# Středoškolská technika 2017

**Setkání a prezentace prací středoškolských studentů na ČVUT**

# Informační systém s aplikací biometrie

**Hrubý Filip**

SPŠ A VOŠ PÍSEK

Karla Čapka 402, 397 11 Písek

## Poděkování

Chtěl bych poděkovat panu Ing. Mgr. Miroslavu Širokému, DiS. za cenné rady při vytváření práce.

Panu Mgr. Janu Turoňovi za pomoc při vytváření programu a panu PhDr. Josefu Havlanovi za možnost pracovat v dílnách i po vyučování. Dále bych rád poděkoval vedení SPŠ a VOŠ Písek za možnost zapůjčení všech potřebných komponentů pro vytvoření dlouhodobé maturitní práce.

## Anotace

Maturitní práce se zabývá zabezpečení přístupu do objektu s pomocí biometrických prvků a evidencí vstupů, kterou zabezpečuje spolu s uživatelským rozhraním databáze v MS Access.

Zaměřuje se na validaci pomocí karty s BAR kódem. Po přiložení karty je zaevidován vstup v databázi a je provedena verifikace uživatele biometrickou metodou otisků prstů. Sériové zapojení zamezuje vstupu uživatelů s platnou přístupovou kartou, kteří nemají uložený otisk prstu v paměti čtečky či naopak.

## Annotation

Graduation thesis deals with security access to the building with the biometric registration inputs which is ensured by the user interface and by MS Access database. It focuses on the validation using a card with BAR code. The number of card is registered in the database and verification is performed using the user's biometric fingerprints. Serial connection prevents the entry of users with a valid access card without fingerprint stored in a memory card reader or vice versa.



## Klíčová slova

Biometrie, Databáze, BAR kód, Otisk prstů, Validace, Verifikace

## Keywords

Bimetrics, Database, BAR code, Fingerprints, Validation, Verification

# Úvod

Cílem práce je vytvořit funkční databázi pro evidenci vstupů menšího podniku s maximálně 100 zaměstnanci. Výstupem z databáze bude minimálně 5 sestav, které budou sloužit k vizualizaci vstupů do objektu a následné možnosti tisku. Např. sestava pro přehled evidence vstupů jednoho zaměstnance v aktuálním či zadaném měsíci.

Automatizované uživatelské rozhraní aplikace (API) bude implementovat USB relé, které bude propojené s databází. Po úspěšném zaevidování vstupu sepne relé a tím se splní první část sériového zapojení systému pro přístup. Pro evidování samotných vstupů do databáze bude využito přístupových karet s čárovými kódy, kdy se po přiložení karty zapíše vstup.

Práce vyhodnotí jednotlivé typy BAR kódů a na základě vyhodnocení bude určen nejvhodnější typ pro tuto aplikaci.

Druhou částí sériového zapojení bude zabezpečení vstupu pomocí biometrických prvků.

Zhodnocení biometrických prvků poskytne podklady pro výběr nejvhodnějšího typu sytému, který bude využit v práci pro zabezpečení vstupu.

Celková funkcionalita výstupu bude databáze s evidencí vstupů pomocí karet s BAR kódy a zabezpečení pomocí biometrické metody.

# Návrh databáze

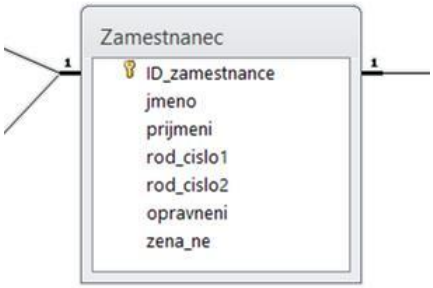
Pro přístupový systém do podniku je využita databáze v programu Microsoft Access 2010. Databáze je ustálený soubor pojmů, technických prostředků a sofistikovaných metod sloužící k hromadnému zpracování dat a vytvoření požadovaných informací v rámci informačního systému. Informační systém je soubor lidí technologických prostředků a metod, který zabezpečuje sběr uchování a zpracování dat k tvorbě prezentace informace k potřebám koncových uživatelů.

Do jednotlivých řádků tabulek je využit vhodný název a datový typy například: automatické číslo, číslo, datum a čas, objekt typu OLE, a také se přiřadí primární a cizí klíče. Náhled prostředí MS Access pro návrhové zobrazení tabulky viz obrázek č. 1 – Tabulka zaměstnance. [1]

| Název pole | Datový typ |
|---|---|
| ID_zamestnance | Automatické číslo |
| jmeno | Text |
| prijmeni | Text |
| rod_cislo1 | Číslo |
| rod_cislo2 | Číslo |
| opravneni | Číslo |
| zena_ne | Ano/ne |

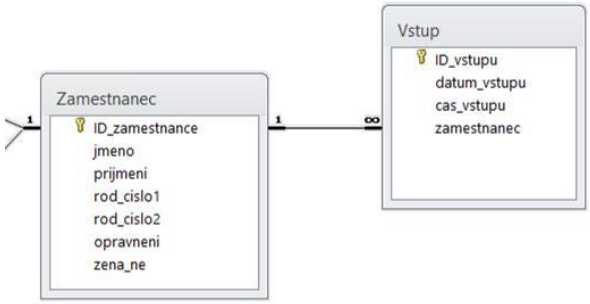
Obrázek č. 1 – Tabulka zaměstnance

Primární klíč je jednoznačné určení entity (osoba, věc, činnost, vlastnost – cokoli jednoznačně identifikovatelné). Pro tabulku zaměstnanců je určen primární klíč **ID_Zamestnance** viz obrázek č. 2 – Primární klíč.




Obrázek č. 2 – Primární klíč

Cizí klíč (sekundární klíč) – odkaz na primární klíč v jiné tabulce (příslušný řádek cizí tabulky rozvíjí řádek zdrojové tabulky přes toto spojení) Pro tabulku vstup je určen cizí klíč **zamestnance**, který odkazuje na primární klíč **ID_Zamestnance** v tabulce zaměstnance viz obrázek č. 3 – Cizí klíč.



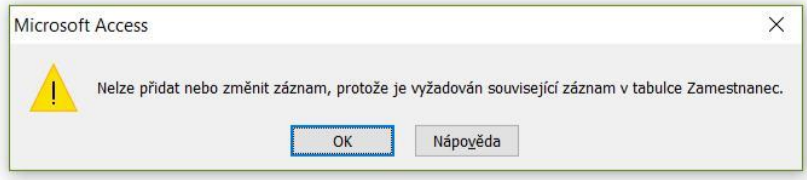

Obrázek č. 3 – Cizí klíč

Při vytváření databáze je vhodné dodržet zásady pro tvorbu databází, jako jsou např. referenční integrita databáze a normální formy. [1]

## Integrita databáze

Integrita databáze znamená, že data v ní uložená jsou konzistentní vůči definovaným pravidlům. Lze zadávat pouze data, která vyhovují předem definovaným kritériím (např. musí respektovat datový typ nastavený pro daný sloupec tabulky, či další omezení hodnot přípustných pro daný sloupec). K zajištění integrity databáze slouží integritní omezení. Jedná se o nástroje, které zabrání vložení nesprávných dat nebo ztrátě nebo poškození stávajících záznamů v průběhu práce s databází.

Při mazání dat, která již ztratila svůj význam (například smažeme-li uživatele), dojede k odstranění i souvisejících záznamů v ostatních databázových tabulkách viz obrázek č. 4 – Odstraněný záznam. [9]




Obrázek č. 4 – Odstraněný záznam

## Druhy integritních omezení

Entitní integritní omezení:

Povinné integritní omezení, které zajišťuje úplnost primárního klíče tabulky (zamezí uložení dat, jež by v těchto polích byla stejná jako v nějakém jiném řádku tabulky).

Doménová integritní omezení:

Zajišťují dodržování datových typů/domén definovaných u sloupců databázové tabulky.

Referenční integritní omezení:

Zabývají se vztahy dvou tabulek, kde jejich relace je určena vazbou primárního a cizího klíče.

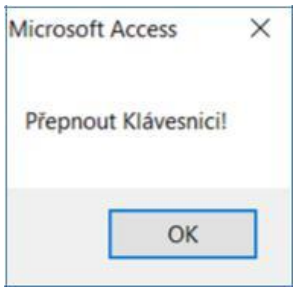
Aktivní referenční integrita:

Definuje činnosti, které databázový systém provede, pokud jsou porušena některá pravidla.

## Dodržování integritních omezení

1. Umístění jednoduchých mechanismů na straně databázového serveru

   Jedná se o nejlepší způsob z hlediska ochrany dat uživateli, avšak obvykle přináší delší odezvu systému a nelze vždy zajistit jejich přenositelnost na jiný databázový systém (varování před často opakovanou chybou u načítání BAR kódu např. při zvolené české klávesnici viz obrázek č. 5 – Integritní omezení).




Obrázek č. 5 – Integritní omezení

2. Umístění ochranných mechanismů na straně klienta

   Pro komfort a nezávislost na databázovém systému je nejlepší volbou integritních omezení nutnost kontrolních mechanismů pro každou operaci. To však může způsobit chyby např. při zadní nového pojmu v aplikaci. V případě většího počtu aplikací je potřeba je následně opravit na více místech.

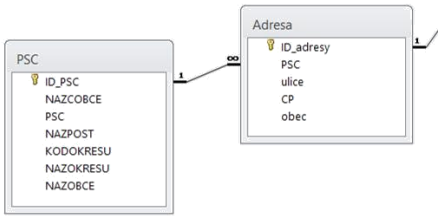
3. Samostatné programové moduly na straně serveru

   V moderních databázových systémech jsou pro tento účel implementovány tzv. **triggery** tj. samostatné procedury, které lze spouštět automatizovaně před a po operacích manipulujících s daty. Tento způsob umožňuje implementaci i složitých integritních omezení. Nevýhody opět přináší provádění na serveru i velmi omezená možnost přenesení na jiný databázový systém. [9]

## Normální formy

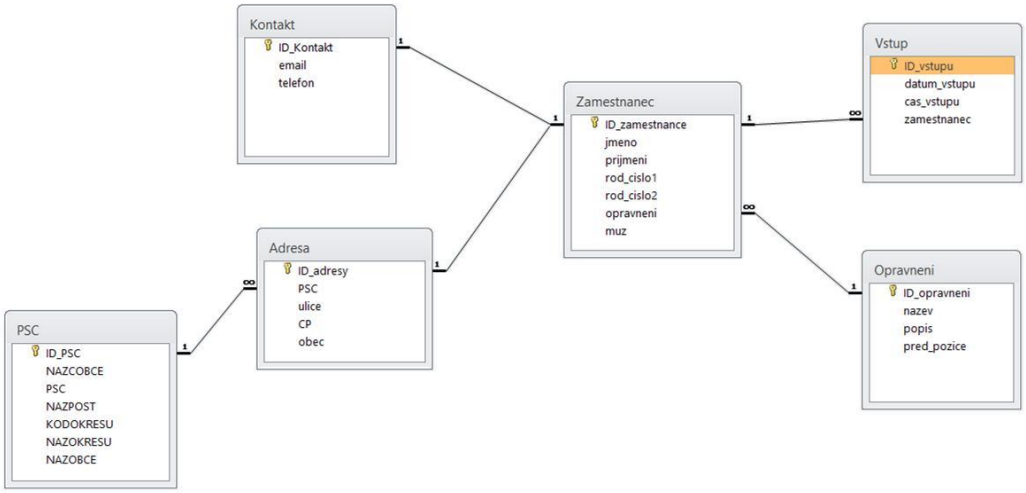
Pod pojmem normalizace rozumíme proces zjednodušování a optimalizace navržených struktur databázových tabulek. Hlavním cílem je navrhnout databázové tabulky tak, aby obsahovaly minimální počet redundantních (nadbytečných) dat. Při vytváření databáze byla dodržena

3. Normální forma: Všechny neklíčové atributy musí být vzájemně nezávislé (odstranění redundancí PSČ+ Město). [1] Viz Obrázek č. 6 – 3. Normální forma.




Obrázek č. 6 – 3. Normální forma

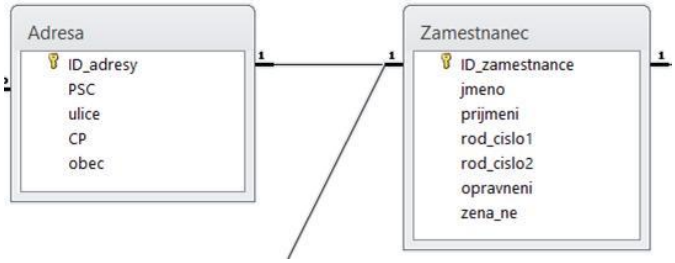
Pro vytvoření vztahů mezi jednotlivými tabulkami využijeme relace v databázových nástrojích, viz Obrázek č. 7 – Relace, kde se propojí jednotlivé tabulky s příslušnou kardinalitou.




Obrázek č. 7 – Relace

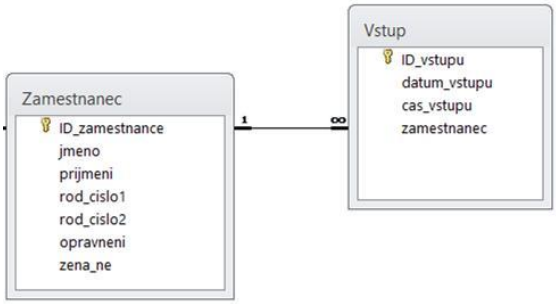
## Kardinalita vztahů v databázích

1:1 – vztah, ve kterém na obou stranách vystupuje pouze jeden objekt dané entity (např. jedna adresa může mít jen jednoho zaměstnance se stejným jménem) viz obrázek č. 8 – Kardinalita typu 1:1




Obrázek č. 8 – Kardinalita typu 1:1

1:N – na jedné straně je jediný objekt, který je ve vztahu s jedním nebo více objekty na straně druhé. Jedná se o typ, který se vyskytuje velmi často (např. vstup a zaměstnanec) viz obrázek č. 9 – Kardinalita typu 1:N



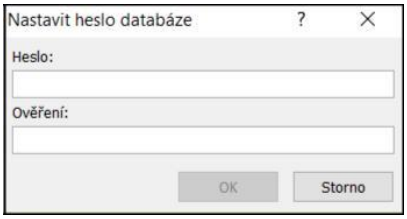

Obrázek č. 9 – Kardinalita typu 1:N

M:N – vztahy, kde vystupuje více objektů na obou stranách (např. zaměstnanec a úkol, kde jeden úkol může řešit více zaměstnanců a současně jeden zaměstnanec může řešit více úkolů)[7].

## Zabezpečení databáze

Databáze je šifrována pomocí hesla v Microsoft Access 2010 (obrázek č. 10 - Šifrování), kde se nastaví heslo podle potřeby uživatele (obrázek č. 11 - Heslo). Microsoft Office využívají pokročilou úroveň šifrování typu **RC4**.


Obrázek č. 10 - Šifrování




Obrázek č. 11 – Heslo

## Funkce RC4

RC4 je klasický symetrický algoritmus s tajným klíčem. Je to proudová š šifra, kterou navrhl Ronald Rivest (RC znamená Rivest‘s Cipher), jeden z vynálezců algoritmu RSA a spoluzakladatel společnosti RSA DSI. Je řádově desetkrát rychlejší než šifra DES[1]. Mimo Microsoft Office je využita i u Oracle Secure SQL či v protopolu Secure Socket Layer 3.0 firmy Netscape. [18]

Tři základní komponenty RC4:

a. S-box
b. Key scheduling algorithm – často se můžeme setkat se zkráceným označením KSA
c. Pseudo-random generation algorithm (PRGA)

1. Nejprve vytvoří pole, typicky o velikosti 256 Bytů. Tomuto poli se často říká S-box. Zpočátku ho inicializuje smyčkou **for** tak, že se v něm budou nacházet vzestupně seřazená celá čísla v intervalu <0; 255> (hodnota indexu prvku pole bude rovna hodnotě prvku).
2. KSA fáze: Toto pole (S-box) prožene zmíněným KSA, které dle uživatelem zadaného klíče provede proházení prvků v poli a přidá Bytů z klíče. Jde o permutaci, která proběhne dle Bytů klíče. U hodnoty v klíči může dojít k přetečení hodnot prvků pole. Klíč má délku v rozmezí 40 a 128 bitů a při permutaci je opakován stále dokola od začátku do konce S-boxu. Na konci kódu KSA prohodí hodnoty prvků pole SBox[i] a SBox[j].
3. PRGA fáze: S-box, který KSA zakódovalo, předá PRGA, které vygeneruje tzv. **keystream**. PRGA vytvoří **keystream**, který má velkou periodu opakování a má mnoho kombinací, jako skutečný náhodný generátor čísel.
4. Zakódování dat (textu) se provede tak, že provede logickou funkci **XOR keystreamu** a dat (textu). Dekódování opět provede funkci **XOR** na zakódovaná data (text) a **keystream**. [15]

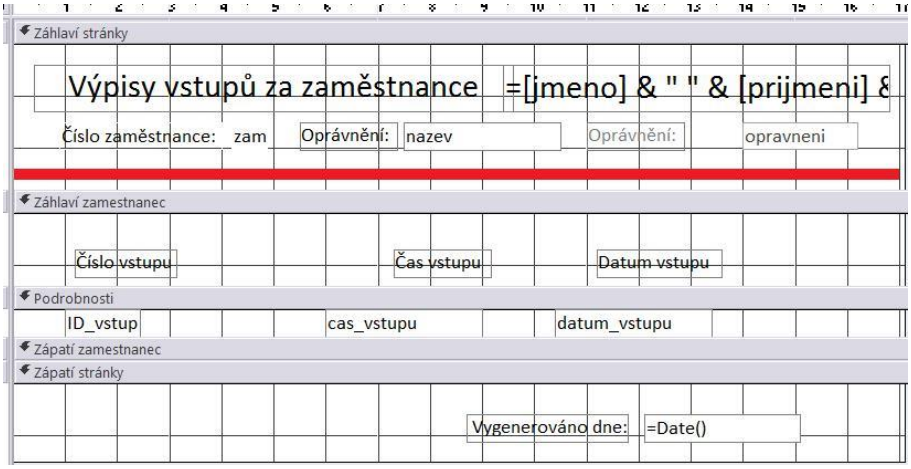
[1] DES – Data (Digital) Encryption Standard [19]

## Sestavy

Sestava je objekt databáze, který lze využít k prezentaci informací v databázi pro některý z následujících účelů, zobrazení nebo distribuce souhrnu dat, archivní snímky dat, poskytování údajů o jednotlivých záznamech, vytváření popisků. [10]

1. Návrhové zobrazení sestavy

Pro vytvoření sestavy a následovné grafické zpracování je využito návrhové zobrazení viz obrázek č. 12 – Návrhové zobrazení sestavy.




Obrázek č. 12 – Návrhové zobrazení sestavy

Ve vlastnostech sestavy se vybere přes SQL dotaz zdroj záznamů (dat) pro následnou vizualizaci vybraných záznamů (dat) viz obrázek č. 13 – SQL dotaz. **SELECT** vybere potřebné pole z jedné či více tabulek, které určuje příkaz **FROM**. Položka **WHERE** u ID_zamestnance z tabulky zamestnance spustí vyskakovací okno s textem „Zadej číslo zaměstnance“, kam se se zadá číslo zaměstnance a z datumu vstupu **WHERE** vybere jen měsíc a následným vyskakovacím oknem „Zadej měsíc“, kam se zadá měsíc.

```
SELECT

Vstup.ID_vstupu, Vstup.datum_vstupu, Vstup.cas_vstupu, Vstup.zamestnanec, Zamestnanec.jmeno,
Zamestnanec.prijmeni, Zamestnanec.ID_zamestnance, Month([datum_vstupu]) AS mesic, Zamestnanec.opravneni, Opravneni.nazev

FROM

(Opravneni INNER JOIN Zamestnanec ON Opravneni.ID_opravneni = Zamestnanec.opravneni)
 INNER JOIN Vstup ON Zamestnanec.ID_zamestnance = Vstup.zamestnanec

WHERE

(((Zamestnanec.ID_zamestnance)=[Zadej číslo zaměstnance]) AND ((Month([datum_vstupu]))=[Zadej měsíc]));
```

Obrázek č. 13 – SQL dotaz

Grafický prvek čáry, vytvořený pro zvýšení přehlednosti úrovně přístupu, je navrhnut v návrhu sestavy přes tlačítko „Zobrazit kód“, kde je možnost případného vylepšování sestavy či formuláře pomocí VBA – Visual Basic for Applications. Viz obrázek č. 14 – užití VBA. **Select Case opravneni** určí, že se podle pole oprávnění bude rozhodovat. Když **opravneni** bude 1, 2 nebo 3 nastaví se barva objektu „Čára22“ na modrou, zelenou nebo červenou.

```
Select Case opravneni

Case 1
Čára22.BorderColor = vbBlue

Case 2
Čára22.BorderColor = vbGreen

Case 3
Čára22.BorderColor = vbRed

End Select
```

Obrázek č. 14 – užití VBA

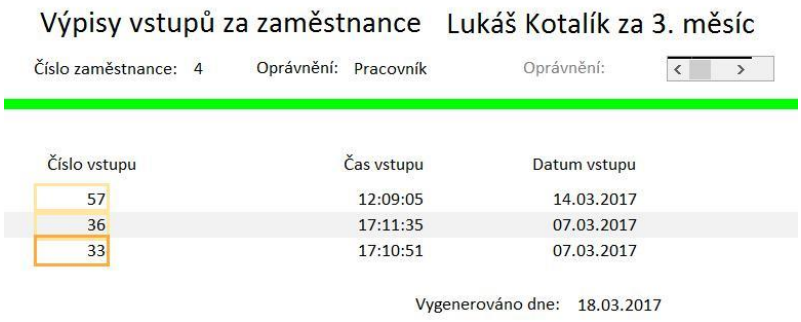
2. Zobrazení sestavy

Je využito k vizualizaci „návrhového zobrazení“. Obrázek č. 15 – Zobrazení sestavy


Obrázek č. 15 – Zobrazení sestavy

3. Zobrazení rozložení

Pro finální rozložení je využito „rozložení sestavy“, kde je možnost upravit poslední detaily rozložení sestavy pro finální náhled a tisk. Obrázek č. 16 – Rozložení sestavy.




Obrázek č. 16 – Rozložení sestavy

4. Náhled sestavy

V „náhled sestavy“ je zobrazeno finální rozvržení sestavy k tisku. Náhled sestav v plné velikosti je k dispozici v příloze číslo 1.

# Verifikace

Pro verifikaci[2] je použita biometrie. Biometrie je vědní obor zabývající se studií a zkoumáním živých organismů, především člověka, a měřením jeho biologických (anatomických a fyziologických) vlastností a také jeho chováním, tzn. behaviorálních charakteristik. Pojem biometrika je odvozený z řeckých slov „bios“ a „metron“. První znamená „život“, druhé pak „měřit, měření“. Kdybychom se chtěli držet doslovného překladu, zněla by biometrie jako „měření živého“. V přeneseném významu jde ovšem o měření a rozpoznávání určitých charakteristik člověka.

Biometrika se věnuje studiu metod vedoucích k rozpoznávání člověka na základě jeho unikátních proporcí nebo vlastností. Existuje mnoho biometrických metod jako například geometrie ruky, geometrie tváře, duhovka oka, sítnice oka, a v neposlední řadě otisk prstu. [2]

## Srovnání biometrií

Tabulka č. 1. Srovnání biometrií zelená = nejlepší; červená = nejhorší

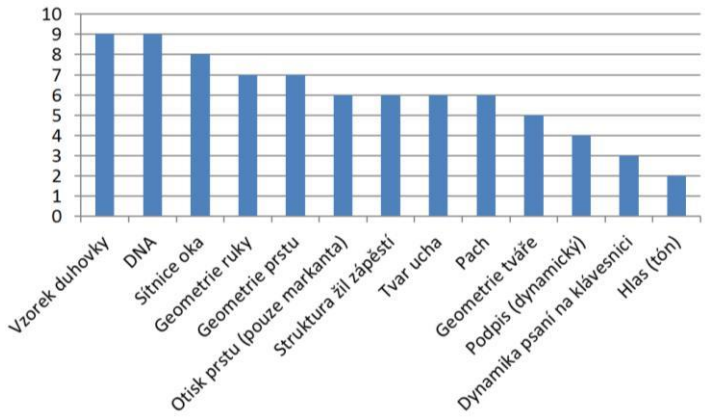
| | Biometrická vlastnost | komfort | přesnost | životnost | dostupnost | cena |
|---|---|---|---|---|---|---|
| 1 | Otisk prstu | 7 | 7 | NE | 4 | 3 |
| 2 | Podpis (dynamický) | 3 | 4 | ANO | 5 | 4 |
| 3 | Geometrie tváře | 9 | 4 | NE | 7 | 5 |
| 4 | Vzorek duhovky | 8 | 9 | NE | 8 | 8 |
| 5 | Sítnice oka | 6 | 8 | ANO | 5 | 7 |
| 6 | Geometrie ruky | 6 | 5 | NE | 6 | 5 |
| 7 | Geometrie prstu | 7 | 3 | NE | 7 | 4 |
| 8 | Struktura žil zápěstí | 6 | 6 | ANO | 6 | 5 |
| 9 | Tvar ucha | 5 | 4 | NE | 7 | 5 |
| 10 | Hlas (tón) | 4 | 3 | ANO | 3 | 2 |
| 11 | DNA | 1 | 7 | NE | 9 | 9 |
| 12 | Psaní na klávesnici | 4 | 1 | ANO | 2 | 1 |
| 13 | *pro srovnání: heslo* | 5 | 2 | ANO | 8 | 1 |

[2] Verifikace – potvrzení pravosti uživatele [4]

## Stálost biometrické vlastnosti v čase

Jedním z nejdůležitějších požadavků na biometrickou vlastnost je stálost v čase, aby nemohlo dojít k její kompromitaci se stárnutím člověka. Důvodů, proč se vlastnost může změnit, je několik. Vliv růstu živé tkáně, opotřebení, biologické stárnutí, špína a nečistoty, zranění a následné hojící procesy a nespecifikované vlivy. Biometrické vlastnosti, které jsou nejméně ovlivněné těmito možnostmi a jsou nejvíce upřednostňovány. Stupeň stálosti v čase je znázorněna v následujícím grafu č. 1 Stálost biometrické vlastnosti v čase (10 znamená nejvyšší stálost v čase, 0 nejnižší). [2]

Graf 1 – Stálost biometrické vlastnosti v čase[2]




## Měření výkonnosti biometrických systémů

Efektivnost biometrických rozpoznávacích systémů lze měřit mnoha statistickými koeficienty.

Charakteristickými výkonnostními mírami jsou: koeficient nesprávného přijetí, koeficient nesprávného odmítnutí, koeficient vyrovnané chyby, doba zápisu etalonu a doba ověření. Takových koeficientů existuje, v závislosti na hloubce zkoumání problému, celá řada.

1. False Acceptance Rate (FAR)

   Koeficient FAR udává pravděpodobnost toho, že neoprávněná osoba je přijata jako oprávněná. Jelikož nesprávné přijetí může často vést ke vzniku škody, FAR je především koeficient udávající míru bezpečnosti. Označuje se jako chyba II. druhu.

   Jde o přijetí, připuštění neregistrované osoby do systému, a tato osoba nemá za normálních podmínek oprávněný přístup do systému. Jde o chybu velmi závažnou; kritickou z bezpečnostního i marketingové hlediska. [2]

Na vzorku 30 lidí (neoprávněných osob) čtečka „sebury 007 –EM“ zamítla všechny testované osoby. Ze vztahu vyplívá 0% pravděpodobnost, že bude vpuštěna neoprávněná osoba. Ve specifikacích čtečky, viz příloha č. 2 – Specifikace čtečky, je změřený FAR 0,001%. Rozdíl oproti specifikaci je důsledkem malého počtu námi testovaných osob.

$$= \frac{}{} \cdot 100\,[\%]$$

$$0 = {}_{30} \cdot 100 = 0\%$$

- počet chybných přijetí
- počet všech pokusů neoprávněných osob o identifikaci

2. False Rejection Rate (FRR)

Koeficient FRR udává pravděpodobnost toho, že oprávněný uživatel je systémem odmítnutý. FRR je především koeficient udávající komfort, protože nesprávné odmítnutí je pro uživatele nepříjemné. Označuje se jako chyba I. druhu.

Jde o odmítnutí, nerozpoznání osoby, která je v systému registrována a má do něj za normálních podmínek oprávněný přístup. Jde o chybu, která nemá z bezpečnostního hlediska velký význam. Marketingově jde ale o nevýhodnou chybu, protože nutí oprávněného uživatele k opakování pokusu o přístup a to má za následek jeho nespokojenost.

Ze vztahu je zřejmá 1% pravděpodobnost, že oprávněný člověk nebude vpuštěn. Ve specifikacích čtečky viz příloha č. x – Specifikace čtečky je změřený FRR 0,1%. Rozdíl oproti specifikaci je důsledkem malého počtu námi testovaných osob.

$$= \frac{}{} \cdot 100\,[\%]$$

$$1 = {}_{100} \cdot 100 = 1\%$$

– počet chybných odmítnutí
– počet všech pokusů oprávněných osob o identifikaci

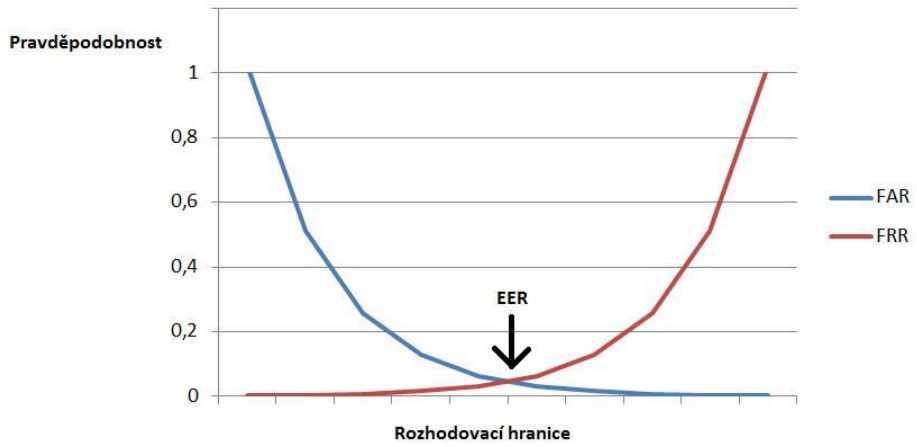
Chyby FFR a FAR jsou kromě častého vyjádření v procentech vyjadřovány i poměrem. Např. FAR 0,001 % odpovídá poměru 1: 100 000. V tomto případě to znamená, že jeden ze sto tisíců neoprávněných pokusů může být připuštěn do systému.

3. False Non-Match Rate (FNMR)

Koeficient FNMR udává poměr toho, že oprávněné osoby jsou nesprávně nerozpoznány během srovnávacího procesu. V porovnání s FRR se liší v tom, že se nezapočítává odmítnutí z důvodu špatné kvality snímaného obrazu. Důležitým pojmem při měření efektivnosti (výkonnosti) biometrických systémů je tzv. křížový koeficient, udávající, s jakou pravděpodobností při jakém nastavení hranice rozhodování nastane jev FAR a FFR současně (tzn. FAR = FFR). Křížový koeficient EER (Equal error rate) je důležitým ukazatelem při nastavování citlivosti systému, udává ideální rozložení chyb FAR a FRR.

Je-li FAR koeficientem bezpečnosti a FRR koeficientem komfortu, je zřejmé, že ve chvíli, kdy jsou v rovnováze, je v rovnováze i celkové nastavení systému. Z diagramu je také patrné, že posouvání hranice jedním či druhým směrem lze systém buď činit více bezpečným, nebo více uživatelsky příjemnějším. Průnik pravděpodobnostních distribučních funkcí FAR – FRR názorně ukazuje, jak se v závislosti na nastavené hranici rozhodování projeví celková pravděpodobnost, že mohou nastat obě chyby stejně pravděpodobně. Viz Graf č. 2 – Distribuční pravděpodobnostní funkce FAR – FRR.

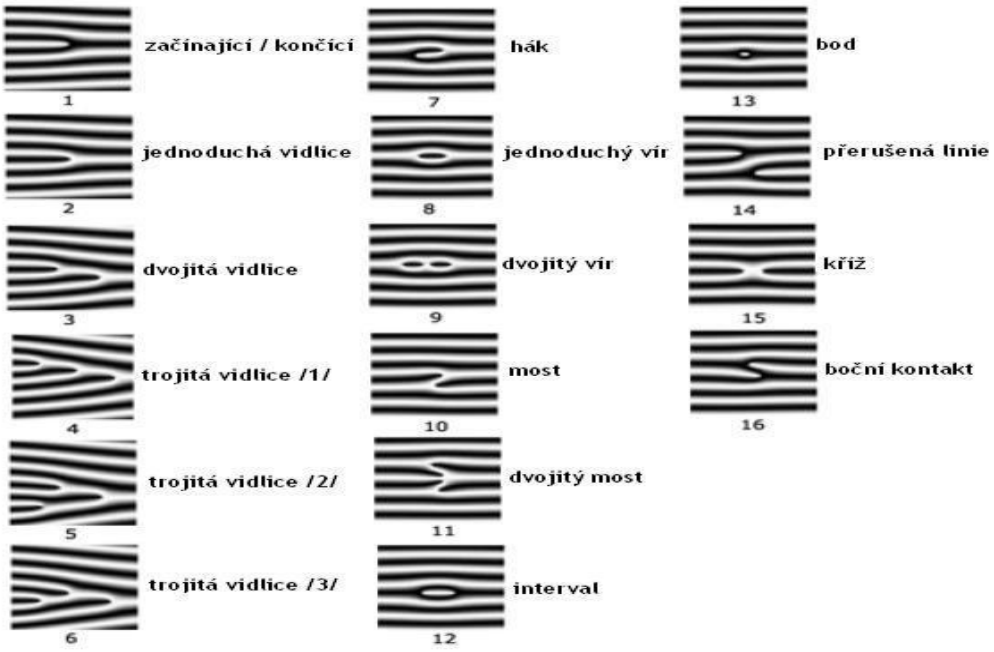
Graf č. 2 – Distribuční pravděpodobnostní funkce FAR – FRR [2]




## Biometrie otisku prstu

Biometrie otisku prstu byla použita z důvodu dostupnosti na pracovišti. Vychází z neopakovatelných kožních papilárních linií na dlaních či ploškách prstů. Používají se hlavně pro svou jedinečnost stálosti v čase. Jedinečnost stálosti v čase znamená, že v průběhu let je otisk prstu neměnný (stejný). Zakulacené smyčky tvořené prohlubněmi a vyvýšeninami, tyto smyčky nazýváme papilární linie. Papilární linie vytvářejí různé obrazce, tyto obrazce nazýváme

daktyloskopické markanty. Tyto obrazce jako první popsal český kněz a vědec J. E. Purkyně. Ten nalezl a popsal devět těchto obrazců. Podle posledních výzkumů je popsáno nejméně šestnáct markantů. Jedním z problémů metody otisku prstu je životnost a narušení papilárních linií. Tyto markanty jsou znázorněny v obrázku č. 17 – Popis daktyloskopických markantů.[3]




Obrázek č. 17 - Popis daktyloskopických markantů

Na vzorku otisku prstu (obrázek č. 18 – Otisk prstu):

1. Interval
2. Vidlice
3. Dvojitá vidlice
4. Most
5. Boční kontakt
6. Začínající / končící


Obrázek č. 18 – Otisk prstu s popisem markantů

## Čtečka otisků prstů

Čtečka otisků prstů Sebury 007-EM (obrázek č. 19 – Čtečka otisků prstů Sebury 007-EM) byla využita z důvodu dostupnosti. Čtečka sejme otisk prstu pomocí příkazů z IR klávesnice a následně ho uloží do paměti zařízení. Poté se uložený otisku porovnává s otiskem přiloženým, což následně rozhoduje o povolení či zamítnutí vstupu.

Specifikace čtečky: Maximálně 120 otisků prstu v paměti, sepnutí relé 10 sekund, krytí IP 53: zařízení je chráněno před prachem a před dotykem drátem a deštěm [12]. Veškeré specifikace čtečky viz příloha číslo 2. Specifikace čtečky otisků prstů.

Obrázek č. 19 – Čtečka otisků prstů Sebury 007-EM

## Zapojení čtečky otisku prstu

Zapojení čtečky otisku prstu viz obrázek č. – 20 zapojení čtečky:

Červený drát: +12V,
Černý: GND (zem)
Modrý: mínus u LED
diody Fialový: GND (zem)

# Validace

Pro validaci[3] jsou vyžity přístupové karty s BAR kódem pro jednotlivé uživatele. BAR kód je nejrozšířenějším prostředkem automatické identifikace neboli „registrace dat bez použití kláves“.

Výhody BAR kódů: přesnost (snižuje chybovost až na jednu miliontinu), rychlost (minimálně třikrát pomalejší než ruční zadávání), flexibilita (jdou použít i v nejextrémnějších podmínkách), produktivita, efektivnost (rychlost odbavování u pokladny se zvýší o desítky), dosledovatelnost a cena. BAR kód se skládá z tmavých čar a ze světlých mezer, které se čtou pomocí specializovaných čteček – snímačů BAR kódů. [6]

## Čtečka BAR kódů

Pro načtení karet je vybrána čtečka BAR kódů Datalogic QuickScan QD2400 (obrázek č. 21 – Čtečka QuickScan).

Obrázek č. 21 – Čtečka QuickScan

Čtečka má definované specifikace: Kabelový 1D i 2D plošný snímač obrazu s technologií Green Spot pro potvrzování přijetí kódu a LED zaměřovacím systémem (viz obrázek č. 23 – zaměřovací systém). Modré zaměřovací světlo a červený laser pro nahrání kódu svítí při stisknutí a podržení tlačítka (viz obrázek č. 24 – Zaměřovací světlo a laser) a zelené při přijetí kódu (viz obrázek č. 22 – Green spot).


Obrázek č. 22 – Green spot


Obrázek č. 23 – Zaměřovací systém

[3] Validace – kontrola vstupních údajů (uživatelů) [4]

Obrázek č. 24 – Zaměřovací světlo a laser

Snímač lze použít jako ruční nebo je možno jej uchytit na stojan. Stupeň krytí IP42 [11] znamená: zařízení je chráněno před vniknutím pevných cizích těles o průměru 1mm a větších a před dotykem drátem a pod kapající vodou ve sklonu 15°[12].

Laserové snímače BAR kódu vyzařují červené světlo. Světlo je pohlcováno černými čárami a odráženo světlými mezerami. Snímač zjišťuje rozdíly v reflexi a ty přeměňuje v elektrické signály odpovídající šířce čar a mezer. Tyto signály jsou převedeny v číslice (písmena), které obsahuje příslušný BAR kód. To tedy znamená, že každá číslice či písmeno je zaznamenáno v BAR kódu pomocí předem přesně definovaných šířek čar a mezer. Data obsažená v BAR kódu mohou zahrnovat takřka cokoliv: číslo výrobce, číslo výrobku, místo uložení ve skladu, číslo série nebo jméno určité osoby, které je např. povolen vstup do jinak uzavřeného prostoru. [6]

## Nejrozšířenější typy BAR kódů

Ukázky kódů byly vygenerovány zde [8]

1. EAN 13 a EAN 8

   Nejznámější BAR kód užívaný pro zboží prodávané v obchodní síti.


2. UCC/EAN 128

   BAR kód využívaný pro označování obchodních a logistických jednotek.


3. Code 128

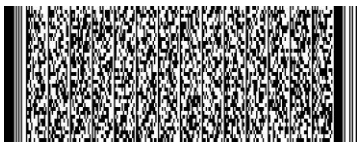
   Univerzální volně použitelný BAR kód ke kódování alfanumerických dat.


4. Code 39

   Kód používaný zejména v automobilovém průmyslu, ve zdravotnictví a v mnoha dalších odvětvích průmyslu a obchodu.

5. PDF 417

   2D kód s velmi vysokou informační kapacitou a schopností detekce a oprav chyb (při porušení kódu) používaný na letenkách.



6. DATAMATRIX

   Maticový 2D kód používaný v armádních aplikacích, v letectví a pro označování elektronických součástek. Často se používá se spojitosti s technologií DPM (Direct Part Marking se používá pro trvalé označování předmětů a automatický sběr dat pomocí specializovaných snímačů). [6]

## Karty pro přístup

Karty pro přístup do objektu o velikosti platební karty či občanského průkazu (85,6 × 54,0) mm budou z papíru a budou laminovány. Budou obsahovat: jméno a příjmení, fotografii zaměstnance, úroveň oprávnění v podobě barevných pruhů a číslo zaměstnance v databázi – v podobě BAR kódu typu Code 128. (Viz obrázek č. 25 – Karta pro přístup do objektu.) Příloha č. 3 – Ukázky karet zaměstnanců

Karty pro návštěvy jsou univerzální a identifikace návštěvy je provedena podle záznamu v knize návštěv vzhledem k časovému období.

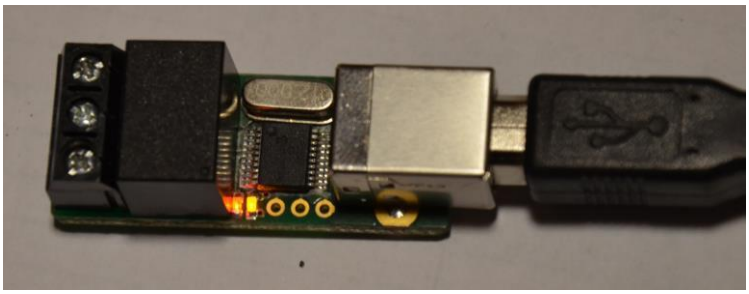

Obrázek č. 25 – Karta pro přístup do objektu

# Program USB relé

Na propojení databáze s elektronickým zámkem je využito USB[4] relé (obrázek č. 26 – USB relé). Relé je elektrická součástka, která obsahuje elektromagneticky ovládané vypínače[14]. Pro ovládání relé je použit program v C#, který se po úspěšném nahrání BAR kódu spustí pomocí

Visual Basic for Application v databázi. C# program otevře komunikaci s relé na portu

sepne relé a spustí časovač na 10 sekund. Po vypršení časovače relé rozepne a vypne se.



Obrázek č. 26 – USB relé

# Popis programu

1. Nastavení časovače

   V tomto příkazu se nastaví časovač na 10 sekund – hodnota Timer je nastavena v ms tzn. nastavení na hodnotu 10 000.

```
static Timer timer = new Timer(10000);
```

2. Otevření USB portu

   Sériová komunikace probíhá na portu **COM4** o rychlosti 9 600 baud[5].

```
SerialPort USB = new SerialPort("COM4", 9600, Parity.None, 8, StopBits.One);
```

3. Nastavení zařízení

   Připojení sériové komunikace k čipu MCP2200, který je součástí USB relé PUSBIO1R[17].

```
SimpleIOClass.InitMCP2200(0x4d8, 0xdf);
```

4. Sepnutí pinu

   Nastaví pin 7 na logickou 1, což sepne pin.

4 USB Universal Serial Bus – univerzální sériová sběrnice, moderní způsob připojení periferií k počítači [13].

[5] Baud – jednotka modulační rychlosti – počet změn za 1 s [16]

```
SimpleIOClass.SetPin(7);
```

5. Start časovače

   Spustí odpočet 10 sekund (viz první bod) časovače.

```
timer.Elapsed += timer_Elapsed;
timer.Start();
```

6. Průběh a konec časovače

   Po doběhnutí časovače do konce nastaví pin 7 na logickou 0, což rozepne relé a ukončí časovač.

```
private static void timer_Elapsed(object sender, ElapsedEventArgs e)
{
    SimpleIOClass.ClearPin(7);
    Environment.Exit(0);
}
```

7. Ukončení programu

   Cyklus **while** zajistí, aby program neskončil před uběhnutí časovače, poté se logicky odpojí sériový port a ukončí program.

```
USB.Close();
while (true) ;
```

8. Volání externího programu v databázi

   Pro spuštění C# programu je využit příkaz **shell**. Za příkaz **shell** se uvede celá cesta k programu. **Windoframe** je nastaven na 0, aby se nezobrazovala konzole programu.

```
Shell "C:\Users\Filip\OneDrive\Dokumenty\Dlouhodobápráce\USB_Control\try.exe", 0
```

# Cenové ohodnocení systému

| Zařízení | Typ | Funkce | Cena v Kč |
|---|---|---|---|
| USB relé | PUSBIO1R | Po přiložení BAR kódu a verifikace v databázi sepne relé | 417 |
| Databáze | MS Access 2010 | Po přiložení BAR kódu zapíše vstup a sepne USB relé | cca 5 000 |
| Systém MS Access | MS Access 2010 | Spuštění a správa dat pro přístup v databázovém systému | 3 832 |
| Čtečka BAR kódů | QuickScan QD2430 | Načtení BAR kódů, jejich dekódování a připsání do databáze | 3 647 |

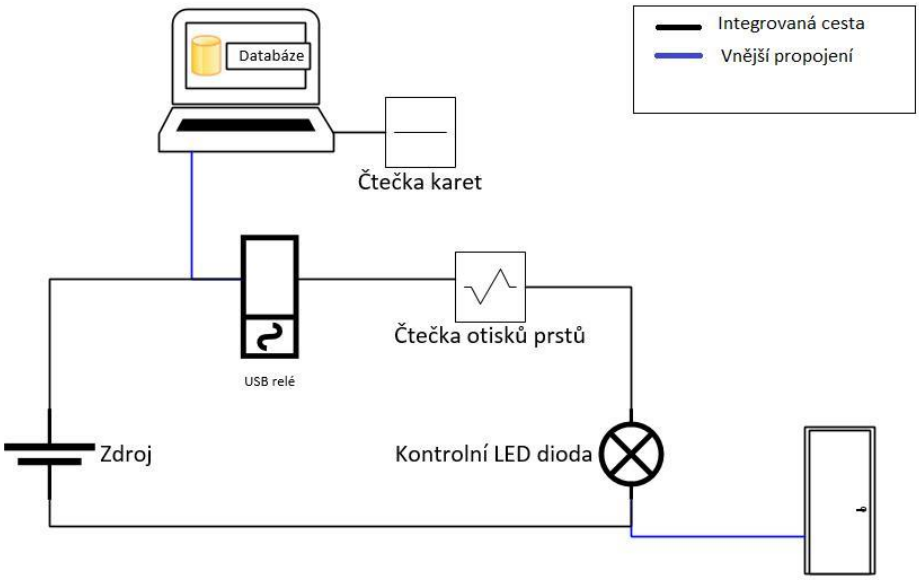
| | | | |
|---|---|---|---|
| Čtečka otisků prstů | Sebury 007 | Vstup pouze pro uživatele, jejichž otisk prstu je uložen ve čtečce | 3 266 |
| **Cena celkem** | | | **16 162** |

Tabulka č. 2 ceny

## Celková funkce systému

## Zapojení

Pro návrh zapojení je využit program Microsoft Visio. USB relé sepne, pokud uživatel vložil kartu a byl správně zapsán do databáze. Po přiložení, evidovaného otisku prstu a karty, se rozsvítí LED dioda a odemknou se bezpečnostní dveře. (Viz obrázek č. 27 – Návrh zapojení.)




Obrázek č. 27 – Návrh zapojení

# Závěr

Úkolem bylo vytvořit informační systém s aplikací biometrie na ovládání přístupu včetně evidence vstupů.

Vytvořená databáze přístupového systému v MS Access poskytuje systém pro podnik s max. 100 zaměstnanci. Systém má za úkol evidovat vstupy zaměstnanců a návštěv pomocí přístupových karet s BAR kódy. Tyto kódy jsou jako validace uživatele a jako verifikace je využita biometrie – otisk prstu zaměstnance v zapojení do série. Návštěva bude muset mít jako doprovod dozor, který bude přikládat otisk prstu, aby se splnilo sériové zapojení a rozsvítila se kontrolní dioda, popř. se odemkl elektronický zámek a vpustil je do podniku.

Databázi, která eviduje vstupy, je tvořena pomocí 6 tabulek s primárními klíči. Pro automatickou aktualizaci podformuláře, který po zapsání vstupu zobrazí posledních šest vstupů, je vytvořen dotaz. Pro jednodušší ovládání databáze jsou tři formuláře a jeden podformulář. První, tzv. úvodní formulář, automaticky spuštěný při načtení databáze, zajišťuje orientaci mezi zbylými formuláři. Druhý formulář zaznamenává vstupy zaměstnanců do tabulky a obsahuje automaticky aktualizovaný podformulář se záznamem posledních průchodů.

Poslední formulář slouží k orientaci mezi sestavami. Snazšího zpracování a vizualizaci dat z databáze je dosaženo pomocí sedmi sestav, což bylo i dalším úkolem. Databáze je navržena do 3. Normální formy. Jsou vytvořena integritní omezení (např. ochrana před zadním přes českou klávesnici). Zabezpečení je zajištěno heslem s šifrováním RC4. Tabulky jsou propojeny relacemi se správnou kardinalitou vztahů.

V práci jsou zhodnocena omezení a vhodnost použití různým biometrických metod. Následně je z důvodu dostupnosti čtečky na pracovišti vybrána metoda s aplikací otisků prstů. Podrobněji je rozepsáno měření výkonnosti biometrií a biometrická metoda otisků prstů.

Biometrickou metodu otisku prstu lze doporučit do méně frekventovaných oblastí objektu a to především z hygienických důvodů. Z hlediska bezpečnosti lze otisk prstu doporučit do objektů s menší bezpečností úrovní, jelikož nesplňuje podmínku „životnosti“ subjektu. Tzn., že při odstranění prstu mohou vzniknout komplikace, jako například neoprávněný přistup. Do objektů s vyšší bezpečnostní prověrkou lze doporučit biometrické zabezpečení např. pomocí sítnice oka, která podporuje životnost. Stejnou metodu lze doporučit i do frekventovanějších míst, protože je hygienicky šetrnější.

Z důvodu jednoduchosti a levného (zdarma) generování kódu je využit BAR kód – Code 128. Ten je obecně jedním z nejrozšířenější a podporuje i nejmenší čísla.

Čtečka Datalogic QuickScan QD2400 je vhodná pro maturitní práci i další použití ve škole, ale pro zavedení systému je vhodnější např. čtečka typu Honeywell Laser skener MS7120. A to především z důvodu možnosti pevného uchycení k systémové desce a nepřetržitého snímání kódů bez nutnosti mačkání tlačítka. Pro objekty s vyšším zabezpečením je vhodnější RFID čtečka a čipové karty, protože BAR kód se dá snáze padělat.

K identifikaci osob slouží karty s fotkou zaměstnance a osobním kódem v podobě BAR kódu typu Code 128. Velikosti karty je (85,6 × 54,0) mm. Karty jsou vytištěné na leský papír a jsou laminovány. Pro vyšší stupeň zabezpečení jsou vhodnější RFID karty, které jsou ale finančně podstatně náročnější.

Rozhraní aplikace pro využívání USB relé je vytvořena v prostředí Visual Studia a programovacího jazyku C#. Program po spuštění sepne relé na 10 sekund. Program se spouští v databázovém systému pomocí příkazu Shell.

Výstupem práce je finančně dostupná verze elektronické evidence přístupu do firmy s aplikací biometrických prvků, která zajišťuje validaci i verifikaci při evidenci vstupu osob do podniku.

# Citace

[1] ŠIROKÝ, Miroslav. *Informační systémy*. Interní materiály SPŠ a VOŠ Písek, Písek, 2015.

[2] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Ostrava, 2008 [cit. 2017-03-15]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/040/.content/sys-cs/resource/PDF/biometricke_metody.pdf

[3] RAK, Roman, et al. *Biometrie a identita člověka : ve forézních a komerčních aplikacích*. 1 vyd. Praha : Grada Publishing, a.s., 2008. 664 s.

[4] Validace. *Slovník cizích slov abz* [online]. 2013, 2017([132]), 1 [cit. 2017-03-15]. Dostupné z: http://slovnik-cizich-slov.abz.cz/web.php/slovo/validace

[5] Verifikace. *Slovník cizích slov abz* [online]. 2013, 2017([133]), 1 [cit. 2017-03-15]. Dostupné z: http://slovnik-cizich-slov.abz.cz/web.php/slovo/verifikace

[6] BAR kódy. *Kodys* [online]. Praha: Kodys, 2016 [cit. 2017-03-15]. Dostupné z: http://www.kodys.cz/carovy-kod.html

[7] Kardinalita vztahu. *Informační technologie* [online]. [Praha]: [Informační technologie], 2017 [cit. 2017-03-15]. Dostupné z: http://informacni-technologie.studentske.cz/2009/02/kardinalita-vztahu.html

[8] Vygenerované BAR kódy. In: *Barcode-generator* [online]. [Berlín]: [barcode-generator], 2014 [cit. 2017-03-15]. Dostupné z: http://www.barcode-generator.org/

[9] *Databáze* [online]. [Brno]: [Misha], 2010 [cit. 2017-03-15]. Dostupné z: http://www.databaze.chytrak.cz/

[10] Úvod k sestavám v aplikaci Access. *Support.office.com* [online]. [Redmond]: [Microsoft], 2017 [cit. 2017-03-15]. Dostupné z: https://support.office.com/cs-cz/article/%25C3%259Avod-k-sestav%25C3%25A1m-v-aplikaci-Access-e0869f59-7536-4d19-8e05-7158dcd3681c?ui=cs-CZ&rs=cs-CZ&ad=CZ&fromAR=1#__toc307733500

[11] Datalogic quickscan QD2400 2D. In: *Gaben* [online]. Ostrava: [Gaben], 2016 [cit. 2017-03-15]. Dostupné z: http://www.gaben.cz/cz/snimace-carovych-kodu/datalogic/datalogic-quickscan-qd2400-2d

[12] Tabulka krytí IP. In: *Elektrika.cz* [online]. [Praha]: [Elektrika.cz], 2016 [cit. 2017-03-15]. Dostupné z: http://elektrika.cz/data/clanky/krip030918

[13] USB: Universal Serial Bus. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2017 [cit. 2017-03-15]. Dostupné z: https://cs.wikipedia.org/wiki/Universal_Serial_Bus

[14] Relé. In: *Význam-slova.com* [online]. [Praha]: Význam slova, 2016 [cit. 2017-03-15]. Dostupné z: http://www.vyznam-slova.com/Rel%C3%A9

[15] RC4. In: *IT Network* [online]. [Praha]: IT Network, 2016 [cit. 2017-03-15]. Dostupné z: http://www.itnetwork.cz/algoritmy/ostatni/pod-poklickou-algoritmu-rc4

[16] Baud. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2017 [cit. 2017-03-15]. Dostupné z: https://cs.wikipedia.org/wiki/Baud

[17] Pandatron. *Pandatron* [online]. Vysoké Mýto: Pandatron.cz, 2017 [cit. 2017-03-14]. Dostupné z: http://pandatron.cz/?shop&sla=22&pn=90120&tx=pusbio1r_-_multifunkcni_rele_s_usb_rozhranim

[18] Úvod k RC4. *CHIP* [online]. 1999, 1999([9]), 1 [cit. 2017-03-18]. Dostupné z: http://crypto-world.info/klima/1999/chip-1999-09-42-44.pdf

[19] DES. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2017-03-18]. Dostupné z: https://cs.wikipedia.org/wiki/Data_Encryption_Standard

# Přílohy

**Příloha č. 1 – Sestavy**

**Příloha č. 2 – Specifikace čtečky otisků prstů**

**Příloha č. 3 – Ukázky karet zaměstnanců**

**Příloha č. 4 – Návod na spuštění**

**Příloha č. 1 – Sestavy**

## Celkový počet vstupů jednotlivých zaměstnanců

| Číslo zaměstnane | Jméno | Příjmení | Počet vstupů |
|---|---|---|---|
| 1 | Jan | Mišoň | 9 |
| 2 | Alex | Nosek | 8 |
| 3 | Tomáš | Klas | 2 |
| 4 | Lukáš | Kotalík | 3 |
| 5 | Martin | Měšťan | 11 |
| 6 | Filip | Hrubý | 12 |
| 7 | Josef | Šanda | 3 |
| 8 | Jan | Vítů | 1 |
| 9 | Marek | Valach | 7 |
| 10 | Návštěva | | 2 |

K datumu: 15.03.2017

## Počet vstupů dopoledne a odpoledne za jednotlivé zaměstnance

| | | | |
|---|---|---|---|
| Číslo zaměstnance: | 1 | Jméno zaměstnance: | Jan Mišoň |
| Počet vstupů dopoledne: | 2 | počet vstupů odpoledne | 7 |
| Číslo zaměstnance: | 2 | Jméno zaměstnance: | Alex Nosek |
| Počet vstupů dopoledne: | 1 | počet vstupů odpoledne | 7 |
| Číslo zaměstnance: | 3 | Jméno zaměstnance: | Tomáš Klas |
| Počet vstupů dopoledne: | 0 | počet vstupů odpoledne | 2 |
| Číslo zaměstnance: | 4 | Jméno zaměstnance: | Lukáš Kotalík |
| Počet vstupů dopoledne: | 0 | počet vstupů odpoledne | 3 |
| Číslo zaměstnance: | 5 | Jméno zaměstnance: | Martin Měšťan |
| Počet vstupů dopoledne: | 1 | počet vstupů odpoledne | 10 |
| Číslo zaměstnance: | 6 | Jméno zaměstnance: | Filip Hrubý |
| Počet vstupů dopoledne: | 4 | počet vstupů odpoledne | 8 |
| Číslo zaměstnance: | 7 | Jméno zaměstnance: | Josef Šanda |
| Počet vstupů dopoledne: | 0 | počet vstupů odpoledne | 3 |
| Číslo zaměstnance: | 8 | Jméno zaměstnance: | Jan Vítů |
| Počet vstupů dopoledne: | 0 | počet vstupů odpoledne | 1 |
| Číslo zaměstnance: | 9 | Jméno zaměstnance: | Marek Valach |
| Počet vstupů dopoledne: | 1 | počet vstupů odpoledne | 6 |
| Číslo zaměstnance: | 10 | Jméno zaměstnance: | Návštěva |
| Počet vstupů dopoledne: | 0 | počet vstupů odpoledne | 2 |

**Příloha č. 2 – Specifikace čtečky otisků prstů**

F007-EM

**Popis**

Čtečka otisků prstů a karet pro venkovní / vnitřní použití. Čtečku je možné zapojit do větších systémů pomocí výstupu Wiegand nebo je možné čtečku provozovat samostatně, kdy se jako výstup použije relé.

| | |
|---|---|
| **Autorizace** | Načtení otisku prstu uživatele, přiložení karty RFID 125kHz |
| **Počet uživatelů** | 160 uživatelů otisků prstů<br>2000 uživatelů karet |
| **Programování** | IR klávesnice,<br>Master prst, Master karta |
| **Výstup** | Výkonový tranzistor , Wiegand 26bit |

**Vlastnosti**

| | |
|---|---|
| Napájení | 12Vdc (10,5 – 13,5) |
| Odběr klid/aktivní | Max. 20/90mA |
| Dveřní relé | Tranzistor FET 2A / 12V |
| Doba aktivace relé | 00 – 99 sec. |
| Poplachový výstup | Tranzistor FET 2A / 12V |
| Doba poplachu | 00 – 99 min. |
| Pracovní teplota | -20 až 60°C |
| Prostředí | venkovní / vnitřní |
| Krytí | IP 53 |
| Kapacita paměti | max. 160 otisků a 2000 karet |
| Uživatelů | Celkem 2160 |
| Master | 2 master otisky (přidání, mazání) |
| Instalační kód | 1 x 4 číslice |
| Rozlišení snímání | 450dpi |
| Rychlost čtení | menší než 1s |
| Čas identifikace | menší než 2s |
| FAR False Accepted Rate (chybně povoleno) | méně než 0,0001% |
| FRR False Rejected Rate (chybně odmítnuto) | méně než 0,01% |
| Provedení | masivní kovový box |
| Rozměry | 115 x 70 x 35 mm |
| Hmotnost | 500g |

**Připojení k napětí**

Po připojení k napětí čtečka přejde do režimu čtení, který je signalizován blikající červenou LED.

**Příloha č. 3 Ukázky karet zaměstnanců**






Příloha č. 4 – Návod na spuštění

Pro instalaci systému dodržujte předepsané kroky:

1. Připojte USB relé.
2. Ve správci zařízení zjistěte na, který čílo COM portu "x" je připojeno USB relé.
3. Zjištěný číslo "x" COM portu přepište v "USB.sln" místo COM 4 na COM x.
4. Relese tento program a změňte jméno z "@try" na "try" či jiné vámi libovolné jméno.
5. Spusťte systém v MS Access zadejte heslo "Admin".
6. V návrhovém zobrazení formuláře Záznam vstupu klikněte na tlačítko "Zobrazit kód".
7. V editaci kódu u příkazu "Shell" uveďte novou cestu k programu.