

**УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ**

**КАТЕДРА “ИНФОРМАЦИОННИ СИСТЕМИ И ТЕХНОЛОГИИ”**

**БАКАЛАВЪРСКА ПРОГРАМА**

**“ИНФОРМАЦИОННИ СИСТЕМИ И ТЕХНОЛОГИИ”**

**КУРСОВ ПРОЕКТ**

на тема:

**ПРОЕКТИРАНЕ И ИЗГРАЖДАНЕ НА СИСТЕМА ЗА КОНТРОЛ НА ДОСТЪП**

**Дипломант:** **Научен ръководител: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Борис Божилов (проф. д.н. И. Гарванов)

редовно обучение

Ф № 46261р

София

2022 г.

**РЕЗЮМЕ**

Божилов, Б. Проектиране и изграждане на система за контрол на достъп.

Научен ръководител проф. И. Гарванов. София 2022.

Катедра «Информационни системи и технологии». Бакалавърска програма

” Информационни системи и технологии”. УНИБИТ. 30 с. Брой източници – 8, приложения – 0.

Целта на настоящата разработка е да се разгледат съвремените системи за контрол на достъп, в различните аспекти на тяхното приложение както и стъпките при проектиране и изграждане на една такава система с нейните специфики.

От поставената цел произтичат следните задачи:

* Да се анализират различните технологии, които се използват в изграждането на такива системи като и спецификите, които налагат различните сфери на приложение
* Да се изложи основната идея и проектира една система за контол на достъп за нуждите на разни потребители
* Да се представи един частично разработен прототип на софтуерно решение в областта на контол на достъп и евиденция за присъствие

Настоящия курсов проект е разработена в Увод, 3 глави и Заключение.

В глава I са анализирани различните технологии за реализация на система за контрол на достъп, където са изтъкнати положителните и отрицателните страни на всяка една от тях, и въз основа на този анализ е избрана технология за реализация на системата.

В глава II е представена основната идея за системата, структурата на системата, хардверната платформа и допълнителния хардуер както и различни възможности за разширяване на основната система.

В глава III е представена вече реализираната функционалност на софтверната разрабока и идеите за по-нататъшното разширяване на функционалността на софтуера

В заключението са изтъкнати възможностите за раелизация на система за контрол на достъп с избраната технология и платформа постигнатите резултати, обобщени са направените анализи и изводи. Посочени са перспективите за по-конкретно прилагане на системата.

Ключови думи: система, контол на достъп, евиденция за присъствие

Съдържание

[УВОД 5](#_Toc93835249)

[I. СИСТЕМИ ЗА КОНТРОЛ НА ДОСТЪП 6](#_Toc93835250)

[1. Най-често исползвани технологии 6](#_Toc93835251)

[1.1. Контрол на достъп чрез въвеждане на ПИН код 7](#_Toc93835252)

[1.2. Контрол на достъп с RFID технология 8](#_Toc93835253)

[1.3. Биометричен контрол на достъп 10](#_Toc93835254)

[1.4. NFC контрол на достъп 11](#_Toc93835255)

[2. Избор на технология за изграждане на системата 12](#_Toc93835256)

[II. ПРОЕКТИРАНЕ НА СИСТЕМАТА ЗА КОНТРОЛ НА ДОСТЪП 13](#_Toc93835257)

[1. Мащабиране на системата 14](#_Toc93835258)

[2. Статистически функции 15](#_Toc93835259)

[3. Технология, хардуер, системен софтуер и инфраструктура 15](#_Toc93835260)

[4. Структура на системата 18](#_Toc93835261)

[5. Система за софтуерна поддръжка 21](#_Toc93835262)

[III. ИЗГРАЖДАНЕ И РАЗШИРЯВАНЕ НА СИСТЕМАТА 23](#_Toc93835263)

[1. Разработка на софтуера за контролния модул 23](#_Toc93835264)

[2. Разработка на административния модул 25](#_Toc93835265)

[2.1. Формата Institutions 26](#_Toc93835266)

[2.2. Формата Users 26](#_Toc93835267)

[2.3. Формата Attendance 27](#_Toc93835268)

[2.4. Формата Monthly report 28](#_Toc93835269)

[3. Визия за развитие на системата 28](#_Toc93835270)

[ЗАКЛЮЧЕНИЕ 29](#_Toc93835271)

[ЛИТЕРАТУРА 30](#_Toc93835272)

# УВОД

Системите за контрол на достъпа са все по-неразделна част от модерния бизнес и дом. В тази разработка ще разкажем за предимствата, ефективността и проложението на системите за контрол на достъпа.

Основните предимства на тези системи са по-голямо удобство и максимална защита и сигурност. В приложението си често се комбинират с евиденция на присъствие. Всъщност разликата обикновено е в софтуерната добавка за следене на работното време (присъствие).

Системата за контрол на достъпа и евиденция за присъствие е важен аспект от техническата защита, в която са обикновено интегрирани две подсистеми, които почти винаги вървят заедно, а те са:

* Контрол на достъпа
* Евиденция за присъствие

Като техника основното е, че контролираният достъп може да бъде едностранен – само за вход или само изход. От друга страна, за да сработи евиденцията за присъствие е нужно да имаме входна точка (начано на присъствие/начало на работния ден) и изходна точка (край на присъствие/край на работния ден).

Така интегрирани, двете подсистеми повишават производителността и ограничават злоупотребите от страна на потребителите (персонал, посетители, студенти и пр).

# СИСТЕМИ ЗА КОНТРОЛ НА ДОСТЪП

Контролът на достъпа е част от общата система за сигурност и често е интегриран с оборудване за видеонаблюдение и с оборудването за алармената сигнализация. Системите за контрол на достъп и евиденция за присъствие са необходими, за да се регламентира достъпа до определени зони от обекта и да се автоматизира процеса на евиденция за присъствие.

## Най-често исползвани технологии

Системите за контрол на достъп и отчитане на работно време включват всички необходими механизми, изпълняващи физическо ограничаване на достъпа. Те представляват комплекс от специализирани хардуерни и софтуерни компоненти, което позволява да се удовлетворят специфичните изисквания за всеки обект. Самия процес на оторизация на потребителите се върши с различни технологии които са се развили във времето или с техни комбинации. Тук ще опишем няколко од тях.

### Контрол на достъп чрез въвеждане на ПИН код

Една от най-древните и често използвани технологии за оторизация е чрез въвеждане на уникална поредица(PIN) от цифри чрез клавиатура. Конкретният код се присвоява на съответен служител и така той се идентифицира от системата.

*Фигура 1 - Клавиатура за въвеждане на PIN код за достъп*

**Положителни страни**

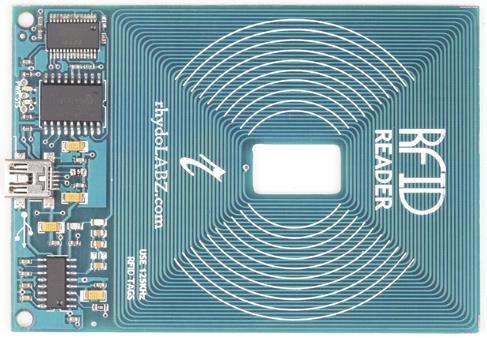
* евтини устройства за оторизация
* висока разпознаваемост на технологията от персонал, посетители и др.
* надеждност и лесна администрация

**Отрицателни страни**

* лесно открадване на кода - чрез визуално наблюдение (напр. Група потребители чакащи да се оторизират и гледащи в клавиатурата), чрез поставяне на различни физически устройства на клавиатурите (разпространено при банкоматите) и др.
* лесно преотстъпване на кода на друго лице с цел заблуда на системата или проникване на едновременно няколко лица с един и същ код (може да се развие софтуерно решение за избягване)
* необходимост от физически достъп до устройството (амортизация, климатични влияния, опасност от вандалщина)
* Както ще научите по-нататък този способ за оторизация все още не е мъртъв, тъй като се използва като комбинация от по-иновативни методи или при критичен отказ на някои от по-напредналите технологии.

### Контрол на достъп с RFID технология

Технология за оторизация чрез радио сигнал от малки разстояния. Принципът е доста прост - активно устройство (четец), което създава определено електромагнитно поле в малък диапазон (5-10 см) и безконтактна карта (има и ключодържатели, пръстени и др.), която е пасивна. Когато картата попадне в полето на четеца, излъчва собствен сигнал, който след декодиране се преобразува в код за достъп.



***Фигура 2 - RFID четец USB ) и карта за достъп (125Khz)***

**Положителни страни**

* ниска амортизация на четците, възможност за изнасяне само на антената на открито
* лесно боравене със системата
* надеждност и лесна администрация
* възможност за допълнителна клавиатура за PIN контрол
* възможност за печат върху картите и тяхното обозначаване - на служител, по групи (служители, посетители, отдели и др.)

**Отрицателни страни**

* сравнително скъпа технология
* допълнителни разходи по подмяна на карти за напускащи/постъпващи служители и други категории ползващи
* влияние от електромагнитни излъчвания
* възможност за повреда на картата (огъване, пречупване)
* възможност за загубване
* възможност за преотстъпване картата на друго, неоторизирано лице (може да се предотврати със софтуерно решение за заснемане на лицето в момента на влизане)

### Биометричен контрол на достъп

Една от най-авангардните технологии за контрол на достъпа е чрез използване на биометрични данни снети от лицето заявяващо достъп - пръстови отпечатъци, ирис на окото, лицев профил и др. По разбираеми причини (техническа сложност и себестойност) най-масово се използва метода за сравняване на пръстови отпечатъци посредством четец с вграден скенер.



*Фигура 3 - Биометричен контрол на достъп с прстов отпечатък*

**Положителни страни**

* лесна и бърза оторизация
* най-висока степен на надеждност при установяване на самоличността
* невъзможно е преотстъпването на биометрична информация
* авангардно и престижно решение

**Отрицателни страни**

* скъпа и технологично сложна система
* сложно администриране и въвеждане на първоначални данни
* сравнително висока норма на амортизация на скенерите и четците
* капризна по отношение на метереологични влияния (влага, температура и др.)
* необходимост от резервен вариант за оторизация (най-често PIN номер) при нарушена цялост

### NFC контрол на достъп

Според редица специалисти еволюционен наследник на RFID е NFC (Near Field Communication) технологията, интегрирана в модерните мобилни телефони, която създава нов универсален интерфейс и дава възможност за запълване на пропуските между съществуващите технологии и устройства чрез нови приложения и услуги.

Разработката на NFC е базирана на съществуващите безконтактни стандарти, които от доста време се използват всекидневно от милиони хора по света. Предназначена е изключително за употреба с мобилни телефони.



*Фигура 4 - NFC технологията, интегрирана в модерните мобилни телефони*

**Положителни страни**

* висока скорост на данните
* възможност за запазване на настройките на NFC етикетите на смартфона и тяхното автоматизирано и незабавно приложение;
* възможността да се използва карта NFC като визитна картичка или пощенска картичка;
* пренос на данни между две устройства, използващи P2P протокол;
* бърза настройка на NFC чипове с опции на системата;
* Възможност за използване на NFC, дори ако чипът не е в смартфона (с някои ограничения).

**Отрицателни страни**

* Максималното разстояние за пренос на данни е строго регулирано и изключително малко;
* възможност за достъп до данни при предаване чрез пресичане на сигнала;
* прекъсване на предаването, при използване на обичайната клетъчна комуникация.

## Избор на технология за изграждане на системата

Съпоставяйки положителните и отрицателните страни на изброените (най-чести) технологии за контрол на достъп, за изграждане на нашата система избираме RFID технологията. Избора е направен поради следните предимства на избраната от нас технология:

* Съвременните системи за контрол на достъп могат лесно и ефективно дабъдат внедрени с помощта на RFID технология.
* Безконтактните RFID карти са отдавна познати и широко използвани средства за контрол на достъпа в административни, обществени, корпоративни, жилищни и производствени сгради.
* Създаването на система за контрол на достъп, контролирана от четци за карти и чипове, е изключително ефективен начин за управление на посещенията в сграда, както и проследяване на присъствие (фирмен и хоноруван персонал, посетители, студенти и пр.). Системата изгражда ефективен пропускателен режим чрез удобна и модерна безконтактна радиочестотна технология.

# ПРОЕКТИРАНЕ НА СИСТЕМАТА ЗА КОНТРОЛ НА ДОСТЪП

Контрол на достъпа в общи черти означава отваряне на електромагнитната ключалка на дадено устройство за възпрепятстване на достъп (врата, разни видове бариери и пр.) само за лица, на които е разрешен достъп до определени (важни) помещения. Подсистемата трябва да има и функция за регистриране на опити за неоторизиран достъп, като и наличие на информация за пространствени и часови зони, в които различните потребители имат различни права. В съчетание с камера, която записва момента на регистрация се решава проблема със злоупотреба с карти т.е. регистрация с чужда самоличност.

Едновременно с контрола на достъпа могат да се водят записи за присъствие на дадено лице на определено място и време. Еевиденцията за присъствие, трябва да има редица функции, като: регистрация на влизане и излизане на всеки потребител, преглед на влизания и излизания, престой, евиденция на закъснения, самоотлъчване и извънреден труд на заетите и пр.

Системата като цяло трябва да има администраторска част за добавяне и изтриване на потребители, определяне на техните права във времевата и пространствена компоненти. Покрай правата за достъп до определени пространствени физически ресурси (зали, помещения и пр.), както достъпа, така и присъствието могат да имат времеви компонент, т.е. те могат да се разрешават постоянно в продължение на 24 часа, 7 дни в седмицата 24/7, или в определен период от време, който може да се повтаря ежедневно или да бъде определен по друг график.

Администраторската част на системата трябва да има възможност за генериране и отпечатване на разни видове отчети.

Независимо от възприетата динамика на системата, основното изискване е системата да работи напълно автономно, без никаква допълнителна намеса от страна на служители, освен когато става въпрос за промяна на структурата на системата и администрация.

## Мащабиране на системата

Системата трябва да бъде модуларна, за да може да се мащабира и се прилага, както в малки предприятие и ведомства с няколко десетки потребители така и по-голями публични институции с голям брой служители или потребители, когато е необходимо:

* избирателно одобрение или забрана за достъп до помещенията на физически лица, като може да се вземе предвид и времето, т.е. достъпът може да бъде разрешен или забранен за определен период от време
* регистрация на лица, така че да е възможно да се следи движението на хора, за да се получи информация къде се намира дадено лице в момента, дали присъства в съоръжение, в коя стая се намира в момента и подобни.
* да се получават различни статистически показатели за определен период от време, свързани с честотата на използване на помещенията, продължителността на престоя, селективността на използване на помещенията от различни лица и др.
* евиденция на работното време на служителите.

В академичните институции тази система би могла да се използва полезно за:

* обективно регистриране на присъствието на студенти и служители на лекции, упражнения, съвети, събрания и други обществени събирания, където е важна точната представа за броя и структурата на присъстващите
* проста автоматизация и поглед върху ефективното използване на лабораторните и други ресурси от студенти и служители, които имат дадени права.

## **Статистически функции**

Системата ще генерира голямо количество данни по време на работа, така че в допълнение към основната си функция да регулира достъпа и върши евиденция за присъствие на лица, статистическият анализ на събраните данни може да осигури показатели за натоварването и използването на помещения, ресурси, потребители (служители, студенти) които са полезни за по-добра организация на графика за използване на помещенията и ресурси, както и за съставяне на оптимален работен график на служителите.

## Технология, хардуер, системен софтуер и инфраструктура

Системата за контрол на достъпа и евиденция на присъствие, описана в тази разработка, ще се основава на използването на технологията RFID (Радиочестотна идентификация). RFID картатите са пасивни и получават енергия за работа от електромагнитното поле на четеца.  RFID четците са устройства, които се използват за предаване на електромагнитни полета към картата, комуникация с картата, както и аудио-визуална индикация, че картата е разчетена правилно.

Системата, бидейки разработвана предимно за учебни цели, ще бъде изградена от PC хадуер с общо предназначение, широко достъпен на пазара по относилтелно ниски цени, базиран на операциона система МS Windows 10.

Контолните модули ще се състоят от Mini PC компютри, оборудвани с USB RFID четци на 125kHz, USB уеб камери, стандартни HID клавиатури с един програмируем бутон (като входящи устройства) и програмируеми релета и електромагнитни ключалки (като изходящи и испълнителни устройства).

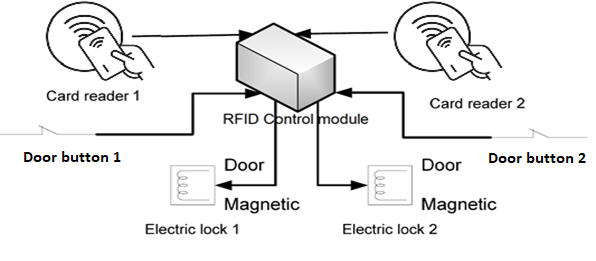
На контолните модули (Mini PC) е предвидено да се изпълнява специално разработено клиентско (Winforms или WPF) приложение, разработено на C#, което всъщност реализира котрола на достъп, проверявайки за дадените права на всеки потребител, регистрира влизане и излизане, както и опити за неоторизиран достъп. В съчетание с камера, която записва лицата в момента на регистрация се решава проблема със злоупотреба с карти т.е. регистрация с чужда самоличност. В случай на физическа повреда на RFID четеца, системата винаги остава заключена, така че не е възможно по този начин да се наруши сигурността на системата.



***Фигура 5 - Intel mini PC - Windows 10 базиран RFID контролен модул***

Към контролния PC модул могат да бъдат свързани два RFID четеца, които могат да съответстват на по една електрическа брава. Бравите се контолират от USB програмируемо реле с два исхода свързано към контролния PC модул. В зависимост от данните на картата, постъпили от RFID четеца, и натискането на клавиша на мини клавиатурата, од контролния модул може да активира една от двете свързани електрически ключалки, която отговаря на натиснатия клавиш на едната от USB клавиатурите с един бутон.

1. Ако контролния PC модул се използва за контрол на достъпа на един вход (врата), тогава и двата четци управляват една и съща ключалка. Това има смисъл, когато четците са физически поставени от различни страни на контролираната врата. В този случай едния четец (в комбинация с притиснатия клавиш на съответната мини клавиатурата с един бутон)[[1]](#footnote-1) се използва за влизане, а другия четец за излизане. USB програмируемата клавиатурата с един бутон се използва за определяне дали е постъпил иск за влизане или излизане, което определя и задействането на съответното устройство за заснемане на изображения (камера).
2. Друг възможен сценарий на използване е, когато един RFID модул контролира достъпа до две различни стаи. В този случай всеки четец (в комбинация с притиснатия клавиш на съответната мини клавиатурата с един бутон) управлява една електрическа брава на входа на съответното помещение. Напускането на стаята е възможно без използване на карта и RFID устройство.



*Фигура 6 - Блок схема на структурата на RFID контолния модул*

Едновременно с контрола на достъпа могат да се води евиденция за достъп на дадено лице на определено място и време, независимо дали ще бъде предоставен достъп или не. В зависимост от конкретните нужди и ситуация, контролния модул може да се използва само за евидения на присъствие или комбинация от евидения на присъствие и контрол на достъпа.

Цялата информация, информация свързана с осъществения или отказан достъп (като ID на лицето, време, одобрен/отказан достъп и снимка от уеб камера се записват в база от данни в локален или отдалечен MS-SQL сървър, за по-нататъшен анализ на статистически данни и генериране на отчети в административния модул.

## Структура на системата

Основните характеристики на системата са модулност, разпределение, проста централизирана администрация, и практически неограничени възможности за разширяване на основната система чрез просто добавяне на контролни модули.

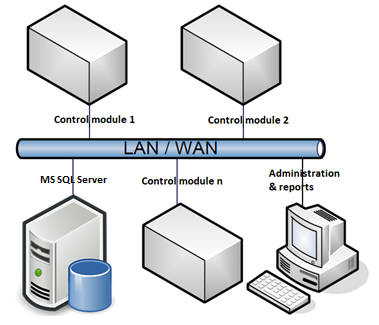
Софтуера който се изпълнява на **контролния модул**, може да се разработи за два режима на работа, on-line и off-line. В онлайн режим на работа RFID контролния модул е свързан чрез LAN/WAN/Internet компютърна мрежа към компютър – сървър, който поддържа функционирането на цялата RFID система, като в този случай ще е възможно да се използват максимално всички възможности, предоставени от системата. Самия софтуер чрез таймер периодично ще проверява за наличие на мрежа и достъп до централния сървър и ще актуализира данните които се отнасят до дадения модул. В случай на одсъствие на мрежа или недостъпност на централния сървър, контролния модул ще минава в off-linе режим на работа.

В офлайн режим контролните модули трябва да работят автономно и напълно независимо от всякакви други устройства. Структурата на RFID системата в този случай ще бъде минимална. Тази минимална конфигурация е доста използваема и е напълно рационално решение, ако се използва за контрол на достъпа до стая или сграда с малък брой потребители. Записването на информацията в този случай ще се върши в локална база данни (SQL Server Express, SQL Lite), а администрирането на такава автономна система може да бъде опростено до въвеждане на таблица с всички кодове и данни за лицата на които е позволен достъп, както и записи на всички събития (влизания, излизания и опити за неоторизиран достъп). Когато контролния модул получи достъп до мрежа цялата събрана информация трябва да се запише на централния сървър.

Други примери за използване на такава автономна off-line мини система могат да бъдат за контрол на влизането на персонала в сграда с един вход или за контрол на достъпа до паркинг, в който контролния модул работи с рампа, а не с ключалка.

В онлайн режим RFID системата с карти трябва да разгърне а истинските си възможности. Тъй като RFID контролните модули в този случай са свързани към сървъра с данни, може да се формира система с произволен брой RFID контролни модула, чиято работа се управлява от базата данни и поддържа от софтуера за администриране на системата.

Системата за контрол на достъпа и евиденция на присъствие с множество RFID контролни модули в мрежа може да се използва за контрол на достъп и евиденция на присъствие в няколко различни сгради, които могат да бъдат произволно разположени и отдалечени, по отношение на което няма ограничения. Единственото изискване е да имат мрежа (LAN/WAN) т.е. връзка към SQL сървъра на базата с данни.



***Фигура 7 - Структура на онлайн системата за контрол на достъп и евиденция за присъствие***

Софтуерът за администрация на системата трябва да овъзможава напълно персонализирани решения за нуждите и изискванията на даден потребител / компания. Програмирането на системата за контрол на достъпа и евиденция на присъствие трябва да позволява създаването на сложна потребителска система с помоща на RFID контролните модули и дадените права на потребителски достъп. Структурата на онлайн системата е показана на фигура 7. Освен директна поддръжка за функционирането на системата, софтуерът трябва да позволява и формиране на различни видове отчети и анализи на събраните данни. От администраторския компютър се извършва пълната настройка на цялата система, както и анализ на данните и генериране на отчети.

## Система за софтуерна поддръжка

Софтуерът за поддръжка на онлайн системата за контрол на достъпа и евиденция на присъствие трябва да се основава на добре проектиран модел на данни, който отразява гъвкавата модулна мрежова структура на хардуерната система, показана на фигура 7.

Отправната точка за проектиране на основен модел на данни са типовете обекти, свързани с такава система и връзки между наблюдаваните типове. Основните „видими“ типове обекти в такава система са:

* Институция
* Сграда
* Вход
* Потребител
* Група
* Карта
* RFID контролен модул

Типовете като институция и сграда могат да бъдат важни, ако се проектира система, включваща множество институции и сгради. В противен случай, ако системата ще се използва само в рамките на една институция и сграда, тези типове могат да бъдат пропуснати. Тези типове не са достатъчни за моделиране на системата, защото няма типове за описание на разрешения, достъп, история на карти и други подобни. За ефективно администриране на голям брой потребители е удобно да се въведат групи потребители, които ще имат еднакви права.

Основната функционалност на системата за контрол на достъп и евиденция на присъствие трябва да се постигне чрез използване на данните от MS-SQL базата данни. Решението за предоставяне на достъп трябва да се взема въз основа на уникална карта, RFID контролен модул и време за достъп.

Запитване към базата данни проверява дали дадения потребител, собственик на регистрираната карта, принадлежи към групата, която има право на достъп в даден момент, до даденото помещение, където се намира RFID четеца. Ако е така, достъпът е предоставен и RFID контролния модул отваря електрическата ключалка. В противен случай опитът за достъп се само регистрира, но ключалката не се отваря. Във връзка с тази основна функционалност, която ще бъде необходима и напълно достатъчна в повечето случаи, са възможни различни допълнителни специфични изисквания.

Като допълнителни изисквания, които биха могли да се наложат е да се разрешава безпрепятствено преминаване през главната входна врата през работно време, а в сградата да се допуска влизане извън работно време само на служители, които имат карта и принадлежат към група, на която е разрешен достъп. В допълнение към това искане добавяме и друго - системата трябва да функционира и в случай на прекъсване на тока.

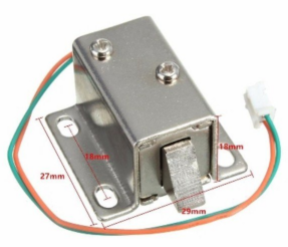
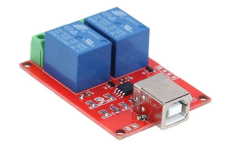
# ИЗГРАЖДАНЕ И РАЗШИРЯВАНЕ НА СИСТЕМАТА

В тази глава е представена вече реализираната функционалност на софтверната разрабока и идеите за по-нататъшното разширяване на функционалността на софтуера.

## Разработка на софтуера за контролния модул

Както вече посочихме в най-чест случай, контролния модул се намира на някоя от входните врати на сградата. На устройството се изпълнява софруер който реализира фукцията за контрол на достъп и функцията за регистрация на потребителите.

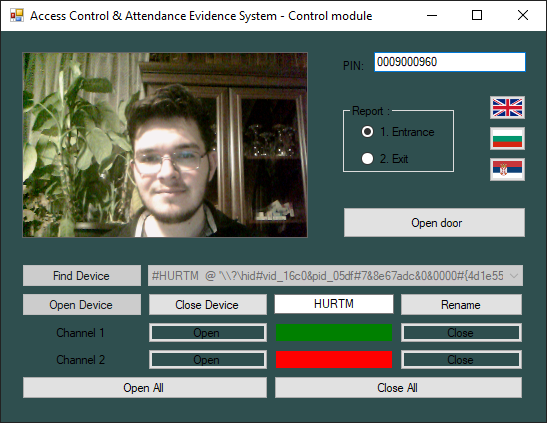
Софтуера се разработва в езика C# и се изпълнява на Intel mini PC устройство, оборудвано с USB RFID четец на карти (125kHz), USB уеб камера, стандартни HID клавиатури с един програмируем бутон (като входящи устройства) и USB програмируемo реле[[2]](#footnote-2) и електромагнитна ключалка на 12V (като изходящи и испълнителни устройства).



***Фигура 8: Входящи и изходящи устройства на контролните модули***

В този етап на разработка приложението има само една форма с два радио бутона, които дефинират събитията **влизане / излизане**, поле за въвеждане на **PIN** код на потребителите от RFID четците на карти, PictureBox за **видео наблюдение** и снемане на изображения и бутон за **отваряне на вратата**. В долната част на формата са визуално представени двата канала на USB програмируемo реле (фигура 9).

Без оглед на това че за контролния модул в режим на експлоатация не е предвиден дисплей, във етап на разработка и настройки (монтаж), желателно е и много полезно всички контроли да са визуализирани за по лесно проследяване на събитията като: постъпване на кодовете от четците, настройки на камерите проследяване на задействането на релетата и пр.



*Фигура 9 – Форма на контролния модул с визуалните контроли/компоненти*

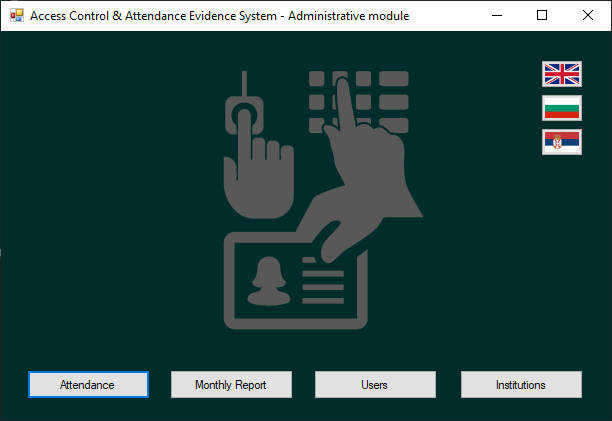
Многократното влизане/излизане(поради разни причини) в един и съсщи ден е овъзможено в софтуера, като общото присъствие се сумира, а събитието излизане не може да се одобри без предварително реализирано събитие влизане.

Към системата може да се добави лесно и цифрова клавиатура за въвеждането на PIN кода, за случай отказ на RFID четеца или повреда/загуба на идентификациона карта от страна на служител.

## Разработка на административния модул

За демонстрация на основната идея и една малка част от проектираната функционалност, разработени са няколко форми за административния модул.

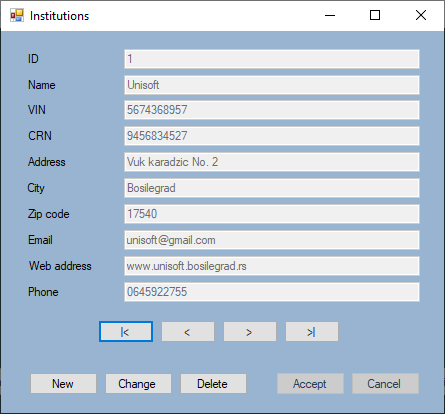
При стартиране на приложението първоначално се зарежда главната форма на приложението, от която се осъществява връзка към останалите форми. Във главната форма са расположени и три командни бутона (с флаговете на съответните държави), чрез които се осъществява превключването на езика на приложението.



*Фигура 10 – Начална форма на административния модул на приложението*

### 2.1. Формата Institutions

В тази форма се въвеждат и актуализират данните за институциите и/или отделите които са поместени в някоя сграда.

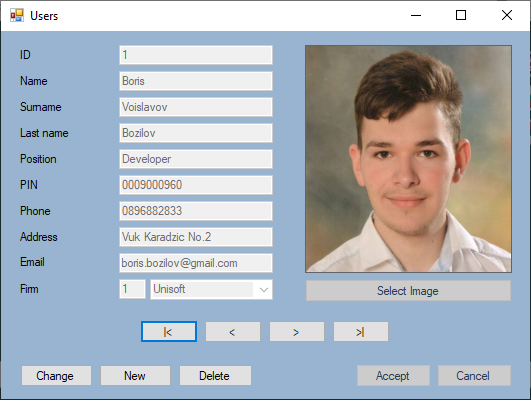


*Фигура 11 – Форма за въвеждане и актуализация на*

*информация за институциите*

### Формата Users

Във формата Users се въвеждат данните за потребителите на системата, на които се позволява достъп.

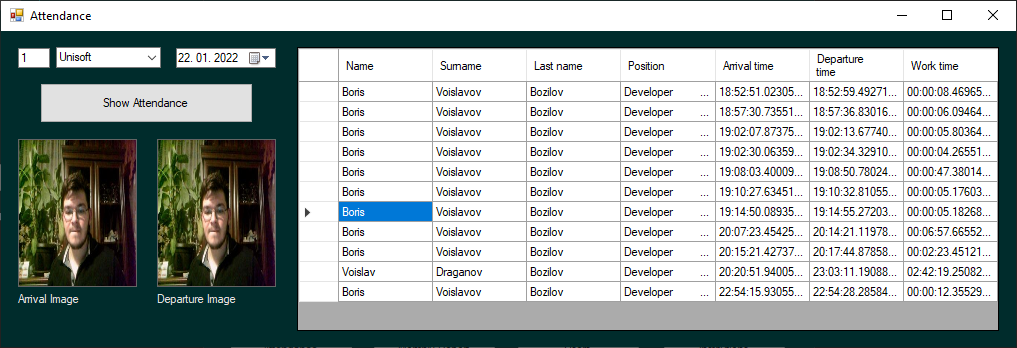


*Фигура 12 – Формата Users (Потребители) за въвеждане и актуализация*

*на информацията за потребтелите*

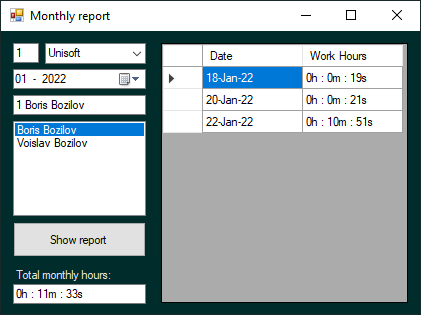
### Формата Attendance

*Фигура 13 – Формата на Attendance (Посещаемост) на английски език*



Формата Attendance служи за визуализация на данните свързани с евидентираните посещения (влизане/излизане). В нея има възможност за избиране на фирмата и датата, за която се отнасят данните. При натискане върху някой от записите в PictureBox-овете се зареждат снимките заснети при влизане и излизане, които служат за предотвратяване от злоупотреби с чужд PIN от страна на заетите, т.е. злоупотреба с чужди карти.

### Формата Monthly report



*Фигура 14 - Формата на Monthly report на английски език*

Формата Monthly report служи за визуализация на данните свързани с работното време на служителите сумарно за всеки ден и общо за целия месец.

## Визия за развитие на системата

Пътят от идея до готов продукт често не е лесен. За да може посочената идея да израсне в използваем продукт, трябва да се доразвие и изчисти в повече аспекти.

Всичко започва с една идея. Никога не може да се каже още от самото начало дали една идея струва или не. Началната идеята често е съвсем проста, но в процеса на разработка, може да израсне в нещо друго, далеч по-сложно и съвършено.

# ЗАКЛЮЧЕНИЕ

RFID технологията в комбинация с PC платформата за общо предназначение и допълнителен специализиран хардуер, разработен за тази платформа и базиран на операциона система МS Windows, заедно с езика за разработка C#, предоставя една изключителна възможност за реализация на система за автоматичен контрол на достъп и евиденция за присъствие. В зависимост от изискванията и сложността на системата могат да се прилагат **off-line** базирани решения (в случай на по-малки и по-прости системи и изисквания), както и **on-line** решения, които позволяват приложение в произволно големи системи със сложни изисквания.

За да се използва напълно потенциалът на тази гъвкава хардуерна архитектура на системата, е необходимо да се проектира софтуер с адекватна структура, който да поддържа такава система.

Чрез настройки на софтуера от страна на RFID контролните модули, както и от страна на модула за администрация, системата може да позволи голяма гъвкавост при адаптация към нови изисквания по време на редовна работа на системата. Възможността за сложни и гъвкави настройки на софтуера би позволила на системата създаване на персонализирани приложения със специфични изисквания на отделни потребители.

# 

# ЛИТЕРАТУРА

# 1.Стъпки за проектиране и изграждане на система за контрол на достъпа и работното време

<https://hybsys.bg/Technology/AccessControl/StepByStep/>

## 

## 2.Контрол на достъп - области на приложение

## http://bells-security.com/new/pdf/Broshure\_HS\_Access\_BG.pdf

## 3.Introduction to RFID Reader (125Khz) – USB

# <https://www.rhydolabz.com/wiki/?p=835>

# 3.Proximity Access Readers: 125kHz Or 13.56Mhz?

<https://sen.news/2018/10/17/proximity-access-readers-125khz-or-13-56mhz>

# 4.RFID системи за контрол на достъп с четци за карти и чипове

# <https://v-maxprotect.com/sistemi-za-kontrol-na-dostyp-cena/kartovi-sistemi-chetci>

**5.NFC технологията в системите за контрол на достъпа**

<https://www.tech-dom.com/bg/nfc-tehnologiyata-v-sistemite-za-kontrol-na-dostapa/2/1733/>

# 6.Module 2x USB controlled relay, 2x10A

# <https://www.gmelectronic.com/module-2x-usb-controlled-relay-2x10a#product-detail>

# 7.Versatile WebCam C# library

<https://www.codeproject.com/Articles/125478/Versatile-WebCam-C-library>

**8.How to capture image with webcam?**

<https://stackoverflow.com/questions/13909106/how-to-capture-image-with-webcam>

1. До момента все още не е намерен начин за определяне от кой от двата RFID четеца е постъпила информацията и оттам се поражда нужда за допълнителен бутон от мини клавиатура, който определя влизане / излизане (1) или съответната врата на стая при втория сценарий (2) [↑](#footnote-ref-1)
2. Модул с две релета (10A), управлявани през USB порт с индикация на състоянието чрез светодиоди. Захранването на модула е през USB, максимално натоварване на контактите е 10A [↑](#footnote-ref-2)