Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Навчально-науковий центр заочної форми навчання*

Кафедра *Комп'ютерної інженерії та систем технічного захисту інформації*

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти *другий (магістерський)*

«Дослідження особливостей використання охоронних СКУД»

Виконав:
студент *2* курсу, групи *СТЗІАмз-18-1*
Роговий М.І.

Спеціальність *125 «Кібербезпека»*
Тип програми *освітньо-професійна*
Освітня програма *«Системи технічного захисту інформації, автоматизація її обробки»*

Керівник *проф. Милютченко І.О.*

Допускається до захисту
Зав. кафедри _____ *проф. Антіпов І.Є.*
(підпис)

2019 р.

Харківський національний університет радіоелектроніки

Факультет *Навчально-науковий центр заочної форми навчання*

Кафедра *Комп'ютерної інженерії та систем технічного захисту інформації*

Рівень вищої освіти *другий (магістерський)*

Спеціальність *125 «Кібербезпека»*

Тип програми *освітньо-професійна*

Освітня програма *«Системи технічного захисту інформації, автоматизація її обробки»*

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«___» _____ 20 ____ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові *Роговому Максиму Івановичу*
(прізвище, ім'я, по батькові)

1. Тема роботи «Дослідження особливостей використання охоронних СКУД»

затверджена наказом по університету від « 11 » 10 2019 р. № 199 Стз

2. Термін подання студентом роботи до екзаменаційної комісії *10 грудня 2019 р.*

3. Вихідні дані до роботи *Дослідити особливості використання сучасних СКУД для приватного бізнесу. Для досягнення поставленої мети необхідно розв'язати наступні задачі: 1) провести аналіз засобів ідентифікації; 2) провести аналіз біометричних систем аутентифікації; 3) провести аналіз контролерів та виконавчих пристроїв СКУД; 4) скласти перелік рекомендацій для розгортання СКУД на обраному прикладі.*

4. Перелік питань, що потрібно опрацювати в роботі
1. Огляд та аналіз сучасних методів та засобів СКУД
2. Огляд та аналіз сучасних пристроїв контролю доступу
3.Огляд та аналіз сучасних виконавчих пристроїв
3. Аналіз недоліків різних СКУД
4. Написання рекомендацій к розгортанню СКУД на підприємстві
5.. Висновки

5. Перелік графічного матеріалу із зазначенням креслень, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

1.Задачі СКУД на підприємстві

2.Схема работы СКУД

3.Класифікація ідентифікаторів доступу СКУД

4.Електронні радіочастотні(RFID)

5.Біометрична ідентифікація

6.Виконавчі пристрої

7.Основні етапи побудови СКУД з точки зору організаційних заходів

8.Розробка регламенту пропускного режиму в компанії

9.Процес вибору підрядника

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Аналіз сучасних методів та засобів СКУД. Визначення та основні можливості.*	*02.09.19 – 20.09.19*	
2	*Аналіз технологій контролю управління доступом*	*21.09.19 – 10.10.19*	
3	*Аналіз виконавчих пристроїв*	*11.10.19 – 10.11.19*	
4	*Розробка рекомендацій щодо впровадження СКУД підприємстві*	*11.11.19 – 30.11.19*	
5	*Перевірка роботи на антиплагіат*	*01.12.19 – 05.12.19*	
6	*Представлення атестаційної роботи на кафедрі*	*10.12.2019*	

Дата видачі завдання *02 вересня 2019 р.*

Студент _____
(підпис)

Керівник роботи _____ проф. Милютченко І.О.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до атестаційної роботи: 74 с., 21 рис., 2 табл.,1 додаток, 15 джерел.

СИСТЕМА КОНТРОЛЯ ВІДДАЛЕНОГО ДОСТУПУ, RFID, РЕЖИМНА ЗОНА, ДОСТУП ДО ПРИМІЩЕННЯ, ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ, ЗАХИСТ ПРИМІЩЕННЯ, СКУД, БІОМЕТРІЯ.

Мета роботи – зробити аналіз сучасних СКУД. Описати етапи впровадження СКУД на підприємстві. Сформувати список рекомендацій, які дозволять заощадити часові та фінансові ресурси.

Галузь використання – служби охорони безпеки підприємств, бізнес від малого до великого.

У результаті виконання атестаційної роботи було проведено аналіз сучасних СКУД, виявлені слабкі сторони. Також були сформульовані рекомендації, які треба врахувати при впровадженні СКУД на підприємстві.

ABSTRACT

Master thesis: 75p., 2 tables, 21fig., 15 sources, 1 add.

RFID, SECURITY ACCESS CONTROL SYSTEMS, MODE ZONE, ACCOMMODATION ACCESS, PROTECTION AGAINST UNAUTHORIZED ACCESS, PROTECTION OF THE ROOM, BIOMETRY

The purpose of the work is to make an analysis of modern access control systems. Describe the stages of implementation of the access control systems (ACS) at the enterprise. Create a list of recommendations that will save time and financial resources.

The area of use is enterprise security services, business from small to large.

As a result of performance of the appraisal work, the analysis of modern ACS was conducted, weaknesses were identified. Recommendations have also been formulated that should be taken into account when implementing the ACS at the enterprise.

ЗМІСТ

Перелік скорочень та термінів ……...7
Вступ.……8
1 СИСТЕМА КОНТРОЛЮ І УПРАВЛІННЯМ ДОСТУПУ……9
1.1. Визначення та основні можливості СКУД …..……..9
1.2. Загальні принципи роботи СКУД…….....13
2 АНАЛІЗ ТЕХНОЛОГІЙ КОНТРОЛЯ УПРАВЛІННЯ ДОСТУПОМ…….23
2.1. Оптичні ідентифікатори СКУД …….....25
2.2. Електронні контактні ідентифікатори СКУД …….25
2.3. Електронні радіочастотні ідентифікатори СКУД……...25
2.4. Біометричні ідентифікатори……..33
2.4.1. Відбитки пальців…….34
2.4.2. Райдужна оболонка ока…….....36
2.4.3. Розпізнавання за обличчям…….37
2.4.4. Розпізнавання за венами руки……..40
2.4.5. Сітківка ока……..40
2.5. Проблеми ідентифікації відвідувачів…….....41
2.6. Виконавчі пристрої……45
3 ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ СКУД НА ФІРМІ «ELTA» …….50
Висновки ……57
Перелік джерел посилання …….....58
Додаток А. Комплект графічних матеріалів …….....60

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АРМ	Автоматизоване робоче місце
АС	Автоматизована система
БД	База даних
ІД	Ідентифікатор доступу
КУД	Контроль і управлення доступом
ПЗ	Програмне забезпечення
СЗІ	Система захисту інформації
СКУД	Система контролю і управленням доступу
ВП	Виконуючий пристрій
ППК	Пристрій перегороджуючий керований
ПП	Перегороджуючий пристрій
НС	Надзвичайна ситуація
СКД	Система контролю доступу
ТЗ	Технічне завдання
ПК	Персональний комп'ютер

ВСТУП

Безпека і захист інформаційних ресурсів, матеріальних цінностей і комерційної таємниці, дисципліна співробітників - необхідні умови нормального існування і успішного розвитку будь-якого підприємства. В даний час одним з найбільш ефективних і сучасних підходів до вирішення завдання комплексної безпеки об'єктів різних форм власності, є використання систем контролю і управління доступом (СКУД). Правильне використання СКУД дозволяє закрити несанкціонований доступ на територію, в будівлю, окремі поверхи і приміщення. У той же час вони не створюють перешкод для проходу персоналу і відвідувачів в дозволені для них зони. Економічний ефект від впровадження СКУД може оцінюватися як зниження витрат на утримання персоналу охорони за вирахуванням вартості апаратури віднесеної на термін її експлуатації і витрат з обслуговування. Непрямий (оперативний) ефект полягає в підвищенні надійності пропускного режиму, ускладненні для зловмисників проникнення на об'єкт. При складанні опису об'єкта, визначенні його характеристик і розробці основних вимог необхідно враховувати два принципово важливі моменти: з якою метою впроваджується система контролю доступу і який очікується ефект від її впровадження. Вибір правильної СКУД, яка враховує і інтегрує обладнання різних виробників, різних поколінь, стане оптимальним вирішенням питання щодо забезпечення контролю доступу.

Метою виконання роботи є детальний аналіз існуючих СКУД. Визначити основні вимоги, яким вони повинні підпорядкуватись. Визначити необхідний перелік питань, які обов’язково повинні бути враховані на підприємстві під час розгортання таких систем.

1.СИСТЕМА КОНТРОЛЮ І УПРАВЛІННЯМ ДОСТУПУ

1.1 Визначення та основні можливості СКУД

СКУД – це сукупність засобів контролю та управління доступом, що володіють технічною, інформаційною, програмною та експлуатаційною сумісністю. Але таке визначення є дуже загальним та на дає можливості зрозуміти повністю суть цього поняття.

Якщо розібратися більш детально, СКУД – є сукупністю сумісних між собою апаратних і програмних засобів, спрямованих на обмеження і реєстрацію доступу людей, транспорту і інших об'єктів в, або з приміщення, будівлі, зони і території тощо.

У більшості випадків СКУД складеться з:

- перегороджуючого пристрою (ПП), який керується дистанційно. Наприклад, двері,турнікети, ворота, тощо;
- зчитувальні пристрої, «зчитувачі». Наприклад, пристрої радіочастотної ідентифікації, біометричні сканери;
- контролери СКУД. Електронні модулі, які керують роботою СКУД, реалізують аутентифікацію об'єктів доступу, керують логікою авторизації для доступу в приміщення, керує замками, пристроями загородження тощо;
- програмне забезпечення СКУД. Необов'язковий елемент, що дозволяє здійснювати централізоване управління контролерами СКУД з персонального комп'ютера (ПК);
- додаткове обладнання, блоки живлення, кнопки, тощо.

Одним з найважливіших понять для розуміння працездатності СКУД є ідентифікатор доступу, або ідентифікатор (так званий носій ідентифікаційної ознаки): унікальна ознака суб'єкта або об'єкта доступу. В якості ідентифікатора може використовуватися код, який треба ввести на терміналі, біометрична ознака або речовинний код (рис. 1.1). Ідентифікатор, який використовує речовинний код - це предмет, в який (на який) за допомогою спеціальної

технології занесена ідентифікаційна ознака у вигляді кодової інформації (карти, електронні ключі, брелоки та ін. пристрої) [2].

В умовах індивідуальних особливостей економічних суб'єктів розглядати можливості СКУД необхідно диференціюючи потреби кожного. Всім СКУД притаманні базові функції, включені в систему за замовчуванням [3]:

• ведення та підтримка баз даних користувачів і карт / ідентифікаторів;

• зберігання фото користувачів у базі даних;

• фіксація дати і часу проходу користувача в базі даних;

• можливість завдання різних рівнів доступу;

• автономна робота контролерів системи зі збереженням основних функцій управління при порушенні зв'язку з комп'ютером;

• реєстрація та зберігання інформації про події в енергонезалежній пам'яті контролерів СКУД;

• збереження ідентифікаційних ознак в пам'яті системи при відмові і відключенні електроживлення;

• відкривання ПП при зчитуванні зареєстрованої в пам'яті системи ідентифікаційної ознаки;

• заборона відкривання ПП при зчитуванні незареєстрованої в пам'яті системи ідентифікаційної ознаки.

Рисунок 1.1 – Методи ідентифікації

Розглянемо важливі додаткові функції, які притаманні більшості СКУД [4]:

1. Облік робочого часу. За допомогою програмної надбудови СКУД дозволяють роботодавцю враховувати час коли працівник приходить на роботу і час, коли виходить з роботи. Кадрові працівники можуть точно визначити час перебування співробітника на робочому місці. На початку дня вбудована в СКУД система обліку робочого часу дозволяє формувати звіт про співробітників, які не пройшли автентифікацію в СКУД. Це дозволяє виявляти тих, хто запізнився або не з'явилися на робоче місце.

2. Можливість апаратної і програмної інтеграції, реєстрація та протоколювання подій в підсистемах ОПС і CCTV. Основний сенс інтеграції - це в першу чергу об'єднання окремих підсистем за допомогою єдиного інтерфейсу, який дозволяв би виконувати і моніторинг, і налаштування системи «з одного вікна». Таким чином, взаємна інтеграція різних систем безпеки істотно полегшує роботу служб безпеки, знижує час реакції на позаштатні ситуації, а також підвищує ефективність ведення розслідування подій на об'єкті.

3. Прохід «з підтвердженням» з боку оператора. Така функція СКУД дуже затребувана на прохідній, коли охоронець контролює прохід і виконує фотоверіфікації співробітника за зображенням, яке система видає на монітор оператора під час піднесення до зчитувача карти доступу. Крім безпосередньої візуальної верифікації в рамках цієї функції може бути виконано порівняння фотографій з відеопотоком, який система видає на робочу станцію оператора.

4. Доступ за правилом «два обличчя і більше». Це правило є затребуваним під час обмеження доступу в спец приміщення. Крім того, в СКУД існує таке поняття, як «господар зони», тобто, в разі його відсутності, доступ в зону буде заборонений будь кому. Зазвичай, це і, подібне йому, правило «ескорт» застосовуються в банківських СКУД.

5. Вхід в режимі «шлюз». Організація шлюзів буває необхідна під час побудови системи контролю доступу в особливо важливі приміщення або

будівлі, такі як банківські сховища і дата-центри. Залежно від архітектурних особливостей об'єкта, а також від фінансових можливостей замовника, можна як встановити готову шлюзову кабіну, так і виконати шлюз у вигляді тамбура, обмеженого двома дверима з зчитувачами на вхід і на вихід.

7. Захист техзасобів і ПЗ від несанкціонованого доступу. Захист від несанкціонованого доступу до налаштувань обладнання ПЗ СКУД є необхідною умовою надійної і ефективної роботи системи, не дозволяє допускати порушення умов допуску.

8. Управління об'єктами з розподіленою філіальною структурою. Наявність системи віддалених філій (особливо для банків і великих корпорацій) є звичайною організаційною структурою, при цьому наявність уніфікованої на всю філіальну систему СКУД підвищує надійність і зручність моніторингу і управління бізнес-процесами. Багатоорганізаційність (тобто функціонування в межах однієї системи ряду «автономних», невидимих одне одному, крім єдиного керуючого центру, систем) - вкрай актуальна саме для бізнес-центрів з безліччю організацій, що орендують офіси.

9. Підключення зчитувачів різних типів. Часто до вимог проектувальника і кінцевого замовника з дизайну і ряду функцій входить підключення до єдиної СКУД зчитувачів різних виробників, а, в деяких випадках, і різних способів ідентифікації (RFID, біометрія і т.п.).

10. Ручне, напівавтоматичне або автоматичне відкривання ППК при НС. Ця функція є необхідною умовою експлуатації об'єктів і приміщень з техніки безпеки.

11. Управління роботою додаткових пристроїв в точках доступу (освітлення, вентиляція, ліфти, технологічне обладнання і т.п.). Ця функція підвищує рівень автоматизації об'єкта, дозволяє значно скоротити витрати на обслуговуючий і контролюючий персонал - загалом, управляти всіма інженерними системами з одного пульта, уніфікувати архіви подій по всіх системах і прив'язувати їх до єдиної бази даних персоналу.

12. Максимальна кількість ідентифікаторів для точки проходу. Під цим розуміється кількість карток, які можуть бути записані на одному контролері. Найбільш вузьким місцем є контролери турнікетів на центральній прохідній, бо через неї ходять всі співробітники і відвідувачі. Для звичайного офісного будинку це обмеження не відіграє великої ролі (кількість співробітників і відвідувачів рідко перевищує кілька тисяч). Однак, якщо мова йде про підприємство з декількома корпусами і великою кількістю співробітників, цей параметр необхідно враховувати.

13. Максимальна кількість контролерів в мережі. Фактично означає максимальну кількість контрольованих точок проходу в системі. Вибираючи СКУД для встановлення, необхідно враховувати, що в подальшому систему, можливо, доведеться масштабувати.

1.2 Загальні принципи роботи СКУД

Існуючі системи контролю доступу (СКД), умовно, можна розділити на дві категорії:

1. Прості, розраховані всього на одні вхідні двері. Зазвичай за такої архітектурі використовуються автономні контролери.

2. Складні, призначені для контролю доступу на великих об'єктах - підприємствах, заводах і банках [5].

Незалежно від конфігурації СКУД, кожна подібна система складається з декількох обов'язкових вузлів. Це - контролери для управління, зчитувачі для ідентифікації, а також всілякі виконавчі пристрої обмеження доступу: турнікети, електромагнітні замки і засувки. Електронні безконтактні карти в якості перепусток є найпоширенішим і зручним засобом ідентифікації в системах контролю доступу.

Принцип роботи всіх систем зводитися до трьох базових дій:

1. Надання права доступу.

2. Ідентифікація.

3. Доступ.

Працює система контролю і управління доступом в такий спосіб: після установки системи контролю доступу на об'єкті, кожен співробітник отримує унікальний ідентифікатор (магнітна картка, безконтактна картка, відбиток пальця, в разі використання біометричних систем) і встановлюються права доступу в різні зони. На вході в зони, що вимагають контролю, встановлюються зчитувачі ідентифікаторів, контролери та електромагнітні замки. Під час піднесення ідентифікатора до зчитувача, зчитувач передає інформацію контролеру, який визначає, чи має даний ідентифікатор право допуску до службового приміщення, і за наявності відповідних прав відкриває доступ. Принцип роботи СКУД показано на рисунку 1.2. Ідентифікатор може одночасно бути пропуском на територію організації і ключем від приміщень, куди співробітникові дозволений доступ. [6]

Всі обмежувальні пристрої підключаються до контролерів системи управління доступом. Контролери призначені для прийому і аналізу інформації з карт доступу, а також для управління різними виконавчими пристроями. До складу обладнання системи контролю доступу можуть входити два типи контролерів: контролери замку і контролери турнікету, кожен з яких відповідає за контроль роботи власного вузла.

Для проходу через турнікет або входу в відповідне приміщення працівники підприємства повинні піднести свою карту доступу до зчитувача, після чого зчитувач передає код пред'явленої карти в контролер, а контролер доступу приймає рішення про дозвіл або заборону проходу на підставі закладеної в нього інформації. У разі, якщо доступ дозволений, система контролю доступу автоматично розблокує турнікет або замок на дверях (рис.1.3).

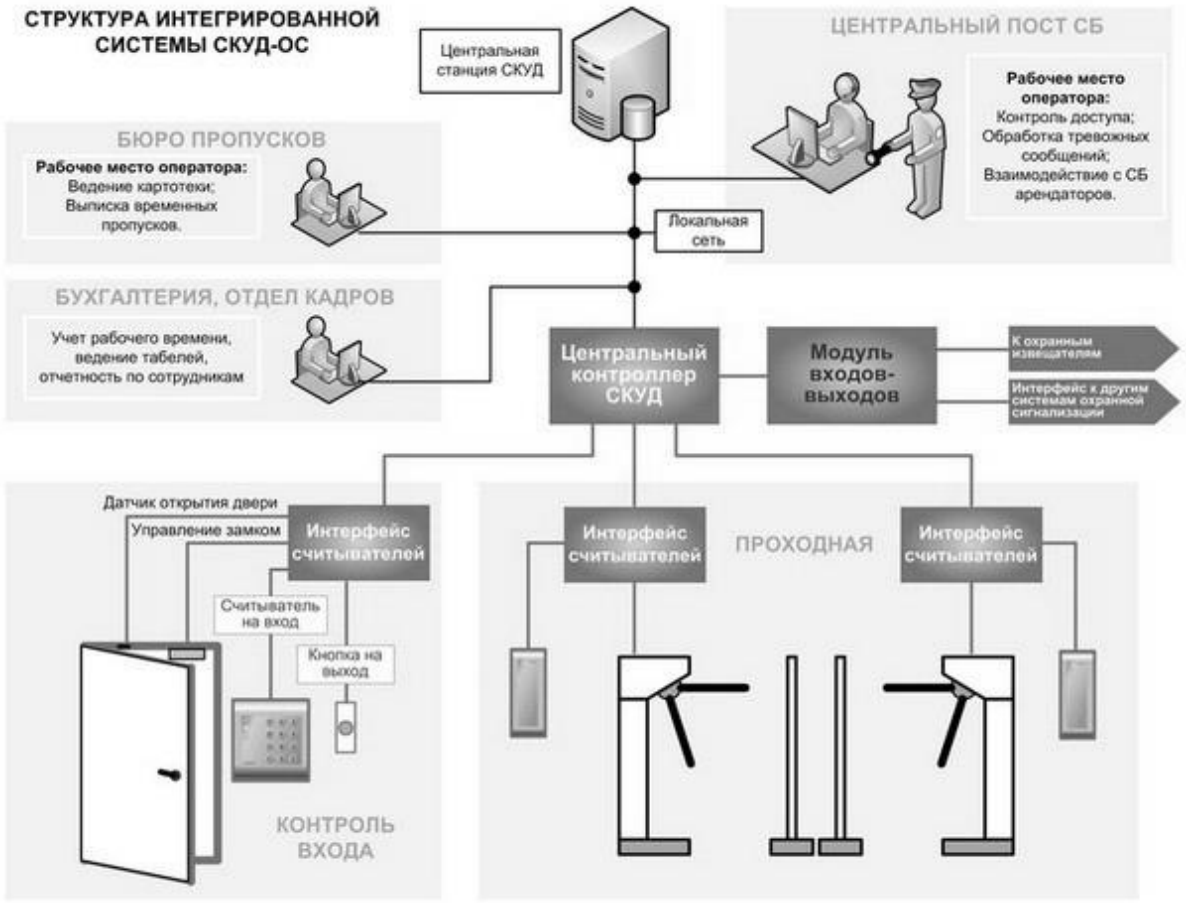

Рисунок 1.2 – Схема роботи СКУД

Рисунок 1.3 – Ідентифікація користувача

Також за допомогою СКУД можна здійснювати контроль в'їзду автотранспорту на територію об'єкту. В цьому випадку, після пред'явлення персонального ідентифікатора відбувається відкриття воріт або підйом шлагбаума (рис. 1.4).

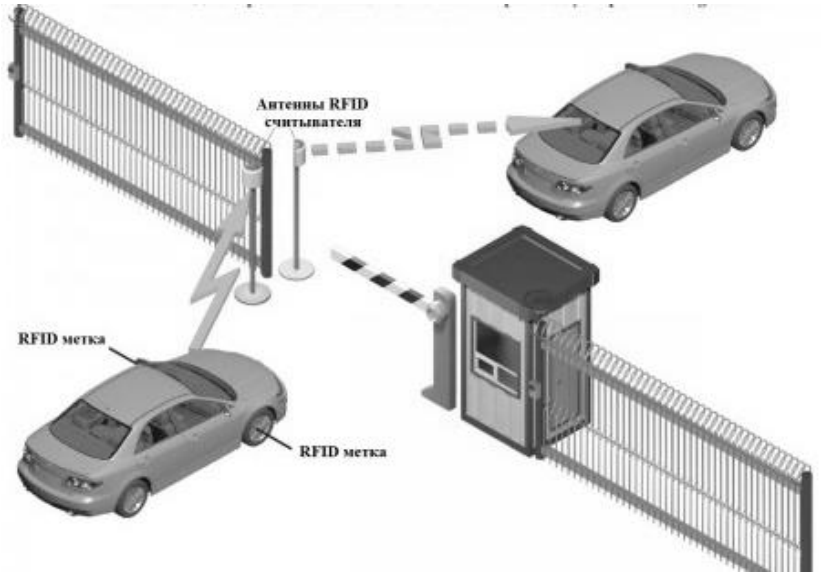

Рисунок 1.4 – Ідентифікація автотранспорту

При детальному розгляді СКУД має більш складну класифікацію, яку буде розглянуто далі.

Зробивши детальний аналіз, засоби і системи СКУД можна класифікувати у такий спосіб (рис. 1.5):

- за способом управління;
- за кількістю контрольованих точок доступу;
- за функціональними характеристиками;
- за видом об'єктів контролю;
- за рівнем захищеності системи від несанкціонованого доступу.

Автономні системи використовуються на об'єктах, де відсутня необхідність постійного моніторингу подій та віддаленого управління ВП.

Отже, автономні СКУД повинні забезпечувати:

• видачу сигналу на відкривання ППК під час зчитування зареєстрованого в пам'яті системи ідентифікаційного пристрою;

• заборона відкривання ППК під час зчитування незареєстрованого в пам’яті системи ідентифікаційного пристрою;

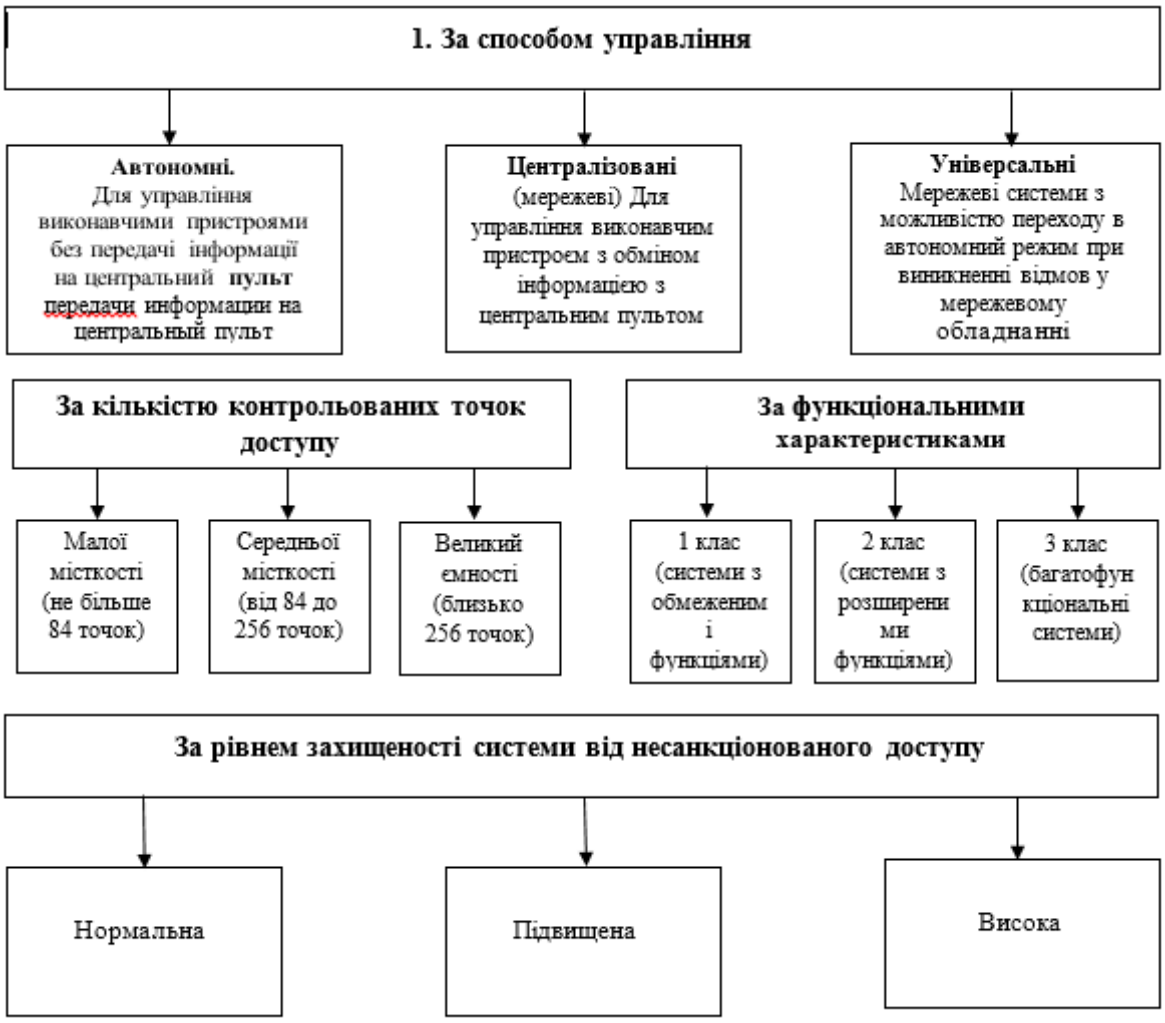

Рисунок 1.5 – Класифікація СКУД

• запис ідентифікаційних ознак в пам'ять системи;

• захист від несанкціонованого доступу під час запису кодів ідентифікаційних ознак в пам'ять системи;

• збереження ідентифікаційних ознак в пам'яті системи за умови відмови і відключення електроживлення;

• ручне, напівавтоматичне або автоматичне відкривання ППК для проходу під час аварійних ситуацій;

• ситуації, пожежі, технічні несправності відповідно до правил встановленого режиму і правил протипожежної безпеки;

• автоматичне формування сигналу закриття на УПУ за відсутності факту проходу;

• видача сигналу тривоги під час аварійного відкриття ППК для несанкціонованого проникнення.

Централізовані (мережеві) СКУД застосовуються в тому разі, якщо необхідно контролювати час проходу відвідувачів і управляти конфігурацією будь-якої частини системи з центрального пульта. Термін «універсальні СКУД» характеризує здатність СКУД переходити в режим автономної системи, яка здатна працювати за умови виникнення відмов керуючих комп'ютерів, мережевого обладнання або обриву зв'язку з контролером. Варто відзначити, що функціонал, що дозволяє автономну роботу під час збоїв у з'єднанні з центральним пультом, вже давно є базовим для будь-якої мережевої СКУД. При побудові універсальних СКУД виділяють централізовану, розподілену і змішану архітектуру.

Централізована архітектура передбачає використання центрального контролера, що здійснює процес управління з використанням спеціалізованих інтерфейсних модулів. Контролер в системах з централізованою архітектурою зберігає всю базу ідентифікаторів і подій, що сталися в системі. Таким чином, поділ функцій прийняття рішень і безпосереднього управління підвищує рівень безпеки СКУД, оскільки сам контролер встановлений на значній відстані від керованого ним перегороджуючого пристрою (ППК). За умови порушення зв'язку контролера з керуючим комп'ютером система продовжує працювати в автономному режимі.

Системи, побудовані на базі розподіленої архітектури, містять БД ідентифікаторів і подій не в одному, а в декількох контролерах. Вони виконують функції управління зовнішніми пристроями і охоронними шлейфами через розташовані на платі реле. Виведення з ладу одного контролера не вплине на роботу інших, а в разі обриву лінії зв'язку між контролерами і комп'ютером система продовжує виконувати основні функції управління процесом доступу в автономному режимі.

СКУД з централізованим управлінням і універсальні повинні відповідати загальним функціональним вимогам для автономних систем і додатково забезпечувати:

• роботу в локальній мережі контролерів СКУД;

• реєстрацію і протоколювання тривожних і поточних подій;

• пріоритетне відображення на екрані керуючого комп'ютера, тривожних подій;

• управління роботою ППК в точках доступу за командами оператора;

• встановлення тимчасових режимів дії ідентифікаторів в точках доступу і рівнів доступу;

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

• автоматичний контроль справності засобів, що входять в систему і ліній передачі інформації;

• можливість автономної роботи контролерів системи зі збереженням основних функцій у випадку відмови зв'язку з пунктом централізованого управління;

• встановлення режиму вільного доступу з пункту управління під час аварійних ситуаціях і надзвичайні події (пожежа, землетрус, вибух і т.п.);

• блокування проходу по точках доступу командою 0 пункту управління в разі нападу;

• можливість підключення додаткових засобів спеціального контролю, засобів догляду.

Найбільш поширеним є підхід до побудови мережевих СКУД з універсальною (змішаною) архітектурою, що допускає використання спеціалізованих зчитувачів з власним буфером пам'яті ідентифікаторів і подій - «інтелектуальних» інтерфейсних модулів. В основі лежить централізована архітектура, тому при пошкодженні лінії зв'язку між центральним контролером і інтерфейсними модулями управління кінцевими пристроями активується автономний режим управління доступом із застосуванням вбудованої буферної

пам'яті на кожній з проблемних ділянок. Системи, побудовані з використанням даного технічного рішення, характеризуються високим рівнем безпеки і надійності.

СКУД встановлюються на об'єктах різних масштабів: від невеликих офісів до заводів і технопарків з декількох будівель. Широке поширення таких систем призводить до стрімкого розвитку технологій, що використовуються. Вибір і налаштування систем безпеки на кожному об'єкті носить індивідуальний характер, тому що залежить від безлічі різних факторів. Цим обумовлено прагнення виробників СКУД до уніфікації технологій, що використовуються.

Універсальні системи повинні забезпечувати автономну роботу під час виникнення відмов у мережевому обладнанні, центральному пристрої або обриві зв'язку, а також відновлення режимів роботи після усунення відмов і відновлення зв'язку. [7]

Також СКУД можна класифікувати за класами.

СКУД 1-го класу - малофункціональні системи малої місткості, що працюють в автономному режимі і здійснюють допуск усіх осіб, які мають відповідний ідентифікатор. У такій системі використовується ручне або автоматичне керування виконавчими пристроями, а також світлова або звукова сигналізація. Типова схема СКУД 1-го класу показана на рисунку 1.6.

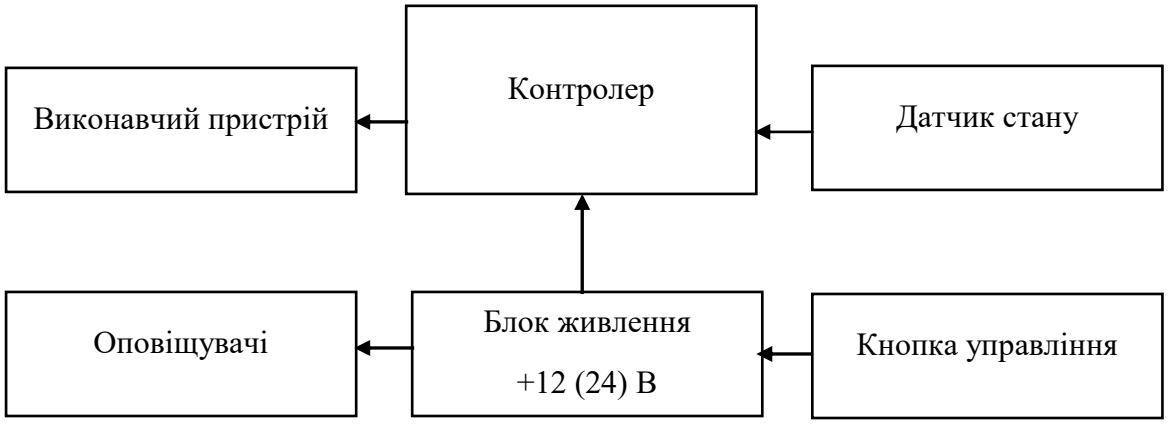

Рисунок 1.6 – Типова схема СКУД 1-го класу (приміщення з одними дверима)

СКУД 2-го класу - монофункціональні системи. Вони можуть бути однорівневими і багаторівневими і забезпечують роботу як в автономному, так і в мережевому режимах. Допуск осіб (груп осіб) може здійснюватися за датою, часовими інтервалами. Система здатна забезпечити автоматичну реєстрацію подій і автоматичне керування виконавчими пристроями. Типова схема СКУД 2-го класу показана на рисунку 1.7.

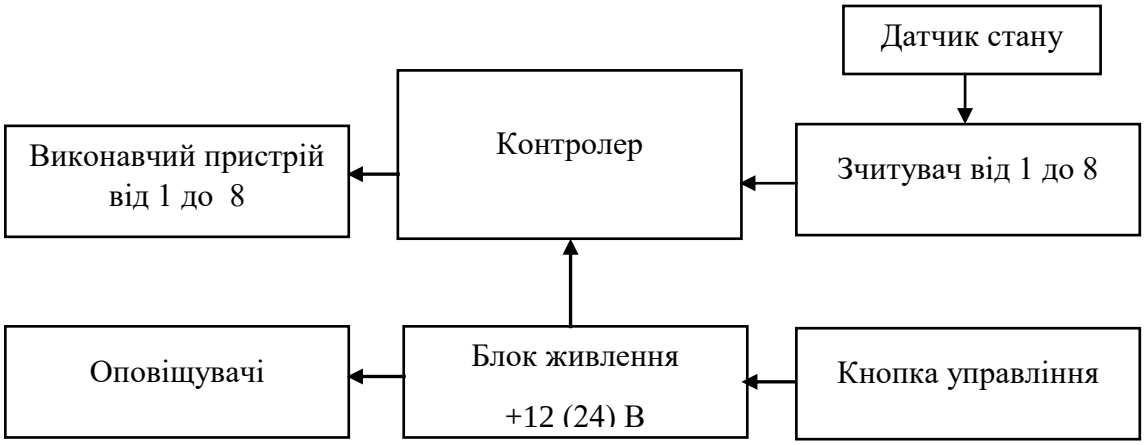

Рисунок 1.7 – Типова схема СКУД 2-го класу

СКУД 3-го класу, як правило, є мережевими. У них використовуються більш складні ідентифікатори і різні рівні мережевої взаємодії (клієнт-сервер, інтерфейси зчитувачів карт Виганда або магнітних карт, спеціалізовані інтерфейси і ін.). [1]

Рисунок 1.8 – Типова схема СКУД 3-го класу (приміщення з одними дверима)

За кількістю точок доступу і користувачів СКУД поділяються на такі види:

- малі, мають кілька одиниць точок доступу (офіси);
- середні, мають десятки точок доступу і тисячі користувачів (банки, підприємства, установи, готелі);
- великі, мають сотні точок доступу і десятки тисяч користувачів (великі промислові підприємства, аеропорти).

Висновки до розділу: Розглянувши функціональні можливості СКУД, вимоги до них, оцінивши методи ідентифікації можна зробити висновок, що СКУД це система, основне завдання якої - управління доступом на задану територію, що включає можливості розмежування прав доступу, що дозволяє проводити ідентифікацію користувача і містить додаткові аналітичні функції.

Сукупність різних методів ідентифікації дозволяє організувати максимальний рівень захисту об'єкта від несанкціонованого доступу. Вибір методів повинен ґрунтуватися на рівні секретності приміщення, до якого надається доступ. Підбір компонентів системи СКУД повинен грантуватися на потребах замовника.

2. АНАЛІЗ ТЕХНОЛОГІЙ КОНТРОЛЮ УПРАВЛІННЯ ДОСТУПОМ

Основою будь-якої системи СКУД є блоки контролерів з підключеними зчитувачами ідентифікаційних ключів, охоронними датчиками і електромеханічними запірними пристроями (замки, шлагбауми, турнікети та ін.).

Контролер - це основна частина системи управління доступом. Саме контролер приймає рішення, пропустити чи ні людини в дані двері. Контролери виконавчих пристроїв СКУД - складні електронні прилади, які можуть бути реалізовані у вигляді окремих блоків або вбудовані в корпус відповідного виконавчого пристрою. Контролер зберігає у своїй пам'яті коди ідентифікаторів зі списком прав доступу кожного.

Крім обміну інформацією з концентраторами СКУД по лініях зв'язку здійснюють: аналіз інформації, що надходить з пристроїв читання електронних ідентифікаторів, пристроїв введення PIN-коду і біометричних ідентифікаторів, видачу на підставі цього аналізу керуючих сигналів на відмикання (замикання) виконавчих пристроїв; контроль стану виконавчих пристроїв (відкрито чи закрито); зберігання в оперативній незалежній пам'яті журналу переміщень; реєстрацію спроб несанкціонованого доступу. Важливо, щоб контролер міг працювати навіть в разі аварії електромережі, мав резервне джерело живлення.

Зчитувач (рідер) - це пристрій, призначений для зчитування спеціальної кодової інформації, що зберігається в ідентифікаторі, та її передачі у вигляді заздалегідь визначеного сигналу в контролер. Зчитувачі можуть бути ручними, стаціонарними і стаціонарними автоматичними, що мають зв'язок з системою.

В якості засобів доступу (ідентифікатора особистості) можуть бути застосовані будь-які контактні або безконтактні карти, електронні ключі або навіть сигнал від відеокамери. В системі контролю і управління доступом стан контрольованих зон, події і звіти можуть відображатися в реальному масштабі часу на екрані комп'ютера.

Відповідно до [8], засоби КУД класифікуються за функціональним призначенням пристроїв, функціональними характеристиками і стійкістю до несанкціонованого доступу. У табл. 1.1 подано класифікацію засобів КУД.

Таблиця 1.1 – Класифікація ідентифікаторів доступу

Вид використовуваних ідентифікаційних ознак	Елемент, який лежить в основі принципу використання	Приклади ідентифікаторів
Оптичні	Мітки, нанесені на поверхню або розташовані всередині ідентифікатора, що мають різні оптичні характеристики у відбитому або минаючому оптичному випромінюванні	Карти з штрих-кодом, топографічні мітки
Електронні контактні	Електронний код, записаний в електронній мікросхемі ідентифікатора	Електронні ключі
Електронні радіочастотні	Радіоканал, використовуваний для передачі даних	Безконтактні карти доступу
Акустичні	Кодований акустичний сигнал	Пристрої генерації акустичних сигналів
Біометричні	Індивідуальні фізичні ознаки людини	Відбитки пальців, геометрія долоні, малюнок сітківки ока, голос, динаміка підпису
Комбіновані	Кілька ідентифікаційних ознак	Безконтактна карта доступу і відбитки пальців
Механічні	Елементи конструкції ідентифікаторів	Механічні ключі з перфораційними отворами

Розглянемо більш детально кожну технологію, яка використовується у СКУД.

2.1 Оптичні ідентифікатори СКУД

Оптичні ідентифікаційні ознаки на даний час практично не використовуються у системах СКУД.

По суті це є штрих-кодові карти – на які наноситься штриховий код, якій містить інформацію про об’єкт. Існує більш складний варіант - штрих-код закривається матеріалом, прозорим тільки в інфрачервоному світлі, зчитування відбувається в інфрачервоній області.

2.2 Електронні контактні ідентифікатори СКУД

Як правило, такі ідентифікатори СКУД виконані у вигляді брелоків. Застосовуються найчастіше в системах контролю доступу, де не потрібен високий клас захищеності, а треба просто відокремити так званих «зівак» від конкретного приміщення.

Головним недоліком таких систем є наявність контакту з гальванічною зв'язком з мікро контролером, інакше кажучи, система не має зчитувача як такого. Ключ Touch-memory являє собою незалежну пам'ять, розміщену в металевому корпусі, з одним сигнальним контактом і одним контактом землі. Диск складається з двох електрично ізольованих половинок. Всередині він порожній. У герметичну порожнину укладена електронна схема на кремнієвому кристалі. У незалежній пам'яті мікросхеми ключа зберігається його персональний код, який являє собою 48-розрядний ідентифікаційний номер, 8-бітний номер типу виробу, 8-бітний код для контролю. Ключ не надійний, бо легко копіюється.

2.3 Електронні радіочастотні ідентифікатори СКУД

RFID (радіочастотна ідентифікація) - метод автоматичної ідентифікації об'єктів, в якому за допомогою радіосигналів зчитуються або записуються дані,

що зберігаються в так званих транспондерах, або RFID-мітках.

Будь-яка RFID-система складається з пристрою, що зчитує (рідер) і транспондера (він же RFID-мітка). Мітка - це пристрій, здатний зберігати дані і передавати їх рідеру безконтактним способом за допомогою радіохвиль.

Класифікація RFID-систем показана на рисунку 2.1

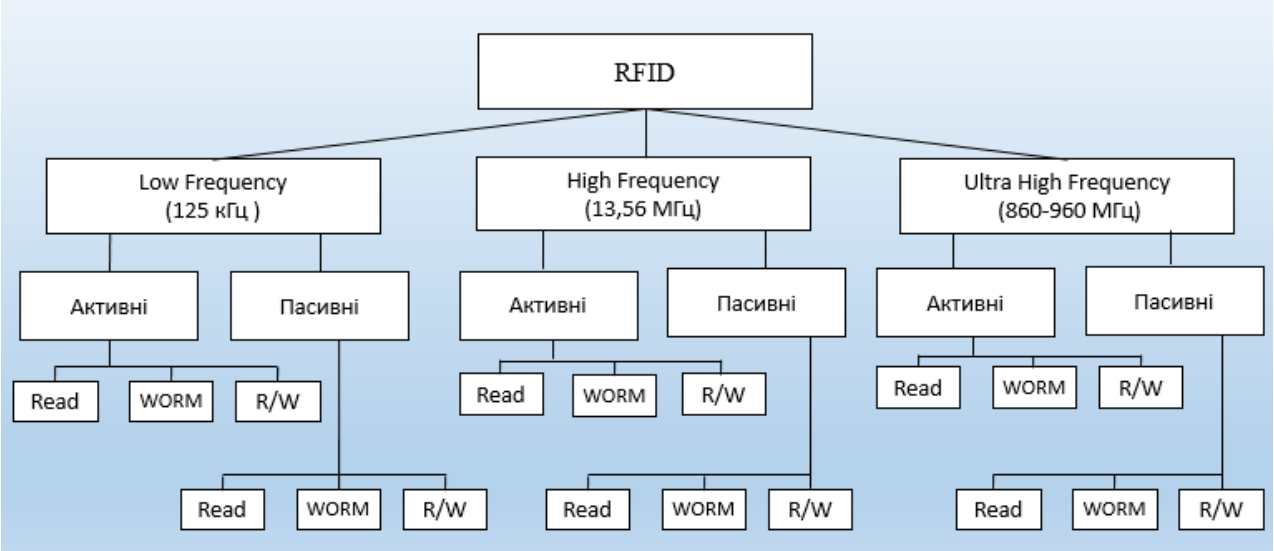

Рисунок 2.1 – Класифікація RFID-систем

Як показано на рисунку 2.1 існує кілька способів класифікації RFID-міток і систем:

- за діапазоном частот;
- за типом джерела живлення;
- за типом пам'яті;
- за виконанням.

Розглянемо більш докладно класифікацію RFID-міток і систем.

За діапазону частот поділяють найбільш поширені такі види:

- низькочастотні proximity карти (125 кГц);
- високочастотні RIFD- карти (13,56 МГц);
- UHF карти доступу.

Низькочастотні RIFD-карти - Low Frequency (LF) - працюють на частоті 125 кГц. По суті, proximity карта - це дистанційний електронний пропуск з вбудованим мікрочіпом і вбудованою антеною у вигляді багатоконтурної (кілька сотень) обмотки, що має унікальний ідентифікаційний код, який широко використовуються в системах контролю, як фізичного, так і логічного доступу для безконтактної радіочастотної ідентифікації.

Обмін інформацією між картою і proximity зчитувачем здійснюється з відкритого протоколу, що робить проксіміті карти досить вразливими для зловмисників.

Низькочастотні RIFD-карти однаково ефективно працюють і з вуличними, і з кімнатними зчитувачами; не вимагають чіткого позиціонування об'єкта і мають низьку вартістю, але існують проблеми зі зчитуванням на великі відстані, а також проблеми, пов'язані з появою колізій при зчитуванні. Виготовляється такі карти доступу, найчастіше, у вигляді пластикової картки.

Високочастотні RIFD-карти - High Frequency (HF) - працюють на частоті 13,56 МГц. Завдяки більш широкій смузі пропускання, високочастотні RIFD-карти дозволяють забезпечити більший рівень безпеки і швидкість дії. Карти доступу, що працюють на частоті 13,56 МГц, дозволяють реалізувати взаємну аутентифікацію між картою і зчитувачем, а також використовувати алгоритми шифрування даних.

Більшість виробників додатково чипують високочастотні карти доступу, для забезпечення додаткових можливостей і підвищення рівня безпеки.

Як і для діапазону низьких частот, в системах, побудованих в діапазоні середніх частот, існують проблеми зі зчитуванням на великих відстанях (відстань роботи до 30 см), зчитування в умовах високої вологості, наявності металу, а також проблеми, пов'язані з появою колізій під час зчитування.

До складу такої системи входять: антена для прийому і передачі сигналу, що зчитує (зчитувач, рідер) і RFID-мітка для зберігання інформації.

Принцип роботи міток вельми простий: приймально-передавальний модуль, як антени у якого є обмотка (первинна). Мітка - це чіп, з вторинною обмоткою відповідно (рис.2.2, рис.2.3).

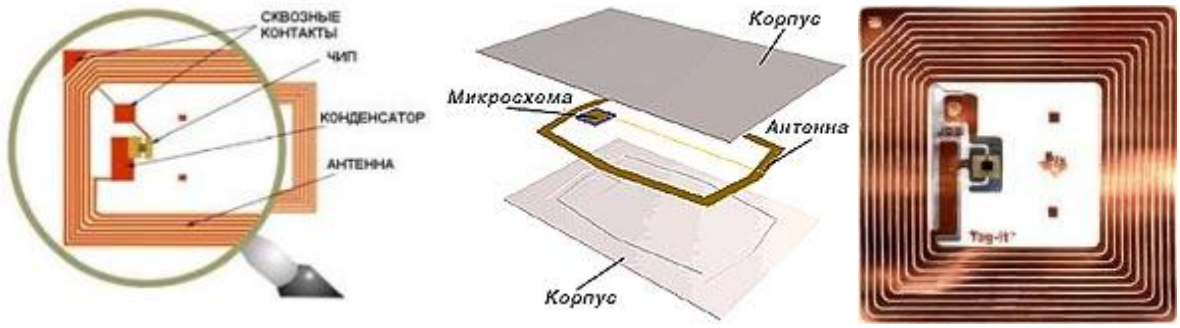

Рисунок 2.2 – Устрій RFID-мітки

Під час, піднесення зчитувача до мітки, через обмотку мітки починає текти струм і від нього живиться чіп, який змінюючи імпеданс в навантаженні обмотки передає інформацію зчитувача. Детальна схема роботи такої системи показана на рисунку 2.3.

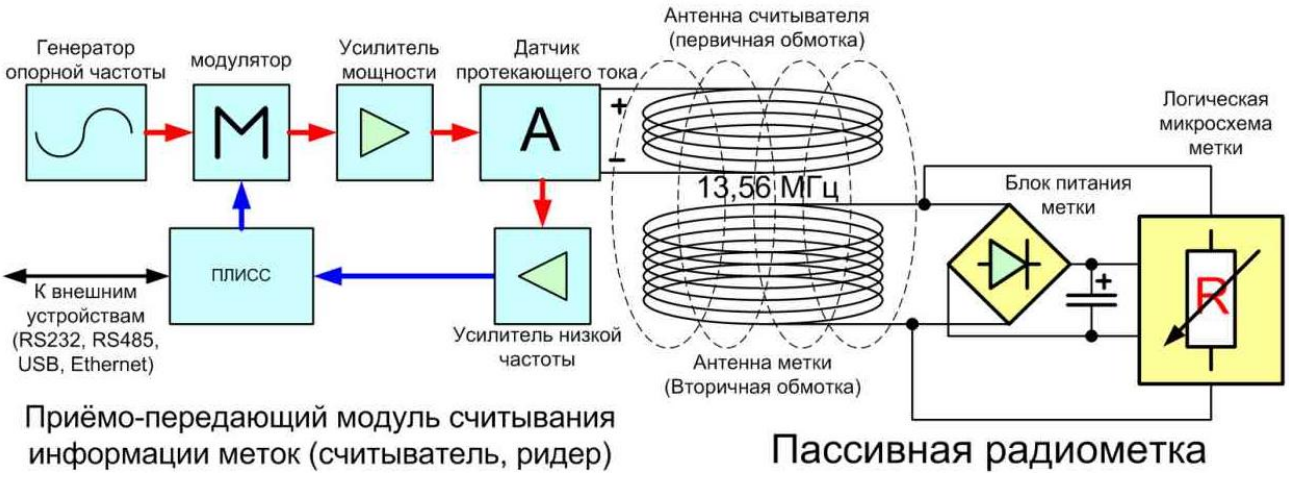

Рисунок2.3 – Схема роботи високочастотної RIFD-системи

Ультрависокочастотні карти доступу - Ultra High Frequency (UHF) - працюють на частоті 860-960 МГц. Використання UHF RIFD-карт дозволяє значно збільшити відстань зчитування. Найчастіше UHF технології використовуються для організації віддаленого зчитування RIFD-міток під час проїзду автотранспорту. Крім того, ультрависокочастотні карти доступу можуть застосовуватися в мультитехнологічних рішеннях для організації в'їзду на територію і входу в будівлю по одній картці.

Мітки даного діапазону мають найбільшу дальністю реєстрації, в багатьох стандартах даного діапазону присутні антиколізійні механізми У високочастотних RFID-системах в порівнянні з середньочастотними і низькочастотними нижче вартість міток, при цьому вище вартість іншого обладнання.

Високочастотні мітки мають одноконтурні обмотки (диполь-антена). Мітки ближнього поля яка є безпосередньо радіомітками, а використовуючи магнітне поле антени, дозволяють вирішити проблему зчитування в умовах високої вологості, присутності води і металу.

Ультрависокочастотних метод працює за наступним принципом. Зчитувач радіоміток є активним приймально-передавальним пристроєм з безперервним випромінюванням носійної частоти. Приймальна частина, відповідно, так само включена постійно. Коливальна енергія випромінюється в ефір через антенну систему.

Радіомітка є чіпом, що забезпечений антеною системою - зазвичай напівхвильової , або чверть хвильової диполь.

Радіомітка приймає за допомогою власної антенною системи високочастотну енергію передану зчитувачем. У чіпі знаходиться мостовий випрямляч (банальний лінійний блок живлення з небанальними мікроскопічними розмірами) і з його допомогою частина прийнятого УВЧ сигналу служить живленням мікросхеми. Після того як мікросхема живиться, починається активне опитування мітки зчитувачем. Відповідна інформація надсилається міткою за допомогою амплітудної модуляції відбитого сигналу,

яка виходить за допомогою зміни ефективної поверхні розсіювання (ЕПР) мітки за допомогою нелінійного елемента - варикапа (діод зі змінною ємністю). Схема роботи показана на рисунку 2.4.

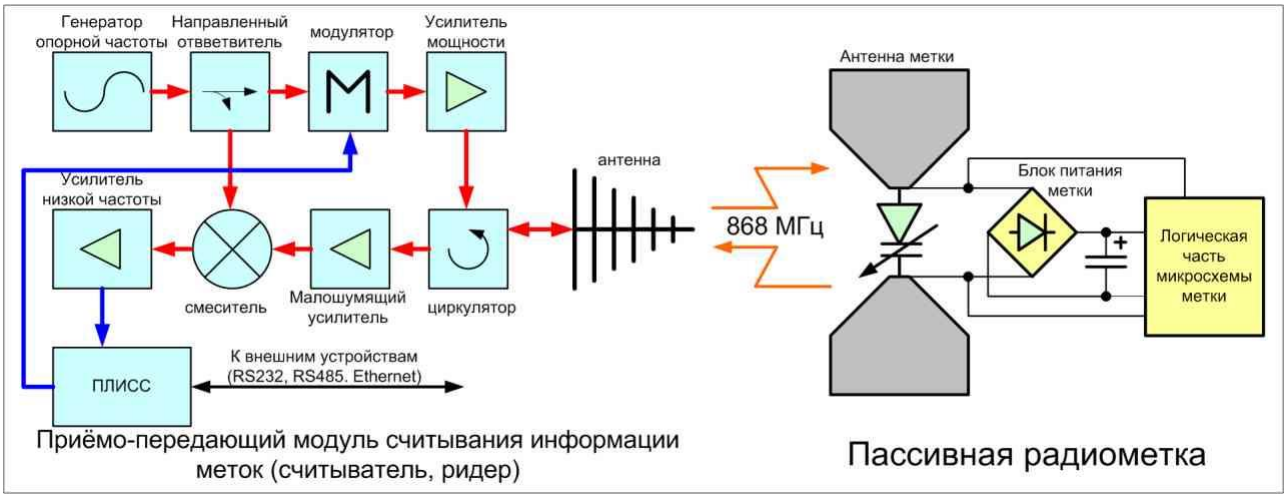

Рисунок 2.4 - Схема роботи ультрависокочастотної RIFD-системи

Дана технологія дозволяє: робити зчитування пасивних міток на відстані до 10 метрів. Середня відстань зчитування міток в промислових умовах становить від півметра до 3-х метрів. Одноразово в поле зчитувача може перебувати до 200 - 300 міток, і всі вони будуть ідентифіковані.

В таблиці 1.2 представлено порівняння різних RFID систем.

Класифікація за джерелом живлення RFID-карти діляться на:

- пасивні;
- напівпасивні;
-активні.

Пасивні RFID-картки не мають власного джерела живлення. Працюють від електричного струму, індукованого в антені карти електромагнітним сигналом зчитувача. Як наслідок, мають мінімальний радіус дії, якого, втім, цілком вистачає для більшості систем. Вартість пасивних RFID-міток - мінімальна.

Електричний струм, індукований в антені електромагнітним сигналом від зчитувача, забезпечує достатню потужність для функціонування кремнієвого CMOS-чіп, розміщеного в мітці, і передачі сигналу у відповідь.

Таблиця 1.2 – Порівняння існуючих RFID систем

	125кГц (LF)	13,56 МГц (HF)	860-928 МГц (UHF) 2,4-5,0 ГГц
Максимальна відстань зчитування	Від 3 до 70 см.	Від 1 до 200 см.	Від 10см. до 10 м.
Швидкість передачі даних радіопозначка-зчитувач	9600 біт/сек	До 64 кбіт/сек.	Від 128 кбіт/сек.
Наявність антіколлізіі	Присутня, але не у всіх мікросхемах	Присутня	Присутня, до 150 міток/сек
Обсяг пам'яті радіомітки	32 – 1024 байту	8 – 16384 байту	64 – 1024 біт (ISO), 64 чи 96 біт (EPC)

Пасивні мітки УВЧ і СВЧ діапазонів (860-960 МГц і 2,4-2,5 ГГц) передають сигнал методом модуляції відбитого сигналу носійної частоти. Антена зчитувача випромінює сигнал несучої частоти і приймає відбитий від мітки модульований сигнал. Пасивні мітки ВЧ діапазону передають сигнал методом модуляції навантаження сигналу несучої частоти. Кожна мітка має ідентифікаційний номер. Пасивні мітки можуть містити перезаписувану незалежну пам'ять EEPROM-типу. Дальність дії міток становить 1-200 см (ВЧ-мітки) і 1-10 метрів (УВЧ і НВЧ-мітки).

Пасивні RFID-картки не мають власного джерела живлення. Працюють від електричного струму, індукованого в антені карти електромагнітним сигналом зчитувача. Як наслідок, мають мінімальний радіус дії, якого, втім,

цілком вистачає для більшості систем. Вартість пасивних RFID-міток - мінімальна.

Електричний струм, індукований в антені електромагнітним сигналом від зчитувача, забезпечує достатню потужність для функціонування кремнієвого CMOS-чіп, розміщеного в мітці, і передачі сигналу у відповідь.

Перевагою пасивних міток є практично необмежений термін їх служби (не вимагають заміни батареї). Недолік пасивних міток в необхідності використання більш потужних пристроїв зчитування інформації, що володіють відповідними джерелами живлення.

Напівпасивні (напівактивні) RFID-карти, вони ж Battery Assisted Passive мають власне джерело живлення, проте його робота є рідкої (і лише частково) спрямована на поліпшення передачі радіосигналу. Радіочастотна ідентифікація, як правило, здійснюється за тим самим принципом, що і в пасивних RFID-картах, а енергія джерела живлення спрямована на інші функції карти доступу. Наприклад, живлення різних датчиків (для подальшого завантаження даних через зчитувач), забезпечення енергією систем захисту карти або живлення мікрочіпа в смарт-картах.

Активні RFID-карти мають власне джерело живлення, що дозволяє значно збільшити радіус дії, а також, завдяки кращій якості передачі сигналу, також можуть генерувати вихідний сигнал більшого рівня, ніж пасивні, дозволяючи застосовувати їх в більш агресивних для радіочастотного сигналу середовищах: воді (включаючи людей і тварин, які в основному складаються з води), металах (корабельні контейнери, автомобілі), для великих відстаней на повітрі. Більшість активних міток дозволяє передати сигнал на відстані в сотні метрів за життя батареї живлення до 10 років. Активні мітки в більшості випадків більш надійні і забезпечують найвищу точність зчитування на максимальній відстані.

Перевагою активних міток в порівнянні з пасивними є значно більша (не менше, ніж в 2-3 рази) дальність зчитування інформації і висока допустима швидкість руху активної мітки щодо зчитувача.

Однак, поліпшення технічних характеристик роботи призводить до збільшення розмірів RFID - карти, а також значного збільшення вартості і обмеженого терміну її роботи.

Класифікація за способом запису інформації. Інформація в пристрій пам'яті радіочастотної мітки може бути занесена різними способами. Спосіб запису інформації залежить від конструктивних особливостей мітки. Залежно від цього розрізняють наступні типи міток:

Read Only - мітки, які працюють тільки на зчитування інформації. Необхідні для зберігання дані заносяться в пам'ять мітки виробником і не можуть бути змінені в процесі експлуатації.

WORM - мітки ('Write Once Read Many ") для одноразового запису і багаторазового зчитування інформації. Вони надходять від виробника без будь-яких даних користувача в пристрої пам'яті. Необхідна інформація записується самим користувачем, але тільки один раз. В разі необхідності змінити дані буде потрібна нова мітка.

R / W - мітки ('Read / Write ") багаторазового запису та багаторазового зчитування інформації.[9-12].

2.4 Біометричні ідентифікатори

Основними методами, які використовують статичні біометричні характеристики людини, є ідентифікація за папілярним малюнком на пальцях, за райдужною оболонкою, геометрією особи, сітківкою ока, малюнком вен руки, геометрією рук. Також існує сімейство методів, які використовують динамічні характеристики: ідентифікація за голосом, динамікою рукописного почерку, серцевого ритму, ходою. Нижче представлено розподіл біометричного ринку (рис. 2.5). У різних джерелах ці дані коливаються на 15-20 відсотків, тому це лише оціночне уявлення.

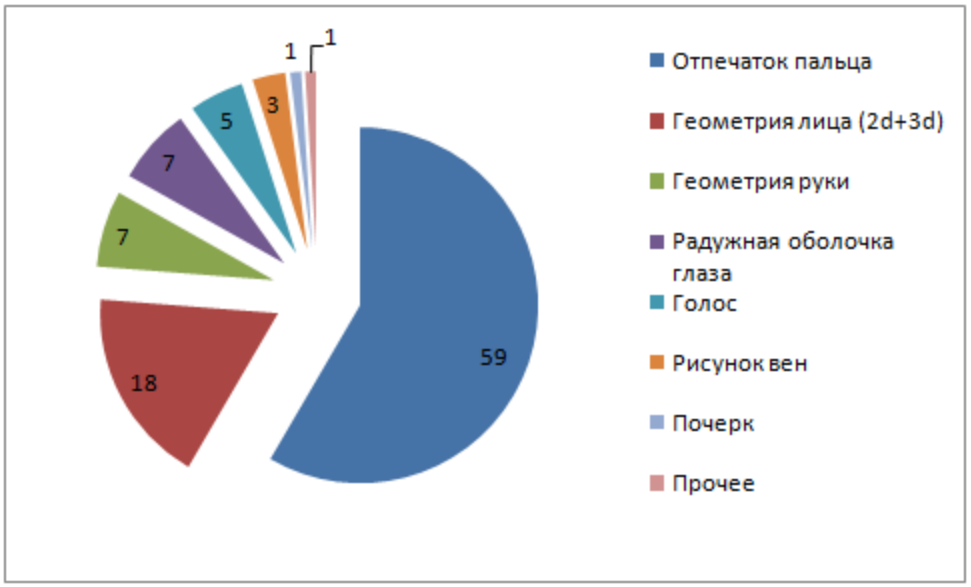

Рисунок 2.5 – Розподіл біометричного ринку

2.4.1 Відбитки пальців

Дактилоскопія (розпізнавання відбитків пальців) - найбільш розроблений на сьогоднішній день біометричний метод ідентифікації особистості. Кожна людина має унікальний папілярний візерунок відбитків пальців (рис. 2.6), завдяки чому і можлива ідентифікація. Зазвичай алгоритми використовують характерні точки на відбитках пальців: закінчення лінії візерунка, розгалуженні лінії, поодинокі точки. Додатково залучається інформація про морфологічну структуру відбитку пальця: відносне положення замкнених ліній папілярного візерунку, «арочних» та спіральних ліній. Особливості папілярного візерунку перетворюються на унікальний код, який зберігає інформативність зображення відбитка. І саме «коди відбитків пальців» зберігаються в базі даних, що використовується для пошуку і порівняння. Час переведення зображення відбитка пальця в код і його ідентифікація зазвичай не перевищує 1 с, в залежності від розміру бази. Час, витрачений на піднесення руки - не враховується.

Рисунок 2.6 – Папілярний візерунок відбитків пальців

Переваги і недоліки методу. Переваги методу. Висока вірогідність - статистичні показники методу краще показників ідентифікації за обличчям, голосом, розписом. Низька вартість пристроїв, які сканують зображення відбитку пальця. Досить проста процедура сканування відбитку.

Недоліки: папілярний візерунок відбитку пальця дуже легко пошкоджується дрібними подряпинами, порізами. Люди, які брали сканери на підприємствах з чисельністю персоналу близько декількох сотень людей заявляють про високий ступінь відмови сканування. Багато зі сканерів неадекватно ставляться до сухої шкірі і не пропускають людей похилого віку.

Під час спілкування на останній виставці MIPS начальник служби безпеки великого хімічного підприємства розповідав що їх спроба ввести сканери відбитків пальців на підприємстві (випробовували сканери різних систем) провалилася - мінімальний вплив хімічних реактивів на пальці співробітників викликав збій систем безпеки сканерів - сканери оголошували пальці підробкою. Так само присутня недостатня захищеність від підробки зображення відбитку, частково викликана широким поширенням методу. Варто відзначити, що велика кількість недоліків викликана широкою поширеністю системи, але ці недоліки існують і проявляються вони доволі часто.[13]

2.4.2 Райдужна оболонка ока

Райдужна оболонка ока є унікальною характеристикою людини. Малюнок райдужки формується на восьмому місяці внутрішньоутробного розвитку, остаточно стабілізується в віці близько двох років і практично не змінюється протягом життя, крім як в результаті сильних травм або різких патологій. Метод є одним з найбільш точних серед біометричних методів.

Система ідентифікації особи за райдужною оболонкою ділиться на дві частини: пристрій захоплення зображення, його первинної обробки і передачі обчислювачеві і обчислювач, що виконує порівняння зображення з зображеннями в базі даних, що передає команду про допуск виконавчому пристрою (рис.2.7).

Рисунок 2.7 – Система ідентифікації особи за райдужною оболонкою

Час первинної обробки зображення в сучасних системах приблизно 300-500 мс, швидкість порівняння отриманого зображення з базою має рівень 50000-150000 порівнянь в секунду на звичайному ПК. Така швидкість порівняння не накладає обмежень на застосування методу в великих організаціях за використання в системах доступу. За умови ж використання

спеціалізованих обчислювачів і алгоритмів оптимізації пошуку, стає можливим навіть ідентифікувати людину серед жителів цілої країни.

Переваги методу. Статистична надійність алгоритму. Захоплення зображення райдужної оболонки можна проводити на відстані від декількох сантиметрів до декількох метрів, при цьому фізичний контакт людини з пристроєм не відбувається. Райдужна оболонка захищена від пошкоджень - а значить не буде змінюватися в часі. Так само, можливо використовувати високу кількість методів, що захищають від підробки.

Недоліки методу. Ціна системи, заснованої на райдужній оболонці вище ціни системи, заснованої на розпізнаванні пальця або на розпізнаванні особи. Низька доступність готових рішень. [13]

2.4.3 Розпізнавання за обличчям.

Існує безліч методів розпізнавання за геометрією особи. Всі вони засновані на тому, що риси обличчя і форма черепа кожної людини індивідуальні. Ця область біометрії багатьом здається привабливою, тому що ми пізнаємо один одного в першу чергу за обличчям. Дана область ділиться на два напрямки: 2-D розпізнавання і 3-D розпізнавання. У кожного з них є переваги і недоліки, проте багато що залежить ще і від області застосування і вимог, пред'явлених до конкретного алгоритму.

2-D розпізнавання особи - один з найбільш статистично неефективних методів біометрії. З'явився він досить давно і застосовувався, в основному, в криміналістиці, що і сприяло його розвитку. В наслідок з'явилися комп'ютерні інтерпретації методу, в результаті чого він став більш надійним, але, безумовно, поступався і з кожним роком все більше поступається іншим біометричним методам ідентифікації особистості. В даний час завдяки поганим статистичним показникам, він застосовується в мультимодальній або, як її ще називають, перехресній біометрії, або в соціальних мережах.

Переваги методу 2-D розпізнавання, на відміну від більшості біометричних методів, не потрібно дороге обладнання. За наявності відповідного обладнання можливість розпізнавання на значних відстанях від камери.

Недоліки. Низька статистична достовірність. Пред'являються вимоги до освітлення (наприклад, не вдається реєструвати осіб, які входять з вулиці в сонячний день). Для багатьох алгоритмів неприйнятність будь-яких зовнішніх перешкод, як, наприклад, окуляри, борода, деякі елементи зачіски. Обов'язкове фронтальне зображення особи, з вельми невеликими відхиленнями. Багато алгоритмів не враховують можливі зміни міміки обличчя, тобто вираз має бути нейтральним.

3-D розпізнавання лиця. Реалізація даного методу є досить складним завданням. Незважаючи на це, в даний час існує безліч методів з 3-D розпізнавання особи. Методи неможливо порівняти один з одним, бо вони використовують різні сканери та бази, використовуються абсолютно різні підходи.

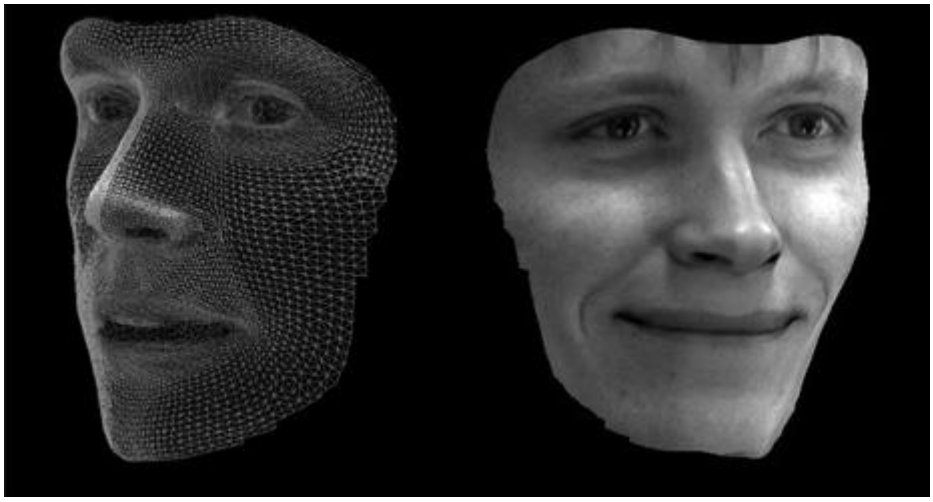

Рисунок 2.8 – Сітка 3-D розпізнавання обличчя**.**

Перехідним від 2-d до 3-d методом є метод, який реалізує накопичення інформації про особу. Цей метод має кращі характеристики, ніж 2d метод, але,

так само як і він, використовує всього одну камеру. Під час занесення суб'єкта до бази суб'єкт повертає голову і алгоритм з'єднує зображення, створюючи 3d шаблон. А під час розпізнавання використовується кілька кадрів відеопотоку.

Найбільш класичним методом є метод проектування шаблону. Він полягає в тому, що на об'єкт (особа) проектується сітка (рис. 2.8). Далі камера робить знімки зі швидкістю десятки кадрів в секунду, і отримані зображення обробляються спеціальною програмою. Промінь, що падає на викривлену поверхню, згинається - чим більше кривизна поверхні, тим сильніше вигин променю. Спочатку при цьому застосовувався джерело видимого світла, що подається через «жалюзі». Потім видиме світло було замінене на інфрачервоне, яке має низку переваг. Зазвичай на першому етапі обробки відкидаються зображення, на яких обличчя не видно взагалі або присутні сторонні предмети, що заважають ідентифікації. За отриманими знімками відновлюється 3-D модель особи, на якій виділяються і видаляються непотрібні перешкоди (зачіска, борода, вуса та окуляри). Потім проводиться аналіз моделі - виділяються антропометричні особливості, які в підсумку і записуються в унікальний код, заносячи в базу даних. Час захоплення і обробки зображення становить 1-2 секунди для кращих моделей.

Так само набирає популярність метод 3-d розпізнавання за зображенням, що отримується з декількох камер.

Переваги методу. Відсутність необхідності контактувати зі скануючим пристроєм. Низька чутливість до зовнішніх факторів, як на самій людині (поява окулярів, бороди, зміна зачіски), так і в його оточенні (освітленість, поворот голови). Високий рівень надійності, який можна порівняти з методом ідентифікації за відбитками пальців.

Недоліки методу. Висока вартість обладнання. Наявні в продажу комплекси перевершували за ціною навіть сканери райдужної оболонки. Зміни міміки обличчя і перешкоди на обличчі погіршують статистичну надійність методу. Метод ще недостатньо добре розроблений, особливо в порівнянні з дактилоскопією, що ускладнює його широке застосування. [13]

2.4.4 Розпізнавання за венами руки

Інфрачервона камера робить знімки зовнішньої або внутрішньої сторони руки. Малюнок вен формується завдяки тому, що гемоглобін крові поглинає інфрачервоне випромінювання. В результаті, ступінь відображення зменшується, і вени видно на камері у вигляді чорних ліній. Спеціальна програма на основі отриманих даних створює цифрову згортку. Не потрібно контакту людини зі сканувальним пристроєм.

Технологія порівнянна за надійністю з розпізнаванням за райдужною оболонкою ока.

Переваги методу. Відсутність необхідності контактувати зі сканувальним пристроєм. Висока вірогідність - статистичні показники методу можна порівняти з показаннями райдужної оболонки. Прихованість характеристики: на відміну від усіх вищенаведених - цю характеристику дуже важко отримати від людини «на вулиці», наприклад сфотографувавши його фотоапаратом.

Недоліки методу. Неприпустиме засвічення сканера сонячними променями і променями галогенових ламп. Деякі вікові захворювання, наприклад артрит - сильно погіршують роботу методу. [13]

2.4.5 Сітківка ока

До недавнього часу вважалося, що найнадійніший метод біометричної ідентифікації і аутентифікації особистості - це метод, заснований на скануванні сітківки ока. Він містить в собі кращі риси ідентифікації за райдужною оболонкою і за венами руки. Сканер зчитує малюнок капілярів на поверхні сітківки ока. Сітківка має нерухому структуру, незмінну в часі, крім як в результаті хвороби, наприклад, катаракти.

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 системах контролю доступу на особливо секретні об'єкти, бо у них один з найнижчих відсотків відмови в доступі зареєстрованих користувачів і практично не буває помилкового дозволу доступу.

На жаль, цілий ряд труднощів виникає під час використання цього методу біометрії. Сканером тут є досить складна оптична система, а людина повинна значний час не рухатися, поки система наводиться, що викликає неприємні відчуття.

Переваги. Високий рівень статистичної надійності. Через низьку поширеності систем, мала ймовірність розробки способу їх «обману».

Недоліки. Складна у використанні система з високим часом обробки. Висока вартість системи. Відсутність широкого ринку пропозиція і, як наслідок, недостатня інтенсивність розвитку методу. [13]

2.5 Проблеми ідентифікації відвідувачів

Протягом декількох десятків років основним засобом ідентифікації в СКУД є пропуск у вигляді пластикової карти. Це контактні і безконтактні карти різних форматів і стандартів, QR- (двомірні) і штрих-коди на фізичних і електронних носіях. Широке поширення подібного роду ідентифікаторів пояснюється головним чином їх низькою вартістю, а також універсальністю - карти доступу легко додавати в будь-яку вже існуючу СКУД. Крім того, smart-карти (наприклад, клас MIFARE) [14], завдяки наявності вбудованої пам'яті, використовуються для сторонніх додатків: муніципальних транспортних систем, програм лояльності тощо. Однак карти доступу мають ряд суттєвих недоліків, які в значній мірі знижують ефективність контролю і обліку потоків відвідувачів і співробітників. Нижче наведені недоліки найбільш поширених технічних рішень для ідентифікації в СКУД.

Втрата / передача карти доступу сторонній особі. Застосування електронних карт доступу або іншого виду фізичних ідентифікаторів за

великого потоку відвідувачів, породжує проблему перевірки фактів нелегального пред'явлення ідентифікатора. Зазвичай це завдання покладається на охоронців-контролерів. Найчастіше контролюючий персонал або ігнорує подібні порушення, або фізично не може відстежувати факти використання зареєстрованих перепусток сторонніми (неавторизованими) відвідувачами. З одного боку, користувач може цілеспрямовано передати свій ідентифікатор стороннім особам. З іншого боку, користувач може втратити карту доступу. При цьому існує велика ймовірність того, що знайшовши її зловмисник зможе визначити, куди і коли дана перепустка надає доступ.

Клонування карти. Великою проблемою карткових ідентифікаторів є технічна можливість їх клонування. Найпоширеніший в нашій країні стандарт безконтактних карт EM-Marine [15] (за оцінками експертів, від 60 до 70% всіх СКУД задіють саме його для ідентифікації) взагалі не має захисту від несанкціонованого зчитування та подальшого клонування. Також популярним є сімейство карт MIFARE на базі чіпів виробництва NXP Semiconductor. Для шифрування даних в них використовуються ліцензійні пропрієтарні криптоалгоритми. Прикладами подібних ВД є MIFARE Plus або MIFARE DESfire EV1. Однак на практиці системи безпеки, реалізовані з використанням карт цих стандартів, зустрічаються в основному на великих підприємствах через їх високу вартість. Стандарт MIFARE Classic популярніший, в тому числі і завдяки можливості виробляти картки на базі неоригінального чіпа, сумісного з протоколами NXP. Вартість таких продуктів близька до EM-Marine. Варто зазначити, що захист цих карт був зламаний за допомогою реверс-інжинірингу в 2008 році, тому, маючи технічні засоби, зловмисник зможе на невеликій відстані зчитати дані картки і відновити їх на іншій картці.

Недоліки біометричних систем. Більшість недоліків СКУД, побудованих з використанням карт доступу, можуть бути усунені за допомогою застосування біометричних терміналів. Користувач не має можливості свідомо передати свій біометричний ідентифікатор третій особі або втратити його. Крім того, завдання дублювання і відтворення біометричних ознак на іншому

носії дуже складно реалізовується. Але сам принцип роботи біометричних терміналів створює ряд складнощів, що перешкоджають їх широкому поширенню. Питома вага біометричних систем в загальній масі встановлених і експлуатованих СКУД залишається незначною. Вартість пристроїв, в основі яких лежить розпізнавання біометричних ознак (дактилоскопія, геометрія руки, обличчя, венозного малюнка, райдужної оболонки ока та ін.) у кілька разів перевищує вартість зчитувачів карт доступу .

У СКУД, що використовують карти доступу, з порівнянням пред'явленого ідентифікатора і БД займається контролер. Зчитувач лише транслює отриманий номер карти для обробки. У переважній більшості біометричних систем метчінг (процес порівняння) виконується самим зчитувачем або терміналом. Після успішної процедури метчінгу можливий один з двох варіантів:

1) термінал сам приймає рішення щодо допуску / затримання користувача і таким чином виконує функцію контролера (управління замком може відбуватися через вбудоване реле);

2) термінал формує пакет даних і відправляє його на сторонній контролер СКУД для обробки.

Перший варіант є дуже популярним: більшість терміналів має можливість підключення до мережі і реле управління замками. Все, що необхідно для отримання закінченої СКУД, - це ПЗ для додавання і видалення користувачів і налаштування правил і алгоритмів доступу. Практично всі виробники терміналів пропонують власний програмний продукт, але, як правило, він має досить скромним функціонал і підходить виключно для внесення нових користувачів в БД або організації доступу в невеликому офісі. Повноцінну СКУД на його базі побудувати неможливо, не кажучи вже про інтеграцію в неї сторонніх комплексів, наприклад, відеоспостереження або охоронної сигналізації. У зв'язку з цим, подібні рішення підходять виключно для невеликих систем з обмеженою кількістю користувачів.

Експлуатація біометричних засобів ідентифікації в складі СКУД

однозначно передбачає другий варіант. В цьому випадку біометричний термінал виступає в ролі контролера СКУД як звичайний зчитувач, який видає інформацію про ідентифікатор (більшість сучасних терміналів працюють по протоколу Wiegand). Однак, варто зазначити, що процедура метчінгу проводиться самим зчитувачем. Іншими словами, оператору системи необхідно додавати / видаляти біометричні ВД в усі зчитувачі за допомогою ПЗ терміналів, а виконувати повсякденні завдання, пов'язані з контролем доступу, - за допомогою ПЗ СКУД. Можна припустити, що для об'єктів з мінімальною плинністю кадрів і відсутністю сторонніх відвідувачів цей варіант прийнятний.

Крім того, актуальним є питання забезпечення безпеки біометричних персональних даних. Потенційні користувачі подібних систем можуть негативно ставитися до процедури збору відбитків пальців або інших параметрів для ідентифікації. Потрібно чітко розмежовувати криміналістичну біометрію та електронні системи доступу, засновані на розпізнаванні біометричних характеристик. В останньому випадку система, як правило, не зберігає шаблон (наприклад, дактилоскопічний відбиток) в чистому вигляді. У процесі додавання користувача в систему сканер дійсно отримує зображення тієї або іншої ознаки. Залежно від терміналу це малюнок дуг, завитків і петель на шкірі пальця, структура сітки вен, геометрія долоні з розставленими пальцями і т.д. Однак в подальшому відбувається процес вилучення з нього опорних даних, таких як відстань між певними точками на відбитку пальця, які після оцифровування не мають нічого спільного з оригіналом. Які саме опорні дані служать для створення віртуального образу ідентифікатора - інформація зазвичай закрита і використовується кожним конкретним виробником як частина пропрієтарного алгоритму. Відновити оригінальний малюнок, навіть отримавши доступ до цифрового шаблону, неможливо. І хоча кожен виробник терміналів докладає багато зусиль для пояснення цих тонкощів, усвідомлення того, що хтось може заволодіти особистими даними, часто відштовхує замовника від вибору на користь біометрії.

Також серйозним недоліком біометричних терміналів є аспект гігієни. Існує велика кількість технік безконтактного сканування біометричних параметрів, але все ж переважна більшість систем реалізовано на контактному дактилоскопічної принципі (зважаючи на широке поширення і невисоку вартість застосування даної технології).

2.6 Виконавчі пристрої

Серед виконавчих пристроїв контролю доступу найбільш розповсюджені наступні запірні або керовані перегороджуючі пристрої: замки, засувки, турнікети (поясні, повнозростові, «квиткові», розсувні, що обертаються трьох або чотириштангові) і шлюзові кабіни (тамбурного типу, ротанти, шлагбауми), автоматичні ворота (розсувні ворота, рухомі ворота, ворота, що складаються, рулетні ворота), ліфти.

Замки для СКУД - це запірні механізми, які встановлюються на двері в якості виконавчих пристроїв. Вони поділяються на кілька типів залежно від особливостей конструкції:

Електромеханічний замок (рис. 2.9) має механічний ригель (засув), що утримує двері в закритому стані, а управління цим ригелем здійснюється відносно малопотужним соленоїдом. Під час закриття дверей взводний ригель замку зводить наявну в замку пружину, при цьому робочий ригель входить у відповідну частину замку і утримує двері в закритому стані. Під час подачі напруги соленоїд скидає фіксатор пружини, і робочий ригель під дією пружини втягується в замок - двері можуть бути відкриті. Після того як двері буде відкрито, а потім закрито, вони знову опиняться в замкненому стані. Передбачається режим, що виключає автоматичне замикання замків і випадкове закривання дверей.[16]

Рисунок 2.9 –Електромеханічний замок

У соленоїдних електрозамках (рис. 2.10) ригель приводиться до руху зусиллям електромагніта. Обладнані таким замком двері можуть бути відкриті тільки в період дії керуючого сигналу. Після зняття цього сигналу зачинені двері залишиться замкненою незалежно від того, чи відкривалася вона. Існують також інші різновиди електромеханічних замків: електро моторні (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 врізаного типу.

Рисунок 2.10 – Приклад соленоїдного електрозамка

Електрозащіпки представляють собою відповідну частину замку і використовуються спільно зі звичайним механічним замком (рис. 2.11). Під час подачі напруги розблокується фіксатор електрозащіпки і двері можуть бути відкриті при висунутому положенні ригеля механічного замка. При цьому використовується механічний замок, який не повинен відкриватися зовні поворотом ручки. За наявності ручки з внутрішньої сторони дверей вона може бути відкрита зсередини поворотом ручки без подачі напруги, що подається на засувку.

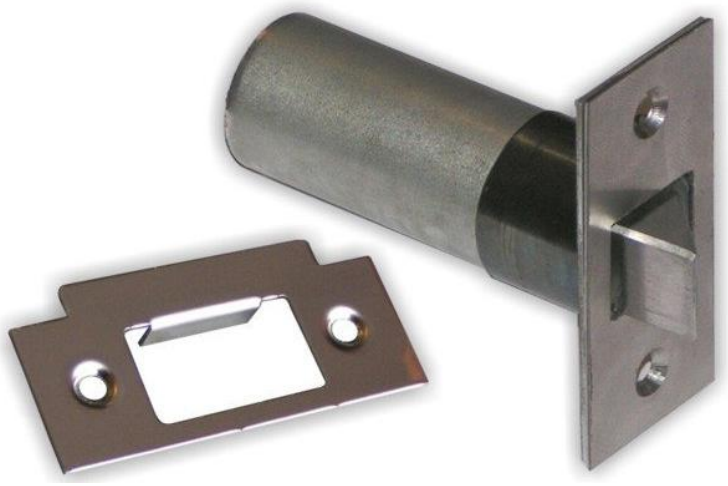

Рисунок 2.11 –Електрозащіпка

Потужні штирові електромеханічні замки сейфового типу під час подачі напруги на спеціальний електромотор здійснюють рух запірних штирів всередину.

Електромагнітні замки (рис. 2.12) складаються з електромагніта, що прикріпляється до дверної коробки, і у відповідь металевої пластини, що монтується на дверях. У черговому режимі на обмотку електромагніту подається постійний струм утримання, що викликає сильне магнітне поле, яке притягує металеву пластину двері, утримуючи її в закритому стані. Під час подачі сигналу на спеціальний вхід пристрою магнітне поле зникає, і двері можуть бути відкриті.

Рисунок 2.12 – Електромагнітні замки

Перевага електромагнітних замків - невеликий, в порівнянні з електромеханічними замками, споживаний струм і відсутність імпульсних викидів напруги під час відкривання. Негативна сторона - великі розміри, грубий промисловий дизайн і повна залежність від наявності електроживлення.

Турнікети. Турнікети систем контролю доступу також можна розділити на два типи: поясні та повнозростові. Принцип роботи турнікета досить добре відомий: якщо запит на доступ правомірний, то механічна система, повертаючись, відкриває прохід на територію, що охороняється.

Турнікети поясні залишають можливість для перестрибування, що випливає з їх назви, загороджувальний бар'єр доходить тільки до поясу людини, тому їх доцільно ставити тільки поруч з постом охорони.

Турнікети повнозростові можна встановлювати в віддалених від поста охорони місцях і використовувати в повністю автоматичному режимі роботи.

Рисунок 2.13 – Приклад турнікетів

Контролери ліфтів. Принцип їх дії полягає в наступному. Система контролю доступу за персональним кодом визначає доступні поверхи і під час спроби потрапити на будь-який поверх, що виходить з цього діапазону, блокує рух ліфта в заборонений сектор.

3.ОСОБЛИВОСТІ ВПРОВАДЖЕННЯ СКУД НА ФІРМІ «ELTA»

Фірма «ELTA» займається екологічними питаннями. Вперше необхідність установки СКУД на фірму з'явилася через те, що персонал не завжди закривав двері і, як наслідок, стали ходити сторонні люди і було скоєно кілька крадіжок особистих речей. Після первинного аналізу стало зрозуміло, що потрібно було обмежити вхід сторонніх осіб в службові приміщення. В даному розділі я розповім нелегкий шлях який ми пройшли і приведу приклади еволюції СКУД на фірмі. Так само буде проаналізовано економічний ефект, якого можна було б досягти, якби подібний аналіз, описаний в роботі, був зроблений раніше. Глибокий аналіз питання дозволив би зекономити гроші та заощадити час, що в певних ситуаціях, важливіше матеріальних витрат.

Перша помилка, якої було допущено, це рішення локального завдання, без розгляду глобальної проблеми. Це означає, що після усвідомлення необхідності впровадження СКУД нами не було враховано, що в подальшому нам може знадобитися система яка масштабується і може стати більш складною. На першому етапі була встановлена найпростіша автономна система на 1 двері, без можливості масштабування і віддаленого доступу.

Друга помилка. Фірма розвивалася і завдання, які потребували вирішення ставали все складнішими, нам довелося відмовитися від встановленої раніше системи. Було розроблено технічне завдання і відправлено його фірмі. Якась компанія, не називатимемо її назву, склала нам кошторис, після чого був підписаний договір на виконання робіт.

Система СКУД була вже більш складною, могла контролювати 6 точок, так само була присутня система обліку кадрів, що дозволяло вести моніторинг персоналу. За 6 місяців система почала давати збої. Було прийняте рішення викликати фірму-установника, яка в результаті не змогла зробити так, щоб система працювала нормально.

Помилка друга полягає в тому, що після складання технічного завдання необхідно проводити тендер на виконання робіт і дуже ретельно збирати інформацію про виконавця.

Помилка третя. Необхідно використовувати тільки якісне обладнання, яке має сервісні центри та гарантійні зобов'язання.

В результаті систему СКУД було демонтовано і прийняте рішення підійти більш серйозно до цього питання. Нижче будуть описаний поетапний план за яким ми розгортали нову систему. Так само буде описаний перелік організаційних заходів, які необхідно зробити на підприємстві.

Етап 1. Проектування системи для подальшої реалізації. На даному етапі було проаналізовано існуючі рішення і технології. Проведено обстеження об'єкту, надано оцінку доцільності, з урахуванням всіх структурних змін, що відбулися на фірмі. Спрогнозовано подальший розвиток проекту з урахуванням майбутніх змін. Проаналізовано ринок СКУД, наявні у кожного виробника технічні рішення і можливість інтеграції їх обладнання з різними системами.

Головним завданням стала оцінка можливості розподіленого функціонування системи за умови централізованого адміністрування.

На основі даних аналізу конфігурації і обстеження об'єктів сформульовані наступні вимоги, які є основою технічного завдання:

• змонтоване обладнання СКУД призначене для безперервної цілодобової роботи в режимі постійного зв'язку з сервером системи.

• максимальне число реєстрованих подій за одну добу - не менше 100000;

• середня щільність потоку подій - не менше 10 подій в секунду (для кожної події забезпечити прийом, обробку та реєстрацію в журналі подій);

• пікова щільність потоку подій - не менше 100 подій в секунду;

• максимальна кількість карт доступу - не менше 10000;

• створення звітів з конфігурації системи;

• створення звітів по всіх подіях, що відбувалися за будь-який проміжок часу;

• розмежування прав доступу;

• облік робочого часу і фіксація фактів запізнення співробітників зі складанням відповідних звітів (за сумарним часом за заданий період часу, за щоденним відпрацьованим часом, детальні звіти з входу і виходу), при цьому фільтри для складання звітів повинні містити дату і час часових періодів звітів, а також, такі поля з бази даних, як : відділ, прізвище, ім'я, по батькові, посада, номер картки;

• відображення фотографій всіх осіб, що ідентифікуються на зчитувачах точок доступу вхідних груп об'єкта (як «на вхід», так і «на вихід»), на моніторах поста охорони;

• нарощування і розширення системи без заміни центрального обладнання і ПЗ;

• автоматична перевірка режиму роботи СКУД для виявлення і корекції;

• створення звітів за подіями технічних засобів;

• санкціонований вхід і вихід в / із зони обмеженого доступу після ідентифікації особи.

Етап 2. Підбір обладнання та складання кошторису

Етап 3. Монтаж та налаштування обладнання. Для користувачів визначаються права доступу і вносяться відповідні обмеження адміністратором системи, за необхідності вносяться дані про прив'язку ідентифікатора, проводиться друк фотографії співробітника. Окрема категорія співробітників, що має доступ в режимні приміщення, надає біометричні відомості, які зв'язуються з карткою користувача.

Проводяться тестові випробування.

Етап 4. Тестування і обслуговування. Після настройки і тестування СКУД організована видача електронних ідентифікаторів користувачам.

Кожен користувач буде проінструктований про порядок використання електронних ідентифікаторів. Доведені вимоги пропускного режиму, порядку формування заявок на виготовлення нових ідентифікаторів і внесення змін в існуючі зони доступу.

Основними ризиками на даному етапі є:

- надання співробітникам невідповідного посадовим обов'язкам права доступу;
- помилки відповідності електронних ідентифікаторів користувачам;
- неможливість доступу в режимні приміщення через невірно введених біометричних даних.

Впровадження СКУД в організації багатостадійний процес, який не обмежується тільки технічними заходами. Більш того, без досить глибоко пророблені ідеології побудови системи не варто приймати технічні рішення. Розглянемо основні етапи побудови СКУД з точки зору організаційних заходів:

1. Усвідомлення потреби. Перш за все керівництво компанії має осмислити необхідність впровадження СКУД, проаналізувати завдання, які можуть бути вирішені завдяки використанню системи, оцінити рівень витрат на впровадження і експлуатацію і зіставити ці витрати з очікуваною вигодою. Така попередня оцінка може бути підставою як для прийняття принципового рішення про створення системи, так і для початкової вироблення технічних вимог.

2. Призначення відповідальних. Після прийняття принципового рішення дуже важливо визначити керівника / координатора проекту і синхронізувати його розуміння завдання з розумінням керівництва.

3. Постановка завдання на впровадження і вибір підрядника. Наступний крок - формальний опис задачі на підставі проведеного аналізу. Такий опис може являти собою короткий (на 2-3 сторінки) документ, що дозволяє потенційному підряднику оцінити перспективи участі в проекті і підготувати чорнову комерційну пропозицію. Під час побудови системи замовнику необхідно не допустити ключової помилки, коли вибір ідеології і технічної реалізації вибудовується «Від підрядника». Іншими словами, спочатку на горизонті з'являється «підрядник» (найчастіше, обраний суб'єктивно), який пропонує і, дуже часто, нав'язує ідеологію і технічні рішення, виходячи зі своїх можливостей і досвіду. При цьому такі рішення далеко не завжди є оптимальними в конкретній ситуації. Взагалі, вибір підрядника це один з

ключових моментів побудови будь-якої технічної системи, і СКУД тут - не виняток. Чим більш ретельно буде проведено процес вибору, тим менше проблем виникне під час реалізації проекту, і тим більше він буде відповідати початковим очікуванням. У державних структурах такий вибір здійснюється за допомогою тендера, що не завжди призводить до оптимального результату, оскільки визначальним критерієм є вартість. Проте, під час підготовки закупівельної документації необхідно детально прописати кваліфікаційні вимоги до учасником процедури. Варто приділити цьому етапу достатньо часу. Згодом це мінімізує ризик вибору несумлінного підрядника.

Процес вибору підрядника може виглядати наступним чином:

• обрання підрядників (3-7 компаній);

• ознайомлення підрядників з технічним завданням;

• взаємодія з підрядниками (ознайомлення з об'єктом, уточнення умов);

• розробка підрядниками комерційних пропозицій;

• аналіз комерційних пропозицій замовником;

• прийняття рішення на підставі комплексної оцінки.

4. Ухвалення проектної та кошторисної документації, укладання договору. Остаточно визначившись з виконавцем робіт з впровадження СКУД, можна приступати до безпосередньої взаємодії з ним. Взаємодія ця починається з детального коригування попередньо обумовленої схеми, уточнення концепції і конкретного обладнання. Під час обговорення ідеології системи, досвід підрядника може виявитися неоціненним, адже далеко не завжди замовник чітко уявляє, як буде функціонувати система, з якими нюансами йому доведеться зіткнутися в процесі експлуатації. Тому важливо на даному етапі отримати від підрядника максимально детальну інформацію. Не останню роль в уточненні специфікації обладнання, кількості і розташування точок доступу і, відповідно, переліку робіт, грає фінансове питання. Мінімізувати витрати можна не тільки шляхом зменшення обсягів устаткування і робіт, а й за рахунок деякого (некритичного) зниження якості або надійності обладнання. На цьому ж етапі проговорюються місця розміщення центрального, кінцевого і

допоміжного обладнання. Не менш важливо приділити увагу документальному оформленню прийнятих рішень. В процесі обговорення може здатися, що сторонами досягнуто повне взаєморозуміння, і необхідність в детальному документуванні прийнятих рішень відсутня. Однак, така ситуація може доставити масу неприємностей, якщо досконально не зафіксувати всі домовленості документально. Немає нічого більш болісного для замовника, ніж працювати за формальною угодою або взагалі без нього. Такі речі зазвичай знижують загальну початкову вартість системи, але можуть значно збільшити її вже в процесі монтажу. Як правило, всі технічні особливості проекту прописуються в ТЗ. Технічне Завдання може бути, як окремо на проектування, так і на систему в цілому. Зазвичай ТЗ пише виконавець робіт і погоджує його із замовником у вигляді додатку до договору. Така ситуація є логічною, оскільки підрядник за визначенням професіонал в цьому питанні. Завдання замовника тут - не піддатися спокусі формального вивчення ТЗ і докладно перевірити документ на відповідність затвердженим рішенням.

Після затвердження проекту, до початку монтажних робіт, необхідно вирішити ряд організаційних моментів:

• приміщення для монтажників (якщо великий обсяг робіт);

• тимчасовий склад для обладнання. Забезпечення збереження обладнання (якщо багато обладнання);

• питання допуску монтажників на об'єкт і контролю;

• питання оперативної взаємодії з бригадою монтажників і головною організацією;

• координація взаємодії монтажників і персоналом, що експлуатує об'єкт підрозділу.

5. Контроль монтажних робіт. Паралельно з супроводом робіт з монтажу обладнання, доцільно почати розробку внутрішніх регламентуючих документів. Навіть якщо в компанії вже діє Регламент контрольно-пропускного режиму, обов'язково необхідно внести в нього зміни, що стосуються СКУД.

6. Розробка внутрішніх нормативних документів і регламентів. Розробка регламенту пропускного режиму в компанії індивідуальний процес, але, в будь-якому разі, в ньому повинні бути відображені такі пункти :

• цілі і завдання;

• точки доступу;

• порядок призначення рівнів доступу;

• порядок видачі перепусток;

• порядок видачі гостьових перепусток;

• порядок вилучення перепусток;

• дії при втраті перепустки;

• нештатні ситуації;

• форми заявок, зовнішній вигляд перепусток, форми звітних документів.

7. Пуско-наладка і введення системи в експлуатацію. Після завершення монтажних робіт підрядник проводить пуско-наладку системи. На цьому етапі необхідно щільно підключити до процесу співробітників, які будуть безпосередньо експлуатувати систему. Співробітники повинні пройти теоретичне навчання, а також, беручи участь в процесі пуско-налагодження, набути практичних навичок. На цьому ж етапі проводиться введення бази даних співробітників в систему, призначення рівнів доступу, прив'язка рівнів доступу до конкретних співробітникам, виготовлення перепусток, видача перепусток співробітникам.

ВИСНОВКИ

Ідентифікація особистості є одним з ключових заходів у забезпеченні безпеки з сучасному форматі ведення бізнесу. Незважаючи на актуальність цього завдання і існування різних технічних рішень в області СКУД, не всі вони можуть комплексно і якісно виконати поставлене перед ними завдання. Так само спостерігається недоліки представлених в літературі методичних рекомендацій, програмного та алгоритмічного забезпечення процесу ідентифікації відвідувачів, що може привести до неправильного вибору системи СКУД і як наслідок може привести до фінансових і часових втрат підприємства.

Правильне впровадження СКУД на підприємствах / фірмах дозволяє вирішити такі завдання:

• контроль і управління доступом на підприємство і його об'єкти;

• можливість обмеження доступу співробітників на підприємство не в свою зміну;

• автоматичне анулювання перепусток персоналу, що більше не працюють на підприємстві;

• точні дані про персонал під час аварій інформаційно забезпечує реалізацію плану ліквідації аварійних ситуацій шляхом своєчасного надання точних і об'єктивних даних про місцезнаходження персоналу на робочих місцях. Візуалізація пересування працівників по території підприємства дозволяє відстежувати вихід людей з небезпечних зон в режимі, наближеному до реального часу;

• облік та контроль робочого часу персоналу.

В роботі була проведена класифікація СКУД, зроблений їх детальний аналіз, виявлені переваги і недоліки, які необхідно враховувати під час вибору таких систем.

Автором описано досвід впровадження таких систем на фірмі «Elta».

Поставлена задача в атестаційної роботи виконана в повному обсязі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. М.: Горячая линия Телеком, 2015. 272 с.

2. Сорокин К. Применение биометрических технологий в обеспечении информационной безопасности бизнеса. //СКУД. Антитеррористм-2013 2013 С. 46-47.

3. Тихонов О.О., Малышева А.С., Шаповалов А.В., Гамбург А.Е., Стасенко Л.А, Курилин А.С. Функции универсальных СКУД: что нужно потребителю. //Системы безопасности 2011 № 4. С. 108-119.

4. Не типичные функции СКУД URL: http://www.secuteck.ru/articles2/sys_ogr_dost/netipichnye-funktsii-skud/
Система контроля и управления доступом. Принцип действия [Электронный ресурс]. – Режим доступа: http://www.intersyst.ru/solutions/165/460/свободный.
Обзор возможностей СКУД [Электронный ресурс]. – Режим доступу: http://www.sistema-dostupa.ru/i03.htm/вільний.

5. ГОСТ Р 51241-2008. «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».

6. ГОСТ Р 54831-2011 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний. – М. : Стандартинформ, 2012. – 16 с

7. Портал «RTLService» - «Принцип работы RFID и ее применение» / Электронные текстовые данные, рис., табл. URL:https://rtlservice.com/ru/company/blog/princip_raboty_tehnologii_rfid_i_ee_primenenie/свободный.

8. Портал «Scanberry». - «Принцип работы RFID и ее применение» / Электронные текстовые данные, рис., табл. URL: https://scanberry.ru/news/perenosnye-rfid-schityvateli-i-skanery/свободный

9. Портал «ИСТОК» - «Принцип работы RFID и ее применение» / Электронные текстовые данные, рис., табл. URL: https://stc-istok.com.ua/-/stati/chto-takoe-rfidсвободный

10. Портал «Молодой ученый» - «Принципы построения систем радиочастотной идентификации / Электронные текстовые данные, рис., табл. URL:https://moluch.ru/archive/115/30590/ свободный

11. Царьов Р.Ю. Біометричні технології: навч. посіб. для вищих навчальних закладів / Р.Ю. Царьов, Т. М. Лемеха. – Одеса: ОНАЗ ім. О.С. Попова, 2016. – 140 с.: іл.

12. Быков О. Что надо знать, заказывая карты Mifare для СКД / О. Быков // Алгоритм безопасности. – 2011. – № 4. – С. 40–41.

13. Быков О. Перевод СКУД с карт EM MARIN на карты MIFARE® : полезные сведения для владельца объекта СКД / О. Быков // Avtoritet.Net. – Электрон. дан. – [Б. м.], 2014. – URL: http://avtoritet.net/library/press/245/8158/articles/8745

14. Портал «Электросам». - «Электромеханические замки » / Электронные текстовые данные, рис., табл. URL: https://electrosam.ru/glavnaja/jelektrooborudovanie/ustrojstva/elektromekhanicheskie-zamki/ свободный

15. Портал «VeryDveri». - «Электромеханический замок для двери и калитки. оптимальный выбор и принцип установки» / Электронные текстовые данные, рис., табл. URL: https://verydveri.ru/furnitura/elektromexanicheskij-zamok-dlya-dveri-i-kalitki.htmlсвободный