**Глава 1. Състояние на проблема по литературни данни**

* 1. **Представяне на системите за контрол на достъп**

Системите за контрол на достъп (СКД) имат за цел да ограничат достъпа до даден ресурс. В зависимост от ресурса може да говорим за ограничение на достъп до софтуерни данни или ограничаване на физическия достъп до даден ресурс. Тъй като двете системи се различават коренно в своите принципи на работа текущата дипломната работа има за цел да изгради СКД до физически ресурс. В най – общата си форма една СКД се състой от следните компоненти: четец, идентификатор, механизъм за ограничаване на достъпа, контролен панел и система взимаща решения за контрола на достъп.

**Идентификатори**

Идентификатора представлява физически обект, парола, биометрични данни на дадено лице или даден вид информация нужна за да се даде достъп до ресурс. Според вида и начина на доставяне на информацията това може да са както следва и не само:

* **Биометрични**: пръстов отпечатък, отпечатък на ръка, лицево разпознаване, разпознаване на ириса на окото, сканиране на ретината на окото, гласово разпознаване.
* **Информация**: пин код, комбинация от числа и букви (парола).
* **Контактни карти**: Карти с магнитна лента, Smart карти.
* **Безконтактни карти**: RFID / NFC базирани карти.
* **Други**: баркод.

**Четци**

Четеца представлява входно устройство за данни, което има за цел прочитане на данните от идентификатор и предаването им на системата за взимане на решение за контрола на достъпа. Вида на четеца се разделя на две основни групи - в зависимост от вида на данните, които се четат и според функционалностите на четеца.

**Четци според вида данни**

* **Баркод**: комбинация от редуващи се светли и тъмни райета (1D - едномерни), които се обработват от оптичен четец. Информация, която носят е на основата на морзов код, но вместо точка и запетая имаме тесни и широки райета. QR кодовете (2D - двумерни) представляват разновидност на баркодовете при които информацията е кодирана под формата на тъмни квадрати на бял фон, като информацията е кодирана както по вертикала, така и по хоризонтала.
* *предимства*: лесен и евтин начин за генериране на идентифициращ елемент, както и лесното му интегриране върху различен набор от предмети.
* *недостатъци*: ниска сигурност, лесен начин за дублиране на реални баркодове, както и генериране на фалшиви.
* **Биометрични:** сканиране на физически атрибут на дадено лице. Сканирането генерира модел, който бива сравнен с образец. Има два режима на работа – 1-към-1 (1-to-1) или 1-към-много (1-to-many). При 1-към-1 освен сканиране на физически атрибут, потребителя е длъжен да въведе парола или да се идентифицира с карта. Сканирания модел бива сравнен с образец асоцииран с паролата – по този начин се постига голямо бързодействие, тъй като модел бива сравнен само с един образец, постига се и по – висока сигурност заради допълнителния начин за идентификация. При 1-към-много сканирания модел се сравнява с всички образци (често равен на броя на потребителите).
* *предимства*: висока сигурност, елиминиране на възможност за изгубена карта, забравена парола, карта дадена на заем
* *недостатъци*: при 1-към-много режим на работа имаме сравнително бавна обработка – сравнение на до 3000 модел за секунда.
* **Информационни**: четеца е снабден с клавиатура, която се използва за въвеждане на нужната информация (най – често парола).
* *предимства*: евтина цена за разработка, лесно програмируема
* *недостатъци*: забравена парола, ниска сигурност
* **Карти с магнитна лента**: картата има магнитна лента изградена от метални частици. Информацията се записва чрез промяна на магнитите свойства на тези частици, като магнитната лента се състой от три пътеки и всяка може да бъде кодирана по различен начин. В четеца има бобина (solenoid) и при физически контакт между картата и четеца се индуцира напрежение.
* *предимства*: евтина цена за изработка, лесно програмируема
* *недостатъци*: податливи на износване, грешно прочитане на информация, широкото им разпространение и стандартизираните подходи на кодиране на информация е довело да изграждането на устройства, които се поставят върху оригиналния четец с цел прочитане на данните.
* **Wiegand**: Името идва от така наречения Wiegand ефект (на името на откривателя John R. Wiegand). Ефекта се наблюдава при жичка направена от феромагнитна сплав между кобалт, желязо и ванадий. Самата жичка е направена от по – твърда обвивка с висока корцетивност и ‚мека‘ сърцевина. Ефекта се изразява в това, че при прилагане на магнитно поле външната обвивка предпазва сърцевината от намагнитване до достигна на магнитния праг (magnetic threshold) на външната обвивка – при което цялата жичка (сърцевина и външна обвивка) променят своята полярност на магнетизацията. В картите са разположени Wiеgand жички по такъв начин, че да се генерира уникален идентификационен код, а в четеца от своя страна има бобина в която се индуцира напрежение, при възникване на Wigand ефекта, което може да бъде анализирано от друго устройство в последствие. Тъй като Wigand четците биват силно разпространени в даден момент във времето, но заради масовото навлизане на безконтактните карти впоследствие, начина им на интегриране с останалата част от системата се запазва и оформя като стандарт наричан още Wiegand interface / protocol с цел новите четци да са съвместими с вече изградените системи.
* *предимства*: тъй като жичките са вградени в картата тук няма износване, трудно дублиране - висока сигурност
* *недостатъци***:** изместени от безконтактните четци заради по – добрата устойчивост на външна намеса и удобството на безконтактната карта
* **Безконтактни** – четеца и картата комуникират чрез радио вълни на определена честота в зависимост от нуждите (скорост и обем на четене на данните, разстояние между идентификатора и четеца). Картите се разделят на два основни вида според начина на комуникация – активни и пасивни. Четеца и картата комуникират чрез принцип наречен индуктивно-резонансен пренос на енергия. Пасивните карти имат три компонента, които са вградени в самата пластика на картата – антена направена под формата на бобина, кондензатор и интегрална схема, която съдържа идентификационната информация в определен формат. Четеца също има антена, която непрекъснато излъчва радио вълни. Когато картата е поставена в обхвата на четеца бобината и кондензатора на карата поглъщат и съхраняват енергията от полето. Тази енергия се обръща до постоянен ток, който захранва интегралната схема. Интегралната схема изпраща информацията, която е съхранена на нея до антената, която изпраща от своя страна информацията то четеца посредством радио вълни. При активните имаме литиева батерия служеща като източник на енергия. Интегралната схема съдържа приемник, който използва батерията за да усили сигнала, също така предавателя използва батерията за да усили сигнала от карата, което позволява комуникация от по – голямо разстояние.
* *предимства*: комуникация от разстояние, възможност за пренос на голям обем данни, протоколи за работа с няколко карти наведнъж.
* *недостатъци***:** възможност за не-оторизиран достъп до данните на картата от разстояние

**Четци според функциите, които изпълнява**

* **Основни (не-интелигентни)**: разчитат идентификатора и предават информацията към контролния панел, не се грижат взимането на решение за контрола на достъп, също така, не отговарят за осъществяването на контрола. Най – често се използва Wiegand протокола за пренос на данните до контролния панел, но има и алтернативи като RS-232, RS-485. Това са най – разпространените видове четци.
* **Полу-интелигентни:** освен разчитането на идентификатора, те разполагат и с всички механизми нужни за осъществяването на контрола на достъп, но не взимат решение са самия достъп. След прочитане на идентификатора информацията се изпраща до контролен панел, който взима решението за контрола на достъп. За комуникацията между четеца и контролния панел най – често се използва RS-485. При проблема комуникация между двете устройства, четеца спира да работи.
* **Интелигенти:** освен разчитането на идентификатора, те разполагат с всички механизми нужни за осъществяването на контрола на достъп както полу-интелигентните четци, освен това притежават памет и процесор, което им позволява да взимат решения относно контрола на достъп. Свързани са към контролен панел посредством RS-485. Ролята на контролния панел е да синхронизира периодично информация за потребителните от сървъра с тази в четците. По – този начин при проблем при комуникацията между четеца и контролния панел, четеца ще продължи да работи.
* **IP:** IP четците са вид интелигентни четци, като основната разлика при тях е липсата на контролен панел. Комуникират директно със сървъра на базата на Ethernet или Wi-Fi.

**Механизъм за ограничаване на достъп**

Механизъм за ограничаване на достъпа. Когато говорим за контрол на достъп до помещение това би бил механизъм за отключване и заключване на врата, който бива управляван директно от четеца или от контролен панел.

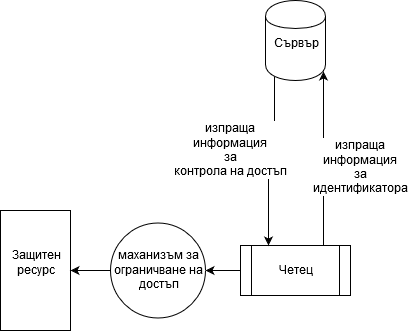
**Система взимаща решения за контрола на достъп**

Устройство, което служи за съхранение и манипулиране на база данни или дава възможност за комуникиране с такава база данни и възможност за сравнение на информация за идентификация спрямо тази в базата данни и предаването на резултат от сравнението посредством даден протокол за комуникация.

**Топология**

След прочитането на идентификатора, четеца изпраща информацията за сравнение с база данни. Сравнението може да бъде направено от сървър, контролен панел или от самия четец. Информацията от сравнението се връща обратно до устройство, което контролира достъпа било то контролен панел или четец. В зависимост от резултата от сравнението потребителя получава съответното ниво на достъп или му бива отказано такова.

Обмяната на информация се осъществява чрез дадена среда за разпространение, съответния протокол за комуникация и стандарт за кодиране на данните.

  
Фигура 1. Базова топология на система за контрол на достъп с централен сървър.

* 1. **Представяне на RFID Arduino базиран четец и сървърна част с комуникация посредством Wi-fi**

**Arduino**

Електрона система специализирана в изграждането на програмируеми едноплаткови микро-контролери. Всяко устройство е снабдено с аналогови и цифрови щифтове (pin) за комуникация с външни устройства, сензори и др. Програмирането се извършва на езиците C / C++ в специализирана среда за разработка (IDE) – Arduino IDE. Към този момент за самата платформа има готови решения за RFID четец и Wi-Fi модул позволяващ връзка със съществуващи мрежи или изграждането на нова такава, и програмни библиотеки с отворен код за тяхното управление, които са използвани в текущата дипломна работа.

**Сървър (база данни, API, обслужващ website)**

Сървъра представлява компютър с определени минимални hardware-ни изисквания нужни за осигуряване на нормалната работа на услугите, които обслужва. В контекста на една система за контрол на достъпа, която използва Wi-Fi комуникация това са най - често база данни, REST API и обслужващ website.

* **База данни**: най – общо представлява стандартизиран начин за работа с данни. Наложи ли се като стандарт във времето те са един основните подходи за съхранение на състоянието на едно приложение върху носител с цел запазването му до следваща нужда. В днешно време когато говорим за база данни най – често се има предвид услуга или сервиз под формата на програмен продукт със стандартизиран начин за работа. В контекста на система за контролиране на достъпа в една база се паси информация за потребителите, нивото им на достъп и различни събития. Най – популярни са: Microsoft SQL Server, MySQL, Oracle Database, MongoDB, SQLite.
* **REST API**: стандарт за работа с ресурси под формата на web услуга. Под ресурс се разбира всяка единица информация, която може да бъде идентифицирана, адресирана или именувана. Най – често един ресурс се идентифицира със своя адрес (URI). Стандарта използва HTTP протокола, като го надгражда с едно основно ограничение - stateless (без състояние) режим на работа. В днешно време под REST API се разбира програмен продукт обслужван от web сървър на определен адрес и набор от услуги предоставени на клиента под формата на под адреси на дадения домейн. Пример за адрес на REST API <http://example.com> и адрес на услуга [http://example.com/api/article/1 където домейна е example.com](http://example.com/api/article/1%20където%20домейна%20е%20example.com). В контекста на система за контролиране на достъпа четеца би се обърнал към REST API-то за да провери дали текущия потребител има нужните права за да достъпи даден ресурс.
* **Website**: група от ресурси под формата на адреси (URI) под общ домейн, публикувани на web сървър. За достъп до website-а се използва HTTP протокола. Основната градивна единица на един website е така наречената web страница. Тя представлява документ в текстов формат, най – често HTML. Най – често един **website** има начална страница и навигационна част за достъп до останалите страници и може да изпълнява разнообразни операции като предоставяне на информация за четене, сваляне на различни документи, извършване на банкови операции и много други. В контекста на система за контролиране на достъпа website-а би имал за цел да предостави на потребителя лесен и удобен начин за администриране на базата данни под формата на различни операции като: отнемане право на достъп на даден потребител, изтриване на информацията за потребител, генериране на справки и много други.
  1. **Защо Arduino базиран четец и Wi-Fi комуникация ?**

В днешно време най – разпространени решения са напълно автономните четци, които съдържат в себе си база данни и сами взимат решението за контрол на достъп. Най – често работят с парола или RFID чип. Те се ползват предимно в сгради с единствен вход. Един от основните недостатъци на тези решения, е че не предлагат никакъв анализ на данните.

Другия вид широко използвано решение е четец свързан към IP контролен панел, който от своя страна комуникира със сървър. Това решение е по – подходящо за сгради с в повече от един вход, също така тези решения предлагат възможност за анализ на данните като много често това е под формата на услуга, която се заплаща допълнително. Недостатъка на тези решения е нуждата от LAN окабеляване между контролера и сървъра. Нуждата от контролен панел също може да бъде разгледана като недостатък заради допълнително оскъпяване и централизацията на потока на данни – ако контролера бъде повреден всички четци свързани към него спират да работят.

Предимствата на Ардуиното са голямата модулност, което позволява по – качествено преизползване на отделни компоненти например: лесно заменяне на Wi-Fi модула без да се налага промяна по модула за RFID четеца или пък смяната на RFID четеца с биометричен без да се налага смяна на Wi-Fi модула. Друго предимство е лесното управление и ниската цена.  
Wi-Fi комуникацията решава проблема с LAN окабеляването както и възможността за преизползване на вече изградени такива мрежи.