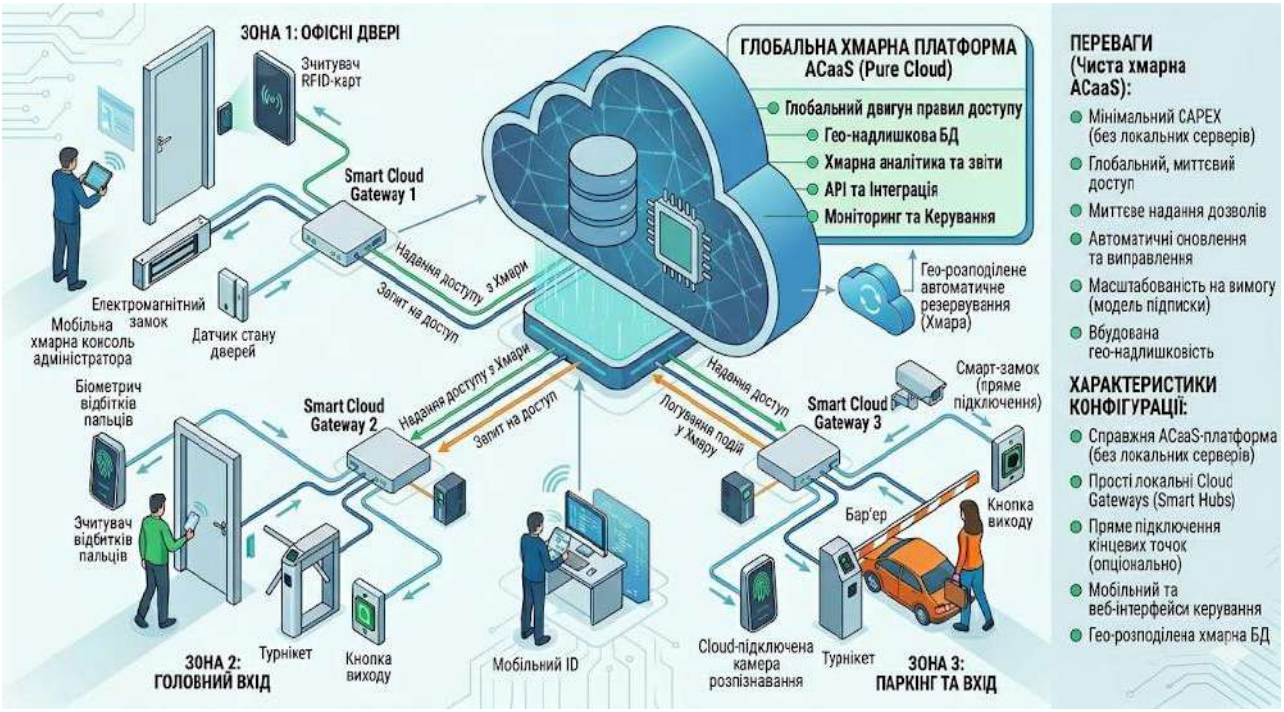


Рисунок 7.3 – Топологія хмарної архітектури ACaaS

Архітектура ACaaS кардинально змінює ідею розгортання, розділяючи систему на дві незалежні площини: управління і даних.

Площина управління розміщується виключно в публічній хмарі. Тут функціонує мікросервісна архітектура (контейнери Docker/Kubernetes), що відповідає за графічний інтерфейс адміністратора, збір та аналіз логів у реальному часі, обробку політик доступу, генерацію звітів та виконання інтеграцій через API (наприклад, з платформами Single Sign-On, такими як Okta або Azure AD, та HR-системами). Використання мікросервісів дозволяє незалежно масштабувати окремі модулі: якщо модуль аналітики перевантажений запитами, хмарний провайдер динамічно виділяє йому додаткові ресурси, не впливаючи на швидкість обробки ідентифікацій.

Площина даних розміщується на об’єктах клієнта. Вона складається з інтелектуальних контролерів та зчитувачів, які підключаються безпосередньо до хмари через зашифровані канали (наприклад, TLS) через Інтернет.

Переваги хмарних рішень для бізнесу є значними. По-перше, це глобальна масштабованість. Менеджери з безпеки можуть керувати десятками різних об’єктів у різних країнах з єдиного веб-браузера або мобільного додатку. Додавання нового офісу вимагає лише встановлення контролерів на дверях та підключення їх до мережі Інтернет; немає потреби розгортати локальні сервери чи встановлювати складні VPN-тунелі між локаціями. По-друге, хмарна модель забезпечує «безшовне» розгортання інновацій (Evergreen IT). Постачальник ACaaS автоматично застосовує оновлення прошивок (Over-The-Air, OTA), виправляє вразливості нульового дня та оновлює серверне програмне забезпечення без жодного втручання з боку локального IT-персоналу клієнта. Крім того, сучасні ACaaS-платформи (наприклад, Brivo, Kisi, Avigilon Alta, ButterflyMX) підтримують мобільні облікові дані, дозволяючи користувачам відкривати двері смартфонами через хмарну верифікацію.

Водночас «чиста» хмарна модель має певні застереження. Оскільки система спирається на публічну інфраструктуру, вона вимагає гарантованого доступу до мережі Інтернет. Більшість сучасних хмарних контролерів розроблені з урахуванням стійкості до відключень мережі: вони кешують базу даних локально, щоб гарантувати прохід авторизованих осіб навіть під час збоїв у роботі провайдера. Однак в автономному режимі адміністратори не зможуть дистанційно додати нових користувачів, змінити розклади або отримувати сповіщення про тривоги в режимі реального часу до моменту відновлення підключення.

Попри численні переваги чистих публічних хмар, повністю мігрувати туди готові не всі організації. Підприємства зі строгими вимогами до безпеки, об’єкти критичної інфраструктури, фінансові установи та оборонні підрядники стикаються з регуляторними обмеженнями, які забороняють зберігати чутливі дані за межами власних дата-центрів. Крім того, на великих промислових комплексах мережеві затримки при опитуванні хмарних серверів можуть знижувати швидкодію складних локальних автоматизацій.

Щоб подолати ці обмеження, індустрія адаптувала «гібридну хмарну архітектуру». Гібридна модель (рис. 7.4) поєднує обчислювальну потужність і гнучкість публічних хмар з високим рівнем контролю, захисту та продуктивності локальної інфраструктури або приватної хмари. Вона не просто передбачає паралельне використання двох середовищ, а створює уніфікований оркестрований простір, де робочі навантаження переміщуються туди, де їхнє виконання є найбільш ефективним з точки зору вартості, безпеки та продуктивності.

Ключовим компонентом гібридної системи є наявність локального гібридного шлюзу або сервера (Hybrid Gateway/Appliance) у межах

корпоративного периметра. Цей шлюз безпосередньо взаємодіє з усіма локальними контролерами дверей, забезпечуючи миттєву маршрутизацію трафіку без звернення до Інтернету. Шлюз збирає логи, проводить первинний аналіз та агрегацію даних, а потім періодично синхронізує їх з хмарною площиною управління.

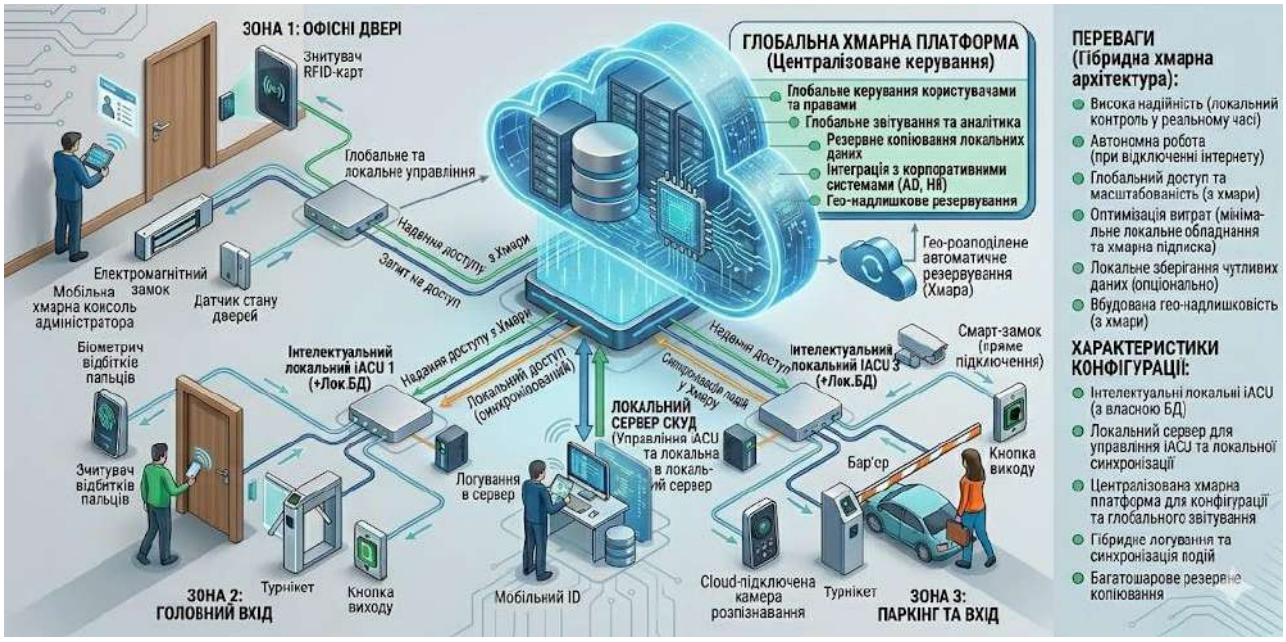


Рисунок 7.4 – Топологія гібридної хмарної архітектури

Найважливішою причиною впровадження гібридної моделі є забезпечення «локальної виживаності». Якщо об’єкт (наприклад, завод або лікарня) втрачає зв’язок з магістральним Інтернет-провайдером, локальний шлюз бере на себе повний контроль. Глобальні правила, складні автоматизації інтеграції з локальними системами відеоспостереження, ліфтовими контролерами та пожежними сигналізаціями продовжують функціонувати в ізольованому контурі. За даними досліджень, 90% великих корпорацій планують перейти саме на гібридні моделі управління IT до 2027 року, оскільки це дозволяє зберігати базу даних співробітників за корпоративним фаєрволом, одночасно використовуючи публічну хмару для масштабування гостьових інтерфейсів чи мобільних додатків. Провідні платформи, такі як Genetec Security Center SaaS, відкрито декларують використання саме гібридно-хмарної архітектури для забезпечення надійного зв’язку між хмарними, локальними та периферійними компонентами.

Надійність архітектури СКУД визначається не лише топологією серверів, але й стандартами зв’язку між апаратними пристроями на базовому рівні. Особливої уваги заслуговує протокол обміну даними між зчитувачем і контролером, а також екосистеми самих контролерів.

На даний час індустрія СКУД активно відмовляється від пропрієтарних контролерів, які прив’язують клієнта до програмного забезпечення одного виробника (vendor lock-in), на користь «відкритої апаратної архітектури». Відкрита архітектура дозволяє замовникам вибирати найкраще програмне забезпечення та безболісно замінювати його в майбутньому, не міняючи дороге периферійне обладнання.

Яскравим прикладом є платформа контролерів від компанії Mercury Security (нині частина HID Global). Панелі Mercury є галузевим стандартом, сумісним з десятками провідних програмних комплексів (наприклад, Genetec Synergis). Новітньою розробкою у цій екосистемі є контролери серії HID Aero, які замінили застарілу лінійку VertX. HID Aero підтримує наскрізне шифрування від ідентифікатора до хоста, забезпечуючи OSDP Secure Channel на порту зчитувача та шифрування TLS у середовищі, що відповідає стандарту FIPS 140-2, для комунікації із сервером управління. Втім, експерти відзначають, що екосистема програмного забезпечення для повної підтримки Aero ще перебуває на стадії розширення, тому традиційні плати Mercury залишаються більш універсальним вибором для великих інтеграцій.

Ще одним впливовим гравцем відкритого ринку є шведська компанія Axis Communications зі своїми IP-базованими контролерами A1001 та A1601. Вони функціонують виключно по Ethernet (з підтримкою PoE/PoE+) і не залежать від пропрієтарних програмних кодів, спираючись на відкриті стандарти ONVIF (Profile A та C) та власний відкритий API VAPIX. Модель A1001 оптимізована для малих об’єктів і має вбудоване базове програмне забезпечення (Axis Entry Manager), що дозволяє їй працювати взагалі без зовнішнього сервера, тоді як високопродуктивний A1601 призначений для корпоративних мереж, містить потужний процесор, розширену кількість входів/виходів та здатен зберігати в локальній пам’яті до 70 000 ідентифікаторів. Інтеграція таких пристроїв відбувається безпосередньо по IP-мережі, що спрощує розгортання в розподілених та хмарних топологіях.

Фінансове обґрунтування вибору між локальною, хмарною та гібридною інфраструктурами є однією з найскладніших задач для IT-директорів та фінансових керівників. Економічна модель прийняття рішень зводиться до вибору між значними одноразовими капітальними витратами та передбачуваними, регулярними операційними витратами.

Об’єктивне порівняння цих моделей неможливе лише на основі початкових прайс-листів. Воно вимагає розрахунку сукупної вартості володіння протягом 5-7 років, що враховує не лише апаратне забезпечення та ліцензії, але й витрати на енергоспоживання, персонал, модернізацію та ризики простоїв.

Успіх впровадження будь-якої зі згаданих макроархітектур залежить від вибору правильного апаратного забезпечення. Відкрита архітектура контролерів (таких як Axis або HID Mercury) гарантує захист інвестицій, усуваючи монопольну залежність від одного виробника програмного забезпечення. Зрештою, вибір архітектури СКУД – це комплексне стратегічне рішення, що вимагає синергії між підрозділами фізичної охорони, інформаційних технологій та фінансів для досягнення оптимального балансу між гнучкістю, безпекою та сукупною вартістю володіння інфраструктурою.

7.2 Інтегрування СКУД з BMS, відеоспостереженням та системами енергоменеджменту

У сучасній інженерії та управлінні комерційною нерухомістю відбувається зсув від ізольованих інженерних мереж до єдиних інтелектуальних екосистем. Традиційно СКУД, системи відеоспостереження, системи управління будівлею (BMS) та системи енергоменеджменту (EMS) функціонували в окремих, непов'язаних інформаційних середовищах, що обмежувало їхню загальну ефективність [1737]. Проте стрімке зростання вартості енергоносіїв, посилення екологічних норм, таких як європейська звітність щодо викидів CO_2, а також еволюція кіберзагроз зумовили необхідність глибокої архітектурної конвергенції [90]. Ця конвергенція перетворює будівлю з пасивного об'єкта, який просто споживає ресурси, на адаптивний кіберфізичний механізм, здатний у режимі реального часу реагувати на присутність людей, оптимізувати енергоспоживання, забезпечувати фізичну безпеку та проактивно виявляти аномалії (рис. 7.5).

Аналіз експлуатаційних даних свідчить, що застосування інформації зі СКУД для управління системами опалення, вентиляції, кондиціонування та освітленням дозволяє знизити експлуатаційні енерговитрати на показники від двадцяти до тридцяти відсотків, водночас підвищуючи рівень комфорту та безпеки для резидентів. Окремі дослідження, проведені лідерами ринку в центральних офісах мегаполісів, фіксують зниження операційного енергоспоживання та викидів вуглецю в переговорних кімнатах на двадцять два відсотки виключно завдяки автоматизації на основі даних про присутність.

Для розуміння синергії інтегрованих рішень необхідно чітко розмежувати ролі BMS та EMS, оскільки на практиці їх часто помилково ототожнюють, незважаючи на їхнє різне функціональне призначення.

Система BMS просторово та логічно орієнтована на внутрішнє середовище об'єкта. BMS працює на основі попередньо заданих уставок, розкладів та локальних датчиків, використовуючи стандартизовані протоколи зв'язку, такі як BACnet, Modbus, LonWorks або KNX. Якщо офісний простір

потребує підтримання температури на рівні двадцяти одного градуса за Цельсієм, алгоритми BMS автоматично регулюють засувки та швидкість вентиляторів для досягнення цього показника.

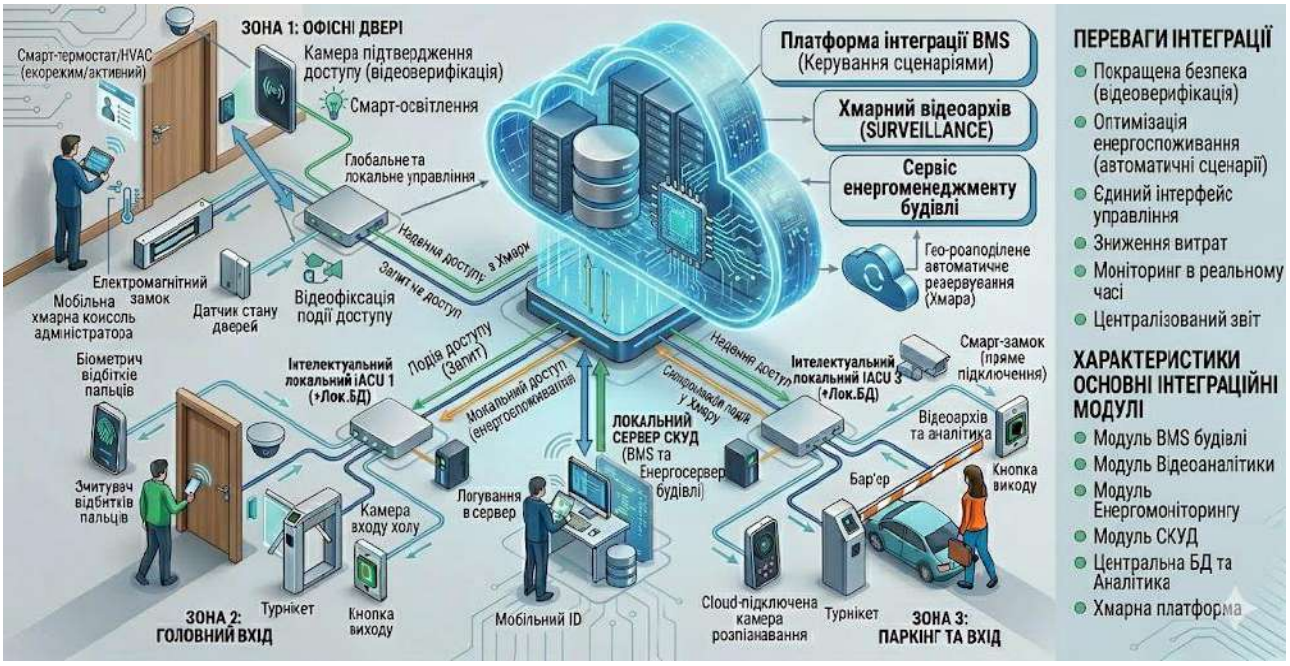


Рисунок 7.5 – Інтеграція СКУД з BMS, відеоспостереженням та системами енергоменеджменту

Натомість система EMS оперує значно ширшим макроскопічним контекстом. Вона керує всіма енергетичними активами об’єкта, включаючи сонячні панелі, акумуляторні батареї, теплові насоси та зарядні станції для електромобілів. EMS постійно взаємодіє із зовнішніми сигналами, такими як динамічні тарифи електромережі, обмеження потужності та загально цільовими показниками викидів CO_2. Інтеграція BMS та EMS створює єдиний стек управління, який стирає межі між комфортом та ресурсною ефективністю. Наприклад, коли інтегрована платформа отримує сигнал про пікове навантаження в зовнішній електромережі, EMS може надіслати команду системі BMS тимчасово підвищити уставку температури охолодження на кілька градусів або зменшити інтенсивність освітлення у приміщеннях з низьким рівнем заповненості.

Такий підхід не лише забезпечує комфорт, але й гарантує верифікований контроль енергоефективності.

Сучасна архітектура корпоративної безпеки вимагає максимально тісної інформаційної взаємодії систем контролю доступу з платформами інтелектуальної відеоаналітики. Технологічна інтеграція систем відеоспостереження та СКУД трансформує підходи до управління об’єктом

захисту, забезпечуючи перехід від пасивного, реактивного спостереження після інциденту до проактивного управління ризиками в реальному часі.

При об'єднанні систем відеоспостереження та СКУД на базі потужних програмних комплексів, таких як Milestone XProtect або SecurOS ACS, метадані подій контролю доступу (наприклад, номер картки, час, ідентифікатор дверей) нерозривно прив'язуються до відповідних відеопотоків у спільній базі даних. Це надає операторам центрів управління безпекою безпрецедентні можливості: візуальне підтвердження особи, алгоритмічне запобігання неточності підрахунку кількості осіб на об'єкті та оптимізації розслідування не стандартних інцидентів.

Так, під час використання електронного ідентифікатора система миттєво виводить у єдиному консолідованому інтерфейсі фотографію власника з офіційної бази даних поруч із живим відеопотоком з камери, встановленої безпосередньо над дверима, унеможливлюючи використання чужих перепусток.

У свою чергу, завдяки інтеграції, відеоаналітика здатна автоматично підраховувати точну кількість осіб, що фактично перетнули периметр після однієї легітимної валідації картки. У разі виявлення розбіжностей (наприклад, авторизовано одну людину, а пройшло двоє), система миттєво генерує тривогу та блокує наступні шлюзи.

Будь-яка нестандартна подія в СКУД, така як багаторазова відмова в доступі через недійсний рівень прав, автоматично створює розумну закладку в архіві відеореєстратора. Це скорочує час, необхідний службі безпеки на пошук відповідних відеофрагментів інцидентів, з кількох годин до лічених секунд.

Глобальна стандартизація інформаційної взаємодії між IP-камерами, програмним забезпеченням управління відео, контролерами СКУД та різноманітними IoT-пристроями забезпечується екосистемою відкритих стандартів ONVIF. Уніфікація через ONVIF дозволяє уникнути прив'язки до одного вендора та будувати гетерогенні системи.

Аналіз сучасного стану інтеграції інженерних, безпекових та енергетичних систем розкриває масштабний перехід усієї будівельної та IT-галузі на принципово новий, кіберфізичний рівень функціонування. Розгляд даної проблематики, від алгоритмів управління до аналізу протоколів зв'язку, дозволяє сформулювати наступні ключові висновки.

По-перше, інформаційні дані остаточно перетворилися на універсальний актив. Глибока інтеграція СКУД із системами BMS трансформує масиви інформації про присутність людей із простого ресурсу для забезпечення периметральної безпеки на високоточний інструмент енергетичної оптимізації. Адаптація вентиляції, клімату та систем освітлення на базі реальної, а також

математично прогнозованої зайнятості приміщень дозволяє стабільно досягати понад двадцяти відсотків економії енерговитрат без жодного негативного впливу на тепловий комфорт користувачів.

По-друге, алгоритмізація та застосування штучного інтелекту змінюють архітектуру управління. Впровадження математичних моделей предиктивного управління та використання камер відеоаналітики на базі нейромереж для підрахунку осіб чи розпізнавання обличь значно розширює горизонти можливостей інфраструктурних систем. Технології розпізнавання обличь більше не є експериментальними; вони стають невід'ємним базовим елементом безконтактного багатофакторного доступу, інтегруючись безпосередньо в платформи відеоспостереження завдяки відкритим профілям ONVIF.

Нарешті, слід відзначити високу технологічну зрілість ринку та рішень. Глобальні вендори (такі як Siemens, Schneider Electric, Honeywell, Genetec, Milestone) вже сьогодні надають надійні комплексні платформи для безшовної конвергенції різних протоколів в єдиний інформаційний простір оператора. Водночас український ринок переконливо демонструє свою стійкість та високу здатність не лише імплементувати найкращі світові практики, а й розробляти конкурентоздатні апаратно-програмні рішення світового рівня для подальшого глобального масштабування.

Підсумовуючи, можна впевнено констатувати, що комплексна, багаторівнева інтеграція цих систем – це не просто тимчасовий тренд зручності для операторів, а безальтернативна довгострокова технологічна стратегія. Вона виступає фундаментальним інструментом для досягнення глобальних цілей вуглецевої нейтральності, забезпечення фінансової життєздатності комерційних активів та створення гнучких, безпечних і комфортних просторів у сучасному цифровому світі. Успішне проектування та розгортання таких інтегрованих кіберфізичних систем у майбутньому неминуче потребуватиме від інтеграторів та замовників глибокої, міждисциплінарної експертизи на складному стику теплотехніки, електроніки, інформаційних систем та передової кібербезпеки.

7.3 Програмне забезпечення великих СКУД: бази даних та серверна логіка

Історично архітектура СКУД базувалася на закритих, пропрієтарних апаратних і програмних комплексах, які функціонували як ізольовані острівці безпеки, що суттєво обмежувало можливості масштабування та створювало жорстку залежність від одного постачальника обладнання [40]. Сучасні вимоги до корпоративної безпеки, навпаки, диктують необхідність переходу до рішень, побудованих на відкритій архітектурі, що дозволяє інтегрувати апаратне забезпечення різних виробників (наприклад, зчитувачі HID, панелі Bosch) з

уніфікованими програмними платформами, такими як Genetec Security Center або LenelS2 OnGuard. Відкрита архітектура забезпечує організаціям стратегічну гнучкість, дозволяючи обирати найкращі у своєму класі пристрої та програмні модулі відповідно до мінливих бізнес-потреб, зберігаючи при цьому єдиний центр управління [22].

Управління географічно розподіленими підприємствами вимагає складних топологій програмного забезпечення, здатних підтримувати єдність політик безпеки на всіх об'єктах. Наприклад, сегментовані архітектури баз даних дозволяють створювати багаторівневі серверні структури, де головний корпоративний сервер накопичує всі транзакції та керує глобальними політиками, тоді як регіональні сервери забезпечують безперебійну роботу на місцях. Подібний підхід реалізується через концепцію федерації, яка здатна об'єднувати сотні або тисячі віддалених локацій відеоспостереження та доступу в єдину глобальну систему моніторингу. Завдяки федерації оператори отримують консолідоване уявлення про всі об'єкти з автоматичною синхронізацією даних апаратних засобів, таких як камери, двері, турнікети та панелі вторгнення, що радикально підвищує операційну ефективність. Для підтримки такої складної екосистеми програмне забезпечення СКУД спирається на передові рішення у проектуванні баз даних, алгоритмах асинхронної обробки подій, протоколах мережевої комунікації та інтеграції з IT-середовищем.

Масштабні системи доступу генерують безперервний потік даних у режимі реального часу, починаючи від запитів на автентифікацію і закінчуючи телеметрією датчиків стану дверей та тривожними сповіщеннями. Традиційна синхронна архітектура, у якій програмні компоненти безпосередньо викликають один одного через блокуючі запити (наприклад, REST API), виявляється неефективною в умовах пікових навантажень [39]. Замість цього розробники сучасних систем корпоративного рівня впроваджують архітектуру, керовану подіями (Event-Driven Architecture, EDA), що дозволяє досягти високої швидкості реагування та слабкої зв'язності між мікросервісами. В середовищі EDA кожна зміна стану (наприклад, надання доступу або примусове відкриття дверей) транслюється як асинхронна подія, на яку незалежно реагують інші підсистеми – модулі відеоспостереження, підсистеми управління ліфтами або аналітичні платформи.

Для обробки запитів від десятків тисяч контролерів та одночасного доступу сотень операторів програмне забезпечення має бути оптимізоване для високої паралельності та мінімальної затримки. Архітектурний шаблон SEDA (Staged Event-Driven Architecture) застосовується для поділу процесу обробки складних запитів на низку автономних етапів, з'єднаних чергами повідомлень.

Такий підхід дозволяє пулам потоків ефективно вилучати запити з черг, виконувати обчислення та передавати результати на наступний етап, запобігаючи виснаженню системних ресурсів навіть у моменти екстремальних навантажень. Розподіл завдань на підзадачі, які можуть виконуватися паралельно, є ключовим фактором зниження затримки на рівні програмного забезпечення.

Ефективність взаємодії між центральним сервером та периферійним обладнанням (контролерами доступу, панелями сигналізації) безпосередньо залежить від використовуваних протоколів зв'язку. Традиційне періодичне опитування пристроїв з боку сервера генерує надлишковий мережевий трафік та спричиняє затримки у виявленні тривог. Тому сучасні індустріальні системи переходять на протоколи з механізмами push-повідомлень, здатні підтримувати постійні з'єднання [11].

Для передачі телеметрії та обміну подіями найчастіше використовується легковагий протокол MQTT (Message Queuing Telemetry Transport), розроблений спеціально для мереж з низькою пропускною здатністю та високою латентністю. Завдяки моделі публікації та підписки (publish/subscribe), MQTT звільняє контролери від необхідності підтримувати прямі з'єднання один з одним; натомість усі пристрої взаємодіють через центрального брокера повідомлень. Окрім MQTT, для безперервного двостороннього зв'язку між клієнтськими застосунками (наприклад, веб-панелями операторів) та сервером використовується протокол WebSockets, який встановлює повнодуплексний канал поверх єдиного TCP-з'єднання.

При розрахунку потужності апаратного забезпечення сервера для обробки тисяч одночасних з'єднань через протоколи сімейства TR-069 або USP/TR-369 необхідно враховувати кількість параметрів моніторингу на кожному пристрої. Впровадження механізмів підтримки постійних з'єднань також вимагає складних стратегій обходу трансляції мережевих адрес (NAT) за допомогою протоколів STUN або XMPP, що додає обчислювального навантаження на мережевий рівень сервера.

Фундаментальним викликом для баз даних масштабних систем безпеки є необхідність одночасної обробки двох діаметрально протилежних робочих навантажень: управління складними реляційними зв'язками конфігурацій (користувачі, розклади, двері, права) та безперервне поглинання колосальних масивів неструктурованих телеметричних даних (події проходу, тривоги). Це зумовлює гостру дискусію щодо вибору між SQL та NoSQL технологіями в індустрії фізичної безпеки [33, 112].

Традиційні реляційні бази даних (SQL), такі як Microsoft SQL Server, Oracle або PostgreSQL, десятиліттями слугували основою корпоративних

систем завдяки своїй здатності підтримувати транзакційну цілісність (ACID) та виконувати складні аналітичні запити. Для зберігання організаційної структури підприємства SQL залишається найоптимальнішим вибором. Однак реляційні системи обмежені жорсткими схемами; міграція даних при додаванні нових параметрів апаратного забезпечення може викликати простої. Крім того, вертикальне масштабування SQL має фізичні ліміти, а горизонтальне партиціювання (sharding) реляційних таблиць вимагає складної логіки на рівні додатку.

У відповідь на ці обмеження, архітектори звертаються до NoSQL-баз даних (наприклад, AWS DynamoDB, Azure Cosmos DB, MongoDB) для обробки потоків подій. NoSQL-системи забезпечують гнучкість схем, що ідеально підходить для зберігання неструктурованих подій у форматі JSON, і пропонують вбудоване горизонтальне масштабування, розподіляючи навантаження між багатьма фізичними вузлами кластера. NoSQL-системи є оптимальним вибором для аналітики великих даних в СКУД, тоді як SQL-бази краще справляються з транзакційною обробкою (OLTP).

При використанні реляційної моделі для збереження журналів, створення окремих таблиць для сотень різних типів подій призводить до деградації архітектури бази даних. Дизайн з використанням моделі EAV хоча й змушує зберігати параметри у строковому форматі замість нативних типів даних, проте радикально знижує експлуатаційні витрати на супровід коду під час оновлень СКУД. Для гібридних багаторегіональних застосувань також застосовуються глобально розподілені бази даних, такі як Oracle Globally Distributed AI Database, які використовують консенсусні алгоритми реплікації (наприклад, Raft) для автоматичного дублювання даних між дата-центрами, забезпечуючи високу продуктивність та дотримання вимог локалізації даних без зміни SQL-коду додатків.

Скомпрометована доступність системи контролю доступу може призвести до критичних наслідків: від блокування персоналу на об’єкті до створення прогалин у периметрі безпеки. Щоб мінімізувати вплив апаратних відмов або збоїв програмних служб, корпоративні СКУД обов’язково розгортаються у конфігураціях високої доступності (High Availability, HA). Кластеризація HA забезпечує стійкість системи шляхом використання надлишкового програмного забезпечення та серверних вузлів, які постійно моніторять стан один одного.

Основний цикл роботи високодоступної архітектури складається з трьох послідовних етапів. По-перше, система здійснює безперервне виявлення збоїв через моніторинг обміну сигналами життєдіяльності між компонентами. По-друге, у разі виявлення втрати зв’язку або зупинки служби виконується

автоматичне аварійне перемикання на резервний хост без необхідності ручного втручання адміністратора. По-третє, система намагається автономно перезапустити або відновити пошкоджений сервіс. Цей підхід ефективно нівелює як апаратні проблеми (збої пам'яті, процесорів чи мережевих адаптерів), так і програмні помилки додатків.

У контексті розгортання баз даних, наприклад Microsoft SQL Server у середовищі СКУД, налаштовується синхронна реплікація між первинним та вторинним серверами. У разі падіння активного вузла, вторинний сервер миттєво підвищується до ролі первинного, гарантуючи повну консистентність даних. Для зменшення витрат на дорогу інфраструктуру мереж зберігання даних (SAN) можуть застосовуватися програмні рішення SANless кластеризації. Наприклад, спеціалізоване програмне забезпечення (наприклад, SafeKit) забезпечує двовузлову кластеризацію з реплікацією в реальному часі для електронних СКУД (Siemens, HID, Nedap), досягаючи показника нульової втрати даних (RPO=0) під час перемикання. Робочі служби управління (наприклад, служби SVN для управління версіями) також об'єднуються у відмовостійкі кластерні групи. Перед активацією HA за допомогою Microsoft Failover Cluster адміністратори повинні завжди перевіряти статус запуску критичних служб серверів управління для успішної ініціалізації кластера.

У великих розподілених СКУД центральний сервер фізично не здатний ухвалювати мілісекундні рішення для тисяч дверей одночасно через мережеві затримки. Відповідно, вся логіка доступу повинна бути завантажена безпосередньо у пам'ять мікропроцесорних контролерів. Для досягнення цієї мети застосовується багаторівневий механізм синхронізації, який перетворює великі конфігураційні інструкції з сервера на послідовність атомарних завдань, що поетапно завантажуються в буфер процесора контролера. Це гарантує безперебійне виконання команд у реальному часі навіть під час оновлення правил доступу. Сучасні контролери оснащені енергонезалежною Flash-пам'яттю, яка зберігає базу даних користувачів після зникнення живлення, а для управління багатопотоковими процесами використовуються апаратні механізми міжпроцесорної комунікації (IPC), де переривання та прапорці статусу координують взаємодію обчислювальних ядер і мережевих модулів.

Здатність апаратних панелей та регіональних серверів працювати в автономному режимі є важливим для виживання системи під час порушення глобального зв'язку (WAN-аварій). Коли з'єднання з центральним сервером втрачається, локальний вузол акумулює всі транзакції та зміни в кеші. Справжній виклик постає після відновлення зв'язку – так звана «проблема узгодження», коли необхідно інтегрувати розрізнені набори даних та вирішити конфлікти паралельних модифікацій.

Класичний підхід блокування ресурсів, який забороняє модифікації для уникнення конфліктів, є неприйнятним для фізичної безпеки, оскільки доступ не може бути призупинений через технічний збій. Натомість системи застосовують «оптимістичну реплікацію», дозволяючи локальні оновлення та вирішуючи суперечності постфактум за допомогою алгоритмів на основі міток часу. Однак у випадку сильного відхилення годинників між пристроями цей метод може давати збої. Тому точна синхронізація часу контролерів із серверами NTP (Network Time Protocol) є життєво необхідною передумовою для коректного вирішення конфліктів. У деяких ситуаціях (як, наприклад, розсинхронізація баз даних у Cisco ACS) втрата синхронізації або «зависання» транзакцій у статусі PENDING може вимагати увімкнення розширеного рівня діагностики або навіть повного перезавантаження служб для відновлення реплікації. Організації також повинні враховувати кіберризики, пов'язані з маршрутизацією трафіку під час аварійного перемикання провайдерів. Інциденти демонструють, що використання резервних, але застарілих маршрутів для відновлення зв'язку може призвести до обходу сучасних рівнів моніторингу та створити непередбачувані загрози для синхронізації баз даних.

Окремим класом розподіленої серверної логіки є управління глобальним забороною повторного проходу (Global Anti-Passback, GAP). Правило GAP забороняє власнику картки передати її колезі після того, як він сам успішно пройшов турнікет. У традиційній архітектурі, якщо вхідний та вихідний турнікети підключені до різних контролерів, рішення про блокування ухвалюється виключно сервером.

Однак сучасні технології дозволяють наділити контролери 100% розподіленим інтелектом. Використовуючи комунікацію типу «Peer-to-Peer» (від вузла до вузла), контролери автоматично синхронізують статуси присутніх користувачів у межах своєї мережевої групи без участі центрального хоста. Якщо зв'язок між контролерами порушується, адміністратори повинні передбачити логіку дій. Наприклад, режим Hard GAP блокуватиме доступ до відновлення зв'язку, тоді як Soft GAP дозволить прохід, але згенерує тривогу «Порушення послідовності» для подальшого розслідування оператором. У масштабних інсталяціях, де бездротові або дротові вузли повинні обмінюватися даними, застосовуються механізми швидкого перемикання між первинним та вторинним контролерами (з визначеними тайм-аутами повторних передач), що забезпечує стабільність зв'язку на фізичному рівні. При використанні радіусних протоколів (PEAP) між контролером та сервером доступу важливо оптимально налаштувати таймінги трафіку, щоб уникнути блокування облікових записів Active Directory через затримки кешування.

СКУД підприємства не може ефективно працювати у вакуумі. Її архітектура повинна інтегруватися з наявною цифровою екосистемою, зокрема системами управління людськими ресурсами та каталогами користувачів [18]. Прикладні програмні інтерфейси (API) усувають необхідність ручного втручання адміністраторів, створюючи надійні комунікаційні мости для автоматичного потоку даних між розрізненими хмарними та локальними платформами.

До впровадження сучасних API адміністраторам доводилося покладатися на періодичний імпорт плоских файлів (CSV, скрипти PowerShell) або SQL-витяги, що призводило до затримок у відкликанні прав та накопичення помилок. Сучасні платформи, такі як SAP Integration Suite або CyberArk Identity, дозволяють конфігурувати детальні схеми перетворення атрибутів, підтримуючи як локальні, так і гібридні IT-середовища з обміном даними у форматі реального часу. Безпека таких інтеграцій гарантується використанням захищених протоколів аутентифікації на кшталт Kerberos та зовнішніх захищених сховищ для зберігання облікових даних API.

Усвідомлюючи важливість патчингу вразливостей (наприклад, zero-days експлойтів), організації докладають величезних зусиль для оновлення серверних операційних систем, проте часто нехтують оновленням прошивок апаратних контролерів. Ручне оновлення мікропрограм для тисяч пристроїв є нераціональним. Тому програмне забезпечення великих СКУД бере на себе функції централізованого оркестрування прошивок, подібно до інструментів рівня дата-центрів (таких як Dell EMC OpenManage Enterprise або хмарні системи забезпечення вузлів Kubernetes). Ці модулі автоматично проводять інвентаризацію всіх підключених контролерів, здійснюють постійний моніторинг стану та ініціюють безпечні оновлення мікропрограм у фоновому режимі. Для уникнення операційних простоїв оновлення плануються на неробочий час. Створення багатофункціональних корпоративних політик управління оновленнями гарантує, що у випадку критичного збою прошивки система зможе ініціювати алгоритми автоматичного відкату, зберігаючи працездатність контролера та цілісність периметра безпеки.

Журналювання подій у СКУД слугує фундаментом для виявлення підозрілої активності, моніторингу політик дотримання нормативів та надання інформації для форензики після кіберінцидентів. Відсутність або слабке налаштування системи аудит-логів позбавляє організацію можливості реконструювати ланцюг подій під час розслідування витоку даних чи несанкціонованого доступу.

Для забезпечення ефективного журналювання організації впроваджують суворі політики зберігання даних, які збалансовують юридичні вимоги,

бюджетні обмеження на зберігання даних та операційні потреби безпеки. Журнали подій безпеки повинні зберігатися значно довше, ніж стандартні журнали продуктивності програм, оскільки багато складних кібератак залишаються непоміченими місяцями.

Сучасним стандартом безпеки є безперервний експорт відфільтрованих журналів зі СКУД до платформ управління інформацією та подіями безпеки (SIEM-систем, таких як Splunk або архітектур CrowdStrike). SIEM-системи забезпечують перехресну кореляцію даних між інфраструктурами. Наприклад, якщо СКУД реєструє спробу несанкціонованого проходу карткою у серверне приміщення, а в цей же момент IT-система фіксує масове завантаження скриптів з невідомої IP-адреси, SIEM миттєво генерує комплексну тривогу про масштабну скоординовану атаку. Оскільки SIEM-платформи та бази даних СКУД є надзвичайно привабливими мішенями для хакерів, їх також необхідно захищати. З боку самих систем управління базами даних інсталюються спеціалізовані модулі аудиту (наприклад, PgAudit для PostgreSQL або вбудований інструментарій Auditing для MongoDB), які фіксують будь-які нелегітимні спроби модифікації структури таблиць (схеми) або виконання SQL-ін’єкцій безпосередньо в середовищі зберігання даних в обхід програмної логіки СКУД.

Таким чином, архітектура програмного забезпечення великих СКУД зазнала фундаментальної трансформації. Відкрита екосистема витіснила закриті пропрієтарні рішення, дозволивши організаціям масштабувати свої системи через федерацію та інтегрувати різноманітні підсистеми в єдине операційне середовище. Це масштабування стало можливим завдяки переходу серверної логіки на подієво-керовану архітектуру (EDA), яка через впровадження шаблонів CQRS, SEDA та Change Data Capture усуває вузькі місця у продуктивності та забезпечує мілісекундні реакції системи.

Вибір підходів до зберігання інформації демонструє глибоку диференціацію – реляційні бази даних (SQL) застосовуються для підтримки цілісності організаційної структури та конфігураційних моделей з використанням EAV-стратегій, тоді як нереляційні рішення (NoSQL) впроваджуються для горизонтально масштабованого управління мільйонами неструктурованих телеметричних подій. Гнучкість зберігання даних підкріплюється вдосконаленням комунікаційних механізмів, де протоколи з постійним з’єднанням (MQTT, WebSockets) прийшли на зміну застарілим моделям опитування, гарантуючи негайне доставлення повідомлень.

Фізична безпека об’єктів залежить від безперервності роботи. Тому програмні комплекси розгортаються з використанням систем високої доступності, кластеризації Active/Standby та рішень для синхронної реплікації.

У разі критичних відключень комунікацій (WAN-аварій) сучасні контролери переймають на себе повний контроль за допомогою алгоритмів розподіленого інтелекту та взаємодії Peer-to-Peer, забезпечуючи локальне виконання правил глобального Anti-Passback та збереження працездатності периметра з подальшим вирішенням конфліктів шляхом оптимістичної реплікації після відновлення зв'язку.

Безшовна інтеграція через API з ERP-системами та корпоративними каталогами ідентифікації дозволяє повністю автоматизувати процеси ротації персоналу, унеможливлюючи залишення активних пропусків після звільнення співробітників. Зрештою, наскрізне криптографічне шифрування на всіх рівнях, разом із централізованими механізмами управління мікропрограмами та потужною аналітикою журналів подій у SIEM, перетворює сучасну СКУД на стійкий кіберфізичний бастіон, здатний протистояти викликам безпеки корпоративного рівня.

Контрольні запитання

1. Опишіть основні етапи роботи циклу High Availability.
2. У чому полягає основна архітектурна відмінність між централізованою та розподіленою моделями СКУД у плані прийняття рішень?
3. У чому полягає різниця між пропрієтарною та сучасною відкритою архітектурою СКУД?
4. У чому полягає різниця між системами управління будівлею та системами енергоменеджменту?
5. Чому великі корпорації та об'єкти критичної інфраструктури надають перевагу гібридній хмарній архітектурі?
6. Чому протокол MQTT вважається більш ефективним за традиційне періодичне опитування пристроїв сервером?
7. Чому сучасні корпоративні СКУД часто використовують гібридний підхід для зберігання даних?
8. Що таке "відкрита апаратна архітектура" контролерів?
9. Що являє собою концепція ACaaS? Назвіть її переваги в контексті Evergreen IT?
10. Як використання нейромереж та технологій розпізнавання обличчя змінює сучасну архітектуру управління доступом?
11. Як зрозуміти трансформацію будівлі з «пасивного об'єкта» на «адаптивний кіберфізичний механізм»?
12. Як реалізується логіка глобальної заборони повторного проходу?
13. Як система інтегрованої відеоаналітики запобігає несанкціонованому проходу декількох осіб за однією перепусткою?

14. Яким чином розподілена архітектура забезпечує "відмовостійкість" системи у разі втрати зв’язку з сервером?

15. Які ключові компоненти формують основу будь-якої СКУД та їх роль?

16. Які критичні вразливості централізованої архітектури роблять її неефективною для великих підприємств?

17. Які переваги надає архітектура EDA у порівнянні із традиційною архітектурою на основі REST API?

18. Які переваги надає операторам центрів безпеки прив’язка метаданих СКУД до відеопотоків у реальному часі?

19. Які протоколи або методи використовуються в розподілених системах для забезпечення консистентності даних та запобігання конфліктам запису?

20. Які чинники зумовили перехід від ізольованих інженерних мереж до єдиних інтелектуальних екосистем у сучасних СКУД?

21. Яку проблему вирішує модель EAV під час проєктування реляційних баз даних в СКУД?

22. Яку роль відіграє екосистема відкритих стандартів ONVIF у побудові сучасних систем безпеки?

23. Яку роль відіграє шаблон SEDA у забезпеченні високої швидкості реагування системи?

РОЗДІЛ 8. Штучний інтелект та кібербезпека в СКУД

8.1 Предиктивна безпека та поведінковий аналіз переміщень

Сучасна корпоративна безпека переходить від традиційних стратегій реагування на інциденти до предиктивного моделювання загроз. Основою цього переходу є безпрецедентне зближення СКУД, масштабованих мереж IoT, розподілених хмарних обчислень та передових алгоритмів штучного інтелекту (ШІ) і машинного навчання (МН). Традиційні системи ідентифікації, архітектура яких історично базувалася виключно на принципі перевірки статичних облікових даних, виявилися вразливими до сучасних багатовекторних атак [81]. До таких загроз належать крадіжка ідентифікаторів, соціальна інженерія, клонування карток, а також використання згенерованих нейромережами підроблених біометричних даних, відомих як deepfakes. Статистика свідчить, що до 68% усіх витоків даних та інцидентів безпеки пов’язані з людським фактором, зокрема зі скомпрометованими обліковими даними, що експлуатують вроджені слабкості застарілих систем СКУД.

Предиктивна безпека у контексті СКУД визначається як комплексна здатність системи безперервно аналізувати історичні тенденції та поточні потоки телеметричних даних у режимі реального часу [116]. Головна мета цього аналізу – виявлення прихованих кореляцій та патернів, прогнозування потенційних порушень безпеки ще до моменту їх фактичного виникнення та автоматичне ініціювання превентивних заходів протидії. Ця нова архітектура принципово змінює фокус – вона більше не ставить тривіальне запитання «хто ви?» на точці проходу, натомість вона постійно запитує «чому ви поводитеся інакше, ніж зазвичай?». Завдяки безшовній інтеграції з хмарними інфраструктурами та технологіями периферійних обчислень (edge computing), сучасні системи СКУД набули здатності обробляти колосальні масиви багатовимірних даних. Вони перетворюють розрізнені сигнали від зчитувачів карток, відеокамер, інфрачервоних сенсорів та датчиків навколишнього середовища у єдину, цілісну картину ситуаційної обізнаності.

Очікується, що до 2027 року глобальна кількість підключених IoT-пристроїв перевищить позначку в 41 мільярд одиниць. Це експоненціально розширює потенційну поверхню атак, роблячи системи вразливими до розподілених атак на відмову в обслуговуванні (DDoS) та впровадження шкідливого програмного забезпечення. Водночас ця щільна мережа сенсорів надає безпрецедентний обсяг «великих даних» для безперервного навчання предиктивних алгоритмів. Проте розгортання таких масштабних моделей стикається зі значними викликами, серед яких високі обчислювальні витрати, вразливість до змагальних атак на самі алгоритми машинного навчання та проблеми інтерпретованості прийнятих ШІ рішень. Для подолання цих бар’єрів індустрія активно досліджує методи конфіденційного машинного навчання, пояснюваного штучного інтелекту та архітектури безпеки на базі периферійних пристроїв.

Аналітика поведінки користувачів та сутностей (UEBA – User and Entity Behavior Analytics), яка спочатку була розроблена для захисту кібернетичних мереж, сьогодні є концептуальним ядром предиктивної фізичної безпеки. Ця технологія використовує комплексні алгоритми неконтрольованого та контрольованого машинного навчання для формування індивідуальних базових ліній нормальної поведінки для кожного співробітника, підрядника, IoT-пристрою або цілої підмережі. Після етапу навчання система починає безперервний моніторинг, порівнюючи кожну поточну транзакцію доступу або просторове переміщення із встановленими еталонами. Передові вендори платформ UEBA, такі як Darktrace, Splunk Enterprise Security, IBM QRadar, Securonix, Exabeam, Rapid7 InsightIDR та Vectra AI, все частіше розширюють

свої алгоритми для кореляції подій з фізичних СКУД та логів мережевої активності. Це створює єдиний гібридний ландшафт захисту.

Математичні моделі виявлення аномалій у СКУД не розглядають відхилення як однорідні події. Натомість вони алгоритмічно розрізняють кілька специфічних типів девіацій, кожна з яких вимагає відмінного методу детекції та відповідного рівня операційної ескалації: точкові, контекстуальні та послідовні аномалії.

Точкові аномалії – це поодинокі події або транзакції, які статистично кардинально відхиляються від загального нормального розподілу даних [117]. У контексті СКУД класичною точковою аномалією є спроба доступу за допомогою бейджа рядового співробітника до критично важливої інфраструктури (наприклад, головної серверної кімнати або сховища), куди ця особа ніколи раніше не намагалася увійти. Системи виявляють такі події через статистичні пороги, допомагаючи миттєво запобігати шахрайству, оскільки навіть єдина така аномалія може сигналізувати про несанкціоноване заволодіння обліковими даними.

Контекстуальні аномалії – цей тип девіацій є значно складнішим для ідентифікації, оскільки сама по собі дія може бути абсолютно легітимною, але стає підозрілою виключно в рамках певного контексту (часу, географії, стану інших систем) [117]. Наприклад, вхід фінансового директора до головного офісу компанії є нормальною та очікуваною подією. Однак той самий вхід, зафіксований системою о 3:00 ночі в неділю, негайно класифікується як контекстуальна аномалія. Виявлення таких подій вимагає від МН-моделей глибокого розуміння багатовимірного нормального стану набору даних.

Послідовні аномалії – найбільш витончений тип відхилень, що виявляється шляхом аналізу довготривалих ланцюгів подій. Окремі дії в такому ланцюзі можуть здаватися цілком легітимними та не перевищувати порогів ризику. Але їх просторово-часова комбінація вказує на структуровану загрозу. Прикладом є серія подій: співробітник спочатку намагається відкрити двері з низьким рівнем безпеки у східному крилі, потім логіниться в систему з незвичного терміналу, а через 10 хвилин його картка застосовується на вході до зони з найвищим рівнем допуску. Інструменти неконтрольованого виявлення аномалій, такі як AECID, застосовують МН-методики для аналізу послідовностей, кореляційного аналізу та проведення статистичних тестів над лог-файлами подій СКУД.

Ключовою інновацією в сучасних системах UEBA є фундаментальний перехід від жорстких бінарних систем сповіщень до парадигми динамічного скорингу ризиків. Традиційні системи страждали від так званої «втоми від сповіщень», генеруючи тривогу на кожне незначне відхилення. Сучасні

алгоритми діють інакше: подібно до накопичення доказів у судовому процесі, система акумулює ризики з плином часу. Замість миттєвого блокування, кожній нетиповій дії алгоритм математично присвоює певну вагу ризику. Доступ адаптивно обмежується або ініціюється виклик охорони лише тоді, коли кумулятивний бал ризику конкретного користувача перевищує розрахований динамічний поріг. Дослідження ефективності цього методу підтверджують вражаючі результати – такий підхід здатен зменшити кількість хибних спрацьовувань на майже 38%, одночасно зберігаючи безпрецедентну точність виявлення справжніх інцидентів безпеки на рівні 94,7%.

Для забезпечення максимально точного скорингу передові платформи застосовують мультифакторний аналіз часових рядів (Multivariate Time-Series Analysis, MTSA), який працює на рівні сирих сигналів з давачів. Наприклад, об'єднуючи синхронізовані багатовимірні потоки даних від магнітних датчиків стану дверей, вбудованих акселерометрів, зчитувачів та відеокамер, МН-моделі здатні здійснювати складну диференціацію. Система може відрізнити безпечні фізичні аномалії – такі як санкціоноване утримання дверей відкритими для внесення великої пошти чи обладнання – від реальних кінематичних загроз, таких як спроби силового відкриття, використання спеціальних інструментів для злому або застосування відмичок, орієнтуючись виключно на часові та кореляційні патерни вібрацій та коливань сенсорів. Цей рівень аналізу перетворює СКУД на потужну, ненав'язливу інтелектуальну оболонку, що забезпечує проактивне виявлення інцидентів без перешкоджання звичайним бізнес-процесам.

Завдяки стрімкому розвитку алгоритмів комп'ютерного зору та нейромережевих архітектур, фокус предиктивної безпеки змістився з локального контролю точок проходу (дверей, турнікетів) на безперервний аналіз переміщень у всьому корпоративному просторі.

Якщо програмне забезпечення СКУД реєструє лише одну валідну транзакцію доступу за допомогою картки, а відеоаналітика водночас фіксує перетин віртуальної межі дверного отвору двома або більше сегментованими об'єктами, система миттєво генерує тривогу. Сучасні 3D-технології оцінки глибини кадру здатні досягати вражаючого рівня точності розпізнавання до 98%, демонструючи надзвичайно високу толерантність до різких змін освітлення, появи довгих тіней та складного перекриття рухомих об'єктів один одним у щільних групах. Це дозволяє не лише генерувати алерти, а й автоматично інтегрувати подібні інциденти до профілю ризику конкретного співробітника, який допустив прохід сторонньої особи.

У кризових сценаріях, коли традиційна лицьова біометрія виявляється неефективною або неможливою (наприклад, через носіння зловмисниками

масок, умисне приховування обличчя, недостатнє освітлення простору або під час хаотичних інцидентів типу active shooter), предиктивна безпека повинна покладатися на альтернативні вектори ідентифікації. Найбільш перспективним з них є аналіз кінематики тіла та біометрія ходи.

Поведінковий ШІ здатний ідентифікувати та безперервно відстежувати індивідів під час їхнього переміщення між полями зору різних камер, глибоко аналізуючи унікальні біомеханічні патерни їхньої ходи, загальну поставу та індивідуальні характеристики рухів тіла. На відміну від лицьової ідентифікації, поведінковий аналіз концентрується на діях та динамічних патернах, що додатково вирішує етичні проблеми надмірного стеження, зберігаючи конфіденційність осіб, які не демонструють підозрілої активності.

Додатково для високоточного розпізнавання рухів у просторі та класифікації фізіологічних станів людини впроваджуються надширокосмугові (Ultra-Wideband, UWB) радари та датчики. Ці пристрої здатні випромінювати радіоімпульси та вимірювати мікроскопічні зміни дистанції між сенсором і специфічними точками на кінцівках людини (наприклад, ногах). Завдяки цьому алгоритми можуть впевнено класифікувати стани: зупинка, активна ходьба, підозріла затримка на місці, або навіть перехід від сидіння до стояння. Використання UWB забезпечує надійне детектування рухів з точністю близько 95% у процесорних середовищах, вимагаючи значно менших обчислювальних ресурсів порівняно зі складними лазерними або LiDAR-системами. Важливо, що UWB-радари ефективно функціонують навіть у задимлених під час пожежі приміщеннях або зонах без освітлення, де оптичні камери повністю безсилі, що робить цю технологію безцінною для пошуку ізольованих людей під час катастроф у будівлях. Дослідження підтверджують, що гібридні системи комп’ютерного зору (на базі YOLO та RetinaNet) здатні швидко локалізувати постраждалих в умовах густого диму, а гібридні нейромережі типу GoogleNet-BiLSTM забезпечують точність розпізнавання підозрілої активності в реальному часі на периферійних пристроях.

Концепція «Аналізу шляхів атаки» (Attack Path Analysis, APA) традиційно застосовувалася в індустрії кібербезпеки для візуалізації та картування потенційних маршрутів латерального руху хакерів у хмарних середовищах та корпоративних мережах. Сьогодні ця потужна аналітична методологія успішно адаптується для потреб фізичної корпоративної безпеки.

Спираючись на дані телеметрії зі СКУД та камер, предиктивні системи алгоритмічно аналізують просторову топологію об’єкта, створюючи динамічні графи переміщень. Мета APA – виявити повну послідовність взаємопов’язаних прогалин у безпеці, вразливостей та неправильних конфігурацій доступу, які зловмисник може використати для просування від початкової точки входу до

так званих «коронних коштовностей» організації – серверних кімнат, сховищ даних або кабінетів топ-менеджменту.

Алгоритми штучного інтелекту встановлюють логічні базові маршрути для різних категорій персоналу. Якщо система фіксує відхилення від цих маркованих безпечних коридорів (наприклад, після ранкового входу через головне лобі співробітник відділу продажів замість свого робочого місця цілеспрямовано прямує до технічних або інженерних приміщень), це негайно класифікується як спроба розвідки або латерального фізичного переміщення. Такі інструменти як VisionAI автоматично відстежують рух уздовж визначених пішохідних шляхів, ідентифікують девіації та збирають доказову базу для навчання персоналу або ескалації інциденту.

Для предиктивної оцінки вразливості систем фізичного захисту (PPS – Physical Protection System) стратегічних об’єктів (наприклад, атомних електростанцій або дата-центрів) дедалі частіше застосовується складний багатошляховий аналіз на базі стохастичного методу Монте-Карло. Передові програмні симулятори, зокрема AVERT від компанії ARES Security та Simajin, дозволяють створювати повноцінні 3D-моделі будівель зі штучним інтелектом, який визначає маршрути персонажів, зони виявлення та ймовірності бойових зіткнень. Замість застарілого детермінованого підходу, який оцінював лише один передбачуваний шлях порушника (модель EASI), ці системи динамічно симулюють тисячі різноманітних векторів атак, що включають випадкові, приховані стратегії, стрімкі прориви та атаки з використанням найменш захищених шляхів. Алгоритм безперервно обчислює ймовірність переривання атаки силами охорони. При цьому критична точка виявлення не є статично закріпленою за певним турнікетом чи дверима, а динамічно зміщується в просторі залежно від змодельованого ШІ шляху зловмисника, що дозволяє генерувати найбільш реалістичні метрики вразливості та планувати превентивні заходи.

Впровадження передових ШІ-алгоритмів у діюче корпоративне середовище неминуче стикається із проблемою застарілої інфраструктури, яка фундаментально не була розроблена для підтримки сучасних API, мікросервісних хмарних архітектур чи інтенсивних процесів машинного навчання. Збереження цих систем обумовлене їхньою роллю у важливих бізнес-процесах, а їх повна та швидка заміна супроводжується величезними капітальними витратами та операційними ризиками.

Основні бар’єри на шляху предиктивної модернізації включають розрізненість даних, жорсткі формати БД, які не дозволяють експортувати метадані, та нестачу обчислювальної потужності на локальних об’єктах [97].

Монолітні архітектури додатків минулого унеможливлюють агрегацію даних у реальному часі, що є необхідним для предиктивної аналітики.

Для економічно доцільного вирішення цієї дилеми розроблено концепцію багаторівневих стратегій фазованого переходу. Замість радикального та ризикованого повного демонтажу старого та монтажу нового обладнання, підприємства активно застосовують проміжні програмні ШІ-шлюзи та апаратні мости.

Ці гібридні підходи дають змогу великим корпораціям розгортати сучасні алгоритми комп'ютерного зору, динамічне профілювання ризиків та поведінковий аналіз поверх старого Wiegand-обладнання, забезпечуючи плавний еволюційний перехід без зупинки безперервних бізнес-процесів.

Сучасний світовий ринок СКУД та відеоспостереження стрімко консолідується навколо закритих, але потужних платформних екосистем. Вони проектуються з метою глибокої інтеграції апаратних сенсорів із просунутими хмарними алгоритмами штучного інтелекту. Аналіз архітектур провідних виробників демонструє багатство стратегій впровадження предиктивної безпеки.

Одна з них – самонавчальна відеоаналітика та нейромережевий пошук Avigilon (Motorola Solutions) сфокусована на глибокій відеоаналітиці з інтенсивним використанням конволюційних нейромереж. Їхня флагманська технологія самонавчальної відеоаналітики Self-Learning Video Analytics здатна високоточно класифікувати різні типи об'єктів (люди або транспортні засоби) на значних відстанях і в складних погодних умовах, ефективно ігноруючи фоновий рух, який не є релевантним для безпеки (наприклад, коливання дерев чи дощ). Інноваційною є розробка функції Unusual Motion Detection. На відміну від традиційних детекторів руху, система безперервно вивчає, який рух є фоновим і типовим для даної сцени (наприклад, стандартний потік автомобілів на перехресті або напрямок руху людей на ескалаторі), і алгоритмічно підсвічує атипові траєкторії, такі як рух транспорту проти потоку, без жодного попереднього налаштування правил оператором.

Для розслідування складних інцидентів застосовується технологія Avigilon Appearance Search – просунута ШІ-пошукова система, преінстальована на мережевих відеореєстраторах. Вона дозволяє слідчим відстежити повний маршрут конкретної особи чи автомобіля через десятки розрізнених камер на великому об'єкті. Пошук здійснюється за фізичним описом, кольором чи типом одягу, статтю або обличчям. Візуальний інтерфейс Focus of Attention радикально змінює парадигму моніторингу – замість класичної «стіни з відеоекранами», яка виснажує увагу, оператор бачить абстрактну візуалізацію об'єкта, яка привертає його увагу виключно до тих зон, де ШІ зафіксував

аномалії, значно оптимізуючи когнітивне навантаження. Обробка потоків надвисокої роздільної здатності забезпечується запатентованою технологією оптимізації пропускної здатності High Definition Stream Management.

Інша стратегія предиктивної безпеки – Verkada впроваджує проактивне стримування (AI Deterrence) та багатокадрові детектори. Архітектура Verkada представляє повністю хмарно-орієнтований підхід, де відсутні локальні NVR-сервери, а запис і обчислення відбуваються гібридно – на самих камерах та у хмарі Command. Головний акцент робиться на автоматизоване алгоритмічне стримування загроз (AI-Powered Deterrence). Вбудовані в IP-камери та розумні інтеркоми потужні мікропроцесори не просто фіксують факт порушення для архіву, а вступають у пряму звукову взаємодію з об'єктом вторгнення.

При виявленні контекстуальної аномалії, наприклад, тиняння особи біля заднього входу складу в неробочий час, система автоматично активує багатокроковий робочий процес стримування.

Більше того, інженери компанії Verkada створили багатокадрові темпоральні моделі ШІ для розпізнавання специфічної кінематичної активності. На відміну від стандартних детекторів, що аналізують одиничний кадр, ці моделі здатні ідентифікувати складні дії в динаміці, такі як падіння людини на виробництві або спроби перелізти через високу огорожу периметра.

Інша компанія Genetec зі своєю відкритою архітектурною платформою Security Center зосереджується на оркестрації та об'єднанні даних. Інтелектуальний модуль Genetec Mission Control діє як центральна нервова система підприємства. Це передова система управління рішеннями, яка не генерує власні відеоаналітичні дані на камерах, а майстерно агрегує потоки даних з тисяч різноманітних датчиків, систем СКУД (зокрема, зчитувачів HID, LenelS2), систем відеоспостереження, ALPR-радарів (розпізнавання номерних знаків) та сенсорів Інтернету речей.

Місія предиктивних алгоритмів Genetec полягає у семантичному фільтруванні шуму. Вбудований рушій правил Rules Engine застосовує алгоритми кореляційного аналізу подій для кваліфікації інцидентів та відокремлення реальних багатофакторних загроз від ізольованих хибних тривог. Головною перевагою платформи є автоматизація стандартних операційних процедур. Наприклад, коли виникає складна послідовна аномалія (система контролю доступу зафіксувала серію відмов доступу + відеоаналітика зафіксувала скупчення людей + індустріальний датчик виявив різке падіння тиску), система Mission Control не просто видає сигнал тривоги. Натомість вона автоматично розгортає покроковий інтерактивний алгоритм дій для оператора на динамічній геоінформаційній карті, паралельно запускаючи фонові автоматизовані процеси відповіді – наприклад, блокування всіх дверей у

визначеному периметрі або надсилання автоматичних email-повідомлень ключовим інженерам.

У свою чергу, HID Global, визнаний світовий лідер у галузі довіреної ідентифікації та облікових даних, концентрує зусилля на глибокому аналізі взаємодій у корпоративному середовищі. Шляхом стратегічного злиття з Bluvision, провідним виробником рішень систем позиціонування в реальному часі (RTLS), компанія HID запровадила екосистему бейджів, оснащених сенсорними маяками Bluetooth. Інтеграція цих даних з платформою Humanyze Elements дозволяє компаніям зі списку Fortune 500 створювати надзвичайно детальні теплові карти переміщення працівників та аналізувати патерни їхньої соціальної колаборації. Додаткова інтеграція технології предиктивної аналітики Innominds iFusion у платформу HID SAFE Facility and Risk Analytics дає змогу обробляти дані з фізичних систем безпеки та історичних архівів доступу за допомогою алгоритмів машинного навчання. Це дозволяє не тільки здійснювати моніторинг заповнюваності приміщень у реальному часі, але й генерувати комплексні індекси ризику для окремих просторів або співробітників, висвітлюючи приховані поведінкові індикатори майбутніх порушень протоколів безпеки.

Створення надійного алгоритмічного прогнозу фізичної присутності людей у конкретних приміщеннях базується на математичному моделюванні. Широкого поширення для цих цілей набули моделі ланцюгів Маркова, які математично описують ймовірності переходу кімнати з одного стану (наприклад, «вільно») у діаметрально протилежний («зайнято») протягом визначеного часового вікна.

Ще однією революційною сферою застосування поведінкових даних зі СКУД та систем відстеження просторового розташування є розширена предиктивна аналітика управління людським капіталом. Корпоративні дані про переміщення, такі як частота ранніх приходів або пізніх затримань в офісі, тривалість перебування в зонах командної колаборації, частота та тривалість перерв, є цінними ранніми індикаторами емоційного стану співробітника.

Сучасні ШІ-моделі на базі нейромереж здатні аналізувати ці дані, щоб допомогти керівникам передбачити зниження залученості, професійне вигорання або високу ймовірність звільнення цінного працівника задовго до того, як це перетвориться на формальну кадрову проблему. Наприклад, компанія IBM розробила спеціалізоване ШІ-програмне забезпечення, яке, аналізуючи патерни корпоративної поведінки, здатне прогнозувати намір працівників покинути компанію з точністю у 96%. Такі інструменти машинного навчання також автоматично виявляють тонкі ознаки зниження «здоров’я команди» – зростання кількості нетипових відсутностей на робочому місці,

зменшення фізичної участі в колективних активностях у зонах відпочинку або загальне зниження динаміки переміщень, сигналізуючи про перехід працівника від статусу «надійного» до «емоційно відстороненого».

Однак впровадження такого всеохоплюючого алгоритмічного моніторингу за співробітниками створює глибокий соціально-етичний парадокс. З одного боку, дослідження корпоративних середовищ засвідчують, що автоматизовані підказки ШІ щодо оптимізації графіків роботи дозволяють знизити загальний рівень емоційного виснаження персоналу в середньому на 25%. З іншого боку, детальне опитування серед працівників Південної Кореї виявило, що постійне використання інструментів ШІ-моніторингу має різко негативний вплив на їхнє почуття психологічної безпеки в офісі, що парадоксальним чином робить таких співробітників значно більш схильними до розвитку професійної депресії та стресу. Це вимагає від архітекторів систем СКУД обережного впровадження аналітики, фокусуючись на агрегованих даних команди, а не на жорсткому індивідуальному мікроменеджменті.

Безпрецедентні можливості масштабного розгортання предиктивних систем безпеки та моніторингу простору неминуче стикаються з фундаментальними юридичними та регуляторними бар'єрами. Найбільш жорсткі обмеження диктують європейський Загальний регламент захисту даних (GDPR), Каліфорнійський закон про конфіденційність споживачів (CCPA) та Закон Південної Африки про захист персональної інформації (POPIA). Суть технологічної проблеми полягає в тому, що для коректного навчання алгоритмів МН потрібні величезні масиви чутливих персональних даних (біометричні шаблони обличчя, щоденні маршрути пересування будівлею, соціальні звички), що створює значні ризики так званого гіпернагляду та порушення права на недоторканність приватного життя. Судові прецеденти є суворими – німецька філія корпорації H&M була оштрафована наглядовими органами на 35,3 мільйона євро саме за використання інтенсивних програм постійного моніторингу співробітників, які порушували їхні громадянські права.

Особливим юридичним викликом для розробників предиктивних СКУД є жорсткі формулювання статті 22 регламенту GDPR. Ця стаття встановлює абсолютне право фізичної особи не підлягати рішенням, які ґрунтуються виключно на автоматизованій обробці даних, включаючи математичне профілювання, якщо таке рішення створює для цієї особи прямі правові наслідки або істотно на неї впливає.

Якщо система поведінкової аналітики на базі штучного інтелекту динамічно знижує рейтинг довіри співробітника через виявлені аномалії в його переміщеннях офісом і в результаті автоматично блокує йому доступ до

робочого комп’ютера або кабінету, європейські регулятори розглядають це як автоматизоване рішення з істотним впливом. Гучна судова практика Суду Європейського Союзу у справі німецького бюро кредитних історій SCHUFA (2023 рік) закріпила надзвичайно широке тлумачення цього правила. Суд постановив: якщо алгоритм самостійно генерує оцінку ризику, на основі якої фактично приймається фінальне рішення (наприклад, про допуск до роботи чи відмову у кредиті), це безпосередньо підпадає під дію Статті 22, навіть якщо на фінальному етапі людина-співробітник лише формально «штампує» згенерований комп’ютером висновок.

Отже, чинне законодавство категорично вимагає застосування архітектури «людина в контурі» для всіх серйозних рішень. Автоматизовані СКУД можуть обмежувати доступ або активувати алгоритми стримування лише як тимчасовий запобіжний захід. Остаточне рішення про статус безпеки співробітника повинно обов’язково передбачати прозорі процедури оскарження, отримання інформації про логіку прийняття рішення та можливість змістовного втручання живої людини-оператора. Хоча нові регіональні законопроекти, такі як очікуваний британський Data Use and Access Bill, можуть дещо спростити ці обмеження для рутинних бізнес-рішень, жорсткий захист біометричних шаблонів безумовно залишатиметься надсуворим. Згідно зі статтею 26 Федерального закону ФРН про захист даних, будь-який моніторинг співробітників дозволяється лише якщо він «об’єктивно необхідний для виконання трудових відносин», і роботодавець зобов’язаний вичерпно збалансувати власні інтереси з невід’ємними правами працівників, попередньо розглянувши менш інвазивні альтернативи.

8.2 Протидія методам соціальної інженерії та технічному злому

Безпека будь-якого об’єкта сьогодні залежить від здатності СКУД протидіяти двом основним векторам атак – соціальній інженерії, що маніпулює людським фактором, та технічному злому, який експлуатує вразливості апаратного та програмного забезпечення.

Соціальна інженерія у контексті СКУД визначається як сукупність психологічних та маніпулятивних технік, спрямованих на отримання несанкціонованого фізичного або логічного доступу шляхом експлуатації людських слабкостей, таких як довіра, ввічливість або страх [123]. На відміну від технічного зламу, соціальний інженер часто не потребує глибоких знань у програмуванні, покладаючись на ретельно розроблені сценарії взаємодії з персоналом.

Найбільш поширеними методами проникнення через точки проходу є tailgating (прохід «на плечах») та piggybacking. Аналіз поведінкових паттернів

свідчить, що ці методи базуються на соціальній нормі ввічливості. При tailgating зловмисник слідує за авторизованою особою без її відома, часто використовуючи моменти високої інтенсивності руху або технічні затримки у закритті дверей. Piggybacking, навпаки, передбачає певну форму соціальної взаємодії, де легітимний користувач добровільно притримує двері для сторонньої особи, сприймаючи її як колегу, кур'єра або відвідувача, який нібито має право на вхід [62].

Зловмисники часто використовують візуальні атрибути для легітимізації своєї присутності: уніформу технічного персоналу, важкі коробки в руках або підроблені посвідчення. У великих організаціях, де працівники не знають один одного особисто, такі методи демонструють надзвичайно високу ефективність. Протидія цим явищам вимагає впровадження як технічних засобів (шлюзових кабін, турнікетів повноростового типу), так і системних тренінгів для персоналу, що формують культуру «нульової довіри» на пунктах пропуску.

Pretexting є більш складною формою соціальної інженерії, де атака проводиться за заздалегідь підготовленим алгоритмом. Зловмисник створює фальшиву особистість (претекст), наприклад, представника IT-відділу, пожежного інспектора або аудитора, щоб отримати доступ до закритих зон або виманити конфіденційні дані, такі як паролі чи коди доступу. Протидія даному методу – впровадження процедури верифікації.

Особливою загрозою є метод Quid Pro Quo (послуга за послугу), коли зловмисник пропонує допомогу у вирішенні технічної проблеми, заманюючи жертву до надання віддаленого доступу або фізичного пропуску в серверне приміщення. Всі ці методи спрямовані на те, щоб змусити людину самостійно обійти встановлені бар'єри безпеки, та вимагають впровадження політик безпеки і контролю відвідувачів.

У свою чергу, технічний аспект зламу СКУД зосереджений на експлуатації слабкостей у методах передачі даних між ідентифікатором, зчитувачем та контролером. Значна частина сучасних об'єктів досі використовує технології, розроблені десятиліття тому, що робить їх легкими цілями для зловмисників.

Використання безконтактних карт, таких як HID Prox або EM-Marine з принципом відкритої трансляції свого серійного номера будь-якому зчитувачу, породило RFID-скіммінг – зчитування даних на відстані. У даному випадку зловмисник, перебуваючи на відстані кількох сантиметрів від жертви (наприклад, у ліфті чи черзі), може зчитати номер карти за допомогою портативного пристрою, такого як Flipper Zero або Proxmark3, і згодом клонувати його на порожню заготовку. Процес займає лічені секунди, а

отримана дублікат-карта сприймається системою як оригінальна, не залишаючи слідів зламу в журналах подій.

Для мінімізації ризиків технічного зламу критично важливою є міграція на сучасні стандарти, що забезпечують наскрізне шифрування даних від карти до сервера управління.

Чіпи серії MIFARE DESFire від компанії NXP представляють собою четверте покоління безконтактних смарт-карт, що базуються на відкритих глобальних стандартах безпеки. Версія EV3 впроваджує кілька інноваційних механізмів захисту, які роблять класичне клонування неможливим.

Ключовим нововведенням є функція Secure Unique NFC, яка генерує унікальний криптографічний код для кожного зчитування. Це означає, що навіть якщо зловмисник перехопить сигнал карти, він не зможе використати його повторно, оскільки кожна сесія вимагає нового динамічного підпису. Крім того, функція Transaction Timer у MIFARE DESFire EV3 дозволяє встановити жорсткий часовий ліміт на виконання транзакції. Це є прямою протидією релейним атакам, де затримка сигналу, спричинена пересилкою даних через інтернет або Bluetooth-подовжувачі, призведе до автоматичного скидання сесії картою.

З поширенням мобільних ідентифікаторів на базі NFC та Bluetooth Low Energy з’явилися нові типи атак, що поєднують методи соціальної інженерії та високотехнологічного перехоплення.

NFC-релейна атака полягає у дистанційній передачі сигналу від карти жертви до зчитувача за допомогою проміжних пристроїв. У 2023-2025 роках спостерігався сплеск атак з використанням ПЗ типу NFCGate, яке дозволяє двом смартфонам працювати як віртуальний подовжувач сигналу. Один зловмисник наближає смартфон до карти жертви (наприклад, у громадському транспорті), а другий у цей же час перебуває біля зчитувача на об’єкті. Дані карти передаються через інтернет у реальному часі, дозволяючи отримати доступ без фізичного володіння картою.

Протидія таким атакам базується на впровадженні функцій контролю близькості, інтегрованих у чіпи MIFARE DESFire EV2/EV3, та використанні багатофакторної автентифікації, де смартфон вимагає біометричного підтвердження або введення PIN-коду перед активацією передачі сигналу NFC.

Біометрична ідентифікація вирішує фундаментальну проблему традиційних СКУД: вона підтверджує особу, а не факт наявності карти. Це важливо для протидії передачі ідентифікаторів та методам соціальної інженерії.

Для особливо чутливих зон (серверні приміщення, сховища) рекомендується використання мультимодальної біометрії або поєднання біометрії з фізичним ідентифікатором. Це створює додатковий бар’єр – навіть

якщо зловмисник клонує карту і отримає фотографію працівника для обходу Face ID, йому буде значно складніше обійти систему, що вимагає одночасної верифікації за двома незалежними біологічними ознаками (наприклад, обличчя та судинний малюнок долоні).

Оскільки сучасні СКУД інтегровані в IT-інфраструктуру організації, вони стають об'єктами мережевих атак. Контролер доступу часто є «слабкою ланкою», через яку зловмисник може отримати доступ до корпоративної мережі або навпаки – скомпрометувати фізичну безпеку через мережу.

Найбільш критичним заходом мережевого захисту є ізоляція трафіку СКУД у окремий VLAN або використання фізично відокремленої мережі управління. Це запобігає «горизонтальному переміщенню» зловмисника, який міг отримати доступ до мережі через вразливу робочу станцію або Wi-Fi.

Для захисту даних у транзиті між сервером та контролерами необхідно використовувати протокол TLS v1.3. TLS v1.3 усуває підтримку застарілих шифрів та прискорює процес встановлення захищеного з'єднання (handshake), забезпечуючи при цьому «форвардну секретність» – стан, при якому компрометація поточного ключа не дозволяє розшифрувати дані минулих сесій.

Таким чином, тільки комплексний підхід дозволяє створити периметр безпеки, здатний витримати як витончені атаки професійних хакерів, так і винахідливі сценарії соціальних інженерів.

8.3 Керування життєвим циклом СКУД

СКУД сьогодні є складними мережевими архітектурами, що вимагають системного підходу до забезпечення їхньої якості протягом усього періоду експлуатації. Міжнародний стандарт ISO/IEC 25010, що входить до серії SQuaRE (System and Software Quality Requirements and Evaluation), надає вичерпну концептуальну базу для оцінки та керування якістю таких систем [60]. Цей стандарт став логічним розвитком стандарту ISO/IEC 9126, значно розширивши сферу охоплення за рахунок додавання таких критичних для сучасної інфраструктури характеристик, як захищеність та сумісність.

Впровадження ISO/IEC 25010 як основного інструменту керування життєвим циклом СКУД вимагає розуміння ширшого контексту серії ISO/IEC 25000 [56]. Ця серія стандартів була розроблена для створення уніфікованої мови між розробниками, замовниками та експертами з оцінки якості. Вона замінила попередні ітерації стандартів, які вважалися занадто вузькими для охоплення нових викликів, таких як хмарні обчислення та IoT. В Україні ці стандарти гармонізовані як національні нормативні документи, зокрема ДСТУ ISO/IEC 25010:2025 [106], який з 2025 року замінений оновленою редакцією, що відображає динаміку розвитку технологій.

Серія SQuaRE структурована за п’ятьма основними дивізіонами, кожен з яких забезпечує певний аспект життєвого циклу системи (табл. 8.1).

Таблиця 8.1 – Структура стандарту ISO/IEC 25010 серії SQuaRE [32]

Нормативний документ та серія	Назва та ключові завдання	Застосування в контексті СКУД
ISO/IEC 2500n	Керування якістю: визначає загальну термінологію, архітектурні моделі та посібники для користувачів	Створення стратегії якості на рівні організації, визначення ролей безпеки та відповідальності
ISO/IEC 2501n	Моделі якості: деталізує характеристики для програмних засобів, систем, даних та якості у використанні	Визначення конкретних вимог до надійності зчитувачів, захищеності протоколів та зручності інтерфейсу оператора
ISO/IEC 2502n	Вимірювання якості: містить математичні визначення метрик та практичні настанови щодо їх застосування	Розрахунок показників доступності системи, часу реакції на тривогу та частоти помилкових спрацювань (FAR/FRR)
ISO/IEC 2503n	Вимоги до якості: допомагає стейкхолдерам специфікувати очікування від продукту на етапі тендеру чи розробки	Формування технічного завдання, яке включає не лише функціонал, а й вимоги до підтримуваності та портативності
ISO/IEC 2504n	Оцінювання якості: регламентує процес проведення перевірок, аудитів та сертифікації	Проведення фінальних випробувань перед введенням СКУД в експлуатацію та періодичних аудитів безпеки

Ця структура забезпечує безперервність процесу: від ідентифікації потреб (2501n) через вимірювання (2502n) до фінальної оцінки відповідності (2504n).

Центральним елементом ISO/IEC 25010 є модель якості продукту, яка складається з восьми характеристик. Для систем безпеки ці характеристики не є рівнозначними; наприклад, захищеність та надійність часто мають вищий пріоритет, ніж портативність.

Функціональна придатність визначає, чи здатна система виконувати задекларовані завдання. У випадку СКУД це означає не лише здатність відкривати замок, а й коректне відпрацювання складної логіки доступу. Функціональна повнота вимагає, щоб система охоплювала всі сценарії, передбачені бізнес-процесами, такі як антипасбек, керування ліфтовими

кабінами або автоматизація шлюзових кабін. Функціональна коректність у біометричних СКУД стає критичною, оскільки точність розпізнавання обличчя або відбитків пальців безпосередньо впливає на рівень захисту об’єкта.

Надійність СКУД оцінюється за її здатністю підтримувати працездатність за заданих умов протягом визначеного часу. Зрілість системи вказує на її готовність до реальної експлуатації без частих програмних збоїв. Доступність є ключовим показником для систем 24/7. Для критичних інфраструктур цей показник часто розраховується як відношення середнього часу до відмови до суми цього часу та середнього часу відновлення.

Відмовостійкість СКУД зазвичай реалізується на рівні апаратної архітектури, коли контролери продовжують приймати рішення про доступ навіть у разі втрати зв’язку з центральним сервером.

У системах з великою кількістю точок доступу та користувачів ефективність продуктивності стає викликом. Часова поведінка вимірює затримку між прикладанням карти до зчитувача та спрацюванням виконавчого пристрою. Ресурсомісткість ПЗ СКУД на серверному рівні повинна бути оптимізована для забезпечення високої пропускної здатності бази даних подій, особливо в періоди пікових навантажень (наприклад, під час зміни на виробництві). Місткість системи повинна дозволяти масштабування без деградації часу відгуку.

Оскільки життєвий цикл СКУД може тривати 20 і більше років, підтримуваність стає фінансово визначальною характеристикою. Модульність дозволяє замінювати окремі зчитувачі або контролери без необхідності перепрограмування всієї системи. Аналізованість допомагає технічному персоналу швидко діагностувати причини відмов, використовуючи розвинені системи логування та діагностики.

Портативність у СКУД проявляється в здатності клієнтського ПЗ працювати на різних операційних системах (Windows, Linux, мобільні платформи) та адаптивності до змін апаратного середовища. Для хмарних СКУД це також включає легкість міграції між різними хмарними провайдерами без втрати даних.

Життєвий цикл СКУД проходить від ініціації до утилізації.

Керування СКУД за стандартами ISO/IEC 25010 вимагає інтеграції вимог до якості в кожен етап системного життєвого циклу. Традиційний підхід часто залишає тестування якості на кінець проекту, що призводить до виявлення критичних вразливостей занадто пізно.

Фаза 1: Концептуалізація та аналіз вимог. На цьому етапі визначаються цілі безпеки організації. Використання ISO/IEC 25010 дозволяє структурувати вимоги, які часто формулюються розмито. Замість вимоги «система має бути

надійною», стейкхолдери повинні вказувати конкретні показники доступності та відмовостійності. Аналіз ризиків на цій стадії допомагає визначити пріоритетність характеристик якості.

Фаза 2: Проектування та архітектурний дизайн. На основі вимог розробляється детальна специфікація. Важливо врахувати не лише функціональні вузли, а й механізми безпеки. «Безпечний життєвий цикл розробки» передбачає проведення аналізу архітектури на наявність вразливостей ще до написання коду. Для СКУД це етап вибору топології мережі (наприклад, використання VLAN для ізоляції трафіку безпеки) та протоколів зв'язку.

Фаза 3: Реалізація та розробка. Для розробників ПЗ СКУД якість коду оцінюється через метрики підтримуваності. Однією з найбільш поширених є цикломатична складність за Маккейбом, яка вимірює кількість лінійно незалежних шляхів у програмі. Високе значення цього показника свідчить про складність тестування та супроводу коду, що в майбутньому призведе до зростання витрат.

Фаза 4: Інтеграція та комплексне тестування. Тестування має бути багаторівневим. Окрім unit-тестів окремих модулів, проводяться навантажувальні тести для перевірки продуктивності та пенетраційні тести для перевірки захищеності. Для СКУД важливим є тестування сценаріїв відмови: наприклад, чи розблокуються двері з магнітними замками при зникненні живлення або спрацюванні пожежної тривоги.

Фаза 5: Впровадження та приймальні випробування. Розгортання системи може здійснюватися шляхом прямої заміни або паралельного запуску. Останній варіант є більш безпечним для діючих об'єктів, оскільки дозволяє перевірити точність перенесення прав доступу. На цьому етапі проводиться навчання персоналу, що впливає на характеристику «Придатність до використання» (Usability).

Фаза 6: Експлуатація та технічне обслуговування. Це найтриваліший етап, що включає моніторинг продуктивності, оновлення прошивок та патчі безпеки. Керування конфігураціями дозволяє відстежувати всі зміни в налаштуваннях системи, що є критичним для розслідування інцидентів.

Фаза 7: Модернізація та виведення з експлуатації. Коли система досягає кінця свого життєвого циклу, необхідно спланувати безпечну утилізацію даних та обладнання. Важливо забезпечити повне видалення персональних даних перед фізичним знищенням або перепродажем апаратних компонентів.

СКУД – це довгострокова інвестиція, але електронні компоненти мають короткий цикл життя. Керування застаріванням є частиною стратегії

підтримуваності за ISO/IEC 25010 і спрямоване на мінімізацію ризиків, пов'язаних з припиненням випуску запчастин або підтримки ПЗ.

Для об'єктивної оцінки СКУД необхідно використовувати кількісні метрики, визначені в дивізіоні ISO/IEC 2502n. Проект Quamoco пропонує використовувати ієрархічні моделі, де якісні аспекти розбиваються на вимірювані фактори.

Для оцінки зовнішніх тривожних систем (включаючи СКУД) використовуються статистичні методи валідації. Наприклад, внутрішня узгодженість моделі оцінки вимірюється за допомогою альфа Кронбаха, де значення вище 0,7 свідчить про високу надійність результатів оцінювання.

Для хмарних СКУД ключовими показниками ефективності (KPI) є:

– MTTD (Mean Time to Detect) – середній час виявлення несанкціонованого доступу або технічної несправності;

– False Positive Rate – частота помилкових блокувань легітимних користувачів, що безпосередньо впливає на задоволеність користувачів;

– Latency – затримка, яку вносять засоби безпеки (наприклад, шифрування або VPN) у процес аутентифікації.

Впровадження ISO/IEC 25010 має значний економічний ефект. Хоча розробка та впровадження системи з високими показниками якості вимагає більших початкових інвестицій, це призводить до суттєвого зниження операційних витрат протягом життєвого циклу.

Система з високим рівнем підтримуваності та портативності дозволяє:

– зменшити витрати на навчання персоналу завдяки інтуїтивному інтерфейсу;

– мінімізувати втрати від простоїв та інцидентів безпеки завдяки високій надійності та захищеності;

– знизити вартість майбутніх модернізацій завдяки модульній архітектурі та використанню відкритих протоколів.

У контексті муніципальних програм, таких як «Безпечне місто», СКУД повинні відповідати вимогам доступності для маломобільних груп населення. Це включає відповідну висоту встановлення зчитувачів, дублювання інформації шрифтом Брайля та забезпечення безперешкодного доступу для осіб з інвалідністю. В моделі ISO/IEC 25010 це підпадає під характеристику «Доступність».

Таким чином, керування життєвим циклом СКУД на основі ISO/IEC 25010 є необхідною умовою для створення стійкої інфраструктури безпеки. Стандарт забезпечує системний підхід, який дозволяє збалансувати технічні можливості, вимоги безпеки та економічну доцільність.

Для успішного керування СКУД рекомендується:

– на етапі ініціації чітко специфікувати вимоги до всіх восьми характеристик якості, уникаючи загальних фраз та фокусуючись на вимірюваних KPI;

– на етапі проектування віддавати перевагу відкритим протоколам (OSDP, ONVIF) та модульній архітектурі для забезпечення довгострокової сумісності та підтримуваності;

– протягом експлуатації впровадити систему постійного моніторингу метрик надійності та захищеності, а також регулярно проводити аудити застарівання компонентів;

– у контексті цифровізації активно використовувати можливості хмарних технологій та мікросервісів, одночасно посилюючи заходи з кібербезпеки та контролю цілісності даних.

Застосування моделі якості SQuaRE перетворює СКУД з простого інструменту обмеження доступу на інтелектуальний актив, здатний адаптуватися до мінливих загроз та технологічних трендів протягом десятиліть.

Контрольні запитання

1. Вкажіть на різницю, на прикладі біометричних систем доступу, між функціональною повнотою та функціональною коректністю?
2. З якими основними викликами зіштовхуєтьься розгортання масштабних моделей машинного навчання у системах безпеки?
3. Назвіть вектори атак на сучасні СКУД.
4. Назвіть ключові KPI для оцінки ефективності хмарних СКУД.
5. Назвіть механізми захисту ідентифікаторів від клонування?
6. Опишіть механізм NFC-релейної атаки.
7. Опишіть структуру серії SQuaRE (ISO/IEC 25000).
8. У чому полягає різниця між методами проникнення tailgating та piggybacking? Яку соціальну норму покладено в їх основу?
9. У чому полягає суть атак типу RFID-скіммінг?
10. У чому полягає фундаментальна зміна парадигми при переході від традиційних СКУД до систем предиктивної безпеки?
11. Чому для критичної інфраструктури рекомендованою є мультимодальна біометрія?
12. Чому для СКУД захищеність та надійність вважається пріоритетнішим за портативність?
13. Що являє собою «претекстинг» у контексті СКУД? Які заходи допомагають ефективно протидіяти цьому методу?
14. Як впровадження динамічного скорингу ризиків впливає на проблему «втоми від сповіщень»?

15. Як характеристика «підтримуваність» впливає на фінансову складову експлуатації СКУД?

16. Яка різниця між контекстуальними та послідовними аномаліями у контексті фізичної безпеки?

17. Яким чином метод "послуга за послугу" дозволяє зловмисникам обійти фізичні бар'єри безпеки?

18. Які ключові зміни, у контексті сучасних інфраструктур, відбулися під час переходу від стандарту ISO/IEC 9126 до ISO/IEC 25010?

19. Які мережеві заходи безпеки є критичноважливими для захисту інтегрованої IT-інфраструктури СКУД?

20. Які особливості впровадження СКУД у межах муніципальних програм?

21. Які переваги надає використання Secure SDLC на етапі проектування архітектури СКУД?

22. Яку роль відіграють технології периферійних обчислень та UWB-радари в сучасних архітектурах безпеки?

23. Яку фундаментальну проблему традиційних СКУД вирішує біометрична ідентифікація?

РОЗДІЛ 9. Проєктування та практична реалізація СКУД

9.1 Огляд об’єкта доступу та формування технічного завдання на проєктування СКУД

Процес створення сучасної СКУД на будь-якому об’єкті – від невеликого офісу до промислового гіганта – починається не з вибору обладнання, а з аналітичного огляду об’єкта та формування технічного завдання. Цей етап є основою, на якій будується вся подальша безпека та ефективність експлуатації. Під час обстеження необхідно акцентувати увагу на характеристиках значущості приміщень об’єкта, його будівельні та архітектурно-планувальні рішення, умови експлуатації, режими роботи, обмеження або, навпаки, розширення права доступу окремих суб’єктів доступу, параметри встановлених (або передбачених для встановлення на цьому об’єкті) пристроїв, які входять до складу СКУД. За результатами обстеження, зазвичай, визначають тактичні характеристики та структуру СКУД, технічні характеристики її компонентів, а також формується технічне завдання на обладнання об’єкта СКУД.

Українське законодавство та система технічного регулювання за останні роки пройшли шлях значної гармонізації з європейськими нормами. Основним документом, що визначає вимоги до проектування та функціонування таких систем, є ДСТУ EN 60839-11-1:2016 «Системи тривожної сигналізації.

Частина 11-1. Системи контролю доступу. Вимоги до систем та компонентів» [97]. Цей стандарт прийшов на зміну застарілим нормам і впровадив поняття ступенів безпеки, які дозволяють точно класифікувати рівень захисту об’єкта залежно від потенційних ризиків.

Стандарт ДСТУ EN 60839-11-1 охоплює не лише технічні характеристики компонентів, а й вимоги до ведення журналів подій, методів ідентифікації та контролю інформаційних потоків. Важливо розуміти, що відповідність цьому стандарту є обов’язковою для об'єктів критичної інфраструктури, банківських установ та державних підприємств. Окрім профільного стандарту, при проектуванні необхідно враховувати загальні умови експлуатації, визначено й в інших нормативних докементах, які стосуються кліматичних впливів та стійкості до агресивних середовищ.

Вибір ступеня безпеки визначає архітектуру системи та тип використовуваного обладнання. У таблиці 1.1 розділу 1 наведено характеристика різних ступенів безпеки, що дозволяє замовнику та проектувальнику знайти оптимальний баланс між вартістю та захищеністю.

Кожен ступінь безпеки висуває свої вимоги до часу автономної роботи, стійкості до зовнішніх впливів та ступеня захисту оболонок. Це безпосередньо впливає на вибір місць розташування обладнання, що повинно враховувати вплив виробничо-технологічних процесів, електромагнітних перешкод від вентиляційних та нагрівальних приладів, а також інтенсивність транспортного потоку поблизу точок проходу.

Обстеження об’єкта – це важливий етап, який не може бути замінений лише роботою з кресленниками [118]. Методичні рекомендації чітко вказують на неприпустимість проведення обстеження виключно за фотографіями чи відеозаписами без безпосереднього візуального огляду. Процес обстеження поділяється на кілька стадій: підготовку, попереднє (візуальне) обстеження та основне (детальне) обстеження.

На етапі підготовки здійснюється аналіз існуючої архітектурно-планувальної документації. Під час візуального огляду інженер повинен приділити особливу увагу пошкодженням конструкцій, які можуть свідчити про перевантаження або порушення граничних станів, оскільки це може вплинути на надійність монтажу дверних дотягувачів та замків. Також аналізуються структурні пошкодження, що могли виникнути внаслідок дії високих температур, що особливо важливо для протипожежних дверей.

Під час огляду формується розуміння зон доступу. Територія об’єкта повинна бути чітко розмежована на зовнішню (неконтрольовану) та внутрішню (захищену) зони. Це диктує логіку встановлення контролерів: вони обов’язково

повинні розташовуватися зсередини захищеної території, щоб запобігти фізичному втручанню в систему або саботажу.

На етапі детального обстеження кожна точка проходу (двері, ворота, турнікет) має бути оцінена за наступними критеріями:

– тип та матеріал конструкції (метал, дерево, скло), що визначає вибір замка (електромагнітний, електромеханічний або ригельний);

– напрямок відкривання дверей та інтенсивність потоку людей;

– наявність та стан евакуаційних шляхів;

– наявність інженерних мереж (живлення, комп'ютерна мережа) поблизу точки проходу.

За результатами попереднього обстеження складається проміжний звіт, що містить попередні висновки про технічний стан систем об'єкта. У підсумку формується паспорт об'єкта, який стає базою для розробки технічного завдання.

Технічне завдання (ТЗ) є юридичним та технічним документом, що фіксує вимоги замовника та зобов'язання проектувальника. В Україні структура ТЗ регламентується ДСТУ 3973-2000 [86] та ДСТУ 2850-94 [82]. Згідно з цими стандартами, ТЗ на розробку системи повинно містити розділи, що охоплюють підставу для виконання робіт, мету, вихідні дані та технічні вимоги.

На основі кращих практик та аналізу вимог до сучасних систем, ТЗ на СКУД повинно включати наступні блоки:

1. Загальні відомості (найменування об'єкта, замовника та виконавця, підстава для проектування).

2. Призначення та цілі створення системи (опис функцій, таких як розмежування доступу, облік робочого часу, фіксація пересування транспорту та ідентифікація номерних знаків).

3. Характеристика об'єкта (опис точок проходу, зон доступу та умов експлуатації).

4. Вимоги до системи в цілому (ступінь безпеки (рівень Grade), вимоги до надійності, електромагнітної сумісності та стійкості до зовнішніх впливів).

5. Вимоги до функцій, що виконуються системою:

– режим автентифікації та контролю доступу (відбитки пальців, обличчя, карти, коди);

– режим обліку робочого часу (фіксація приходу/відходу, статистика запізнень);

– управління виконавчими пристроями (замками, турнікетами, шлагбаумами).

6. Вимоги до видів забезпечення:

– програмне забезпечення (редагування бази персоналу, моніторинг подій у реальному часі, генерація звітів, хмарне управління);

– інформаційне забезпечення (вимоги до бази даних, шифрування та зберігання архівів);

– технічне забезпечення (специфікації контролерів, зчитувачів та засобів ідентифікації).

7. Вимоги до інтеграції (взаємодія з іншими охоронними інформаційними системами – відеоспостереженням та охоронно-пожежною сигналізацією).

Всі ці етапи створення ТЗ пояснює схема, яку подано на рисунку 9.1.

Рисунок 9.1 – Структурна схема створення технічного завдання

Важливо, щоб ТЗ враховувало кількість співробітників та відвідувачів, а також специфіку бізнес-процесів компанії. Наприклад, для режимних об’єктів силові лінії керування замками повинні бути захищені з внутрішньої сторони, щоб унеможливити відкриття дверей шляхом короткого замикання кабелів із зовнішнього боку.

9.1.1 Архітектурно-планувальні й будівельні рішення

Шляхом вивчення кресленників, обходу та огляду об’єкта, а також проведення необхідних замірів визначають:

– кількість входів/виходів та їх геометричні розміри (площа, лінійні розміри, пропускна здатність);

– матеріал будівельних конструкцій;

– кількість окремих будинків та число їх поверхів;

– кількість відкритих майданчиків;

– розташування опалювальних й неопалюваних приміщень і їх кількість.

9.1.2 Умови експлуатації

Шкідливий вплив навколишнього середовища необхідно враховувати лише для виконавчих пристроїв, зчитувачів та контролерів, які застосовують у приміщеннях де немає опалення або працюють за особливих умов (підвищена вологість, мінусові температури тощо).

Для надійної роботи СКУД, у межах об’єкта захисту, доцільно враховувати вплив електромагнітних перешкод, перепади напруги живлення, віддаленість зчитувачів та контролерів від керуючого центру, заземлення складових частин системи.

9.1.3 Інтегровані системи охорони

На сьогодні, будь-який великий та особливо важливий об’єкт володіє усім набором технічних засобів безпеки. Різноманіття цих систем на одному об’єкті призводить до неефективності їх роботи й труднощів, які пов’язані з їх управлінням та обслуговуванням.

Питання безпеки людей у разі виникнення надзвичайних ситуацій є пріоритетним при проектуванні СКУД. Згідно з ДБН В.2.5-56:2014 [77], СКУД повинна бути інтегрована з системою пожежної сигналізації.

Існує два основних правила, яких необхідно неухильно дотримуватися при монтажі СКУД на шляхах евакуації – виключити несанкціонований доступ у звичайному режимі та забезпечити безперешкодне розблокування всіх замків для евакуації людей при пожежі.

Згідно з нормами проектування, передбачаються такі механізми розблокування:

– автоматичне розблокування (при надходженні сигналу «Пожежа» від пожежної централі (ППКП) живлення електромагнітних або електромеханічних замків має вимикатися автоматично);

– дистанційне розблокування (оператор на посту охорони повинен мати можливість відкрити всі двері одним натисканням кнопки або через інтерфейс програмного забезпечення);

– механічне розблокування (біля кожного виходу, обладнаного СКУД, обов’язково встановлюється сертифікована кнопка аварійного відкривання дверей, яка розриває ланцюг живлення замка фізично).

Особливі обмеження накладаються на приміщення з великим скупченням людей. Наприклад, якщо в приміщенні перебуває понад 50 осіб, воно повинно мати не менше двох евакуаційних шляхів, а двері не можуть відкриватися всередину, якщо кількість присутніх перевищує 15 осіб. Найкращим рішенням для евакуаційних виходів є встановлення протипожежних дверей із системами

«антипаніка» – спеціальними штангами, які дозволяють відкрити двері простим натисканням тіла.

Об’єднання усіх систем в єдиний програмно-апаратний комплекс із загальним інформаційним середовищем та єдиною базою даних дозволяє:

1. Мінімізувати капітальні витрати на оснащення об’єкта. Апаратна частина скорочується за рахунок виключення дублюючої апаратури (до уваги беруть усі системи, які призначені для об’єднання в одне ціле) та із-за збільшення ефективності роботи кожної із них.

2. На основі повної та об’єктивної інформації, яка надходить оператору, значно скорочується час на прийняття відповідних рішень (припинення несанкціонованого проникнення, проходу або інших надзвичайних ситуацій, які відбуваються в зоні або об’єкті захисту);

3. Оптимізувати необхідну кількість постів охорони (знизити витрати на їх утримання) та зменшити вплив суб’єктивного людського чинника;

4. Чітко розмежувати права доступу (свої та сторонні СД) до приміщень, які охороняються, з отриманням відповідної інформації;

5. Автоматизувати процеси взяття/зняття приміщень під/з охорони, увімкнення камер спостереження, контролю шлейфів охоронно-пожежної сигналізації.

При створенні інтегрованої системи охорони (ІСО) необхідно враховувати:

– можливість спільної синхронізації усіх складових її пристроїв;

– можливість інтеграції наявних пристроїв як на програмному, так і апаратному рівнях;

– можливість організації ліній зв’язку стандартних інтерфейсів RS 485 та RS 232 (за умови значної відстані між пультами системи сигналізації та управління доступом).

СКУД – це енергозалежна система, і її працездатність під час відключення основного живлення є критичною. Проектування повинно включати розрахунок джерел безперебійного живлення та ємності акумуляторів.

Проектування СКУД – це складний багатогранний процес, успіх якого залежить від якості проведення огляду об’єкта та точності формулювання технічного завдання. Системний підхід дозволяє перетворити СКУД з витратної частини бюджету на інструмент підвищення ефективності бізнесу.

Чітке структурування вимог згідно з ДСТУ 3973-2000 дозволяє уникнути конфліктів між замовником та підрядником і гарантує отримання системи з необхідним функціоналом.

9.2 Вибір обладнання за категорією об’єкта

Вибір засобів ідентифікації безпосередньо впливає на рівень безпеки та пропускну здатність точок проходу. Сучасні системи пропонують широкий спектр технологій (табл. 9.1).

Таблиця 9.1 – Вибір типів ідентифікаторів СКУД залежно від об’єкта доступу

Тип ідентифікації	Опис технології	Об’єкт доступу	Переваги та особливості
Біометрія	Відбиток пальця, геометрія обличчя, малюнок вен, райдужна оболонка ока	Режимні об’єкти, банківські сховища	Найнадійніший метод; неможливо втратити чи передати
RFID-карти/брелоки	EM-Marine, Mifare, HID (безконтактні)	Офіси, промислові підприємства	Висока швидкість зчитування, низька вартість карт
Мобільний доступ	NFC, Bluetooth (смартфон як ключ)	Сучасні бізнес центри, коворкінги	Зручність; смартфон завжди у користувача
Кодова клавіатура	Введення цифрового пароля	Допоміжні приміщення	Відсутність потреби у фізичних носіях
Розпізнавання номерів	Відеоаналіз автомобільних номерів	Парковки, логістичні центри	Автоматизація в’їзду без зупинки авто

При виборі біометричних систем необхідно враховувати режим роботи: автономний (система працює на одній точці проходу) або мережевий (пристрої об’єднані для централізованого керування). Комбіновані режими, де для доступу вимагається і карта, і відбиток пальця, значно підвищують рівень безпеки та відповідають вимогам Grade 3 та 4.

Виконавчі пристрої повинні відповідати типу точки проходу [3, 69, 74]. Для пішохідних зон це можуть бути турнікети-триподи, роторні турнікети або автоматичні хвіртки. Для автотранспорту – шлагбауми, автоматичні ворота або болларди. Окрему увагу слід приділити дверній автоматиці та дотягувачам, які забезпечують гарантоване закриття дверей після проходу.

Процес ідентифікації та віднесення об’єктів до критичної інфраструктури в Україні регламентується Законом України «Про критичну інфраструктуру» [107] та постановою Кабінету Міністрів України №1109 від 9 жовтня 2020 року [128]. Категоризація є необхідним механізмом для мінімізації витрат

суб’єктами господарювання на заходи з кіберзахисту та фізичної безпеки, оскільки вона дозволяє визначити оптимальну модель захисту, адекватну потенційним ризикам. Стан захищеності об’єкта критичної інфраструктури визначається як стан, за якого забезпечується його функціональність, безперервність роботи та спроможність надавати основні послуги населенню.

Методика категоризації базується на узагальненій нормованій оцінці рівня критичності об’єкта (POKI), яка розраховується на основі секторальних та міжсекторальних критеріїв (табл. 9.2). Ці критерії враховують соціальну значущість (кількість постраждалого населення), суспільну значущість (вплив на надання послуг), економічну значущість (обсяг збитків) та значущість для національної безпеки і обороноздатності країни.

Таблиця 9.2 – Категоризація критичності об’єктів доступу

Категорія критичності	Опис об’єкта та його значення	Нормована оцінка
I категорія	Особливо важливі об’єкти державного значення	$0,8 < POKI \leq 1$
II категорія	Життєво важливі об’єкти регіонального значення	$0,63 < POKI \leq 0,8$
III категорія	Важливі об’єкти галузевого або місцевого значення	$0,37 < POKI \leq 0,63$
IV категорія	Об’єкти місцевого значення з обмеженим впливом	$0,2 < POKI \leq 0,37$

Рішення щодо віднесення об’єкта до певної категорії приймається робочими групами в уповноважених органах державної влади. Це рішення безпосередньо впливає на ТЗ до СКУД, оскільки для об’єктів I та II категорій вимоги до кіберзахисту та фізичної надійності є максимально суворими, що часто потребує погодження ТЗ з Адміністрацією Держспецзв’язку.

На об’єктах I категорії критичності управління ризиками безпеки спрямоване на запобігання інцидентам та мінімізацію наслідків, що вимагає встановлення чітких лімітів ризику. В контексті СКУД це означає впровадження дублюючих контролерів, резервованих ліній зв’язку та систем безперебійного живлення, здатних підтримувати роботу системи протягом 24 … 48 годин.

Для об’єктів критичної інфраструктури I-II категорій обов’язковим є використання обладнання Grade 3 або Grade 4. Це передбачає обов’язковий моніторинг стану всіх компонентів системи, шифрування протоколів передачі даних та використання багатофакторної аутентифікації.

На об’єктах критичної інфраструктури та великих підприємствах (I-III

категорії) застосовуються виключно мережеві контролери. Переваги мережевої архітектури полягають у можливості централізованого управління, моніторингу подій у реальному часі та гнучкому налаштуванні часових зон і рівнів доступу.

Для об’єктів IV категорії критичності або малих офісів можуть застосовуватися автономні контролери, інтегровані зі зчитувачем. Вони є економічно вигідними та простими в установці, проте мають суттєві обмеження: відсутність централізованого журналу подій та складність при необхідності масової зміни прав доступу. Ринок України представлений брендами Dahua, Hikvision, ZKTeco та вітчизняними рішеннями, що дозволяє підібрати обладнання за критерієм «ціна-якість».

Впровадження мобільних ідентифікаторів (смартфон замість карти) є трендом 2024-2025 років для бізнес-центрів та офісів III категорії.

Для об’єктів критичної інфраструктури мобільний доступ може використовуватися лише як допоміжний фактор або для доступу в зони з низьким рівнем ризику, тоді як для режимних приміщень пріоритет залишається за фізичними смарт-картами з високим ступенем апаратного захисту.

Виконавчі механізми (турнікети, шлюзові кабіни, шлагбауми) обираються залежно від необхідної пропускної здатності та рівня фізичного захисту об’єкта (табл. 9.3).

Таблиця 9.3 – Вибір виконавчих механізмів за інтенсивністю потоку

Тип турнікета	Пропускна здатність (осіб/хв)	Рівень безпеки	Сфери застосування
Трипод	25-30	Середній	Навчальні заклади, прохідні заводів
Швидкісний прохід	40-60	Високий	Бізнес центри, міністерства, аеропорти
Повноростовий	15-20	Найвищий	Військові об’єкти, АЕС, периметр підприємств
Шлюзова кабіна	2-5	Максимальний	Банківські сховища, секретні об’єкти

Повноростові турнікети виключають можливість перестрибування або пролізання під ними, що робить їх ідеальними для зовнішнього периметра об’єктів I-II категорій. Вони часто виготовляються з нержавіючої сталі для захисту від корозії в умовах відкритого повітря.

Для об’єктів, де важлива інклюзивність (наприклад, лікарні чи державні установи), обов’язковим є встановлення широких проходів шириною

900 … 1200 мм для вільного проїзду інвалідних візків та пронесення великогабаритних речей.

Таким чином, для об’єктів I та II категорій (особливо важливих та життєво важливих) вибір повинен бути зосереджений на обладнанні найвищого класу надійності (Grade 3 або 4), використанні захищеного протоколу OSDP та багатофакторної біометричної ідентифікації. Для об’єктів III та IV категорій допускається використання гнучких мережевих рішень з акцентом на мобільний доступ та хмарні технології, що дозволяє оптимізувати витрати без критичної втрати функціональності.

9.2.1 Вимоги, яким мають відповідати виконавчі пристрої

Виконавчі пристрої, під час подачі від контролера керуючого сигналу, повинні забезпечувати відкриття/закриття запірного механізму або загороджувального пристрою та володіти, при цьому, необхідною пропускною здатністю. Параметри керуючого сигналу (напруга, струм і тривалість) зазвичай узгоджуються, за конкретним видом загороджувальних пристроїв, із нормативними документами.

Рекомендованою величиною напруги живлення є +12 В або +24 В, однак для деяких видів приводів виконавчих пристроїв (ворота, масивні двері, шлагбауми) допускається використання електроживлення від мережі ~220/380 В. При цьому умисне пошкодження зовнішнього електричного ланцюга не повинно призводити до відкривання загороджувального пристрою.

У випадку зникнення електроживлення в системі має бути передбачено як наявність резервного джерела струму для живлення виконавчих пристроїв, так і механічне аварійне відкривання загороджувальних пристроїв. Слід пам’ятати, що аварійна система відкриття має бути захищеною від можливості використання її для несанкціонованого проникнення.

Ще одним питанням на яке необхідно звернути увагу – це захист виконавчих пристроїв від шкідливого впливу, який спричиняють зовнішні чинники (електромагнітні поля, статична електрика, нестабільна напруга живлення, пил, вологість, температура) та вандалізму.

Під час вибору доводчиків необхідно враховувати навантаження (вагу) загороджувального пристрою та кількість його циклів відкриття/закриття (цей параметр зазначають в технічних характеристиках на виріб).

9.2.2 Вимоги, яким мають відповідати пристрої ідентифікації доступу

Зчитувачі, перш за все, повинні забезпечувати надійне зчитування ідентифікаційної ознаки із ідентифікатора, перетворення його в електричний сигнал та його передачу на контролер.

Зазвичай, зчитувачі захищають від радіочастотного сканування та різноманітних маніпулювань, які пов’язані із перебором та підбором коду.

Під час введення невірного коду зчитувач блокується на певний час (цей параметр зазначають в технічних характеристиках на виріб). Час блокування вибирають таким чином, щоб забезпечити необхідну пропускну здатність під час обмеженого числа спроб підбору. За умови введення трьох хибних спроб коду має видаватися сигнал тривоги. Для систем, які працюють в автономному режимі, тривожний сигнал передається на звуковий/світловий оповіщувач, а для систем, які працюють від мережі електричного живлення – на центральний пульт із можливістю дублювання звуковим/світловим оповіщувачем. Зауважимо, що тривожний сигнал системи має видаватись під час будь-якого акту вандалізму.

Конструкція, зовнішній вигляд та надписи які наносять на ідентифікатор або зчитувач не повинні розкривати таємність коду.

Аналогічно як і для виконавчих пристроїв, до пристрої ідентифікації також висувають певні вимоги, які пов’язані із захистом від шкідливих впливів, які формують зовнішні чинники, та вандалізму.

Зауважимо, що ідентифікатори повинні бути захищеними від підробки та копіювання. Виробник повинен гарантувати, що будь-який код ідентифікатора не повторюється, в протилежному випадку – вказує умови повторюваності коду та заходи щодо запобігання використання ідентифікаторів з однаковими кодами.

У технічних характеристиках, на конкретні види ідентифікаторів, вказують мінімум кодових комбінацій.

Для автономних систем, за мірою необхідності, суб’єкт доступу має мати можливість змінити або перевстановити код (не менше 100 разів). При цьому, зміна коду повинна бути можливою лише після введення чинного коду.

Під час вибору ідентифікаторів необхідно звернути увагу на те, що клавіатура забезпечує низький рівень безпеки, магнітні картки – середній, Proximity, Wiegand-картки та електронні ключі типу «Touch Memory» – високий, а біометричні – дуже високий рівень безпеки.

9.2.3 Вимоги, яким мають відповідати пристрої контролю та управління доступом

Контролери, які працюють в умовах автономного режиму, повинні забезпечувати прийом інформації від зчитувачів, її обробку та генерування сигналів управління, які надходять у виконавчі пристрої.

Контролери, які ж працюють від мережі змінного струму, повинні забезпечувати:

– обмін інформацією, за лінією зв’язку, між контролерами та керуючим комп’ютером або провідним контролером;

– збереження пам’яті, налаштувань і кодів ідентифікаторів під час втрати зв’язку з керуючим комп’ютером (контролером), відключення живлення та переході на резервне живлення;

– контроль ліній зв’язку між окремими контролерами та між контролерами й керуючим комп’ютером.

У тому випадку, коли не застосовуються модеми або помножувачі, то відстань між окремими компонентами СКУД, для гарантованої її роботи, не повинна перевищувати зазначеної у технічних характеристиках довжини.

Слід пам’ятати, що протоколи обміну інформацією та інтерфейси, які застосовуються у СКУД повинні бути стандартних типів. При цьому, види і параметри інтерфейсів повинні відповідати нормативним документам на них із врахуванням загальних вимог ДСТУ 2373-94 (Інтерфейс послідовний радіального типу для автоматизованих систем управління роззосередженими об’єктами. Загальні вимоги).

Рекомендовані типи інтерфейсів:

– RS 485 – між контролерами;

– RS 232 – між контролерами та керуючим комп’ютером.

За допомогою програмного забезпечення здійснюється:

– ініціалізація ідентифікаторів (занесення кодів ідентифікаторів в пам’ять системи);

– задавання характеристик контрольованих точок;

– установка тимчасових інтервалів доступу (вікон часу);

– установка рівнів доступу для користувачів;

– протоколювання поточних подій;

– ведення баз даних;

– збереження даних та встановлень під час аварій та збоїв в системі.

У свою чергу програмне забезпечення повинне бути стійким до випадкових та навмисних впливів (відключення керуючого комп’ютера; програмного скидання керуючого комп’ютера; апаратного скидання керуючого комп’ютера; випадкове натискання кнопок клавіатури; випадковий перебір пунктів меню програми).

Працездатність системи й збереження у ній даних, повинна зберігатись як після її перезапуску, так і під час дії на неї випадкових та навмисних впливів. Ці дії не повинні впливати на відкривання загороджувальних пристроїв і зміну діючих кодів доступу.

Слід пам’ятати, що будь яке програмне забезпечення, яке використовується в СКУД, має бути захищеним від навмисних впливів, які здійснюються з метою зміни налаштувань системи. Вид та ступінь захисту встановлюються в технічних умовах на види засобів або системи в цілому. При

цьому, відомості, які наводяться у технічній документації, не впливають на секретність захисту.

Програмне забезпечення, за необхідності, має бути захищеним від несанкціонованого копіювання. Стійкість ПЗ до захисту від несанкціонованого доступу здійснюється за допомогою паролів (кількість рівнів доступу за паролями має бути не менше трьох).

Рекомендовані рівні доступу за типом суб'єктів доступу:

– адміністратор – доступ до усіх функцій контролю а доступу;
– оператор – доступ лише до функцій поточного контролю;
– системний – доступ до функцій конфігурації програмного забезпечення без доступу до функцій, які забезпечують управління виконавчих пристроїв.

Зауважимо, що під час введення пароля на екрані дисплея не повинні відображатися знаки, а число символів пароля має бути не менше п'яти.

9.2.4 Вимоги, яким має відповідати електроживлення

Основне електричне живлення СКУД здійснюється від мережі змінного струму частотою 50 Гц та номінальної напруги 220 В.

Працездатність системи має зберігатись за різних відхилень від номінального значення напруги мережі від -15 до +10% та частоти до ±1 Гц.

Електроживлення окремих СКУД допускається здійснювати й від інших джерел для яких притаманні свої параметрами вихідної напруги, вимоги до яких встановлено у нормативних документах на типи цих систем.

Електропостачання технічних засобів СКУД здійснюється від вільної групи провідників щита електроживлення (освітлення). За відсутності на об'єкті такого щита або вільної групи провідників на ньому замовником має бути встановлено окремий щит електричного живлення на необхідну кількість груп. Щит електроживлення, який встановлено поза приміщення, яке охороняється, необхідно розташовувати в металевій шафі, яка закривається та блокується під час відкривання.

У випадку втрати електричного живлення від основної мережі СКУД має мати резервні джерела живлення (РДЖ). Номінальна напруга резервного джерела живлення повинна бути +12 В або +24 В. Перехід на резервне живлення і назад має відбуватись автоматично без порушення встановлених режимів роботи та функціонального стану СКУД.

Резервне джерело живлення має забезпечувати функціонування системи під час зникнення напруги живлення в мережі на час не менше восьми годин роботи системи.

Слід пам'ятати, що під час використання, у якості РДЖ, акумулятора необхідно здійснювати його автоматичне підзарядження.

Акумуляторні батареї (виняток – необслуговуваних) розташовуються, як правило, у спеціальних акумуляторних приміщеннях на стелажах відповідно до вимог технічних умов і є стійкими до впливу агресивних середовищ.

Свинцеві акумулятори ємністю не більше 72 А/год та лужні акумуляторні батареї ємністю не більше 100 А/год й напругою до 60 В можуть бути встановленими у загальних виробничих не вибухо- і не пожежонебезпечних приміщеннях в металевих шафах із відокремленою припливно-витяжною вентиляцією.

Акумуляторні установки повинні бути обладнані відповідно до вимог «Правила побудови електроустановок».

Під час використання, в якості джерела резервного живлення, акумулятора або сухих батарей необхідно передбачити індикацію розряду акумулятора або батареї нижче допустимої межі. Для автономних систем індикація розряду повинна бути світлова або звукова, для мережевих систем сигнал розряду акумулятора повинен передаватися на центральний пульт. Хімічні джерела струму (елементи живлення), які вбудовано в активні ідентифікатори повинні забезпечувати працездатність засобів контролю та управління доступом не менше п’яти років.

9.2.5 Обладнання СКУД для автономного режиму роботи

СКУД 1-го та 2-го класів (див. п.2.1), які працюють в автономному режимі, зазвичай інсталюються в: квартирі, котеджі, невеликих офісах, магазинах, аптеках, готелях та малозначущих зонах на важливих об’єктах. Це дозволяє раціонально зменшити число каналів, які будуть обслуговуватись більш дорожчими СКУД 3-го й 4 -го класів. Такі СКУД – це невеликі та недорогі системи, які обслуговують, як правило, до восьми загороджувальних пристроїв (дверей, воріт, турнікетів). Зауважимо, що СКУД 1-го і 2-го класів прийнято застосовувати й на більш важливіших об’єктах (в приміщеннях), якщо необхідний рівень безпеки забезпечується системами охоронної сигналізації та відеонагляду.

На рисунку 9.2 подано приклад виконання СКУД в приміщення з одними дверима. Як бачимо в цю систему входять: контролер, який з’єднано із зчитувачем, кодова клавіатура, виконавчий пристрій (замок), давач стану дверей, кнопка автоматичного відкривання дверей, яка розташовується із внутрішньої сторони дверей, зовнішні звуковий і/або світловий сповіщувач та джерело живлення. Така система здатна забезпечити два способи контролю доступу: перевірку лише карток або подвійну перевірку – карток та кодового пароля.

У цій системі можливим є встановлення, так званого, офісного режиму. Його зміст полягає у тому, що СД відкриває закритий замок за допомогою

ідентифікатора та проходить в контрольовану зону. Із середини такий замок не блокується, а просте натискання на ручку призводить до відкриття дверей (такий режим встановлюється за бажанням замовника, а застосування кнопки автоматичного відкривання дверей є необов'язковою). (наприклад, для того, щоб кожен раз не підходити до дверей (не натискувати) і відкривати її зсередини, коли стукають відвідувачі.

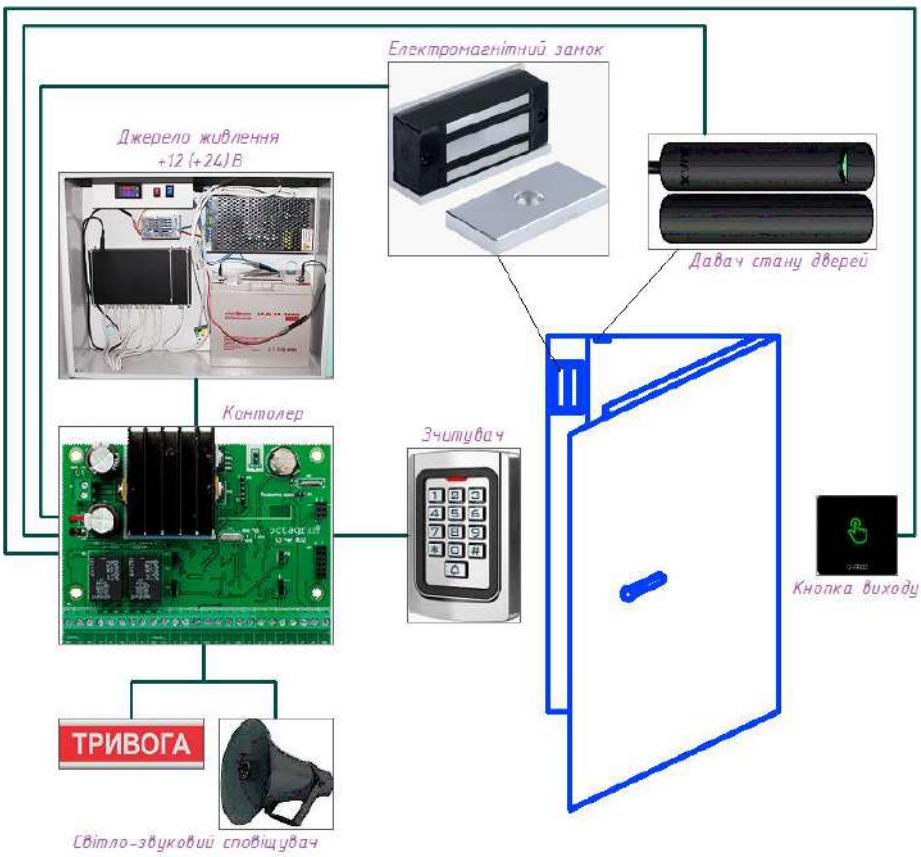


Рисунок 9.2 – Приклад облаштування СКУД приміщенням з одними дверима

Під час реалізації цього варіанту СКУД на об'єкті рекомендується:

– використовувати пристрої, які володіють тамперним (антисаботажним) захистом для запобігання навмисного взлому корпусу контролера/зчитувача (міцний металевий корпус, металева кодонабірна клавіатура та вбудована індикація режимів роботи);

– використовувати лише ті пристрої, до складу яких входить незалежна пам'ять, яка дозволяє зберігати дані тривалий час;

– використовувати пристрої, які дозволяють змінювати інтервал розблокування дверей;

– програмування системи здійснювати за допомогою майстер-картки та кодонабірної клавіатури.

Така будова СКУД може варіюватися у широких межах і мінімально складатись з одного конструктивно закінченого блоку (рис. 9.3), який об'єднує у собі зчитувач, контролер, виконавчий пристрій (защібка, ригель або засувка) та індикатори режимів роботи. При цьому СКУД працює в режимі звичайного замка, тобто при збігу кодів ідентифікатора і зчитувача запірний механізм спрацьовує і розблоковує двері, дозволяючи прохід.

Рисунок 9.3 – Приклади виконання розумних дверних замків

Під час розширення системи КУД додатково може встановлюватись ще один зчитувач, який контролюватиме прохід у зворотню сторону (організація багаторівневого контролю доступу), виносні світлові/звукові сповіщувачі, пристрої автоматичного відкривання/закривання дверей. На рисунку 9.4 наведено приклад можливого виконання СКУД об'єкта з декількома дверима, яка працює в автономному режимі.

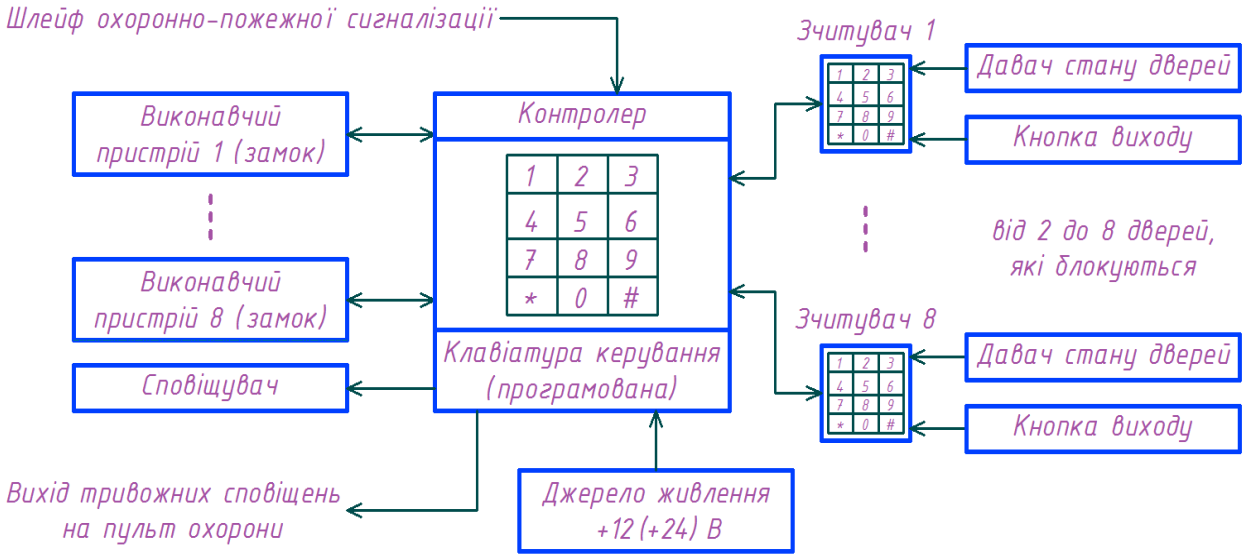


Рисунок 9.4 – Приклад облаштування СКУД приміщенням з декількома дверима [110]

Цей варіант системи відрізняється від попереднього лише розширенням функцій та об’ємом пам’яті керуючого контролера та його конструкцією. Зчитувачі та виконавчі пристрої розташовуються в різних конструктивних блоках, а управління ними здійснюється через загальний контролер.

До такої СКУД уже можна ввести наступні додаткові функції:

– контроль проходу за двома напрямками;

– автоматичне відкриття та закриття дверей під час аварійних та тривожних ситуаціях;

– передача тривожних повідомлень на пульт охорони;

– реєстрація подій за допомогою друкуючого пристрою, який напряму підключається до контролера.

Програмування системи прийнято здійснювати або за допомогою майстер-картки й клавіатури керування, або комп’ютера.

В кінцевому вигляді, дана система, може нагадувати СКУД, яка працює в мережевому режимі. Для цього застосовують будь-який контролер, який, у цьому режимі, інтегрує роботу інших контролерів або застосувати додатковий модуль зв’язку для об’єднання контролерів, в одне ціле, через інтерфейс RS 485.

9.2.6 Обладнання СКУД для мережевого режиму роботи

СКУД 3-го та 4-го класів призначені для оснащення великих об’єктів з підвищеними вимогами до безпеки (банки, великі установи та фірми тощо).

Основною перевагою таких систем є їх можливості до практично необмеженого розширення (дозволяють обслуговувати десятки тисяч користувачів). Для відносно невеликих та недорогих систем 3-го класу притаманною є побудова системи СКУД, за якої в одну контрольовану лінію інтерфейсу RS 485 підключаються усі контролери, а база даних завантажується до одного лише керуючого контролера (майстер-контролер). Така побудова системи дозволяє забезпечити гнучкість реалізації СКУД в інтер’єрі приміщення, мінімізувати комунікаційні з’єднання та великі відстані між об’єктами управління.

Ефективність роботи СКУД 4-го класу обумовлюється можливістю створювати розгалужені, досить численні з’єднання контролерів та комп’ютерів в єдину систему. Модульність побудови таких систем дозволяє забезпечити:

– гнучкість набору обладнання;

– простоту та легкість монтажу, технічного обслуговування та ремонту;

– можливість розширення системи;

– цінову ефективність;

– легкість під’єднання до пристроїв сервісної автоматики (управління ліфтом, освітленням, системами кондиціонування тощо).

На рисунку 5.4 наведено структурну схему побудови СКУД 3-го класу (для 64 дверей контрольованої зони) на базі багатофункціонального контролера, який володіє модульною конструкцією.

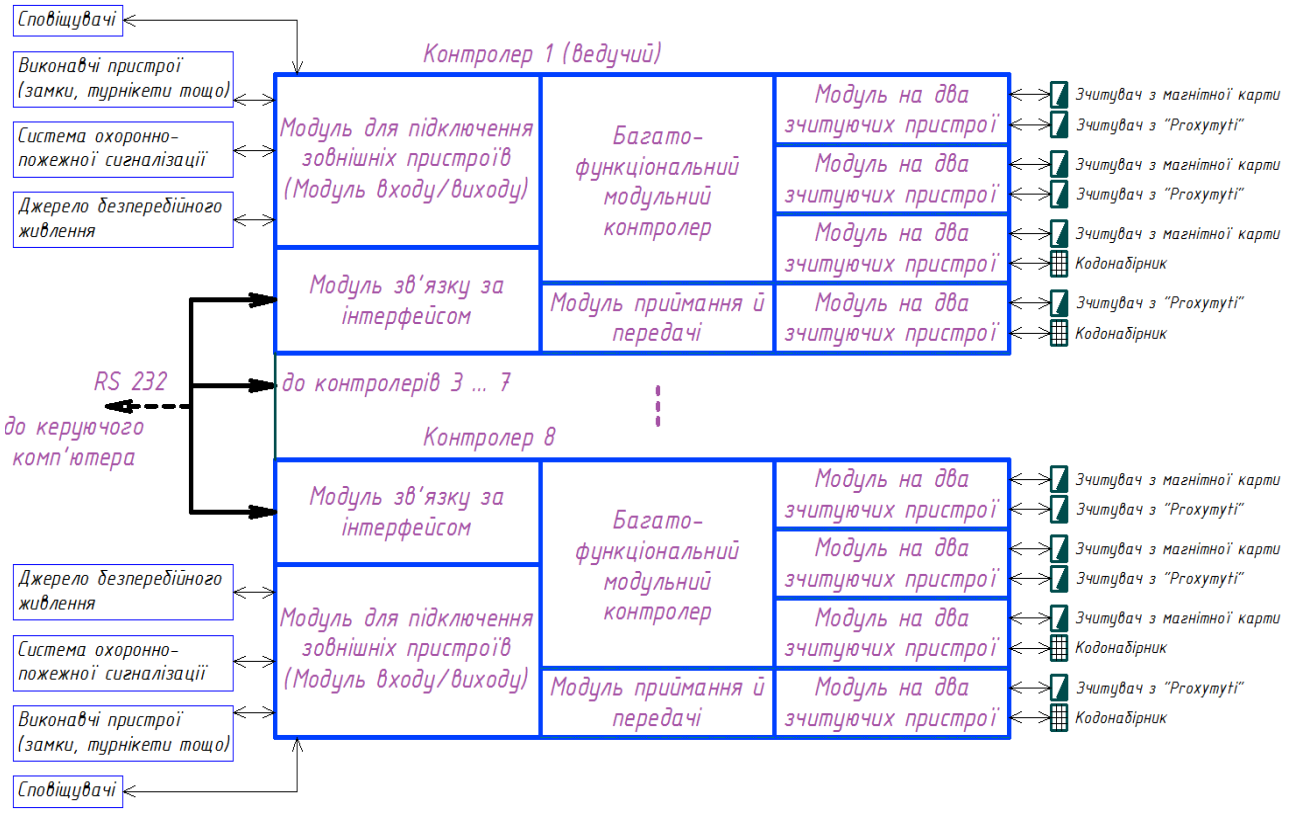


Рисунок 9.5 – Структурна схема СКУД 3-го класу [110]

З'єднання контролерів між собою та їх підключення до різних периферійних пристроїв, які входять до складу системи, забезпечується різними модулями. До одного контролера може бути підключено до восьми зчитувачів різного типу. Підключення зчитувачів здійснюється через відповідний модуль зчитування, що працює з двома зчитуючими пристроями. Окрім зчитувачів, він контролює також й давачі стану дверей, кнопки їх відкривання та інші допоміжні пристрої.

Інформація про стан інших зовнішніх пристроїв надходить до контролера через модуль входу/виходу. За допомогою цього модуля контролер управляє роботою виконавчих пристроїв та пристроєм видачі тривожних сповіщень. Модуль зв'язку, інтерфейсом RS 485, дозволяє інтегрувати наявні контролери до єдиної системи протяжністю один кілометр, а також, за необхідності, об'єднати їх з керуючим комп'ютером у комп'ютеризовану систему за допомогою інтерфейсу RS 232. Модуль приймання/передачі управляє роботою зчитувачів безконтактних карток (Proximity). Варто пам'ятати, що один контролер може обслуговувати до 10000 користувачів. При цьому, для

збільшення числа користувачів необхідно передбачити модуль розширення пам’яті.

На рисунку 9.6 подано варіант побудови СКУД 4-го класу.

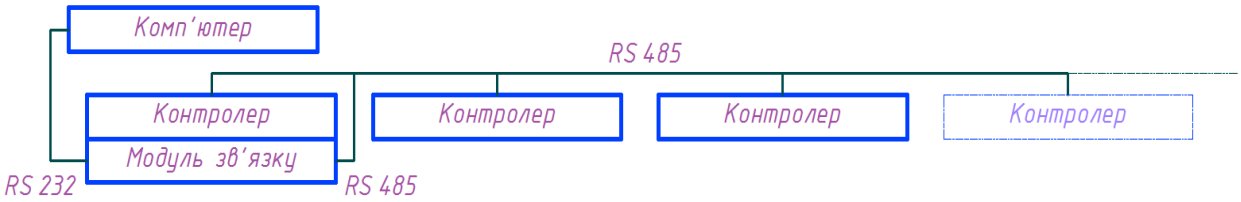


Рисунок 9.6 – Структурна схема побудови СКУД 4-го класу з однією гілкою

Системи 4-го класу прийнято будувати на базі таких же багатофункціональних контролерів, як використовують для побудови СКУД 3-го класу. Під час створення комп’ютерної мережі, яка налічує не більше 32-ох контролерів її доцільно об’єднати в одну гілку (рис. 5.6). У цьому випадку модуль зв’язку включають у перший за порядком контролер гілки. Він забезпечить зв’язок між цим контролером та комп’ютером через інтерфейс RS 232. Обмін інформацією між контролерами відбуватиметься за інтерфейсом RS 485. Окрім цього, на модуль зв’язку покладені функції перетворення формату та швидкості передачі даних RS 232/RS 485. Слід пам’ятати, що кожен із контролерів у гілці має свою адресу.

Подальше нарощування системи можливе лише за рахунок організації декількох (до 10) гілок контролерів. Приклад організації двох гілок подано на рисунку 9.7.

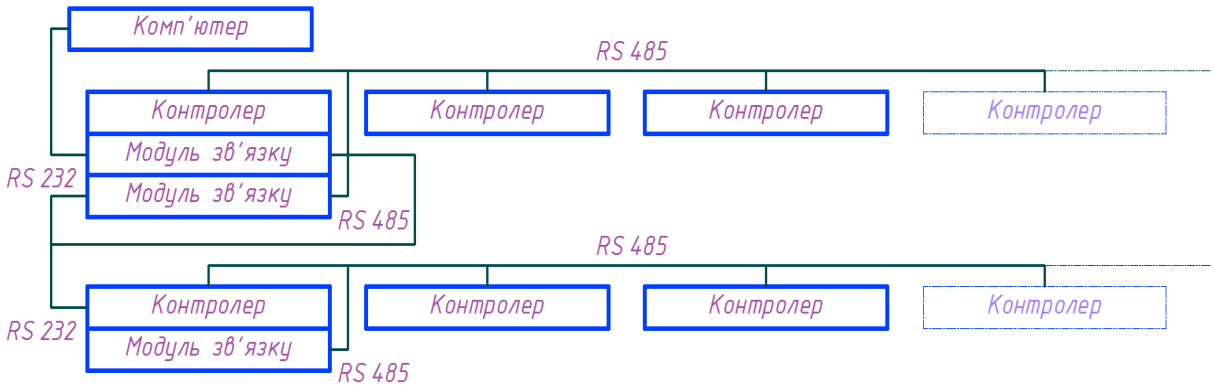


Рисунок 9.7 – Структурна схема побудови СКУД 4-го класу з декількома гілками

Модуль зв’язку першого контролера перетворює з одного боку потік даних, які надсилаються з керуючого комп’ютера на контролер, а з іншого – потік вихідних даних, який паралельно подаються на адресні модулі зв’язку у

гілках. Кожен адресний модуль зв'язку обмінюється даними з контролерами у гілках та модулями зв'язку. Така розширена мережа дозволяє обслуговувати до 320 контролерів і 2048 контрольованих точок.

За необхідності гілка контролерів може бути збільшена ще на один кілометр. Для цього необхідно підключити таку гілку (рис. 9.8) до першого контролера нової гілки через модуль зв'язку (інтерфейс RS 485).

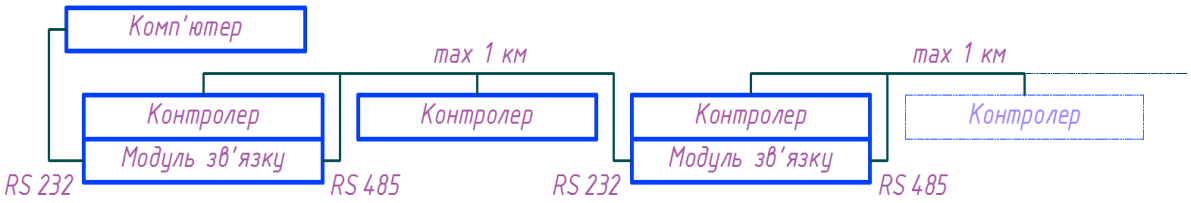


Рисунок 9.8 – Збільшення довжини гілки шляхом використання двох модулів зв'язку

Наявність описаних модулів багатофункціонального контролера створює додаткові можливості із управління різноманітною периферією системи. В якості контрольованих точок можуть виступати зчитувальні пристрої (головки), Pin-клавіатура, замкнені/розімкнені контакти кнопок, реле, вихідні контакти різних об'ємних або поверхневих сповіщувачів. У якості виконавчих пристроїв застосовують електромагнітні замки, шлагбауми, турнікети, пристрої тривожного сповіщення та освітлення, камери відеоспостереження.

Логічний пристрій (процесор) контролера, за допомогою відповідного програмного забезпечення, формує необхідні параметри доступу у кожній контрольованій точці, тобто конфігурувати систему. При цьому сервісний персонал може задавати їх з комп'ютера, що дозволяє реалізовувати на практиці різноманітні варіанти організації контролю й управління доступом, гнучко змінюючи їх відповідно до поточних вимог.

Програмне забезпечення надає великі сервісні можливості оператору, виводячи додаткову інформацію на дисплей (плани приміщень із зазначеними точками доступу, індикація несанкціонованих проникнень, повні або короткі звіти про реєстрацію події тощо).

9.2.7 Розміщення технічних засобів СКУД на об'єкті

Пристрої центрального управління (персональні комп'ютери), які є основою СКУД, рекомендовано встановлювати в окремих службових приміщеннях, які захищено від доступу сторонніх осіб (приміщення служб безпеки або пульта охорони об'єкта).

Основні положення, за якими розробляються режими роботи усієї системи безпеки, визначаються керівним складом служби безпеки, виходячи із

загальної концепції забезпечення безпеки об'єкта. Керуюче програмне забезпечення завантажують в центральний керуючий та допоміжні комп'ютери або контролери й замикаються секретними кодами.

Персонал охорони, а також інших служб, які підключено до загальної комп'ютерної мережі, не повинні мати доступ до програмних засобів та можливості впливати на встановлені режими роботи (винятком є особи, які відповідають за ці роботи).

Під час об'єднання комп'ютерів у мережу необхідно розділяти функціональні можливості серед користувачів цієї мережі й відповідно до цього розташовувати комп'ютери у визначених приміщеннях об'єкта (рис. 9.9).

Ведучий контролер та контролери, які працюють на декілька загороджувальних пристроїв, рекомендовано розміщувати у спеціальних металевих шафах або нішах, на зручній, для технічного обслуговування, висоті. При цьому, дверцята таких шаф або ніш необхідно блокувати охоронною сигналізацією. Контролери, які поєднано в одному корпусі із виконавчими або зчитуючими пристроями, рекомендовано обладнувати тамперними корпусами, для запобігання несанкціонованому відкриттю. Самі корпуса контролерів необхідно виконувати із міцного матеріалу, який дозволить захистити контролер від актів вандалізму. Контролери, які керують роботою зчитувачів або виконавчих пристроїв одних дверей, які працюють за двома напрямками, рекомендовано встановлювати із внутрішньої сторони зони захисту.

Рисунок 9.9 – Розміщення комп'ютерів СКУД, які інтегровано в мережу об'єкта

Для того щоб уникнути збоїв у роботі або виходу з ладу контролерів категорично забороняється їх до джерела живлення, від якого одночасно живиться й виконавчий пристрій, якому притаманна велика індуктивність обмоток. З метою виключення таких небажаних наслідків в цьому обладнані передбачають наявність спеціальних демпфуючих пристроїв або елементів, які дозволяють гасити імпульсні перешкоди (викликані ЕРС самоіндукції обмотки виконавчого пристрою).

Під час роботи пристроїв контролю та управління, які працюють в умовах мережевого режиму, необхідно враховувати появу різноманітних перешкод і збоїв, які будуть виникають через неправильний монтаж ліній з'єднань та їх довжин. Для нормальної роботи пристроїв СКУД у цьому режимі рекомендують:

– для шини RS 485 використовувати високоякісний екранований кабель витої пари;

– за великої довжини під'єднувального кабелю підключати до шини кінцеві та погоджуючі елементи (точна кількість елементів підключення залежить від характеристик кабелю);

– для уникнення блукаючих струмів заземляти пристрої та екрановану обплетку кабелів в одній точці (за можливості біля ведучого контролера);

– за великої довжини кабелів заземлення слід виконувати у різних точках, але обов'язково використовувати спеціальні методи та пристрої захисту від перешкод;

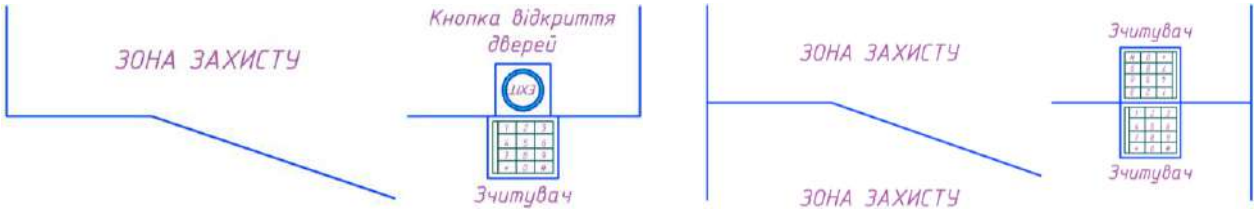
– для великої довжини кабелю використовувати шинні підсилювачі.

9.2.8 Встановлення зчитувачів та виконавчих пристроїв

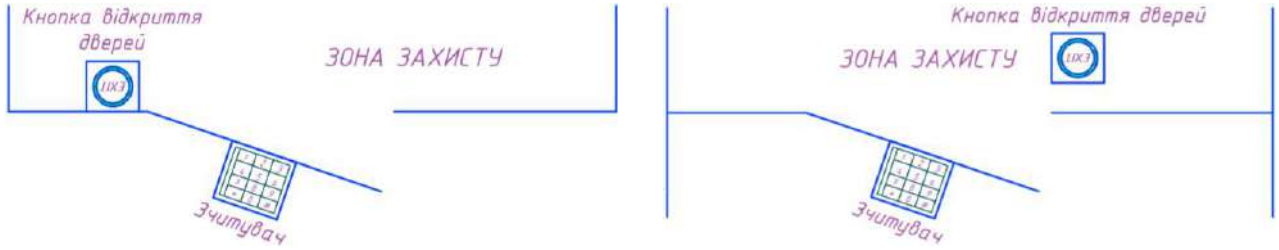
Залежно від типу зчитувача, пропускної спроможності та організації системи безпеки об'єкта в цілому їх рекомендовано встановлювати як біля загороджувальних пристроїв, так і безпосередньо на них. На рисунках 9.10 та 9.11 наведено варіанти розміщення й монтажу зчитувачів та виконавчих пристроїв.

Зчитувачі «Proximity» найзручніше розташовувати як на стіні (у тому числі й замасковано в стіні) перед загороджувальними пристроями, так і з внутрішньої сторони пристрою загородження (наприклад, на внутрішній стороні неметалевих дверей, якщо їх товщина не перевищує 10 см). Під час монтажу зчитувача на металевій основі, враховуючи рекомендації , необхідно забезпечити відстань між основою зчитувача та металізованою поверхнею не менше 25 мм. У тому випадку, коли стіна, за якою встановлено зчитувач, є занадто товстою або виготовлена із металу (містить металеву арматуру), то встановлення зчитувача допускається на тій відстані, яка забезпечує необхідний захист від можливого несанкціонованого проходу.

Розташування зчитувачів на стінці



Розташування зчитувачів на вхідних дверях



Розташування зчитувачів за стінкою та за вхідними дверима

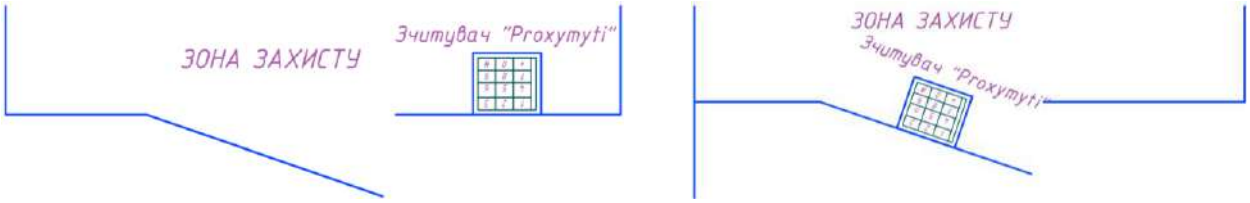


Рисунок 9.10 – Варіанти розміщення зчитувачів СКУД [110]

Зчитувачі магнітних та Wiegand-карт, електронних ключів і клавіатури рекомендовано розташовувати на стіні або безпосередньо на загороджувальних пристроях, на висоті, яка є зручною для суб’єкта доступу.

З метою уникнення перешкод або виходу з ладу зчитувачі магнітних карт (за винятком тих, які поєднано із виконавчими пристроями) не рекомендується встановлювати надто близько до тих виконавчих пристроїв, які здатні створювати потужні електромагнітні поля (соленоїдні, магнітні замки тощо).

Електромагнітні защібки рекомендовано монтувати у дверній коробці. Дана конструкція дозволяє блокувати ригель замка, який змонтовано на дверях, під час їх закривання та розблоковувати його при подачі сигналу від контролера. Окрім цього, відзначимо, що таке виконання защібки дозволяє повністю зберегти фурнітуру дверей.

Електромеханічні замки рекомендовано встановлювати на дерев’яних та металевих дверях масою до 100 кг за умови середнього прохідного навантаження (100 … 200 проходів за день). Застосування таких замків для дверей із високим прохідним навантаженням є неефективним через їх високе механічне зношення, як наслідок зниження надійності та терміну служби. У переважній своїй більшості електромеханічні замки встановлюють на дверях (накладні або врізні), але іноді зустрічаються варіанти їх розташування на дверній коробці.

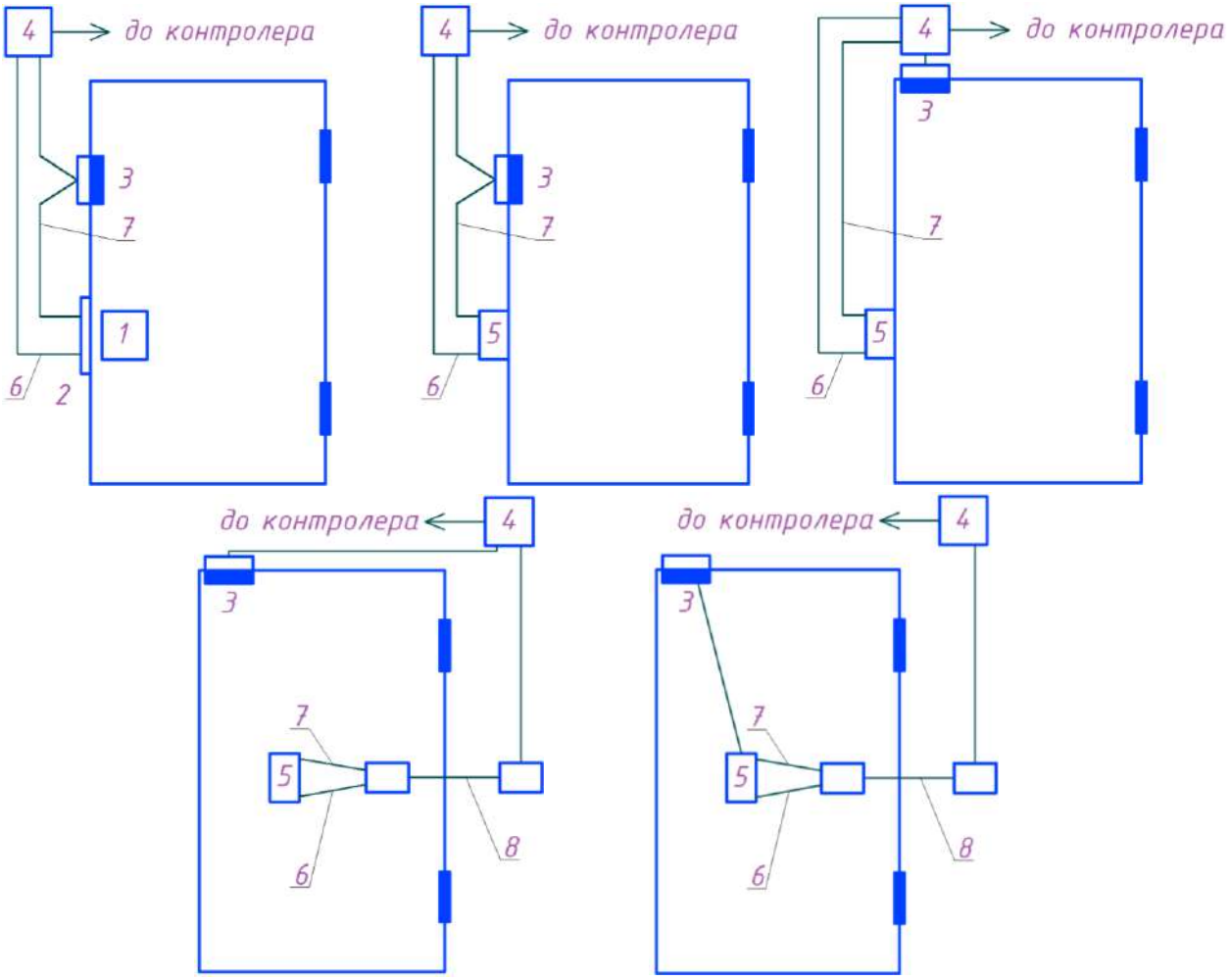


Рисунок 9.11 – Варіанти можливого розташування виконавчих пристроїв на дверних конструкціях [110]

1 – механічний замок; 2 – електромагнітна защіпка; 3 – давач стану дверей (геркон); 4 – з'єднувальна коробка; 5 – електромеханічний або електромагнітний замок; 6 – кабель живлення замка (для дверей, які виконано із горючого матеріалу – подвійна ізоляція ПХВ або металорукав); 7 – ланцюги управління та контролю; 8 – гнучкий перехід (кабелепровід)

Електромагнітні замки рекомендовано встановлювати на дерев'яних та металевих дверях масою до 650 кг в умовах високого прохідного навантаження (більше 200 проходів за день). Відсутність рухомих деталей (схильність до тертя і зношування) у конструкції такого замка роблять його, з точки зору експлуатаційних властивостей, більш довговічним. Основною особливістю електромагнітного замка є постійне живлення електричним струмом обмотки його електромагніту, так як під час зникнення живлення (аварійне відключення або навмисний обрив провідників) замок деактивується та відкривається. Як бачимо, для надійної роботи електромагнітного замка необхідно або дублювати його механічним замком, або застосовувати додаткове резервне живлення.

За умови спільного використання магнітно-контактних сповіщувачів, у якості давачів стану (положення) дверей з електромагнітними або електромеханічними замками перші необхідно розташовувати якомога далі від других.

Під час монтажу виконавчих пристроїв (замки, доводчики, приводи тощо), які потребують для своєї роботи підведення електричного живлення, необхідно використовувати спеціальні пристрої та кабелі, які дозволять забезпечити електро- та пожежобезпечність (особливо для горючих конструкцій), а також захистити кабель від пошкоджень при відкритті/закритті дверей (гнучкі кабелепроводи).

9.3 Експлуатація, технічне обслуговування та аудит СКУД

9.3.1 Експлуатація СКУД

Професійна експлуатація СКУД вимагає розуміння життєвого циклу обладнання, нормативних вимог та постійної готовності до протидії новим кіберзагрозам. Надійність СКУД визначається не лише якістю компонентів, а й системністю підходу до їх обслуговування та регулярністю аудитів, що дозволяють виявити приховані вразливості до моменту їх експлуатації зловмисниками.

Сучасна СКУД функціонує як послідовність інтелектуальних етапів, де кожен крок має бути верифікований системою [14]. Процес починається з ідентифікації користувача, де пред’являється ідентифікатор або мобільний пристрій.

Передача даних від зчитувача до контролера є етапом, де визначається фізична безпека каналу. Контролер, як «мозок» системи, аналізує отриманий код, порівнює його з внутрішньою базою даних та приймає рішення про керування перешкоджальним пристроєм (замком, турнікетом або шлагбаумом).

Експлуатація СКУД – це безперервний процес управління правами доступу, моніторингу подій та підтримки актуальності бази даних [21]. Адміністратор системи відповідає за реєстрацію нових користувачів, призначення їм відповідних рівнів доступу та часових зон.

На етапі розгортання, особливо в хмарних рішеннях, важливо правильно налаштувати робочий простір та API для взаємодії між контролерами та сервером. Реєстрація передбачає створення унікального профілю компанії або об’єкта, де кожен контролер прив’язується через MAC-адресу та сертифікати доступу для забезпечення захищеного каналу зв’язку [43].

Важливою частиною експлуатації є навчання персоналу. Співробітники повинні розуміти, як правильно користуватися зчитувачами, як діяти в разі відмови в доступі та якими є правила безпечного поводження з

ідентифікаторами. Це включає розробку внутрішніх інструкцій та проведення регулярних інструктажів.

9.3.2 Технічне обслуговування СКУД

Технічне обслуговування (ТО) СКУД не є разовою дією, а являє собою чітко регламентовану послідовність робіт, спрямованих на запобігання відмовам. Без регулярного догляду механічні частини зношуються, датчики забруднюються, а акумулятори втрачають ємність, що в сукупності робить об’єкт вразливим.

Регламентні роботи зазвичай поділяються на кілька категорій залежно від періодичності та складності [4].

Щоденний огляд включає перевірку комплектності та візуальну цілісність обладнання. Необхідно переконатися у відсутності підтікань, якщо мова йде про гідравлічні доводчики, та в справності світлової індикації зчитувачів.

Щомісячне обслуговування є більш глибоким та фокусується на функціональності:

– очищення поверхонь зчитувачів від пилу та жиру, що важливо для біометричних сенсорів та QR-терміналів;

– перевірка сили утримання електромагнітних замків та регулювання доводчиків (температурні зміни впливають на швидкість зачинення дверей, що може призвести до ударів або неповного закриття);

– тестування кнопок «Вихід» та аварійних кнопок розблокування (контакти кнопок можуть окислюватися, що призведе до неможливості залишити приміщення в критичний момент).

Раз на три місяці необхідно проводити ревізію електричних з’єднань. Вібрація від роботи дверей та температурні деформації призводять до ослаблення гвинтових затискачів у клемних колодках контролерів. Також проводиться перевірка заземлення, що є важливим для захисту від статичної електрики та наведень.

Річне обслуговування включає повний аудит програмного забезпечення:

– оновлення прошивок контролерів та зчитувачів для закриття виявлених вразливостей;

– резервне копіювання бази даних та очищення журналів подій від застарілої інформації, що уповільнює роботу системи;

– перевірка актуальності прав доступу (видалення облікових записів звільнених співробітників та перегляд привілеїв адміністраторів).

У разі відключення мережі 220 В, безпека об’єкта повністю лягає на плечі джерел безперебійного живлення та акумуляторних батарей.

Акумулятори в СКУД працюють у буферному режимі, проте вони піддаються природній деградації. Реальний термін служби свинцево-кислотних

акумуляторів (AGM) складає 3 … 5 років, але за несприятливих умов (висока температура, глибокі розряди) він може скоротитися вдвічі.

Для підтримки працездатності акумуляторів, які не використовуються, їх необхідно заряджати раз на 2-3 місяці. Важливо пам’ятати, що пошкоджені або старі акумулятори не можна утилізувати як звичайне сміття – вони підлягають передачі в спеціалізовані пункти прийому через вміст токсичного електроліту та свинцю.

Коли система виходить з ладу, час відновлення стає вирішальним фактором безпеки. Систематичний підхід до діагностики дозволяє швидко знайти першопричину, яка в 68% випадків криється не в самому пристрої, а в живленні або проводці.

При виникненні проблеми (наприклад, зчитувач не реагує на карту), рекомендується слідувати протоколу:

1. Перевірка статусу в ПЗ. Чи бачить контролер зчитувач? Які події фіксуються в журналі? Якщо події «Доступ заборонено», проблема в правах користувача. Якщо подій немає – проблема в залізі.

2. Перевірка живлення. Вимірювання напруги на клемах зчитувача. Вона повинна бути стабільною 12 В DC. Навіть падіння до 10 В може призвести до того, що зчитувач буде світитися, але не зможе зчитати карту.

3. Діагностика шини даних. Використання мультиметра для перевірки напруги між GND та лініями D0/D1. В нормі там має бути від 4,2 до 4,9 В. Якщо напруга близька до 0 В, це свідчить про коротке замикання порту або обрив дроту.

4. Тест ідентифікатора. Перевірка декількох різних карт. Це дозволяє виключити вихід з ладу конкретної антени в картці користувача.

5. Аналіз механіки. Якщо замок клацає, але двері не відчиняються – проблема в механічному перекосі дверної коробки або заїданні ригеля. Механічний знос через високу інтенсивність проходів (понад 500 на день) скорочує термін служби замків до 2-3 років.

9.3.3 Методологія аудиту СКУД

Аудит СКУД – це не просто перевірка працездатності замків, а комплексне оцінювання ризиків. Він охоплює технічний стан обладнання, відповідність юридичним нормам та кіберзахищеність.

Процес технічного та фізичного аудиту починається з візуального та інструментального контролю. Аудитор повинен переконатися, що до контролерів та кабельних трас неможливо отримати фізичний доступ без спрацювання тривожної сигналізації. Важливо перевірити, чи не заблоковані вентиляційні отвори обладнання та чи не піддається воно впливу вологи або агресивних середовищ.

Одним із ключових етапів є аналіз журналів подій. Це запис усіх дій у системі (хто, коли і де намагався пройти, хто змінював налаштування та які тривоги виникали). Журнали допомагають виявити аномалії, такі як спроби підбору паролів на зчитувачах-клавіатурах або повторні проходи за однією картою.

У великих організаціях права доступу часто стають хаотичними. Аудит повинен підтвердити, що:

– доступ надається за принципом необхідності для виконання посадових обов'язків;

– власники активів періодично переглядають списки користувачів;

– тимчасові гостьові картки автоматично анулюються після завершення терміну дії;

– налаштовані коректні часові зони та розклади для святкових днів, щоб уникнути ситуацій, коли офіс відкритий у неробочий час.

Збір біометричних даних та ведення журналів проходів безпосередньо стосується юридичного аудиту. Нагадаємо, що в Україні обробка таких даних регулюється Законом №2297-VI «Про захист персональних даних» [119]. Аудит повинен встановити відповідність наступним принципам:

– законність та прозорість (наявність письмової згоди працівників на збір біометрії та їх інформування про мету використання СКУД);

– мінімізація даних – система не повинна збирати надмірну інформацію (наприклад, зберігати повні відбитки пальців, якщо для ідентифікації достатньо лише векторного шаблону);

– обмеження зберігання (дані мають знищуватися після досягнення мети або звільнення працівника, а факт знищення повинен фіксуватися відповідним актом);

– захищеність (база даних повинна бути зашифрована, а доступ до неї – суворо обмежений).

Недотримання цих норм може призвести до значних штрафів або судових позовів від співробітників, особливо у випадках витоку біометричної інформації, яку, на відміну від пароля, неможливо змінити.

Сучасні атаки на СКУД часто відбуваються не через злам дверей, а через мережеві протоколи або програмні дефекти. Розуміння цих вразливостей є обов'язковим для фахівця з аудиту.

Аудит повинен включати сканування на наявність відомих вразливостей у ПЗ та прошивках [14]. Наприклад:

– CVE-2019-25279 (зберігання паролів у відкритому тексті в базі даних SQLite, що робить їх легким здобутком при отриманні доступу до файлової системи пристрою);

– CVE-2025-59097 (незахищений SOAP API дозволяє зловмиснику в мережі переконфігурувати контролери та відкрити всі двері без автентифікації);

– CVE-2025-1960 (використання стандартних облікових даних, які не були змінені при встановленні, що дає повний контроль над системою).

Для мінімізації ризиків необхідно впроваджувати сегментацію мережі, відключати невикористовувані служби та регулярно проводити тестування на проникнення.

Контрольні запитання

1. Де повинні розташовуватися контролери СКУД відносно зон доступу і чому?
2. Для яких типів установ відповідність стандарту ДСТУ EN 60839-11-1 є обов’язковою?
3. З чого розпочинається процес створення сучасної СКУД на об’єкті?
4. На яких об’єктах СКУД показник Grade 3 або Grade 4 є обов’язковим?
5. Наведіть приклади кіберзагроз, які можуть виникнути через використання стандартних паролів або незахищених API у системі.
6. У чому полягає конструктивна перевага електромагнітних замків у порівнянні з електромеханічними?
7. У чому полягає перевага мережевої архітектури СКУД?
8. У чому полягає роль адміністратора системи під час безперервної експлуатації СКУД?
9. Чому падіння напруги на клемах зчитувача до 10 В вважається критичним?
10. Чому при монтажі ліній зв’язку RS-485 важливо використовувати екрановану виту пару та заземлення в одній точці?
11. Як інтенсивність людського потоку впливає на вибір типу турнікета?
12. Яка вимога висувається до дверей у приміщеннях, де одночасно перебуває понад 15 осіб?
13. Яка критична особливість електромагнітних замків вимагає використання резервного живлення або дублювання механічним замком?
14. Який алгоритм дій обслуговуючого персоналу, якщо зчитувач перестав реагувати на карту доступу?
15. Який нормативний документ є основним документом, який визначає вимоги до проектування СКУД та впроваджує поняття ступенів безпеки?
16. Яким чином категорія критичності об’єкта впливає на технічне завдання та вибір обладнання для СКУД?
17. Яких вимог безпеки необхідно дотримуватися під час монтажу виконавчих пристроїв на дверях?

18. Яких юридичних принципів необхідно дотримуватися під час збору біометричних даних в СКУД?

19. Які вимоги висуваються до електроживлення СКУД у разі зникнення напруги в основній мережі?

20. Які механізми розблокування СКУД передбачено нормами проектування на випадок пожежі?

21. Які нормативні документи регламентують структуру технічного завдання на розробку СКУД в Україні?

22. Які обмеження існують для встановлення електромеханічних замків щодо ваги дверей та інтенсивності їх використання?

23. Які етапи формують послідовність функціонування сучасної СКУД?

24. Які основні параметри точок проходу оцінюються на етапі детального обстеження?

25. Які рівні доступу до програмного забезпечення СКУД рекомендовано розмежовувати?

26. Які технічні параметри використовуються для захищеного підключення контролерів?

27. Які типи технологій ідентифікації пропонує сучасний ринок СКУД? Для яких типів об’єктів вони найбільш підходять?

28. Яку перевагу дає об’єднання СКУД, відеоспостереження та сигналізації в єдину інтегровану систему охорони?

РОЗДІЛ 10. Методологія та практика управління ІТ-проєктами в СКУД

Сучасні СКУД складають критичну частину ІТ-інфраструктури будь-якого сучасного підприємства. Управління такими проєктами вимагає конвергенції знань у сферах фізичної безпеки, системної інженерії, кібербезпеки та стратегічного менеджменту. Специфіка СКУД як об’єкта управління полягає в її мультидисциплінарності, де апаратна частина повинна безперебійно взаємодіяти з програмними комплексами, базами даних та зовнішніми бізнес-системами, такими як ERP або системи обліку робочого часу.

10.1 Проєкт СКУД, як об’єкт управління

10.1.1 Теоретико-методологічні засади визначення СКУД у системній інженерії

Сучасна парадигма розвитку систем безпеки розглядає СКУД не як ізольований набір технічних засобів, а як складний інформаційно-комунікаційний проект, інтегрований у загальну архітектуру підприємства. У

контексті управління IT-проєктами СКУД визначається як людино-машинна система, що забезпечує автоматизовану реалізацію політик безпеки шляхом ідентифікації, автентифікації та санкціонування доступу об’єктів до ресурсів. Складність такого проекту обумовлена необхідністю синхронізації фізичного рівня (замки, турнікети), логічного рівня (програмне забезпечення, протоколи зв’язку) та організаційного рівня (регламенти доступу).

Згідно з науковими підходами до проєктування подібних систем, проєкт впровадження СКУД характеризується високою вартістю помилки на етапі проєктування. Будь-яке відхилення у виборі архітектури може призвести до вразливостей у контурі фізичного захисту або до критичних збоїв у роботі мережевої інфраструктури організації. Тому управління таким проєктом вимагає використання гібридних методологій, де планування апаратної частини відбувається за каскадною моделлю (Waterfall), а розробка та інтегрування програмних модулів – за гнучкими методами (Agile). Це дозволяє забезпечити стабільність фізичного контуру за збереження адаптивності програмної складової [115].

10.1.2 Місце СКУД в ієрархії інформаційних систем та рівні інтегрування

У загальній структурі IT-інфраструктури СКУД займає проміжне місце між системами фізичної безпеки та корпоративними управлінськими системами класу ERP або HCM. Успішне управління проєктом передбачає чітку вертикальну інтеграцію даних. На нижньому рівні ієрархії знаходяться периферійні пристрої, які взаємодіють із фізичним середовищем. На середньому рівні – контролери, які виконують логічну обробку подій у режимі реального часу. Верхній рівень представляє серверне програмне забезпечення, яке інтегрується з Active Directory для синхронізації облікових записів персоналу. В таблиці 10.1 узагальнена інформація взаємодії СКУД з корпоративними системами. Такий багаторівневий підхід дозволяє перетворити СКУД з інструменту простого обмеження проходу на джерело аналітичних даних для бізнесу.

Узагальнення поточної практики впровадження свідчить, що проекти, які не передбачають інтегрування з HR-системами на етапі планування, втрачають до 40% своєї потенційної ефективності вже у перший рік експлуатації [113].

10.1.3 Класифікація проєктів СКУД та технологічні вектори розвитку

Управління проєктом СКУД суттєво залежить від обраної технологічної бази та масштабу системи. Вибір архітектури СКУД є важливим управлінським рішенням, що визначає складність проєкту та необхідні ресурси. Традиційні архітектури включають централізовані моделі (клієнт-сервер), де всі дані обробляються єдиним сервером, та розподілені системи з багатьма шлюзами для великих або територіально рознесених об’єктів. Останнім часом

спостерігається стрімкий розвиток хмарних рішень (Cloud-based PACS), які пропонують високу масштабованість та нижчі витрати на обслуговування локальної інфраструктури, проте висувають підвищені вимоги до стабільності інтернет-зв'язку та безпеки каналів передачі даних.

Таблиця 10.1 – Матриця функціональної взаємодії СКУД з корпоративними системами

Рівень інтеграції	Об'єкт взаємодії	Тип обміну даними	Цільова функція проекту
Інфраструктурний	Мережеве обладнання (VLAN)	Ізольовані пакети TCP/UDP	Забезпечення мережевої безпеки та сегментації
Авторизаційний	LDAP / Active Directory	Синхронізація токенів та прав	Автоматизація створення облікових записів доступу
Управлінський	ERP / HRM системи	Дані про час проходу (лог-файли)	Автоматизація табелювання та обліку робочого часу
Безпековий	Відеоспостереження	Тривожні події та відеоверифікація	Створення єдиного ситуаційного центру безпеки

Локальні системи зазвичай реалізуються в межах малих офісів і не вимагають складної мережевої конфігурації. Мережеві проєкти передбачають створення розподіленої системи з централізованим керуванням, що є актуальним для університетських кампусів або промислових підприємств. Найбільш інноваційними є хмарні проєкти, оскільки дозволяють винести обчислювальну потужність за межі об'єкта, зменшуючи капітальні витрати на серверну інфраструктуру.

Іншим вектором класифікації є метод ідентифікації. У наукових дослідженнях підкреслюється, що вибір ідентифікатора є ключовим технічним ризиком проєкту. Традиційні безконтактні картки мають високий ризик передачі стороннім особам, тоді як біометричні системи вимагають складних процедур захисту персональних даних. Узагальнена класифікація за типами проєктних рішень наведена в таблиці 10.2.

Останні дослідження вказують на те, що майбутнє проєктів СКУД лежить у площині мультимодальної ідентифікації, де поєднуються два або більше чинника доступу для критичних точок проходження [70].

10.1.4 Управління ризиками проекту СКУД

Ризики в проєктах СКУД мають подвійну природу – вони стосуються як

успішності виконання самого ІТ-проєкту, так і безпеки об’єкта, який охороняється. Управління ризиками передбачає їх ідентифікацію, оцінку впливу та розробку стратегій мінімізації.

Таблиця 10.2 – Класифікація проектів СКУД за складністю реалізації та типом ідентифікації

Тип проекту	Технологічний стек	Основна перевага	Складність управління
Автономний	RFID (125 кГц), кодові панелі	Низька вартість, простота монтажу	Низька
Корпоративний	RFID (13,56 МГц, Mifare Desfire)	Високий захист від копіювання карт	Середня
Біометричний	FaceID, відбитки вен, райдужна оболонка ока	Неможливість передачі ідентифікатора	Висока (Legal&Tech)
Мобільний	NFC, Bluetooth Low Energy	Зручність, використання смартфонів	Середня (програмна сумісність)

Управління ризиками сумісності та безпеки передачі даних є центральним елементом інженерної складової проєкту. Одним із найсерйозніших технічних ризиків є використання застарілих стандартів зв’язку між зчитувачами та контролерами. Історично поширений протокол Wiegand у сучасних дочлідженнях класифікується як «небезпечний» через відсутність шифрування та односторонню природу зв’язку. Це створює ризик атаки типу «sniffing», де зловмисник може перехопити код карти безпосередньо з провідників між зчитувачем та контролером.

Для мінімізації цих ризиків керівники проєктів повинні наполягати на використанні сучасних смарт-карт (наприклад, MIFARE DESFire EV3) та протоколу OSDP, що дозволяє уникнути атак повторного відтворення та використання несанкціоновано придбаних чистих карток.

Перехід на протокол OSDP забезпечує двосторонній зв’язок, що дозволяє контролеру в реальному часі відстежувати стан зчитувача (наприклад, спробу демонтажу). В таблиці 10.3 нгаведена інформація щодо інтерфейсів передачі даних з точки зору їх безпеки.

Перехід на OSDP вимагає від проєктного менеджера більш ретельного підбору обладнання, оскільки не всі контролери та зчитувачі підтримують цей стандарт у повній мірі. Проте, з точки зору довгострокової експлуатації, це знижує витрати на модернізацію системи у випадку посилення вимог безпеки.

В умовах публічних закупівель або великих корпоративних проєктів значну роль відіграють корупційні ризики. Типовими є нечітке визначення

предмета закупівлі для обмеження конкуренції або умисне приховування частин технічної документації. Для мінімізації цих ризиків рекомендується:

– залучати незалежних експертів до підготовки тендерної документації;

– проводити попередні консультації з ринком через електронні системи закупівель;

– впроваджувати суворі системи внутрішнього контролю та розподілу обов'язків при плануванні.

Таблиця 10.3 – Аналіз безпекових характеристик інтерфейсів передачі даних

Тип ризику	Протокол Wiegand	Протокол OSDP	Наслідки для безпеки проекту
Клонування	Висока ймовірність	Захищено (AES-128)	Wiegand передає дані у відкритому вигляді, що дозволяє легко копіювати картки
Саботаж (розрив)	Не виявляється	Миттєве виявлення	OSDP має двосторонній зв'язок; система знає, якщо зчитувач офлайн
Перехоплення	Легко	Неможливо	OSDP використовує «безпечний канал» для захисту від прослуховування лінії
Дистанція	До 150 м	До 1200 м	OSDP базується на RS-485, що дозволяє будувати великі мережі з меншою кількістю контролерів

Операційні ризики також включають технічні збої обладнання та програмні помилки. Це вимагає розробки планів безперервності бізнесу та відновлення після збоїв, особливо для систем, які працюють у режимі 24/7.

10.1.5 Чинники надійності, відмовостійкості та живучості системи

Специфікою СКУД як ІТ-проєкту є вимога до надвисокої доступності. Якщо пошта або CRM-система можуть бути недоступні протягом певного часу без катастрофічних наслідків, то збій СКУД може призвести до блокування евакуаційних виходів або неможливості доступу до серверних приміщень. У зв'язку з цим, управління проєктом повинно включати розробку плану забезпечення живучості системи при втраті зв'язку з центральним сервером.

Узагальнення принципів побудови надійних систем безпеки дозволяє виділити три рівні автономності:

1. Перший рівень – автономність контролера, який повинен володщіти достатньою внутрішньою пам'яттю для зберігання БД користувачів та подій.

2. Другий рівень – резервування живлення, що забезпечує роботу системи протягом 4-12 годин після відключення основної мережі.

3. Третій рівень – дублювання серверів бази даних та каналів зв'язку.

Використання метрик MTBF (середній час між відмовами) та MTTR (середній час відновлення) дозволяє кількісно оцінити надійність запропонованого проектного рішення.

10.1.6 Економічне обґрунтування: аналіз ROI та сукупної вартості володіння (TCO)

Заключним етапом ініціації проєкту є доведення його економічної доцільності. Для СКУД розрахунок ROI базується не на прямому доході, а на економії витрат. Основний внесок у окупність робить автоматизація обліку робочого часу. Слід зазначити, що навіть на підприємстві із середньою чисельністю персоналу впровадження СКУД дозволяє скоротити втрати від запізнень та передчасних відходів на 5 … 12%.

Окрім цього, керівник проєкту повинен враховувати TCO (Total Cost of Ownership), який включає витрати на закупівлю та витрати на експлуатацію протягом 5 років. Сюди входять оновлення програмного забезпечення, заміна акумуляторів, перевипуск втрачених карт та технічна підтримка. Розрахунок ROI для проекту СКУД можна представити через наступне узагальнення – зменшення витрат на фізичну охорону плюс економія фонду оплати праці завдяки точному обліку часу має перевищувати TCO протягом терміну окупності, який зазвичай становить 18 … 24 місяці [72].

Рентабельність інвестицій ROI у СКУД не завжди вимірюється прямим прибутком. Вона часто базується на економії від запобігання втратам (крадіжки, несанкціонований доступ) та оптимізації процесів (автоматичний табель обліку робочого часу). Для розрахунку використовується класичний вираз:

$$ROI=([\text{Чистий прибуток (або економія)} - \text{витрати}] / \text{витрати})\times 100\%. \quad (10.1)$$

Під час розрахунку ROI важливо уникати помилок, пов’язаних з ігноруванням непрямих витрат, таких як вартість створення контенту для навчання або витрати на аналітику ризиків. Позитивний показник ROI підтверджує окупність вкладень, тоді як нульовий або від’ємний вказує на необхідність перегляду стратегії або архітектури проекту.

Зазначимо, що управління IT-проєктами в СКУД є мульти-дисциплінарною областю, де успіх залежить від синергії технічних, правових та економічних чинників. Перехід до використання сучасних протоколів (OSDP), дотримання стандартів (ДСТУ, GDPR) та інтегрування з корпоративними системами управління персоналом роблять СКУД ключовим елементом цифрової трансформації сучасної організації. Розуміння цих особливостей дозволяє проєктному менеджеру мінімізувати ризики на початкових етапах

життєвого циклу проєкту та забезпечити створення ефективної системи захисту об’єкта.

10.2 Використання сучасного програмного забезпечення СКУД для управління IT-проєктами

Сучасна парадигма управління IT-проектами вимагає високої точності в обліку ресурсів та суворого дотримання політик безпеки. Програмне забезпечення СКУД сьогодні виступає як центральна інфокомунікаційна платформа, яка інтегрує фізичну безпеку з бізнес-аналітикою. Використання такого ПЗ дозволяє автоматизувати значну частину функцій проєктного менеджменту, зокрема моніторинг присутності розробників на робочих місцях, розмежування доступу до серверних приміщень та лабораторій, а також формування об’єктивної звітності для стейкхолдерів.

10.2.1 Функціональна архітектура програмного забезпечення СКУД як інструменту проектного менеджменту

Функціональна структура сучасного ПЗ СКУД базується на модульному принципі, що дозволяє адаптувати систему під специфічні потреби конкретного IT-проекту. Основним ядром системи є модуль адміністрування, який забезпечує керування базою даних персоналу та розподіл прав доступу за ролями в проєкті (Project Manager, Developer, QA Engineer, DevOps). Важливим елементом є модуль моніторингу подій у реальному часі, який надає візуалізацію переміщень персоналу та стан точок доступу на інтерактивних планах приміщень.

Окремої уваги заслуговує модуль обліку робочого часу, який у проєктному менеджменті використовується для валідації фактично відпрацьованого часу порівняно з даними, внесеними у системи трекінгу задач (наприклад, Jira або Redmine). Таке порівняння дозволяє виявити аномалії у продуктивності та оптимізувати навантаження на команду. Узагальнення функціональних модулів програмного забезпечення СКУД представлено у таблиці 10.4.

Інтегрування ПЗ СКУД у загальний контур управління IT-підприємством дозволяє підвищити точність бюджетування проектів на 15 … 20% за рахунок виключення помилок ручного обліку часу [115].

10.2.2 Хмарні технології та модель ACaaS в управлінні розподіленими проєктами

Розвиток концепції хмарних обчислень призвів до появи моделі ACaaS, яка є особливо актуальною для IT-проектів із територіально розподіленими командами. Використання хмарного програмного забезпечення СКУД усуває необхідність розгортання та підтримки власної серверної інфраструктури, що

знижує капітальні витрати проекту. Керівник проекту отримує доступ до панелі управління системою через веб-інтерфейс або мобільний додаток з будь-якої точки світу, що дозволяє оперативно реагувати на інциденти або змінювати права доступу для нових учасників команди.

Таблиця 10.4 – Функціональні модулі програмного забезпечення СКУД у контексті управління проєктами

Назва модуля	Основна функція для PM (Project Manager)	Значення для успіху проєкту
Адміністрування персоналу	Керування ролями та рівнями доступу	Забезпечення конфіденційності розробок
Облік робочого часу	Автоматичне формування табелів	Об’єктивна оцінка витрат на персонал
Аналітична звітність	Аналіз дисципліни та відвідуваності	Виявлення ризиків вигорання або простоїв
Інтеграційний шлюз (API)	Синхронізація з ERP та системами PM	Створення єдиного інформаційного простору

Мобільні додатки, які інтегровано з ПЗ СКУД, виконують роль віртуальних ідентифікаторів та інструментів самообслуговування для співробітників. Наприклад, розробник може через додаток подати запит на тимчасовий доступ до лабораторії тестування, а менеджер проекту – миттєво його затвердити. Такий підхід суттєво прискорює внутрішні комунікації та усуває бюрократичні затримки в ході реалізації проекту. Узагальнення переваг хмарних рішень порівняно з локальними наведено в таблиці 10.5.

Таблиця 10.5 – Порівняння локального та хмарного програмного забезпечення СКУД для ІТ-проєктів

Критерій порівняння	Локальне ПЗ (On-premise)	Хмарне ПЗ (ACaaS)
Початкові інвестиції	Високі (сервер, ліцензії)	Низькі (передплата)
Масштабованість	Складна (потребує модернізації заліза)	Легка (зміна тарифного плану)
Доступність даних	Лише з корпоративної мережі	З будь-якого пристрою через Інтернет
Оновлення безпеки	Відповідальність ІТ-відділу	Автоматично провайдером

Як бачимо, хмарні системи СКУД забезпечують вищий рівень безперервності бізнесу (Business Continuity), оскільки дані дублюються у географічно розподілених дата-центрах, що захищає проєктну інформацію від локальних технічних збоїв [125].

10.2.3 Аналітика та прийняття рішень на основі даних СКУД

Сучасне програмне забезпечення СКУД виступає джерелом «великих даних» (Big Data), які за правильного аналізу стають цінним інструментом для прийняття управлінських рішень. Керівник ІТ-проєкту може використовувати аналітичні звіти для виявлення закономірностей у поведінці команди. Наприклад, аналіз часу перебування спеціалістів у різних зонах офісу може вказати на неефективність планування робочого простору або на надмірну кількість нарад, які відволікають від розробки.

Інтеграція ПЗ СКУД із системами бізнес-аналітики дозволяє створювати складні дашборди, де дані про фізичну присутність поєднуються з метриками виконання задач. Це дає можливість оцінити реальну трудомісткість окремих етапів проєкту та врахувати ці дані під час планування майбутніх спринтів. Важливим аспектом виступає предиктивна аналітика: система може сигналізувати про підвищений ризик звільнення ключового співробітника на основі зміни його звичного графіку роботи або частоти відвідування офісу.

Аналіз економічного аспекту впровадження аналітичних інструментів підтверджує, що автоматизація збору та обробки даних в СКУД дозволяє скоротити час на адміністративне управління проектом на 10 … 12% [113].

10.2.4 Роль програмного забезпечення у забезпеченні кібербезпеки та конфіденційності проєкту

Для ІТ-проєктів, де інтелектуальна власність є головним активом, ПЗ СКУД виконує функцію першого ешелону захисту від внутрішніх загроз. Сучасне програмне забезпечення підтримує розширені політики безпеки, такі як правило «двох осіб» для входу в серверні приміщення або антипассбек (Anti-Passback), що унеможливлює передачу ідентифікатора іншій особі.

Особлива увага в ПЗ приділяється захисту персональних даних учасників проєкту. Програмні комплекси, які відповідають вимогам GDPR, забезпечують автоматичне знеособлення логів через певний період часу та надають інструменти для швидкого видалення інформації про звільнених співробітників. Узагальнення заходів кіберзахисту на рівні ПЗ наведено у таблиці 10.6.

Програмне забезпечення СКУД необхідно розглядати як невід’ємну частину загальної системи управління інформаційною безпекою (ISMS) проєкту, оскільки фізичний доступ до робочих станцій та серверів часто є найпростішим шляхом для компрометації ІТ-продукту [126].

Таким чином, використання сучасного програмного забезпечення СКУД у менеджменті ІТ-проектів трансформує систему безпеки з пасивного бар’єру в активний інструмент оптимізації бізнес-процесів. Завдяки модульній архітектурі, хмарним технологіям та потужній аналітиці, ПЗ СКУД забезпечує

керівника проєкту об’єктивними даними для ефективного управління ресурсами, підвищення дисципліни та надійного захисту інтелектуальних активів.

Таблиця 10.6 – Заходи захисту інформації в ПЗ СКУД

Метод захисту	Технічна реалізація в ПЗ	Мета заходу
Шифрування БД	Алгоритми AES-256/RSA	Захист конфіденційності логів та шаблонів
Рольовий доступ (RBAC)	Налаштування прав операторів	Обмеження доступу до конфіденційних звітів
Аудит дій	Журналювання всіх змін у системі	Виявлення несанкціонованих дій адміністраторів
Двофакторна автентифікація	Інтеграція з TOTP/SMS/біометрією	Захист входу в консоль управління

Подальший розвиток таких систем вбачається у більш глибшому інтегруванні з алгоритмами штучного інтелекту для автоматизації прогнозів успішності проєктів на основі аналізу поведінкових чинників команд.

10.3 Життєвий цикл проєкту впровадження СКУД

Життєвий цикл проекту впровадження СКУД є фундаментальною концепцією, яка визначає послідовність стадій від моменту виникнення ідеї до виведення системи з експлуатації. На практиці цей цикл розглядається як інтегрований процес, де інженерні рішення тісно переплітаються з алгоритмами обробки інформації та нормами фізичної безпеки. На відміну від розробки програмного забезпечення, життєвий цикл СКУД має виражену матеріальну складову, що накладає додаткові обмеження на логістику та терміни реалізації.

Ефективне управління проєктом СКУД базується на чіткому дотриманні фаз життєвого циклу, що забезпечує системний підхід та мінімізацію відхилень від стратегічних цілей. Життєвий цикл охоплює п’ять основних етапів:

– ініціювання;
– планування;
– виконання;
– моніторинг і контроль;
– завершення.

10.3.1 Фаза ініціації: обстеження об’єкта та визначення цілей

Фаза ініціації є відправною точкою, де закладається фундамент майбутньої системи. Ключовим процесом на цьому етапі виступає передпроєктне обстеження об’єкта, яке в професійному середовищі називається безпековим аудитом. Аудит передбачає не лише візуальний огляд приміщень, а

й аналіз потоків персоналу в часи пік, виявлення критичних точок доступу та оцінку існуючої інженерної інфраструктури (СКС, електропостачання). На основі отриманих даних керівник проєкту формує бізнес-цілі, які повинні бути конкретними та вимірюваними. Наприклад, ціллю може бути скорочення часу ідентифікації на прохідній до 0,5 секунди або забезпечення 100% реєстрації всіх відвідувачів у хмарному сховищі.

Результатом ініціації є формування концепції безпеки, яка включає модель загроз та визначення категорій доступу для різних груп користувачів. Зауважимо, що чітко визначена політика доступу на етапі ініціації дозволяє уникнути до 40% змін у технічному завданні на пізніх стадіях проекту [114]. Узагальнення цілей наведено в таблиці 10.7.

Таблиця 10.7 – Матриця бізнес-цілей та технічних вимог на етапі ініціації

Бізнес-ціль проекту	Технічна вимога	Інструмент реалізації
Підвищення дисципліни	Фіксація часу входу/виходу	Модуль обліку робочого часу (ОРЧ)
Захист конфіденційної інформації	Багаторівнева ідентифікація	Біометричні зчитувачі та RFID
Оптимізація витрат на охорону	Дистанційне керування точками	Мережеві IP-контролери
Забезпечення безпеки праці	Аварійне розблокування	Інтеграція з пожежною сигналізацією

10.3.2 Фаза планування: розробка технічного завдання та вибір архітектури

Фаза планування є найбільш наукоємною частиною життєвого циклу. На цьому етапі розробляється технічне завдання за вимогами ДСТУ EN 60839-11-1:2019. ТЗ стає юридичним та технічним документом, що регулює взаємовідносини між замовником та виконавцем. Центральним питанням планування є вибір архітектури системи, яка визначає логіку прийняття рішень про допуск СД.

Централізована архітектура передбачає, що вся логіка зосереджена на сервері. Це полегшує адміністрування, але робить систему вразливою до розриву каналів зв’язку. Децентралізована архітектура базується на інтелектуальних контролерах, які працюють автономно, зберігаючи локальну базу ідентифікаторів. Гібридна модель є найбільш збалансованою для сучасних ІТ-проєктів, оскільки дозволяє контролерам приймати рішення самостійно, синхронізуючи події з центральною базою даних у реальному часі. Як бачимо, вибір архітектури має базуватися не лише на аналізі латентності мережі, але й на вимогах, які висуваються до відмовостійкості системи [126].

Узагальнюючи процес планування, слід зазначити, що на цій стадії також визначається технологічний стек – типи ідентифікаторів, протоколи зв'язку (Wiegand чи OSDP) та методи шифрування даних. Помилка у виборі архітектури на етапі планування може призвести до експоненціального зростання сукупної вартості володіння системою у майбутньому.

10.3.3 Фаза реалізації: монтаж та розгортання програмного забезпечення

Фаза реалізації розпочинається після затвердження проєктної документації. Вона включає два паралельні процеси: фізичний монтаж обладнання та розгортання програмної інфраструктури. Монтажні роботи охоплюють встановлення виконавчих пристроїв (електрозамків, турнікетів), прокладання кабельних ліній та монтаж контролерів у захищених шафах. Важливим аспектом є забезпечення безперебійного живлення усіх вузлів СКУД.

Програмна частина реалізації включає інсталяцію серверного ПЗ, налаштування баз даних та конфігурацію мережевих параметрів контролерів. На цьому етапі проводиться інтеграція СКУД із суміжними системами, наприклад, з Active Directory для автоматизації створення облікових записів. Слід зауважити, що успіх реалізації залежить від координації між інженерною групою та IT-відділом замовника, особливо у питаннях мережевої безпеки та виділення VLAN для трафіку СКУД [113].

10.3.4 Фаза завершення: випробування та передача в експлуатацію

Завершальна фаза життєвого циклу спрямована на верифікацію та валідацію створеної системи. Приймально-здавальні випробування проводяться за спеціальною методикою, яка включає перевірку працездатності кожної точки проходу у звичайному та аварійному режимах. Керівник проєкту повинен переконатися, що система реагує на спроби несанкціонованого доступу та правильно реєструє події в базі даних.

Окремим критичним процесом є навчання персоналу. Адміністратори системи повинні опанувати навички керування правами доступу, а співробітники охорони – методи реагування на тривожні події. Передача виконавчої документації включає в себе структурні схеми підключень, кабельні журнали, ліцензійні сертифікати та інструкції з експлуатації. Завершення проєкту фіксується актом введення в експлуатацію, що є підставою для початку гарантійного періоду та сервісного обслуговування. Слід пам'ятати, що якісна виконавча документація дозволяє знизити на 25% витрати на майбутню модернізацію системи.

Процеси, у межах цих фаз, не завжди лінійні; вони часто ітеративно повторюються, що особливо характерно для розробки ПЗ у складі СКУД, де

тестування та уточнення вимог можуть відбуватися паралельно з виконанням робіт.

10.4 Управління вимогами та вибір технологічного стеку

Процес управління вимогами у проєктах систем контролю та управління доступом є критичним етапом, що визначає відповідність майбутньої системи очікуванням стейкхолдерів та технічним стандартам безпеки. В інженерії безпекових систем вимоги поділяються на функціональні (що система має робити) та нефункціональні (надійність, швидкість, безпека даних). Керівник проєкту на цьому етапі виступає медіатором між службою безпеки, IT-департаментом та адміністрацією об'єкта, оскільки їх запити часто є взаємовиключними.

10.4.1 Методи збору та пріоритезації вимог

Збір вимог розпочинається з аналізу нормативного поля, де ключовим орієнтиром виступає ДСТУ EN 60839-11-1:2019. Цей нормативний документ диктує мінімальні рівні захисту залежно від типу об'єкта. Наступним методом є інтерв'ю з представниками різних відділів. Служба безпеки підприємства, зазвичай, наполягає на максимальній суворості ідентифікації та глибокому інтегруванні з відеоспостереженням. У той же час HR-відділ формує вимоги до зручності використання системи для обліку робочого часу, гнучкості розкладів та автоматизації звітів.

Для узагальнення зібраних даних використовується матриця відстеження вимог, яка пов'язує кожну технічну специфікацію з конкретною бізнес-потребою. Важливим аспектом є вирішення конфліктів вимог, наприклад, коли вимога, яка стосується високої швидкості проходу ТД суперечить вимозі обов'язкової подвійної біометричної автентифікації. У таких випадках прийнято застосовувати метод пріоритезації MoSCoW, що дозволяє виділити критично важливі функції від бажаних. З цього слідує, що ефективність СКУД на 60% залежить від точності формулювання вимог на етапі ініціації та планування [115].

10.4.2 Вибір технологій ідентифікації: безпека проти бюджету

Вибір методу ідентифікації є центральним рішенням у формуванні технологічного стеку. На сучасному ринку домінують три основні напрямки: радіочастотна ідентифікація (RFID), біометричні технології та мобільний доступ. Вибір конкретної технології безпосередньо впливає на капітальні витрати та терміни реалізації проєкту, оскільки впровадження біометрії потребує тривалішого часу на збір та реєстрацію шаблонів користувачів у порівнянні з видачею карт. Порівняльний аналіз технологій ідентифікації в проектах СКУД представлено в таблиці 10.8.

Таблиця 10.8 – Порівняльний аналіз технологій ідентифікації в проєктах СКУД

Технологія	Стійкість до копіювання	Швидкість розпізнавання	Вплив на бюджет	Основна перевага
RFID (Mifare Desfire)	Висока (AES шифрування)	< 0,2 с	Середній	Надійність та стандартизація
Біометрія (FaceID)	Дуже висока	0,3 … 1,0 с	Високий	Неможливість втрати ідентифікатора
Мобільний доступ (NFC)	Висока	< 0,5 с	Середній	Зручність та відсутність фізичних карт
Біометрія (Вени долоні)	Максимальна	0,8 … 1,5 с	Дуже високий	Гігієнічність та висока точність

На практиці прийнятио вважати, що використання застарілих RFID-карт у нових проєктах є недопустимим через критичні вразливості, які дозволяють клонувати ідентифікатор за допомогою дешевого обладнання. Керівник проєкту повинен враховувати не лише вартість самих зчитувачів, але й вартість володіння системою (ТСО), включаючи витрати на перевипуск карт у разі їх втрати чи пошкодження. Біометричні системи, попри вищу початкову вартість, демонструють кращу окупність у довгостроковій перспективі за рахунок відсутності фізичних носіїв [113].

Узагальнюючи вище викладене, слід зазначити, що успіх третього етапу життєвого циклу проєкту залежить від здатності проєктного менеджера трансформувати розмиті побажання стейкхолдерів у чіткий та безпечний технологічний стек, що відповідає актуальним загрозам та економічним обмеженням організації.

10.5 Інтегрування та системна взаємодія у проєктах СКУД

Сучасний етап розвитку систем фізичної безпеки характеризується переходом від ізольованих інженерних рішень до створення комплексних інтегрованих систем безпеки. Управління проєктом інтегрування СКУД із суміжними інформаційними та безпековими системами є найбільш складним етапом, оскільки він потребує синхронізації протоколів передачі даних та узгодження бізнес-логіки різних департаментів організації. Як бачимо основна її мета полягає у створенні синергетичного ефекту, де сукупна ефективність об’єднаних систем перевищує суму ефективностей кожної з них окремо.

10.5.1 Взаємодія СКУД із системами відеоспостереження

Інтеграція СКУД із системами охоронного телебачення (CCTV) є

фундаментальною для забезпечення верифікації подій у реальному часі. Технічна реалізація такої взаємодії зазвичай базується на використанні програмних інтерфейсів (API) або спеціалізованих комплектів розробника (SDK), що дозволяють обмінюватися тривожними метаданими між серверами. Ключовим функціональним елементом тут виступає відеоверифікація: у момент зчитування ідентифікатора система автоматично відображає на моніторі оператора відео у реальному часі із відповідної камери та архівне фото користувача з бази даних СКУД.

Узагальнення переваг такої інтеграції дозволяє виділити автоматизацію процесу виявлення правопорушень, таких як передача карти іншій особі або прохід «паровозиком». Крім того, події СКУД стають своєрідними закладками в архівах відеоспостереження, що в десятки разів пришвидшує пошук необхідних фрагментів під час проведення службових розслідувань. Як підкреслюється в дослідженнях з методології безпеки, використання інтелектуальних модулів розпізнавання обличь дозволяє реалізувати сценарій двофакторної автентифікації без залучення додаткових фізичних зчитувачів [1].

10.5.2 Управління інтеграцією з охоронно-пожежною сигналізацією

Взаємодія СКУД з охоронно-пожежною сигналізацією (ОПС) є критичною з точки зору забезпечення безпеки життєдіяльності та відповідності державним будівельним нормам (ДБН). Управління таким підпроєктом вимагає реалізації двох рівнів інтегрування: апаратного та програмного.

Апаратний рівень передбачає пряме підключення виходів пожежних контролерів до входів контролерів СКУД через релейні схеми («сухий контакт»). Це гарантує безумовне розблокування шляхів евакуації навіть у разі повної відмови серверного програмного забезпечення або виходу з ладу локальної мережі.

Програмний рівень інтегрування дозволяє автоматизувати оповіщення персоналу про тривогу та формувати звіти про кількість осіб, які залишилися в будівлі на момент інциденту. Важливо враховувати вимоги ДСТУ EN 60839, які регламентують пріоритетність сигналів пожежної безпеки над командами блокування доступу. Будь-яка помилка в управлінні цим аспектом проєкту несе не лише технічні ризики, а й пряму юридичну відповідальність за безпеку людей на об’єкті [125]. Порівняння рівнів взаємодії наведено в таблиці 10.10.

10.5.3 Автоматизація обліку робочого часу через HR- та ERP-системи

Інтегрування СКУД із системами управління ресурсами підприємства (ERP) та бухгалтерськими модулями (SAP, Oracle) є ключовим інструментом підвищення економічної ефективності організації. На цьому етапі управління проєктом СКУД трансформується у повноцінний IT-проект з обробки великих даних. Основна задача полягає в автоматичній передачі подій «Вхід» та

«Вихід» до модулів обліку робочого часу. Це дозволяє виключити людський чинник під час формування табелів, автоматично розраховувати запізнення, понаднормові години та прогули.

Таблиця 10.10 – Аналіз рівнів інтеграції СКУД з системами ОПС

Рівень інтегрування	Метод реалізації	Надійність	Функціональність
Апаратний	Пряме релейне з'єднання	Максимальна (працює без ПЗ)	Лише розблокування ТД
Програмний	Протоколи TCP/IP, OPC, API	Середня (залежить від мережі)	Моніторинг, звіти, логіка сценаріїв
Комбінований	Апаратне розблокування + ПЗ	Найвища (рекомендовано)	Повний контроль та безпека

Для реалізації такої взаємодії керівник проєкту має забезпечити розробку або налаштування шлюзів обміну даними, які використовують SQL-запити або REST API. Важливим аспектом є синхронізація довідників персоналу: будь-які зміни в HR-системі (прийом на роботу, звільнення, відпустка) повинні миттєво відображатися в базі даних СКУД. Узагальнення практики впровадження свідчить, що така автоматизація дозволяє скоротити адміністративні витрати на 10 … 15% за рахунок оптимізації роботи бухгалтерії та HR-департаменту [113]. Технологічні параметри взаємодії узагальнено в таблиці 10.11.

Таблиця 10.11 – Характеристики інтегрування СКУД з корпоративними IT-системами

Тип системи	Механізм взаємодії	Об'єкти обміну	Бізнес-ефект
HR-система	SQL View, REST API	Картки персоналу, графіки	Актуалізація прав доступу
Бухгалтерія	XML/JSON вивантаження	Табелі робочого часу	Автоматизація нарахування заробітної плати
Active Directory	Протокол LDAP	Логіни, групи доступу	Єдина точка управління правами

Слід зауважити, що системне інтегрування є вищим ступенем розвитку проєктів СКУД. Вона вимагає від проєктного менеджера розуміння не лише принципів роботи фізичних замків та контролерів, а й знань у сфері системної архітектури, протоколів мережевої взаємодії та методологій обробки корпоративної інформації. Успішне інтегрування перетворює СКУД на

динамічний інструмент управління бізнесом, що забезпечує не лише безпеку, а й сталий розвиток організації [126].

10.6 Кібербезпека в проєктах СКУД

Сучасний етап розвитку систем контролю та управління доступом характеризується повною конвергенцією фізичної та інформаційної безпеки. Оскільки сучасна СКУД функціонує як складний інфокомунікаційний вузол у загальній ІТ-інфраструктурі підприємства, вона автоматично стає об’єктом кіберзагроз, характерних для будь-яких IoT-пристроїв. Управління кібербезпекою в таких проєктах не обмежується лише встановленням антивірусного ПЗ на сервері, а охоплює захист усієї вертикалі передачі даних: від зчитувача на дверях до бази даних на центральному вузлі.

10.6.1 Захист каналів зв’язку та шифрування даних

Основним вектором атак на СКУД є перехоплення даних у каналах зв’язку. Управління проєктом у цій частині передбачає впровадження багаторівневого захисту трафіку. На рівні взаємодії зчитувача з контролером важливим є перехід від незахищених інтерфейсів до використання протоколу OSDP із підтримкою технології Secure Channel. Це забезпечує автентифікацію пристроїв та шифрування за алгоритмом AES-128, що унеможливлює атаки типу «людина посередині» (Man-in-the-Middle) та клонування ідентифікаторів безпосередньо з лінії зв’язку.

На вищому ієрархічному рівні – між IP-контролерами та сервером управління – захист базується на використанні протоколів TLS або SSL. Керівник проєкту повинен забезпечити створення ізольованого мережевого сегмента (VLAN) для систем безпеки, що дозволяє відокремити трафік СКУД від загального корпоративного потоку даних та мінімізувати ризик горизонтального розповсюдження шкідливого ПЗ у разі компрометації робочих станцій персоналу. Технічні параметри захисту каналів узагальнено в таблиці 10.12.

Відсутність шифрування будь-якої ділянки ланцюга робить усю систему безпеки об’єкта фіктивною, оскільки сучасні засоби кібератак дозволяють імітувати сигнал відкриття замка навіть без наявності фізичного ключа [126].

10.6.2 Управління вразливостями прошивок та системне зміцнення

Другим аспектом кібербезпеки є менеджмент вразливостей апаратного та програмного забезпечення. Контролери СКУД мають свій життєвий цикл, що за відсутності регулярного оновлення прошивок робить їх вразливими до експлойтів. Управління проєктом має включати регламент регулярного патч-менеджменту, де кожне оновлення від виробника проходить попереднє тестування на стенді перед розгортанням на діючому об’єкті.

Таблиця 10.12 – Технології захисту комунікаційних вузлів у проєктах СКУД

Сегмент мережі	Протокол захисту	Метод шифрування	Цільова безпекова функція
Зчитувач – контролер	OSDP v2.2	AES-128	Захист від копіювання карт та перехоплення коду
Контролер – сервер	IP/TLS 1.3	AES-256	Автентифікація пристроїв у локальній мережі
Сервер – база даних	IPsec/VPN	RSA/AES	Цілісність та конфіденційність архіву подій
Клієнтське ПЗ – сервер	HTTPS	SSL/TLS	Захист сесій адміністраторів та операторів

Системне зміцнення передбачає деактивацію усіх невикористовуваних сервісів та портів на контролерах (наприклад, Telnet, FTP або HTTP без шифрування). Важливо також забезпечити контроль цілісності завантажувача, щоб запобігти завантаженню шкідливого коду на рівні заліза. Як бачимо, успішна кіберзахищеність системи базується на принципі мінімальних привілеїв, де кожен компонент системи має доступ лише до тих ресурсів, які необхідні для його безпосередньої роботи [113].

Слід підкреслити, що кібербезпека в СКУД – це безперервний процес управління ризиками. Тільки поєднання стійкого шифрування, регулярного оновлення систем та суворого дотримання норм захисту персональних даних дозволяє створити надійний фундамент для функціонування сучасної системи контролю доступу в умовах зростаючих глобальних кіберзагроз.

10.7 Управління ризиками та якістю в проєктах СКУД

Управління ризиками та забезпечення якості в проєктах впровадження СКУД є взаємопов’язаними процесами, які визначають надійність системи та задоволеність кінцевого користувача. Оскільки СКУД інтегрує в собі фізичні бар’єри, електронні компоненти та складне програмне забезпечення, ризики мають гібридний характер. Якість системи, своєю чергою, вимірюється не лише відсутністю дефектів, а й точністю алгоритмів ідентифікації та швидкістю реакції виконавчих механізмів.

10.7.1 Ідентифікація та аналіз специфічних ризиків

Управління ризиками розпочинається з класифікації загроз, які можуть вплинути на терміни, бюджет або функціональність проєкту. Перша категорія ризиків пов’язана із логістикою та постачанням високотехнологічного обладнання. У сучасних умовах глобального дефіциту напівпровідників

затримки у постачанні специфічних контролерів або біометричних сенсорів можуть призвести до зупинки проєкту на критичних етапах. Керівник проєкту повинен розробляти стратегії диверсифікації постачальників та формувати резервний фонд критичного обладнання на етапі ініціації.

Друга група ризиків стосується етапу монтажу та пусконалагоджувальних робіт. Помилки під ча інсталяції електромагнітних замків, неправильне розрахування падіння напруги в кабельних лініях або порушення регламентів встановлення зчитувачів призводять до прихованих дефектів, які проявляються лише під час пікових навантажень. Третя категорія ризиків охоплює програмну несумісність. Інтегрування СКУД із існуючим ПЗ замовника (наприклад, застарілими версіями ОС або специфічними драйверами сторонніх виробників) часто створює конфлікти, які потребують додаткових витрат на розробку програмних «латок».

Узагальнення ключових ризиків та методів їх нівелювання представлено в таблиці 10.13.

Таблиця 10.13 – Матриця стратегічних ризиків проекту СКУД

Категорія ризику	Опис загрози	Наслідки для проекту	Стратегія реагування
Технологічний	Несумісність протоколів OSDP та Wiegand	Неможливість підключення зчитувачів	Попередній аудит сумісності заліза
Логістичний	Дефіцит компонентів на ринку	Зрив дедлайнів на 2-4 місяці	Закупівля критичних позицій авансом
Експлуатаційний	Високий рівень помилкових відмов	Черги на прохідних, агресія персоналу	Тонке налаштування порогів чутливості
Юридичний	Витік біометричних шаблонів	Судові позови, штрафи GDPR	Шифрування БД та аудит доступу

Зауважимо, що превентивне управління ризиками в IT-безпеці дозволяє знизити ймовірність критичних збоїв на 35% за рахунок впровадження етапу тестування концепції (PoC) перед масштабним розгортанням [114].

10.7.2 Метрики якості та точність ідентифікування

Якість СКУД як IT-продукту оцінюється через набір кількісних показників, які й визначають ефективність її роботи. Найбільш критичними для проєктів із використанням біометрії є показники точності розпізнавання.

Помилковий допуск (FAR) визначає ймовірність того, що система надасть доступ особі, яка не має на це прав. Для об’єктів критичної інфраструктури цей показник має прагнути до нуля (наприклад, 10-6). Натомість помилкова відмова (FRR) вказує на частоту випадків, коли легітимний користувач не може потрапити на об’єкт. Високий FRR суттєво знижує ергономіку системи та створює затримки.

Іншим важливим показником є латентність системи – час від моменту прикладання ідентифікатора до моменту спрацювання виконавчого пристрою. У великих корпоративних мережах швидкість ідентифікації залежить від продуктивності бази даних та пропускної здатності каналів зв’язку. Узагальнення метрик якості наведено в таблиці 10.14

Таблиця 10.14 – Ключові показники якості функціонування СКУД

Назва метрики	Цільові показники	Вплив на бізнес-процес
Помилковий допуск (FAR)	< 0,0001%	Рівень фізичної захищеності об’єкта
Помилкова відмова (FRR)	< 0,1 … 1%	Лояльність персоналу та швидкість проходу
Швидкість ідентифікації	< 0,5 … 0,8 с	Пропускна здатність КПП
Коефіцієнт готовності	> 99,9%	Безперервність бізнес-процесів організації

Відповідно до ДСТУ EN 60839-11-1:2019, якість системи визначається її стійкістю до маніпуляцій та саботажу. Керівник проєкту повинен переконатися у тому, що система логує не лише успішні проходи, а й кожну спробу підбору пароля або фізичного втручання в роботу контролера. Якість проекту прийнято закладати не на етапі монтажу, а на етапі валідації вимог, де визначаються допустимі межі похибок системи [115].

10.7.3 Контроль та забезпечення якості (QA/QC)

Процес забезпечення якості включає регулярне проведення технічних аудитів та стрес-тестування системи. В межах проєкту СКУД це означає імітацію пікових навантажень (наприклад, одночасний прохід великої кількості працівників під час перезмінки) та перевірку роботи системи в умовах відсутності зв’язку з сервером. Контроль якості монтажних робіт здійснюється шляхом вимірювання опору ліній зв’язку та перевірки зусилля утримання електромагнітних замків.

Слід зазначити, що успішне управління ризиками та якістю перетворює СКУД із набору технічних засобів на гарантований сервіс безпеки. Системний підхід до вимірювання KPI та своєчасна реакція на ідентифіковані ризики

дозволяють мінімізувати сукупну вартість володіння системою та забезпечити її стабільну роботу протягом усього життєвого циклу [72].

10.8 Експлуатація та супровід у життєвому циклі СКУД

Завершення фази впровадження СКУД та підписання акта введення в експлуатацію знаменує перехід системи до стадії операційного функціонування, яка є найтривалішою в її життєвому циклі. Управління експлуатацією в проєктах СКУД вимагає трансформації підходу від проектного менеджменту до управління сервісами (ITSM). Оскільки система безпосередньо впливає на безпеку об’єкта та безперервність бізнес-процесів, її супровід базується на чітко визначених угодах про рівень сервісу (SLA), які регламентують надійність, доступність та швидкість відновлення працездатності.

10.8.1 Планування сервісного обслуговування та метрики SLA

Основним інструментом управління експлуатацією є Service Level Agreement (SLA), який встановлює кількісні та якісні показники роботи системи. У проєктах СКУД ключовою метрикою прийнято вважати коефіцієнт готовності (A), який розраховується за наступним виразом:

$$A = MTBF / (MTBF+MTTR), \quad (10.2)$$

де MTBF – середній час між відмовами;

MTTR – середній час відновлення.

Для об’єктів із високими вимогами до безпеки цей показник має складати не менше 99,99%.

Угода про рівень сервісу передбачає класифікацію інцидентів за рівнем критичності. До першої категорії належать події, які призводять до повного блокування центральних прохідних або втрати цілісності бази даних, що вимагає реакції фахівців протягом 1-2 годин. Друга категорія охоплює несправності окремих точок доступу в другорядних приміщеннях, а третя – консультаційні запити або планову заміну ідентифікаторів. Узагальнення параметрів сервісного обслуговування наведено в таблиці 10.15.

Ефективність експлуатації СКУД залежить від наявності запасних частин, інструментів та пристроїв безпосередньо на об’єкті, що дозволяє виконувати вимоги SLA щодо швидкого відновлення критичних вузлів [125].

10.8.2 Превентивне обслуговування та управління ресурсами

На відміну від багатьох IT-систем, СКУД потребує регулярного фізичного обслуговування механічних та електронних компонентів.

Регламентні роботи включають перевірку ємності акумуляторів резервного живлення, чищення оптичних давачів турнікетів, перевірку зусилля утримання електромагнітних замків та оновлення прошивок контролерів. Програмна частина експлуатації передбачає регулярне резервне копіювання бази даних, дефрагментацію індексів SQL-сервера та аудит прав доступу користувачів.

Таблиця 10.15 – Структура рівнів підтримки (SLA) у проектах СКУД

Рівень критичності	Опис інциденту	Час реакції (SLA)	Пріоритет відновлення
Критичний (P1)	Повна відмова сервера або блокування евакуаційних шляхів	До 2 годин	Негайне (24/7)
Високий (P2)	Вихід з ладу контролера на 4–8 точок проходу	Від 4 до 8 годин	Протягом робочого дня
Середній (P3)	Поломка окремого зчитувача або дотягувача дверей	До 24 годин	Плановий виїзд
Низький (P4)	Програмні звіти, додавання нових користувачів	До 48 годин	За графіком

Зауважимо, що важливим аспектом є управління життєвим циклом обладнання. Кожен компонент СКУД має свій термін експлуатації (наприклад, 5 років для акумуляторів, 7 … 10 років для контролерів). Керівник проєкту на етапі експлуатації повинен планувати бюджет на поетапну заміну морально та фізично застарілих елементів, щоб уникнути лавиноподібного зростання відмов. Узагальнення витрат на експлуатацію дозволяє оптимізувати сукупну вартість володіння системою [72].

10.8.3 Масштабування системи та технологічна модернізація

Під час розвитку організації виникає потреба в масштабуванні СКУД, яка проходить за двома сценаріями: горизонтальним (додавання нових ТД) та вертикальним (підвищення інтелектуальних можливостей існуючої системи). Сучасні ІТ-проєкти СКУД орієнтовані на використання хмарних технологій, що дозволяє централізовано керувати доступом у територіально розподілених філіях без розгортання локальних серверів у кожному офісі.

Технологічна модернізація передбачає перехід на більш безпечні методи ідентифікації, наприклад, заміну застарілих RFID-карт на мобільні ідентифікатори або біометричне розпізнавання обличь. Це потребує не лише заміни зчитувачів, а й оновлення серверного ПЗ та перегляду політик безпеки. Параметри успішного масштабування системи наведено в таблиці 10.16.

Як бачимо, сучасні підприємства все частіше обирають гібридні моделі експлуатації, де критична інфраструктура безпеки залишається локальною, а

аналітичні модулі та облік робочого часу виносяться в хмару для зручності віддаленого доступу менеджменту [113].

Таблиця 10.16 – Стратегії масштабування та оновлення СКУД

Напрям розвитку	Технічна реалізація	Перевага для організації
Горизонтальне масштабування	Додавання IP-контролерів у нових зонах	Єдиний контур безпеки для всіх філій
Технологічне оновлення	Перехід з Wiegand на OSDP	Підвищення кіберстійкості системи
Міграція в хмару (ACaaS)	Перенос бази даних на зовнішні хости	Зниження витрат на власну інфраструктуру
Функціональне розширення	Інтеграція з системами відеоаналітики	Автоматизація детекції інцидентів

Таким чином: експлуатація та супровід є фазою, на якій підтверджується реальна окупність проєкту СКУД. Системний підхід до управління сервісом через механізми SLA, регулярне превентивне обслуговування та готовність до технологічного масштабування забезпечують довговічність інвестицій замовника. Успішне управління життєвим циклом системи дозволяє не лише підтримувати високий рівень безпеки, а й адаптувати СКУД до постійно мінливих потреб бізнесу та нових кіберзагроз.

Контрольні запитання

1. На якому етапі життєвого циклу проєкту закладається якість системи?
2. Назвіть ключові відмінності параметрів обслуговування СКУД між критичним рівнем (P1) та низьким рівнем (P4).
3. У чому полягає відмінність життєвого циклу СКУД від розробки програмного забезпечення?
4. У чому полягає критична вразливість протоколу Wiegand у порівнянні з стандартом OSDP?
5. У чому полягає основна мета створення комплексних інтегрованих систем безпеки?
6. Чому для взаємодії СКУД із охоронно-пожежною сигналізацією обов’язковою є реалізація саме апаратного рівня інтегрування?
7. У чому полягає різниця між горизонтальним масштабуванням та технологічним оновленням СКУД?
8. У чому полягає різниця між функціональними та нефункціональними вимогами, які висуваються до СКУД?
9. У чому полягає суть принципу «мінімальних привілеїв» та «системного зміцнення» в СКУД?

10. Чому під час впровадження проєктів СКУД рекомендовано використовувати гібридні методології?

11. Чому під час переходу СКУД до стадії операційного функціонування рекомендують трансформувати підхід від проєктного менеджменту до управління сервісами?

12. Як модуль обліку робочого часу в СКУД допомагає виявляти аномалії у продуктивності розробників?

13. Яка технологія ідентифікації здатна забезпечити максимальну стійкість до копіювання?

14. Який нормативний документ є ключовим орієнтиром під час аналізу вимог до рівнів захисту об’єкта?

15. Яким чином інтегрування програмного забезпечення СКУД у загальну систему управління IT-підприємством впливає на фінансові показники проєктів?

16. Яким чином інтегрування СКУД з корпоративними системами впливає на ефективність проєкту?

17. Які заходи фізичного та програмного превентивного обслуговування проводять для забезпечення стабільної роботи СКУД?

18. Які категорії ризиків виділяють під час впровадженні СКУД?

19. Які особливості децентралізованої архітектури СКУД у порівнянні з централізованою?

20. Які паралельні процеси включає у себе фаза реалізації проєкту?

21. Які переваги надає модель ACaaS для територіально розподілених команд у порівнянні з локальними рішеннями?

22. Які протоколи та методи шифрування рекомендовано використовувати на різних рівнях ієрархії СКУД для забезпечення цілісності системи?

23. Які рівні автономності необхідно забезпечувати під час проєктування СКУД?

24. Які специфічні заходи кібербезпеки та захисту даних реалізовують в програмному забезпеченні СКУД?

25. Які технічні методи використовуються для обміну даними між СКУД та корпоративними IT-системами?

26. Які технічні помилки під час монтажу та пусконалагоджувальних робіт в СКУД можуть призвести до появи прихованих дефектів?

27. Яку роль відіграє предиктивна аналітика у сучасних СКУД для управління персоналом проєкту?

28. Яку роль відіграє створення ізольованого мережевого сегмента у мінімізації ризиків для корпоративної мережі та СКУД?

ПЕРЕЛІК ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. 2012/0011(COD). Personal Data Protection: Processing and Free Movement of Data (General Data Protection Regulation). URL: https://surl.li/rwlihu (дата звернення: 18.04.2026).
2. 2D Codes Explained: What’s the Difference Between a Data Matrix Code and a QR Code? URL: https://www.domino-printing.com/en/blog/2021/the-difference-between-a-data-matrix-code-and-a-qr-code (дата звернення: 18.04.2026).
3. Access Control Maintenance & Troubleshooting Guide. URL: https://veritech-security.com/access-control-maintenance-and-troubleshooting/ (дата звернення: 18.04.2026).
4. Access Control System Failure Risks and Troubleshooting for Property Managers. URL: https://surl.li/hcprli (дата звернення: 18.04.2026).
5. Access Control Systems : Security, Identity Management and Trust Models. URL: https://surl.li/pophrl (дата звернення 18.04.2026).
6. Best Guide to Power Over Ethernet. URL: https://www.phihong.com/best-guide-to-power-over-ethernet/ (дата звернення: 18.04.2026).
7. Boddu Raghu. SAP Access Control. Quincy : SAP PRESS, 2023. 695 p.
8. Brian Rhodes. Access Control. URL: https://surl.lu/xvxphm (дата звернення 18.04.2026).
9. Bunsen, Auston. Decoding the Wiegand Protocol. URL: https://surl.li/zhtsmx (дата звернення: 18.04.2026).
10. Cepeda, Raul Jr. NFC vs BLE Credentials: Determine which is Right for You. URL: https://www.rfideas.com/about-us/blog/nfc-vs-ble-credentials-determine-which-right-you (дата звернення: 18.04.2026).
11. Chadha, Aarshdeep Singh. Designing a Scalable Database System for High-Volume Data with Real-Time Analytics. URL: https://surl.li/ongxwp (дата звернення: 18.04.2026).
12. CMMC і біометрична автентифікація. URL: https://surl.lu/fbywey (дата звернення: 18.04.2026).
13. Comprehensive Review of the Palm Vein Unlocking Technology. URL: https://www.eufy.com/blogs/smart-lock/palm-vein-unlocking-technology (дата звернення: 18.04.2026).
14. CVE-2025-1960: Authentication Bypass Vulnerability. URL: https://surl.li/ejzzkf (дата звернення: 18.04.2026).
15. Data protection basics. URL: https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-basics_en (дата звернення: 18.04.2026).
16. EEVblog® Electronics Community Forum: RS485 vs Ethernet. URL: https://surl.lt/canrgu (дата звернення: 18.04.2026).

17. EMS vs BMS: Differences and integration explained. URL: https://tibo.energy/blog/ems-vs-bms/ (дата звернення: 18.04.2026).

18. Enabling Global Antipassback on Access Manager Roles. URL: https://surl.li/yvnzri (дата звернення: 18.04.2026).

19. Energy Harvesting with the Wiegand Effect. URL: https://surl.li/jflyiw (дата звернення: 18.04.2026).

20. ESP Key RFID Wiegand Interception Tool. URL: https://labs.ksec.co.uk/product/esp-rfid-tool/ (дата звернення: 18.04.2026).

21. GDPR та захист персональних даних: чек-лист для українського бізнесу. URL: https://surl.li/vbuyrm (дата звернення: 18.04.2026).

22. Genetec access control solutions : Access control that goes beyond security. URL: https://www.genetec.com/products/access-control (дата звернення: 18.04.2026).

23. GRADE 4 – The Highest Level of Security in Access Control. RACS 5 with a Compliance Certificate. URL: https://www.roger.pl/en/blog/blog-news/grade-4-the-highest-level-of-security-in-access-control-racs-5-with-a-compliance-certificate (дата звернення: 18.04.2026).

24. Graph-Based Access Control. URL: https://surl.lt/xxsdna (дата звернення: 18.04.2026).

25. Harold F. Tipton, Micki Krause. Information Security Management : Handbook. URL: https://surl.lu/oqhegu (дата звернення 18.04.2026).

26. IEC 60839-11-5. Alarm and electronic security systems – Part 11-5: Electronic access control systems – Open supervised device protocol (OSDP). URL: https://surl.li/quupci (дата звернення: 18.04.2026).

27. Islas, Fernando Aguilar. Graph-Based Security & Entitlements: Transforming Access Control for the Modern Enterprise. URL: https://surl.li/gebsek (дата звернення: 18.04.2026).

28. ISO/IEC 14443-1:2018(E). Cards and Security Devices for Personal Identification – Contactless Proximity Objects – Part 1: Physical Characteristics. URL: https://surl.li/ncpojd (дата звернення: 18.04.2026).

29. ISO/IEC 15693-1:2018(E). Cards and Security Devices for Personal Identification – Contactless Vicinity Objects – Part 1: Physical Characteristics. URL: https://surl.li/yhuhhd (дата звернення: 18.04.2026).

30. ISO/IEC 16022. Information Technology – Automatic Identification and Data Capture Techniques – Data Matrix Bar Code Symbology Specification. URL: https://surl.li/bejkmo (дата звернення: 18.04.2026).

31. ISO/IEC 18004. Information Technology – Automatic Identification and Data Capture Techniques – QR Code Bar Code Symbology Specification. URL: https://surl.li/vjvoti (дата звернення: 18.04.2026).

32. ISO/IEC 25000 – Software Quality Requirements and Evaluation. URL: https://surl.li/qzytyo (дата звернення: 18.04.2026).

33. Khan, W., Kumar, T., Zhang, C., Raj, K., Roy, A. M., & Luo, B. (2023). SQL and NoSQL Database Software Architecture Performance Analysis and Assessments – A Systematic Literature Review. Big Data and Cognitive Computing, 7(2), 97. https://doi.org/10.3390/bdcc7020097

34. Kirichenko, Natalia. UKRAINE: Data Protection Laws of the World. URL: https://surl.li/nelycg (дата звернення: 18.04.2026).

35. Kramarz, Jakub. The Tick – The Next Evolution in RFID Security Testing! URL: https://surl.li/ivbsnk (дата звернення: 18.04.2026).

36. Kris Hermans. Mastering Access Control : A Comprehensive Guide to Learn Access Control. Traverse City : Independently published, 2023. 393 p.

37. Lin, G., Casillas, A., Sheng, M., & Granderson, J. (2023). Performance Evaluation of an Occupancy-Based HVAC Control System in an Office Building. Energies, 16(20), 7088. https://doi.org/10.3390/en16207088

38. Locks and Keys – A Brief History. Here's How They Have Evolved over the Years. URL: https://www.lockrite.org/blog/locks-and-keys-a-brief-history-heres-how-they-have-evolved-over-the-years/ (дата звернення: 18.04.2026).

39. Long, Y., Bao, Y., & Zeng, L. (2024). Research on Edge-Computing-Based High Concurrency and Availability «Cloud, Edge, and End Collaboration» Substation Operation Support System and Applications. Energies, 17(1), 194. https://doi.org/10.3390/en17010194

40. Matej Csányi. Access Control in Operating Systems. URL: https://is.muni.cz/th/uny2u/ xcsanyi_bc.pdf (дата звернення 18.04.2026).

41. Mercer, Silas. Bluetooth vs NFC Mobile Access: Which Mobile Credential Tech is More Convenient? URL: https://ngteco.com/blogs/workforce-insights/bluetooth-vs-nfc-mobile-access (дата звернення: 18.04.2026).

42. Mike Chapple. Access Control and Identity Management. Burlington : World Headquarters Jones & Bartlett Learning, 2021. 376 p.

43. Multiple Critical Vulnerabilities in dormakaba Access Manager. URL: https://surl.li/ccrasm (дата звернення: 18.04.2026).

44. Open Supervised Device Protocol (OSDP). URL: https://surl.li/hswmuf (дата звернення: 18.04.2026).

45. Overview of Power over Ethernet (PoE) Technology. URL: https://tripplite.eaton.com/pages/overview-of-power-over-ethernet-technology (дата звернення: 18.04.2026).

46. Palm Vein Recognition Device Access Control Innovative uses Strengths. URL: https://gdsinmar.com/info-detail/palm-vein-recognition-device-access-control-innovative-uses-strengths (дата звернення: 18.04.2026).

47. Process personal data lawfully. URL: https://surl.lt/nhvlmw (дата звернення: 18.04.2026).

48. QR Code vs Data Matrix Code – What is the Difference? URL: https://surl.li/rvitfr (дата звернення: 18.04.2026).

49. Technical White Paper: RS-485 Basics Series. URL: https://surl.li/khqcuk (дата звернення: 18.04.2026).

50. The Evolution of Key Control: From Ancient Artifacts to Modern Systems. URL: https://www.handytrac.com/evolution-of-key-management/ (дата звернення: 18.04.2026).

51. The Evolution of Locks: From Ancient Times to Modern Day. URL: https://www.pagesecurity.co.uk/blog/the-evolution-of-locks-from-ancient-times-to-modern-day/ (дата звернення: 18.04.2026).

52. The First Burglar Alarm. URL: https://waynealarm.com/antiques-corner/the-first-burglar-alarm/ (дата звернення: 18.04.2026).

53. The Future of Access Control In 2026. URL: https://surl.li/lzozpl (дата звернення: 18.04.2026).

54. The History of Security Systems – From Antiquity to Apps. URL: https://lloydsecurity.com/history-security-systems/ (дата звернення: 18.04.2026).

55. The History of the Alarm System. URL: https://surl.li/illqlg (дата звернення: 18.04.2026).

56. The ISO/IEC 25000 series of standards. URL: https://surl.li/lubwkc (дата звернення: 18.04.2026).

57. The Transport Layer Security (TLS) Protocol Version 1.3. URL: https://datatracker.ietf.org/doc/html/rfc8446 (дата звернення: 18.04.2026).

58. Thomas Norman. Electronic Access Control. URL: https://surl.li/oybgwe (дата звернення 18.04.2026).

59. Understanding Card Data Formats. URL: https://surl.li/tldhpq (дата звернення: 18.04.2026).

60. Understanding ISO/IEC 25010: A Comprehensive Framework for Software Quality Evaluation. URL: https://surl.li/pdukok (дата звернення: 18.04.2026).

61. Understanding the Vulnerabilities of the Standard Wiegand Format. URL: https://surl.li/curale (дата звернення: 18.04.2026).

62. What are Tailgating and Piggybacking Attacks? URL: https://surl.li/ybajzh (дата звернення: 18.04.2026).

63. What is the difference between RS485 and Ethernet? URL: https://surl.li/dipnpj (дата звернення: 18.04.2026).

64. What Security Integrators Need to Know About OSDP. URL: https://surl.li/kwjzml (дата звернення: 18.04.2026).

65. Wiegand in access control: A Kisi guide. URL: https://www.getkisi.com/guides/wiegand (дата звернення: 18.04.2026).

66. Wood, Simon. What is Relationship Based Access Control (ReBAC)? URL: https://surl.lu/uxucps (дата звернення: 18.04.2026).

67. Zuberek, W. M. Petri Nets and Timed Petri Nets: Basic Concepts And Properties. URL: https://memorial.scholaris.ca/server/api/core/bitstreams/4a74a2c2-46e6-43f5-b3c5-fa0f4ff4caca/content (дата звернення: 18.04.2026).

68. Аутентифікація, авторизація та ідентифікація: як не сплутати. URL: https://surl.li/yxejin (дата звернення: 18.04.2026).

69. Біометричні рішення #1 в індустрії. URL: https://surl.li/nnunhx (дата звернення: 18.04.2026).

70. Бурячок В. Л., Толубко В. Б. Інформаційна та кібербезпека: соціотехнічний аспект. Київ : ДУТ, 2021. 252 с.

71. Бутенко Л. І., Шарадкін Д. М. Безперервна біометрична автентифікація користувачів на основі клавіатурного почерку. URL: https://cit.lntu.edu.ua/index.php/cit/article/view/840 (дата звернення: 18.04.2026).

72. Васильєв С. П. Економічне обґрунтування інвестицій в IT-інфраструктуру безпеки. Економіка та менеджмент. Дніпро : В-во ДНУ, 2025. С. 102–110.

73. Види біометричної аутентифікації. URL: https://surl.li/lenznr (дата звернення: 18.04.2026).

74. Все про турнікети: від переваг і особливостей до правильного вибору. URL: https://surl.li/snxfkb (дата звернення: 18.04.2026).

75. Все, що потрібно знати про біометричні рішення контролю доступу. URL: https://surl.li/bxseit (дата звернення: 18.04.2026).

76. Голосова біометрія: що це, як працює та навіщо вона банкам? URL: https://surl.li/rpbigq (дата звернення: 18.04.2026).

77. ДБН В.2.5-56:2014 Системи протипожежного захисту. Зі Зміною №1. [Чинний від 2019-11-01]. Вид. офіц. Київ: ВГО «Український союз пожежної та техногенної безпеки», 2014. 190 с.

78. Довгий С. О., Копійка О. В. IT-інфраструктура як базова складова цифрової трансформації : монографія. Київ : В-во «Юстон», 2023. 458 с.

79. Домофонні ключі. Типи ключів, їх характеристики і переваги. URL: https://surl.li/sujiii (дата звернення: 18.04.2026).

80. Дослідження підпису та почерку. URL: https://surl.li/ponhpk (дата звернення: 18.04.2026).

81. Дрок І. С., Бреславська М. Є., Головатий Д. І. Партнерство поліції та громади: сучасні стратегії безпеки: практ. посіб. Дніпро : Дніпров. держ. ун-т внутр. справ, 2025. 96 с.

82. ДСТУ 2853-94. Програмні засоби ЕОМ. Підготовлення і проведення випробувань. [Чинний від 1996-01-01]. Вид. офіц. Київ : ТОВ «Софтпроект», 1994. 120 с.

83. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. [Чинний від 1996-01-01]. Вид. офіц. Київ : Інститут проблем надійності машин і споруд, 1994. 34 с.

84. ДСТУ 2861-94. Надійність техніки. Аналіз надійності. Основні положення. [Скасовано від 2026-01-01]. Вид. офіц. Київ : Асоціація «Надійність машин та споруд», 1994. 12 с.

85. ДСТУ 3135.0-95. Безпека побутових та аналогічних електричних приладів. Загальні вимоги (ГОСТ 30345.0-95) (IEC 60335-1:1991). [Скасовано від 2026-01-01]. Вид. офіц. Київ: Держспоживстандарт України, 1995. 115 с.

86. ДСТУ 3973-2000. Система розроблення та поставлення продукції на виробництво. Правила виконання науково-дослідних робіт. Загальні положення. [Чинний від 2001-07-01]. Вид. офіц. Київ : ДП «ДБЦ КТ «Мікротек», 2000. 14 с.

87. ДСТУ 4000-2000. Системи тривожної сигналізації охоронні теле(відео) системи і системи контролювання доступу. Терміни та визначення. [Чинний від 2001-07-01]. Вид. офіц. Київ : Міністерство внутрішніх справ України, 2001. 23 с.

88. ДСТУ 7237:2011. Система стандартів безпеки праці. Електробезпека. Загальні вимоги та номенклатура видів захисту. [Чинний від 2011-08-01]. Вид. офіц. Київ : Держспоживстандарт України, 2011. 18 с.

89. ДСТУ 8280:2015. Вироби електротехнічні. Методи випробовування на тривкість до дії зовнішніх кліматичних чинників. [Чинний від 2017-07-01]. Вид. офіц. Київ : ДП «ДСЦ «ЕЛХІМ», 2015. 40 с.

90. ДСТУ 8828:2019. Пожежна безпека. Загальні положення. [Чинний від 2020-01-01]. Вид. офіц. Київ : ТК25 «Пожежна безпека та протипожежна техніка», 2019. 30 с.

91. ДСТУ EN 50130-4:2017. Системи тривожної сигналізації. Частина 4. Електромагнітна сумісність. Стандарт на однорідну продукцію. Вимоги щодо несприйнятливості для складників систем тривожної сигналізації про пожежу, проникнення, напад, суспільну небезпеку та систем відеоспостереження і контролювання доступу (EN 50130-4:2011; A1:2014, IDT). [Чинний від 2019-01-01]. Вид. офіц. Київ : ТК22 «Електромагнітна сумісність та стійкість радіоелектронних, електронних та електротехнічних засобів», 2017. 28 с.

92. ДСТУ EN 50133-2-1:2012. Системи тривожної сигналізації. Системи контролювання доступу охоронного призначення. Частина 2-1. Загальні вимоги

до складників систем (EN 50133-2-1:2000, IDT). [Чинний від 2013-07-01]. Вид. офіц. Київ : ТК 165 «Індустрія безпеки», 2013. 9 с.

93. ДСТУ EN 55014-1:2019. Електромагнітна сумісність. Вимоги до побутових електроприладів, електричних інструментів та аналогічної апаратури. Частина 1. Емісія завад (EN 55014-1:2017, IDT; CISPR 14-1:2016, IDT). [Чинний від 2019-09-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2017. 195 с.

94. ДСТУEN 60065:2019. Аудіо-, відео- та аналогічна електронна апаратура. Вимоги щодо безпеки (EN 60065:2002, IDT; IEC 60065:2001, MOD). Зі змінами та поправкою. [Чинний від 2019-07-15]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2019. 315 с.

95. ДСТУ EN 60068-2-57:2022. Випробування на вплив навколишнього середовища. Частина 2-57. Випробування. Випробування Ff. Вібрація. Історія та метод синусоїдації (EN 60068-2-57:2013, IDT; IEC 60068-2-57:2013, IDT). [Чинний від 2023-13-31]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2022. 44 с.

96. ДСТУ EN 60529:2018. Ступені захисту, забезпечувані кожухами (Код IP) (EN 60529:1991; A1:2000; A2:2013; AC:1993; AC:2016, IDT; IEC 60529:1989; A1:1999; A2:2013; Cor 2:2015, IDT). [Чинний від 2020-07-01]. Вид. офіц. Київ : ТК135 «Безпека промислової продукції та засоби індивідуального захисту працюючих», 2018. 46 с.

97. ДСТУ EN 60839-11-1:2014. Системи тривожної сигналізації та електронні системи безпеки. Частина 11-1. Електронні системи контролювання доступу. Вимоги до системи та її складників (EN 60839-11-1:2013; EN 60839-11-1:2013/AC:2013, IDT). [Чинний від 2017-08-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2017. 65 с.

98. ДСТУ EN 60839-11-2:2017. Системи тривожної сигналізації та електронні системи безпеки. Частина 11-2. Електронні системи контролювання доступу. Правила застосування (EN 60839-11-2:2015, IDT). [Чинний від 2017-08-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2017. 62 с.

99. ДСТУ EN 60839-11-31:2017. Системи тривожної сигналізації та електронні системи безпеки. Частина 11-31. Електронні системи контролювання доступу. Основний протокол сумісності на основі веб-сервісів (EN 60839-11-31:2017, IDT). [Чинний від 2017-08-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2017. 104 с.

100. ДСТУ EN 61000. Електромагнітна сумісність. URL: https://surl.lu/grlifw (дата звернення: 18.04.2026).

101. ДСТУ EN IEC 55014-2:2022. Електромагнітна сумісність. Вимоги до побутових приладів, електричних інструментів і подібних пристроїв. Частина 2. Захищеність. Стандарт сімейства продуктів (EN IEC 55014-2:2021,

IDT; CISPR 14-2:2020, IDT). [Чинний від 2023-12-28]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2022. 32 с.

102. ДСТУ EN IEC 60079-0:2019. Вибухонебезпечні середовища. Частина 0. Устаткування. Загальні вимоги (EN IEC 60079-0:2018, IDT; IEC 60079-0:2017, IDT). [Чинний від 2020-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2019. 180 с.

103. ДСТУ EN IEC 60839-11-33:2022. Системи тривожної сигналізації та електронні системи безпеки. Частина 11-33. Електронні системи контролю доступу. Конфігурація контролювання доступу на основі веб-сервісів (EN IEC 60839-11-33:2021, IDT; IEC 60839-11-33:2021, IDT). [Чинний від 2023-12-31]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2023. 70 с.

104. ДСТУ IEC 60839-11-32:2017. Системи тривожної сигналізації та електронні системи безпеки. Частина 11-32. Електронні системи контролювання доступу. Моніторинг контролювання доступу на основі веб-сервісів (IEC 60839-11-32:2016, IDT). [Чинний від 2017-12-15]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2017. 142 с.

105. ДСТУ ISO/IEC 14443-1:2008. Картки ідентифікаційні. Картки на інтегрованих мікросхемах безконтактні. Картки близької взаємодії. Частина 1. Фізичні характеристики (ISO/IEC 14443-1:2000, IDT). [Чинний від 2010-01-01]. Вид. офіц. Київ : ТК105 «Банківські та фінансові системи і технології», 2013. 10 с.

106. ДСТУ ISO/IEC 25010:2025. Інженерія систем і програмних засобів. Вимоги до якості систем і програмних засобів та її оцінювання (SQuaRE). Модель якості продукту (ISO/IEC 25010:2023, IDT). [Чинний від 2025-12-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2025. 50 с.

107. Закон України «Про критичну інфраструктуру». URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 18.04.2026).

108. Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами : посібник. URL: https://surl.lu/dctgfk (дата звернення: 18.04.2026).

109. Кайдик О. Л., Терлецький Т. В., Пугач С. О., Угрин Д. І., Артеменко О. І. Моделювання та підвищення надійності ідентифікації суб’єктів доступу в СКУД на основі гібридних PCA-алгоритмів. *Комп’ютерно-інтегровані технології: освіта, наука, виробництво*, 2025. №61. С. 82–90. URL: https://doi.org/10.36910/6775-2524-0560-2025-61-12.

110. Кайдик О. Л., Терлецький Т. В. Системи контролю та управління доступом : конспект лекцій. URL: https://surl.lu/mrxcvi (дата звернення: 18.04.2026).

111. Контроль доступу на основі ролей (Role-Based Access Control або RBAC) у пайплайні CI/CD: DevSecOps. URL: https://surl.lt/phcefj (дата звернення: 18.04.2026).

112. Лавренчук С. В., Кайдик О. Л., Мельник К. В., Конкевич Л. М., Лук'янчук Ю. В. Гібридна SQL/NoSQL архітектура для оптимізації продуктивності IoT-моніторингу якості повітря. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*, 2025. №61. С. 112–118. URL: https://doi.org/10.36910/6775-2524-0560-2025-61-16.

113. Мельник Ю. В. Цифрова трансформація бізнес-процесів: економічний аспект. Львів : В-во Львівської політехніки, 2025. 210 с.

114. Павлов О. Г. Менеджмент проектів у сфері інформаційних технологій. Київ : Видавничий дім «Кондор», 2023. 312 с.

115. Петренко І. М. Методологія управління ІТ-проектами в галузі безпеки. *Праці ЛНТУ*. Луцьк : ЛНТУ, 2026. С. 89–95.

116. Предиктивна аналітика. URL: https://surl.li/yuvmea (дата звернення: 18.04.2026).

117. Предиктивна аналітика: ключові переваги та перспективи ринку. URL: https://surl.li/ngvwck (дата звернення: 18.04.2026).

118. Про затвердження Методики проведення обстеження та оформлення його результатів. Наказ №144 від 06.08.2022. URL: https://ips.ligazakon.net/document/re38234?an=92 (дата звернення: 18.04.2026).

119. Про захист персональних даних : Закон України № 2297-VI від 12.02.2025 р. URL: https://surl.li/btatjz (дата звернення: 18.04.2026).

120. Про захист персональних даних : Проєкт Закону України №8153 від 25.10.2022 р. URL: https://surl.li/upsmsl (дата звернення: 18.04.2026).

121. Система контролю доступу (СКУД). Принцип дії, склад, особливості застосування. URL: https://surl.li/rmroxs (дата звернення: 18.04.2026).

122. Смарт-карти у повсякденності або як вони спрощують рутинні завдання. URL: https://surl.li/xyjppb (дата звернення: 18.04.2026).

123. Соціальна інженерія. URL: https://surl.li/qszetf (дата звернення: 18.04.2026).

124. Сучасні засоби обмеження доступу та система керування відвідувачами. URL: https://surl.li/ppdwnl (дата звернення: 18.04.2026).

125. Ткаченко В. М. Стандартизація систем безпеки в Україні: шлях до європейської інтеграції. *Технічні науки та технології*. Чернігів : ЧНТУ, 2023. С. 142–150.

126. Ткачов В. В. Сучасні інфокомунікаційні системи та мережі: протоколи та технології. Запоріжжя : НУ «Запорізька політехніка», 2022. 80 с.

127. У Китаї створили систему розпізнавання людей за ходою. URL: https://ukr.media/science/378491/ (дата звернення: 18.04.2026).

128. Циплинський Ю. Порядок віднесення об’єктів до об’єктів критичної інфраструктури. Вимоги до кіберзахисту об’єктів критичної інфраструктури. URL: https://surl.li/twnuvv (дата звернення: 18.04.2026).

129. Що таке система контролю та управління доступом (СКУД) і для чого вона потрібна? URL: https://journal.vencon.ua/ua/sistema-kontrolya-i-upravleniya-dostupom-prostymi-slovami (дата звернення: 18.04.2026).

130. Що таке СКУД і як це працює? URL: https://surl.li/ixoqch (дата звернення: 18.04.2026).

131. Що таке смарт-картка? URL: https://surl.li/ggqjen (дата звернення: 18.04.2026).

132. Що таке технологія розпізнавання райдужної оболонки ока? URL: https://surl.li/ayfcpe (дата звернення: 18.04.2026).

133. Що таке хмарні технології? Переваги та недоліки хмарних сервісів. URL: https://edin.ua/shho-take-xmarni-texnologi%D1%97-i-navishho-voni-potribni/ (дата звернення: 18.04.2026).

134. Як працює система контролю доступу (СКД або СКУД)? URL: https://surl.li/xqidjj (дата звернення: 18.04.2026).

135. Як працює технологія розпізнавання відбитків пальців? URL: https://surl.lu/rffewd (дата звернення: 18.04.2026).

Кайдик О.Л., Терлецький Т. В., Угрин Д. І., Кондіус І. С. Системи контрою та управління доступом : навч. посіб. для студентів технічних спеціальностей. Луцьк: ЛНТУ, 2026. 240 с.

Укладачі: авторський колектив за загальною редакцією Олега КАЙДИКА.

Технічне корегування: Олег КАЙДИК, Тарас ТЕРЛЕЦЬКИЙ.

Підписано до друку __ травня 2026 р.
Формат 60х90/8. Папір офсетний. Гарн. Таймс.
Ум. друк. арк. 15,00. Замовлення ___.
Наклад 200 прим.

Відділ іміджу та промоцій ЛНТУ
вул. Львівська, 75, м. Луцьк, 43018; rvv@lntu.edu.ua
Свідоцтво Державного комітету телебачення
та радіомовлення України серія ДК№4123 від 28.07.2011 р.