МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Державний університет інформаційно-комунікаційних технологій

СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ НА ОБ'ЄКТИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Курс лекцій

для студентів спеціальності

125 «Кібербезпека та захист інформації»

Київ 2024

УДК 004.934:681.391

Схвалено Вченою радою Навчально-наукового інституту захисту інформації Державного університету інформаційно-комунікаційних технологій (протокол № 9 від 22.04.2024 р.).

Котенко А.М. Курс лекцій для студентів з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації» з дисципліни «Системи контролю та управління доступом на ОІД»/ А.М. Котенко. Державний університет інформаційно-комунікаційних технологій,–К., ДУІКТ, 2024. – 79 с.

ЗМІСТ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

1. Лекції з дисципліні «Системи контролю та управління доступом на ОІД» для студентів спеціальності 125 «Кібербезпека та захист інформації» охоплюють розділи курсу навчання, що пов’язані з питаннями організації захисту об’єктів інформаційної діяльності у контексті забезпечення їх інформаційної безпеки.

2. Мета лекційних занять полягає у ознайомленні студентів з існуючими системами, що забезпечують санкціонований доступ людини на об’єкт інформаційної діяльності.

Дисципліна вивчає склад систем контролю управління доступом, принцип їх функціонування та особливості застосування на ОІД.

Результатомвивченнянавчальноїдисципліниє набуття студентомнаступних компетентностейпов’язанихізздатністю:

- знати та розуміти предметну область та розуміти професійну діяльність;
- здійснювати технологічне управління побудовою систем захисту інформації на основі аналізу джерел загроз та засобів їх впливу на об’єкти інформаційної безпеки та ризиків інформаційної безпеки;
- проводити атестацію та сертифікацію технічних засобів та інформаційних ресурсів;
- проводити атестацію та сертифікацію об'єкта інформаційної діяльності спираючись на облік та обстеження виробів, продукції, обладнання об’єкта в тому числі і спеціального призначення з фіксуванням результатів у відповідних документах.

Лекція № 1.

Тема: Загальна концепція безпеки та принципи створення фізичної системи безпеки інформації

Зміст лекції:

1. Організація контрольно-пропускного режиму на підприємстві.
2. Призначення СКУД. Класифікація СКУД.
3. Основні можливості системи контролю й керування доступом.

1. Організація контрольно-перепускного режиму на підприємстві.

Для впорядкування допуску співробітників і відвідувачів (клієнтів), а також транспорту на територію і в приміщення підприємства, що охороняється організовується контрольно-пропускний режим (КПР) - комплекс організаційно-правових обмежень і правил, які визначають порядок пропуску через контрольно-пропускні пункти (КПП) в окремі будівлі (приміщення) людей, транспорту і матеріальних засобів. КПР є одним з ключових моментів в організації системи безпеки на підприємстві. З цих позицій він являє собою комплекс організаційних заходів (адміністративно-обмежувальних), інженерно-технічних рішень і дій служби безпеки.

Механізм здійснення КПР грунтується на застосуванні «заборон» і «обмежень» щодо суб'єктів, що перетинають кордони охоронюваних об'єктів, для забезпечення інтересів підприємства. Такий механізм повинен відповідати вимогам чинного законодавства, статуту підприємства, а також іншим нормативно-правовим актам, що регулюють діяльність підприємства. Основні напрямки створення КПР на підприємстві: визначення та оцінка вихідних даних, розробка заходів та нормативних документів, обладнання КПП. Система контролю і управління доступом є третім рубежем захисту після системи відеоспостереження та охоронно-пожежної сигналізації.

Тут і далі під «підприємством» будемо розуміти ту чи іншу організацію незалежно від форми власності. Підприємство може складатися з об'єктів.

Цілі і завдання створення контрольно-пропускного режиму

Основними цілями створення КПР є:

• захист законних інтересів підприємства, підтримка порядку внутрішнього управління;

• захист власності підприємства, її раціональне та ефективне використання;

• зростання прибутків підприємства;

• внутрішня і зовнішня стабільність підприємства;

• захист комерційних секретів і прав на інтелектуальну власність.

КПР як частина системи безпеки дозволяє вирішити наступні завдання:

• забезпечення санкціонованого проходу співробітників і відвідувачів, ввезення/вивезення продукції і матеріальних цінностей, ритмічної роботи підприємства;

• запобігання безконтрольного проникнення сторонніх осіб та транспортних засобів на охоронювані території і в окремі будівлі (приміщення);

• своєчасне виявлення загроз інтересам підприємства, а також потенційно небезпечних умов, що сприяють нанесенню підприємству матеріальної та моральної шкоди;

• створення надійних гарантій підтримки організаційної стабільності зовнішніх і внутрішніх зв'язків підприємства, відпрацювання механізму оперативного реагування на загрози та негативні тенденції;

• припинення посягань на законні інтереси підприємства, використання юридичних, економічних, організаційних, соціально-психологічних, технічних та інших засобів для виявлення і ослаблення джерел загроз безпеці підприємства.

КПР можна визначити як систему забезпечення нормативних, організаційних і матеріальних гарантій виявлення, попередження і припинення посягань на законні права підприємства, його майно, інтелектуальну власність, виробничу дисципліну, технологічне лідерство, наукові досягнення і охоронювану інформацію і як сукупність організаційно-правових обмежень і правил, встановлюють порядок пропуску через КПП співробітників об'єкта, відвідувачів, транспорту ввезення / вивезення матеріальних цінностей.

Нормативні гарантії полягають у тлумаченні та реалізації норм права, з'ясуванні меж їх дії, у формуванні необхідних правовідносин, визначенні та забезпеченні правомірної діяльності підрозділів і працівників підприємства з приводу її безпеки, використання обмежувальних заходів, застосування санкцій до фізичних і юридичних осіб, які посягають на законні інтереси підприємства.

Організаційні гарантії формуються шляхом розробки, побудови та підтримки високої працездатності загальної організаційної структури управління процесом виявлення і придушення загроз діяльності підприємства, використання ефективного механізму стимулювання його оптимального функціонування, а також відповідної підготовки кадрів.

Матеріальні гарантії формуються за рахунок виділення і використання фінансових, технічних, кадрових, інтелектуальних, інформаційних та інших ресурсів підприємства, що забезпечують своєчасне виявлення, ослаблення і придушення джерел загрози, запобігання і локалізацію можливого збитку, створення сприятливих умов для діяльності підприємства.

Основні заходи КПР розробляються службою безпеки підприємства, затверджуються його керівником і оформляються інструкцією про КПР.

Відповідальність за організацію КПР покладається на начальника служби безпеки. Практичне здійснення КПР покладається на охорону (чергових по КПП, контролерів, охоронців), працівники якої повинні знати встановлені на об'єкті правила КПР, діючі документи по порядку пропуску на об'єкт (з об'єкта) співробітників і відвідувачів, ввозу/вивезення товарно-матеріальних цінностей .

КПР може бути встановлений як в цілому по підприємства, так і в окремих корпусах, будівлях, відділах та інших спеціальних приміщеннях.

Підготовка вихідних даних для організації контрольно-пропускного режиму

Розробка заходів та нормативних документів КПР починається з визначення вихідних даних. Доцільно запропонувати наступний порядок визначення та оцінки вихідних даних.

Організаційна структура підприємства, розташування його окремих елементів і характер виробництва (діяльності) на них. З'ясування цих питань дозволяє вирішити наступні практичні завдання:

виділити об'єкти, майданчики, будівлі та приміщення, на яких необхідно організувати КПР;

визначити характер КПП для пропуску співробітників і транспортних засобів.

Оцінка «добового обсягу» потоків транспортних засобів, вантажів, матеріальних цінностей і людей (персоналу фірми і відвідувачів), що проходять через КПП і в окремі будівлі (приміщення). Тільки на основі оцінки реального стану місць пропуску можна оцінити пропускну спроможність діючих КПП і привести її у відповідність із завданнями об'єкта. Така оцінка дозволить вибрати оптимальний варіант автоматизації та контролю проходу (проїзду) на охоронювані території.

Виділення (за ступенем важливості) категорії об'єктів, транспортних засобів і вантажів, а також категорії осіб, які перетинають встановлені межі. Для досягнення чіткості у визначеннях пропонується приміщення і територію об'єкта класифікувати залежно від умов доступу і ступеня захищеності.

Для організації пропускного режиму також необхідно розподілити об'єкти підприємства (будинку, приміщення) на такі зони: загальнодоступні, закриті та обмеженого доступу. Визначення категорій режиму може дати чітку відповідь на питання, які потрібно прояснити при організації КПР і розробці вихідної документації з обладнання об'єкта технічними засобами охорони. Закріплення за приміщенням конкретної категорії допомагає регламентувати і обґрунтувати:

- умови доступу співробітників підприємства і відвідувачів в ту чи іншу зону,
- пропозиції адміністрації підприємства з вироблення оптимального варіанту порядку пропуску осіб, транспортних засобів та матеріальних цінностей на об'єкти підприємства;
- наявність і вид фізичної охорони;
- види використовуваних технічних засобів для забезпечення безпеки.

Розробка інструкції про перепускний режим.

Оцінюючи вихідні дані, розробник визначає основні положення інструкції про КПР. Практичне вирішення питань, пов'язаних з організацією пропускного режиму, оформляється у вигляді «Інструкції про пропускний режим». **Зазначена інструкція повинна визначати систему організаційно-правових охоронних заходів, що встановлюють дозвільний порядок (режим) проходу (проїзду) на підприємство (з підприємства), і може включати шість розділів:**

- загальні положення;
- порядок проходу через КПП підприємства;

- порядок в'їзду (виїзду) транспортних засобів і провезення матеріальних цінностей;
- види перепусток і порядок їх оформлення;
- обов'язки посадових осіб з підтримання КПР;
- облік і звітність, порядок зберігання перепусток, печаток.

У розділі **Загальні положення** зазначаються:
- нормативні документи, на підставі яких складався інструкція,
- визначення КПР і мета його введення,
- посадові особи, на яких покладається організація та практичне керівництво контрольно-пропускний системою;
- санкції до порушників КПР;
- вимоги до обладнання різних приміщень.

У розділі**Порядок проходу через КПП підприємства** визначається порядок пропуску співробітників підприємства, відряджених осіб і відвідувачів через КПП. У цьому розділі рекомендується:
- перелічити всі КПП і їх призначення, опис, розташування і едину нумерацію;
- викласти вимоги до обладнання КПП;
- встановити порядок проходу співробітників і відвідувачів на територію підприємства і в його категорійовані приміщення;
- визначити права і основні обов'язки контролерів КПП;
- встановити приміщення, де забороняється приймати відвідувачів і представників сторонніх організацій.

У розділі **Порядок в'їзду (виїзду) транспортних засобів і провезення матеріальних цінностей** визначається порядок допуску на підприємство транспортних засобів, ввезення/вивезення продукції, документів і матеріальних цінностей. У цьому розділі зазначаються:

- порядок допуску на територію об'єкта (з об'єкта) підприємства автотранспорту, що належить даному підприємству;

- порядок в'їзду та стоянки на території об'єктів транспорту, що належить співробітникам на правах особистої власності;

- порядок пропуску автомашин сторонніх організацій, які прибули з вантажем на адресу об'єкта в робочий і неробочий час;

- порядок ввезення/вивезення товарно-матеріальних цінностей;

- правила оформлення документів на вивезення (винесення) матеріальних цінностей з території об'єктів підприємства.

У розділі**Види перепусток і порядок їх оформлення** визначаються:
- види перепусток, їх кількість і статус;
- опис перепусток;
- порядок оформлення і видачі перепусток;
- порядок заміни та перереєстрації перепусток;
- заходи, що проводяться при втраті пропуску співробітником.

У розділі**Обов'язки посадових осіб з підтримання КПР** докладно описуються обов'язки посадових осіб з підтримання КПР як у нормальному режимі, так і при виникненні надзвичайних ситуацій (НС).

Розділ**Облік і звітність, порядок зберігання перепусток, печаток** присвячується обліку та звітності документації, що ведеться на КПП, і порядку зберігання пропусків і печаток.

При розробці інструкції про КПР визначаються види і групи перепусток які діятимуть на підприємстві. На великих підприємствах, як правило, встановлюється декілька видів перепусток. Це можуть бути постійні, тимчасові, разові і матеріальні пропуску. Зразки бланків перепусток розробляються адміністрацією об'єкта (службою безпеки). За своїм зовнішнім виглядом і змістом пропуску повинні відрізнятися один від одного і мати деякими ступенями захисту. Всі види перепусток, за винятком матеріальних, оформляються і видаються бюро перепусток(або іншим підрозділом) за письмовими заявками. Види пропусків визначаються залежно від специфіки підприємства. Матеріальні перепустки для вивезення (винесення) товарно-матеріальних цінностей видаються адміністрацією підприємства. Термін дії пропуску визначається інструкцією про КПР. Матеріальні пропуску повинні вилучатися на КПП і здаватися в бюро перепусток. Зразки діючих перепусток повинні знаходитися на КПП. Для навчання працівників охорони виділяється необхідне число зразків пропусків.

Встановлюючи і забезпечуючи порядок переміщення персоналу і відвідувачів по території підприємства, система КГ1Р вирішує не тільки питання безпеки підприємства, а й питання раціональної організації праці.

У контрольно-пропускному залі влаштовуються проходи, які обладнано технічними засобами охорони та фізичними бар'єрами. У комплекти обладнання, як правило, входять:

- засоби механізації, автоматизації системи контролю доступу;
- фізичні бар'єри (огорожі, турнікети, хвіртки);
- основне і резервне освітлення;
- засоби зв'язку і тривожної сигналізації;
- системи відеоконтролю.

Турнікети призначені для керування потоками людей і регулювання входу (виходу). В якості засобів контролю доступу можуть використовуватися різні турнікети. Останнім часом найбільш широке поширення отримали електромеханічні турнікети, які на відміну від громіздких і незручних в управлінні механічних легко управляються з пульта охоронця і можуть працювати в складі автоматизованої системи контролю доступу. Для здійснення надійного контролю частіше використовуються «нормально закриті» турнікети: роторні турнікети-вертушки, турнікети-триподи і хвіртки.

Хвіртки застосовуються для управління потоками людей, організації вільного проходу в одну сторону (на вхід або вихід) і заборони проходу в іншу. Хвіртки широко використовуються в магазинах, аеропортах, вокзалах. Застосування хвірток для контролю доступу неефективно, це пов'язано з тим, що хвіртки не поділяють потік людей по одному, так як після відкриття хвіртки через неї можуть пройти кілька людей. Хвіртки можуть встановлюватися для організації вільного виходу, тоді як контроль входу довіряють триподі або вертушкам.

Турнікети-триподи з трьома планками, що перетиняються, є одним з найбільш оптимальних засобів для здійснення контролю санкціонованого проходу. Триподи мають сучасний елегантний вигляд і легко монтуються. Триподи дозволяють здійснювати ефективний контроль доступу, так як розділяють потік людей по одному, забезпечуючи при цьому високу пропускну здатність. Триподи можуть застосовуватися в системах електронних прохідних, в тому числі в умовах великого потоку людей. Для запобігання можливості підлізти під планки турнікета або перескочити через них на турніку рекомендується встановлювати спеціальні датчики, які спрацьовують при спробі несанкціонованого проходу.

Роторні турнікети-вертушки застосовуються в тих випадках, коли необхідно повне перекриття зони проходу. Вони можуть бути різними за висотою - від поясних до турнікетів на повний зріст.

Для організації в'їзду (виїзду) транспорту створюються транспортні КПП. До складу транспортного КПП входить доглядова майданчик і службові приміщення.

Контрольно-проїзні пункти для пропуску авто-та залізничного транспорту обладнуються:

- розсувними або розпашними воротами і шлагбаумами з механічним, електромеханічним і гідравлічним приводами, а також пристроями для аварійної зупинки воріт і відкривання їх вручну,
- контрольними майданчиками з помостами для перегляду автомобілів;
- світлофорами, попереджувальними знаками і світловими табло типу «Бережися автомобіля» та ін;
- телефонного та тривожної зв'язком і освітленням для огляду транспорту.

Доглядова майданчик призначена для розміщення автомобілів при їх огляді. Доглядові майданчики можуть розташовуватися як на території підприємства, так і за її межами, на території, що безпосередньо примикає до КПП.

Доглядова майданчик повинен відповідати наступним вимогам:

- мати достатню площу для розміщення оглядаємо транспорту і технічних засобів для забезпечення нормальних умов роботи охорони;
- виключати можливість несанкціонованого проникнення на об'єкт (з об'єкта) людей і транспортних засобів;
- забезпечувати при встановленій інтенсивності руху в будь-який час доби і року огляд автомобільного транспорту та перевозимих вантажів;
- бути ізольованою від інших споруд, що не мають відношення до охорони об'єкта та обладнанню КПП;
- забезпечувати заходи безпеки охорони при виконанні обов’язків.

Розміри досмотрових майданчиків можуть становити: 10-12 м в довжину і 5 ¬ 6 м завширшки. На проїжджій частині майданчика виділяється місце зупинки транспорту для огляду, обмежене двома лініями «СТОП», виконаними білою фарбою Транспортні КПП можуть обладнуватися світлофорами, вагами для зважування автомобілів, досмотровою ямою або естакадою для огляду

вантажів, механізованими пристроями для автоматичного відкриття і закриття воріт з фіксаторами.

Електромеханічне обладнання КПП для автомобільного транспорту зазвичай містить: електродвигуни приводу воріт; кінцеві вимикачі автоматичного відключення електродвигунів при повністю закритих і відкритих стулках воріт, магнітні пускачі електродвигунів, електрообладнання світлофорів; кабельні, силові лінії.

Доглядові майданчика по периметру обладнуються фізичними бар'єрами і кордоном сигналізації. Майданчики, як правило, затуляються парканом з металевої сітки або декоративних грат висотою до 2,5 м. На майданчику обладнуються основні і допоміжні механізовані ворота. Основні ворота встановлюються на лінії основного огорожі об'єкта, а допоміжні - на протилежній стороні досмотрового майданчика. Замість воріт можуть застосовуватися механізованому ¬ ванні шлагбауми. На автомобільних КПП використовуються ворота з обмеженням і без обмеження габаритів по висоті. По конструкції вони можуть бути орними або розсувними (висувними). Ворота повинні обладнуватися фіксаторами Для регулювання руху транспорту, що проходить через проїзди доглядових майданчиків КПП, можуть застосовуватись двосекційні світлофори з лінзами червоного і зеленого кольору.

2. Призначення СКУД. Класифікація СКУД.

Захист будь-якого об'єкта включає кілька рубежів, число яких залежить від рівня режимності об'єкта. При цьому у всіх випадках важливим рубежем буде система управління контролю доступом (СКУД) на об'єкт.

Під СКУД розуміється сукупність програмно-технічних і організаційно-методичних засобів, за допомогою яких вирішується завдання контролю і управління доступом до приміщення підприємства і окремих приміщень, а також оперативний контроль за пересуванням персоналу і часу його знаходження на території підприємства.

Такі системи можуть здійснювати контроль переміщення людей і транспорту по території охоронюваного об’єкта, забезпечувати безпеку персоналу і відвідувачів, а також збереженість матеріальних і інформаційних ресурсів підприємства. Системи контролю й керування доступом використовуються на промислових підприємствах, в офісах, магазинах, на автостоянках і автосервісах, в житлових приміщеннях.

Інтерес до систем контролю і управління доступом зростає ще й тому, що наявність такої системи важливо для ефективної роботи підприємства. Контроль не тільки істотно підвищує рівень безпеки, але й дозволяє оперативно реагувати на поведінку персоналу і відвідувачів. Також важливим завданням для багатьох підприємств є необхідність контролювати графік і вести облік робочого часу. Особлива увага приділяється системам, що дозволяє вибудовувати необхідні конфігурації з стан дротяних блоків, враховуючи всі особливості підприємства.

Існуючі керівні документи у цілому поділяють СКУД за наступними ознаками:

- за способом управління;
- число контрольованих точок доступу;
- функціональні характеристики;
- виду об'єктів контролю;
- рівню захищеності системи від несанкціонованого доступу.

Також відповідно до керівних документів всі СКУД діляться на чотири класи.

СКУД 1-го класу - малофункціональні системи малої ємності, що працюють в автономному режимі і здійснюють допуск всіх осіб, які мають відповідний ідентифікатор. У такій системі використовується ручне або автоматичне керування виконавчими пристроями, а також світлова або/і звукова сигналізація.

СКУД 2-го класу - монофункціональні системи. Вони можуть бути одноріневими і багаторівневими і забезпечують роботу як в автономному, так і в мережевому режимах. Допуск осіб (груп осіб) може здійснюватися за датою, тимчасових інтервалах. Система здатна забезпечити автоматичну реєстрацію подій і автоматичне управління виконавчими пристроями.

СКУД 3-го і 4-го класів, як правило, є мережевими. У них використовуються більш складні ідентифікатори та різні рівні мережевої взаємодії (клієнт-сервер, інтерфейси зчитувачів карт Віганда або магнітних карт, спеціалізовані інтерфейси та ін.)

3. Основні можливості системи контролю й керування доступом.

Основні можливості, які надає установка СКУД на об’єкті, що охороняється:

Контроль і керування доступом -це основна функція системи. Як уже було замічено раніше, за допомогою даної функції виробляється поділ прав доступу співробітників у певні приміщення, а також відмова в доступі небажаним особам. Крім того, можливо дистанційне керування пристроями, що блокують (замки, турнікети та ін.). СКУД дозволяє заборонити прохід для співробітників у святкові й вихідні дні, а також після закінчення робочого дня.

Збір і надання статистики. СКУД збирає інформацію про осіб, які пройшли через певні крапки контролю доступу. По кожному співробітнику можливе одержання наступної інформації: час входу й виходу, спроби доступу в заборонені для нього приміщення й зони, а також спроби проходу в недозволений час. Також можливо відстежити переміщення співробітника по території із вказівкою місця й часу. Таким чином, всі виявлені порушення трудової дисципліни можуть бути занесені в особисту справу співробітника, а керівництво порушника сповіщене в робочому порядку. Крім того, випливаючи інформації про останню крапку проходу, СКУД дозволяє визначитимісцезнаходження співробітника в будь-який момент часу.

Доступ співробітника тільки по особистому ідентифікаторі. При проході за допомогою ідентифікаційної карти на екрані монітора в пункті охорони може відображатися вся інформація зі співробітника і його фотографія, що виключає можливість проходу по чужому ідентифікаторі. Також на рівні правил реакції СКУД можна забезпечити захист від передачі ідентифікатора іншій особі й блокувати повторний вхід на територію об'єкта по тій же самій карті доступу.

Облік робочого часу. За допомогою убудованої в СКУД системи обліку робочого часу, реєструється час виходу на роботу й час відходу з робочого місця. У результаті надається можливість визначити сумарний час перебування співробітника на робочому місці з урахуванням обідів. А на самому початку дня, наприклад, в 9:30 система обліку робочого часу, убудована в СКУД, може формувати груповий звіт про співробітників, що не пройшли через контрольну крапку входу на територію. Це дозволяє в масовому порядку виявляти спізнілих або не співробітників, що з'явилися на робоче місце. Аналогічний звіт можна одержати й наприкінці робочого дня на пункті виходу з території підприємства або офісу.

Автономність роботи системи. СКУД оснащується системою безперебійного живлення, що дозволяє не переривати роботу у випадку відключення електрики в будинку. Також система контролю доступом завдяки функціоналові контролера має можливість продовжувати роботу, наприклад, при виході керуючого комп'ютера з ладу.

Охорона об'єкта в реальному часі. СКУД дає можливість ставити певні приміщення на охорону й знімати їх з охорони. Крім того, у реальному часі можна одержувати відомості про всілякі позаштатні й тривожні ситуації через спеціальні оповіщення відповідальних осіб. Крім цього в базі дані системи реєструються всі тривожні події й події, що дає можливість доступу до цієї інформації надалі при необхідності. Завдяки наявним у СКУД засобам, співробітник охорони зі свого робочого місця за допомогою комп'ютера має можливість не тільки управляти дверима й турнікетами, але й подавати сигнали тривоги. У комп'ютер СКУД у співробітника охорони можуть бути занесені поповерхові плани будинку зі схемою розташування контролерів обмеження доступу.

Віддалене керування системою через інтернет або з мобільного телефону. Якщо при установці підключити СКУД до мережі Інтернет, то в адміністрації з'являється можливість вести віддалене керування й контроль за роботою системи. Аналогічне можна сказати й про можливість керування СКУД зі свого мобільного телефону.

Інтеграція СКУД з іншими системами безпеки й охорони. Системиконтролю й керування доступом прекрасно сполучаються й вбудовуються з іншими системами безпеки: системою відеоспостереження, охоронною й пожежною сигналізацією. Так, наприклад, контроль доступом разом з відеоспостереженням забезпечують абсолютний контроль над охоронюваними приміщеннями. При виникненні позаштатної ситуації така система в найкоротший термін дозволить виявити й заблокувати порушника.

При інтеграції СКУД і охоронною сигналізацією є можливість настроїти спільну реакцію системи на несанкціоноване проникнення в те або інше приміщення. Наприклад, можна включити сирену на пункті охорони, тривожну лампу або ж і зовсім заблокувати всі двері в необхідній частині будинку. Інтеграція СКУД із системою пожежної сигналізації дозволяє автоматично розблокувати двері, турнікети й прохідні у випадку пожежі. Всі ці міри значно спрощують евакуацію персоналу в настільки важкий період.

Лекція № 2.

Тема: Склад системи контролю та управління доступом

Зміст лекції:

1. Ідентифікатор користувача.
2. Контролери СКУД.
3. Пристрої ідентифікаціїособи.

1. Ідентифікатор користувача.

Ідентифікатор користувача - це пристрій або ознака, за якою визначається користувач. Для ідентифікації застосовуються атрибутні і біометричні ідентифікатори. Як атрибутні ідентифікатори використовують автономні носії ознак допуску: магнітні картки, безконтактні проксіміті-карти, брелоки «тач-мемори», різні радіобрелки. Біометричні - зображення райдужної оболонки ока, відбиток пальця, відбиток долоні, риси обличчя і багато інших фізичні ознаки. Кожен ідентифікатор характеризується певним унікальним двійковим кодом. У СКУД кожному коду ставиться у відповідність інформація про права і привілеї власника ідентифікатора. У даний час застосовуються:

- безконтактні радіочастотні проксіміті-карти (proxmity) - найбільш перспективний в даний час тип карт. Безконтактні картки спрацьовують на відстані і не вимагають чіткого позиціонування, що забезпечує їх стійку роботу і зручність використання, високу пропускну здатність;

- магнітні картки - найбільш широко поширений варіант.

Існують карти з низькокоерцитивною і висококоерцитивною магнітною смугою і з записом на різні доріжки;

- карти Виганда (Wiegand) - названі по імені вченого, який відкрив магнітний сплав, у якого прямокутної петлею гистерезиса;

- штрих-кодові карти - на карту наноситься штриховий код. Є окремі норми-яття більш складний варіант - штрих-код закривається матеріалом,

- прозорим тільки в інфрачервоному світлі, зчитування відбувається в ІЧ-області;

- ключ-брелок «тач-меморі» (touch-memory) - металева таблетка, всередині якої розташований чіп ПЗУ.

Ідентифікатори користувачів СКУД можуть мати різний статус. Для забезпечення більшості необхідних в реальному житті вимог, як мінімум, треба, щоб контролери підтримували такі типи карт:

- постійна: для співробітників підприємства;

- тимчасова: з обмеженням терміну дії;

- «разова»: автоматично анулюється після вичерпання числа проходів;

- одноразова - окремий випадок разової карти.

2. Контролери СКУД.

Контролери - пристрої, призначені для обробки інформації від зчитувачів ідентифікаторів, ухвалення рішення і управління виконавчими пристроями. Саме контролери дозволяють прохід через пропускні пункти. Контролери різняться ємністю бази даних і буфера подій, що обслуговуються пристроїв ідентифікації.

Контролер СКУД складається з чотирьох основних частин (рис. 2.1): зчитувача, схем обробки сигналу, прийняття рішення і схеми буфера подій

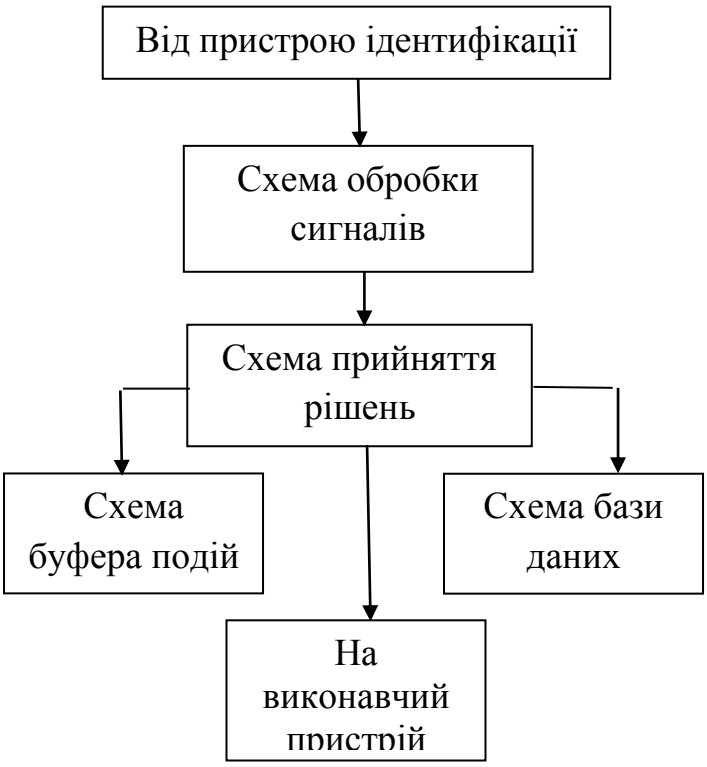

Рис. 2.1. Схема контролера СКУД

Зчитувач карт (пристрій ідентифікації) передає інформацію на схему обробки сигналів контролера. Далі інформація в цифровому вигляді видається на схему прийняття рішення, яка заносить факт спроби проходу в схему буфера подій, запитує схему бази даних на предмет правомірності проходу і в разі позитивної відповіді пускає в хід виконавчий пристрій. Обмеження вже знято, але система контролю доступу ще не завершила обробку інформації: сам факт проходу саме цю людину заноситься в схему буфера подій.

Незалежно від типу застосовуваних зчитувачів контролери повинні підтримувати такі режими доступу:

- по одній карті і / або ПІН-коду;
- доступ з підтвердженням оператором;
- контроль кількості людей в приміщенні (мінімум і максимум).

Останнє важливо в ситуаціях коли, наприклад, за умовами служби в приміщенні не повинно залишатися менш одного (двох, трьох) осіб.

Основу сучасних СКУД складають автоматичні і автоматизовані СКУД. У них процедура перевірки може включати також сопоставління особи, що перевіряється з відеопортретом на моніторі контролера. Сучасні автоматичні і автоматизовані СКУД в залежності від способу управління поділяються на **автономні, мережеві (централізовані) і розподілені (комбіновані)**

Автономні контролери - повністю закінчені пристрої, призначені для обслуговування, як правило, однієї точки проходу. Можливість об'єднання з іншими аналогічними контролерами не передбачена. Існує багато видів таких пристроїв: контролери, суміщені зі зчитувачем, контролери, вбудовані в електромагнітний замок і т. д. В автономних контролерах застосовуються зчитувачі самих різних типів. Як правило, автономні контролери розраховані на обслуговування невеликого числа користувачів, зазвичай не більше 500 осіб. Вони працюють з одним виконавчим пристроєм без передачі інформації на центральний пункт охорони і без контролю з боку оператора. Прикладом подібної системи контролю доступу може служити досить проста комбінація: «електромагнітний замок + зчитувач карт ідентифікації». Якщо необхідно контролювати тільки одні двері і в майбутньому розширення системи контролю доступу не планується, це оптимальне і досить недороге рішення.

Мережеві контролери можуть працювати в мережі під управлінням компьютера. У цьому випадку рішення приймає персональний комп'ютер з встановленим спеціалізованим програмним забезпеченням. Мережеві контролери застосовуються для створення СКУД будь-якого ступеня складності. Число мережевих контролерів в системі може бути від двох до кількох сотень з обміном інформацією з центральним пунктом охорони і контролю. У цьому випадку розміри системи контролю доступу визначаються по числу пристроїв ідентифікації, а не за кількістю контрольованих дверей, оскільки на кожні двері може бути встановлено один-два пристрої ідентифікації в залежності від застосовуваної технології проходу.

Використовуючи мережеві контролери, адміністрація отримує ряд додаткових можливостей:

- отримання звіту про присутність або відсутність співробітників на роботі;
- уточнення місцезнаходження конкретного співробітника;
- ведення табеля обліку робочого часу;
- складання звіту про переміщення співробітників практично за будь-який період часу;

- формування часових графіків проходу співробітників;
- ведення бази даних співробітників (електронної картотеки).

Мережеві СКУД використовуються на великих підприємствах і в тих випадках, якщо потрібні її специфічні можливості, такі, як облік робочого часу співробітників. Мережеві контролери об'єднуються в мережу.

До базових характеристик мережевих контролерів відносять такі кількісні характеристики:

- число підтримуваних точок проходу;
- обсяг бази даних користувачів,
- обсяг буфера подій.

Число підтримуваних точок проходу. Оптимальне рішення в цьому випадку наступне: один мережевий контролер на дві точки проходу, так як загальні ресурси (корпус, джерело живлення з акумулятором) потрібні в меншій кількості. Контролери з великим числом обслуговуваних дверей існують, але їх небагато з наступних причин:

- висока вартість джерела живлення на 4-5 Ампер з резервуванням;
- збільшується вартість комунікацій між контролером і дверима. Крім того, якщо двері розташовані далеко один від одного, то стає проблемою і прокладка дроти живлення замка, так як при токах споживання близько 1 А виникають великі втрати.

Обсяг бази даних користувачів визначається виключно кількістю людей, які будуть ходити через максимально напружену точку проходу (прохідну).

Обсяг буфера подій визначає, скільки часу мережева система зможе працювати при вимкненому (завислому, згорілому) комп'ютері, не втрачаючи інформації про події. Наприклад, для офісу з числом співробітників близько 20 осіб обсягу буфера подій, що дорівнює 1000, може вистачити на тиждень. А для заводської прохідної, через яку проходить 3 тис. чоловік, і буфера на 10 тис. подій з працею вистачить на добу.

Практично всі контролери підтримують інтерфейс Віганда, і практично всі типи зчитувачів, в тому числі і біометричні, підтримують цей формат.

Сучасний контролер доступу повинен підтримувати гнучку систему тимчасових розкладів, на основі яких приймається рішення про доступ тієї чи іншої людини. При цьому стандартні тижневі цикли з вихідними днями - це найпростіше рішення. Реально ще потрібно задавати свята, робочі дні в свята, а найголовніше різні «плаваючі» графіки по типу «доба через три» і т. П У професійному контролері тимчасові розкладу можуть управляти не тільки доступом користувачів, а й автоматично відкривати і закривати двері в заданий час, ставити на охорону і знімати приміщення з охорони (при наявності охоронних функцій), перемикати додаткові реле.

Комбіновані контролери поєднують функції мережевих і авто-автономних контролерів. При наявності зв'язку з керуючим комп'ютером (онлайн)

контролери працюють як мережеві пристрої при відсутності зв'язку - як автономні.

Суміжні функції контролерів. В першу чергу це функції підтримки охоронно-пожежної сигналізації, інтеграції з підсистемами телеспостереження і керування деякими функціями оповіщення і пожежегасіння. можлива також підтримка локальних комп'ютерних мереж з різними робочими станціями і правами доступу, передачі інформації через Інтернет.

3. Пристрої ідентифікації особистості (зчитувачі).

Для ідентифікації особистості сучасні електронні системи контролю доступу використовують пристрої декількох типів в залежності від застосовуваного виду ідентифікатора користувача. У літературних джерелах, присвячених опису різних СКУД, часто можна зустріти підміну поняття аутентифікація, поняттям верифікація. Це пов'язано, по видимому, з наступним:

- в науці існує поняття «верифікація» (від лат. verus - істинний і facio - роблю), яке означає перевірку, емпіричне підтвердження теоретичних положень науки шляхом зіставлення їх з спостерігаються об'єктами, тактильними даними, експериментом;
- в програмуванні та інформатики існує поняття «авторизація користувача», яке означає перевірку відповідності користувача терміналу в мережі ЕОМ пред'явленим ідентифікатором (застосовується для захисту від несанкціонованого доступу і вибору відповідного режиму обслуговування);
- в програмуванні існує також поняття «верифікація», яке означає формальне доказ правильності програми, а також контроль, перевірку вводяться оператором даних.

Таким чином, існує деякий перетин в визначеннях, пов’язаний з використанням слів «перевірка» і «підтвердження». Звідси перенесення названих термінів в іншу предметну область (СКУД), очевидно, носить досить умовний характер. Вони означають встановлення автентичності особистості (об'єкта). Допуск здійснюється при безпосередньому «фізичному контакті» з користувачем в процесі ідентифікації та автентифікації його особистості. *Ідентифікація* - це процедура впізнання об'єкта (людини-користувача) за пред'явленим ідентифікатором, встановлення тотожності об'єкта або особи за сукупністю загальних і приватних ознак. На відміну від ідентифікації *автентифікація* має на увазі встановлення автентичності особистості на основі повідомляються перевіряється суб'єктом відомостей про себе. Такі відомості називають ідентифікаційними ознаками.

Пристрої ідентифікації (зчитувачі) розшифровують інформацію, записану на картках або ключах інших типів, і передають її в контролер частіше у

вигляді цифрової послідовності. Зчитувачі карток доступу можуть бути контактні і безконтактні. Можливі такі способи введення ознак:

- ручний, здійснюваний шляхом натискання клавіш, повороту перемикачів і т. д;
- контактний - в результаті безпосереднього контакту між людиною і ідентифікатором;
- дистанційний (безконтактний) при піднесенні ідентифікатора до зчитувача на певну відстань.

Для отримання інформації про біологічних ознаках людини використовують спеціальні біометричні зчитувачі (термінали), а введення ПІН-коду здійснюється з клавіатур різних типів

Саме зчитувачі визначають зовнішній вигляд і основні експлуатаційні характеристики всієї системи. Розглянемо принципи їх роботи.

Кнопкові клавіатури Принцип дії досить ясний: якщо набраний на клавіатурі код доступу вірний, то прохід на територію, що захищається дозволений. Кодонабірні пристрої іноді поєднуються зі зчитувачем карт, у цьому випадку код служить для підтвердження факту 20 анкціонованого використання карти.

Зчитувчі штрих-кодів в даний момент практично не встановлюються у системи контролю доступу, оскільки підробити пропуск надзвичайно просто на принтері або на копіювальному апараті.

Зчитувачі магнітних карт. Основним елементом зчитувача магнітних карт є магнітна головка, аналогічна магнітофонного. Код ідентифікації зчитується при пересуванні карти з магнітною смугою.

Основні переваги таких ідентифікаторів:

- вартість зчитувачів і магнітних карт досить низька;
- можлива зміна коду магнітної карти за допомогою кодувальника.

Основні недоліки:

- захищеність від несанкціонованого доступу невелика, оскільки порушник, заволодівши на досить обмежений час чужій картою, може підробити стільки її дублікатів, скільки йому потрібно;
- зчитувачі магнітних карт досить ненадійні в експлуатації: магнітні головки з часом засмічуються і зміщуються;
- низька пропускна здатність такої системи контролю доступу, оскільки часто доводиться ідентифікувати магнітну карту кілька разів;
- карти з магнітною смугою вимагають досить дбайливого зберігання, необхідно уникати впливу електромагнітних полів.

З наведених причин складні системи контролю доступу досить рідко комплектуються подібними пристроями ідентифікації особистості. Магнітні картки метро - виключення з правила, що пояснюється дешевизною технології.

Зчитувачі безконтактних карт (інтерфейс Віганда). Зчитувач являє собою індукційну котушку з двома магнітами, яка знаходиться в пластиковому або металевому корпусі і для повної герметичності залита спеціальним ізоляційним матеріалом. При проведення пластикової карти через зчитувач система контролю доступу отримує бінарний код карти. Зчитування ведеться безконтактним індукційниим методом.

Коротко про головне:

- висока надійність завдяки простоті пристрою;
- неможливість підробки пластикової карти, так як відсутня інформація про структуру;
- висока стійкість пластикової карти до зовнішніх впливів: щоб зіпсувати карту, її необхідно зламати.

Зчитувачі проксіміті-карт Такі карти дозволяють робити дистанційну ідентифікацію особистості. Усередині зчитувача знаходиться приймально-передавальна антена і електронна плата обробки сигналів.

Зчитувачі ключів «тач-меморі». Зчитувач «тач-меморі» вкрай простий і представляє з себе фактично контактну площадку, призначену для дотику спеціальних ключів. Ключ «тач-меморі» являє собою спеціальну мікросхему, розміщену в циліндричному корпусі з нержавіючої сталі.

Порівняння різних технологій ідентифікації особистості, найбільш поширених в сучасних системах контролю доступу, проводиться по найбільш важливим для споживача параметрами. Переваги та недоліки різних технологій ідентифікації наведені в табл. 2.1.

Таблиця 2.1

Переваги та недоліки різних технологій ідентифікації

Параметр	Інтерфейс Віганда	Проксіміті-технологія	Магнитні карти
Витрати на експлуатацію зчитувача	-	Низькі	Великі
Скритність коду	Высока	Середня	Низька
Час життя карти	Великий	Великий	Малий
Час життя зчитувача	Великий	Середній	Малий
Впливелектромагнітних полів	-	Високий	Високий
Вартість інсталяції	Середня	Висока	Низька
Вартість експлуатації	Низька	Середня	Висока
Можливість зміни коду	-	-	Є
Пропускна здастність	Середня	Висока	Низька

З порівняння різних технологій ідентифікації особистості можна зробити наступні висновки:

- системи контролю доступу, що використовують магнітні картки, не отримали широкого поширення;

найбільш практичною є технологія, яка використовує інтерфейс Віганда;

- в тих випадках, коли треба забезпечити високу пропускну здатність, скритність місця установки зчитувача або необхідність дистанційного доступу найбільш доцільно застосовувати проксіміті-технологію;
- з метою розширення сфери застосування системи контролю доступу повинні містити в собі комплекс, спільно використовує інтерфейс Віганда і проксіміті-технологію.

Найменш захищеними від фальсифікації вважаються магнітні карточки, найбільш захищеними - карти Віганда і проксіміті. Карти Віганда мають високі надійність і стійкість до зовнішніх впливів, невисоку вартість зчитувача карт, практично неможливо підробити.

Біометричні зчитувачі. Проблема виключення підробки і крадіжки ідентифікаторів вирішується шляхом використання індивідуальних ознак людини - біометричних ідентифікаторів: відбитків пальців, геометрії кисті руки, малюнка райдужної оболонки і кровоносних судин сітківки ока, теплового зображення особи, динаміки підписи, спектральних характеристик мови.

Діапазон проблем, вирішення яких може бути знайдено з використанням цих нових технологій, надзвичайно широкий:

- запобігти проникненню зловмисників на охоронювані території і в приміщення за рахунок підробки, крадіжки документів, карт, па¬ролей;
- обмежити доступ до інформації і забезпечити персональну відповідальність за її збереження;
- забезпечити допуск до відповідальних об'єктах тільки сертифікованих фахівців;
- уникнути накладних витрат, пов'язаних з експлуатацією систем кон-троля доступу (карти, ключі);
- виключити незручності, пов'язані з втратою, псуванням чи елементарним забування ключів, карт, паролів;
- організувати облік доступу і відвідуваності співробітників.

В даний час відомий ряд технологій, які можуть бути задіяні в системах безпеки для ідентифікації особи за відбитками пальців (як окремих, так і руки в цілому), рисами обличчя (на основі оптичного і інфрачервоного зображень), райдужній оболонці очей, голосу і другім характеристикам.

Всі біометричні технології мають загальні підходи до вирішення завдання ідентифікації, хоча всі вони розрізняються зручністю застосування і точністю результатів. Будь-яка біометрична технологія застосовується поетапно:

- сканування об'єкта;
- витяг індивідуальної інформації;
- формування шаблону;
- порівняння поточного шаблону з базою даних.

Дуже важливим є питання про пропускну здатність біометричної системи контролю доступу. Оскільки обсяг даних, які аналізуютьсязчитувачем, дуже великий, то навіть простий перебір бази даних про-виходить досить довго. Щоб зменшити час аналізу, біометричні зчитувачі мають зазвичай додатково вбудовану клавіатуру, на якої користувач набирає свій особистий код доступу і тільки після цього приступає до процесу біометричної ідентифікації. Перевага біометричної системи контролю доступу полягає також в тому, що ідентифікується не предмет (ключ «тач-меморі», проксімітікарта), а сама людина. Використовувана характеристика нерозривно пов'язана з ним - «біометричний паспорт» неможливо втратити, передати або забути вдома.

Лекція № 3.

Тема: Типи атрибутивних ідентифікаторів

Зміст лекції:

1. Ідентифікаційні картки з магнітною доріжкою.
2. Ідентифікаційні карти з магнітним барій-феритовим прошарком.
3. Ідентифікаційні картки кодовані за принципом Віганда.
4. Безконтактні радіочастотні проксиміті-карти.
5. Ідентифікаційні картки зі скритим штриховим кодом (бар- код).
6. Оптичні ідентифікаційні картки.
7. Голографічні ідентифікаційні картки.
8. Ідентифікаційні картки зі штучним інтелектом (смарт-карти).
9. Безконтактні ідентифікаційні картки.
10. Пластикові ключі.

1. Ідентифікаційні картки з магнітною доріжкою.

Цей тип карток був розроблений ще в 60-і рр. XX ст., Але з тих пір був істотно вдосконалений: збільшена інформаційна ємність, зносостійкість, підвищилася захищеність від зловживань. У ранніх зразках запис інформації велася магнітним полем напруженістю 300 Ерстед. Це не забезпечувало надійний захист від випадкового або навмисного стирання. Крім того, запис магнітним полем такої напруженості дозволяла порушникам досить просто підробляти такі картки, не вдаючись до по-мощі складного обладнання. Усунути ці недоліки вдалося шляхом застосування спеціальних магнітних матеріалів, що вимагають для запису магнітного поля напруженістю 4000 Ерстед. Такі магнітні матеріали в кінці 1970-х рр. вперше стала застосовувати фірма 3М. В даний час досягнута щільність запису 75 біт / см. Висока щільність запису дає можливість зберігати на картці досить великий обсяг інформації.

Для підвищення ступеня захищеності карток, поряд зі звичайною інформацією про власника, може наноситися, наприклад, спеціальний захисний код, що описує структуру матеріалу, з якого вони виготовляються. При випуску картки в обіг структурні особливості її основи в цифровому коді записуються на магнітну доріжку. При перевірці спеціальний оптико-електричний пристрій, що зчитує, сканує картку, просвічуючи її поверхню, після чого система автоматично визначає відповідність отриманих даних записаному коду.

2. Ідентифікаційні картки з магнітним барій-феритовим прошарком.

У таких картках магнітний шар є серединою «сендвіча» з несучою основи (з фотографією та особистими даними власника) і пластикового покриття. Розташування в ньому і полярність зарядів барій-феритових частинок утворюють код. Перевагою таких карток є найнижча вартість в порівнянні з

усіма іншими видами і підвищена захищеність від копіювання. Однак вони не забезпечують надійного захисту від випадкового або навмисного стирання або зміни вбудованого коду. Крім того, вони недостатньо зносостійкі. Область їх застосування обмежена тими сферами, де не потрібно скільки-небудь високий рівень безпеки при контролі доступу.

3. Ідентифікаційні картки, кодовані за принципом Віганда.

Картки Віганда представляють собою пластикову картку, в яку при виготовленні запресовані хаотично розташовані відрізки проводів зі спеціального магнітного сплаву. Зчитування карти відбувається за допомогою електромагнітного поля, індукованого зчитувачем. При проведені карти через щілину зчитувача два ряди проводків, запаяних в карту, викликають різнополярні сплески індукційного струму, який перетворюється в двійковий код. Карти Віганда мають хороші експлутаційні характеристики.

Завдяки відсутності рухомих частин і герметичності корпусу карта відрізняється високою надійністю і довговічністю функціонування, високою стійкістю по відношенню до спроб фізичного руйнування і несприятливим кліматичним умовам, зокрема, може працювати в діапазоні температур від -40 до + 70 ° С. До недоліків цієї технології можна віднести досить високу (у порівнянні з магнітними) вартість виготовлення карток при їх короткому життєвому циклі. Крім того, в порівнянні з магнітною доріжкою щільність запису інформації тут менше приблизно на третину (рис. 3.1).

Рис. 3.1. Безконтактна карта (інтерфейс Віганда)

4. Безконтактні радіочастотні проксіміті-карти.

Зчитувач генерує електромагнітне випромінювання певної частоти і при внесенні карти в зону дії зчитувача це випромінювання через вбудовану в карті антену живить чіп карти. Отримавши необхідну енергію для роботи, карта пересилає на зчитувач свій ідентифікаційний номер за допомогою електромагнітного імпульсу певної форми і частоти. Сама проксіміті-карта складається з приймально-передавальної антени і електронного чіп.

5. Ідентифікаційні картки з прихованим штрих-кодом (бар-код).

Невидимий штриховий код впечатується в основу картки і зчитувача за допомогою випромінювання інфрачервоного спектру. Код утворюється за рахунок зміни тіней при проходженні ІЧ-випромінювання через картку і має високий ступінь захищеності від підробки. Однак ця технологія доволі дорого коштує, хоча вартість таких карток і нижче, ніж вартість карток Віганда

6. Оптичні ідентифікаційні картки.

Кодування інформації на таких картках здійснюється приблизно так само, як під час запису даних на оптичних дисках - комп'ютерних носіях. Зчитування проводиться лазером. Сучасна технологія забезпечує дуже високу щільність запису, тому ємність пам'яті таких карток обчислюється мегабайтами. Це дозволяє зберігати не тільки букви і цифри даних, але і зображення і звукову інформацію. Картки цього типу мають низьку вартість і високу ступінь захищеності від несанкціонованого копіювання. Однак висока щільність зберігання інформації вимагає досить дбайливого ставлення і складних пристроїв, що зчитують терміналів. Виготовляються корпорацією Drexler Technology Corp., США (картка LaserCard) і торонтскою фірмою Optical Recording Corp.

7. Голографічні ідентифікаційні картки.

Використовувані при виготовленні таких ідентифікаційних документів тривимірні голограми формуються на основі інтерференції двох або кількох когерентних хвильових полів. Застосування голограми поряд з підвищеним захистом документів від фальсифікації забезпечує високу щільність запису інформації (до 10 біт інформації, що міститься в зображенні на 1 мм). Підвищена захищеність документів обумовлена тим, що технічна реалізація методів голографії відрізняється достатньою складністю і вимагає застосування спеціальної апаратури.

Одним з видів голограм, нанесення яких не пов'язане зі значними витратами, є друковані голограми. За допомогою так званої «райдужної голограми» формується друкована основа, на яку потім може бути нанесено велике число голографічних відмінних ознак справжності ідентифікаційного документа. Істотним достоїнством друкованих голограм є те, що вони можуть наноситися на використовувані в даний час документи. Це дозволяє помітно підвищити рівень захищеності посвідчень від фальсифікацій при порівняно низьких витратах.

Більш високий рівень захисту забезпечують голограми, засновані на ефекті об'ємного відображення Інформація, що міститься в них, може зчитуватися безпосередньо при звичайному освітленні (т. б. без допоміжної апаратури). Дані, що наносяться на документ за допомогою голограми, можуть

являти собою як окремі букви і цифри знаки, так і складну комбінацію букв і цифр, графічних і фотографічних символів.

Інтерференційна діаграма, що містить інформацію, розподіляється квазіслучайно по всій площі та на всю глибину емульсійного шару голограм розглянутого виду, що обумовлює труднощі при спробі фальсифікувати ідентифікаційний документ. Інформація, що міститься в голограмі стає видимою в променях звичайного світла, джерелом якого може бути, наприклад, настільна лампа. Інформація подається у вигляді реального або уявного зображення.

Одним з нових перспективних видів голограм є так звані «голограми Даусмана». Розроблена технологія нанесення інформації забезпечує можливість поєднання в одному фотоемульсійному шарі зображення буквено-цифрових даних, чорно-білого фотографічного знімка, а також об'ємно-рефлексійні голограми. Виготовлені з використанням цієї технології документи отримали назву «посвідчення посвідченні», тому що інформація чорно-білого зображення повністю збігається з даними, що містяться в голограмі. Будь-які зміни в чорно-білому фотознімку виявляються відразу шляхом його порівняння з голограмою. Дана голографічна технологія формування ознак особливо ефективна для таких ідентифікаційних документів, як посвідчення особи, закордонний паспорт і т. д.

При необхідності голограми можуть застосовуватися і для зберігання біометричних даних (наприклад, відбитків пальців). Подібна система розпрацюємо німецькою фірмою Siemens ДО. Для забезпечення надійного захисту від спроб фальсифікації або копіювання ідентифікаційних карток фірма застосувала ще і шифрування даних.

Голографічні методи захисту інформації на документах, поряд з високою надійністю, мають і низку недоліків. До них відносяться, наприклад, висока складність апаратури автоматизації процесу контролю, досить жорсткі вимоги до гарантування безпеки документа Найбільшу ефективність забезпечує напівавтоматична апаратура, яка функціонує за участю оператора-контролера, який аналізує результати порівняння та приймає рішення про пропуск на об'єкт.

8. Ідентифікаційні картки зі штучним інтелектом (смарт-карти).

Такі документи містять вмонтовані в основу мініатюрні інтегральні мікросхеми - пристрій і мікропроцесор. Одна з переваг карток цього типу - можливість реєстрації значного обсягу ідентифікаційних даних. Вони мають досить високим ступенем захищеності записаної в них інформації від фальсифікації і різного роду зловживань. У літературі зустрічаються інші назви цих карток - «розумні» або «інтелектуальні».

Обчислювальний мікроблок цієї картки містить три типи запам’ятовуючих пристроїв (ЗП). Для зберігання програмного забезпечення існує пам'ять типу ПЗУ (постійне ЗП), в яку інформація заноситься фірмою-виробником на етапі випуску картки в обіг і не допускає внесення будь-яких змін в зберігаються інструкції.

Для зберігання проміжних результатів обчислень і інших даних тимчасового характеру застосовується пам'ять типу пристрої довільної вибірки. Вона управляється вбудованим мікропроцесором, який здійснює контроль за процесом взаємодії зі зчитувачем. Після відключення електричного живлення інформація тут не зберігається.

Пам'ять третього типу - програмуємий постійний запам'ятовуючий пристрій (ППЗУ) - надається користувачеві для запису персональної інформації. Вона також знаходиться під управлінням вбудованого мікропроцесора. Тільки по його команді в цю пам'ять можуть вноситися будь-які зміни. Записана інформація не стирається і при відключенні електричного живлення. У пам'яті цього типу, як правило, виділені три зони: відкритого доступу, робоча і секретна.

У відкритій зоні може зберігатися, наприклад, персональна інформація користувача (ім'я, адреса і т. д.), Зчитування якої допускається стороннім терміналом відповідного типу. Однак будь-які зміни в записах можуть проводитися тільки з дозволу користувача і за допомогою спецапаратури.

Робоча зона призначена для занесення специфічної інформації, зміна і зчитування якої допускається тільки по команді користувача і при наявності відповідних технічних засобів.

У секретній зоні записується ідентифікує інформація, наприклад, особистий номер або код-пароль. Крім того, тут же зазвичай зберігаються тимчасові і територіальні повноваження користувача з доступу до об'єктів і приміщень. Інформація секретної зони може бути зчитана лише терміналом системи контролю доступу, для якого призначена дана картка. Зміни також вносяться тільки по команді цієї системи.

Збережені тут дані не розкриваються ніякої сторонньої зчитує апаратурою, в тому числі фірми-виробника. Секретна інформація заноситься в цю зону при реєстрації користувача контрольно-пропускний системою. До недавнього часу в якості такої пам'яті застосовувалися пристрої, що запам'ятовують СППЗУ (програмоване постійне ЗУ яке можна стирати). Внесена інформація могла бути стерта тільки за допомогою ультрафіолетового випромінювання і спецьобладнання. Більш сучасним типом пам'яті є ЕСППЗУ - електрично стираємий програмуємий постійний запам’ятовуючий пристрій, який на відміну від попереднього більш довговічний (термін служби - до декількох років) і має більшу гнучкість.

Деякі інтелектуальні картки дозволяють зберігати цифрові образи біометричних характеристик користувача (динаміку розпису, відбитка пальця, долоні, геометричних параметрів кисті, малюнка очного дна, портретного зображення). З метою захисту від несанкціонованого використання ідентифікаційних карток, що застосовуються користувачами таких систем, електронний «портрет» зберігається в пам'яті в цифровому закодованому вигляді, що значно ускладнює відновлення записаної інформації і її підробку зловмисниками.

9. Безконтактні ідентифікаційні картки.

Такі картки з вигляду не відрізняються від всіх інших, але поряд зі звичайною атрибутикою містять вбудований мініатюрний приймач, який здійснює дистанційне взаємодія зі зчитувачем системи контролю доступу.

В якості комунікаційного засобу при дистанційному зчитуванні можуть служити спрямоване електромагнітне поле (мікрохвильові радіосигнали), оптичний промінь (інфрачервоне випромінювання) або акустичні хвилі (ультразвук).

Особливість безконтактних зчитувачів в порівнянні з іншими пристроями полягає в тому, що зовнішній елемент їхньої конструкції (антена) може бути вмонтована, наприклад, в стіну поряд з охоронюваною дверима Це забезпечує скритність і відповідно захист від спроб фізичного руйнування.

Відстань, на якому взаємодіє безконтактна ідентифікаційна картка з антеною пристрою, що зчитує, в сучасних безконтактних контрольно-пропускних автоматах може змінюватися в залежності від конкретної моделі від декількох сантиметрів до 10 м і більше.

Найбільшого поширення зараз отримали мікрохвильові зчитувачі і ідентифікаційні картки з вбудованою електронною схемою або «електронні жетони» (які користувач може носити у внутрішній кишені, портфелі або прикріпленими до зв'язки ключів). Такі ідентифікатори називають ще «електронними мітками».

Розрізняють такі типи електронних міток.

Пасивні електронні мітки Працюють на основі перевипромінення електричної енергії від мікрохвильового радіопередавача терміналу. Сигнал мітки вловлюється радіоприймачем терміналу, після чого подаються відповідні команди на механізм відмикання дверей.

Напівактивні електронні мітки. Містять мініатюрну батарею, яка є джерелом електроживлення для приймача. Сам приймач знаходиться зазвичай в режимі очікування, а при попаданні в зону дії мікрохвильового випромінювача поста видає сигнал певної частоти, що приймається терміналом системи.

Активна електронна мітка. Являє собою мікрохвильовий передавач-радіомаяк, який транслює сигнал певної частоти (для деяких моделей кодований) у безперервний спосіб.

Найбільш прості моделі безконтактних контрольно-пропускних терміналів, розвиток яких почалося ще на початку 1970-х рр. в США, могли транслювати лише груповий сигнал, що не підрозділяючи користувачів окремо. Надалі з розвитком електронної технології з'явилися ідентифікаційні картки, які крім мікросхеми приймача включали до свого складу пристрій. У цій пам'яті зберігається багатозначний код, який при обміні сигналами переноситься в контрольний термінал і ідентифікується відповідно до повноважень конкретного користувача.

Наприклад, напівактивна електронна мітка була розроблена німецькою фірмою Burcka Systems в якості пропуску безконтактного типу. Її вбудована пам'ять дозволяє зберігати скільки завгодно велику кількість програмованих

кодових комбінацій, що допускають до того ж їх дистанційне зміна. Максимальна відстань зчитування складає 3 м. Пропуск можна носити під одягом, так як мікрохвильовий сигнал проникає навіть через щільний (текстильний і шкіряний) матеріал верхнього одягу. В якості джерела живлення використовується мініатюрна літієва батарея з терміном служби 10 років.

Сучасні проксиміті-ідентафікатори представляють собою електронні перепустки у вигляді пластикових карток або брелків і досить широко використовуються в системах контролю доступу. Вони забезпечують безконтактне дистанційне розпізнавання (ідентифікацію) персонального коду власника електронними зчитувачами. У перекладі на російську мову proximity (проксіміті) означає «близькість». Однак ця близькість досить умовна, оскільки відстань між проксиміті-ідентифікатором і зчитувачем в залежності від потужності зчитувача і типу ідентифікатора може варіюватися від декількох сантиметрів до 2,5 м

Спеціальні електронні зчитувачі проксіміті-ідентифікаторів розпізнають особу його власника по записаному на ідентифікатор персональному коду. Механізм розпізнавання (зчитування) базується на дистанційній радіочастотній технології. Проксиміті-зчитувач постійно посилає радіосигнал. При попаданні в зону дії зчитування проксиміті-ідентифікатор активізується і посилає у відповідь сигнал, що містить унікальний код доступу, записаний в пам'яті його електронної схеми. Зчитування коду з проксиміті-ідентифікатора відбувається на визначеній відстані від зчитувача, т. б. без безпосереднього контакту. При цьому позиціонування ідентифікатора щодо зчитувача не має значення.

Все проксиміті-ідентифікатори діляться на дві групи - **пасивні і активні.**

В даний час використовуються як активні, так і пасивні проксиміті-ідентифікатори. **Пасивний** проксиміті-ідентифікатор не містить вбудованого джерела енергії, він абсолютно герметичний і має практично необмежений термін служби. При цьому відстань, на якому він працює стабільно, становить від 10 до 50 см від зчитувача. Як правило, такі ідентифікатори використовуються для швидкого і надійного обслуговування великого потоку людей, наприклад допуск їх через прохідну підприємства. **Активний** проксиміті-ідентифікатор може працювати на відстані від одного до трьох метрів, але вимагає постійного контролю ступеня заряду вбудованої батареї і її своєчасної заміни (зазвичай не частіше ніж через 5 років). Так, наприклад, автомобільні проксиміті-ідентифікатори HID ProxPass працюють на відстані до 2,5 м Велика відстань зчитування активного ідентифікатора дозволяє використовувати його в системах контролю в'їзду-виїзду автомобілів, проводити контроль переміщення великогабаритних вантажів, вагонів або контейнерів.

Все проксиміті-ідентифікатори HID відрізняються високим ступенем за-захищеності від підробки. Завдяки відсутності механічного контакту між проксиміті-ідентифікатором і зчитувачем, ідентіфткатор не зношується, і термін його служби практично не обмежений. Проксиміті- ідентифікатори володіють достатньою механічною міцністю, стійкі до вигинів, ударів, не бояться вологи і забруднення.

На проксиміті-ідентифікатори можна наносити написи, фотографії, логотипи. Для цього застосовуються спеціальні ПВХ на¬клейкі, а фотозображення і малюнки на поверхні тонких проксимітіідентифікаторів друкуються на спеціальних принтерах.

10. Пластикові ключі.

Пластикові ключі використовуються в усіх розглянутих вище способах кодування. Їх відмінність полягає в конструктивному способі відмикання, зовні нагадує спосіб відмикання звичайного механічного замку - вставляння ключа в свердловину, перевірку доступу і індикацію власнику ключа дозволу на відкриття замку (поворот ключа).

Цей ідентифікатор відрізняється більш високим ступенем зносоустікості у порівнянні з ідентифікаційними картками. У пам'яті такого ключа зберігається особистий номер його власника Принцип перевірки заснований на порівнянні вводиться користувачем номера з номером, що зберігається в пам'яті ключа, який зчитується терміналом при його вставлянні в проріз.

На згадку ключа зазвичай заноситься наступна інформація:

- системний ідентифікаційний номер (унікальний для кожної установки і надається фірмою-виробником при замовленні системи; максимальне число різних системних номерів понад 65 тис.);
- призначений для користувача ідентифікаційний номер (визначається покупцем при випуску та програмуванні ключа; можна замовити до 9999 різних номерів);
- рівні доступу (для автономного зчитувача до 256 рівнів система надає доступ від даного рівня і вище);
- дні тижня (7 днів тижня співвіднесені з тимчасовими зонами; комбінація дня тижня і тимчасової зони визначає право доступу через будь-який зчитувач в будь-який даний час);
- тимчасові зони (кожна система має до 16 окремими зона¬мі, які можуть бути призначені користувачеві);
- кодонабірна панель (для важливих об'єктів в пам'яті ключа може зберігатися до 10 різних цифр).

Термінали на базі комбінації зчитувача і кодонабірного пристрою. Комбінування методів автентифікації особистості дозволяє повисіть надійність захисту від несанкціонованого доступу. Однак при цьому збільшується час виконання процедури перевірки.

В даний час різними закордонними фірмами освоєний випуск цілого ряду моделей.

Найбільший інтерес представляє комбінований термінал фірми Security Dynamics. Використовувана ідентифікаційна картка (за розміром схожа на стандартну кредитну, але вдвічі товщі її) містить вбудований мікропроцесор, мініатюрний джерело живлення, рідкокристалічний індикатор, електронний годинник, а також пристрої, що запам'ятовують двох типів з довільною вибіркою (ЗУПВ) і постійне (ПЗУ). Кожну хвилину на індикаторі висвічується

число з псевдовипадкової послідовності, алгоритм генерації якої відомий мікрокомп'ютеру системи. Так що термінал «знає», яке конкретне число, на який ідентифікаційної картці, в який конкретний період часу буде записано. По суті цей псевдовипадковий номер служить паролем протягом 60 с

Процедура перевірки виглядає наступним чином. Користувач вводить за допомогою клавіатури свій особистий ідентифікаційний номер, а потім то число, яке відображене в даний момент на індикаторі його ідентіфікаційної картки. Система визначає коректність цього числа для даної карти і відрізка часу.

Для протидії загрозам перехоплення особистого коду законного користувача може бути запрограмована така можливість, коли замість роздільного введення даних власником ідентифікаційної картки набирається на клавіатурі сума ідентифікаційного номера та числа, прочитаного на індикаторі.

Лекція № 4.

Тема: Структури побудови систем контролю та управління доступом

Зміст лекції:

1. Централізована структура.
2. Розгалужена структура.
3. Змішана структура.
4. Програмне забезпечення для великих СКУД.

1. Централізована структура.

У СКУД для великого розподіленого об'єкта з різною структурою використовуються потужні центральні контролери, які здійснюють процес управління з використанням спеціалізованих віддалених інтерфейсних модулів. Особливості застосування визначають вимоги, що пред'являються до програмного забезпечення для таких систем. Найчастіше використовують СКУД з централізованою або розподіленою архітектурою, але іноді застосовується і архітектура змішаного типу.

У великої розподіленої системі контролю і управління доступом, особливо при великих відстанях між окремими будівлями охороняємого об'єкту, Кожна будівля має мати свій центральний контролер. Це забезпечує автономне функціонування системи безпеки кожної будівлі в разі порушення зв'язку між окремими об'єктами. Число підключаємих зчитувачів на один контролер, як правило, коливається від 16 до 96, тому зазвичай потужності одного контролера цілком вистачає для створення СКУД окремого об'єкта у великій розподіленої системі. Контролери централізованих СКУД є чисто логічними пристроями і не управляють дверима, т. Е не мають релейних виходів управління замками, входів для підключення зчитувачів СКУД Функції управління дверима, іншими зовнішніми пристроями виконують зовнішні інтерфейсні модулі і релейні блоки. Вони, як правило, встановлюються недалеко від об'єктів управління (двері, охоронні шлейфи та ін.) Для обміну інформацією між контролером і інтерфейсними модулями найбільш часто використовується інтерфейс RS-485, проте вже з'явилися системи, в яких можливе підключення інтерфейсних модулів за стандартом LAN.

Слід також зазначити, що найбільш потужні центральні контролери нараховують кілька комунікаційних інтерфейсів Я8-485, що забезпечує широке охоплення території великих будівель без застосування підсилювачів інтерфейсу Фактично можна прокласти свій інтерфейс Я8-485 в декількох напрямках від центрального контролера. Що стосується мережевого інтерфейсу, то для великих об'єктів можливість підключення інтерфейсних модулів СКУД до центрального контролера за стандартом LAN вельми актуальна, оскільки в цьому випадку з'являється перспектива використання існуючої на об'єкті мережевої інфраструктури і істотного зниження витрат на

прокладку комунікацій. Контролер в системах з централізованою архітектурою зберігає всю базу даних ідентифікаторів і подій, що сталися в системі. Розташовується він зазвичай недалеко від керуючих комп'ютерів (серверів) в місцях найвищої захищеності (кімнати охорони, серверні та ін.). Поділ функцій прийняття рішень і безпосередньо управління підвищує ступінь безпеки СКУД, так як сам контролер добре захищений і встановлений на великій відстані від керованого ним УПУ Крім того, такий підхід допомагає знизити вартість великих систем, оскільки ціна контролера «розчиняється» в загальній вартості системи. Слід зазначити, що самі контролери можна об'єднувати в мережі, дозволяючи тим самим створювати СКУД значного масштабу (рис. 4.1.). При порушенні зв'язку контролера з комп'ютером система працює в автономному режимі. Іншими словами, централізована система - це жорстка владна вертикаль або піраміда, коли нагорі керівний контролер («начальник»), а нижче - звичайні інтерфейсні модулі («виконувачі»), які власне і реалізують керуючі команди.

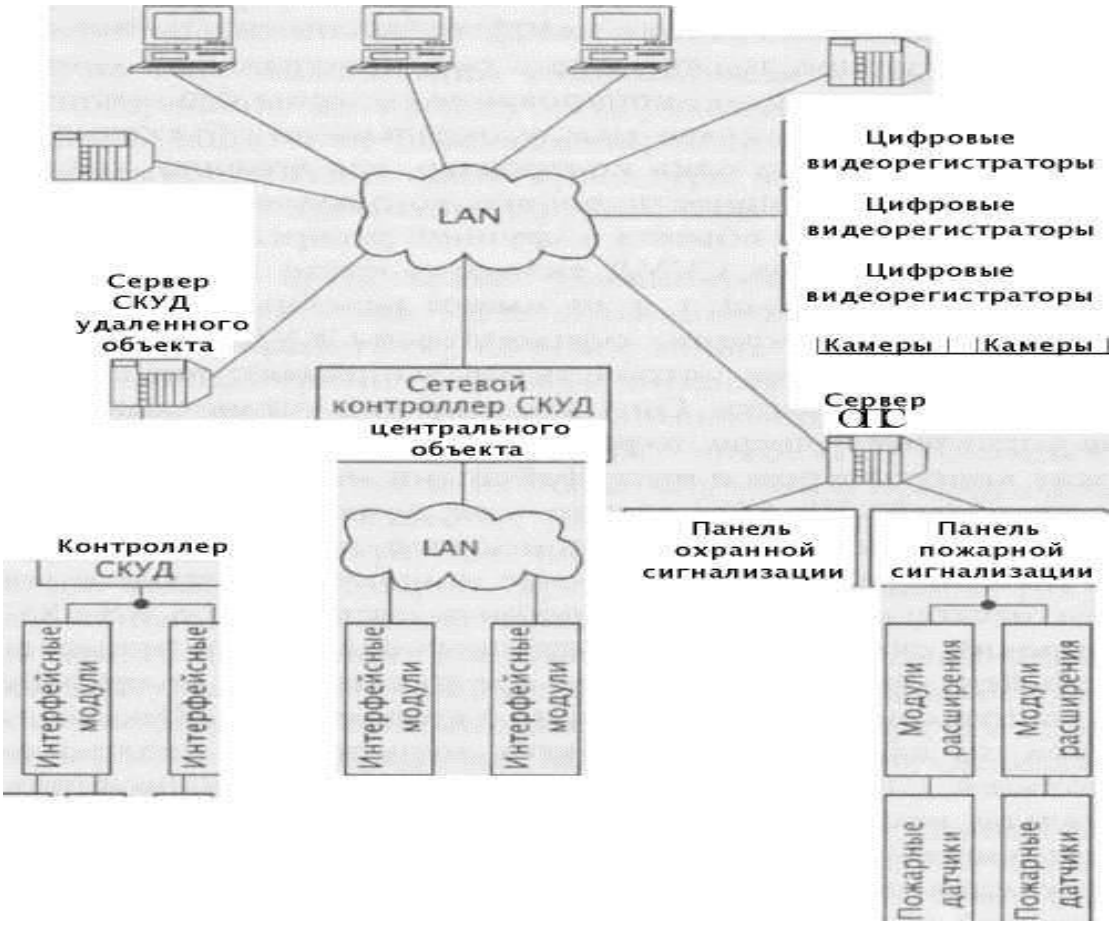

Рис. 4.1. Варіант побудови СКУД з централізованоюструктурою

2. Розгалужена структура.

Відмінна особливість СКУД з розподіленою струкутрою полягає в тому, що база даних ідентифікаторів (і подій в системі) міститься не в одному, а в декількох контролерах. Вони зазвичай виконують функції управління зовнішніми пристроями і охоронними шлейфами через реле і входи охоронної

сигналізації, розташовані безпосередньо на платі самого контролера. Ці контролери, як правило, встановлюються безпосередньо всередині захищаються ними приміщень. Це не знижує ймовірності несанкціонованого маніпулювання контролером, але має свої плюси - при такому підході менш критично порушення зв'язку між контролером і інтерфейсним модулем (як у звичайній централізованій системі). У разі обриву лінії зв'язку між контролерами і комп'ютером система продовжує виконувати основні функції управління процесом доступу в автономному режимі. Виведення з ладу одного контролера не вплине на роботу інших. Найбільш часто в системах з розподіленою архітектурою контролер управляє проходом в 2-4 двері. При використанні таких СКУД на великих розподілених об'єктах слід пам'ятати, що кожна окрема будівля, швидше за все, буде оснащуватися своєї підсистемою, що складається з групи контролерів зі своїм комп'ютером, що управляє. Така особливість пов'язана з обмеженням довжини найбільш часто використовуваних в таких системах інтерфейсів - RS-485. Прокладка ліній зв'язку між віддаленими будинками потребує застосування підсилювачів інтерфейсу, а це не завжди зручно і трохи знижує надійність, тому можна розглядати систему в цілому як сукупність підсистем декількох будівель. Якщо перейти на будівельну термінологію, то розподілена СКУД - це певна кількість контролерів - «виконробів», які відповідають тільки за свою ділянку робіт і самі ж їх виконують. Вони самостійно аналізують і зберігають частину інформації про функціонування своєї невеликої частини системи.

3. Змішана структура.

Зазвичай такі системи виходять з СКУД з централізованою структуроюшляхом додавання спеціалізованих зчитувачів або інтерфейсних модулів з власним буфером пам'яті ідентифікаторів і подій - «інтелектуальних інтерфейсних модулів». Можна сказати, що кожен такий модуль є невеликим контролером СКУД, який можна порівняти з контролером в розподіленій системі. Завдяки використанню даного технічного рішення досягається надмірне резервування функцій, різко підвищується ступінь безпеки системи. Оскільки контролер в СКУД з централізованою архітектурою керує найбільшою кількістю дверей, пошкодження лінії зв'язку між ним і інтерфейсними модулями управління кінцевими пристроями може привести до блокування значної частини або навіть всієї системи. Локальний зчитувач або проміжний інтерфейсний блок, що володіє вбудованим буфером пам'яті, в цьому випадку переходить в автономний режим управління доступом (на своїйділянці). Системи, побудовані з використанням даних модулів, мають найвищий ступінь безпеки і виняткову надійність функціонування. Для великих розподілених СКУД зі змішаною апаратною архітектурою важливо, що деякі виробники мають в номенклатурі інтерфейсні модулі з можливістю підключення до центрального контролеру по LAN-інтерфейсу. При наявності розвинених мережевих комунікацій на території об'єкта подібні модулі

встановлюються в віддалених будівлях, що надає системі додаткову гнучкість і дозволяє економити значні кошти.

Таким чином, змішана система - це владна вертикаль, або піраміда з можливістю передачі частини функцій управління на більш низький рівень в разі виникнення екстреної ситуації

4. Програмне забезпечення для великих СКУД.

Програмні комплекси для великих розподілених СКУД мають свої особливості, які необхідно мати на увазі при виборі ПО для систем малого і середнього масштабу.

Одним з найбільш поширених варіантів СКУД є невелика ізольована система. Її головна характеристика полягає в тому, що всі модулі (управління базою даних, ядро, функціональні модулі, драйвери обладнання та ін.) Встановлюються і запускаються на одному комп'ютері. До цього ж комп'ютера підключається і все обладнання. Комп'ютер при цьому повинен володіти достатньою обчислювальною потужністю і об'ємом пам'яті для виконання всіх програмних модулів, а також адекватним вихідній задачі дисковим простором - для зберігання бази даних системи Основні переваги подібної системи - простота інсталяції, обслуговування, контролю ліній зв'язку і низька вартість рішення. З недоліків можна відзначити, перш за все, відключення деяких функцій при «зависанні» або виключенні комп'ютера, можливість адміністрування тільки на одному комп'ютері, уповільнення реакцій комплексу при великій кількості підключеного обладнання. Для великої розподіленої системи найважливішим негативним фактором виявиться необхідність підключення всього керованого обладнання в комплекті з комп'ютером, що часто просто неможливо.

При використанні централізованої системи з віддаленим управлінням все службові модулі комплексу (ядро, драйвери обладнання та логіка) функціонують на одному комп'ютері - центральному сервері системи, а запуск керуючої консолі можливий не тільки на даному комп'ютері, але і на інших машинах мережі. У такій системі центральний комп'ютер повинен володіти ще більшими обчислювальною потужністю, об'ємом пам'яті і дисковим простором, ніж в одного користувача системі. Однак в даній схемі з'являється можливість задіяти не надто потужні компьютери з невеликими дисками в якості клієнтських робочих станцій. Переваги очевидні: простота установки, обслуговування і контролю ліній зв'язку, так як все обладнання підключено до одного комп'ютера. У такій системі легко контролювати стан функціональних модулів і драйверів обладнання, так як всі вони функціонують на одній машині. Недоліки в значній мірі такі ж, як в попередньому варіанті.

Для централізованої системи головним негативним фактором буде той же - необхідність підключення всього керованого обладнання до одного комп'ютера (сервера).

У великих СКУД іноді використовується варіант, при якому сервер управління базою даних системи і ядро працюють па центральному сервері, а

драйвери обладнання та логіки розподілені по всій мережі. Запуск керуючих консолей можливий на будь-якому комп'ютері мережі, що робить управління більш гнучким. Необхідність розподілу по мережі драйверів обладнання та логіки пов'язана в основному з тим, що будівлі підприємства розподілені по території і частина обладнання може перебувати доста¬точно далеко від центрального сервера. Оскільки частина модулів винесена з центрального сервера системи на інші комп'ютери, навантаження на централь¬ний сервер знижується. Застосування такої архітектури виправдано при на¬лічії великій території з розподіленим по ній керуючим обладнанням. У цьому випадку немає необхідності прокладати комунікації з усіх точок до центрального серверу. Досить підключити апаратуру до найближчого комп'ютера мережі і запустити на цьому комп'ютері обслуговуючий драйвер При цьому вимоги до потужності даного комп'ютера залишаються відносно скромними.

Треба відзначити, що в разі розподіленого запуску програмних модулів постає завдання контролю їх стану. Для спрощення роботи в ПО системи повинні бути вбудовані спеціальні засоби, що дозволяють адміністратору зі свого робочого місця контролювати роботу модулів на інших комп'ютерах, запускати або зупиняти їх.

Виділимо найбільш важливі переваги і недоліки такого ПО. До переваг слід віднести:

- простоту 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 прокладці ліній зв'язку.

Недоліками можна вважати:

- вимога контролю адміністратором стану розподілених по системі модулів;
- необхідність наявності на об'єкті навченого персоналу.

ПО з такою структурою підходить для побудови СКУД і інтегрованих систем безпеки (ІСБ) заводів, аеропортів, банків, офісів крупних компаній, інститутів та інших великих об'єктів, що мають значну територію з великим числом окремих будинків і споруд.

У загальному випадку програмне забезпечення СКУД надає користувачю наступні стандартні можливості:

- програмування тимчасових інтервалів, які двері (ворота) відкриті зовсім, відкриваються при скануванні ідентифікаційною карткою (або автентифікації користувача на біометричних терміналах) або закриті наглухо, а також включення / вимикання за розкладом або за показниками приладів, освітлення, вентиляції, ліфтів, датчиків охоронної сигналізації;

- програмування вихідних днів і свят, коли допуск надається тільки певним особам;
- створення декількох ієрархічних груп користувачів в залежності від рівня наданого їм допуску;
- виконання функції «ні кроку назад», що перешкоджає тому, щоб один співробітник, пройшовши через двері передав свою картку іншій людині (т. е. визначається часовий інтервал, протягом якого картка не може відкрити двері ще раз, або на виході з приміщення встановлюється ще один зчитувач, і картка може знову «зайти», тільки попередньо «вийшовши»);
- якщо комп'ютер підключений до системи постійно, на нього може бути виведено план території, що охороняється з усіма точками контролю доступу, дверима, проходами, розташуванням датчиків і т. п., на якому в режимі реального часу відображаються всі події, що відбуваються;
- оператор системи постійно контролює обстановку і в разі не-обходимо може прийняти необхідні по обстановці рішення

Зазвичай великі СКУД працюють в сукупності з системами охоронної сигналізації та телевізійного спостереження. В цьому випадку, наприклад при спробі несанкціонованого проникнення в приміщення, оснащене СКУД або датчиками охоронної сигналізації, включаються телекамери і блокуються виходи. Система може програмуватися на розблокування всіх виконавчих пристроїв в екстрених випадках. Подібний набір функцій закладено, наприклад, в програмному забезпеченні систем безпеки «Multi Net 5100» (працює в середовищі OS / 2) фірми «DIEBOLD».

Типові можливості математичного та програмного забезпечення досить великих СКУД дозволяють вирішувати завдання контролю за відвідувачами, контролю за винесенням матеріальних цінностей, автоматизувати ряд функцій служби патрулювання і т. Д.

Кожному відвідувачеві на вході видається ідентифікаційна картка з дозволом на доступ в заданий час в певні зони. На виході картка повинна здаватися. При цьому можливий оперативний контроль місць відвідування, а в разі затримки на об'єкті поза межами заданого временного інтервалу подається сигнал тривоги.

Для винесення матеріальних цінностей на будь-якій робочій станції системи може бути сформований список предметів, який скріплюється «електронним підписом» уповноваженого керівника. При цьому вводиться особистий ідентифікаційний номер співробітника, який виносить предмети. При підході до прохідної цей список автоматично (за пред'явленням ідентифікаційної картки співробітника) виводиться на дисплей контролера, який звіряє список.

Гнучкість ПО сучасних систем контролю доступу дозволяє достатньо легко змінювати їх конфігурацію, змінювати задані умови перебування в приміщеннях і на території для будь-якого співробітника.

З метою підвищення надійності функціонування СКУД їх програмне забезпечення може передбачати функціонування центральних робочих станцій в зв'язці двох машин в режимі паралельної обробки даних.

Лекція № 5.

Тема лекції: Біометричні засоби ідентифікації особи

План лекції:

1. Класифікація та основні характеристики біометричних засобів ідентифікації особи.
2. Статичні методи ідентифікації.

1. Класифікація та основні характеристики біометричних засобів ідентифікації особистості.

Переваги біометричних ідентифікаторів на основі унікальних біологічних, фізіологічних особливостей людини, однозначно удостоверяющіх особистість, привели до інтенсивного розвитку відповідних коштів. В біометричних ідентифікаторів використовуються статичні методи, засновані на фізіологічних характеристиках людини, т. Е. На унікальні характеристики, даних йому від народження (малюнки папілярних ліній пальців, райдужної оболонки очей, капілярів сітківки очей, теплове зображення особи, геометрія руки, ДНК), і динамічні методи (почерк і динаміка підпису, голос і особливості мови, ритм роботи на клавіатурі). Передбачається використовувати такі унікальні статичні методи, як ідентифікація по подноггевому шару шкіри, за обсягом зазначених для сканування пальців, формі вуха, запаху тіла, і динамічні методи - ідентифікація по руху губ при відтворенні кодового слова, по динаміці повороту ключа в дверному замку і т. д. Класифікація сучасних біометричних засобів ідентифікації показана на рис. 5.1.

Біометричні ідентифікатори добре працюють тільки тоді, коли оператор може перевірити дві речі: по-перше, що біометричні дані отримані від конкретної особи саме під час перевірки, а по-друге, що ці дані збігаються із зразком, що зберігається в картотеці. Біометричні характеристики є унікальними ідентифікаторами, але питання їх надійного зберігання і захисту від перехоплення і раніше залишається відкритим

Біометричні ідентифікатори забезпечують дуже високі показники: ймовірність несанкціонованого доступу - 0,1 - 0,0001%, ймовірність помилкового затримання - частки відсотків, час ідентифікації - одиниці секунд, але мають більш високу вартість у порівнянні із засобами атрибутної ідентифікації. Відомі розробки СКУД, засновані на зчитуванні і порівняно конфігурацій сітки вен на зап'ясті, зразків запаху, перетворених в цифровий вигляд, аналізі носить унікальний характер акустичного відгуку середнього вуха людини при опроміненні його специфічними акустичними імпульсами і т. д.

Тенденція значного поліпшення характеристик біометричних ідентифікаторів і зниження їх вартості призведе до широкого застосування біометричних ідентифікаторів в різних системах контролю і управління

доступом. В даний час структура цього ринку представляється наступним чином: верифікація голосу - 11%, розпізнавання особи - 15%, сканування райдужної оболонки ока - 34%, сканування відбитків пальців - 34%, геометрія руки - 25%, верифікація підпису - 3%.

Рис. 5.1. Класифікація сучасних біометричних засобів ідентифікації

Будь-яка біометрична технологія застосовується поетапно:

- сканування об'єкта;
- витяг індивідуальної інформації;
- формування шаблону;
- порівняння поточного шаблону з базою даних.

Методика біометричної автентифікації полягає в наступному. Користувач, звертаючись із запитом до СКУД на доступ, перш за все, ідентифікує себе за допомогою ідентифікаційної картки, пластикового ключа або особистого ідентифікаційного номера. Система по пред'явленому користувачем ідентифікатором знаходить в своїй пам'яті особистий файл (еталон) користувача, в якому разом з номером зберігаються дані його біометрії, попередньо зафіксовані під час процедури реєстрації користувача. Після цього користувач пред'являє системі для зчитування обумовлений носій біометричних параметрів. Зіставивши отримані і зареєстровані дані, система приймає рішення про надання або заборону доступу.

Таким чином, поряд з вимірювачами біометричних характеристик СКУД повинні бути обладнані відповідними зчитувачами ідентифікаційних карток або пластикових ключів (або цифровою клавіатурою).

Говорячи про точність автоматичної автентифікації, прийнято виділяти два типи помилок Помилки 1-го роду («помилкова тривога») пов'язані з забороною

доступу законному користувачеві. Помилки 2-го роду («пропуск цілі») - надання доступу незаконному користувачеві. Причина виникнення помилок полягає в тому, що при вимірах біометричних характеристик існує певний розкид значень. У біометрії абсолютно неймовірно, щоб зразки і знову отримані характеристики давали повний збіг. Це справедливо для всіх біометричних характеристик, включаючи відбитки пальців, сканування сітківки ока або впізнання підпису. Наприклад, пальці руки не завжди можуть бути поміщені в один і той же стан, під тим же самим кутом або з тим же самим тиском. І так кожен раз при перевірці.

Рівень надійності, дозволений для системи контролю доступу, може бути абсолютно різним, проте рівень помилкових відмов істинним користувачам не викликає будь-якого занепокоєння, в той час як рівень фальшивих доступів фактично повинен бути доведений до нуля.

Оскільки рівень надійності при порівнянні може в кінцевому підсумку регулюватися з тим, щоб задовольнити запити конкретного споживача, надзвичайно важливо цьому користувачеві реально уявляти собі, чого дана система здатна досягти. Найбільшу ступінь заклопотаності вносить те, що фірми-виробники часто задають ступень точності: 0,01% (тобто 1 помилка на 10 000 випадків автентифікації).

2. Реалізація статичних методів біометричного контролю.

2.1. Ідентифікація по малюнку папілярних ліній

Застосування даної технології набуло широкого поширення в системах автоматичної ідентифікації по відбитку пальця (AFIS).

Весь процес ідентифікації займає не більше кількох секунд і не вимагає зусиль від тих, хто використовує дану систему доступу. В даний час вже виробляються подібні системи розміром менше колоди карт. Певним недоліком, який стримує розвиток даного методу, являється упередження частини людей, які не бажають залишати інформацію про своїх відбитках пальців. При цьому контраргументом розробників апаратури є запевнення в тому, що інформація про папілярний візерунку пальця не зберігається - зберігається лише короткий ідентифікаційний код, побудований на базі характерних особливостей відбитка вашого пальця. За цим кодом можна відтворити візерунок і порівняти його з відбитками пальців, залишеними, припустимо, на місці злочину. Переваги доступу по відбитку пальця - простота використання, зручність і надійність. Хоча відсоток помилкових відмов при ідентифікації становить близько 3%, помилка помилкового доступу - менше 0,00001% (1 на 1 000000).

Існує два основних алгоритму порівняння отриманого коду з наявними в базі шаблоном: по характерних точках і по рельєфу всієї поверхні пальця. У першому випадку виявляються характерні ділянки і запам’ятовується їх взаємне розташування. У другому випадку запам'ятовується вся «картина» в цілому. У сучасних системах використовується також комбінація обох алгоритмів, що дозволяє підвищити рівень надійності системи.

Традиційно американські компанії займають лідируючі позиції в розробці біометричних систем безпеки, в цьому напрямку успішно працюють такі фірми, як Identix, T-Netix, American Biometric Company, National Registry, sagem, Morpho, Verditicom, Infenion.

З метою ідентифікації особи по малюнку папілярних ліній пальця перевіряється набирає на клавіатурі свій ідентифікаційний номер і поміщає вказівний палець на віконце скануючого пристрою. При співпадінні одержуваних ознак з еталонними, попередньо закладеними в пам'ять ЕОМ і активізованими при наборі ідентифікаційного номера, подається команда виконавчому пристрою. Хоча малюнок папілярних ліній пальців індивідуальний, використання повного набору їх ознак надмірно ускладнює пристрій ідентифікації. Тому з метою його здешевлення застосовують ознаки, найбільш легко вимірювані автоматом. Випускають порівняно недорогі пристрої ідентифікації за відбитками пальців, дія яких заснована на вимірі відстані між основними дактилоскопічними ознаками. На величину ймовірності помилки впізнання впливають також різні фактори, в тому числі температура пальців (рис. 5.2). Крім того, процедура автентифікації у деяких користувачів асоціюється з процедурою зняття відбитків у злочинців, що викликає у них психологічний дискомфорт.

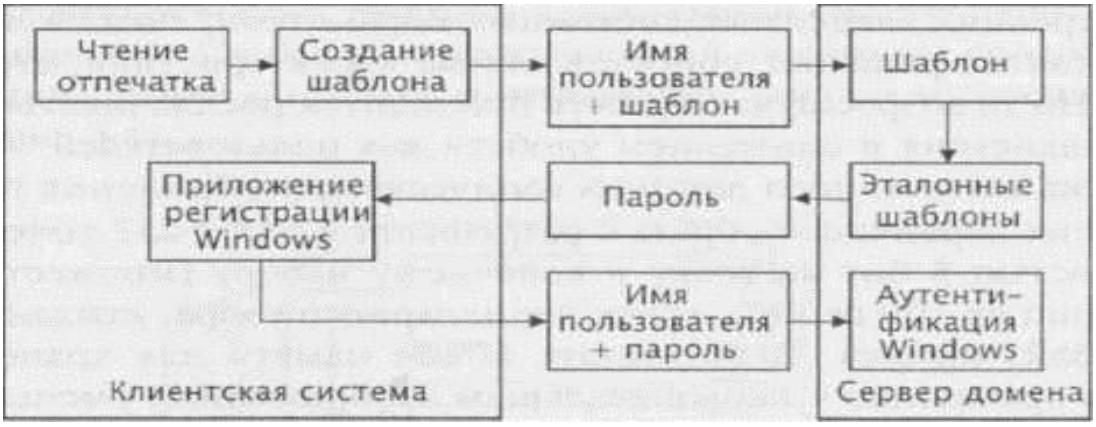

Рис. 5.2. Процес автентифікації по відбиткам пальців

Дактилоскопія побудована на двох основних якостях, властивих папілярним узорам шкіри пальців і долонь:

- стабільність малюнка візерунка протягом усього життя людини;
- унікальність малюнка, що означає відсутність двох індивідуумів з однаковими дактилоскопічними відбитками.

Розпізнавання відбитку пальця засноване на аналізі розподілу особих точок (кінцевих точок і точок розгалуження папілярних ліній), местоположення яких задається в декартовій системі координат.

Для зняття відбитків в режимі реального часу застосовуються спеціальниі контактні датчики різних типів. Системи ідентифікації за відбитками пальців випускаються протягом майже трьох десятків років

Американська фірма Fingermatrix запропонувала термінал Ridge Reader, який завдяки процедурі компенсації різних відхилень, виникаючих при знятті

відбитка пальця в реальних умовах, а також застосовуємому способу «очищення» зображення і відновлення папілярного візерунка (який може бути «затуманений» з -за наявності на пальці бруду, масла або поту) допускає коефіцієнт помилок 1-го роду не більше 0,1%, 2-го роду - не більше 0,0001%. Час обробки зображення становить 5 с, реєстрації користувача становить 2-3 хв. Для зберігання одного цифрового відбитку (стандарту) витрачається 256 байт пам'яті.

Компанія De La Rue Printrak Inc. виробляє систему PIV-100 на базі терміналу автентифікації за відбитками пальців. Крім цих терміналів, до складу апаратури входять центральний процесор, контрольний пульт, дисплей, принтер, накопичувачі на Вінчестерських дисках (для зберігання бази даних), накопичувачі на гнучких дисках (для резервної пам'яті).

У цій системі необхідні коефіцієнти помилок можуть вибиратися в залежності від необхідного рівня забезпечення безпеки шляхом підстроювання внутрішніх залежних системних параметрів, таких як порогові значення прийняття рішення, стратегія розпізнавання. Але за високу точність доводиться розплачуватися зменшенням швидкодії і зниженням зручностей для користувачів. Автоматична обробка отриманого дактилоскопічного зображення починається з перетворення первинного образу з дозволом 512 х 512 крапок зображення і щільністю 8 біт на точку до кінцевого набору (безлічі), яка складається приблизно з 100 особливих точок папілярного візерунка, кожна з яких займає 3 байт пам'яті. В результаті обсяг пам'яті для зберігання одного відбитка в порівнянні з початковим зображенням зменшується приблизно в 1000 разів. Зіставлення двох дактилоскопічних образів - оригінального і еталонного, що зберігається в пам'яті системи, - проводиться за допомогою деякої кореляційної процедури. Час реєстрації користувача в базі даних - менше 2 хв; вся процедура перевірки користувача займає близько 10 с, з яких 2 з йде на автентифікацію, т. е. на обчислення по співставленню відбитків.

Говорячи про надійність автентифікаційної процедури з використанням відбитка пальця, необхідно розглянути також питання про можливість їх копіювання і використання іншими особами для отримання несанкціонованого доступу. В якості однієї з можливостей по обману терміналу спеціалісти називають виготовлення штучної кисті з необхідними відбитками пальців (або вилучення «оригіналу» у законного власника). Але існує і спосіб боротьби з такою фальсифікацією. Для цього до складу термінального обладнання повинні бути включені інфрачервоний детектор, який дозволить зафіксувати теплове випромінювання від руки (або пальця), і (або) фотоплетізмограф, який визначає наявність змін відбиття світла від поверхні потоку крові.

Іншим способом підробки є безпосереднє нанесення папілярного візерунка пальців законного користувача на руки зловмисника за допомогою спеціальних плівок або плівкоутворюючих складів. Такий спосіб досить успішно може бути використаний для отримання доступу через КПП. Однак в цьому випадку необхідно отримати якісні відбитки пальців законного користувача, причому саме тих пальців, які були зареєстровані системою, і саме в певній послідовності (наприклад, якщо система налаштована на перевірку не одного,

адвох і більше пальців по черги), але ця інформація невідома законному користувачю і, отже, він не може увійти у змову з порушником.

За оцінками західних експертів до 80% ринку біометрії сьогодні займають пристрої ідентифікації за відбитками пальців. Це пояснюється наступним: по-перше, це один найдоступніших і недорогих методів, по-друге, методика ідентифікації за відбитками пальців проста у використанні, зручна і позбавлена психологічних бар'єрів, які є, наприклад, у систем, що вимагають впливу на очей світловим пучком.

Відомі три основні підходи до реалізації систем ідентифікації за відбитками пальців. Найпоширеніший на сьогодні спосіб будується на використанні оптики - призми і декількох лінз із вбудованим джерелом світла (рис. 5.3).

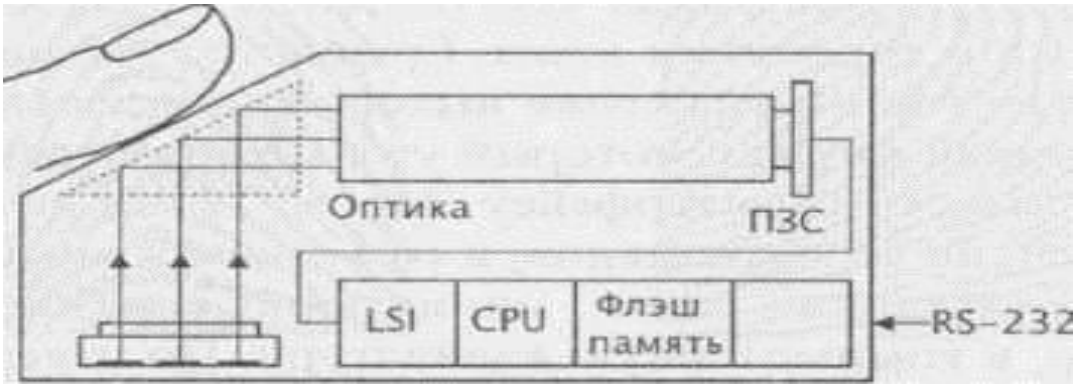

Рис. 5.3. Функціональна схема системи ідентифікатора

Світло, що падає на призму, відбивається від поверхні, що стикаються з пальцем користувача, і виходить через іншу сторону призми, потрапляючи на оптичний сенсор (зазвичай, монохромна відеокамера на основі ПЗС- матриці), де формується зображення. Недоліки такої системи: відбиття сильно залежить від параметрів шкіри - сухості, присутності масла, бензіну, інших хімічних елементів. Наприклад, у людей із сухою шкірою спостерігається ефект розмиття зображення і в результаті - висока частка хибних спрацьовувань.

Інший спосіб використовує методику вимірювання електричного поля пальця з використанням напівпровідникової пластини. Коли користувач встановлює палець в сенсор, він виступає в якості однієї з пластин конденсатора (рис. 5.4). Інша пластина конденсатора - це поверхня сенсора, яка складається з кремнієвого чіпа, що містить 90 тис. конденсаторних пластин з кроком зчитування 500 точок на дюйм. В результаті виходить 8-бітове растрове зображення гребенів і западин пальця.

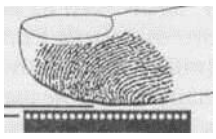

Рис. 5.4. Система ідентифікації на основінапівпроводникової пластини

Природньо, в даному випадку жировий баланс шкіри і ступінь чистоти рук користувача не має ніякого значення. Система ідентифікації в цьому випадку, виходить набагато більш компактна. Недоліки методу - кремнієвий чіп вимагає експлуатації в герметичній оболонці, а додаткові покриття зменшують чутливість системи. Крім того, певний вплив на зображення може досить сильно зовнішнє електромагнітне випромінювання.

Існує ще один метод реалізації таких систем. Його розробила компанія «Who Vision Systems». В основі їх системи TactileSense - електрооптичний полімер. Цей матеріал чутливий до різниці електричного поля між гребенями і западинами шкіри. Градієнт електричного поля конвертується в оптичне зображення з високою роздільною здатністю, яке потім переводиться в цифровий формат, який вже можна передавати в ПК по паралельному порту або USB-інтерфейсу. Метод також нечутливий до стану шкіру і ступеня її забруднення, в тому числі і хімічного. Разом з тим, зчитувач має мініатюрні розміри і може бути вбудовано, наприклад, в комп'ютерну клавіатуру. За твердженням виробників, система має колосально низьку собівартість (на рівні декількох десятків доларів).Характеристики деяких методів наведені у табл. 5.1.

Таблиця 5.1

Характеристики типових систем ідентифікації по відбиткам пальців

Властивості	Оптична система	Напівпровідникова технология	Електрооптичний полімер
Невеликі розміри	Ні	Да	Да
Сприйнятливість до сухоїшкіри	Ні	Да	Да
Міцність поверхні	Середня	Низька	Высока
Енергоспоживання	Середнє	Низьке	Низьке
Ціна	Середня	Висока	Низька

Отриманий одним з описаних методів аналоговий відеосигнал перетворюється у цифрову форму, після чого з нього витягується набір характеристик, унікальних для цього відбитка пальця. Ці дані однозначно ідентифікують особу. Дані зберігаються і стають унікальним шаблоном відбитка пальця конкретної людини. При подальшому зчитуванні нові відбитки пальців порівнюються з збереженими в базі.

У найпростішому випадку при обробці зображення на ньому виділяються характерні точки (наприклад, координати кінця або роздвоєння папілярних ліній, місця з'єднання витків). Можна виділити до 70 таких точок і кожну з них охарактеризувати двома, трьома або навіть великим числом параметрів. В результаті можна отримати від відбитка пальця до п'ятисот значеній різних характеристик.

Більш складні алгоритми обробки з'єднують характерні точки і зображення векторами і описують їх властивості і взаєморозташування (рис. 5.5). Як правило, набір даних, одержуваних з відбитка, займає до 1 Кбайт.

З міркувань безпеки ряд виробників (SONY, Digital Persona і ін.) Використовують при передачі даних засоби шифрування. Наприклад, в системі U are U фірми «Digital Persona» застосовується 128-бітовий ключ, і, крім цього, все що пересилаються пакети мають тимчасову позначку, що виключає можливість їх повторної передачі.

Алгоритм обробки дозволяє зберігати не саме зображення, а його «образ» (набір характерних даних).

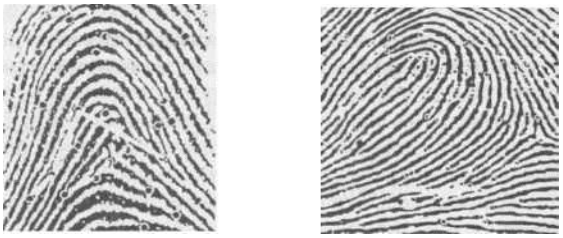

Рис. 5.5. Відображення відбитка пальця та його «образ»

Зберігання даних і порівняння при ідентифікації відбувається в комп'ютері. Практично кожен виробник апаратної частини разом з системою постачає і унікальне програмне забезпечення, адаптоване найчастіше під WindowsNT.

Оскільки більшість систем призначені для контролю доступу до компьютерної інформації і орієнтовані у першу чергу на рядового користувача, ПО відрізняється простотою і не вимагає спеціальної установки.

Слід зазначити одну особливість СКУД, в якій використовуються відбитки пальців: такі пристрої більш громіздкі, ніж інші типи зчитувачів. Це пов'язано з тим, що, по-перше, немає необхідності економити місце на робочому столі, а по-друге, зчитувачі повинні бути автономні. Тому, крім сканера, в один корпус поміщають пристрій прийняття рішення і зберігання інформації, клавіатуру (для збільшення ступеня захищеності) і рідкокристалічний дисплей (для зручності настройки і експлуатації).

При необхідності до системи може бути підключений зчитувач карт (смарт, магнітних і т. Д.). Існують і більш екзотичні моделі. Наприклад, фірма SONY помістила в корпус приладу динамік, а фірма «Mytec» вважає, що майбутнє за інтеграцією біометрії і таблеток Button.

Відзначимо, що всі представлені пристрої призначені для роботи тільки всередині приміщення. Поверхня сканера повинна бути чистою, тому апріорі виключаються запилені склади, бензоколонки і т. Д. Найбільш часте застосування - банківські системи (доступ до сейфів, сховищ цінностей), контроль доступу в різні клуби і заміські резиденції, системи електронної комерції.

2.2 Ідентифікація по райдужній оболонці очей

Першовідкривачем в області ідентифікації особистості по райдужній оболонці ока є доктор Джон Даугман. У 1994 р він запатентував в США метод розпізнавання райдужної оболонки ока (US Patent S, 291, 560). Розроблені ним алгоритми використовуються досі.

За допомогою цих алгоритмів необроблені відеозображення очей перетворюються в унікальний ідентифікаційний двійковий потік Iris-код, отриманий в результаті визначення позиції райдужки, її межі та виконання інших математичних операцій для опису текстури райдужки у вигляді послідовності чергування фаз, схожою на штрих-код.

Отриманий таким чином Iris-код використовується для пошуку збігів в базах даних (швидкість пошуку - близько 1 млн. порівняння Iris-кодів в 1 с) і для підтвердження або непідтвердження заявленій особистості

Перевага сканерів для райдужної оболонки ока полягає в тому, що вони не вимагають від користувача зосередження на цілі, так як зразок плям на райдужній оболонці знаходиться на поверхні ока. Фактично відеозображення ока може бути відсканована на відстані менше 1 м, що робить можливим використання сканерів для райдужної оболонки ока, припустимо, в банкоматах. Розробкою технології ідентифікації особистості на основі принципу сканування райдужної оболонки ока в даний час займаються більше 20 компаній, в тому числі British Telecom, Sensar, японська компанія Oki.

Розрізняють активні і пасивні системи розпізнавання. У системах першого типу користувач повинен сам налаштувати камеру, пересуваючи її для більш точного наведення. Пасивні системи простіше у використанні, оскільки камера в них налаштовується автоматично. Висока надійність цього обладнання дозволяє застосовувати його навіть у виправних установах.

Як приклад сучасної системи ідентифікації на основі аналізу райдужної оболонки ока розглянемо рішення, запропоноване компанією LG [8]

Система IrisAccess дозволяє менш ніж за 1 з відсканувати малюнок радужної оболонки ока, обробити і порівняти з 4 тис. Інших записів, які вона зберігає у своїй пам'яті, а потім послати відповідний сигнал в охоронну систему. Технологія - повністю безконтактна. На основі зображення райдужної оболонки ока будується компактний цифровий код розміром 512 байт. Пристрій має високу надійність в порівнянні з більшістю відомих систем біометричного контролю, підтримує об'ємну базу даних, видає звукові інструкції російською мовою, дозволяє інтегрувати в систему карти доступу і ПІН-клавіатури. Один контролер підтримує чотири зчитувача Система може бути інтегрірована з LAN Система IrisAccess 3000 складається з оптичного пристрою внесення до реєстру E01J3000, віддаленого оптичного пристрою R01J3000, контрольного пристрою розпізнавання ICLI3000, плати захоплення зображення, дверний інтерфейсної плати і PC-сервера. Якщо потрібно здійснювати контроль за декількома входами, то ряд віддалених пристроїв, включаючи ICU3000 і R01J3000, може бути підключений до PC-сервера через локальну мережу (LAN).

Цікавим є камера для ідентифікації особи шляхом сканування райдужної оболонки ока, яка використовується в системах захисту і безпеки для комп'ютерів типу десктоп/лептоп. Розробки візуальних систем (Vision Systems) компанії Panasonic і добре показавші себе на практиці розробки в області ідентифікації особистості на основі малюнка райдужної оболонки очей компанії Iridian Technologies дозволили створити легкі у використанні і відрізняючіся високою точністю засоби, які можна використовувати в широкому діапазоні сучасних і майбутніх потребностей в області забезпечення безпеки.

Камера Authenticam компанії Panasonic в поєднанні з програмним продуктом PrivatelD ™ компанії Indian Technologies представляє собою економічно вигідний і надійний шлях забезпечення безпеки доступа. Для такої камери характерні безпеку і простота використання. Досить поглянути в об'єктив камери з відстані приблизно 50 см, і менш ніж через 2 з відбудеться захоплення зображення.

Програмний продукт PrivatelD ™ обробляє малюнок веселкової оболонки очей і кодує отриману інформацію у вигляді 512-байтовой записи IrisCode. Ці записи вводяться для зберігання в пам'ять і використовуються для порівняння з іншими записами кодів IrisCodes - для ідентифікації особистості при будь-яких транзакціях і ділових операціях, коли для порівняння представляється райдужна оболонка ока живу людину.

Диференціатор ключів для ідентифікації особи по малюнку райдужної оболонки ока здійснює пошук в базі даних для знаходження відповідного ідентифікаційного коду. При цьому база даних може складатися з необмеженого числа записів кодів IrisCode.

Технологія допуску, заснована на скануванні райдужної оболонки ока, вже кілька років успішно застосовується в державних організаціях США і в установах з високим ступенем секретності (зокрема, на заводах з виробництва ядерного озброєння). Ефективність цього способу доведена, він безпечний для користувача і надійний в роботі. Він забезпечує моментальну автентифікацію особистості, призначену для заміни символів ПІН-кодів і паролів.

Багато експертів підкреслюють «незрілість» технології, хоча потенціальні можливості методу досить високі, тому що характеристики рисунка райдужної оболонки людського ока досить стабільні і не змінюються практично протягом усього життя людини, несприйнятливі до забруднення і ран. Відзначимо також, що райдужки правого і лівого ока по малюнку істотно розрізняються. Цей метод ідентифікації відрізняється від інших більшою складністю у використанні, більш високою вартістю апаратури і жорсткими умовами реєстрації.

2.3. Ідентифікація по капілярах сітківки очей.

При ідентифікації по сітківці ока вимірюється кутовий розподіл кровоносних судин на поверхні сітківки щодо сліпої плями очі і інші ознаки. Капілярний малюнок сітківки очей різниться навіть у близнюків і може бути з великим успіхом використаний для ідентифікації особи. Всього налічують

близько 250 ознак. Такі біометричні термінали забезпечують високу достовірність ідентифікації, яку можна порівняти з дактилоскопії, але вимагають від особи, що перевіряється фіксації погляду на об'єктиві сканера.

Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, спрямованого через зіницю до кровоносних судинах на задній стінці ока. Сканери сітківки ока набули широкого поширення в СКУД особливо секретних об'єктів, так як у них один з найнижчих відсотків відмови в доступі зареєстрованих користувачів і практично не буває помилкового дозволу доступу. Однак зображення райдужної оболонки має бути чітким, тому катаракта може негативно впливати на якість ідентифікації особистості.

Початок розробок цього напрямку ідентифікації відноситься до 1976 року, коли в США була утворена компанія Eye Dentify, яка до теперішнього часу зберігає монополію на виробництво комерційних систем автентифікації по сітківці.

Основним пристроєм для системи такого типу є бінокулярний об'єктив. При здійсненні процедури автентифікації користувач повинен припасти очима до окулярів і, дивлячись всередину, сфокусувати погляд на зображенні червоного кольору. Потім йому слід дочекатися зміни кольору на зелений (що вкаже на правильне фокусування) і натиснути на кнопку пуску. Сканування очного дна виконується джерелом інфрачервоного випромінювання, безпечного для очей. Досить дивитися у вічко камери менше хвилини. За цей час система встигає підсвітити сітківку і отримати відбитий сигнал. Для сканування сітківки використовується інфрачервоне випромінювання низької інтенсивності, спрямоване через зіницю до кровоносних судинах на задній стінці ока. Відбите від сітківки випромінювання фіксується спеціальної чутливої камерою.

Заміри ведуться по 320 точок фотодатчиками і результуючий аналоговий сигнал за допомогою мікропроцесора перетворюється в цифровий вигляд. При цьому використовується алгоритм швидкого перетворення Фур'є. Отриманий цифровий вектор, що складається з коефіцієнтів Фур'є, порівнюється з зареєстрованим еталоном, що зберігається в пам'яті системи. Завдяки такому методу перетворення і представлення зображення очного дна для зберігання кожного еталона витрачається по 40 байт. Пам’ять терміналу Eye Dentification System 7.5, що реалізує цей алгоритм, розрахована на запам'ятовування до 1200 еталонів. Час реєстрації випадках становить приблизно 30 с, час автентифікації - 1,5 с

З точки зору безпеки дана система вигідно відрізняється від усіх інших, що використовують біометричні термінали, не тільки малим значенням коефіцієнтів помилок як 1-го, так і 2-го роду, а й використанням специфічного автентіфікаціонного атрибута, який практично неможливо негласно підмінити для обману системи при перевірці.

До недоліків подібних систем слід віднести психологічний фактор: не кожна людина зважиться подивитися в невідоме темне, де щось світить в око. До того ж треба стежити за становищем очей щодо отвору, оскільки подібні системи, як правило, чутливі до неправильної орієнтації сітківки. Сканери для сітківки очей отримають велике поширення при організації доступу до

надсекретних системам, оскільки гарантують один з найнижчих відсотків відмови в доступі зареєстрованих користувачів і майже нульовий відсоток помилок.

Лекція № 6.

Тема лекції: Динамічні методи біометричного контролю

План лекції:

1. Ідентифікація по почерку.
2. Ідентифікація по голосу.
3. Ідентифікація по ритму роботи на клавіатурі.

1. Ідентифікація по почерку і динамікі підпису/

Основою автентифікації особистості по почерку і динаміці написання контрольних фраз (підписи) є унікальність і стабільність динаміки цього процесу для кожної людини, характеристики якої можуть бути виміряні, переведені в цифровий вигляд і піддані комп'ютерної обробки.

Розробка автентифікаційних автоматів на базі аналізу почерку (підпису - як варіанти об'єкта дослідження), призначених для реалізації контрольно-пропускної функції, була розпочата ще в початку 1970-х р В даний час на ринку представлено кілька ефективних терміналів такого типу.

Підпис - такий же унікальний атрибут людини, як і його фізіолого-етичні характеристики. Крім того, це і більш звичний для будь-якої людини метод ідентифікації, оскільки він, на відміну від зняття відбитків пальців, не асоціюється з кримінальною сферою. Одна з перспективних технологій автентифікації заснована на унікальності біометричних характеристик руху людської руки під час письма. Зазвичай виділятимуть два способи обробки даних про підписи: просте порівняння зі зразком і динамічну верифікацію. Перший вельми ненадійний, тому що заснований на звичайному порівнянні введеної підписи зі зберігаючимися в базі даних графічними зразками. Через те, що підпис не може бути завжди однаковим, цей метод дає великий відсоток помилок. Спосіб динамічної верифікації вимагає набагато складніших обчислень і дозволяє в реальному часі фіксувати параметри процесу підпису, такі, як швидкість руху руки на різних ділянках, сила тиску і тривалість різних етапів підпису. Це дає гарантії того, що підпис не зможе підробити навіть досвідчений графолог, оскільки ніхто не в змозі в точності скопіювати поведінку руки власника підпису. Користувач, використовуючи стандартний дігітайзер і ручку, імітує свою звичайну підпис, а система зчитує параметри руху і звіряє їх з тими, що були заздалегідь введені в базу даних. При збігу образу підпису з еталоном система прикріплює до підписуємого документу інформацію, що включає ім'я користувача, адресу його електронної пошти, посаду, поточний час і дату, параметри підписи, що містять кілька десятків характеристик динаміки руху (напрямок, швидкість, прискорення) та інші. Ці дані шифруються, потім для них обчислюється контрольна сума, і далі все це шифрується ще раз, утворюючи так звану біометричну мітку. Для настройки системи знову зареєстрований користувач від п'яти до десяти разів

виконуєпроцедуру підписання документа, що дозволяє отримати усереднені показники і довірчий інтервал.

Ідентифікацію за підписом не можна використовувати всюди, зокрема, цей метод не підходить для обмеження доступу в приміщення або для доступу в комп'ютерні мережі. Однак в деяких областях, наприклад в банківській сфері, а також усюди, де відбувається оформлення важливих документів, перевірка правильності підпису може стати найбільш ефективним, а головне, необтяжливим і непомітним способом. До сих пір фінансове співтовариство не поспішало приймати автоматизовані методи ідентифікації підписи для кредитних карток і перевірки заяви, тому що підписи все ще занадто легко підробити. Це перешкоджає впровадженню ідентифікації особистості по підпису в високотехнологічні системи безпеки.

Пристрої ідентифікації по динаміці підпису використовують геометричні або динамічні ознаки рукописного відтворення підпису в реальному масштабі часу. Підпис виконується користувачем на спеціальній сенсорній панелі, за допомогою якої здійснюється перетворення змін прикладеного зусилля натискання на перо (швидкості, прискорення) в електричний аналоговий сигнал. Електронна схема перетворює цей сигнал в цифровий вигляд, пристосований для машинної обробки. При формуванні «еталона» необхідно враховувати, що для одного і того ж людини характерний деякий розкид характеристик почерку від одного акта до іншого. Щоб визначити ці флуктуації і призначити рамки, користувач при реєстрації виписує свій підпис кілька разів. У результаті формується якась «стандартна модель» (сигнатурний еталон) для кожного користувача, яка записується в пам'ять системи.

Системи автентифікації по почерку поставляються на ринок, наприклад, фірмами Inforete і De La Rue Systems (США), Thompson T1TN (Франція) і рядом інших. Англійська фірма Quest Micropad Ltd випустила пристрій QSign, особливістю якого є те, що сигнатурний еталон може зберігатися як в пам'яті системи, так і в пам'яті ідентифікаційної карточки користувача. Граничне значення коефіцієнтів помилок може змінюватися в залежності від необхідного ступеня безпеки. Підпис виконується звичайною кульковою ручкою або олівцем на спеціальній сенсорної панелі, що входить до складу терміналу.

Основна перевага підпису в порівнянні з використанням, наприклад, дактилоскопії в тому, що це поширений і загальновизнаний спосіб підтвердження своєї особи (наприклад, при отриманні банківських вкладів). Цей спосіб не викликає «технологічного дискомфорту», як буває в разі зняття відбитків пальців, що асоціюється з діяльністю правоохоронних органів. У той же час підробка динаміки підпису - справа дуже важкоздійснювана (на відміну, скажімо, від відтворення малюнка підписи). Причому завдяки розпису не на папері, а на сенсорної панелі, значно ускладнюється копіювання зловмисником її накреслення.

Ідентифікація за ритмом роботи на клавіатурі заснована на вимірюванні часових інтервалів між двома послідовними ударами по клавішам при друкуванні знаків.

2. Ідентифікація по голосу і особливостям мови.

Біометричний підхід, пов'язаний з ідентифікацією голосу, зручний в застосуванні. Однак основним і визначальним недоліком цього підходу є низька точність ідентифікації. Наприклад, людина з застудою або ларингітом може зазнавати труднощів при використанні даних систем. Причинами впровадження цих систем є повсюдне розповсюдження телефонних мереж і практика вбудовування мікрофонів в комп'ютери і периферійні пристрої. Як недоліки таких систем можна назвати чинники, що впливають на результати розпізнавання: перешкоди в мікрофонах, вплив навколишнього оточення на результати розпізнавання (шум), помилки при проголошенні, різне емоційний стан перевіряємого в момент реєстрації еталона і за будь-якої ідентифікації , використання різних пристроїв реєстрації під час запису еталонів і ідентіфікації, перешкоди в низькоякісних каналах передачі даних і т. п.

При розгляді проблеми автентифікації по голосу важливими питаннями з точки зору безпеки є наступні:

Як боротися проти використання магнітофонних записів парольних фраз, перехоплених під час встановлення контакту законного користувача з аутентифікаційних терміналом?

Як захистити систему від зловмисників, що володіють здатністю до імітації голосу, якщо їм вдасться дізнатися парольний фразу?

Відповіддю на перше питання є генерація системою псевдовипадкових паролів, які повторюються слідом за нею користувачем, а також застосування комбінованих методів перевірки (доповнюючи введенням ідентифікаційної картки або цифрового персонального коду).

Відповідь на друге питання не таке однозначне. Людина виробляє свою думку про специфіку сприйманого голосу шляхом оцінки деяких його характерних якостей, не звертаючи увагу при цьому на кількісну сторону різноманітних дрібних компонент мовного сигналу. Автомат же навпаки, не володіючи здатністю вловлювати узагальнену характеристику голосу, свій висновок робить, грунтуючись на конкретних параметрах мовного сигналу і виробляючи їх точний кількісний аналіз.

Специфічне слухове сприйняття людини призводить до того, що бездоганне відтворення професійними імітаторами голосів можливе лише тоді, коли наслідувати суб'єкт характеризується яскраво вираженими особливостями вимови (інтонаційної картиною, акцентом, темпом мови і т. д.) Або тембру (гугнявість , шепелявістю, картавістю і т. д.). Саме цим можна пояснити той факт, що навіть професіональні імітатори виявляються не в змозі наслідувати ординарним, не примітним голосам.

На противагу людям розпізнають автомати, вільні від суб'єктивного ставлення до більш прийнятною образам, виробляють автентіфікацію (розпізнавання) голосів об'єктивно, на основі строго детермінованих і апріорі заданих ознак. Володіючи «нелюдським» критерієм оцінки схожості голосів, системи сприймають голос людини через призму своїх ознак. Внаслідок цього, чим складніше і «не зрозумілішим» буде сукупність ознак, за якими автомат

розпізнає голос, тим менше буде вірогідність його обману. У гоже час, незважаючи на те, що проблема імітації дуже важлива і актуальна з практичної точки зору, вона все ж далека від остаточного рішення. Перш за все до кінця не ясний відповідь на питання, які саме параметри мовного сигналу найбільш доступні наслідування і які з них найбільш важко піддаються йому.

Вибір параметрів мовного сигналу здатних щонайкраще описати індивідуальність голосу є, мабуть, найважливішим етапом при побудові систем автоматичної автентифікації по голосу. Такі параметри сигналу, звані ознаками індивідуальності, крім ефективності подання інформації про особливості голосу диктора, повинні володіти рядом інших властивостей. По-перше, вони повинні бути легко вимірювані і мало залежати від чинників, що заважають навколишнього середовища (шумів і перешкод) По-друге, вони повинні бути стабільними в часі. По-третє, не повинні піддаватися імітації.

Постійно ведуться роботи по підвищенню ефективності систем ідентіфікації по голосу. Відомі системи аутентифікації по голосу, де застосовується метод спільного аналізу голосу і міміки, бо, як виявилося, міміка мовця характерна тільки йому і буде відрізнятися від мовця ті ж слова міміки іншої людини.

Розробляються комбіновані системи, що складаються з блоків ідентіфікації і верифікації голосу. При вирішенні задачі ідентифікації знаходиться найближчий голос (або кілька голосів) з фонотеки, потім за результатом рішення задачі верифікації підтверджується або спростовується приналежність фонограми конкретній особі. Система практично використовується при забезпеченні безпеки деяких особливо важливих об'єктів.

Останнім часом ведуться активні розробки з удосконалення і модифікації голосових систем ідентифікації особистості, пошук нових підходів для характеристики людської мови, комбінації фізіологічних і поведінкових факторів.

Завдання підвищення надійності розпізнавання може бути вирішена за рахунок залучення граматичної і семантичної інформації в системах розпізнавання мови. Для вирішення цього завдання розроблена (за участю експертів: лінгвістів, рядових носіїв мови) модель вхідного мови, що враховує особливості їх граматичної та семантичного поведінки (28 основних граматичних класів, близько 300 граматичних розрядів слів), її комп'ютерне втілення - лінгвістична база знань (ЛБЗ) і лінгвістичний процесор (ЛП). До складу ЛБЗ входять: великий граматичний словник - об'ємом близько 100000 одиниць; словники словосполучень; словники уніграм і лексичних біграм; граматичні таблиці і словник моделей управління. Програми синтактіко-семантичного аналізу, що входять до складу ЛП, забезпечують: швидке відсіювання малоймовірних варіантів розпізнавання (локальний аналіз), облік виявлених при аналізі граматичних подій, що характеризують регулярність граматичної структури і ступінь граматичності пропозиції в цілому або окремих груп (і тим самим можливість вибору в якості остаточного результату розпізнавання неграматичних, але допустимих в мові варіантів). Для вирішення багатокритеріальної задачі вибору остаточного варіанту були розроблені

спеціальні евристики метарівня. Лінгвістичний модуль (ЛБЗ і ЛП) дозволяє підвищити надійність акустичного і фонетичного розпізнавання з 94-95 до 95-97%.

Приділяється увага проблемам автоматизованого формування та супроводу ЛБЗ систем розпізнавання мови (для англійської та російської мов): побудова тезауруса, корекція словника лексичних n-грам на основі синтактіко-семантичної інформації і ін. Нові методи, як показують результати експериментів, дозволяють підвищити надійність розпізнавання ще на 1%.

Сьогодні ідентифікація по голосу використовується для управління доступом в приміщення середнього ступеня секретності, наприклад, лабораторії виробничих компаній. Лідерами в розробці таких систем є компанії T-Netix, ITT Nuance, Veritel. В системі фірми Texas Instruments (TI) парольні фрази складалися з 4-словного пропозиції, причому кожне слово було односкладових. Кожна фраза була 84 байтами інформації. Час автентифікації становило 5,3 с. Для запобігання використанню зарання записаного на магнітофон пароля система генерувала слова в довільній послідовності. Загальний час перевірки на КПП становило 15 с на одну людину. Для чотирьох пральних фраз помилка 1-го роду склала 0,3%, 2-го роду - 1%.

3. Ідентифікація за ритмом роботи на клавіатурі.

Сучасні дослідження показують, що клавіатурний почерк користувача володіє деякою стабільністю, що дозволяє досить однозначно ідентифікувати користувача. Застосовуються статистичні методи обробки вихідних даних і формування вихідного вектора, який є ідентифікатором даного користувача. В якості вихідних даних використовують тимчасові інтервали між натисканням клавіш на клавіатурі і час їх утримання. При цьому тимчасові інтервали між натисканням клавіш характеризують темп роботи, а час утримання клавіш характеризує стиль роботи з клавіатурою - різкий удар або плавне натискання.

Ідентифікація користувача по клавіатурного почерку можлива наступними способами:

- по набору ключової фрази;
- по набору довільного тексту.

Принципова відмінність цих двох способів полягає в тому, що в першому випадку використовується ключова фраза, що задається користувачем в момент реєстрації його в системі (пароль), а в другому випадку використовуються ключові фрази, які генеруються системою кожен раз в момент ідентифікації користувача. Маю на увазі 2 режиму роботи:

- навчання;
- ідентифікація.

На етапі навчання користувач вводить деяке число раз запропоновані йому тестові фрази При цьому розраховуються і запам'ятовуються еталонні характеристики даного користувача. На етапі ідентифікації розраховані оцінки порівнюються з еталонними, на підставі чого робиться висновок про збіг або розбіжності параметрів клавіатурного почерку. Вибір тексту, на якому

виконується навчання системи, - досить важний етап для нормального функціонування системи. Пропоновані користувачу фрази необхідно підбирати таким чином, щоб використовувані в них символи повністю і рівномірно покривали робоче поле клавіатури. Більш того, якщо в процесі навчання системи видно, що статистичні характеристики окремих клавіш мають істотний розкид, необхідно формувати чергову тестову фразу таким чином, щоб зменшити цю невизначеність. Можлива організація «неявного» процесу навчання системи, коли програма перехоплює весь введення з клавіатури і відповідно розраховує еталонні характеристики користувача. Дана процедура досить легко організовується практично в будь-який операційній системі. В DOS для цього використовується перехоплення переривань від клавіатури, в Windows - стандартний механізм пасток (hooks).

Однак існує ряд обмежень щодо застосування даного способу на практиці. Застосування методу ідентифікації по клавіатурного почерку доцільно тільки по відношенню до користувачів з досить великим досвідом роботи з комп'ютером і сформованим почерком роботи на клавіатурі, т. Е. До програмістам, секретарям і т. Д. В іншому випадку ймовірність неправильного впізнання «легального» користувача суттєво зростає і робить непридатним даний спосіб ідентифікації на практиці. Виходячи з теорії машинопису і діловодства можна визначити час становлення почерку роботи з клавіатурою, при якому досягається необхідна ймовірність ідентифікації користувача: приблизно 6 місяців.

У задачі ідентифікації користувача по клавіатурного почерку важливим етапом є обробка первинних даних. В результаті цієї обробки вхідної потік даних розділяється на ряд ознак, що характеризують ті чи інші якості ідентифікованої особистості. Надалі ці ознаки, піддаючись статистичної обробки, дозволяють отримати ряд еталонних характеристик користувача.

Початковий етап обробки даних - фільтрація. На цьому етапі з потоку даних видаляється інформація про «службових» клавішах - клавішах управління курсором, функціональні клавіші і т. І.

Потім виділяється інформація, що відноситься до наступних характеристиках користувача:

- кількість помилок при наборі;
- інтервали між натисканнями клавіш;
- час утримання клавіш;
- число перекриттів між клавішами;
- ступінь аритмічності при наборі;
- швидкість набору.

Збільшити число еталонних характеристик, а отже, збільшити надійність системи можна, виконавши поділ вхідного потоку на дані, що відносяться до лівій і правій руці відповідно. Роботу даного алгоритму можна побудувати, спираючись на ряд досить простих правил, наприклад: клавіша SHIFT натискається, як правило, мізинцем лівої руки; клавіша ENTER - п'ятим або другим пальцем правої руки і т. п. Причому, аналізуючи відносний час між натисканням клавіші ENTER і попередньої клавіші, можна з певною

ймовірністю передбачити, яким пальцем була натиснута клавіша ENTER, так як час натискання цієї клавіші мізинцем буде істотно менше, ніж для будь-якого іншого пальця. Процес реалізації алгоритму достатньо складний, так як для цього необхідно використовувати рекурсивні алгоритми аналізу вхідного потоку даних.

В останні роки застосовують нейромережевий підхід до задачі ідентифікації Нейронні мережі - це узагальнена назва декількох груп алгоритмів, що володіють одним цінним властивістю: вони вміють навчатися на прикладах, витягуючи приховані закономірності з потоку даних. Якщо між вхідними та вихідними даними існує якийсь зв'язок, нехай навіть не виявляємий традиційними кореляційними методами, нейронна мережа здатна автоматично налаштуватися на неї з заданим ступенем точності.

Застосування нейромережевого підходу до задачі ідентифікації користувача по клавіатурного почерку дозволяє вирішити ряд проблем, що виникають при використанні стандартних методів статистичної обробки вхідного потоку даних.

Зокрема, застосування статистичних методів обробки даних базується на твердженні, що вхідні величини підпорядковані нормальному закону розподілу, хоча в ряді випадків це твердження не так. Наприклад, проведені дослідження показують, що час утримання клавіш - при малому кроці дискретизації - описується перетином двох нормальних розподілів, що призводить до великих погрішностей при розрахунку еталонних характеристик користувача.

Крім того, нейронна мережа має властивість фільтрації випадкових перешкод, присутніх у вхідних даних, що дозволяє відмовитися від алгоритмів згладжування експериментальних залежностей, необхідних при статистичній обробці даних.

Найбільш перспективним методом рішення задачі ідентифікації користувача по клавіатурного почерку представляється використання тришарового перцептрону Розенблатта наступної конфігурації:

- первинний шар - вхідний, складається з К формальних нейронів з лінійною активаторною функцією, де К - розмірність вхідного вектора, що містить параметри клавіатурного почерку користувача;
- другий шар - прихований, складається з К формальних нейронів з сігмоідною активаторною функцією,
- третій шар - вихідний, складається з п формальних нейронів з сигма-їдною активаторною функцією, де п - число зареєстрованих користувачів.

Пропонований підхід до задачі ідентифікації користувача по клавіатурному почерку дозволяє збільшити розмірність вектора, що містить еталонні характеристики користувача. Застосування нейронних мереж позволяет спростити математичний апарат обробки даних і зменшити ймовірність виникнення помилок другого роду - позитивного результату ідентифікації для незареєстрованих користувачів. В результаті можливе істотне підвищення надійності і стійкості роботи систем ідентифікації користувача по клавіатурного почерку.

4. Біометричні технології майбутнього.

Спектр технологій, які можуть використовуватися в системах безпеки, постійно розширюється. В даний час ряд біометричних технологій знаходиться в стадії розробки, причому деякі з них вважаються дуже перспективними. До них відносяться технології на основі:

- термограми особи в інфрачервоному діапазоні випромінювання;
- характеристик ДНК;
- клавіатурного почерку;

аналіз структури шкіри і епітелію на пальцях на основі цифрової ультразвукової інформації (спектроскопія шкіри);

- аналіз відбитків долонь;
- аналіз форми вушної раковини;
- аналіз характеристик ходи людини;
- аналіз індивідуальних запахів людини;
- розпізнавання за рівнем солоності шкіри;
- розпізнавання по розташуванню вен.

Технологія побудови та аналізу термограми є одним з останніх досягнень в області біометрії. Як виявили вчені, використання інфрачервоних камер дає унікальну картину об'єктів, що знаходяться під шкірою обличчя. Різні щільності кістки, жиру і кровоносних судин строго індивідуальні і визначають термографічну картину особи користувача. Термограма особи є унікальною, внаслідок чого можна впевнено розрізняти навіть абсолютно схожих близнюків. З додаткових властивостей цього підходу можна відзначити його інваріантність по відношенню до будь-яких косметичних або косметологічних змін, включаючи пластичну хірургію, зміни макіяжу і т. п., А також скритність процедури реєстрації.

Технологія, побудована на аналізі характеристик ДНК (метод геномої ідентифікації) є, по всій видимості, хоча і самої тривалої, але і найбільш перспективною з систем ідентифікації. Метод заснований на тому, що в ДНК людини є поліморфні локуси (локус - положення хромосоми (в гені або алелі), часто мають 8-10 алелей. Визначення набору цих алелей для декількох поліморфних локусів у конкретного індивіда дозволяє отримати свого роду геномну карту , характерну тільки для цієї людини. Точність даного методу визначається характером і кількістю аналізованих поліморфних локусів і на сьогодня дозволяє досягти рівня 1 помилки на 1 млн осіб.

Динаміку ударів по клавіатурі комп'ютера (клавіатурний почерк) при друкуванні тексту аналізує спосіб (ритм) друкування користувачем тієї або іншої фрази. Існують два типи розпізнавання клавіатурного почерку. Перший призначена для автентифікації користувача при спробі отримання доступу до обчислювальних ресурсів. Другий здійснює моніторінговий контроль вже після надання доступу і блокує систему, якщо за комп'ютером почав працювати не та людина, з яким доступ був наданий спочатку. Ритм роботи на клавіатурі, як показали дослідження ряду фірм і організацій, є досить індивідуальною характеристикою користувача і цілком придатний для його ідентіфікації і

автентифікації. Для вимірювання ритму оцінюються проміжки часу або між ударами при друкуванні символів, розташованих в визначеній послідовності, або між моментом удару по клавіші і моментом її відпускання при друкуванні кожного символу в цій послідовності. Хоча другий спосіб вважається більш ефективним, найкращий результат досягається спільним використанням обох способів. Відмінною особливістю цього методу є його дешевизна, так як для аналізу інформації не потрібно ніякого устаткування, крім клавіатури. У літературі описані 4 математичних підходу до вирішення задачі розпізнавання клавіатурного почерку користувача ЕОМ: статистичний, ймовірносно-статистичний (на базі теорії розпізнавання образів) і нечіткої логіки (на основі нейромережевих алгоритмів).

Слід зазначити, що в даний момент дана технологія знаходиться в стадії розробки, і тому складно оцінити ступінь її надійності, особливо з урахуванням високих вимог, що пред'являються до систем безпеки.

Для ідентифікації людини по руці використовують кілька біометричних параметрів - це геометрична форма кисті руки або пальців, розташування підшкірних кровоносних судин долоні, візерунок ліній на долоні. Технологія аналізу відбитків долонь стала розвиватися порівняно недавно, але вже має певні досягнення. Причиною розвитку цієї технології послужив той факт, що пристрої для розпізнавання відбитків пальців мають недолік - їм потрібні тільки чисті руки, а відбиток брудного пальця система може і не розпізнати. Тому ряд компаній-розробників (наприклад, у Великобританії) зосередилися на технології, яка аналізувала не малюнок ліній на шкірі, а обрис долоні, яке також має індивідуальний характер. Аналогічна система, що працює з відбитками пальців, успішно використовується британськими поліцейськими вже три роки. Але одних лише відбитків пальців, як стверджують криміналісти, часто виявляється недостатньо. До 20% слідів, що залишаються на місці злочину - це відбитки долонь. Однак їх аналіз традиційними засобами досить трудомісткий. Комп'ютеризація цього процесу дозволить використовувати відбитки долонь більш широко і призведе до істотного збільшення розкриття злочинів. Слід зазначити, що пристрої сканування долоні, як правило, мають високу вартість, і тому оснастити ними велике число робочих місць не так вже й просто.

Технологія аналізу форми вушної раковини є однією з найбільш останніх підходів в біометричної ідентифікації людини. За допомогою навіть недорогий WEB-камер можна отримувати досить надійні зразки для порівняння та ідентифікації. Цей спосіб недостатньо вивчений, в літературі і достовірна інформація про поточний стан справ відсутня.

Лекція № 7.

Тема лекції: Контролери СКУД

План лекції:

1. Автономні контролери.
2. Мережеві контролери.
3. Розгалужені контролери.

1. Автономні контролери.

Контролери - інтелектуальний елемент системи контролю управління доступом, підрозділяють на автономні, мережні і інтегровані. Контролерів в системі може бути кілька, а в великих системах вони ще й багаторівневі. Контролери низького рівня встановлюються зазвичай поблизу зчитувача і з завданням справляються самі, якщо ж зустрічають незнайому карту, запитують контролер більш високого рівня, який їх координує. У більш складних випадках запит йде на центральний комп'ютер, який зберігає всю базу даних. У мінімальному варіанті контролер може бути вбудований в корпус зчитувача. Іноді всі проблеми лягають на стандартний комп'ютер. Хороші контролери обов'язково підтримують режим зв'язку з віддаленим комп'ютером по телефонній лінії. Це дозволяє централізовано координувати базу даних у всіх філіях однієї організації, і, крім того, мати оперативні рапорти про всі позаштатних ситуаціях.

Автономні (локальні) СКУД, керовані мікрокомп'ютером, як правило, обслуговують один КПП (можливо, з декількома лінійками проходу і відповідно контрольними терміналами). Ідентифікаційна інформація про користувачів і їхні повноваження зберігається в локальній базі даних. СКУД такого типу найбільш прості по конфігурації, але і найменш надійні з точки зору можливості виведення їх з ладу. Вони можуть застосовуватись в основному на тих об'єктах, де не потрібен високий рівень безпеки. Часто в літературі такі системи звуться однодверними.

Найчастіше до контролера можна підключити до двох зчитувачів, які встановлюються на двоє дверей або на одну для контролю входу та виходу. Один з зчитувачів можна замінити на клавіатуру для набору коду. Крім цього, система дозволяє підключати електрозамки, кнопки виходу, геркони, ІЧ-датчики, сирену і ін.

Існують однодверні системи, аналогічні описаної вище, але в них зчитувач і контролер об'єднані в один корпус, т. б. блок, який приймає рішення про відкриття замку, знаходиться в зчитувальному модулі. Це, з одного боку, здешевлює систему, але з іншого - зменшує функціональні можливості, а головне - збільшує ймовірність злому корпусу зчитувача і замикання контактів, до яких підключений замок.

У ще більш дешевих системах поєднуються в одному корпусі приймаються рішення блок, клавіатура для набору коду, зчитувач і замок. Найбільшого поширення такі системи отримали в готелях.

На об'єктах з вимогами підвищеної безпеки застосовуються контролери з цифровим управлінням реле замку. Виносний модуль реле замку монтується безпосередньо біля замку і управляється особливим цифровим кодом. Найчастіше в автономних системах використовуються зчитувачі магнітних карт «тач-меморі» і проксиміті, набагато рідше - біометричні засоби, індентифкатори Віганда або інші зчитувачі.

Але в більшості автономних систем зчитувачі суміщені з клавіатурою для набору індивідуального коду. За допомогою клавіатури здійснюється програмування систем.

Системи на основі одного або кількох автономних контролерів здійснюють всі необхідні дії, властиві СКУД, автономно (без використання комп'ютера, що управляє).

Контролери в таких системах зобов'язані мати власний буфер пам'яті номерів карт (ідентифікаторів) і відбуваються в системі подій. Зазвичай вони мають вихід на локальний принтер для роздруківки протоколу подій. Програмуються зазначені контролери, як правило, з будь-яких кнопкових панелей або за допомогою майстер-карт, що дозволяють заносити в пам'ять контролера нові карти і видаляти старі. Один контролер в таких системах зазвичай керує доступом в одну (максимум - дві) двері. В якості ідентифікаторів (електронних перепусток) в таких системах можуть застосовуватися: магнітні карти, електронні «таблетки» - «і Button», радіочастотні PROX-карти і ін. Всі пристрої управління дверима та охоронними шлейфами (реле управління замком, входи для підключення датчика двері , кнопки виходу і охоронних датчиків) розташовуються в автономних системах зазвичай на платі самого контролера. Часто сам контролер конструктивно об'єднується в одному корпусі зі зчитувачем. Найбільш прості автономії системи (часто звані - «готельними») взагалі об'єднують в одному корпусі контролер прийняття рішень, зчитувач/клавіатуру і електрозамок. Слід, однак, відзначити, що дана міра, що дозволяє знизити собівартість системи, може призвести до зниження безпеки, збільшуючи ймовірність злому системи

З метою підвищення безпеки в найбільш досконалих автономних системах застосовується винесене цифрове реле управління замком. Дана міра дозволяє запобігти спробам проникнення в приміщення шляхом прямого підключення електрозамка до проводів живлення

У деяких системах передбачена можливість розширення. Досягається це різними способами:

- за рахунок об'єднання окремих контролерів в мережу (використання додаткового мережевого модуля на додаток до контролера);
- шляхом збільшення потужності і ускладнення самого контролера, що дозволяє підключати до нього більше двох зчитувачів.

В обох випадках для зв'язку контролерів між собою або з периферійними виконавчими модулями часто використовується будь-якої стандартний

інтерфейс, наприклад RS-485. Слід, однак, пам'ятати, що програмувати доводиться кожен контролер окремо (незважаючи на обмін даними між ними). Для систем з числом дверей більше трьох даний процес може виявитися дуже виснажливим і трудомістким (особливо при великій кількості користувачів). У цьому випадку кращим є установка найпростіших мережевих СКУД.

2. Мережеві контролери.

Мережі контролерів бувають однорангові (однорівневі) і багаторангові (багаторівневі), де число рівнів рідко перевищує два.

У одноранговій мережі є єдина шина (вона може подовжуватися за рахунок повторювачів або розгалужувачів). У тимчасової мережі всі її вузли (контролери доступу) мають рівні права (рис. 7.1).

Рис. 7.1. Однорангова мережа

Недоліки однорангової мережі:

- необхідність мати в кожному контролері повну базу даних (список користувачів, їх прав і т. д.);
- неможливість реалізації деяких глобальних функцій, що вимагають взаємозалежної роботи декількох контролерів (наприклад, глобальний «антіпасбек» - заборона повторного проходу). Цей недолік має місце тільки в мережах, де комп'ютер є провідним, т. б. обмін інформацією відбувається тільки за його ініціативою. Якщо мережа контролерів працює на принципі довільного доступу, не¬достаток відсутня.

Переваги: максимальна «живучість» мережі, оскільки кожен контролер має все необхідне для автономної роботи при вимкненому («завислому») комп'ютері або пошкодженні мережі. Для систем безпеки це є суттєвим фактором

У **багаторанговій** мережі контролерів є провідний, або майстер-контролер, який координує роботу «відомих» контролерів, реально керуючих однією або декількома точками проходу (рис. 7.2). Такі системи мають як переваги, так і недоліки.

Рис. 7.2. Багаторангова мережу

Недоліки багаторангової мережі:

- порушення роботи системи при пошкодженні зв'язку між майстер-контролером і веденими контролерами, оскільки значна частина інформації і алгоритмів є, прерогативою майстер контролера;
- подорожчання невеликих систем за рахунок високої вартості майстер-контролера (через його явної надмірності).

Переваги багаторангової мережі:

- централізована пам'ять для баз даних, що сьогодні не дуже важливо;
- реалізація всіх функцій навіть при виключенні комп'ютера;
- виграш у вартості однієї точки проходу при середніх і великих розмірах системи.

Оцінюючи загальну топологію, необхідно відзначити, що сегменти мережі можуть існувати в рамках системи в єдиному екземплярі (див. Рис. 7.1, 7.2), або таких сегментів може бути багато (рис. 7.3), тобто обладнання СКУД може підключатися ні до єдиному ПК, а до будь-якого з ПК, об'єднаних, в свою чергу, в комп'ютерну мережу. Варіант, показаний на рис. 2, дозволяє будувати мережі будь-якого масштабу (при наявності компьютерної мережі між робочими станціями). Далеко не всі системи забезпечують підключення обладнання до будь-якого з ПК в мережі.

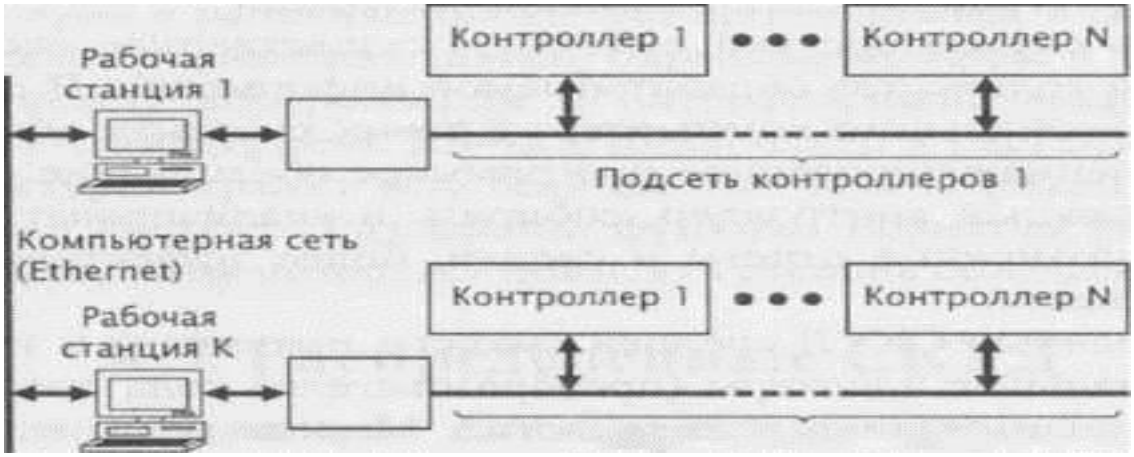

Рис. 7.3. Повна схема мережі СКУД

Мережеві (централізовані) СКУД знаходяться під безпосереднім і постійним управлінням центрального комп'ютера системи охорони об'єкта, обслуговуючого всі периферійні ланки КПП. База даних централізована. Застосування таких систем економічно виправдано, лише коли до центрального комп'ютера підключено досить велике число терміналів - від декількох десятків і більше. Перевага таких систем в тому, що вони на відміну від автономних дозволяють вести централізовану реєстрацію часу проходу службовців і здійснювати статистичну машинну обробку цих відомостей, а також оперативно вводити всі необхідні зміни до режиму доступу тих чи інших осіб або в цілому на об'єкт.

Мережеві СКУД здатні забезпечити високий рівень безпеки об'єкта. Для підвищення надійності функціонування системи може бути застосована паралельна обробка даних на двох ПЕОМ.

Число контролерів залежить від ємності системи та максимального числа зчитувачів, що обслуговуються одним контролером.

Зазвичай для збільшення ефективності роботи і зменшення вартості всієї системи безпеки об'єкта централізовані СКУД дозволяють здійснювати інтеграцію з датчиками сигналізації.

Особливість систем середньої місткості - істотне збільшення числа користувачів і кількості оброблюваної інформації. У зв'язку з цим використання персонального комп'ютера в таких системах обов'язково. Компьютер і його спеціалізоване програмне забезпечення дозволяють програмувати кожен контролер, збирати й аналізувати інформацію, складати всілякі звіти і зведення, більш ефективно відстежувати ситуацію на об'єкті.

Централізовані СКУД середньої місткості прив'язані до конкретної технології. Спеціальні адаптери (перетворювачі) коду дозволяють під’єлнати зчитувачі різних технологій. Багато виробників навіть заявляють про те, що їх система інтегрується з будь-яким зчитувачем. Але, як правило, або це твердження недостатньо обгрунтовано, або вимагає серйозних додаткових витрат на установку нових модулів.

Головна особливість таких СКУД в тому, що вони мають можливість конфігурації апаратури і управління процесом доступу з компьютерних терміналів (терміналу). Різні СКУД мають свої індивідуальні особливості і розрізняються по архітектурі, можливостям, масштабом (граничному числу зчитувачів/дверей), числу керуючих компьютерів, типу застосовуваних зчитувачів, ступеня стійкості до злому, ступеню стійкості до електромагнітних впливів.

Більшість мережевих СКУД зберігають багато корисних ознак автономних систем, основне з яких - робота без використання комп'ютера, що управляє. Це означає, що при виключенні комп'ютера, що управляє система фактично перетворюється в автономну. Контролери даних систем так само, як і автономні контролери, мають власний буфер пам'яті номерів карт користувачів і подій, що відбуваються в системі. Наявність в системі комп'ютера дозволяє службі безпеки оперативно втручатися в процес доступу і здійснювати управління системою в режимі реального часу. Найважливішим елементом

мережевихСКУД є програмне забезпечення (ПО). Воно відрізняється великою різноманітністю як за можливостями - від відносно простих програм для одного керуючого терміналу, що дозволяють додавати в базу даних нових користувачів і прибирати вибулих, до найскладніших програм з архітектурою клієнт-сервер.

У системах даного класу використовуються потужні центральні контролери, які здійснюють процес управління великим числом периферійних виконавчих пристроїв. Наприклад, один контролер AAN-100 компанії Apollo може керувати процесом доступу в 96 дверей. Як правило, контролери в таких системах є чисто електронними пристроями і не містять релейних виходів. У таких системах функції управління зовнішніми пристроями та охоронними шлейфами зазвичай виконують зовнішні інтерфейсні модулі і релейні блоки, що встановлюються, в свою чергу, недалеко від об'єктів управління (двері, охоронні шлейфи та ін.). Для обміну інформацією між контролером і інтерфейсними модулями найбільш часто використовується інтерфейс RS-485. Контролер в системах з централізованою архітектурою зберігає всю базу даних ідентифікаторів і подій, що сталися в системі. Поділ функції прийняття рішень і безпосереднього управління дозволяє підвищити ступінь безпеки СКУД.

3. Розгалужені СКУД.

Можливості контролерів найбільш повно розкриваються в розподілених СКУД.

РозгалуженіСКУД найбільш досконалі з точки зору організації процесу обробки інформації в системі, так як найкращим чином протистоять збійних і аварійних ситуацій, зокрема, при збоях в роботі центрального ПК, порушення цілісності провідної лінії, що зв'язує його з периферією і т. д.

Периферійні пункти оснащені локальними мережами на базі мікрокомпьютерів (контролерів), які виконують процедуру перевірки самостійно, а центральний комп'ютер включається в роботу лише для актуалізації локальних баз даних і статистичної та логічної обробки інформації.

Ще одна відмінна риса системи такого класу - можливість зв'язку вхідних і вихідних пристроїв різних контролерів системи. Наприклад, можна запрограмувати систему так, щоб спрацьовування датчика сигналізації біля входу в офіс, викликало блокування електрозамків, підключених до кількох контролерів, контролюючим прилеглі приміщення.

Крім того, програмне забезпечення великих систем дозволяє використовувати для управління відразу кілька комп'ютерів і здійснювати розподіл виконавчих функцій між ними. Наприклад, можна на комп'ютер адміністратора покласти обов'язки відстежувати місцезнаходження співробітників і використання ними робочого часу; оператору комп'ютера відділу кадрів зобов'язати поповнювати базу даних, друкувати пропуску; на прохідну встановити комп'ютер з програмами, що допомагають ідентифікувати особу, а на пост охорони - виводити тривожну графіку і т. д.

На рис. 7.4. показана схема розгалуженої мережі СКУД. Відмітнаособливість СКУД зрозподіленою архітектуроюполягає в тому,що база даних

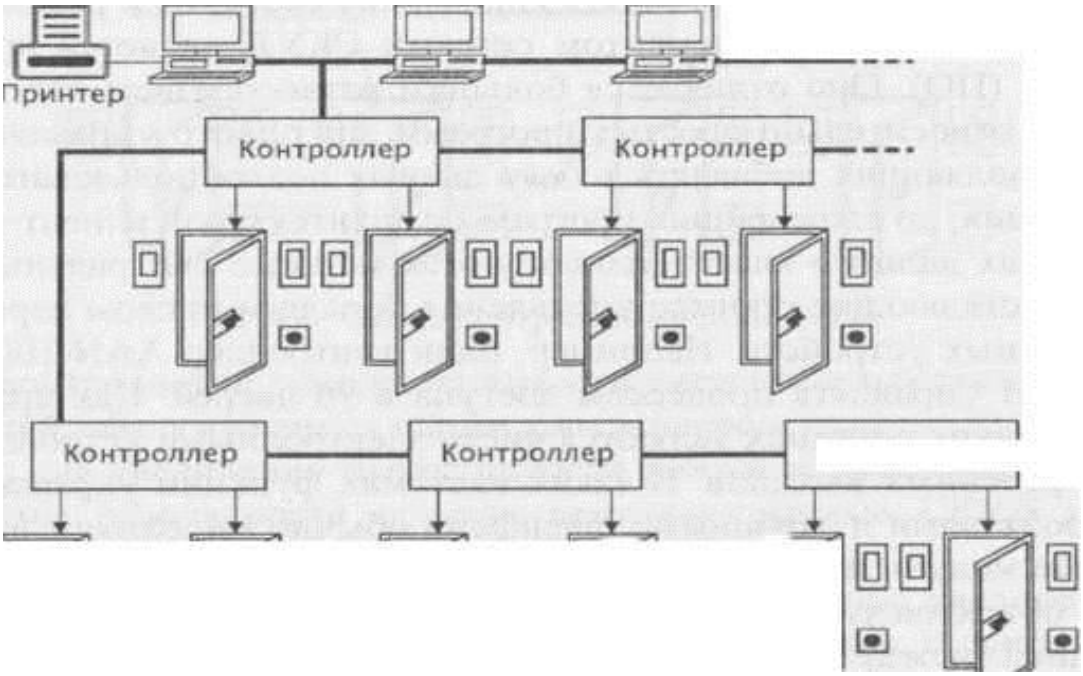

Рис. 7.4. Схема розгалуженої мережі СКУД

ідентифікаторів (і подій в системі) міститься не в одному, а в декількох контролерах, які, як правило, самі виконують функції управління зовнішніми пристроями і охоронними шлейфами через реле і входи охоронної сигналізації , розташовані безпосередньо на платі самого контролера.

Великі системи, як правило, працюють в найтіснішому взаємодії з іншими інженерними системами об'єкта: охоронною сигналізацією, з системами телевізійного спостереження і контролю, з системами життєзабезпечення, оперативного зв'язку та ін.

Через неможливість віддаленої установки від об'єкта управління дані контролери встановлюються безпосередньо всередині захищаються ними приміщень. Це не сприяє зниженню ймовірності несанкціонірованного маніпулювання контролером, але має свої плюси - при обриві лінії зв'язку між контролерами і комп'ютером система продовжує виконувати основні функції з управління процесом доступу в автономному режимі. Найбільш часто в системах з розподіленою архітектурою контролер може управляти проходом в 1-2 двері.

Розподілені системи мають також ту перевагу, що завдяки своїй модульній конструкції дозволяють нарощувати потужність СКУД поступово, переходячи від локальних пунктів до розподіленої мережі; простіше виконується модернізація обладнання; аварія на окремому КПП не впливає на роботу всієї мережі; для обробки перевірених осіб потрібно менше часу.

З систем з централізованою архітектурою зазвичай виходять системи зі змішаною логікою шляхом додавання спеціалізованих зчитувачів або

інтерфейсних модулів з власним буфером пам'яті ідентифікаторів і подій. Завдяки використанню такого технічного рішення досягається надмірне резервування функцій, різко підвищує ступінь безпеки системи. Оскільки контролер в СКУД з централізованою архітектурою керує найбільшою кількістю дверей, пошкодження лінії зв'язку між ним і інтерфейсними модулями управління кінцевими пристроями може привести до блокування значної частини або всієї системи. Локальний зчитувач з власною базою даних в цьому випадку переходить в автономний режим управління доступом на своїй ділянці. Системи, побудовані з використанням даних модулів, мають найвищим ступенем безпеки.

4. Контролери СКУД iSecure Pro.

Реалізацію контролера розглянемо на прикладі контролерів iSecure Simplex СКУД iSecure Pro компанії SimplexGrinnell, які являють собою самостійні мікропроцесорні системи з розподіленою обробкою даних. Вони призначені для управління пристроями контролю доступу та охоронної сигналізації, такими, як зчитувачі, клавіатури, дверні магнітоконтактні датчики, кнопки виходу, дверні замки, сирени та інші, а також для забезпечення взаємозв'язку системи контролю доступу з системами і базами даних різних підрозділів компанії. При втраті зв'язку з керуючим комп'ютером вбудована в контролер програма дозволяє йому функціонувати самостійно до відновлення зв'язку.

Всі контролери системи контролю доступу iSecure інтегруються з апаратно-програмною платформою комплексної системи безпеки iSecure PRO Simplex і забезпечують стандартну організацію мереж Ethernet, TCP / IP, LAN / WAN і інтеграцію з діючими в компанії інформаційними системами. Для ефективного управління ресурсами контролери iSecure мають розподілений рівень інтелекту, а для зниження експлуатаційних витрат - вбудовану функцію самодіагностики.

Основні характеристики контролерів iSecure Simplex:

- iSecure має модульну, конфігуровані і легко расширяемую схему;
- розподілена інтелектуальна архітектура контролера дозволяє виконувати безперервну самодіагностику і реєстрацію збоїв, забезпечуючи його надійне функціонування і звільняючи головний вузол від рутинних операцій;
- спеціальний пакет засобів графічної діагностики представляє оператору інформацію на трьох рівнях: загальний вигляд всієї мережі, внутрішня конфігурація і статус кожного контролера системи контролю доступу, а також статус всіх пристроїв доступу і модулів контролера4
- кожен контролер iSecure Simplex може мати індивідуальну конфігурацію в мережі, яка дозволяє об'єднувати сотні контролерів, що підтримують тисячі зчитувачів магнітних карт, охоронних датчиків, дверей доступу і інших пристроїв;

- знімні модулі конфігурації контролера замінюються безпосередньо на об'єкті, що прискорює процес їх обслуговування і скорочує експлуатаційні витрати;
- через інтерфейсні плати контролери підтримують різні віди зв'язку.

Використовуючи Ethernet TCP / IP, можна значно скоротити витрати на монтаж і обслуговування системи, з'єднавши контролери через вже існуючі локальні або глобальні мережі. У контролерах віддалених об'єктів використовується плата модемного зв'язку:

- контролери сумісні з широким спектром обладнання систем безпеки компанії Simplex, включаючи систему нового покоління iSecure Pro Simplex, а також з обладнанням інших виробників;
- при застосуванні відмовостійкої архітектури мережі iSecure Path з автоматичною реконфігурацією й потоків даних контролери забезпечують максимальну живучість усієї системи безпеки в разі пошкодження ліній зв'язку.

Всі контролери iSecure Simplex мають російські сертифікати. Схема підключення контролера в систему контролю доступу iSecure PRO Simplex показана на рис. 7.5.

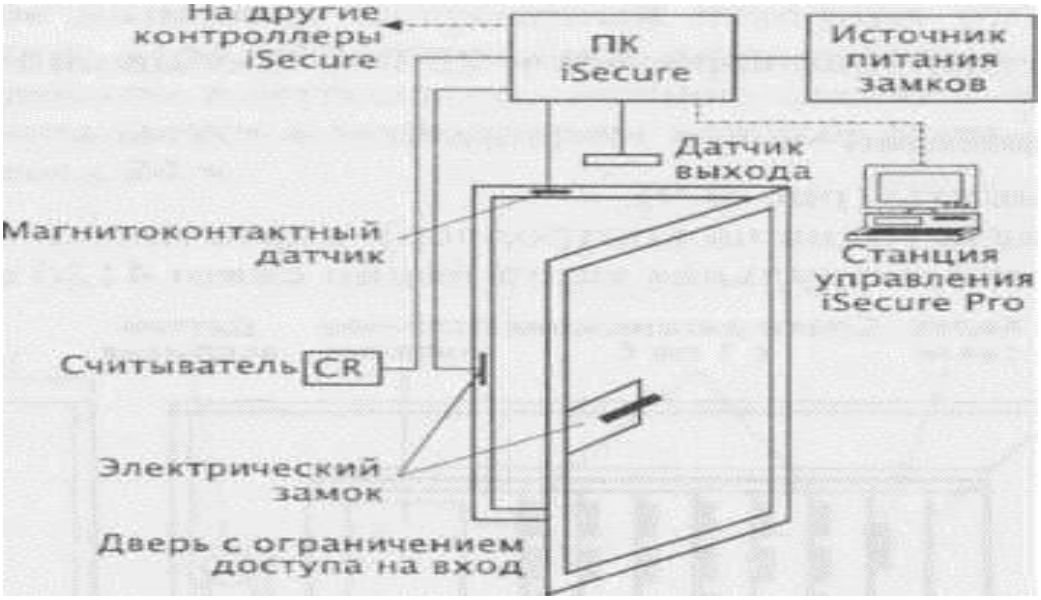

Рис. 7.5. Схема підключення контролера в систему контролю доступу iSecure PRO Simplex

Конструктивні і технічні характеристики контролерів iSecure системи контролю доступу Simplex розглянуті нижче.

1 Внутрішня архітектура. На материнській платі контролера розташовані: слот ЦПУ для карти ЦПУ з 32-розрядних вбудованим процесром Intel, слот карти зв'язку для провідний мережевий карти 4120, або модульної мережевої карти 4120, шість) слотів розширення для модулів входів / виходів і модулів підключення зчитувачів, а також джерело живлення з вузлом зарядки батарей.

Контролер має компактні розміри, що дозволяють встановлювати його в невеликих приміщеннях. Датчик розтину кришки корпусу забезпечує захист від несанкціонованого доступу до вузлів контролера.

Технічні характеристики контролера:

- вбудований 32-розрядний процесор компанії 1Me1;
- внутрішня самодіагностика і вбудований індикатор стану;
- підтримує клавіатури і зчитувачі проксиміті-карт, магнітних карт, Виганда-карт, біометричних даних, радіочастотних приймачів і карт зі штрих-кодом;
- можливість програмування формату карти.

Робочі можливості з підтримки:

- до 8 форматів карток на контролер;
- до 96 контрольованих входів;
- до 48 релейних виходів;
- до 5000 власників карток і 3000 повідомлень (стандартна конфігурація);
- до 50000 власників карток і 25000 повідомлень (розширювана конфігурація);
- до 12 зчитувачів.

Використовуються наступні модулі розширення: модуль для підключення 2 зчитувачів, модуль з 16 контрольованими входами, модуль з 8 релейними виходами, модуль з 8 контрольованими входами/8 релейними виходами, модуль з 8 контрольованими входами. всі входи можуть бути сконфігуровані для моніторингу як двох, так і чотирьох станів.

Лекція № 8

Тема лекції: Виконавчі пристрої СКУД

План лекції:

1. Електричні замки.
2. Турнікети.

1. Електричні замки.

Для того щоб пройти через вхід, контрольований СКУД, система на підставі обмежень, заданих для власника ідентифікатора, приймає рішення про приведення у дію виконавчих механізмів і пристроїв, безпосередньо регулюють доступ. В даний час існують різні способи захисту входу в приміщення, що охороняється: прості і укріплені двері, хвіртки з електромагнітними і електромеханічними замками або засувками, трьохштангові турнікети (триподи), напівростові та повноростові турнікети, автоматизовані прохідні, шлюзові кабіни (тамбур шлюзи), ворота, шлагбауми та інші. Всі пристрої, перераховані вище, можуть використовуватися як автономно, так і в складі СКУД.

У СКУД передбачаються заходи щодо забезпечення стійкості до розтину зловмисниками замків і запірних механізмів, за запобігання-обертанню спостереження за введенням ідентифікаційних ознак та копіювання еталонних ознак ідентифікаторів.

Так як перегороджуючі пристрої можуть піддаватися руйнуючим і неруйнуючим впливам зловмисників, то їх по механічній стійкості стандарт класифікує наступним чином:

- підвищена стійкість до злому шляхом нанесення ударів і застосуванні інструментів;
- висока стійкість, яка характеризується кулє- та вибухостійкістю суцільного перекриття прохідного отвору.

Електричні замки і засувки

Електричні замки рекомендується використовувати в якості основного замикаючого пристрою в денний час. Ці замки на відміну від механічних відкриваються дистанційно по електричному сигналу і використовуються спільно з домофонами, кодовими панелями, зчитувачами карток різних типів. Електрозамки діляться на два класи: електромагнітні та електромеханічні.

Електромагнітні замки представляють собою корпус з електромагнітом і відповідну металеву пластину. Пластина кріпиться на дверному полотні, а сам замок - на одвірку. Електромагнітний замок утримує двері в закритому стані за рахунок зусилля потужного електромагніту. При знеструмленні замку двері залишаються відкритими, тому для забезпечення роботи в умовах відключення напруги живлення необхідно застосовувати блоки гарантованого живлення.

Електромеханічний замокмає механічний ригель (засув), утримуючий двері в закритому стані, а управління цим ригелем здійснюється відносно

малопотужним соленоїдом. При закритті дверей підводящий ригель замку зводить наявну в замку пружину, при цьому робочий ригель входить у відповідну частину замку і утримує двері в закритому стані. При подачі напруги соленоїд відпускає фіксатор пружини, і робочий ригель під дією пружини втягується в замок - двері можуть бути відкриті. Після того як двері буде відкрита, а потім закрита, вона знову опиниться в замкненому стані. Передбачається режим, виключаючий автоматичне замикання замків і випадкове закривання дверей.

У соленоїдних електрозамках ригель приводиться в рух зусиллям електромагніта. Обладнана таким замком двері можуть бути відкриті тільки в період дії керуючого сигналу. Після зняття цього сигналу зачинені двері залишиться замкненою незалежно від того, відкривалася чи вона. Існують також інші різновиди електромеханічних замків: електромоторні (ригель приводиться в рух електромотором з редуктором), з ручним приводом ригеля (ригель приводиться в рух поворотом ручки, а електромагніт розблокує механізм приводу). Електромеханічні замки можуть бути накладного і врізного типу.

Електрозащілки представляють собою відповідну частину замку і використовуються спільно зі звичайним механічним замком. При подачі напруги розблокується фіксатор електрозащілки, і двері можуть бути відкриті при висунутому положенні ригеля механічного замка. При цьому використовується механічний замок не повинен відкриватися зовні поворотом ручки. При наявності ручки з внутрішньої сторони дверей вона може бути відкрита зсередини поворотом ручки без подачі напруги, що управляє на засувку. Спеціальні моделі соленоїдних замків і електрозащілок призначені для обладнання аварійних виходів. Такі замки відкриваються при відключення напруги живлення.

При виборі моделі замку необхідно враховувати, які приміщення і для яких цілей передбачається обладнати замком. При цьому необхідно врахувати: масу, конструкцію, матеріал двері, необхідну інтенсивність користування, різні функціональні особливості системи, що включає замок. Все це визначає надійність і довговічність роботи електрозамку.

Довідникидверей (закриватели) служать для примусового закривання дверей і забезпечують надійну роботу електрозамків. Регулюючі клапани дозволяють вибрати необхідну швидкість закривання дверей. Для дверей різного розміру можна підібрати відповідний довідник. Моделі також відрізняються конструктивним виконанням, дизайном, рядом додаткових функцій: фіксація двері в положенні «відкрито», прискорення в завершальній фазі закривання - «грюкіт» і ін.

2. Турнікети.

Відповідно до ГОСТ Р 51241-98 все турнікети відносяться до розділу «Пристрої перегороджують керовані (УПУ)» і класифікуються за такими двома ознаками:

- вид перекриття отвору;
- спосіб управління УПУ.

По виду перекриття отвору розрізняють наступні види турнікетів:

- з частковим перекриттям отвору;
- з повним перекриттям отвору;
- з блокуванням об'єкта в отворі (шлюзи, кабіни прохідні).

За способом управління УПУ ділять на пристрої:

- з ручним керуванням;
- з напівавтоматичним керуванням;
- з автоматичним управлінням.

А. Гінце пропонує більш спрощену порівняно з ГОСТ Р 51241-98 класифікацію. В основу такої класифікації покладено принцип функціональності. Відповідно до цієї ознаки всі турнікети можна розділити на УПУ, здійснюють повне або неповне перекриття отвору, а також «нормально закриті» або аномально відкриті ».

Принцип роботи турнікета СКУД простий: якщо запит на доступ правомірний, то механічна система, повертаючись, відкриває прохід на територію, що охороняється.

До основних видів турнікетів відносяться:

- хвіртки;
- триподи;
- роторні поясні турнікети;
- турнікети з висувними стулками;
- турнікети з відкидними стулками на електроприводи;
- роторні повнопрофільні або повнозростові турнікети.

Нормально відкриті турнікети мають більш високу пропускну здатність, але не виключають можливість проходу декількох притиснувшихся один до одного людина.

Найбільш поширені трилопатеві турнікети з обертовим в одному напрямку перепиняють пристроєм - триподи і роторні Вони забезпечують гарантований одноразовий прохід однієї людини. Перегороджуючий пристрій трипода виконано у вигляді обертового блоку з трьома циліндричними брусами (штангами), розташованими під кутом 120 °. Обертаємий блок кріпиться збоку зони проходу. При обертанні кожен з брусів фіксується в горизонтальному положенні, перегороджуючи шлях людині. Роторні турнікети бувають висотою до пояса людини (поясні) і в повний зріст (повнозростові). Турнікети забезпечують повне перекриття зони проходу, а через загороджувальний бар'єр поясного турнікета можна перелізти або перестрибнути, тому він розміщується на посту охорони і управляється натисненням на його педаль ногою вахтера.

Турнікети забезпечують високу пропускну здатність - до 60 осіб в 1 хв., Вони дешевше шлюзових кабін, але їх конструкція не заважає порушнику застосувати проти співробітників охорони зброю. Крім того, розміри простору між загороджувальними бар'єрами встановлюються виходячи з розмірів людини середньої комплекції, що створює незручності для товстунів і при проносах великогабаритних носяться речей. Для підвищення ефективності

захисту турнікети оснащуються датчиками, які спрацьовують при нерегламентованій поведінці людини, наприклад, спробі перестрибнути через загороджуючий бар'єр.

Електромеханічні турнікети є традиційними виконавчими механізмами систем контролю доступу. Вони застосовуються для облаштування входів в приміщення або обмеження входу в окремі частини приміщень, а деякі моделі - для обмеження входу на територію. На відміну від двері, обладнаної електрозамком, турнікет є виконавчими пристроєм, що забезпечує прохід людей «по одному». Для управління електромеханічними турнікетами можуть використовуватися пульти ручного управління, а також будь-які пристрої контролю доступу: зчитувачі карток різного типу, електронні ключі, радіобрелки, клавіатури, приймачі жетонів і т. д. Це дозволяє включати турнікети до складу мережевих комп'ютеризованих систем контролю доступу.

Різноманітність областей застосування турнікетів обумовлює різноманітність їх типів: від мініатюрних турнікетів, що встановлюються в автобусах, до повнопрофільних моделей високого ступеня секретності для обладнання входів на територію, що охороняється і швидкісних моделей з дуже високою пропускною здатністю для станцій громадського транспорту. Найбільш популярні моделі турнікетів: турнікети-триподи, турнікети-«вертушки »(роторні), турнікети-хвіртки.

Турнікети-триподи з трьома перепиняють планками - оптимальний вибір, якщо необхідно обладнати прохідну підприємства, банку, адміністративної установи або організації та здійснювати контроль з метою запобіганню сторонніх осіб на підприємство (рис. 8.1).

Вони поділяють потік людей по одному, забезпечуючи при цьому високу пропускну здатність. У режимі однократного проходу через турнікет в дозволеному напрямку може пройти одна людина, після чого турнікет автоматично повертається в закрите положення. При необхідності пропуску групи осіб встановлюється режим багаторазового проходу в потрібному напрямку, можливий режим вільного проходу. Напрямок прохода висвічується на табло. У разі екстрених ситуацій можливе механічне розблокування планок за допомогою ключа або їх демонтаж. При відключенні від джерела турнікет переходить на роботу від акумулятора.

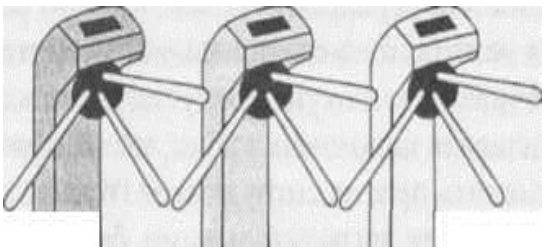

Рис.8.1. Турнікети-триподи стрьома перегороджуючими планками

Турнікети й хвіртки - найбільш популярний вид турнікета. Це обумовлено їх невисокою вартістю і компактністю. Триподи мають сучасний елегантний зовнішній вигляд, легко монтуються.

Ступінь захисту цих турнікетів відносно невисока в порівнянні з більш складними моделями, так як через перегороджують планку можна перелізти або проповзти під нею. Однак такий турнікет встановлюється, як правило, в місцях постійної присутності співробітника охорони. Крім того, підвищити безпеку можна установкою інфрачервоних датчиків, які спрацьовують при спробах перелізти через турнікет або проникнути під перегороджуючою планкою. В цьому випадку спрацьовування датчика викличе сигнал тривоги, який може бути поданий на сирену, в приміщення охорони або включити відеозапис дій зловмисника.

Роторні турнікети, або так звані «вертушки», призначені для регулювання входу / виходу на прохідних підприємств, військових і спеціальних об'єктів, де необхідно повне або майже повне перекриття зони проходу.

Вони можуть бути різними за висотою: від поясних до турнікетів на повний зріст. Ступінь захисту вельми висока.

Установка двох роторних турнікетів один за іншим дозволяє організувати шлюз-тамбур. Це зручно при необхідності жорсткого контролю доступа, наприклад, на митниці.

Роторні турнікети можуть працювати в автономному режимі з управлінням від пульта охоронця, а також у складі СКУД. У режимі однократного проходу через турнікет в дозволеному напрямку людина штовхає планки у дозволеному напрямку, після чого відбувається автоматичний доворот «вертушки» у вихідне закрите положення. При не-обходимо пропуску групи осіб встановлюється режим багаторазового проходу в потрібному напрямку, можливий режим вільного проходу. У разі екстрених ситуацій можлива механічне розблокування лопатей за допомогою ключа. При відключений від джерела турнікет переходить на роботу від акумулятора.

Турнікети-хвіртки широко використовуються в магазинах, аеропортах, вокзалах для організації вільного проходу в одну сторону і заборони проходу в іншу сторону, а також в банках, установах, на підприємствах для організації вільного виходу.

Хвіртки можна використовувати в системах контролю доступу, але для більш повного захисту необхідно підключати до хвіртки датчики проходу і організувати додатковий контроль. Ці турнікети не поділяють потік людей по одному і після відкриття хвіртки через неї можуть пройти кілька людей.

Автоматична електромеханічна хвіртка з приводом автоматично відчиняється по команді з пульта охорони або при спрацьовуванні ІЧ датчика. Створку при необхідності можна притримати або штовхнути швидше. Електромеханічна хвіртка без приводу управляється від пульта, але при проході створка відводиться рукою. При відключенні від джерела хвіртка працює від акумулятора.

Механічна хвіртка не має дистанційного керування і просто механічно забезпечує вільний прохід в одну сторону і заборона проходу в іншу сторону.

Після проходу людини створка хвіртки будь-якої моделі автоматично повертається у вихідне положення і блокується. В екстрених випадках хвірткуможна відкрити звичайним ключем, а створку повернути рукою, звільнивши прохід.

Огородження призначені для формування потоків людей, обмеження зон проходу.

При обладнанні прохідних турнікетами різного типу часто оказується, що зона проходу перекрита в повному обсязі і є необхідність в огородженні. Огородження можна виконати в єдиному дизайні з турнікетами. Як заповнень можна використовувати тоновані або дзеркальні скла з нанесенням логотипу замовника. Огородження легко монтуються і можуть бути будь-якій висоти і форми.

Турнікети поясні залишають можливість для перепригування, оскільки, як випливає з їх назви, загороджувальний бар'єр доходить тільки до пояса людини. При їх використанні практично неможливо забезпечити захист від перекидання предметів, тому такі турнікети обов'язково повинні бути встановлені в зоні видимості охорони.

Турнікети повнозростові встановлюють у віддалених від поста охорони місцях і використовують в повністю автоматичному режимі роботи.

Турнікети роторні використовуються на режимних підприємствах, таких, як атомні станції, військові об'єкти, аеропорти, а також в банках, на стадіонах, складських комплексах, в офісах. Вони являють собою металоконструкцію зі сталевої рами, що обертається центральної колони зі штангами і додаткової системи огорож. Існує кілька модифікацій повноростових турнікетів, що відрізняються як конструктивно, так і функціонально. Наприклад, існують турнікети з одним або двома проходами, з двома, трьома або чотирма перегороджуючими лопатями, з прямими або закругленими штангами, зроблені цілком з полірованої нержавійки, анодовані або фарбовані. Є моделі з додатковою дахом, що мають освітлення і дренаж, моделі зі скляними бічними панелями і перегороджуючими елементами, виконаними з міцного пластику. Існують також моделі турнікетів з інтегрованими дверима. Інтегрована двері можуть бути дуже корисні, наприклад якщо потрібно провезти через турнікет візок або організувати евакуацію персоналу. Крім того, існують спеціальні конструкції, які мають 2 проходу для персоналу та інтегровану двостулкові двері між ними, що дозволяє при необхідності навіть проїжджати через подібний пристрій на автокарах і автомобілях.

Для організації максимально захищених проходів в офісах, банках і на аналогічних об'єктах з підвищеними вимогами до зовнішнього вигляду прохідних кращі більш естетичні повноростові турнікети, виконані зі скла. Подібні пристрої з кулестійким склом, обладнані зчитувачами, датчиками контролю положення людини і навіть ваговій системою, обмежують доступ на об'єкт, поділяють людський потік і при цьому мають всі достоїнства звичайних дверей - захищають фойє від холоду, а також дозволяють створити необхідний дизайн інтер'єру та фасаду будівлі .

За типом приводу турнікети поділяють на механічні, електромеханічні і турнікети з серводвигуном. Механічні турнікети, як правило, встановлюються на виході з об'єкта і дозволяють безперешкодно виходити, але не допускають проникнення на територію, що охороняється (забезпечують односторонній прохід). Електромеханічні турнікети і турнікети з серводвигуном можуть працювати в складі СКУД і управлятися зовнішніми контролерами інших систем.

Принцип дії всіх турнікетів приблизно однаковий. Якщо картка користувача дійсна, турнікет розблокується. Турнікет провертається вручну (якщо немає вбудованого двигуна), і користувач, пройшовши між стулок, виявляється на території, що охороняється. Одночасно можна пройти тільки одній людині і тільки в одному напрямку. У режимі шлюзування турнікет може бути зупинений в проміжній позиції, блокуючи переміщення користувача з метою запросити додаткове підтвердження особи - введення ПІН-коду, пред'явлення біометричних ідентифікаторів (відбитка пальця, геометрії руки і т. д.). Існують моделі з інтегрованою ваговою платформою, де вага користувача, що пред'явив картку і увійшов в контрольований сегмент, порівнюється з даними з бази даних.

Для того щоб турнікет міг працювати в вуличних умовах необхідно забезпечити волого і пилозахищеність системи, а також стійкість до впливу низьких температур.

Кабіни з обертовими дверима ROTANT є повноростовими електромеханічними турнікетами, лопаті і стіни яких виготовляються з бронескла (кулестійкого або стійкого до пробивання). Обертові двері можуть мати 3-4 лопаті, або 2 сектори. На відміну від звичайних повноростових турнікетів в кабіни з обертовими дверима вбудовуються металодетектори. При виявленні зброї у проходить людини ротор такої кабіни переходить в реверсний режим обертання, змушуючи порушника вийти назад з кабіни. Однак при подібному алгоритмі роботи знижується пропускна здатність шлюзу і ускладнюється вихід людей з приміщення, що охороняється. Ця проблема вирішується установкою додаткових напівкруглих розсувних дверей на виході з кабіни. Таке рішення застосовується, наприклад, в кабінах ROTOCOM виробництва фірми SAIMA і PRIORA TONDA фірми TONALI.

При спрацьовуванні металодетектора напрямок обертання ротора цих кабін не змінюється. Замість цього прохід порушника в приміщення, що охороняється блокується за допомогою додаткових дверей, що закриваються тільки перед порушником. Вихід з приміщення при цьому залишається відкритим і пропускна здатність кабіни не знижується. Додаткові розсувні двері можуть встановлюватися як з однієї, так і з двох сторін кабіни. При цьому описаний алгоритм роботи діє як при вході, так і при виході з приміщення, що охороняється.

Кабіни з обертовими дверима, як і тамбур-шлюзи, можуть працювати в ручному і автоматичному режимах, інтегруються з СКУД. Основною перевагою кабін з обертовими дверима є їх дуже висока пропускна здатність. До недоліків цих кабін, в першу чергу, відноситься їх велика вартість.

Області використання шлюзових кабін різних типів визначаються вимогами до пропускної спроможності та обмеженнями за вартістю. Кабіни з дверима, що обертаються, мають найбільшу пропускну здатність і водночас найвищу вартість. Напівавтоматичні тамбури, навпаки, відрізняються низькою вартістю та невисокою пропускною здатністю. Автоматичні шлюзи мають середні значення вартості, пропускної спроможності і дозволяють найбільш надійно контролювати доступ на об'єкт, що охороняється.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Юдін О. К. Інформаційна безпека держави / О. К. Юдін. — К.: Консум. — 2005. — 576 с.
2. Pankanti Sh., Bolle R.M., Jain A. Biometrics The future of identification. London, 2010. 167 с.
3. Електронний ресурс. – Режим доступу:https://deps.ua/ua/knowegable-base/reference-information/7824.html
4. Електронний ресурс: https://www.zkteco.com/en/
5. https://books.google.com.ua/books?id=XPC9ucFbddsC&pg=PA1&hl=ru&source=gbs_toc_r&cad=1#v=onepage&q&f=false