МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Луцький національний технічний університет

СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 (F) Інформаційні технології спеціальності 126 (F6) Інформаційні системи та технології денної та заочної форм навчання

Луцьк 2025

УДК 681.52:004.056
С34

Рекомендовано до видання вченою радою факультету комп'ютерних та інформаційних технологій ЛНТУ, протокол № ___ від _____ 2025 року.

Голова Вченої ради факультету КІТ _____ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки _____ Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № ___ від _____ 2025 року.

Укладачі: _____ Олег КАЙДИК, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

_____ Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та безпеки ЛНТУ

_____ Анатолій ТКАЧУК, кандидат технічних наук, доцент кафедри електроніки та телекомунікацій ЛНТУ

Рецензент: _____ Роман ЧУБАЙ, інженер-проектувальник 1 категорії ТОВ «Єврофест»

Відповідальний за випуск: _____ Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та безпеки ЛНТУ

С34 Системи контролю та управління доступом: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 (F) Інформаційні технології спеціальності 126 (F6) Інформаційні системи та технології денної та заочної форм навчання / уклад. О. Л. Кайдик, Т. В. Терлецький, А. А. Ткачук. Луцьк : ЛНТУ, 2025. 132 с.

У пропонованому виданні міститься сім лекцій до курсу «Системи контролю та управління доступом».

Конспект лекцій спрямовано на розвиток критичного мислення у здобувачів освіти та допомагає не лише узагальнити і структурувати різнопланови матеріал для полегшення його засвоєння, але й поглибити розуміння концепції безпеки, функціонування та інтеграції систем контролю та управління доступом

ВСТУП

В умовах стрімкого розвитку інформаційних технологій та зростання загроз несанкціонованого доступу до матеріальних та нематеріальних активів, інженерно-технічна захист об'єктів набуває критичного значення. Одним із найбільш ефективних й комплексних підходів до вирішення цієї задачі є використання систем контролю та управління доступом (СКУД).

СКУД являє собою сукупність апаратних та програмних засобів, спроектованих для централізованого або локального керування проходом людей, транспорту та інших об'єктів на територію, у будівлі, на окремі поверхи, у приміщення та зони з обмеженим доступом. Правильне проєктування та використання СКУД є фундаментом у забезпеченні безпеки будь-якого сучасного об'єкта – від промислових підприємств і фінансових установ до адміністративних будівель та центрів обробки даних.

Справжня ефективність СКУД досягається завдяки її здатності до спільної роботи з іншими інженерними системами безпеки: охоронно-пожежна сигналізація; системи відеонагляду та системи життєзабезпечення.

Конспект лекцій з курсу «Системи контролю та управління доступом» є важливим навчально-методичним ресурсом, який систематизує та інтегрує ключову інформацію, зібрану із широкого кола першоджерел, стандартів та практичних рекомендацій. Його метою є надання здобувачам освіти, які навчаються за освітньою програмою «Інформаційні системи та технології охорони і безпеки», цілісного розуміння принципів проєктування, архітектури, апаратного та програмного забезпечення СКУД, а також сформувати у них необхідні компетентності.

ЗМІСТ

Сторінка

ЗМІСТОВНИЙ МОДУЛЬ 1. Вступ до систем контролю та управління доступом

ТЕМА 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА СКУД

План:

1.1 Основні поняття, термінологія та визначення системи контролю та управління доступом.

1.2 Критерії оцінювання СКУД та їх класифікація.

1.3 Вимоги, які висуваються до СКУД.

1.1 Основні поняття, термінологія та визначення системи контролю та управління доступом

В загальному випадку, система контролю та управління доступом (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.

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.

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.

Верифікація – порівняння ідентичності двох різних суб'єктів доступу.

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

Процедура ідентифікації, як правило, складається із наступних етапів:

– виявлення та зчитування ІО;

– порівняння виявленого ІО 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.

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. 1.1).

Рисунок 1.1 – 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 магазину, 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.

Точка доступу (ТД) – частина об'єкта, яка обладнана відповідними технічним засобами, у якій здійснюють контроль та управління доступом.

Можливість того або іншого суб'єкта/об'єкта переміщуватись через точки доступу визначаються рівнем його доступу. При цьому 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 окремовзятого СД/ОД.

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.

1.2 Критерії оцінювання СКУД та їх класифікація

Критеріями оцінювання СКУД прийнято вважати як основні технічні характеристики, так і її функціональні можливості.

До основних технічних характеристик системи відносять:

- рівень ідентифікації;
- кількість контрольованих зон (місць);
- пропускна здатність;
- кількість користувачів;
- умови експлуатації.

За рівнем ідентифікації доступу СКУД поділяють на:

- однорівневі – ідентифікація здійснюється за однією із ознак (QR-код);
- багаторівневі – ідентифікація здійснюється за декількома ознаками (RIF-мітка та біометрія).

За кількістю контрольованих зон (місць) СКУД поділяють на:

– малої місткості (до 16);

– середньої місткості (від 16 до 64);

– великої місткості (понад 64).

За умовами експлуатації СКУД поділяють на:

– системи для роботи в закритих приміщеннях;

– системи для роботи закритих неопалюваних приміщеннях;

– системи для роботи під навісом на вулиці в умовах помірного холодного клімату;

– системи для роботи на вулиці в умовах помірного холодного клімату;

– системи для роботи за особливих умов (підвищена вологість, запиленість, вібрації тощо).

До основних функціональних можливостей необхідно віднести:

– можливість оперативного перепрограмування;

– схемно-технічний та програмний захист від вандалізму й саботажу;

– високий рівень секретності, імітаційної стійкості й криптозахисту;

– автоматична ідентифікація за ознаками, які властиві лише для СД;

– розмежування повноважень співробітників і відвідувачів за доступом в приміщення та на об’єкт в цілому;

– надійне механічне замикання контрольованих місць з можливістю аварійного ручного відкриття;

– автоматичний збір та аналіз даних;

– вибірковий друк даних.

За технічними характеристиками та функціональними можливостями СКУД умовно поділяють на чотири класи (табл. 1.1).

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

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.

Таблиця 1.1 – Класифікація СКУД

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	На об'єктах, де необхідним є лише обмеження доступу сторонніх осіб (функція замка)
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 (відкриття/закриття)	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
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

Кінець таблиці 1.1

1	2	3	4
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 інтегрованих системах охорони та інтегрованих системах безпеки та управління системами життєзабезпечення

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:

– 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).

1.3 Вимоги, які висуваються до СКУД

Як уже зазначалось СКУД призначені як для забезпечення санкціонованого входу до зон обмеженого доступу і виходу з них шляхом ідентифікації особи за комбінацією різних ознак, так і для запобігання несанкціонованого проходу до них.

Відповідно до діючих нормативних документів СКУД формують: пристрої перешкоджаючі керовані (ППК), які входять до складу загороджувальних конструкцій та виконавчих пристроїв; пристрої для введення ідентифікаційних ознак (ПВІО), які входять до складу зчитувачів та ідентифікаторів; пристроїв управління (ПУ), які входять до складі апаратних та програмних засобів.

Зчитувачами та ППК зазвичай обладнують головний та службові входи; контрольовано-перепускні пункти (КПП); приміщення, у яких зосереджено матеріальні цінності та інші приміщення за рішенням відповідальних керівників.

Пропуск СД до контрольованої зони через пункти контролю доступу необхідно здійснювати в будівлю та службові приміщення – за однією ознакою,

а входи в зони обмеженого доступу (сховища цінностей, сейфові кімнати, кімнати зберігання зброї) – не менше ніж за двома ідентифікаційними ознаками.

На практиці СКУД повинна забезпечувати виконання наступних функцій:

– 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.

У тих контрольованих зонах, де необхідним є контроль збереження предметів, слід встановлювати СКУД, яка контролюватиме несанкціоноване їх винесення з охоронюваних приміщень/будівель за спеціальними ідентифікаційними мітками.

На практиці ППК, до складу яких входять виконавчі пристрої, забезпечують:

– часткове або повне перекриття пройому проходу;
– автоматичне та ручне (за умови аварійної ситуації) відкривання;
– блокування СД/ОД всередині ППК (прохідні кабіни, шлюзи тощо);
– необхідну пропускну здатність.

Зчитувачі ПВІО повинні забезпечувати:

– зчитування ідентифікаційної ознаки із наданого ідентифікатора;

– порівняння введеної ідентифікаційної ознаки із тією, яка зберігається в пам'яті або БД пристрою управління;

– формування сигналу на відкривання ППК при ідентифікації СД/ОД;

– обмін інформацією із ПУ.

Слід пам'ятати, що пристрої для введення ідентифікаційних ознак мають бути захищеними від маніпулювання шляхом перебору або підбору ідентифікаційних ознак.

Ідентифікатори ПВІО мають забезпечувати зберігання ідентифікаційної ознаки протягом усього терміну експлуатації для ідентифікаторів без вбудованих елементів електроживлення і не менше 3 років – для ідентифікаторів із вбудованими елементами електроживлення. При цьому, конструкція, зовнішній вигляд та написи на ідентифікаторі або зчитувачі не повинні нести інформацію про застосовувані коди.

Пристрої управління забезпечують:

– прийом інформації від ПВІО, її оброблення, відображення в заданому вигляді та формування сигналів управління ППК;

– ведення бази даних СД/ОД контрольованої зони з можливістю задання характеристик їх доступу (коду, тимчасового інтервалу доступу, рівня доступу тощо);

– ведення електронного журналу реєстрації проходів СД/ОД через точки доступу;

– пріоритетне виведення інформації про тривожні ситуації в точках доступу;

– контроль справності та стану ППК, ПВІО та ліній зв'язку між ними.

Конструктивно СКУД будуються за модульним принципом, що дозволяє забезпечити:

– взаємозамінність змінних однотипних технічних засобів;

– зручність технічного обслуговування та експлуатації, а також ремонтопридатність;

– виключення можливості несанкціонованого доступу до елементів управління;

– санкціонований доступ до всіх елементів, вузлів і блоків, які потребують регулювання, обслуговування або заміну під час їх експлуатації.

Слід пам'ятати, що вибір обладнання СКУД та місця його встановлення необхідно проводити у відповідності до чинного законодавства та відповідних нормативних документів.

Рекомендована література: [1; 2; 3; 4; 5; 7; 8].

Запитання для самоконтролю

1. Ідентифікатор та етапи процедури ідентифікації в СКУД.
2. Класи СКУД та їх характерні ознаки.
3. Компоненти СКУД та їх функції.
4. Назвіть основні критерії оцінювання СКУД.
5. Однорівневі та багаторівневі СКУД.
6. У якому випадку СКУД може видати сигнал тривоги або заблокувати ППК?
7. Що являє собою доступ, рівень доступу та точка доступу в СКУД? Зони доступу та їх класифікація.
8. Що являє собою модульний принцип побудови СКУД?
9. Яка відмінність між ідентифікацією та автентифікацією?
10. Яка процедура передбачає порівняння ідентичності двох різних суб'єктів доступу?
11. Які функції в СКУД виконують пристрої перешкоджаючі керовані?

ТЕМА 2. ОРГАНІЗАЦІЯ СКУД

План:

2.1 Узагальнена структурна схема СКУД.

2.2 Структура зон доступу.

2.3 Маршрути переміщення суб'єкта доступу.

2.4 Особливості точок доступу.

2.5 Математична модель СКУД.

2.1 Узагальнена структурна схема СКУД

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.

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.

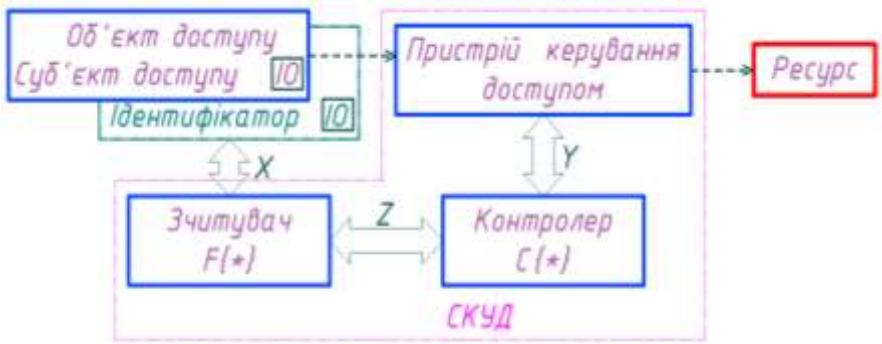


Рисунок 2.1 – Узагальнена структурна схема СКУД

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) M ідентифікаційних ознак x_{km} суб'єкта або об'єкта (ідентифікатора), які володіють K параметрами, визначаються у загальному матрицею X. Елемент матриці x_{km} являє собою k-й параметр (функцію) m-ої ознаки.

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

Алгоритм перетворення визначається арифметичним оператором F:

$$Z=F\{X\}.$$

Контролер, у загальному випадку, порівнює ознаки Z з усіма зразками Z_i^o, які зберігаються в БД системи, тим самим визначаючи порядковий номер «і» ОД/СД або фіксуючи відсутність його еталонної ознаки Z_i^o, 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 Y_i вихідних сигналів:

$$Y_i=C\{Z, Z_i^o\}|_{i=1, \ldots, I}.$$

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.

2.2 Структура зон доступу

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.

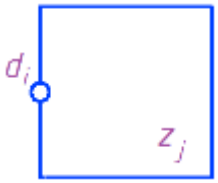


Рисунок 2.2 – Проста зона

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.

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.

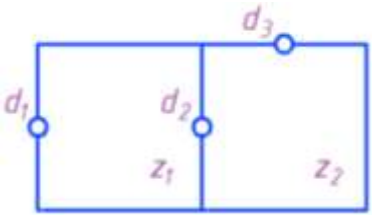


Рисунок 2.3 – Взаємопов'язані зони

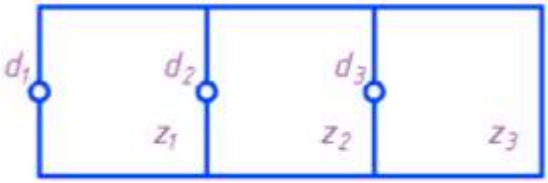


Рисунок 2.4 – Послідовнопов'язані зони

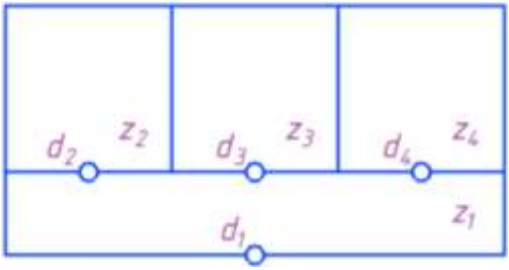


Рисунок 2.5 – Паралельнопов'язані зони

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

Вкладені зони. 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).

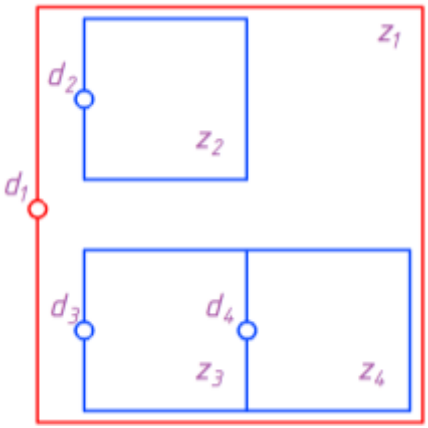


Рисунок 2.6 – Вкладені зони

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.

2.3 Маршрути переміщення суб'єкта доступу

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.

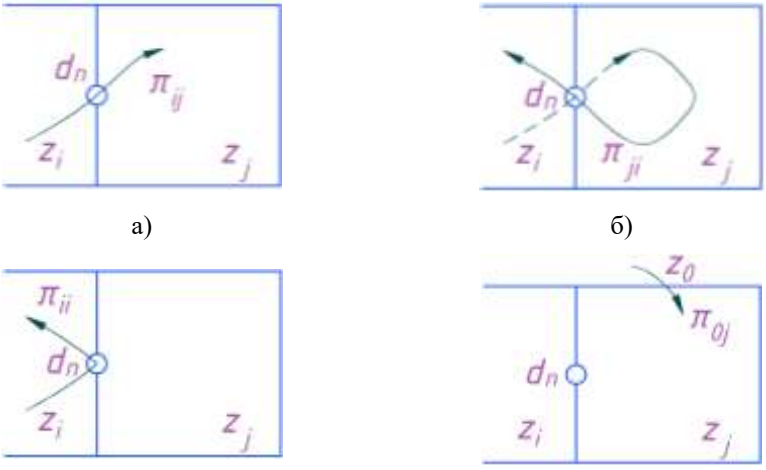


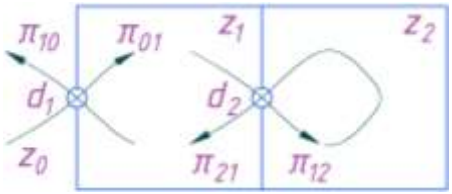
Рисунок 2.7 – Можливі варіанти руху суб'єкта доступу

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

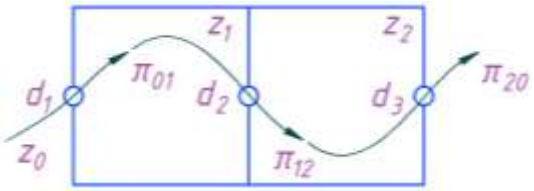
Далі (рис. 2.7, б) він може переміщуватись всередині зони z_j та вийти з неї назад через ту ж саму ТД. Таким чином, переходи з різним порядком індексів відрізняються напрямком переміщення.

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.



а)



б)

Рисунок 2.8 – Маршрути руху суб'єкта доступу

Таким чином, перехід π_{ij} означає наступне:

– за умови коли $i \neq 0, j \neq 0$ – переміщення СД з і-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.

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:

$$\pi_{01}, \pi_{12}, \pi_{21}, \pi_{10}. \quad (2.1)$$

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

Наведена послідовність переходів (2.1) 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:

$$\pi_{01}, \pi_{12}, \pi_{20}. \quad (2.2)$$

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.

2.4 Особливості точок доступу

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).

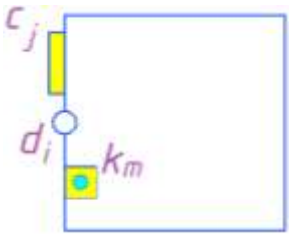


Рисунок 2.9 – Позначення елементів обладнання точки доступу

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

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).

2.4.1 Точка доступу з одностороннім контролем

В цьому випадку система контролює переміщення суб'єкта доступу лише в одному напрямку. Переміщення у зворотньому 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 зворотньому 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.

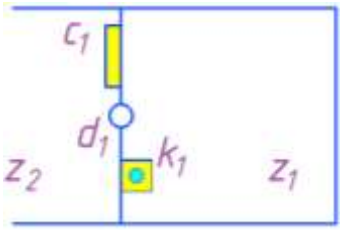


Рисунок 2.10 – Точка доступу з одностороннім контролем

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 c_x на вході. На виході монтується елемент неконтрольованого управління загороджувальним пристроєм (наприклад, кнопка управління дверима або турнікетом).

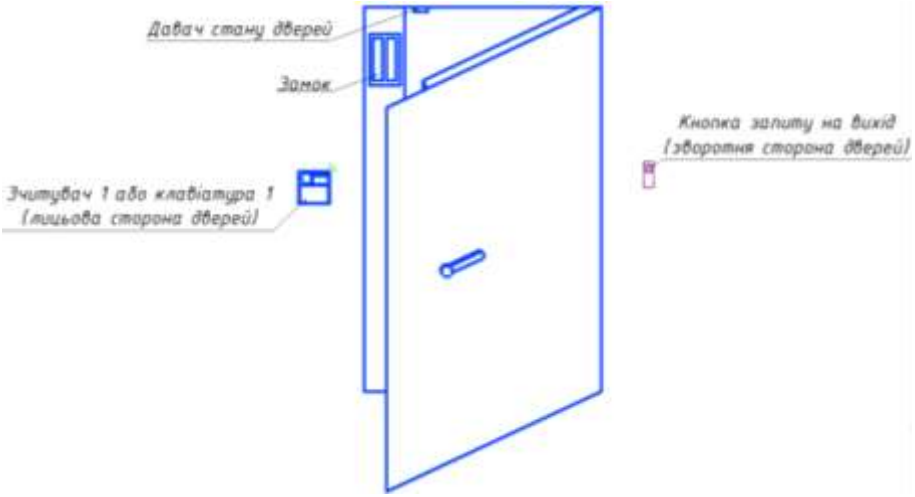


Рисунок 2.11 – Технічні засоби точки доступу з одностороннім контролем

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.

2.4.2 Точка доступу з двостороннім контролем

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).

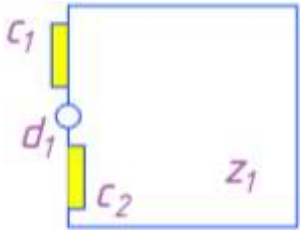


Рисунок 2.12 – Точка доступу з двостороннім контролем

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

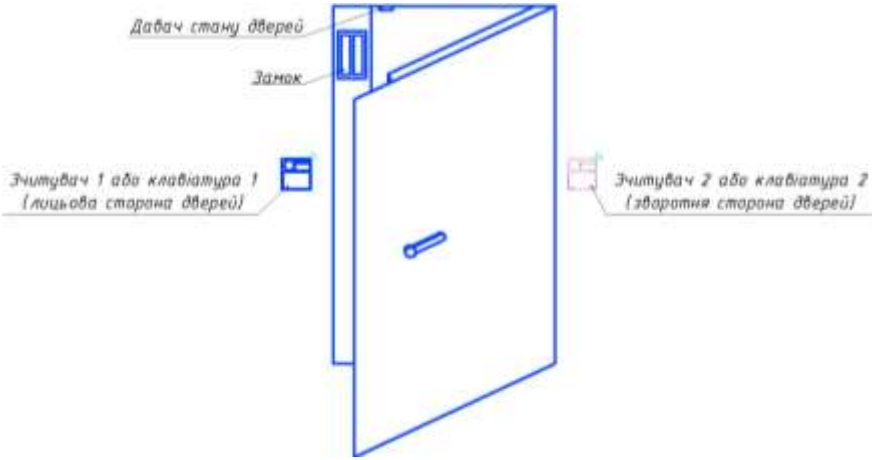


Рисунок 2.13 – Технічні засоби точки доступу з двостороннім контролем

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.

2.4.3 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 може бути їх схема наведена на рисунку 2.14.

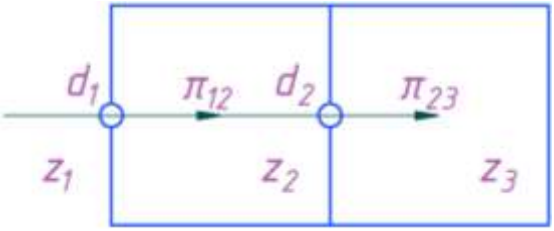


Рисунок 2.14 – Пов'язані точки доступу з направленим переміщенням

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 послідовнопов'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 наступним чином:

$$У_i(d_1, d_2, ..., d_n, \Delta t_1, \Delta t_2, \Delta t_m, \Delta T_1, \Delta T_2, \Delta T_l). \quad (2.3)$$

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:

$$У_i(d_1, d_2, ..., d_n). \quad (2.4)$$

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 (2.3).

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

$$У_1(d_1), У_2(d_1, d_2) \text{ та } У_3(d_1, d_2, d_3). \quad (2.5)$$

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

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

Монотонність в СКУД базується на тому, що:

– категорія доступу кожної наступної із послідовнопов'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 і>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 (5). Прикладом некоректного рівня є запис $У_3(d_1, d_3)$ – тут дозволена третя ТД, але заборонена друга.

2.5 Математична модель СКУД

Для опису системи контролю та управління доступом прийнято використовувати математичний апарат теорії множин та поданням СКУД у вигляді графа.

2.5.1 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. В загальному випадку множина D у свою чергу поділяється на I-підмножин D_i до складу яких входять елементи d_i. 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:

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

Слід врахувати що для підмножин ТД, які не перетинаються: $z_i \in Z_j$, i=j; $z_i \notin Z_j$, i≠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. 16 і 17 діаграмами Ейлера - Венна з різним штрихуванням.

Аналогічно сукупність зон доступу z всій СКУД може бути визначена множиною Z, якій належать ці точки доступу z∈Z. З огляду на згадану вище специфіку об'єктів (кілька структурних підрозділів з різними категоріями доступу зон), множина Z розділяється на J підмножин Zj з елементами zj. Підмножини Zi ⊂ Z, j = 1, ..., J є власними підмножинами множини Z. Як і підмножини точок доступу, підмножини Zj можуть бути як пересічними, так і непересічними, тобто (Z1 ∪ Z2 ∪ ... ∪ ZJ) = Z. При цьому для непересічних підмножин zi ∈Zj, i = j; zi∉Zj, i ≠ j. Проілюструємо вищесказане на прикладах об'єктів зі пов'язаними зонами доступу, наведеними на рис. 5 і 6. Відповідні підмножини D1, D2, D3 точок доступу Di показані на рисунку 2.15, а та 2.15, б, як діаграми Ейлера-Венна з різними зонами контрасту.

а) б)

Рисунок 2.15 – Підмножини точок доступу
а) – послідовнопов'язані зони; б) – паралельнопов'язані зони

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

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

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

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

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

В обох прикладах підмножини D мають загальну ТД 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 $(d_1, d_3, d_4) \in D2$.

Аналогічне подання може бути використано й для підмножин Z_j зон.

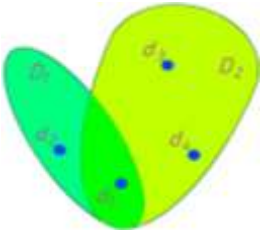


Рисунок 2.16 – Підмножина точок доступу

2.5.2 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) p_{ij} 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 ТД 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 p_m, 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 вони називаються суміжними. Ребра з однаковими кінцевими вершинами називаються 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.

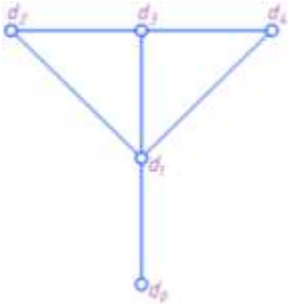


Рисунок 2.18 – Граф СКУД з паралельнопов’язаними зонами

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

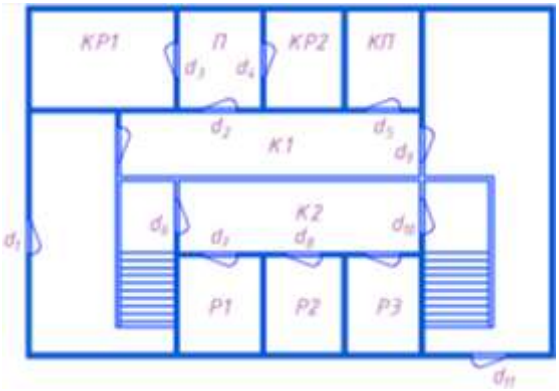


Рисунок 2.19 – План контрольованого об’єкта

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 КР1 і КР2. Доступ до них здійснюється з коридору К1 через приймальню П. Контроль доступу до приймальні й кабінети реалізується відповідно точками доступу d_2, d_3 і d_4. З

коридору К1 доступний прохід до кімнати переговорів КП через ТД d_5.

На другому поверсі розташовано комерційний відділ. Для контролю проходу в коридор встановлено ТД d_6. Доступ в робочі кабінети відділу Р1, Р2 контрольованого (в межах відділу) доступу (d_7, d_8) і не контрольованого Р3 здійснюється з коридору К2. При цьому, доступ в кабінет Р3 вільний з коридору К2 (в тому числі і для осіб, які мають доступ до кімнат Р1 та Р2).

Як з коридору К1, так і К2 в аварійній (пожежної) ситуації можливо вийти через відповідні точки доступу d_9 і d_{10}, які стають автоматично доступними в надзвичайній ситуації.

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.

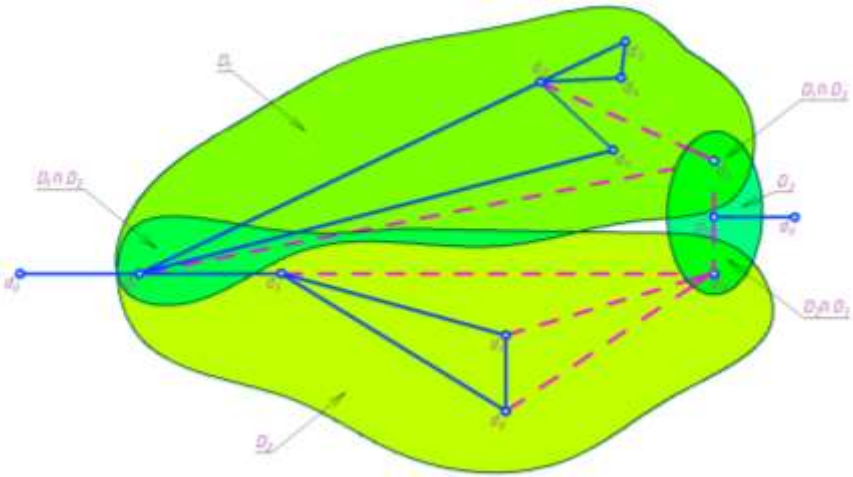


Рисунок 2.20 – Граф, який визначає взаємозв'язок точок доступу

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 ТД d_1.

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

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

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

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

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} і d_{11}, тобто переходи, які використовуються лише в аварійній ситуації, позначені пунктиром. Розглянутий граф – це неорієнтований (ненаправлений) планарний граф 11-го порядку.

2.5.3 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 M – кількість інформаційних ознак, а K – максимальна кількість параметрів однієї з ознак. Тоді матриця отримає наступний вигляд:

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

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:

$$Z=F\{X\}.$$

де

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

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_i^0 (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_i^0 по черзі, тим самим визначаючи номер і суб'єкт доступу, який володіє цим ідентифікатором, або фіксує відсутність еталона Z_i^0, 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 i) та інформації про рівень доступу i-го СД/ОД, які зберігається в базі даних, контролер формує матрицю Y_i вихідних сигналів:

$$Y_i = C\{Z, Z_i^0\}|_{i=1, \dots, I}$$

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_i^0, метою якої є виявлення співпадіння з еталонною. Або необхідно визначити значення і, за якого буде виконуватись умова:

$$Z-Z_i^0=0.$$

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

Рекомендована література: [1; 2; 3; 5; 7].

Запитання для самоконтролю

1. Від чого залежать основні особливості СКУД?
2. Дайте визначення терміну «вкладених зон» та про що необхідно пам'ятати про схемне їх подання?
3. Дайте визначення терміну «маршрут суб'єкта доступу». Наведіть відмінність між замкнутим та відкритим маршрутом.
4. Наведіть класифікацію точок доступу за їх розташуванням на контрольованому об'єкті та характером взаємодії одна з одною.
5. Назвіть можливі підходи до вибору вершин графа під час моделювання СКУД.
6. Назвіть основні елементи, які включає у себе СКУД.
7. Опишіть принцип роботи ТД, де контролюється і фіксується напрямок переміщення (використовуються окремі зчитувачі).
8. Опишіть процес перетворення інформаційних ознак СД/ОД.
9. Основні типи зон контрольованого доступу та звідки можливий доступ до кожної з них?
10. Поясніть принцип «безперервності» функціонування СКУД.
11. Поясніть, чим відрізняються переходи π_{ij} та π_{ji}.
12. Сформуйте принцип «Монотонності» в СКУД для послідовно-пов'язаних зон.
13. У чому полягає відмінність між послідовнопов'язаними та паралельно-пов'язаними зонами доступу?
14. Що означає перехід π_{ii} в контексті СКУД?
15. Що означає, коли один індекс зони доступу дорівнює нулю?

16. Що таке «шлюз» у контексті пов'язаних точок доступу?

17. Що являє собою «повний замкнутий маршрут» та «квазізамкнений маршрут».

18. Що являє собою «проста (одиночна) зона» контрольованого доступу, і яка її ключова характеристика?

19. Як прийнято термінології позначати перехід/переміщення СД із зони z_i в зону z_j?

20. Як у графі СКУД визначається ребро (гілка), яка з'єднує дві кінцеві вершини?

21. Як формується множина точок доступу D в СКУД, і на які підмножини вона поділяється?

22. Який математичний апарат використовують для опису СКУД?

23. Які ключові процедури (окрім протоколювання подій та управління виконавчими пристроями) виконують сучасні автоматизовані СКУД?

24. Які компоненти включає в себе пристрій управління доступом?

25. Яку ключову функцію виконує контролер під час ідентифікації?

ТЕМА 3. МЕТОДИ ТА ЗАСОБИ ІДЕНТИФІКАЦІЇ В СКУД

План:

3.1 Основні методи та типи ідентифікації.

3.2 Пасивна радіочастотна технологія ідентифікації.

3.3 Штрихові коди.

3.4 Карти Віганда.

3.5 Безконтактні смарт-карти.

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).

Ото ж, для ідентифікування слід використовувати:

– 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; форма предмета 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.

1.1.2 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.

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 можна досягнути під час використання біометричних ознак.

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.

1.1.3 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.

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	Маніпулювання	Копіювання	Примус	Пошкодження	
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 характеризує користувача	В	В	В	П…В	Н	Н…В	В
Примітка: Н – низька; С – середня; П – підвищена; В – висока							

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 Пасивна радіочастотна технологія ідентифікації

У сучасних СКУД радіочастотний принцип (технологія) ідентифікації набуває більш ширшого поширення завдяки своїм можливостям та перевагам. 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).

Варто зауважити, що на практиці, найбільш широко, оперують термінами радіочастотна технологія ідентифікації та проксіміті-технологія.

3.2.1 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. 3.1).

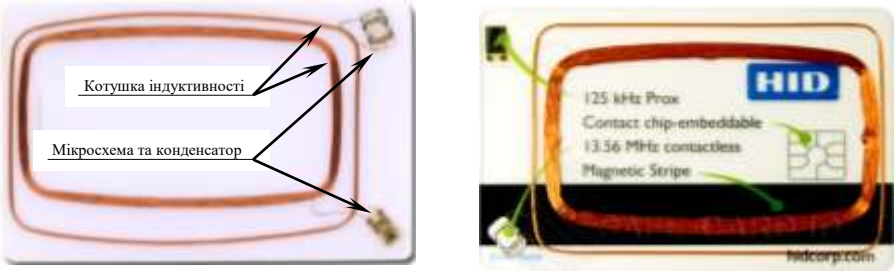


Рисунок 3.1 – Будова карти радіочастотної ідентифікації

Індуктивність, у залежності від використовуваного діапазону частот, може виконуватися у вигляді котушки або друкованих провідників. Слід пам'ятати, що для діапазону частот у 125 кГц індуктивність котушки знаходиться в межах декількох мГн, в той час як для частоти 13,56 МГц достатньою є котушка з індуктивністю в декілька мкГн.

На практиці 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. 3.2) 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.

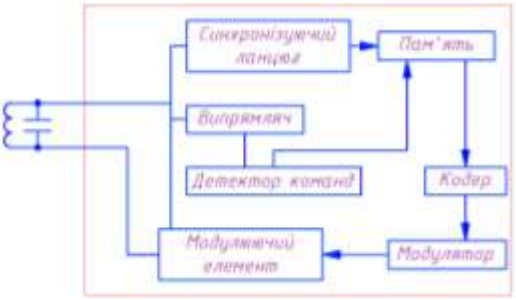


Рисунок 3.2 – Функціональна схема безконтактного ідентифікатора

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. 3.3). 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.

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

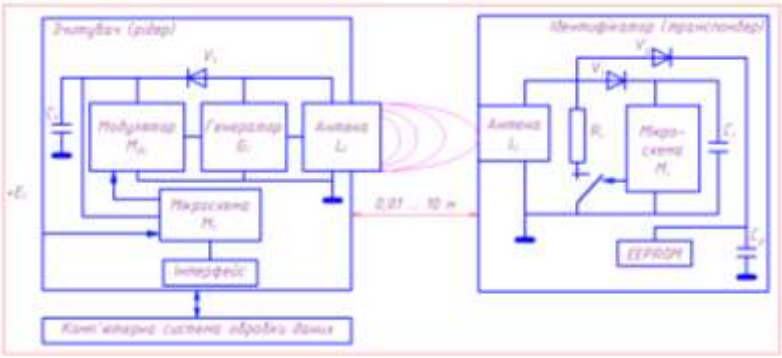


Рисунок 3.3 – Функціональна схема радіочастотного пристрою ідентифікації

Типовий сеанс зв'язку між зчитувачем та картою складається з наступних 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. 3.4).

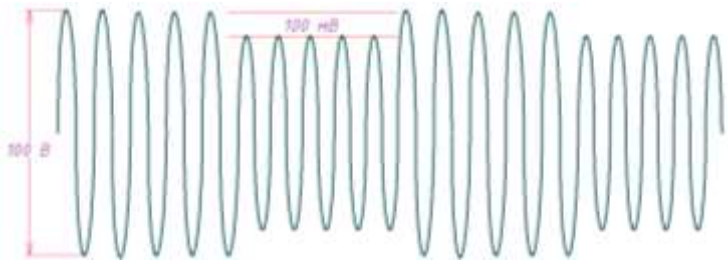


Рисунок 3.4 – Амплітудно-модульований сигнал

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. Це призводить до зміни напруги несучого коливання в контурі зчитувача.

3.2.2 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 відомими є багато способів кодування, однак в системах радіочастотної ідентифікації найбільшого поширення набули наступні (рис. 3.5):

1. Прямий код. Для даного випадку найпростішого дворівневого коду нулю відповідає низький рівень сигналу, а одиниці – високий. Інформаційні переходи співпадають з границею біт. На практиці цей код позначають 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.

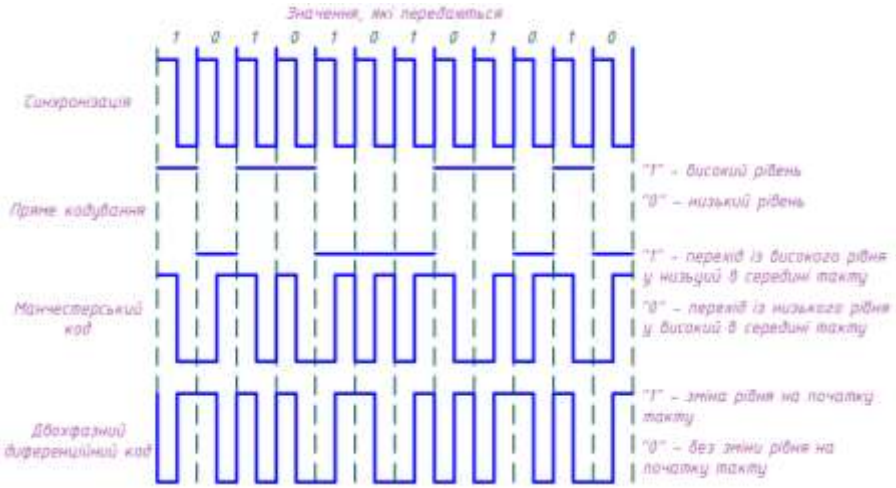


Рисунок 3.5 – Способи кодування даних

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. На практиці, 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.

3.2.3 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).

3.3 Штрихові коди

Штрихові коди досить широко використовують під час ідентифікації СД.

Найбільш поширеним є їх застосування для маркування товарів.

Штриховий код являє собою групу смуг різної ширини (рис. 3.6), які наносять на поверхню ідентифікатора.

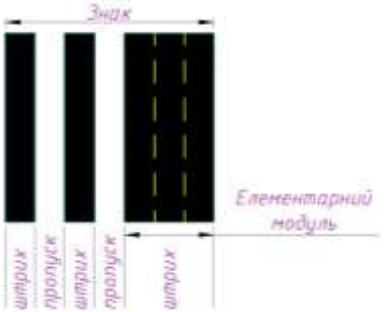


Рисунок 3.6 – Знак штрихового коду

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).

Існують різні способи кодування інформації, які називають штрих-кодовим кодуванням. На практиці, прийнято розрізняти одноплощинні (лінійні) та двохплощинні штрих-коди (рис. 3.7).

а) б) в)

Рисунок 3.7 – Приклади штрих-кодів
а – одноплощинний (Code 128); б, в – двохплощинні (PDF-417 та 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. Зауважимо, що така система дозволяє кодувати невеликий об'єм інформації (до 20…30 символів, зазвичай цифр).

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. 3.8).

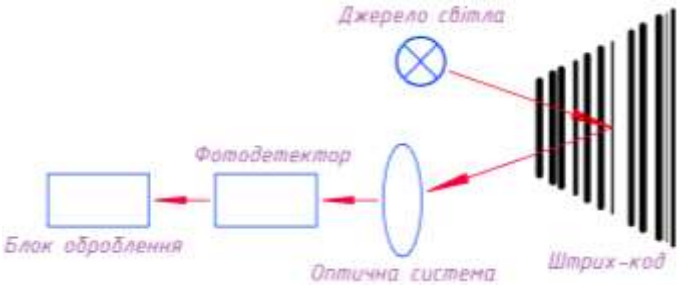


Рисунок 3.8 – Будова зчитувача штрих-коду

Джерело світла випромінює, на штриховий код, світловий потік із певною довжиною хвилі. Відбите світло відбивається назад та фокусується на фотодетекторі. Фотодетектор 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.

3.3.1 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. 3.9).

а) б) в)

Рисунок 3.9 – Приклади штрихового коду сімейства 2 of 5
а) – Interleaved; б) – Industrial та в) – Matrix

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. 3.10).

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.

Рисунок 3.10 – Структура штрихового коду Interleaved

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.

Слід пам’ятати, що 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».

3.3.2 Код Code 39

Штриховий код Code 39 є кодом змінної довжини та дозволяє відобразити 43 символи (рис. 3.11), 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.

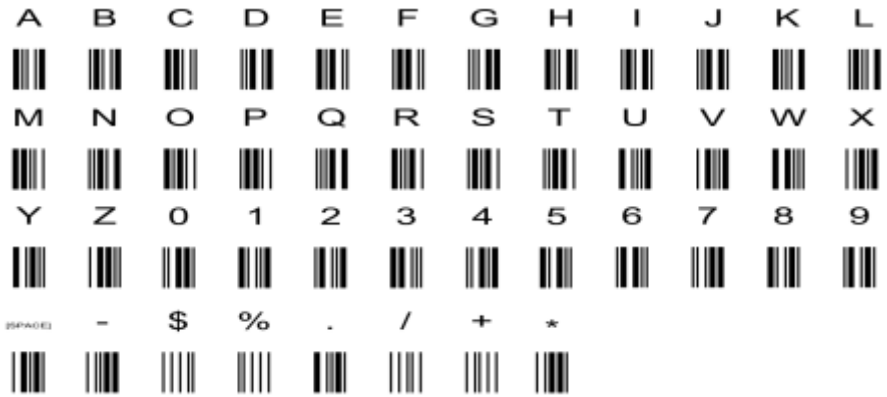
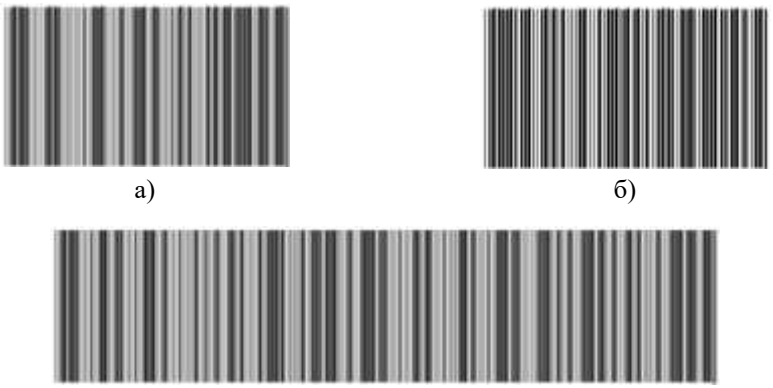


Рисунок 3.11 – Відображення символів у штриховому коді Code 39

Іноді, цей код називають «Code 3 of 9». Його назва пов'язана із структурою зображення знаків «3 з 9» (рис. 3.12), 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 3.12 – Приклади штрихового коду сімейства 3 of 9
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 $3{,}33\times10^{-7}$.

3.3.3 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. 3.13).

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 3.13 – Приклади штрихового коду сімейства Aztec
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:

– низька 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.

3.4 Карти 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.

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 дротика Віганда. На початку вісімдесятих років стали випускати карти і зчитувачі, засновані на Wiegand-ефекті. Приклад такої карти наведено на рисунку 3.14.

Рисунок 3.14 – Карта Віганда

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.

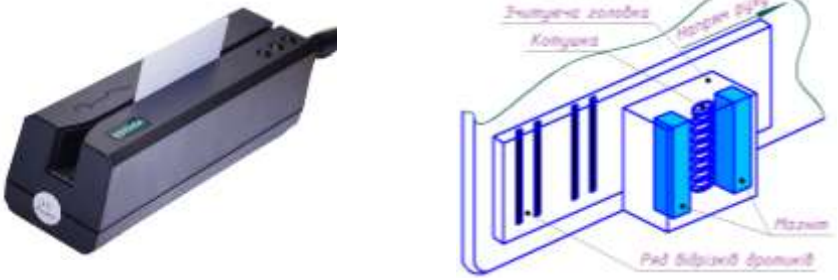
Кількість відрізків та відстань між ними визначають ідентифікаційний код картки. На практиці прийнято використовувати 26-бітові коди, які й визначають кількість відрізків дротиків в карті. Її інформаційна ємність визначає 67108864 можливих комбінацій та зводить до мінімуму ймовірність формування двох 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 10^{7}).

3.4.1 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.

На практиці, 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. 3.15, б). При цьому Wiegand-дротики переміщаються відносно неї.



а) б)

Рисунок 3.15 – Кардрідер
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. 3.16). 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. 3.16) 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.

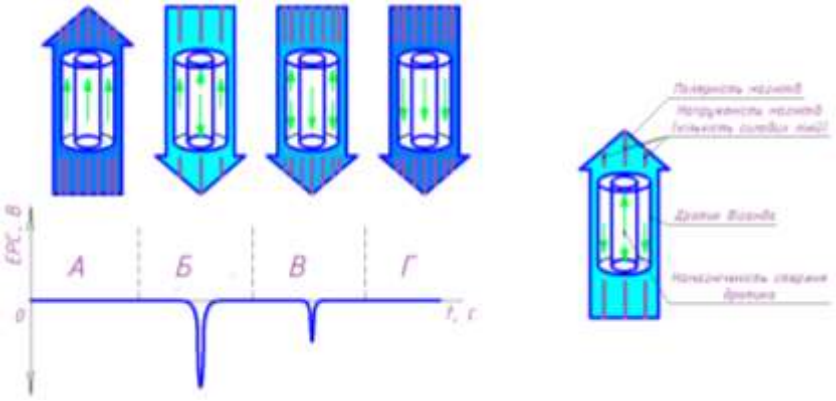


Рисунок 3.16 – Процес формування сигналів

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.

Під час магнітного перемикання Wiegand-проволочки в котушці зчитувача наводиться ЕРС індукції тривалістю близько 10 мкс (рис. 3.17). 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.

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.

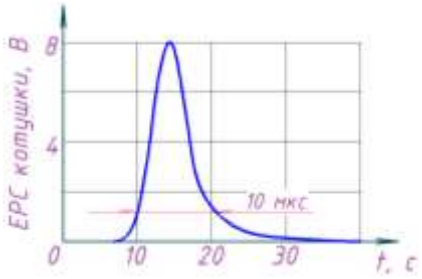


Рисунок 3.17 – Імпульс ЕРС котушки зчитувача

3.4.2 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;

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

– висока 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).

3.4.3 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 3.18 показано часову діаграму на виході зчитувача під час передачі двійкового числа «01101». Кожен імпульс відповідає зміні логічних рівнів напруги з +5 до 0 В.

Формат представлення даних визначається загальним числом записаних на карті біт інформації і їх розподілом за групами (полями) даних. Один із найбільш поширених – 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.

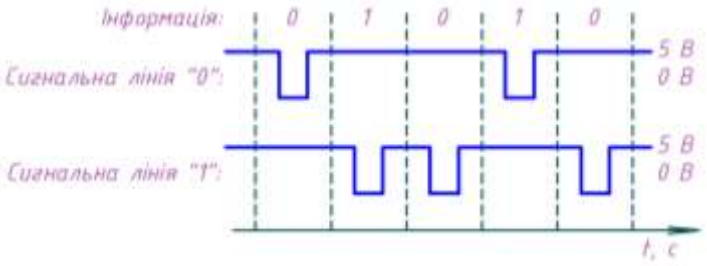


Рисунок 3.18 – Часова діаграма імпульсів на виході зчитувача

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).

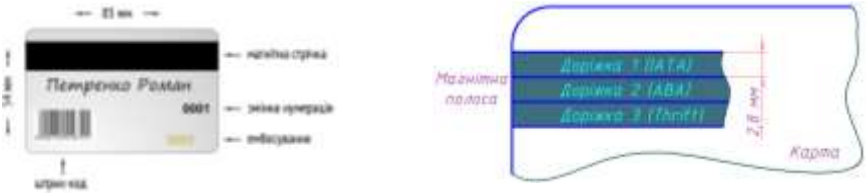
Окрім системного коду, номера карти та бітів контролю парності, на карту може бути записано й номер випуску карти (issue code).

3.4.4 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. 3.19, б), причому положення доріжок, їх ширина і глибина запису регламентуються стандартами ANSI (American National Standards Institute) 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 (BPI), кожен символ кодується 7 бітами. Всього на неї можна записати до 79 символів.



а) б)

Рисунок 3.19 – Пластикова карта з магнітною стрічкою
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:

1101001000000101001101101110011110001000000101110010011111111000 01

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. 3.20).

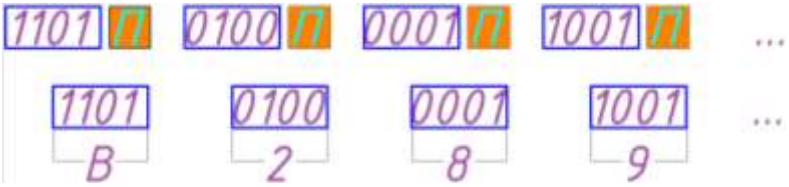


Рисунок 3.20 – Перетворення даних

Отримані блоки перетворюються в десяткову форму.

Запис інформації на магнітну смугу здійснюється за допомогою пристрою запису магнітних карт (encode). Магнітна 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 зміни 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, це відповідає бінарнону «0», а якщо два рази – «1». На рисунку 3.21 подано розподіл поляризації магнітного поля на доріжці, що відповідає двійковому рядку «000101010».

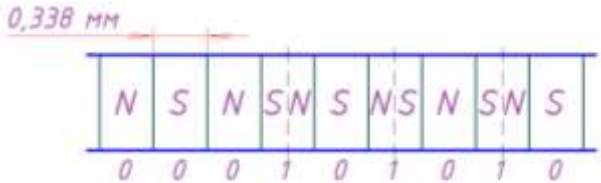


Рисунок 3.21 – Поляризація магнітного поля на доріжці

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.

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 системах КУД може бути доцільним у тому випадку, коли необхідно забезпечити мінімальну вартість карт (наприклад, на автоматизованих парковках, у вигляді перепусток в метро чи на виставки 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.

3.5 Безконтактні смарт-карти

Безконтактні смарт-карти поєднують у собі переваги безконтактних proximity- та смарт-карт. 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. 3.22).

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.

Рисунок 3.22 – Комбінована безконтактна смарт-карта

3.5.1 Електронні таблетки

Електронні таблетки (touch memory) набули досить широкого поширення завдяки своїй простоті (а отже, дешевизні) та надійності, стійкості до механічних впливів. Вперше даного роду ідентифікатори були розроблені компанією Dallas Semiconductor. Конструктивно електронна таблетка (рис. 3.23) 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.

Зчитувач (рис. 3.24), 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. 3.23, 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;

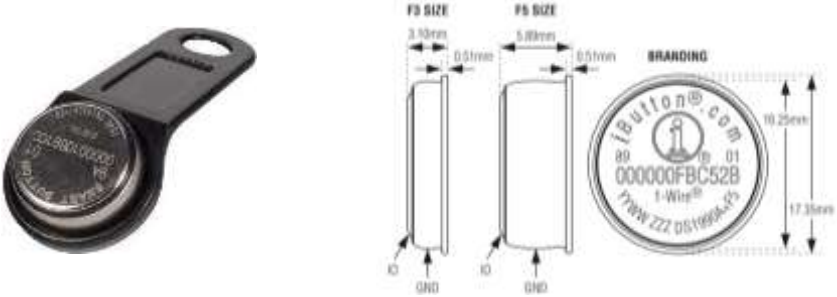
– енергонезалежний перепрограмовуваний запам’ятовуючий пристрій (ППЗП);

– 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)

Рисунок 3.23 – Електронний ідентифікатор типу «Touch memory»
а) – вигляд загальний; б) – технічні параметри

а) б) в)

Рисунок 3.24 – Зчитувач ключів
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. Обсяг 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).

3.5.2 Смарт-карти

Контактні смарт-карти, так само як і електронні таблетки, набули досить широкого застосування. Конструктивно такий ідентифікатор (рис. 3.25) виконаний у вигляді пластикової карти, на якій закріплена мікросхема з декількома (зазвичай 6 … 8) контактами (рис. 3.26).

а) б)

Рисунок 3.25 – Контактна смарт-карта
а) – без контактного чіпа; б) – з контактним чіпом

Рисунок 3.26 – Будова контактної смарт-карти
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

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. 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).

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.

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.

Рекомендована література: [1; 2; 3; 4; 5; 7; 8].

Запитання для самоконтролю

1. На основі якого фізичного способу відбувається зчитування інформації?
2. Наведіть приклади носія ідентифікаційної ознаки для кожного методу.
3. Назвіть методи ідентифікації суб'єктів у СКУД.
4. Назвіть основні недоліки використання магнітних карт у сучасних СКУД, що обмежують їх застосування.
5. Назвіть типові різновиди смарт-карт.
6. Назвіть чинники, які найбільше впливають на максимальну дальність зчитування пасивних радіочастотних ідентифікаторів.
7. Опишіть конструктивні особливості «електронної таблетки» та принцип її роботи.
8. Опишіть конструктивні особливості Wiegand-дротика.
9. Опишіть основні елементи пасивного радіочастотного ідентифікатора та поясніть, який фізичний принцип забезпечує живлення мікросхеми та обмін інформацією із зчитувачем у діапазонах довгих і коротких хвиль.
10. Порівняйте симетричний та асиметричний режими формування Wiegand-ефекту за принципом використання магнітних полів.
11. Поясніть особливість коду Interleaved 2 of 5 та Code 39.
12. Поясніть суть процесу обміну інформацією між пасивним ідентифікатором та зчитувачем.
13. У чому полягає відмінність між квазістатичними та квазідинамічними біометричними ознаками?
14. У чому полягає основний недолік прямого коду (NZR) у системах радіочастотної ідентифікації?
15. У чому полягає суть Wiegand-ефекту?
16. У чому полягає суть таких несанкціонованих дій як: спостереження; маніпулювання та копіювання?
17. Що виступає інформаційним параметром у штриховому коді та що являє собою таке елементарний модуль?
18. Яка принципова відмінність, з точки зору обсягу закодованої інформації та способу зчитування, між одноплощинними (лінійними) та

двохплощинними штрих-кодами?

19. Яка проблема може виникнути, якщо в зоні дії зчитувача одночасно перебуває декілька пасивних ідентифікаторів?

20. Який вид несанкціонованих дій, з точки зору подолання СКУД, є найбільш небезпечним?

21. Який термін вважають найбільш вдалим для позначення безконтактної технології ідентифікації та чому?

22. Який фізичний елемент використовується в картах Віганда для генерації сигналу?

23. Які переваги поєднують у собі безконтактні смарт-карти та чим вони схожі на proximity-карти?

24. Які стандарти підтримуються безконтактними смарт-картками, яка їх робоча частота та максимальна дальність зчитування?

25. Які типи штрих-кодів найчастіше використовуються в СКУД?

26. Які функціональні елементи включає у себе електронна частина ключа touch memory?

ТЕМА 4. БІОМЕТРИЧНІ СИСТЕМИ ІДЕНТИФІКАЦІЇ

План:

4.1 Біометричний метод ідентифікації.

4.2 Ідентифікація на основі квазістатистичних ознак.

4.3 Ідентифікація на основі квазідинамічних ознак.

4.4 Перспективні напрямки біометричних систем ідентифікації.

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 варто 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 Біометричний метод ідентифікації

Під час запису біометричних ознак в пам'ять системи необхідно переконатись у достовірності опрацьованої нею інформації для подальшої успішної ідентифікації СД. 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 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 належить уповноваженому користувачу;

– пред'явлений біометричний ідентифікатор не належить уповноваженому користувачу.

Отже, СБІ здійснюється прийняття рішень про дозвіл або заборону доступу (табл. 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 ($P_{п.д.}$)	Хибний дозвіл на доступ ($P_{х.д.}$)
Надано не дійсний ідентифікатор	Несанкціонований доступ ($P_{н.д.}$)	Санкціонований відмова у доступі ($P_{с.д.}$)

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

$$P_{п.д.}+P_{х.д.}=1.$$

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

$$P_{н.д.}+P_{с.д.}=1.$$

На практиці прийнято виражати ймовірність $P_{н.д.}$ через FAR (False Acceptance Rate) або FMR (False Match Rate), а $P_{х.д.}$ – через FRR (False Rejection Rate) або FNMR (False Non-Match Rate). Помилковий 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 $P_{н.д.}$ і $P_{х.д.}$, 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 $P_{х.д.}$, що дозволить уникнути затримок під час проходу СД. На об'єктах із підвищеною категорією надійності, яка не вимагає високої пропускної здатності, необхідно зменшити $P_{н.д.}$ (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 ($P_{в.р.}$). 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). На практиці така характеристика виражається через параметр FTE (Failure To Enroll Rate).

4.2 Ідентифікація на основі квазістатистичних ознак

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 р. 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.

Структурну схему такої системи подано на рисунку 4.1.

Рисунок 4.1 – Структурна схема зчитувача відбитка пальців

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.

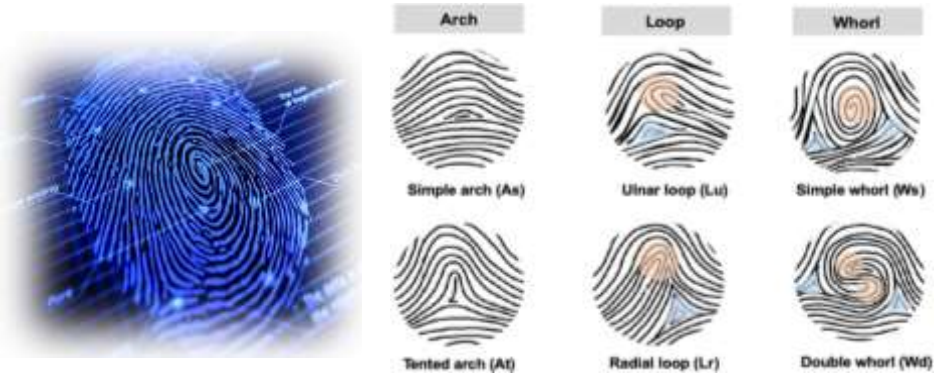


Рисунок 4.2 – Характерні особливості відбитка пальця

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. 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 базі даних інформації про велику кількість користувачів.

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).

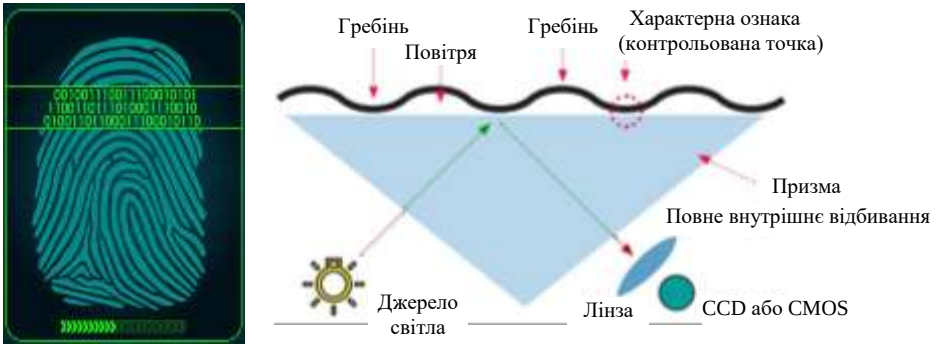


Рисунок 4.3 – Функціональна схема оптичного зчитувача відбитка пальця

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.

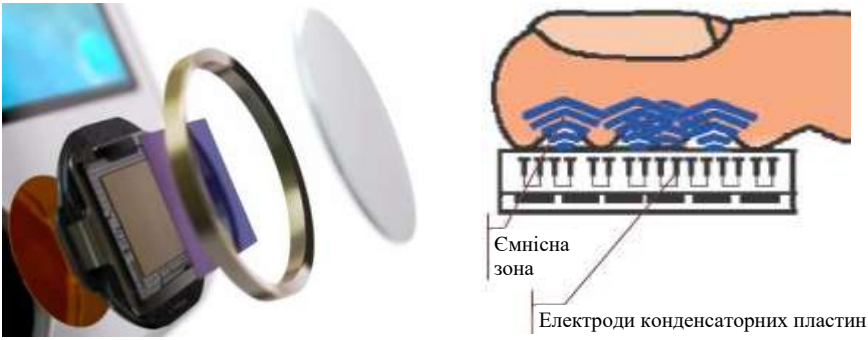


Рисунок 4.4 – Напівпровідниковий зчитувач відбитка пальця

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.

На практиці 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 першкод, 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.

4.2.2 Райдужна оболонка ока

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}.

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 при 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. 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).

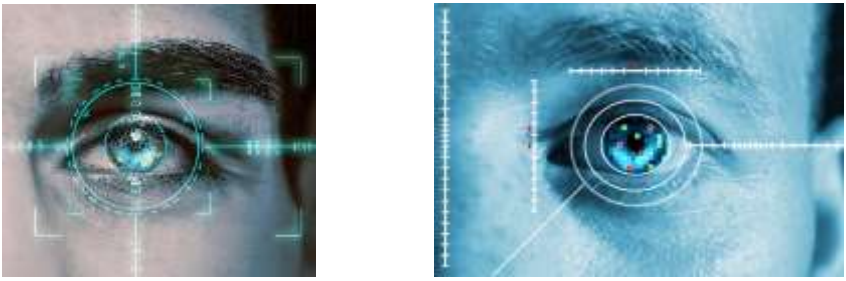


Рисунок 4.5 – Область зчитування райдужної оболонки ока

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%.

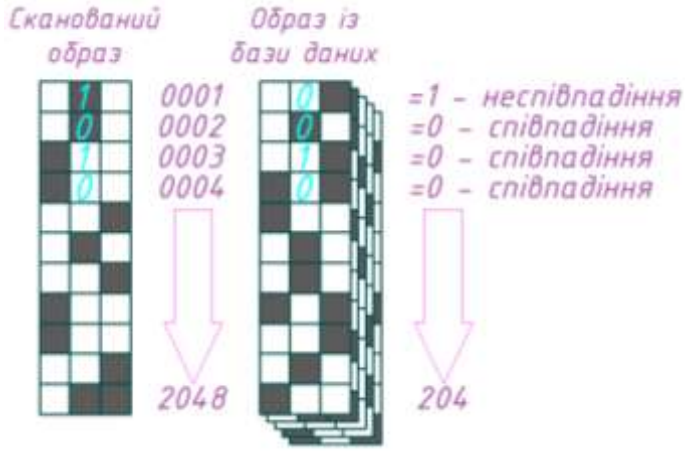


Рисунок 4.6 – Обчислення відстані Хеммінга

Логічний оператор, який виключає операцію «АБО», прийнято реалізовувати хоча б на 32-розрядному процесорі, який дозволяє достатньошвидко 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 райдужної оболонки 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 Ідентифікація на основі квазідинамічних ознак

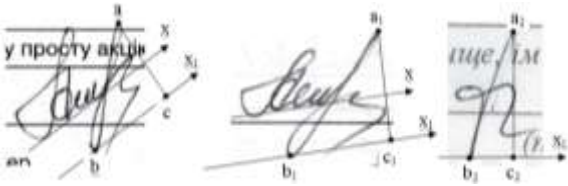
Основною специфічною особливістю ідентифікації та автентифікації СД на основі квазідінамічних біометричних ознак є можливість істотної зміни цих ідентифікаційних ознак у часі. Ці зміни можуть бути пов’язані із великою кількістю зовнішніх чинників, які безпосередньо впливають на людину, а також його фізіологічних особливостей (фізичний стан, настрій тощо).

4.3.1 Аналіз підпису

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.

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

а)



б)

в)

Рисунок 4.7 – Ідентифікаційна ознака за підписом
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.

4.3.2 Голосова ідентифікація

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.

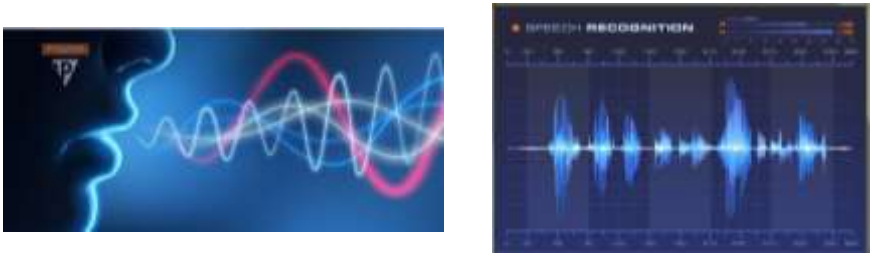


Рисунок 4.8 – Ідентифікаційна ознака за голосом

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. Ідентифікація за голосом залишається зручним, але, в той же час, не надійним способом ідентифікації СД.

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).

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

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

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.

Рисунок 4.11 – Фрагменти програмного забезпечення CCTV для пошуку зловмисників за ходою

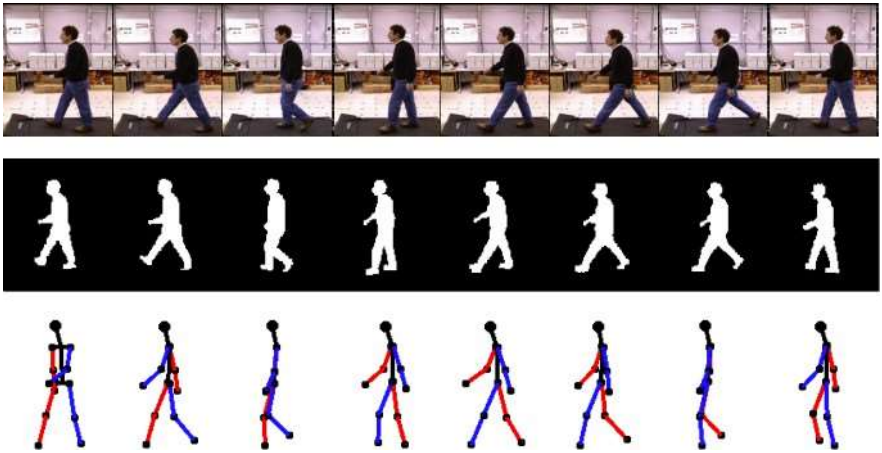


Рисунок 4.12 – Розкадровка відеозапису, яка фіксує різні фази циклу кроку

4.4 Перспективні напрямки біометричних систем ідентифікації

Дослідження, які здійснюються у сфері біометричних технологій, дозволяють суттєво розширити список застосовуваних принципів ідентифікації.

На практиці, добре відомі системи, які ідентифікують особу за клавіатурним почерком. Цей метод засновано на тому, що під час швидкого набору тексту на клавіатурі комп'ютера інтервал між натисканнями клавіш та їх відпускання, а також тривалості утримання клавіш є унікальними для кожної людини. Він дозволяє поєднати у собі два незалежні методи ідентифікації, які засновано на запам'ятовувані людиною (пароль або кодовий вираз, які вводяться з клавіатури) та її фізичних характеристиках (клавіатурний почерк).

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.

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.

Рекомендована література: [1; 2; 3; 5; 7; 8].

Запитання для самоконтролю

1. На чому заснований біометричний метод ідентифікації СД?
2. На якій ознаці базується технологія ідентифікації за ходою?
3. Назвіть ключову характеристику райдужної оболонки ока людини, яка робить її ідеальною для ідентифікації.
4. Назвіть послідовність основних етапів, з яких складається процес занесення біометричних образів до бази даних системи.
5. Поясніть у чому суть параметра «відстань Хеммінга» в контексті порівняння образів райдужної оболонки ока.
6. У чому полягає відмінність між основними алгоритмами роботи зчитувача відбитків пальців?
7. У чому полягає суть перевірки достовірності зчитаної еталонної інформації під час запису біометричних ознак?
8. Що робить небажаним зберігання зображень відбитків пальців у початковому вигляді? Як вирішити цю проблему?

9. Що таке ймовірність відмови системи у реєстрації користувача $P_{в.р.}$ та через який параметр його виражають на практиці?

10. Як визначити ймовірності $P_{х.д.}$ та $P_{н.д.}$ спираючись на матрицю рішень системи біометричної ідентифікації.

11. Яка основна особливість квазідинамічних біометричних ознак?

12. Яка основна складність пов'язана із голосовою ідентифікацією?

13. Яка особливість покладена в основі методу ідентифікації особи за клавіатурним почерком?

14. Який напрямок автентифікації суб'єкта доступу використовує його індивідуальні особливості генетичного коду?

15. Який принцип покладено в основу ідентифікації за відбитком пальця?

16. Якими параметрами виражаються ймовірності $P_{х.д.}$ та $P_{н.д.}$ через помилки першого та другого роду?

17. Які біометричні системи входять до першої групи (за типом ознак) та чому їх ідентифікаційні ознаки отримали назву «квазістатичні»?

18. Які біометричні системи належать до другої групи (за типом ознак), і чому їх називають «квазідинамічними»?

19. Які динамічні параметри враховують під час автоматизованого аналізу підпису для досягнення необхідної надійності ідентифікації?

20. Які типи характерних елементів виокремлють з папілярного малюнка для створення відбитка пальця?

21. Які чинники впливають на спектральний склад мови?

22. Яку критично важливу перевірку здійснює система перед аналізом біометричних ідентифікаційних ознак людини?

ЗМІСТОВНИЙ МОДУЛЬ 2. Вибір та реалізація систем контролю доступом

ТЕМА 5. ВИБІР СКУД ДЛЯ ОБЛАШТУВАННЯ ОБ'ЄКТА ДОСТУПУ

План:

5.1 Огляд об'єкта доступу на можливість застосування СКУД.

5.2 Вимоги, які висуваються до основних компонентів СКУД.

5.3 Типові варіанти СКУД.

5.1 Огляд об'єкта доступу на можливість застосування СКУД

Вибір варіанту обладнання об'єкта засобами СКУД слід розпочинати із його обстеження. 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.

У технічному завданні вказують:

– призначення системи, технічне обґрунтування та опис системи;

– розміщення складових частин системи;

– умови експлуатації складових частин системи;

– основні технічні характеристики системи (пропускна здатність до зони доступу (особливо в годину-пік); максимально можливе число користувачів на один зчитувач; максимальне число та види карток-перепусток);

– вимоги, які висуваються до системи, з точки зору маскування й захисту від вандалізму складових частин СКУД;

– повідомлення про тривожні та аварійні ситуації і прийняття відповідних заходів для їх припинення або попередження;

– можливість роботи системи та збереження даних без комп’ютера або у разі його відмови;

– програмне забезпечення системи;

– вимоги до безпеки;

– вимоги до електроживлення;

– обслуговування і ремонт системи;

– вимоги до можливості включення системи СКУД до складу інтегрованої системи безпеки.

5.1.1 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.

5.1.2 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.

5.1.3 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.

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).

5.2 Вимоги, які висуваються до основних компонентів СКУД

5.2.1 Вимоги, які висуваються до виконавчих пристроїв

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 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).

5.2.2 Вимоги, які висуваються до пристроїв 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.

5.2.3 Вимоги, які висуваються до пристроїв 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.

Рівень доступу – сукупність часових інтервалів доступу (вікон часу) та місць проходу (маршрутів переміщення), які встановлено для конкретного СД або групі осіб, яким дозволено доступ у задані зони, які охороняються у встановлені тимчасові інтервали.

У свою чергу програмне забезпечення (ПЗ) 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.

5.2.4 Вимоги, які висуваються до 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. Номінальна напруга резервного джерела живлення повинна бути +12 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 джерела резервного живлення, 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.

5.3 Типові варіанти СКУД

5.3.1 СКУД для автономного режиму роботи

СКУД 1-го та 2-го класів, 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 5.1 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.

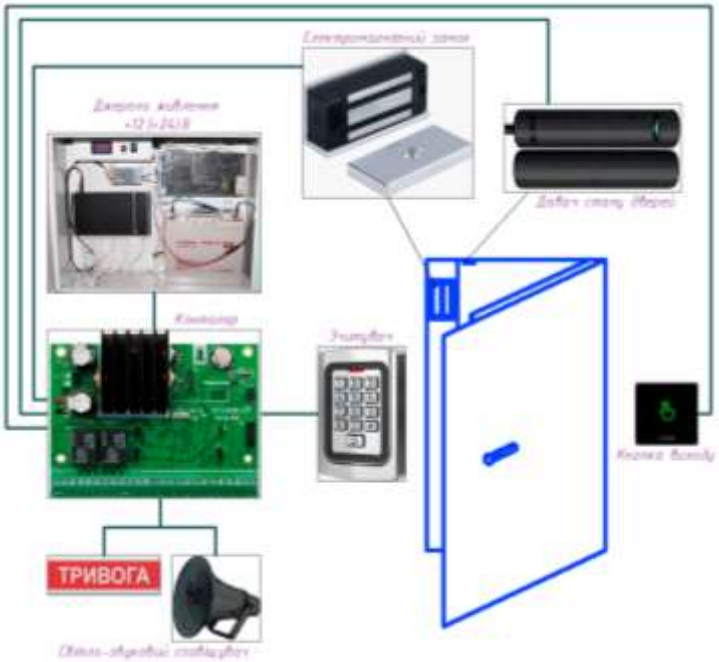


Рисунок 5.1 – Приклад облаштування СКУД приміщенням з одними дверима

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. 5.2), який об'єднує у собі зчитувач, контролер, виконавчий пристрій (защібка, ригель або засувка) та індикатори режимів роботи (рис. 5.2). При цьому СКУД працює в режимі звичайного замка, тобто при збігу кодів ідентифікатора і зчитувача запірний механізм спрацьовує і розблоковує двері, дозволяючи прохід.

Рисунок 5.2 – 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 5.3 наведено приклад можливого виконання СКУД об'єкта з декількома дверима, яка працює в автономному режимі.

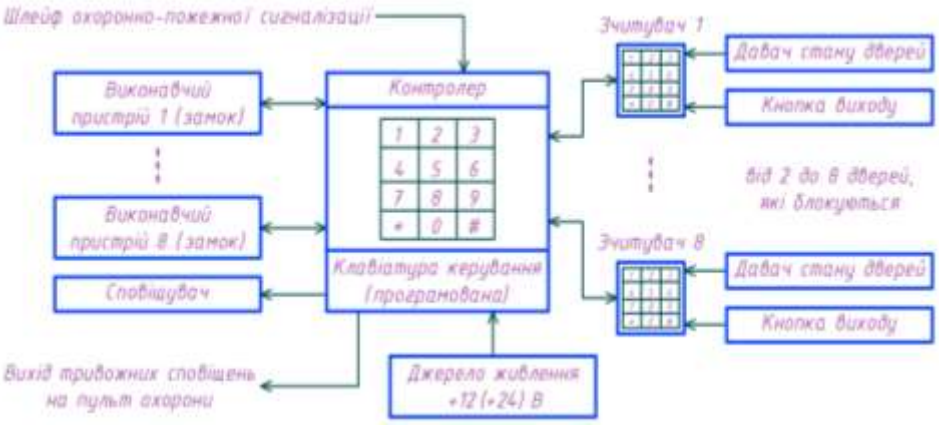


Рисунок 5.3 – Приклад облаштування СКУД приміщенням з декількома дверима

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.

5.3.2 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.

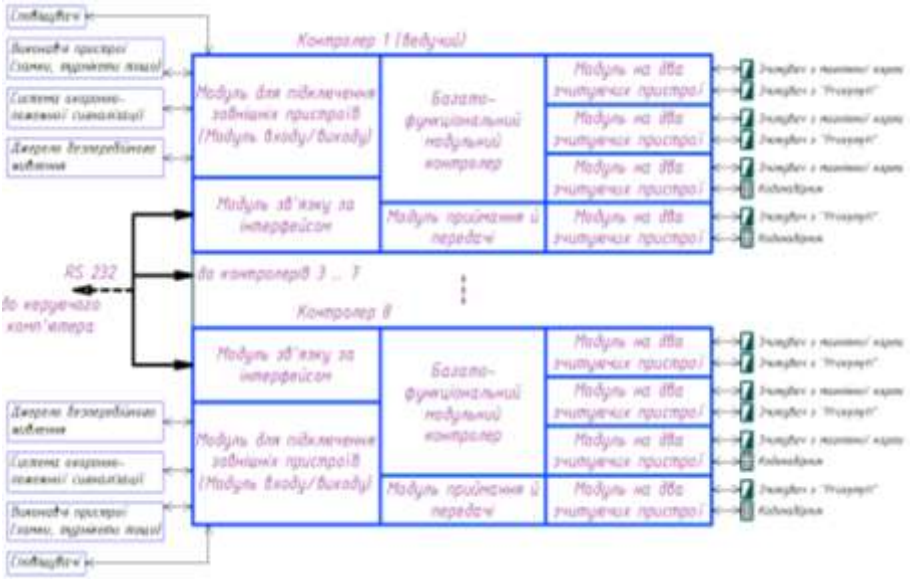


Рисунок 5.4 – Структурна схема СКУД 3-го класу

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 5.5 подано варіант побудови СКУД 4-го класу.

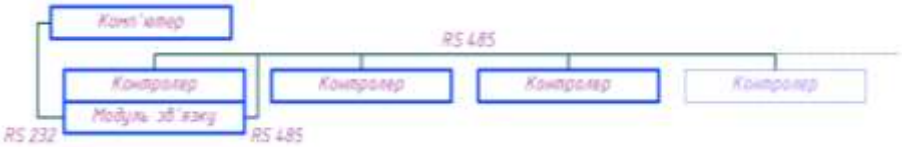


Рисунок 5.5 – Структурна схема побудови СКУД 4-го класу з однією гілкою

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 5.6.

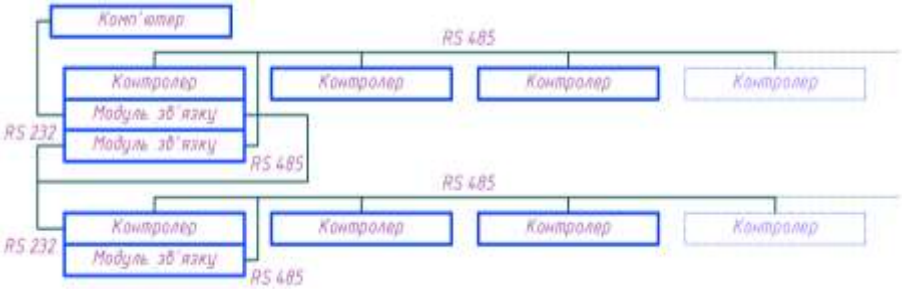


Рисунок 5.6 – Структурна схема побудови СКУД 4-го класу з декількома гілками

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. 5.7) до першого контролера нової гілки через модуль зв'язку (інтерфейс RS 485).

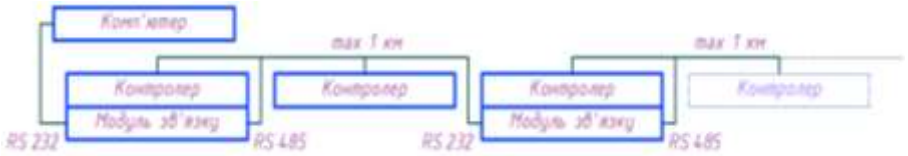


Рисунок 5.7 – Збільшення довжини гілки шляхом використання двох модулів зв'язку

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).

5.3.3 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. 5.8).

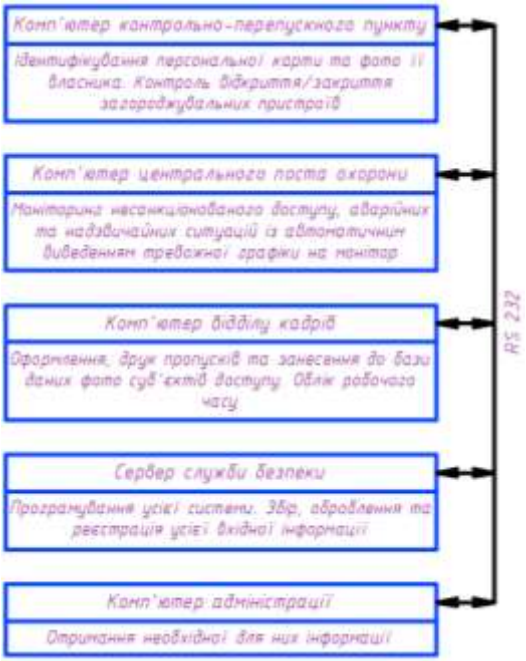


Рисунок 5.8 – Розміщення комп'ютерів СКУД, які інтегровано в мережу об'єкта

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.

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.

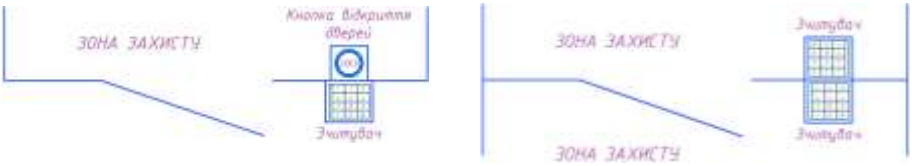
5.3.4 Зчитувачі та виконавчі пристрої

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 5.9 та 5.10 наведено варіанти розміщення й монтажу зчитувачів та виконавчих пристроїв.

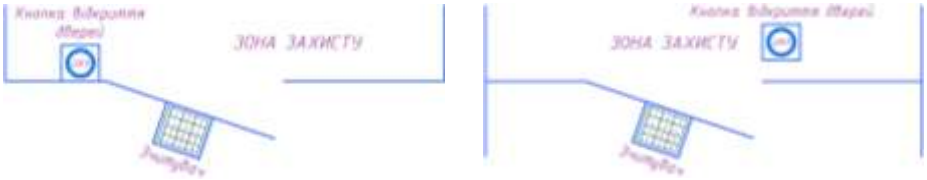
Зчитувачі «Proximity» найзручніше розташовувати як на стіні (у тому числі й замасковано в стіні) перед загороджувальними пристроями, так і з внутрішньої сторони пристрою загородження (наприклад, на внутрішній стороні неметалевих дверей, якщо їх товщина не перевищує 10 см). Під час монтажу зчитувача на

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

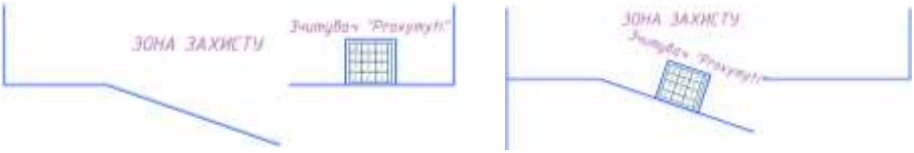


Рисунок 5.9 – Варіанти розміщення зчитувачів СКУД

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.

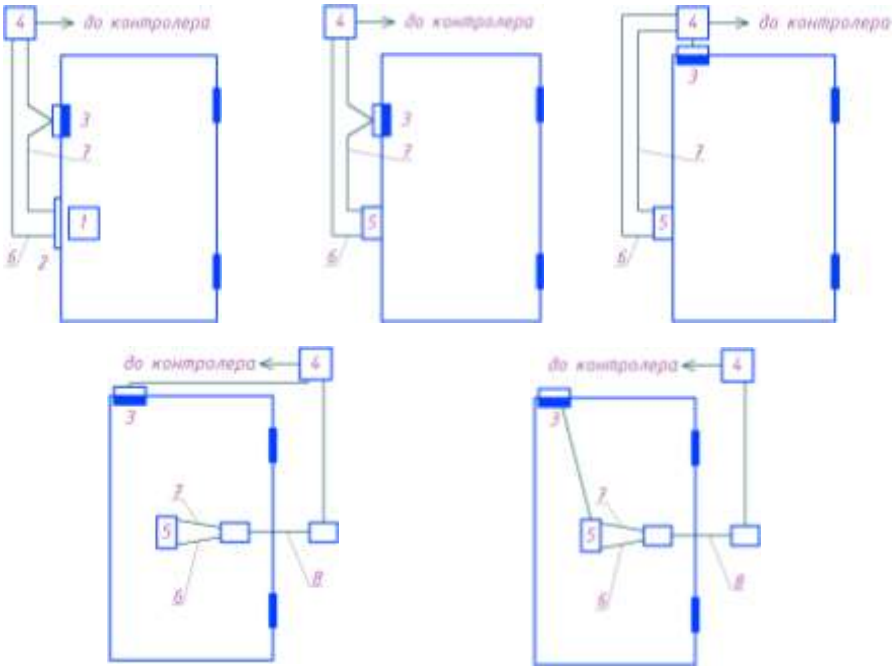


Рисунок 5.10 – Варіанти можливого розташування виконавчих пристроїв на дверних конструкціях
1 – механічний замок; 2 – електромагнітна защіпка; 3 – давач стану дверей (геркон); 4 – з'єднувальна коробка; 5 – електромеханічний або електромагнітний замок; 6 – кабель живлення замка (для дверей, які виконано із горючого матеріалу – подвійна ізоляція ПХВ або металорукав); 7 – ланцюги управління та контролю; 8 – гнучкий перехід (кабелепровід)

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.

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).

Рекомендована література: [1; 2; 3; 5; 7].

Запитання для самоконтролю

1. Для яких об'єктів призначені СКУД 3-го та 4-го класів (мережевий режим) та яка основна перевага?
2. Для яких об'єктів прийнято інсталювати СКУД 1-го та 2-го класів, які працюють в автономному режимі?
3. З чого необхідно розпочинати вибір варіанту обладнання об'єкта засобами СКУД?
4. На яких ключових характеристиках об'єкта доцільно акцентувати свою увагу під час його обстеження?
5. Наведіть рекомендовані типи стандартних інтерфейсів для СКУД.
6. Назвіть основні технічні характеристики системи, які необхідно вказати в технічному завданні на оснащення об'єкта засобами СКУД.
7. Назвіть, від найнижчого до найвищого, рівні безпеки, які можна забезпечити різними типами ідентифікаторів.
8. Після скількох хибних спроб має видаватися сигнал тривоги і чому?
9. Що являє собою «офісний режим» в автономній СКУД та у чому

полягає його суть для СД, який знаходиться всередині контрольованої зони?

9. Як слід захищати систему аварійного відкривання СКУД?

10. Які архітектурно-планувальні та будівельні характеристики об'єкта визначають під час його огляду та вивчення відповідних креслеників?

11. Які вимоги висувають до монтажу виконавчих елементів СКУД?

12. Які вимоги висувають до резервних джерел живлення в СКУД?

13. Які вимоги прийнято висувати до виконавчих пристроїв у разі зникнення основного джерела живлення?

14. Які додаткові функції можна реалізувати у розширеній автономній СКУД для об'єкта з декількома дверима?

15. Які заходи безпеки має забезпечувати зчитувач у випадку багаторазового введення невірного коду?

16. Які кінцеві результати визначають за підсумками обстеження об'єкта перед формуванням технічного завдання на СКУД?

17. Які ключові функції повинні забезпечувати контролери, які працюють від мережі змінного струму?

18. Які основні компоненти формують мінімальну СКУД для приміщення з одними вхідними дверима та забезпечує два способи контролю доступу?

19. Які шкідливі чинники впливають на надійність роботи СКУД?

ТЕМА 6. ОСОБЛИВОСТІ СКУД ДЛЯ ВЕЛИКИХ РОЗПОДІЛЕНИХ ОБ'ЄКТІВ ДОСТУПУ

6.1 Централізована архітектура СКУД.

6.2 Розподілена архітектура СКУД.

6.3 Змішана архітектура СКУД.

6.4 Програмне забезпечення для великих СКУД.

Для СКУД великого розподіленого об'єкта, якому притаманна довільна архітектура, прийнято застосовувати потужні центральні контролери, які здійснюють процес управління шляхом використання спеціалізованих віддалених інтерфейсних модулів. Особливості їх застосування визначають вимогами, які висуваються, перш за все до програмного забезпечення. На практиці найчастіше використовують СКУД із централізованою або розподіленою архітектурою, в окремих випадках – архітектура змішаного типу.

6.1 Централізована архітектура СКУД

У великій розподіленій системі КУД, особливо за великих відстаней між окремими будівлями об'єкта, які охороняється, кожна з них повинна мати свій

центральний контролер. У разі порушення зв'язку між окремими об'єктами саме це й забезпечить автономне функціонування системи безпеки кожної будівлі. Слід пам'ятати, що кількість підключених зчитувачів на один контролер коливається від 16 до 96. Це говорить про те, що потужності одного контролера цілком вистачає для створення СКУД окремого об'єкта у великій розподіленій системі.

Контролери централізованих СКУД це логічні пристрої та не керують дверима, тобто не мають релейних виходів керування замками чи/або входів для підключення зчитувачів СКУД. Функції керування дверима або іншими зовнішніми пристроями перебирають на себе зовнішні інтерфейсні модулі та релейні блоки (як правило, їх встановлюють недалеко від об'єктів управління).

Для обміну інформацією між контролером та інтерфейсними модулями найчастіше використовують інтерфейс RS 485, проте, на сьогодні, широко застосовують й системи, у яких підключення інтерфейсних модулів відбувається стандартом LAN.

Слід пам'ятати, що найбільш потужні центральні контролери володіють декількома комунікаційними інтерфейсами RS 485, а це дозволяє широко охопити територію великих будівель без застосування підсилювачів інтерфейсу. Що стосується мережевого інтерфейсу, то для великих об'єктів можливість підключення інтерфейсних модулів СКУД до центрального контролера за стандартом LAN є дуже актуальним, оскільки з'являється перспектива використання існуючої, на об'єкті, мережевої інфраструктури (суттєве зниження витрат на прокладання комунікацій).

Контролер в системах із централізованою архітектурою дозволяє зберігати усю базу даних ідентифікаторів та подій, які відбуваються у системі. Розташовується він зазвичай недалеко від керуючих комп'ютерів (серверів) в місцях найвищої захищеності. Розділення функцій прийняття рішень та безпосереднього управління підвищує ступінь безпеки СКУД, оскільки сам контролер є добре захищеним та, зазвичай, розташований на великій відстані від керованого ним загороджувального пристрою. Зауважимо, що саме такий підхід допомагає знизити вартість великих систем, оскільки ціна контролера «розчиняється» у загальній вартості системи.

Варто пам'ятати, що самі контролери можна також об'єднувати в мережі, дозволяючи тим самим створювати СКУД великого масштабу (рис. 6.1). У випадку порушення зв'язку контролера із комп'ютером така система буде працювати в автономному режимі. Іншими словами, централізована система – це жорстка владна вертикаль або піраміда, коли нагорі керівний контролер («начальник»), а нижче – звичайні інтерфейсні модулі («виконавці»), які власне

й реалізують керуючі команди.

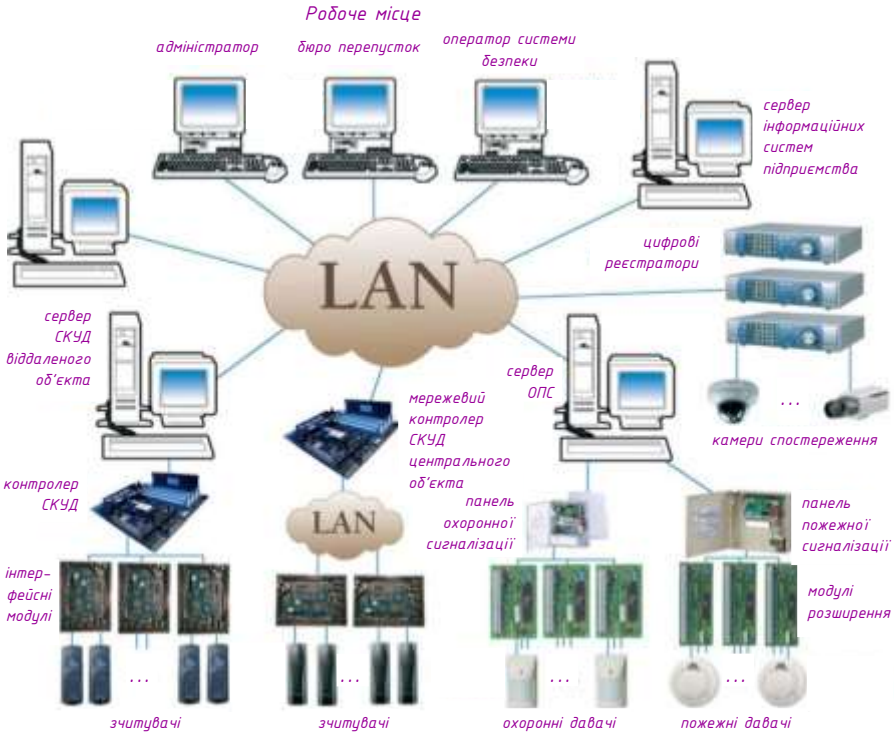


Рисунок 6.1 – Варіант побудови СКУД із централізованою архітектурою

6.2 Розподілена архітектура СКУД

Відмінною рисою СКУД із розподіленою архітектурою є те, що база даних ідентифікаторів (або подій у системі) міститься не в одному, а у декількох контролерах. Вони зазвичай виконують функції управління зовнішніми пристроями та охоронними шлейфами через реле й входи охоронної сигналізації, які розташовуються безпосередньо на платі самого контролера. Ці контролери, як правило, встановлюють всередині приміщень, які й захищаються ними. Це не дозволяє знизити ймовірність несанкціонованого маніпулювання контролером, але має свої плюси – такий підхід є менш критичним з точки зору порушення зв'язку між контролером та інтерфейсним модулем (як у звичайній централізованій системі). У випадку обриву лінії зв'язку між контролерами й комп'ютером система продовжує виконувати основні функції управління

процесом доступу в автономному режимі (виведення з ладу одного контролера не вплине на роботу інших).

Найчастіше у системах із розподіленою архітектурою контролер управляє проходом у 2-4 зони захисту. За умови використання таких СКУД на великих розподілених об'єктах необхідно пам'ятати, що кожна окрема будівля, швидше за все, буде оснащуватися своєю підсистемою, яка буде складатись із групи контролерів, які будуть керуватись сервером (керуючим комп'ютером). Ця особливість пов'язана із обмеженням довжини, часто використовуваних, в таких системах, інтерфейсів – RS 485 та струмової петлі силою 20 мА.

Монтаж ліній зв'язку між віддаленими об'єктами вимагає застосування підсилювачів інтерфейсу, а це не завжди зручно та призводить до незначного зниження надійності. У цьому випадку систему доцільно розглядати як сукупність підсистем декількох об'єктів. Іншими словами, розподілена СКУД – це деяка кількість контролерів – «виконробів», які відповідають тільки за свою ділянку робіт, яку й самі ж виконують. Вони самостійно аналізують та зберігають частину інформації про функціонування своєї невеликої частини системи.

6.3 Змішана архітектура СКУД

Зазвичай, такі системи, отримують з СКУД із централізованою архітектурою, шляхом додавання спеціалізованих зчитувачів або інтерфейсних модулів, які мають власний буфер пам'яті ідентифікаторів або подій – «інтелектуальних інтерфейсних модулів». При цьому, кожен такий модуль, у порівнянні із контролером розподіленої системи, є невеликим контролером СКУД.

Завдяки використання цього технічного рішення можна досягнути надлишкового резервування функцій, що стрімко підвищує ступінь безпеки системи. Оскільки контролер в СКУД із централізованою архітектурою управляє великою кількістю загороджувальних пристроїв, то пошкодження лінії зв'язку між ним та інтерфейсними модулями управління виконавчими пристроями може призвести до блокування значної частини або й навіть усієї системи. В даному випадку, локальний зчитувач або проміжний інтерфейсний блок, який має вбудований буфер пам'яті, переходить в автономний режим управління доступом (лише на своїй ділянці). Слід зауважити, що системи, які побудовано на цих модулях, володіють найвищим ступенем безпеки та винятковою функціональною надійністю.

Для великих розподілених СКУД із змішаною апаратною архітектурою важливим моментом виступає наявність, в номенклатурі окремих виробників,

інтерфейсних модулів із можливістю підключення до центрального контролера за LAN-інтерфейсом. За наявності, на території об'єкта, розвиненої мережі комунікацій такі модулі, зазвичай, встановлюють у віддалених будівлях, що надає системі додаткової гнучкості та дозволяє економити кошти.

Таким чином, змішана система – це владна вертикаль, або піраміда із можливістю передачі частини функцій управління на нижчий рівень за умови виникнення надзвичайної ситуації.

6.4 Програмне забезпечення для великих СКУД

Для програмних комплексів великих розподілених СКУД притаманні свої особливості, які обов'язково враховують під час вибору ПК для систем малого та середнього масштабу.

Одним із найбільш поширених варіантів СКУД є невелика ізольована система. Її основною характеристикою є те, що усі модулі (управління базою даних, ядро, функціональні модулі, драйвери обладнання тощо) встановлюються та запускаються на одному комп'ютері до якого підключають й усе інше обладнання. Зауважимо, що ПК, при цьому, повинен володіти достатню обчислювальну потужність та достатнім об'ємом пам'яті, який буде задіяним для виконання усіх програмних модулів та зберігання бази даних системи.

Основні переваги наведеної системи – простота інсталяції, обслуговування, контролю ліній зв'язку та низька вартість. З недоліків доцільно виокремити: відключення деяких функцій під час «зависання» або вимикання комп'ютера; можливість адміністрування лише на одному комп'ютері; уповільнення реакцій комплексу під час підключення великої кількості обладнання. Найбільшим недоліком, для великої розподіленої системи, залишається необхідність підключення усього керованого обладнання до центрального комп'ютера, що часто є нездійсненним.

Під час використання централізованої системи із віддаленим управлінням усі службові модулі комплексу (ядро, драйвери обладнання та логіки) функціонують на одному комп'ютері – центральному сервері системи, а запуск керуючої консолі можливий не лише на ньому, але й на інших машинах мережі. В цій системі центральний комп'ютер повинен володіти ще більшою обчислювальною потужністю, об'ємом пам'яті та дисковим простором, ніж у системі з одним користувачем (комп'ютером). Для даної схеми властиво використовувати у якості клієнтських робочих станцій не надто потужні комп'ютери із невеликим об'ємом накопичувального диску.

Основні переваги: простота встановлювання, обслуговування та контролю ліній зв'язку, так як усе обладнання підключено до одного комп'ютера. У такій

системі легко контролювати стан функціональних модулів і драйверів обладнання, так як усі вони функціонують на одній машині. Недоліки – у загальному такі ж, як і в попередньому варіанті. Основний недолік централізованої системи, той самий – необхідність підключення усього керованого обладнання до одного комп'ютера (сервера).

У великих СКУД іноді використовується варіант, за якого сервер управління базою даних системи і ядро працюють на центральному сервері, а драйвери обладнання і логіки розподілено по усій мережі. При цьому, запуск керуючих консолей можливий на будь-якому комп'ютері мережі, що робить управління більш гнучким. Необхідність розподілу за мережею драйверів обладнання та логіки пов'язана, в основному, з тим, що будівлі об'єкта захисту розподілено по території, а частина обладнання може знаходитися відносно далеко від центрального сервера. Оскільки частину модулів винесено з центрального сервера системи на інші комп'ютери, навантаження на центральний сервер знижується.

Застосування цієї архітектури виправдано лише за наявності великої території із розподіленим по ній керуючим обладнанням. Тут немає необхідності прокладати комунікації з усіх точок до центрального сервера, достатньо підключити виконавчі пристрої системи до найближчого комп'ютера мережі й запустити на ньому обслуговуючий драйвер. При цьому вимоги до потужності такого комп'ютера залишаються відносно «скромними».

У випадку розподіленого запуску програмних модулів постає завдання контролю їх стану. Для спрощення роботи в ПЗ системи мають бути вбудованими спеціальні засоби, які дозволятимуть адміністратору зі свого робочого місця контролювати роботу модулів на інших машинах, запускати або зупиняти їх.

Найбільш важливими перевагами є: простота підключення завдяки можливості приєднання обладнання до найближчого комп'ютера; можливість створення дуже великих СКУД високої надійності для великих розподілених об'єктів; підвищення загальної швидкості роботи системи за рахунок зниження навантаження на центральний сервер; зниження вартості монтажу системи завдяки економії на монтажі ліній зв'язку. Недоліками прийнято вважати: вимога контролю адміністратором стану розподілених за системою модулів; необхідність на об'єкті навченого персоналу.

ПЗ із такою структурою підходить для побудови СКУД та інтегрованих систем безпеки (ІСБ) заводів, аеропортів, банків, офісів великих компаній, інститутів та інших великих об'єктів, які мають великі території зі великою кількістю окремо розташованих будівель та споруд.

У загальному випадку програмне забезпечення СКУД надає користувачеві такі стандартні можливості:

– програмування часових інтервалів, для дверей/воріт, які відкриті повністю, які будуть відкриватися під час сканування ідентифікаційної картки (або автентифікація СД на біометричних зчитувачах/терміналах), які будуть закриті наглухо, а також вмикання/вимикання за розкладом або за показами приладів освітлення, вентиляції, ліфтів, давачів охоронно-пожежної сигналізації;

– програмування вихідних днів та свят, коли допуск надається лише для встановлених осіб;

– створення декількох ієрархічних груп користувачів залежно від рівня наданого для них допуску;

– виконання функції «ні кроку назад», що перешкоджає тому, щоб один співробітник, пройшовши через двері, передав свою картку іншій особі (визначається тимчасовий інтервал, протягом якого картка не може відкрити двері ще раз, або на виході із приміщення встановлюється ще один зчитувач, і картка може знову «зайти», тільки коли попередньо «вийшла»);

– якщо комп'ютер підключено до системи та працює постійно, то на його дисплей можна вивести план території, яка охороняється, із усіма точками доступу (двері, проходи, розташуванням давачів тощо), на якому, в режимі реального часу, будуть відображатись усі події;

– оператор системи постійно контролює обставини і у разі необхідності може прийняти необхідні рішення відповідно до ситуації, яка склалась.

Зазвичай, великі СКУД працюють у поєднанні із системами охоронної сигналізації та телевізійного спостереження. Наприклад, під час спроби несанкціонованого проникнення до приміщення, яке обладнано СКУД або давачами охоронної сигналізації, вмикаються телекамери та блокуються виходи. При цьому, у випадках екстрених події, систему можна запрограмувати на розблокування усіх виконавчих пристроїв.

Як бачимо, типові можливості математичного й програмного забезпечення досить великих СКУД дозволяють вирішувати різні завдання пов'язані із контролем суб'єктів доступу, із контролем за винесенням матеріальних цінностей тощо.

Гнучкість ПЗ сучасних систем контролю доступу дозволяє достатньо легко змінювати їх конфігурацію, змінювати задані умови перебування в приміщеннях і на території для будь-якого суб'єкта доступу. З метою підвищення надійності функціонування СКУД їх програмне забезпечення може передбачати функціонування центральних робочих станцій у зв'язці двох машин в режимі паралельної обробки даних.

Рекомендована література: [1; 2; 5; 6; 7].

Запитання для самоконтролю

1. Назвіть ключову функціональну особливість «інтелектуальних інтерфейсних модулів».
2. Назвіть та поясніть стандартні можливості, які надає програмне забезпечення СКУД користувачеві?
3. Опишіть основні функції, які виконують контролери у розподіленій архітектурі СКУД.
4. Поясніть перевагу розподіленої архітектури з точки зору стійкості до локальних відмов.
5. Поясніть, чому використання стандарту LAN є актуальним для великих об'єктів?
6. У чому полягає відмінність централізованої системи з віддаленим управлінням від невеликої ізольованої системи?
7. У чому полягає функціональне розділення між центральним контролером та зовнішніми пристроями у централізованій СКУД?
8. У який режим переходить локальний зчитувач або проміжний інтерфейсний блок із вбудованим буфером пам'яті під час пошкодження лінії зв'язку з центральним контролером?
9. Чому монтаж ліній зв'язку між віддаленими об'єктами вимагає застосування підсилювачів інтерфейсу?
10. Що дозволяє створити СКУД великого масштабу?
11. Що надає системі використання інтерфейсних модулів із можливістю підключення до центрального контролера за LAN-інтерфейсом?
12. Як саме великі СКУД інтегруються з іншими системами безпеки?
13. Як створюються системи із змішаною архітектурою СКУД?
14. Яка архітектура програмного забезпечення СКУД використовується для великих розподілених об'єктів (заводів, аеропортів)?
15. Яка основна вимога висувається до ПК у невеликої ізольованій СКУД?
16. Який критичний ризик централізованої архітектури СКУД допомагає мінімізувати змішана архітектура?
17. Якими рисами володіє СКУД із розподіленою архітектурою та централізованою, з точки зору зберігання бази даних ідентифікаторів/подій?
18. Які інтерфейси зв'язку обмежують довжину ліній у розподілених СКУД?
19. Які переваги та недоліки притаманні архітектурі із розподіленим запуском програмних модулів?

ТЕМА 7. ЗАГОРОДЖУВАЛЬНІ КЕРОВАНІ ПРИСТРОЇ В СКУД

7.1 Класифікація ЗКП.
7.2 Загальні технічні вимоги, які висуваються до ЗКП.
7.3 Виконавчі пристрої для контролю суб'єкта доступу у приміщенні.
7.4 Виконавчі пристрої для контролю суб'єкта доступу на КПП.
7.5 Електричні замки.

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.

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.

7.1 Класифікація ЗКП

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.

Класифікація засобів контролю та управління доступом подана на рисунку 7.1.

7.2 Загальні технічні вимоги, які висуваються до ЗКП

Засоби та системи контролю й управління доступом повинні виготовлятися відповідно до чинних вимог, стандартів та інших нормативних документів на

них. У таких засобах та системах необхідно передбачати проведення регламентних технічних робіт із обслуговування, а самі вони повинні забезпечувати можливість як цілодобової, так і позмінної роботи.

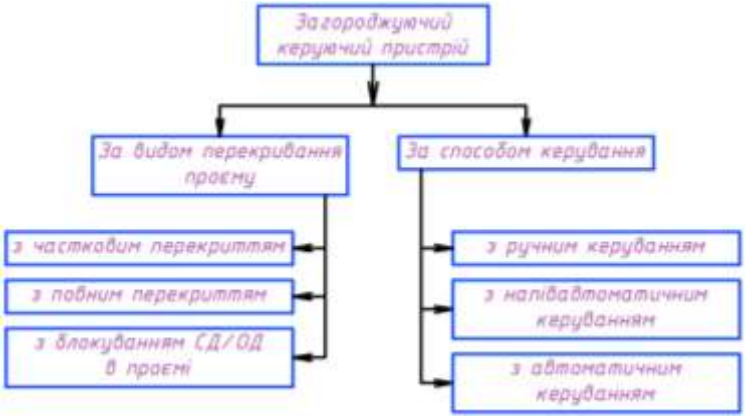


Рисунок 7.1 – Класифікація засобів контролю та управління доступом

Засоби КУД, які призначені для побудови СКУД, 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.

7.2.1 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. 7.2).

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 7.2 – Варіанти обходу загороджувального пристрою

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.

7.2.2 Вимоги, які висуваються до електромагнітної сумісності ЗКП

Засоби та системи КУД залежно від стійкості до впливу електромагнітних перешкод (за стандартами серій ДСТУ EN 50130 та ДСТУ EN 61000) 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» та ДСТУ EN 55014-2:2017 «Електромагнітна сумісність. Вимоги до побутових електроприладів, електроінструментів та аналогічних виробів. Частина 2. Несприйнятливість до завад».

7.2.3 Вимоги, які висуваються до стійкості ЗКП на несанкціоновані дії

Вимоги, які висуваються до стійкості ЗКП на несанкціоновані дії (НСД) встановлено в ДСТУ EN 50133-1:2010 «Системи тривожної сигналізації. Системи контролювання доступу для застосування в охоронних цілях. Частина 1. Системні вимоги» 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. 7.1).

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.

Таблиця 7.1 – 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.					

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.

Зауважимо, що системи та засоби КУД високої стійкості підлягають обов'язковій сертифікації за вимогами захисту від несанкціонованого доступу до інформації.

7.2.4 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» та ДСТУ 2861-94 «Надійність техніки. Аналіз надійності. Основні положення» 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.

7.2.5 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 системи контролю й управління доступом конкретного типу відповідно до кліматичного виконання і категорії виробів за ДСТУ 8280:2015 «Вироби електротехнічні. Методи випробовування на тривкість до дії зовнішніх кліматичних чинників».

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)».

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» та ступеня жорсткості виробів за ДСТУ 6098:2009 «Методи випробування на стійкість до механічних зовнішніх чинників, що впливають на машини, прилади та інші технічні вироби. Випробування на вплив вібрації з відтворенням заданої акселерограми процесу».

7.2.6 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, 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 заряджання.

7.2.7 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», 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».

Матеріали та комплектувальні вироби, 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».

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 7.2

Таблиця 7.2 – 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

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.

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» або іншим нормативним документам, які регламентують вимоги до виробів, які експлуатуються у вибухонебезпечних середовищах.

7.2.8 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.

2.7.9 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» 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.

7.3 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. 7.3) 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.

а)

б)

Рисунок 7.3 – Монтаж доводчика дверей
а) – на дверях; б) – на дверній коробці

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. 7.4) і защіпки (рис. 7.5), які на практиці поділяють на електромеханічні і електромагнітні.

а)

б)

Рисунок 7.4 – Електричні керовані замки
а) – електромеханічний; б) – електромагнітний

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.

Рисунок 7.5 – Електрозащіпка

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.

7.4 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. 7.6) 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 7.6 – Напівзростовий турнікет
а) – нормальнозакритий; б) – нормальновідкритий

У турнікетах-триподах (рис. 7.7) 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.

Рисунок 7.7 – Турнікет-трипод електромеханічний

Роторний турнікет (рис. 7.8) – це турнікет із вертикально розташованою віссю, на якій закріплено три або чотири лопаті, які утворюють перегородки для запобігання несанкціонованому проходу.

а) б)

Рисунок 7.8 – Роторний турнікет
а) – з трьома лопатями; б) – з чотирма лопатями

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.

Зазвичай нормальновідкриті турнікети, які використовуються в метро (рис. 7.9), 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.

Рис. 7.9 – Нормальновідкритий турнікет, який використовується в метро

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.

Повнозростові турнікети (рис. 7.10) являють собою виконавчий пристрій на повний зріст людини, який містить трьох- або чотирьохлопатеву вертушку

розташовану на його вертикальній осі для запобігання несанкціонованому проходу.

Рис. 7.10 – Повнозростовий турнікет

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. 7.11, 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. 7.11, б) 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.

а) б) в)

Рисунок 7.11 – Повнозростові пропускні пристрої шлюзового типу
а) та б) – пропускні кабіни (тамбур-шлюзи); б) – трьохлопатевий турнікет блокуючого типу

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.

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).

Рекомендована література: [2; 4; 5; 7; 8].

Запитання для самоконтролю

1. За яким принципом відбувається блокування дверей в електромеханічному та електромагнітному замку?
2. За якими критеріями визначають підвищену та високу стійкість ЗКП?
3. На які класи поділяють виконавчі пристрої в залежності від ступеня їх застосування?
4. Наведіть та поясніть ключові переваги нормальновідкритих турнікетів над нормальнозакритими турнікетами.
5. Назвіть категорії класифікації ЗКП за видом перекривання проєму.
6. Назвіть основні показники надійності ЗКП.
7. Назвіть особливості та параметри вибору замкового пристрою.
8. Назвіть та опишіть основні показники стійкості до НСД руйнівного типу, які поширюються на ЗКП.
9. Назвіть та опишіть способи керування, за якими класифікуються ЗКП.
10. Опишіть конструктивні особливості турнікета-трипода та роторного турнікета.
11. Опишіть характерні особливості шлюзових тамбурів, які забезпечують підвищений рівень безпеки.
12. Поясніть критичну відмінність між електромеханічними та електромагнітними замками щодо їх стану у випадку аварійної ситуації.
13. Поясніть принципову відмінність між типами напівзростових турнікетів.
14. У чому полягає принцип шлюзування, і як він реалізується в пропускних кабінах?
15. У яких випадках рекомендовано не застосовувати резервування електроживлення виконавчих пристроїв ЗКП?

16. Функціональне призначення доводчика дверей та які ключові параметри слід враховувати під час його вибору.

17. Як відбувається підведення електричного живлення та керуючих сигналів до електромеханічних та електромагнітних замків;

18. Яким чином в ЗКП забезпечують аварійне відкривання?

19. Яким чином виконавчі пристрої визначають рівень та якість виконання функції затримання?

20. Яким чином у турнікетах досягається виключення несанкціонованого їх проходу?

21. Які допустимі відхилення напруги та частоти мережі змінного струму повинні зберігати ЗКП для забезпечення працездатності?

22. Які завдання замовника вирішуються за допомогою напівзростових турнікетів?

23. Які ключові критерії слід враховувати під час вибору типу пропускного пристрою для контрольно-пропускного пункту?

24. Які основні функції повинні забезпечувати загороджувальні керовані пристрої?

25. Які пристроїв, які забезпечують фізичне перешкоджання доступу, прийнято відносити до ЗКП?

26. Які режими управління передбачені для ЗКП?

27. Яку ключову функцію реалізують виконавчі пристрої в СКУД?

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Access Control Systems : Security, Identity Management and Trust Models. URL: https://surl.li/pophrl (дата звернення 28.08.2025).
2. Boddu Raghu. SAP Access Control. Quincy : SAP PRESS, 2023. 695 p.
3. Brian Rhodes. Access Control. URL: https://surl.lu/xvxphm (дата звернення 28.08.2025).
4. Harold F. Tipton, Micki Krause. Information Security Management : Handbook. URL: https://surl.lu/oqhegu (дата звернення 28.08.2025).
5. Kris Hermans. Mastering Access Control : A Comprehensive Guide to Learn Access Control. Traverse City : Independently published, 2023. 393 p.
6. Matej Csányi. Access Control in Operating Systems. URL: https://is.muni.cz/th/uny2u/ xcsanyi_bc.pdf (дата звернення 28.08.2025).
7. Mike Chapple. Access Control and Identity Management. Burlington : World Headquarters Jones & Bartlett Learning, 2021. 376 p.
8. Thomas Norman. Electronic Access Control. URL: https://surl.li/oybgwe (дата звернення 28.08.2025).

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

Системи контролю та управління доступом: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 (F) Інформаційні технології спеціальності 126 (F6) Інформаційні системи та технології денної та заочної форм навчання / уклад. О. Л. Кайдик, Т. В. Терлецький, А. А. Ткачук. Луцьк : ЛНТУ, 2025. 132 с.

Комп'ютерний набір та верстка: О. Л. Кайдик.

Редактор: в авторській редакції.

Підп. до друку «___» _____ 2025 р.
Формат 60x84/16. Папір офс. Гарн. Таймс.
Ум. друк. арк. 8,25. Обл. – вид. арк. 7,72.
Тираж _50_ прим. Зам. ______.

Луцький національний технічний університет
43018 м. Луцьк, вул. Львівська, 75