**Univerzita Pardubice**
**Fakulta ekonomicko-správní**
**Ústav systémového inženýrství a informatiky**

# Integrace biometrických prvků do firemních přístupových systémů

**Daniel Šturma**

**Bakalářská práce**
**2025**

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2024/2025

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

| | |
|---|---|
| Jméno a příjmení: | **Daniel Šturma** |
| Osobní číslo: | **E22692** |
| Studijní program: | **B0688A140004 Informatika a systémové inženýrství** |
| Specializace: | **Informační a bezpečnostní systémy** |
| Téma práce: | **Integrace biometrických prvků do firemních přístupových systémů** |
| Zadávající katedra: | **Ústav systémového inženýrství a informatiky** |

## Zásady pro vypracování

Cílem práce je návrh nového přístupového systému s integrací biometrických prvků pro zlepšení zabezpečení ve firmě.

Osnova:
- Úvod do problematiky přístupových systémů.
- Využití biometrických prvků v přístupových systémech.
- Popis současného stavu v dané oblasti ve vybrané firmě.
- Návrh nového přístupového systému s integrací biometrických prvků.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

BLOKDYK, Gerardus. Access Control Systém A Complete Guide – 2020 Edition. Vyd. Toronto: 5STARCooks, 2021. ISBN 978-1867340690.
KYNCL, Jaromír. Bezpečnost objektu ve světle moderních technologií. Vyd. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-8026071150.
MALTONI, Davide; MAIO, Dario; JAIN, Anil, PRABHAKAR, Salil. Introduction to Biometrics. Vyd. New York: Springer US, 2014. ISBN 978-1489985439.
SINJINI, Mitra; GOFMAN, Mikhail. Biometrics in a data driven world: trends, technologies, and challanges. 1. vyd. Boca Raton: CRC Press, Taylor & Francis, 2017. ISBN 978-1498737647.

Vedoucí bakalářské práce: **Ing. Renáta Máchová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2024**
Termín odevzdání bakalářské práce: **30. dubna 2025**

L.S.

**prof. Ing. Jan Stejskal, Ph.D.** v.r.
děkan

**prof. Ing. Jitka Komárková, Ph.D.** v.r.
garant studijního programu

V Pardubicích dne 1. září 2024

## PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci s názvem „Integrace biometrických prvků do firemních přístupových systémů“ vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 04. 2025

Daniel Šturma

**PODĚKOVÁNÍ**:

Tímto bych rád poděkoval své vedoucí bakalářské práce Renátě Máchové za její odborné vedení, cenné rady a poskytnuté materiály. Dále děkuji firmě XY za spolupráci a poskytnutí potřebných informací. Poděkování patří také mé rodině a přátelům za morální podporu během tvorby této práce.

## ANOTACE

*Bakalářská práce se zaměřuje na návrh nového přístupového systému s integrací biometrických prvků. V první části je uveden úvod do problematiky přístupových systémů, následně jsou popsány biometrické prvky s možnostmi jejich využití. Ve druhé části je představen současný stav zabezpečení firmy a následně je navržen nový přístupový systém s integrací biometrických prvků.*

## KLÍČOVÁ SLOVA

*Biometrie, mechanické a elektronické přístupové systémy, přístupové systémy, zabezpečení, návrh přístupového systému*

## TITLE

Integration of Biometric Elements into Corporate Access Control Systems

## ANNOTATION

*The bachelor's thesis focuses on the design of a new access control system with the integration of biometric elements. The first part introduces the topic of access control systems and describes biometric technologies along with their possible applications. The second part presents the current state of the company's security and subsequently proposes a new access control system integrating biometric elements.*

## KEYWORDS

*Biometrics, mechanical and electronic access control systems, access control systems, security, access control system design*

# OBSAH

## SEZNAM TABULEK

# SEZNAM OBRÁZKŮ

# SEZNAM ZKRATEK

2FA – Dvoufaktorová autentizace

CSV – Typ souboru v programu Excel

FAR – False Accaptance Rate (míra falešného přijetí)

FBI – Federal Bureau of Investigation

FRR – False Rejection Rate

GPDR – General Data Protection Regulation

IT – Informační Technology

NFC – Near Field Communication

PIN – Personal Identification Number

PIV – Personal Identity Verification

RFID – Radio-Frequency Identification

USB – Flash disk (Universal Seriál Bus)

# ÚVOD

S rostoucí digitalizací a technologickým pokrokem ve světě, neustále narůstá potřeba efektivní ochrany citlivých informací a majetku. Firmy a instituce čelí stále sofistikovanějším hrozbám, a proto je zajištění bezpečnosti jedním z nejpodstatnějších prvků jejich fungování. Mechanické a elektronické přístupové systémy, jako jsou mechanické zámky nebo přístupové karty, jsou v některých případech dostačující, ale nejsou dokonalé.

Biometrické systémy, které využívají naše unikátní fyziologické a behaviorální charakteristiky, proto představují významnou možnost řešení, jak naše přístupové systémy vylepšit a tím zvýšit úroveň zabezpečení. V kombinaci s mechanickými či elektronickými metodami, jako jsou hesla, PINy či karty, dokážou biometrické prvky přinést vyšší zabezpečení se záložními metodami pro přihlášení, čímž poskytují robustní ochranu proti neoprávněnému přístupu.

Tato práce se zaměřuje na možnosti, jak se vyhnout nedostatkům v mechanických a elektronických přístupových systémech za pomoci integrace biometrie. Práce se konkrétně zaměřuje na ochranu majetku a citlivých dat jak ve fyzické, tak i virtuální podobě ve firmě. Dále se zabývá problematikou přístupových systémů, typy přístupových systémů, využití biometrických prvků v přístupových systémech a legislativou a právními aspekty spojenými s biometrickými technologiemi.

Cílem práce je návrh nového přístupového systému s integrací biometrických prvků pro zlepšení zabezpečení ve firmě.

V této práci bude nejprve popsán úvod do problematiky přístupových systémů, dále bude popsáno využití biometrických prvků v přístupových systémech. Následně bude popsán současný stav v dané oblasti ve vybrané firmě a na závěr bude navržen nový přístupový systém s integrací biometrických prvků.

# 1. LEGISLATIVA TÝKAJÍCÍ SE PŘÍSTUPOVÝCH SYSTÉMŮ

Využití přístupových systémů ve firmách, ať už mechanických, elektronických nebo biometrických, podléhá právním předpisům zaměřeným na ochranu osobních údajů a bezpečnost. Základním legislativním rámcem v Evropské unii je Obecné nařízení o ochraně osobních údajů (GDPR, Nařízení EU 2016/679), které stanovuje podmínky pro zpracování osobních údajů, včetně biometrických. Biometrická data, jako jsou otisky prstů nebo rozpoznávání obličeje, jsou považována za citlivé údaje a jejich použití je možné jen za jasně definovaných podmínek, například na základě oprávněného zájmu (například zajištění bezpečnosti) nebo zákonné povinnosti (pokud zákon výslovně žádá po firmě nebo organizaci použití biometrických dat).[1]

V českém právním prostředí doplňuje GDPR Zákon č. 110/2019 Sb., o zpracování osobních údajů, který upřesňuje některé výjimky a povinnosti správců údajů. Zaměstnavatelé využívající přístupové systémy musí respektovat i Zákon č. 262/2006 Sb., Zákoník práce, který chrání soukromí zaměstnanců a omezuje možnosti monitorování jejich docházky. [2][3]

Firmy musí při zavádění jakéhokoli přístupového systému zajistit, že zpracování osobních údajů je přiměřené a odůvodněné. U mechanických a elektronických systémů, jako jsou karty nebo kódy, je právní regulace nižší, protože obvykle nezpracovávají citlivé údaje. U biometrie je nutné provést posouzení vlivu na ochranu osobních údajů, informovat subjekty (jako například zaměstnanci firmy nebo externí dodavatelé) o účelu a způsobu zpracování a zavést bezpečnostní opatření proti neoprávněnému přístupu nebo zneužití dat. Přednost by měly mít méně invazivní metody, pokud jsou pro daný účel dostatečné. [1][3]

# 2. ÚVOD DO PROBLEMATIKY PŘÍSTUPOVÝCH SYSTÉMŮ

Využití přístupových sytému sahá až do dávné minulosti, což dokládají archeologické nálezy z oblastí Mezopotámie a Egypta. Jedná se o první formy zámků, často jednoduché dřevěné závory k zajištění dveří, později vyvinuté z kovů, jako je bronz a železo. Starověké civilizace se tak snažily chránit svůj majetek a prostor, což bylo důležité zejména po zemědělské revoluci. Zhruba okolo 1. století našeho letopočtu byl tento typ zámku zdokonalen Římany. Většina zámků objevených po tomto období se těmto velice podobá, včetně některých zámků dnešních.

S příchodem 20. století a rozvojem elektroniky se objevily první elektronické přístupové systémy, jako jsou karty s magnetickým pruhem, čipové karty a PIN kódy. Tyto technologie umožnily centralizovanou kontrolu přístupu, což výrazně zvýšilo flexibilitu, účinnost a správu bezpečnostních opatření. Mechanické zámky a klíče byly postupně v budovách s vysokou potřebou ochrany nahrazovány sofistikovanějšími elektronickými systémy, které poskytovali vyšší úroveň ochrany majetku, citlivých dat či informací. Tato zlepšená bezpečnost byla dosažena nejen tím, že byli tyto elektronické systémy mnohem odolnější vůči narušitelům, tak i tím že čipové karty mohli být po jejich ztrátě jednoduše vymazány ze systému a nahrazeny novými.

Tyto mechanické a elektronické přístupové systémy mají ale též své limity. Pokud uživatel ztratí autentizační prostředek, může se před vymazáním této karty ze systému dostat do chráněných prostor neoprávněná osoba. Tyto systémy mohou být dále náchylné k útokům, jako je kopírování identifikačních karet, prolomení PIN kódu tzv. Brute-Force a v některých případech stačí pouhé vytvoření kopie fyzických klíčů. Tyto bezpečnostní nedostatky vedly k potřebě rozvoje nových technologií, které by tyto slabiny snížily nebo i dokonce eliminovali.

Právě v reakci na tyto nedostatky se v posledních desetiletích prosazují biometrické přístupové systémy. Jedná se například o otisky prstů, obličejové rysy, oční retinu nebo hlas jedince. Biometrie téměř eliminuje potřebu fyzických klíčů nebo karet, čímž snižuje riziko přístupu neoprávněné osoby do prostor. Další výhodou je i pohodlí uživatele, kteří si nadále nemusí pamatovat hesla či nosit identifikační karty.

Moderní zabezpečení často kombinují mechanické či elektronické a biometrické přístupové systémy. Tento přístup známý jako dvoufaktorová autentizace, zvyšuje úroveň zabezpečení tím, že kombinuje více autentizačních prvků. To sebou ale přináší i otázku, zda neklesá úroveň zabezpečení dosaženého využitím biometrie, která má právě mechanické a elektronické systémy nahradit.

S pokrokem v oblasti umělé inteligence, automatizace a robotiky se ochrana přesouvá na novou úroveň. V některých prostředích jsou nasazeny složité algoritmy, které zkoumají nahrávky z kamer, detekují neobvyklé chování a upozorňují na bezpečnostní hrozby. Fyzická přítomnost strážných se tak začíná měnit na dozor nad moderními technologiemi, zatímco lidé se zaměřují na řešení komplexních situací, které vyžadují lidské rozhodování.

# 3. TYPY PŘÍSTUPOVÝCH SYSTÉMŮ

Tato kapitola se zaměřuje na jednotlivé typy přístupových systémů a jejich využití. Nejprve jsou představeny mechanické a elektronické přístupové systémy, které zahrnují mechanické zámky, čipové karty, PIN kódy nebo magnetické karty, a jejich role v zabezpečení. Následně se kapitola věnuje biometrickým přístupovým systémům, které využívají fyziologické nebo behaviorální charakteristiky jednotlivců k identifikaci a autentizaci uživatelů. V potaz jsou brány výhody i omezení jednotlivých přístupových metod s ohledem na bezpečnost, uživatelský komfort a možnosti integrace v moderních přístupových systémech.

Základní princip, na kterém přístupové systémy fungují, je mechanický nebo elektronický mechanismus, který fyzicky uzamyká dveře, například pomocí **deadboltu**. Tento mechanismus funguje na stejném principu, ať už je odemykán klíčem, čipovou kartu nebo jakoukoli jinou elektronickou či biometrickou autorizací. Rozdíl tedy spočívá především v metodě ověření uživatele.[4][5]

## 3.1. Mechanické a elektronické přístupové systémy a jejich využití

Mechanické a elektronické přístupové systémy zajišťují kontrolu a zabezpečení přístupu tím, že určují, kdo může a kdo nemůže vstoupit do určitých prostor nebo získat přístup k citlivým informacím ukládaným na elektronických zařízení. Tyto systémy umožňují přístup pouze určitým osobám, kterým bylo přiděleno konkrétní oprávnění. Pro uživatele, kterým bylo toto oprávnění přiděleno, přináší elektronické přístupové systémy pohodlnější a rychlejší pohyb mezi prostory nebo mezi firemními dokumenty v počítačových systémech. Identifikace v rámci těchto systémů probíhá například pomocí RFID karet. Každý typ systému má své specifické výhody a nevýhody, které je důležité zvážit před jejich integrací do používání. [4][5]

**Hlavní prvky přístupového systému:**

**Autentizace** je proces, kterým je ověřena identita uživatele. Například pokud uživatel zadá své uživatelské jméno a heslo na bankovní účet, e-mail, Facebook a podobně je jejich osobnost autentizována. Tento proces ale není vždy dostatečný, jelikož se ověřuje pouze identita a ta sama o sobě neomezuje, k čemu má uživatel přístup. [4][5]

V některých případech může systém při autentizaci vyžadovat dodatečné potvrzení totožnosti uživatele pomocí dvoufaktorové autentizace (2FA), zejména při přístupu k citlivějším informacím nebo provádění určitých akcí. Pro autentizaci se může používat jednorázově vygenerovaný kód, fyzický klíč například ve formě USB disku, biometrie jedince

nebo jiné metody. Tento proces má zajišťovat, že uživatel nemá pouze správné přístupové údaje, ale že se jedná přímo o uživatele s těmito právy. [4][5]

**Autorizace** je další ochranou vrstvou ověřovacího procesu. Jedná se o přiřazení práv a oprávnění systémem, určuje, k čemu konkrétně má tento uživatel přístup po ověření své identity. I když je tedy uživatel autentizován správnými údaji, autorizace zajišťuje, že má přístup pouze k určitým datům nebo může provádět pouze určité akce, například číst data ale nikoli je spravovat. [5][6]

**Přístup** k požadovanému zdroji je udělen poté, co uživatel úspěšně dokončí autentizaci a systém autorizaci. [4][5]

**Správa** přístupových systémů umožňuje organizacím flexibilně přidávat nebo odstraňovat autentizační a autorizační oprávnění pro různé uživatele a systémy. V dnešních složitých IT prostředích, která kombinují cloudové služby s lokální infrastrukturou, však může být tento proces náročný na koordinaci a údržbu. To zapříčiňuje růst organizace, časté změny uživatelů a rolí, různé úrovně zabezpečení a složité přístupové modely, legislativní požadavky a další. [4]

**Audit** v přístupových systémech slouží k monitorování a hodnocení všech přístupů a aktivit uživatelů, aby bylo dohledatelné, zda jsou přístupová práva využívána správně a v souladu s bezpečnostními zásadami organizace. [4]

### 3.1.1. Mechanické přístupové systémy

Mechanické přístupové systémy jsou starším způsobem zabezpečení objektů, který využívá fyzické prvky, jako jsou klíče a mechanické kódové zámky. Tyto systémy nevyžadují elektroniku ani napájení a spoléhají se na mechanické zamykací mechanismy pro kontrolu přístupu.

**Zámky a klíče**

Zámky a klíče jsou standartní a nejjednodušší typ přístupového systému pro zabezpečení budov, automobilů a většiny domácností. Nejpoužívanějším typem mechanického zámku je takzvaný cylindrový zámek, který funguje na principu stavítek s pružinami, které se po vsunutí klíče narovnají do požadované polohy a umožní tak otočení klíčem, který spustí otáčení cylindru. Ten ale funguje pouze jako komponent, který umožňuje odemknutí celého zámkového mechanismu. Cylindr se při otáčení zachytí o zub kovové závory čímž jí otočením posouvá přímo do otvoru, v rámu dveří, nebo naopak z otvoru vysouvá při odemykání. [7][8]

**Mechanické kombinační zámky**

Mechanické kódové zámky jsou bez klíčovým přístupovým systémem, který umožňuje otevření dveří nebo jiného zabezpečeného prostoru pomocí správné číselné kombinace. Tento typ zámku nepoužívá žádné elektronické prvky a funguje pouze na základě mechanického nastavení kombinace a přesného zarovnání vnitřních součástí. [9]

Základním principem těchto zámků je sada otočných kotoučů nebo disků, které jsou uvnitř propojeny s blokovacím mechanismem. Každý kotouč obsahuje zářez, který musí být, při správném zadání kódu, zarovnán s odemykacím mechanismem. Pokud uživatel otočí číselníkem na správné hodnoty a ve správném pořadí, všechny kotouče se postupně nastaví do správné polohy, což umožní odemknutí závory nebo uvolnění deadboltu. [9]

Tyto zámky jsou často využívány na trezorech, zavazadlech, skříňkách nebo zabezpečených dveřích, kde je potřeba eliminovat riziko ztráty klíče, přičemž stále poskytují bezpečnostní ochranu bez nutnosti elektronického napájení. [9]

Dnes už nejsou tak často využívány v oblasti přístupových systémů do objektů, z důvodu nízké ochrany a jednoduchého prolomení. [9]

### 3.1.2. Elektronické přístupové systémy

Elektronické přístupové systémy využívají elektricky řízené mechanismy k ověření oprávnění uživatele a umožnění přístupu. Tyto typy přístupových systémů umožňují efektivní kontrolu vstupu bez nutnosti použití mechanických klíčů. Elektronické přístupové systémy jsou široce využívány v zabezpečení budov, přístupu do chráněných prostor a správě docházky. [11][12]

**Čipové karty**

S čipovými kartami se dnes díky jejich širokému uplatnění lze setkat na mnoha místech. Jejich využití sahá od platebních systémů a identifikačních karet až po přístupové systémy budov. [11][12][14]

Čipové karty obsahují integrovaný mikročip, který umožňuje ukládat a zpracovávat data. Tato data, která mohou zahrnovat identifikační čísla, přístupová práva a další informace, se načítají pomocí čtečky. Čtečka následně ověří oprávnění a na základě toho povolí, nebo zamítne přístup. Existují ve dvou hlavních variantách [11][12][14]:

- **Kontaktních karty,** obsahují čip samotný a k němu je připojen vodivý materiál, který je viditelný i z vnější strany karty. Tento typ vyžaduje fyzický kontakt se čtečkou, kdy je karta vložena do zařízení, s kterým je navázán kontakt pomocí

vodivého materiálu, které umožňuje přenos dat. Tento typ karty se často používá u platebních terminálů nebo SIM karet v mobilních telefonech.

- **Bezkontaktní karty** využívají RFID nebo NFC technologie pro bezdrátovou komunikaci se čtečkou, a proto se stačí k zařízení kartou pouze přiblížit a dojde k bezdrátovému přenosu dat. Typickým příkladem tohoto typu karty jsou karty pro vstupy do budov nebo i moderní bezkontaktní platební karty.

Vzhledem k tomu, že čipové karty často uchovávají citlivá data, je bezpečnost hlavním aspektem. Pro zajištění bezpečnosti se používají i další mechanismy:

**Šifrování:** Data se během přenosu mezi kartou a čtečkou šifrují, čímž se ztíží jejich neoprávněné přečtení. Některé karty dokonce využívají dynamické šifrování, kde se pro každou operaci používají unikátní klíče a algoritmy. K těmto šifrování dochází buď při přenosu dat, nebo jsou data na kartě již zašifrována. To znemožňuje útočníkovi zneužít odcizený klíč pro opakované transakce. [10][11][14]

**Kryptoprocesory:** Jedná se o specializované čipy, které provádějí kryptografické operace přímo na kartě. To umožňuje generování, ukládání a správu šifrovacích klíčů a zvyšuje celkovou bezpečnost systému. [10][13]

Čipové karty vyžadují pro přenos informací externí zdroj energie, jelikož obvykle vlastní zdroj, jako je baterie nebo akumulátor neobsahují. Místo toho se spoléhají na energii dodávanou čtečkou. U kontaktních karet je energie předávána při fyzickém kontaktu se čtečkou, při vložení karty do čtečky, je elektrický proud okamžitě přenášen, což aktivuje čip na kartě a umožňuje mu provádět potřebné operace. Bezkontaktní karty využívají technologii elektromagnetického pole pro přenos energie, při přiblížení karty ke čtečce, zachytí karta elektromagnetické pole generované čtečkou, čímž je čip na kartě aktivován, tímto je eliminována nutnost fyzického kontaktu. Dnešní čipové karty často kombinují oba přístupy, což umožňuje jejich použití jak při fyzickém kontaktu, tak při bezkontaktní interakci se čtečkou.[10]

Čipové karty přináší mnohé výhody oproti například tradičním klíčům, vyšší úroveň zabezpečení, jelikož je obtížné je zkopírovat nebo zfalšovat, snadnou správu a nastavení přístupových prvá pro různé uživatele, tím že administrátor může definovat kdo má přístup do kterých prostor v jakém čase a také že ze systému je možné snadno v případě ztráty kartu vymazat, nebo dočasně zablokovat. [11][12][13]

Nevýhodou těchto systémů je vysoká pořizovací cena a že i přes vysokou úroveň zabezpečení existují techniky, jak data z karet zkopírovat. [14]

**RFID tagy**

RFID neboli identifikace na základě rádiových frekvencí. Využívá se od identifikace zboží v obchodech, tagy na drahém zboží jako ochrana proti krádeži, sledování zásilek v logistice, pozorování pozic hlídek okolo objektů, co potřebují ochranu až po přístup do budov či evidence docházky a dalších využití. [14][15][16][17]

Systém se skládá ze tří hlavních částí: RFID tagu, který obsahuje mikročip s jedinečným identifikačním číslem a anténu pro komunikace, RFID čtečky, která zachytává signál z tagu, a softwaru pro zpracování a analýzu nasbíraných dat. RFID čtečka vysílá rádiový signál, který aktivuje tag (v případě pasivního tagu), nebo komunikuje přímo s aktivním tagem, který má vlastní zdroj energie. [14][15][16][17]

Skládá se ze tří základních komponentů [16][18]:

**RFID tag:** jedná se o malé zařízení obsahující mikročip s uloženým identifikačním číslem a anténou pro komunikaci. Tagy mohou být pasivní (bez vlastního zdroje energie) nebo aktivní (s vlastním zdrojem energie).

**RFID čtečka:** Jedná se o zařízení, které vysílá rádiové vlny, ty aktivují RFID tag, který začne vysílat informace zpět ke čtečce která je přijímá. Následně informace z tagu dekóduje a předává je do systému pro další zpracování.

**Software:** Software ke zpracování a analýze dat z RFID tagů. Může se jednat o jednoduchý systém pro evidenci docházky nebo o komplexní systém pro správu skladu.

RFID tagy se dále dělí na dva základní typy [8][14][16][17][18]:

**Pasivní RFID:** Tento typ nemá vlastní zdroj energie a spoléhá na energii vysílanou čtečkou. Když se pasivní tag dostane do blízkosti čtečky, elektromagnetické pole čtečky tag aktivuje. Po aktivaci začne tag modulovat a vysílat signál, aby předal své uložené informace zpět ke čtečce. Pasivní RFID tagy se běžně využívají pro krátké vzdálenosti (od několika centimetrů po několik metrů), například u docházkových systémů, skladových položek v maloobchodě anebo knihovnách kvůli jejich nízké ceně.

**Aktivní RFID:** Aktivní tagy naopak vlastní zdroj energie obsahují, díky čemuž mohou vysílat svůj signál samostatně bez nutnosti externí aktivace. Vlastní zdroj jim také umožňuje komunikovat s čtečkami na větší vzdálenosti (až několik desítek metrů) a umožňují přenos většího množství dat. Často se používají v logistice nebo sledování vozidel a majetku, kde je nutný větší dosah a vyšší přenos dat.

Aktivní RFID tagy se dále dělí na „transpondéry“ a „beacony“ [17][18]:

**Transpondéry:** Ty se aktivují v okamžiku, kdy přijmou rádiový signál od čtečky, a poté vysílají svůj signál zpět.

**Beacony**: Na rozdíl od transpondérů, slouží pro sledování v reálném čase a nejsou aktivovány čtečkou. Místo toho jsou neustále v provozu a vysílají rádiový signál v reálném čase, nebo v předem nastavených intervalech, které mohou být nastaveny na sekundy, minuty, hodiny či dokonce dny.

RFID systémy pracují v různých frekvenčních pásmech, která ovlivňují dosah a rychlost přenosu dat. Mezi nejčastěji používaná pásma patří [15][18]:

**Nízké frekvence:** Mají pouze krátký dosah do 10 cm a nízkou rychlost přenosu dat. Využívají se pro identifikaci zvířat a kontrolu přístupu.

**Vysoké frekvence:** Střední dosah do 1 m s vyšší rychlostí přenosu dat. Často využívány pro bezkontaktní platby.

**Ultra vysoké frekvence:** Dlouhý dosah až 12 m s vysokou rychlostí přenosu dat. Používané pro logistiku a sledování zásilek.

**Mikrovlnné frekvence:** Velmi dlouhý dosah až 100 m s vysokou rychlostí přenosu dat. Vhodná pro sledování vozidel a mýtné systémy.

U tohoto typu přístupového systému je výhodou bezkontaktní identifikace, díky které je urychlen proces kontroly přístupu, nízká pořizovací cena RFID tagů, je snadno přizpůsobitelný různým potřebám, moderní RFID systémy disponují i šifrováním a dalšími bezpečnostními prvky. [16][17]

Nevýhodou může být nákladnost zavedení, zranitelnost, co se týče čtení a kopírování dat z tagu či rušení signálu kvůli velkému množství rádiových vln, což může ovlivnit spolehlivost systému. [16]

**Magnetické karty**

Magnetické karty jsou dalším typem způsobu pro ukládání dat pro účely identifikace a kontroly přístupu. I přes to, že se jedná o technologii zastaralou a v mnoha případech nahrazenou technologiemi jako čipové karty nebo RFID tagy, stále se s nimi lze setkat v mnoha oblastech. Uplatnění si nacházejí v podobě vstupních karet do budov, v hotelech pro přístup do pokojů, jako permanentky do fitness center nebo identifikační karty na školách, a to z jednoduchého důvodu cenové dostupnosti a spolehlivosti. [14][19]

Nejčastěji je možné je spatřit právě v podobě karty, ale v některých případech se může jednat o přívěšek, klíčenku nebo dokonce ve formě jízdenky či vstupenky. Všechny tyto podoby obsahují tenkou vrstvu magnetického materiálu, ve kterém jsou drobné magnetické částice. Tyto částice se chovají jako miniaturní magnety a mohou být polarizovány v jednom ze dvou směrů. Je možné si tento proces představit jako přepisovaní řady nul a jedniček představující směr magnetizace, pomocí změny magnetické polarity částic. [14]

Magnetický proužek je běžně rozdělen do tří stop, dle standardu ISO/IEC 7813. Data se zapisují přímo do jednotlivých stop, na magnetickém proužku, kde každá stopa, může být naprogramována specifickými údaji. [14][19][20]

Při přiblížení nebo protažení karty čtečkou čtecí zařízení detekuje specifické vzory v magnetickém poli. Čtečka snímá tyto vzory a převádí je do digitální podoby, v které dále provádí dekódování a zpracování informace pro identifikaci nebo autentizaci uživatele. [19]

Mezi výhody tohoto systému patří nízká nákladovost na výrobu i použití, jednoduchost a snadná implementace a taky jejich odolnost neboli že data na nich uložená jsou relativně trvanlivá. [14][19]

Bohužel mají tyto karty velké nevýhody, kvůli kterým nejsou často viděny v přístupových systémech s vysokou úrovní zabezpečení. Data na nich se dají relativně snadno zkopírovat nebo smazat, magnetické proužky mají omezenou kapacitu pro ukládání dat a při špatném zacházení se mohou poškodit poškrábáním či vystavením magnetickému poli. [14][19]

**PIN kódy**

PIN kódy (Personal Identification number) jsou číselné kódy které slouží jako základní způsob ověření identity uživatele. Nejčastěji se lze setkat s kódem čtyřmístným, ale i delším. Slouží jako jednoduché ale rychlé řešení autentizace v mnoha oblastech, včetně přístupových systémů. Je možné se s nimi setkat u platebních karet ve formě CVV kódu, mobilních telefonů, bankovních účtů, počítačů a notebooků nebo pro aktivaci a deaktivaci alarmů a dalších bezpečnostních systémů. [14][21]

PIN kódy fungují na velice jednoduchém principu, uživatel zadá svůj PIN kód na klávesnici nebo na displeji zařízení. Systém následně porovná kód zadaný uživatelem s kódem uloženým v databázi, pokud se tyto dva kódy shodují, identita uživatele bude ověřena a bude mu udělen přístup. [14][18][21]

Jejich bezpečnost závisí primárně na jejich délce a složitosti. Čtyřmístný PIN kód lze totiž relativně snadno prolomit hrubou silou, protože existuje pouze deset tisíc možných kombinací.

Tomu se dá ale relativně snadno předejít přidáním více číslic, nebo v lepším případě v kombinaci čísel s písmeny a různými symboly, v tomto případě se již ale nejedná o PIN ale o heslo. [14][21][22]

Jako další bezpečnostní opatření se dá zavést dvoufaktorová autentizace nebo omezený počet pokusů zadání kódu, kdy po překročení se může zařízení zablokovat, nebo dokonce smazat všechna na něm uložená data. [5][21]

Největšími výhodami těchto kódů je jejich jednoduchost na zapamatování a použit, rychlost autentizace a velice nízké náklady na zavedení. [21]

Tyto kódy sebou ale nesou i velké nevýhody, jako je nízká bezpečnost kvůli snadnému prolomení, lidský faktor ve formě zapomnětlivosti a hrozby „prokecnutí“ kódu nebo okoukání kódu neoprávněnou osobou. [21]

I přes tyto nevýhody jsou PIN kódy vysoce využívaným typem zabezpečení našich zařízení, bankovních účtů a různých přístupových systémů právě díky zmiňované jednoduchosti. [21]

**NFC čipy**

NFC (komunikace v blízkém poli) je bezdrátová technologie, která umožňuje snadnou a bezpečnou výměnu dat mezi dvěma zařízeními na krátkou vzdálenost, obvykle do 4 cm a maximálně 20 cm. S NFC se lze setkat na denní bázi v mnoha oblastech. Nejčastěji je lze spatřit v podobě bezkontaktních plateb mobilním telefonem, v přístupových systémech využívající buď telefony pro vstup, karty se zabudovaným NFC nebo v některých případech dokonce NFC čipech zabudovaných v dlani uživatele. Dále se využívá pro identifikaci osob, sdílení dat či jako reklama s NFC tagem umístěným například na plakátu, který umožňuje zákazníkům získat další informace o produktu pouhým přiložením telefonu k tagu. [6][14][15][23]

Tato technologie využívá elektromagnetické pole, které jedno zařízení vytváří, například čtečka, a druhé zařízení jej detekuje. Komunikace mezi těmito zařízeními probíhá na frekvenci 13,56 MHz, která je využívána i technologií RFID. Tato technologie se dělí na pasivní a aktivní [6][23]:

**Pasivní NFC:** To nedisponuje vlastním zdrojem, na místo toho získává energii právě z elektromagnetického pole generovaného čtečkou, tímto se i čip probouzí a umožní odeslání informací do čtečky. Tento typ NFC je schopný data, na něm uložená, pouze odesílat, ale číst data jiná nemůže.

**Aktivní NFC:** Zařízení, například chytrý telefon, na rozdíl od pasivních, obsahují vlastní zdroj energie, což umožňuje vytvářeni vlastního elektromagnetického pole. Tato vlastnost umožňuje oboustrannou komunikaci mezi čtečkou a NFC čipem, nebo mezi dvěma zařízeními vybavenými NFC čipem. Což znamená že zařízení může nejen data odesílat, ale také přijímat.

NFC čipy mohou také fungovat v různých režimech [6][15][23]:

**Režim čtení/zápis:** Zařízení v tomto režimu NFC čte informace například z NFC štítku nebo je zapisuje.

**Emulace karty**: Jedná se o zařízení, které se chová například jako bezkontaktní karta. S tímto zařízením je možné přijít do kontaktu v podobě mobilního telefonu, který napodobuje funkce debetní karty nebo karty přístupové.

**Peer to peer režim:** Tento režim umožňuje výměnu dat mezi dvěma NFC zařízeními, lze využít pro sdílení kontaktů či souborů. Toto umožňují pouze aktivní NFC čipy.

NFC komunikace se zabezpečuje pomocí šifrování a autentizace, aby bylo zabráněno neoprávněnému přístupu k datům. Data se před přenosem šifrují, aby se zabránilo jejich odposlechu a dále zařízení často vyžadují autentizaci například pomocí pin kódu nebo otisku prstů či skenu obličeje. [6]

Výhodou této technologie je pohodlí a rychlost, jelikož stačí pouze přiložit kartu nebo telefon ke čtečce a během několika milisekundu je hotovo, jsou také vysoce bezpečné díky šifrování a autentizaci, mají vysokou flexibilitu a jsou relativně finančně dostupné. [6][23]

NFC nemá mnoho velkých nevýhod, například že ne všechna zařízení NFC podporují, stálo riziko útoků i s vysokou mírou zabezpečení. Ale jako hlavní nevýhodu je často uváděn nízký dosah v rámci centimetrů. [23]

## 3.2. Biometrické přístupové systémy a jejich využití

Biometrie je vědní obor zabývající se automatickým rozpoznáváním jednotlivců na základě jejich fyziologických či behaviorálních charakteristik, či jejich kombinací. Jejich hlavním cílem je poskytnutí spolehlivé metody autentizace nebo identifikace osoby bez nutností bez nutnosti používat fyzické identifikační karty či hesla. Tímto způsobem biometrie umožňuje určit totožnost osoby na základě toho, „kým je“, a ne na základě toto, „co vlastní“ nebo „co si pamatuje“. [24][25][26]

Lidé využívali tělesné charakteristiky již po tisíce let, zejména obličeje či hlasy osob, aby jeden druhého poznali. V dnešním moderním světě je biometrická technologie využívána stále

častěji, a to nejen v oblastech jako je kriminalistika či bezpečnost, ale také se s ní lze setkat ve formách jako jsou zabezpečení mobilních telefonů, tabletů či další elektroniky, bankovních či jiných aplikacích, či dokonce nahrazení klíče pro vstup do budov. [24][25]

Aby byla fyziologická či behaviorální charakteristika považována za biometrickou vlastnost, musí splňovat několik základních podmínek. První z nich je **univerzálnost**, což znamená, že daná charakteristika musí být přítomná u všech jedinců v populaci, nebo alespoň u většiny. Dále je důležitá **jedinečnost**, která spočívá v dostatečné variabilitě charakteristiky mezi jednotlivci. **Stálost** je dalším nezbytným kritériem, protože charakteristika by měla být v průběhu času stabilní a neměnit se výrazně. A poslední je **měřitelnost**, která říká, že je nutné, aby byla charakteristika měřitelná a přesně vyhodnotitelná. [24][25]

Kromě základních podmínek musí být splněny i další požadavky. Mezi ně patří **výkon**, což znamená, že charakteristika musí poskytovat vysokou úroveň přesnosti při identifikaci či ověřování identity osoby. To zahrnuje nízké míry falešně přijatých (FAR) a falešně zamítnutých (FRR) výsledků. Další podmínkou je **ochrana soukromí**, tedy charakteristika by měla být navržena tak, aby její využívání neporušovalo soukromí jednotlivců více, než je nezbytné. Poslední podmínkou je **přijatelnost** neboli že daná biometrická vlastnost by měla být společensky přijatelná a lidé by ji měli být ochotni používat bez obav nebo odporu. [24][25]

V praxi se biometrické systémy dělí do dvou hlavních kategorií dle způsobu využití [24][25]:

- **Identifikace** (1:N) – systém porovná vzorek se všemi záznamy v databázi, aby našel shodu. Může se jednat například o systém, který kontroluje všechny otisky prstů v databázi, aby zjistil, kdo patří k nalezenému otisku na místě činu,
- **Verifikace** (1:1) – systém porovnává biometrický vzorek jen s jedním konkrétním záznamem, který odpovídá tvrzení uživatele o jeho identitě, které může mít podobu zadání jména a hesla uživatele do systému.

**Princip fungování biometrických systémů**

Všechny, zde popsané, biometrické systémy fungují na principu rozpoznávání a analýzy vzorů fyziologických či behaviorálních vlastností jedinců. Skládá se ze čtyř hlavních částí a rozhodnutí [24][25][26][28]:

**Senzor (vstupní zařízení)**

Senzor zachytává biometrická data jedince, pro různé typy dat se využívají různé typy senzorů, například [24][25][28]:

- **Otisky prstů** – optické, kapacitní či ultrazvukové senzory,
- **Rozpoznávání obličeje** – 2D kamery (nejjednodušší a nejméně výkonný způsob), 3D kamery či infračervené skenery,
- **Duhovka a sítnice** – infračervené skenery,
- **Hlasová biometrie** – mikrofon,
- **Dynamika psaní na klávesnici** – software pro sledování úhozů (například TypingDNA).

Senzor musí získat kvalitní vzorek pro následné zpracování. Pokud vzorek není kvalitní, systém by měl požadovat opakované sejmutí vzorku. [24][28]

**Extrakce rysů**

Získaný vzorek je dále zpracován, aby byly odstraněny šumy, vylepšena kvalita obrazu nebo zvuku. Dále systém extrahuje specifické rysy jedince. U otisku prstů se analyzují papilární linie, u rozpoznávání obličeje se analyzuje poloha a tvar očí, nosu, obočí, rtů, brady a jejich celková vzdálenost mezi sebou, a u hlasové biometrie se analyzuje frekvenční odezva hlasu. Tyto vzorky se převádějí na matematické reprezentace, které se používají pro porovnání. [24][28]

**Porovnání s šablonami**

Tato část slouží k porovnání extrahovaných rysů, které byli převedeny na matematické hodnoty, s uloženými šablonami v databázi. Výsledkem je tzv. „matching score“, neboli skóre podobnosti mezi vzorkem a uloženými daty. V situaci, kdy hodnota „matching score“ překročí nastavené minimum podobnosti, systém vyhodnotí vzorek jako shodující se. [24][25][28]

**Databáze šablon**

Databáze šablon je biometrickým systémem využívána pro uchování šablon jedinců. Při registraci musí nový uživatel poskytnout biometrický vzorek, který systém převede do šablony a uloží jej do databáze. Obvykle se ukládá více šablon na jedince, aby se braly v potaz změny v biometrických rysech jedince, šablony se také v databázi se mohou časem aktualizovat, pro kompenzaci změn. [24][25][28]

**Rozhodnutí**

Další částí fungování biometrických systémů je rozhodovací proces a výstup systému. Biometrické systémy nemohou pracovat s absolutní shodou, jelikož biometrická data v drtivé většině případů vykazují odchylky od šablony v důsledku [24][25][28]:

- **Fyziologických změn** (stárnutí, úrazy),
- **Nepřesnosti senzorů** (špatné světlo u kamery či suchá kůže u snímače otisků prstů).

Rozhodnutí systému se tedy provádí na základě stanovené prahové hodnoty. Každé porovnání biometrických údajů generuje „matching score“. Pokud je skóre vyšší než stanovená prahová hodnoty, systém vrátí pozitivní výsledek. Prahová hodnota musí být nastavena tak, aby minimalizovala chyby, jako jsou [24][25][28]:

- **False Acceptance Rate** (FAR) – míra chybného přijeté neoprávněného uživatele,
- **False Rejection Rate** (FRR) – míra chybného zamítnutí oprávněného uživatele.

Výstupem tohoto procesu může být [24][25]::

- **Autentizace** – Akceptováno či odmítnuto (například přihlášení do telefonu)
- **Identifikace** – identifikován či neidentifikován (například hledání zločince v databáze)
- **Chybové hlášení** – špatně sejmutý vzorek (například chybové hlášení při přihlašování do telefonu)

### 3.2.1. Fyziologické biometrické technologie

**Otisky prstů**

Otisky prstů patří mezi nejrozšířenější fyziologické biometrické technologie, používané jak v kriminalistice, tak v běžné identifikaci a autentizaci uživatelů. Každý člověk má jedinečný otisk prstu, který se po dosažení dospělosti, pokud nezapočítáme vnější vlivy, mění pouze minimálně, a proto je spolehlivým identifikačním znakem. [25][28]

S tímto typem biometrické technologie je možné se setkat v mnoha oblastech, zejména mobilních telefonech, přístupových systémech, bankovnictví či v kriminalistice. Moderní chytré telefony běžně využívají otisk prstu k odemykání zařízení nebo autorizaci plateb. Docházkové systémy ve firmách používají snímače otisků prstů k registraci příchodu a odchodu zaměstnanců. Dále se využívají pro vstup do budov, zabezpečení objektů nebo k ověřování identity při přístupu k citlivým informacím na počítačích a v databázích. [25][26][28]

Při analýze otisku prstu se skenují uspořádání papilárních linií, což jsou hřebeny a údolí na povrchu kůže. Tyto linie tvoří složité vzory, které jsou u každého jedince unikátní. Mezi hlavní aspekty skenování patří [25][28]:

- Směr a průběh papilárních linií – systém analyzuje, jak se linie stáčí, spojují a větví,

    - Hustota linií – měří se vzdálenost mezi jednotlivými liniemi, což napomáhá přesnějšímu rozpoznání.,

- Globální vzory otisku – otisky prstů lze rozdělit do tří základních skupin [25][28]:
    - Oblouky – linie přecházejí z jedné strany na druhou bez výrazných smyček,
    - Smyčky – linie se stáčejí zpět do oblouku,
    - Víry – linie tvoří spirálové nebo kruhové vzory.

Mezi výhody otisků prstů jednoznačně patří jejich jedinečnost, která je udržena i mezi dvojčaty, a stabilita v čase. Další výhodou je rychlost autentizace, jelikož moderní snímače umí ověřit otisk prstu během zlomku sekundy. Kromě toho je tato technologie i cenově dostupná. [25][28]

Otisky prstů sebou také nesou nevýhody, u některých jedinců, například u manuálních pracovníků, může docházet k opotřebení či poškození papilárních linií, které mohou vést k problémům při jejich rozpoznání. Další nevýhodou je možnost podvrhu, tento problém se ale pomalu stává minulostí, jelikož moderní senzory rozlišit mezi živou tkání a falešnými otisky. [25][28]

**Rozpoznávání obličeje**

Rozpoznávání obličeje je jedním z nejdynamičtějších technologií v rámci biometrických přístupových systémů, které identifikuje nebo ověřuje totožnost osoby na základě jejich rysů obličeje. Systém funguje bez fyzického kontaktu a umožňuje rychlou a pohodlnou autentizaci uživatelů. [25][29]

S rozpoznáváním obličeje se v současnosti využívá v mnoha odvětvích, od běžných komerčních zařízení až po bezpečnostní systémy. V přístupových bezpečnostních systémech se využívá při vstupu do budov, kancelářích či na letištích, lze se s nimi také setkat v mobilních zařízeních jako jsou mobilní telefony, tablety, počítače nebo v platebních systémech a dalších. [25][29]

Biometrické systémy analyzují unikátní rysy obličejů, které jsou u každého člověka specifické a jedinečné. Mezi hlavní patří [25][30][31]:

- Vzdálenost mezi pozorovanými body obličeje – např. mezi očima, nosem a ústy,
- Struktura a tvar obličeje – celková geometrie obličeje,

- Tepelné a infračervené charakteristiky – pouze u systémů využívajících 3D mapování obličeje nebo infračervené senzory,
- Mezi další rysy mohou dále patřit například textura pleti či barva kůže.

Rozpoznávání obličeje přináší výhody jako bezkontaktní autentizace, rychlost, vysoká přesnost a škálovatelnost pro široké spektrům použití. [25][29]

Přes jeho výhody si tento systém nese i mnoho nevýhody, přesnost může být ovlivněna změnami v osvětlení, stárnutím uživatele, změnou výrazu nebo úhlem pohledu. Významnou nevýhodou jsou i etické a právní otázky ohledně soukromí a možného zneužití dat. [25][29]

**Skenování duhovky a sítnice**

Tyto dvě technologie patří mezi ty nejpřesnější biometrické metody využívané pro identifikaci či autentizaci osob. Obě pracují na principu snímání unikátních struktur oka, duhovka obsahuje složité vzory pigmentace, zatímco sítnice se specifikuje jedinečným uspořádáním cévního řečiště. Jejich vysoká přesnost v kombinaci s obtížností prolomení z nich činí perfektní volbu pro oblasti s vysokými bezpečnostními požadavky. [25][32]

Tyto technologie jsou využívány v řadě oblastech, především v bezpečnostních a přístupových systémech. Mohou být využívány v zabezpečených objektech, vládních institucích, vojenských zařízeních nebo bankovních trezorech. Na letištích se využívá pro urychlení celních a pasových kontrol. [25][32]

Při provádění identifikaci či autentizace analyzují specifické rysy oka, které jsou u každého člověka jedinečné. Mezi hlavní rysy patří [25][32]:

- Duhovka, u které se zkoumá vzor pigmentace (jedinečné uspořádání barevných vzorů), struktura vláken duhovky (detaily textury a jemné linie) a kontrastní prvky (tmavší a světlejší oblasti v duhovce).
- Sítnice, zde se zkoumají cévní vzory sítnice (unikátní rozložení krevních cév na zadní straně oka), hloubková struktura cév (jejich hustota a propojení) a odraz infračerveného světla (snímání odraženého světla z cév, což umožňuje vytvoření detailního mapování cév).

Tyto dvě metody přináší výhody ve formě extrémně vysoké přesnosti, stability vzoru po celý život, odolnost proti prolomení a bezkontaktní autentizace, což zvyšuje hygienu a komfort uživatele. [25][32]

Na druhé straně jsou nevýhody této technologie, kde mezi hlavní patří vysoké náklady na implementaci nebo nutnost uživatelské spolupráce. Ale největší nevýhodou jsou opět etické a právní otázky související s uchováváním biometrických dat a jejich možným zneužitím. [25][32]

**Geometrie ruky**

Tento typ biometrické technologie využívá měření fyzických charakteristik ruky, jako je její tvar, velikost, délka a šířka prstů, rozložení kloubů nebo zakřivení dlaně. Jedná se o jednu z méně invazivních metod biometrie. Vyniká svou jednoduchostí použití a přijatelnou úrovní přesnosti. [25][33][34]

S tímto typem systému se lze setkat zejména v přístupových či docházkových systémech, a to převážně tam kde není nutná extrémně vysoká přesnost. Je možné jej tedy spatřit například při vstupech do kancelářských budov, skladů nebo do některých škol. V některých případech se kombinuje s dalšími biometrickými metodami pro zvýšení bezpečnosti. Také se lze setkat s kombinací systémů g**eometrie ruky** a **rozpoznávání otisku dlaně**. [25][34]

Při procesu identifikace či autentizace systém analyzuje specifické vlastnosti ruky. Mezi hlavní vlastnosti patří [25][33]:

- Celkový tvar ruky – jedná se o obrys dlaně a její proporce,
- Rozměry prstů a dlaně – měří se délka a šířka jednotlivých částí ruky,
- Vzdálenosti mezi klouby – měření rozestupů mezi jednotlivými klouby.

Mezi výhody geometrie ruky patří rychlost ověřování, nízké náklady na pořízení i provoz těchto systémů, nevyžaduje složité výpočty a díky tomu ani zařízení s příliš vysokým výkonem. Oproti jiným biometrických technologiím je méně invazivní, jelikož nevyžaduje detailní snímání kůže, ani nepříjemné zásahy do soukromí. [25][33][34]

Na druhou stranu nedisponuje příliš vysokou přesností, také se mohou objevit problémy s rozměry ruky, ať už kvůli úrazům, stárnutí či otokům, což ovlivní identifikaci či autentizaci. Také je oproti jiným systémům snazší ji obejít pomocí podvržených modelů ruky. [25][33][34]

**Rozpoznávání otisku dlaně**

Jedná se jednu z přesnějších metod identifikace či autentizace osob. Analyzuje fyzické charakteristiky jako jsou papilární linie, rýhy, záhyby a různé vzory kůže na dlani. Tyto vzoru jsou u každého člověka specifické a jedinečné, podobně jako u otisků prstů, ale na rozdíl od

nich používá celou plochu ruky, což zvyšuje její přesnost a spolehlivost rozpoznávání oproti otisku prstů. [25][35]

S touto metodou je možné se setkat v různých oblastech, ale nejčastěji v bezpečnostních a přístupových systémech, přitom zejména v oblastech, kde je vyžadováno vysoké zabezpečení prostoru či informací. Konkrétně mohou být viděny například ve vládních institucích, podnikových přístupových systémech nebo v bankovnictví. Někdy se tato technologie kombinuje ještě s dalšími. [25][35]

Při rozpoznávání otisku dlaně se analyzují specifické rysy dlaně, například [25][35]:

- Papilární linie – stejně jako u otisku prstů se analyzují jedinečné vzory linií na povrchu dlaně,
- Klíčové rýhy a záhyby kůže – velké rysy, které zůstávají stabilní po celý život,
- Rozložení pórů – některé pokročilé systémy analyzují i texturu kůže.

Hlavní výhodou této technologie je její vysoká přesnost díky unikátnosti vzorů kůže a větší ploše použité pro skenování. Také je tato metoda hůře napodobitelná oproti geometrii ruky, což její zvyšuje její bezpečnost. [25][35]

Nevýhody zahrnují nutnost čisté a nepoškozené dlaně, systém sice zohledňuje určitou míru odchylek, ale musí být pečlivě vyvážena, aby nedocházelo k příliš vysoké míře falešného přijetí (FAR). [25][35]

**Skenování žil v dlani**

Skenování žil v dlani je jedna z nejpřesnějších biometrických technologií, identifikuje či autentizuje osoby na základě jejich jedinečného vzoru žil pod povrchem kůže. Tyto metoda využívá infračerveného světla, které proniká do tkáně a odhaluje rozložení cév a žil. Jedná se o velice stabilní biometrickou charakteristiku jedince, na kterou téměř nepůsobí běžné faktory, jako jsou stárnutí, únava, stres, poškození vnějšími vlivy atd. [25][36][37]

Tato metoda identifikace či autentizace je využívána v přístupových systémech, bankovnictví či zdravotnictví. Setkat se s ní lze v zabezpečených objektech, jako jsou banky, datová centra a vládní instituce, kde je požadována vysoká úroveň zabezpečení. V budoucnu by mohli snímače otisků prstů v mobilních zařízeních kombinovat jak analýzu papilárních linií, tak i žilních vzorů. [25][36][37]

Tato technologie se zaměřuje na specifické jedinečných vlastností žilního systému dlaně, mezi které patří [25][36][37]:

- Struktura žilního vzoru – systém zkoumá rozvětvení, tloušťku, směr a vzájemné propojení, které nelze duplikovat,
- Hloubková struktura žil – skenování zachycuje nejen povrchové žíly, ale i hlubší cévní systém,
- Absorpce infračerveného světla – metoda využívá infračervené senzory ke zvýraznění cév, které absorbují světlo odlišně od okolní tkáně.

Hlavními výhody této metody patří vysoká přesnost, odolnost proti podvrhům a stabilita vzorů po celý život. Bezkontaktní skenování navíc přináší výhodu v podobě hygieny, jelikož nevyžaduje přímý fyzický kontakt se snímačem. [25][36][37]

Existují zde ale určité nevýhody, jako jsou vysoké náklady na implementaci, citlivost na kvalitu snímku. Systém může být také citlivý na extrémní zdravotní stavy, například špatný krevní oběh, které ovlivňuje viditelnost cév. [25][36][37]

### 3.2.2. Behaviorální biometrické technologie

**Rozpoznávání hlasu**

Rozpoznávání hlasu je biometrická behaviorální metoda identifikaci či autentizace založená na analýze unikátních charakteristik řeči. Každý člověk má jedinečné rysy hlasu, které lze počítačově zpracovat a porovnat s dříve uloženými vzorky. Může se jednat o textově závislou metodu, kdy uživatel musí vyslovit konkrétní frázi, nebo textově nezávislou, kdy systém rozpoznává hlas bez ohledu na to, co je řečeno. [25]

Tato technologie se uplatňuje v řadě oblastí. Nejčastěji slouží pro autentizaci a přístupové systémy, umožňuje například odemčení zabezpečených dveří hlasem namísto zadávání hesla či používání karty. Dále se mohou vyskytovat v systémech kontroly přístupu k citlivým informacím, nebo jako jedna z vícefaktorových metod ověřování uživatele v zabezpečených systémech. [25]

Co se při rozpoznávání hlasu zkoumá [25]:

- Mohou se analyzovat vlastnosti jako je výška hlasu, tón, přízvuk, výslovnost a frekvenční charakteristika.

Výhodou hlasové identifikace/autentizace je to že není považována za tak invazivní jako některé fyziologické metody identifikace/autentizace. Lacinější instalace systému, pro provoz stačí běžný mikrofon. Hlas osoby v sobě také nese užitečné informace o jeho stavu, například úroveň stresu či emocí. [25]

Tato metoda sebou také nese určité nevýhody, například závislost na schopnosti osoby mluvit, pokud je osoba nemocná či má poškozené hlasivky, systém nemusí osobu rozpoznat, další je citlivost na okolní hluk, v tomto případě také záleží na tom, jak je systém implementován, jakou citlivost snímání mikrofon má atd. Mezi další může patřit proměnlivost hlasu uživatele nebo možnost napodobení hlasu. [25]

**Dynamika psaní**

Dynamika psaní, známá také jako „keystroke dynamics“, je metoda behaviorální biometrie, která slouží k rozpoznávání nebo ověřování uživatele na základě jeho specifického způsobu psaní na klávesnici. Funguje na předpokladu, že každý člověk má unikátní rytmus a vzorec úhozů, zejména v časových intervalech mezi jednotlivými stisky kláves, dle kterých lze osobu identifikovat. Díky tomu může systém rozpoznat osobu bez ohledu na to co zrovna píše. [25]

S touto technologií se lze setkat zejména v situacích, kde vyžadováno vysoké zabezpečení. Praktické uplatnění tato technologie nachází při vzdáleném přihlašování a obecně všude, kde osoby pracují s klávesnici a je třeba průběžně kontrolovat jejich přístup. Výhodou je, že nevyžaduje žádný speciální hardware ani senzory, k analýze stačí jen běžná klávesnice a software pro zaznamenávání a porovnávání psaní. [25]

Systém zaznamenává několik charakteristik dynamiky psaní [25]:

- Doba stisku klávesy – čas, po který je klávesa stisknutá,
- Čas mezi stiskem dvou kláves – časový interval mezi stisknutím dvou po sobě jdoucích kláves,
- Chybovost a opravy – jak často osoba dělá překlepy jakým způsobem je opravuje,
- Tlak na klávesnici – systém analyzuje sílu stisku kláves, což přidává další úroveň zabezpečení. Tento parametr není dostupný na běžných klávesnic, ale pouze u klávesnici disponujících tlakovým senzorem.

Výhodou této metody je její relativně jednoduchá instalace, kdy potřebujeme pouze specifický software a jakoukoli klávesnici, případně klávesnici s tlakovými senzory (není nutností). Sběr dat a ověřování osob může být nepřerušované a nenápadné, mohou být například získávána na pozadí běžné práce na počítačích apod. [25]

Nevýhodou této metody je to že není tak jednoduše implementovatelná pro identifikaci či autentizaci, jako pro ověřování že se jedná stále o tu stejnou osobu. Dalšími nevýhody mohou být variabilita a nestálost vzorců psaní, jelikož osoba nemusí vždy psát stejnou rychlostí. To

znamená, že systém musí být dostatečně flexibilní a správně nastavit prahové hodnoty pro rozpoznání. Pokud by ale byli tyto limity příliš přísné, může docházet k častým falešným odmítnutím oprávněných uživatelů, nebo naopak. [25]

**Dynamika chůze**

Dynamika chůze, známá také jako „Gait recognition“, představuje specifický vzorec pohybů, které člověk vykonává při chůzi. Jde o naučený pohybový projev, který je však výrazně ovlivněn fyzickými charakteristikami jedince, například jeho hmotností, výškou, podílem svalové hmoty, držením těla, ale také typem obuvi či oblečení. Myšlenkou je že každá osoba, má svůj jedinečný charakteristický styl chůze, díky kterému může být ověřován. [25]

Biometrická analýzy chůze nachází uplatnění například na veřejných místech, jako jsou letiště nebo nádraží. Také může sloužit ke kontrole strážných hlídajících firemních areály nebo jiné objekty, kde umožňuje ověření a sledování pohybu oprávněných či neoprávněných osob. [25]

Dynamika chůze sleduje specifické pohybové charakteristiky, mezi které patří například [25]:

- Rychlost chůze – průměrná doba mezi jednotlivými kroky a celkové tempo chůze,
- Délka kroku – vzdálenost mezi jednotlivými došlapy,
- Doba kontaktu nohy se zemí – časový interval, po který zůstává nova na zemi při každém kroku,
- Symetrie pohybu – porovnání levé a pravé strany těla při chůzi,
- Změny v rytmu chůze – změny tempa a pravidelnost kroků,
- Koordinace těla – koordinace pohybu rukou a nohou během chůze,
- Postoj a držení těla – sklon trupu a vyvážení při chůzi.

Výhodou této technologie je pohodlí a nenápadnost pro osobu, ověřování může probíhat průběžně, aniž by osoba musela vykonávat jakýkoli specifický úkon. Další výhodou je, že nevyžaduje drahé specializované senzory, postačí standardní kamerový systém se specifickým softwarem nebo běžné pohybové senzor. [25]

Nevýhodou dynamiky chůze je její proměnlivost, která může být ovlivněna zdravotním stavem, únavou, typem obuvi či povrchem, po kterém se člověk pohybuje. To může vést ke snížení přesnosti identifikace. Další omezení spočívá v tom, že tato biometrická metoda

předpokládá, že osoba je schopen chůze, což ji činí nepoužitelnou pro osoby s pohybovým postižením (například osoby na invalidním vozíku). Existuje také riziko napodobení chůze, kdy by se útočník mohl pokusit imitovat styl chůze oprávněné osoby, čímž by mohl systém oklamat. [25]

# 4. POPIS FIRMY A SOUČASNÉHO ZABEZPEČENÍ

Pro svou bakalářskou práci jsem si vybral skutečnou firmu, která si nepřeje být jmenována. Dále bude v textu nazývána jako firma XY.

Cílem této práce je návrh nového přístupového systému s integrací biometrických prvků pro zlepšení zabezpečení ve firmě. V rámci tohoto návrhu bude popsán současný stav přístupových systémů firmy, identifikovány nedostatky v zabezpečení, představen návrh nového přístupového systému a odůvodněny navržené změny.

## 4.1. Základní informace o firmě XY

Firma XY se zabývá výrobou elektronických součástek, elektrických zařízení a strojů, přičemž její činnost zahrnuje jak výrobu, tak opravy zařízení pracujících na malém napětí. Mezi další činnosti patří velkoobchod a maloobchod, poskytování ubytovacích služeb, příprava a vypracování technických návrhů, grafické a kresličské práce a projektování elektrických zařízení.

Firma XY se řadí mezi malé podniky, jelikož má méně než 50 zaměstnanců, roční obrat pod 10 milionů eur a bilanční sumu do 10 milionů eur.

Sídlo firmy XY se nachází na okraji vesnice, obklopené travnatou plochou a několika domy ve vzdálenosti přibližně 50 metrů. Budova č.1 je ze tří stran obklopena řadou stromů. Budova č. 2 se nachází několik metrů od první budovy, na opačné straně silnice vedoucí mezi objekty. V její blízkosti stojí chata, zatímco část budovy sousedí s polem a z levé strany ji obklopuje travnatá plocha. Ani jedna z budov není chráněna oplocením, výjimku tvoří pouze budova č. 1, která je, jak bylo zmíněno, částečně oddělena ze 3 stran stromy.

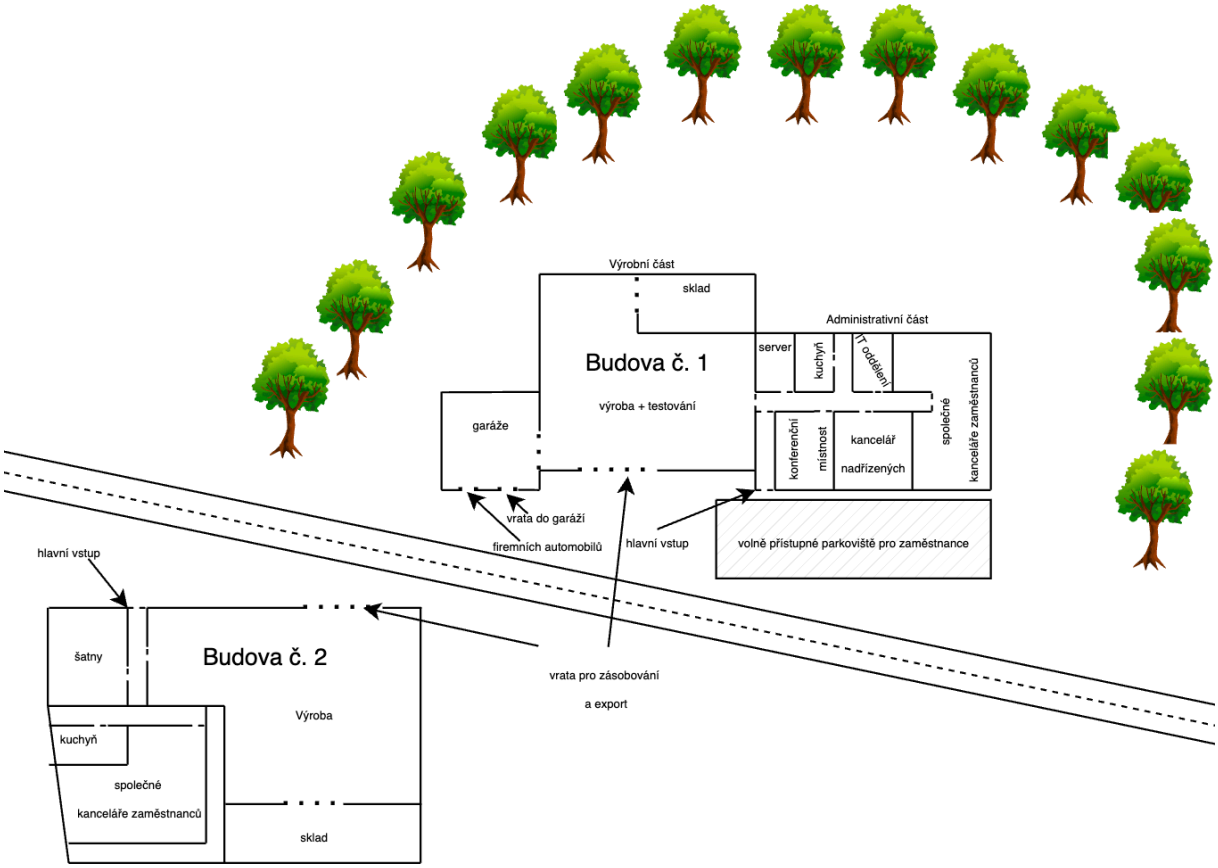
Umístění firmy v této méně frekventované části vesnice zvyšuje riziko neoprávněného přístupu a obcházení přístupových systémů, jelikož omezený dohled poskytuje více času na pokusy o narušení zabezpečení.

## 4.2. Popis objektu firmy XY a jeho zabezpečení

Objekt firmy XY, vyobrazený na Obrázek 1, zahrnuje dvě hlavní budovy. Budova č. 1 kombinuje výrobní, administrativní a technické prostory. Ve výrobní části se nachází garáže a výroba samotná propojená se skladem a prostorem pro testování. Administrativní část budovy zahrnuje IT oddělení, společnou kancelář zaměřenou na návrhy a technickou dokumentaci,

kancelář nadřízených, serverovnu a další. Před administrativní částí budovy se také nachází volně přístupné parkoviště, které není nijak chráněno.

Budova č. 2 je primárně výrobní a skladovací halou. Kromě toho obsahuje také šatny pro zaměstnance a kanceláře určené komunikaci s dodavateli i odběrateli. Tato budova je bezdrátově připojena na stejný server jako Budova č. 1, díky čemu je umožněna centralizovaná správa dat.




**Obrázek 1:** Plán areálu firmy s vyznačením přístupových bodů

*Zdroj: vlastní zpracování*

### Budova č. 1

Budova č. 1 je v současné době zabezpečena kombinací mechanických a elektronických přístupových systémů. **Hlavní vstup** do budovy je zajištěn **zámkem na klíč** a alarmovým systémem, do kterého se musí zadat ihned po vstupu **PIN kód** pro deaktivaci. Po vstupu do budovy je možné volně přejít do konferenční místnosti nebo kuchyňky, které jsou zabezpečeny pouze zámkem na klíč, ale zřídka se uzamykají. Přístup do **kanceláří zaměstnanců**, včetně kanceláře nadřízených a **IT oddělení** je přístupný pouze po přiložení **RFID karty** ke čtečce. **Serverovna** je jediná místnost, která vyžaduje vyšší úroveň zabezpečení, tudíž je před vstupem požadována **RFID karta a PIN kód** jako dodatečnou autentizaci.

**Výrobní část budovy** je od administrativní části oddělena dveřmi s madlem, jejichž otevření z obou stran je povoleno přiložením **RFID karty** ke čtečce, která se nachází vedle dveří. Součástí výrobních prostor je také **sklad**, do kterého mají přístup pouze oprávněné osoby po autentizaci **RFID kartou**. Sklad je vybaven sekčními výsuvnými vraty, které zůstávají otevřeny do doby, než je přiložena **RFID karta** ke čtečce k jejich uzavření. Stejným způsobem jsou ovládána i **vrata pro zásobování a expedici**. Vstup do skladu a vrata do výroby jsou dále monitorovány kamerovým systém. Vrata skladu jsou také vybavena bezpečnostním mechanismem, který se automaticky aktivuje, pokud nejsou manuálně uzavřena. Po 8 hodinách od jejich otevření vydají zvukové upozornění a následně se sama zavřou.

**Garáže**, které jsou propojené s výrobní částí budovy, jsou přístupné pouze skrze výrobní prostory a vstup do nich je umožněn pomocí **RFID karty**. Vrata lze otevřít buď manuálně z vnitřní strany garáže, nebo pomocí dálkového ovladače, který je umístěn ve dvou firemních vozidlech.

**Budova č. 2**

Budova č. 2 je zabezpečena stejným způsobem jako Budova č. 1. **Hlavní vstup** je chráněn **zámkem na klíč** a alarmovým systémem uvnitř, do kterého se musí ihned po vstupu **PIN kód** pro deaktivaci. Po vstupu do budovy je možné volně přejít do kuchyňky, která je zabezpečena stejným způsobem jako v Budově č. 1.

Přístup do **výrobní části** je oddělen dveřmi s madlem, do této části je povolen přístup po autentizaci **RFID kartou**. **Vrata pro zásobování a export**, stejně jako vstup do skladu, fungují na stejném principu jako v Budově č. 1, pro otevření i zavření je vyžadováno přiložení **RFID karty** oprávněnou osobou. Vstup do skladu a vrata do výroby jsou také monitorovány kamerovým systém.

V druhém patře budovy se nachází **kanceláře zaměstnanců**, vstup do nich je umožněn po přiložení **RFID karty** ke čtečce, která umožňuje přístup pouze oprávněným osobám.

## 4.3. Vymezení prostor na základě významnosti pro chod společnosti

Analýza rizik bude zaměřena na prostory, ve kterých se uchovávají nebo zpracovávají citlivé informace, jako jsou technické dokumentace, konstrukční plány zařízení, projektová dokumentace, smlouvy s odběrateli a dodavateli, finanční údaje, data o zaměstnancích a další důvěrné informace. V případě jejich ztráty nebo odcizení by společnosti mohly hrozit právní, finanční a reputační následky.

Konkrétně se jedná o serverovnu, která slouží jako centrální úložiště dat a dalších dokumentů společnosti, kancelář vedení, kde jsou uchovávány smlouvy, různé plány a důvěrné a finanční dokumenty, IT oddělení, kde probíhá správa sítě, zabezpečení a jiných systémů firmy a společné kanceláře zaměstnanců, jak v budově č. 1 tak v budově č. 2, kde se pracuje s provozními a interními dokumenty.

## 4.4. Analýza rizik

Na základě vymezených prostor, byla vyhotovena analýza rizik pomocí metody PNH. Analýza se zaměřuje na hodnocení rizik spojených s přístupovými systémy jednotlivých analyzovaných prostor s citlivými informacemi.[38]

**Výsledky metody PNH a bodový rozsah**

Tabulka 1 představuje výběr nejzávažnějších identifikovaných rizik, které byly hodnoceny pomocí bodového výpočtu metody PNH. Do tabulky byly zařazeny pouze hrozby s bodovým hodnocením odpovídajícím **prvním třem stupňům závažnosti**, dle

Tabulka 2, tedy s hodnotou 30 a více bodů. Hodnoty v rozmezí 60-75 značí nepřijatelné riziko, 45-59 nežádoucí riziko a 30 až 44 mírné riziko, které je vhodné dále řešit.[38]

Analýza ukázala, že identifikovaná rizika se vyskytují ve všech sledovaných místnostech, a to v rozsahu od mírných až po nepřijatelná. Nejzávažnější situace byla zaznamenána v serverovně kde se vyskytují dvě rizika spadající do nejvyššího stupně závažnosti. Významné nedostatky byly dále odhaleny v kanceláři vedení a IT oddělení, kde se objevují hrozby související se ztrátou, krádeží RFID karty či lidskou chybou.

Společné kanceláře zaměstnanců v budově č. 1 a 2 vykazují výskyty lidských chyb a ztrát přístupových karet, což odpovídá prostor s větším pohybem osob a sdíleným pracovním prostředím.

Celkově analýza potvrdila, že rizika současného přístupového systému se nevztahují pouze na jednotlivé místnosti, ale na všechny.

Zbylá rizika s nižší závažností a výpočet celé analýzy rizik, která zde nejsou uvedena, jsou součástí Přílohy A**.**

**Tabulka 1:** Přehled nejzávažnějších rizik hodnocených metodou PNH

| Místnost | Riziko | Výpočet PNH | | | | Stupeň rizika |
|---|---|---|---|---|---|---|
| | | P | N | H | Získané body (R) | |
| Server | Lidská chyba | 5 | 5 | 3 | 75 | I. |
| Server | Ztráta RFID karty | 5 | 4 | 3 | 60 | I. |
| Kancelář vedení | Lidská chyba | 4 | 5 | 3 | 60 | I. |
| IT oddělení | Lidská chyba | 4 | 5 | 3 | 60 | I. |
| Kancelář vedení | Ztráta RFID karty | 4 | 4 | 3 | 48 | II. |
| IT oddělení | Ztráta RFID karty | 4 | 4 | 3 | 48 | II. |
| Společné kanceláře zaměstnanců v budově č.1 a 2 | Lidská chyba | 3 | 5 | 3 | 45 | II. |
| Server | Krádež RFID karty | 5 | 2 | 4 | 40 | III. |
| Server | Fyzická manipulace s přístupovým systémem | 5 | 2 | 4 | 40 | III. |
| Společné kanceláře zaměstnanců v budově č.1 a 2 | Ztráta RFID karty | 3 | 4 | 3 | 36 | III. |
| Kancelář vedení | Krádež RFID karty | 4 | 2 | 4 | 32 | III. |
| Kancelář vedení | Fyzická manipulace s přístupovým systémem | 4 | 2 | 4 | 32 | III. |
| IT oddělení | Krádež RFID karty | 4 | 2 | 4 | 32 | III. |
| IT oddělení | Fyzická manipulace s přístupovým systémem | 4 | 2 | 4 | 32 | III. |
| Server | Odposlech/Odpozorování PIN kódu | 5 | 2 | 3 | 30 | III. |

*Zdroj: vlastní zpracování*

Tabulka 2, znázorňuje pětistupňovou škálu hodnocení rizik dle bodové hodnoty R. Každému rozmezí bodů odpovídá určitý stupeň rizika a doporučený způsob reakce – od bezvýznamných rizik, která není nutné řešit, až po nepřijatelná rizika, u nichž je nezbytné okamžité nápravné opatření.[38]

**Tabulka 2:** Škála hodnocení rizik

| **Hodnota R** | **Stupeň rizika** | **Popis** |
|---|---|---|
| **60-75** | **I.** Stupeň | **Nepřijatelné riziko – nutná** okamžitá nápravná opatření |
| **45-59** | **II.** Stupeň | **Nežádoucí riziko – doporučená** nápravná opatření |
| **30-44** | **III.** Stupeň | **Mírné riziko – vhodné** zlepšení zabezpečení |
| **15-29** | **IV.** Stupeň | **Akceptovatelné riziko – není** potřeba zásadních opatření |
| **<15** | **V.** Stupeň | **Bezvýznamné riziko – riziko** zanedbatelné, není potřeba řešit |

*Zdroj: vlastní zpracování*

# 5. VÝBĚR A NÁVRH NOVÉHO PŘÍSTUPOVÉHO SYSTÉMU S VYUŽITÍM BIOMETRICKÝCH PRVKŮ

Cílem této kapitoly je nejprve stanovit vhodnou metodu biometrického přístupového systému, následně provést výběr konkrétního zařízení, které bude v rámci návrhu nového přístupového systému využito, a závěrem navrhnout samotné řešení přístupového systému s využitím biometrických prvků. Pro výběr bude využita Saatyho metoda, která umožní porovnat dostupné alternativy na základě stanovených kritérií a jejich vzájemné důležitosti.

## 5.1. Výběr metody biometrického přístupového systému

Výběr této technologie reaguje na hrozby identifikované v provedené analýze rizik, která v citlivých prostorách firmy označila jako podstatné zejména krádež nebo ztrátu RFID karty, odpozorování přístupového PIN kódu, lidské chyby a fyzickou manipulaci s přístupovým systémem. Zavedením biometrického přístupového systému dochází k eliminaci některých těchto hrozeb plně, například riziko ztráty, zcizení či klonování RFID karet, jelikož žádný externí nosič není zapotřebí. Stejně tak odpadá možnost odpozorování PIN kódu, jelikož uživatel nezadává žádné vstupní údaje.

Snížení rizik nastává také u fyzické manipulace se zařízením, jelikož moderní teminály s biometrickým ověřováním jsou většinou vybaveny Tamper ochranou, která detekuje právě fyzické pokusy o manipulaci s terminálem. Tato technologie také minimalizuje rizika spojená s lidským faktorem, především v oblasti neopatrného zacházení s přístupovými prostředky. Nadále však mohou přetrvávat hrozby vyplívající z provozní nepozornosti, jako je například neúplné dovření vstupních dveří.

Po konzultaci s vedením firmy a s ohledem na dostupné informace o různých typech biometrických technologií byl pro zabezpečení přístupů do firemních prostor zvolen typ systému založený na otiscích prstů. Toto rozhodnutí bylo učiněno především na základě vhodného poměru mezi bezpečností, pořizovací cenou, provozní spolehlivostí a komfortem uživatelů. Technologie otisků prstů navíc nabízí optimální dostupnost a splňuje potřeby firmy. [26]

Systémy využívající otisky prstů jsou dlouhodobě zavedenou technologií, která se vyznačuje velmi nízkými hodnotami chybovosti. Kvalitní komerční čtečky otisků prstů dosahují hodnot FAR přibližně 0,1 až 0,01 % a FRR zhruba 0,1 až 1% v závislosti na konkrétním modelu zařízení a jeho nastavení. Tato míra přesnosti umožňuje vysokou úroveň zabezpečení bez toho,

aby docházelo k častým FR oprávněných zaměstnanců. Další výhodou těchto systémů je možnost nastavení citlivosti čteček, tudíž pokud by docházelo k častým FR, můžeme nastavení upravit, čímž se hodnota FRR sníží ale zároveň zvýšíme hodnotu FAR.[39][40]

Také se lze v dnešní době setkat se čtečkami otisků prstů prakticky na denní bázi, protože většina moderních telefonů je touto technologií vybavena. Díky tomu můžou být uživatelé s tímto způsobem autentizace dobře obeznámeni.

## 5.2. Vymezení rozhodovacího problému

Po stanovení metody biometrického přístupového systému, kterou se stávají otisky prstů, je nutné zvolit konkrétní řešení, tedy čtečku otisků prstů. Vzhledem k relativně široké nabídce, s různými specifikacemi, funkcemi a cenou vzniká rozhodovací problém.

Každá z potenciálních variant nabízí jinou výši zabezpečení, komfort a efektivnost správy nebo technologickou vyspělost. Proto je nutné přistoupit k výběru s využitím vícekriteriálního hodnocení, které umožní zohlednit více kritérií současně a zároveň určit jejich důležitost. Výběr nesmí být postaven pouze na jednom parametru, jednotlivé varianty se totiž liší v mnoha ohledech.

Cílem rozhodovacího procesu je tedy vybrat variantu, která nejlépe odpovídá stanoveným kritériím. Samotné rozhodování bude prováděno použitím Saatyho metody.

## 5.3. Omezující kritéria pro rozhodovací proces

**Autonomní jednotka**

První omezující kritérium představuje požadavek, aby se jednalo o autonomní jednotku, tedy aby terminál obsahoval všechny nezbytné komponenty pro svůj samostatný provoz. Autonomní biometrický terminál obsahuje nejen samotný snímač otisku prstu, ale také řídící elektroniku pro zpracování biometrických dat, paměť pro ukládání šablon otisků a uživatelských přístupových oprávnění, rozhraní pro přímé ovládání elektrického zámku a také signalizační prvky týkající se úspěšné autentizace či zamítnutí.

**Minimální kapacita registrovaných otisků prstů systému**

Druhé omezujícím kritériem je minimální kapacita systému z hlediska počtu uživatelů, a to alespoň 100 osob (na osobu alespoň 2 otisky, tudíž minimálně 200 otisků prstů). I když aktuální počet zaměstnanců ve firmě činí pod 50 osob, je pro firmu důležité zvolit terminál s dostatečnou rezervou pro možnost budoucího rozšíření firmy, bez nutnosti dalších úprav přístupových systémů.

Minimální kapacita 100 osob je dnes navíc považována v podstatě za naprosto minimální hodnotu, především u profesionálních zařízení pro firemní použití.

**Cena pod 21 000 Kč za kus**

Jako třetí omezující kritérium byla stanovena maximální pořizovací cena jednoho terminálu ve výši 21 000 Kč bez DPH. Tato hranice byla zvolena s cílem udržet celkové náklady na pořízení čteček a jejich instalaci do 150 000 Kč bez DPH. Náklady na instalaci jsou firmou stanoveny na 40 000 Kč bez DPH, přičemž tyto práce zajišťuje externí dodavatel (třetí strana).

**Přítomnost Tamper ochrany (ochrana proti neoprávněné manipulaci nebo demontáži zařízení)**

Jako čtvrté omezující kritérium byla zvolena přítomnost Tamper ochrana, kde každý terminál vhodný pro rozhodovací proces musí být vybaven alespoň základní Tamper ochranou. Přítomnost tohoto bezpečnostního opatření je povinná, aby bylo zajištěno alespoň minimální zabezpečení proti neoprávněnému zásahu.

**Dohledatelnost technické dokumentace**

Jako poslední kritériem je dohledatelnost technické dokumentace, které udává že do rozhodovacího procesu budou zařazeny pouze ty varianty, u nichž jsou, nebo byly, dohledatelné informace o technických a provozních parametrech. Tím je zajištěno, že lze všechny varianty porovnat dle stanovených kritérií.

## 5.4. Hodnotící kritéria pro rozhodovací proces

**Pořizovací cena všech terminálů (biometrických čteček)**

Toto kritérium vyjadřuje celkové náklady na pořízení všech potřebných čteček otisků prstů, (terminálů), včetně DPH. Přednost mají terminály jejichž celková pořizovací cena je nižší.

Jedná se o kritérium kvantitativní minimalistické.

**Technologie snímače otisku prstů**

V rámci kritéria technologie snímače otisků prstů neboli senzoru, budou porovnávány dva hlavní typy senzorů, optické a kapacitní.

Kapacitní senzory obecně mohou poskytovat vyšší přesnost a lepší zabezpečení, protože dokážou efektivněji rozpoznat živou tkáň od umělých či padělaných otisků. Jsou také odolnější vůči povrchovému poškození, špíně nebo opotřebení bez nutnosti dalšího krytí senzoru.

Optické senzory mohou naopak nabízet nižší pořizovací cenu, jednodušší údržbu a dostatečnou spolehlivost pro méně náročné prostředí. Jejich nevýhodou může být menší odolnost vůči padělkům, to se kompenzuje různými algoritmy na rozeznávání falešných otisků prstů, nebo větší citlivost na znečištění.

Nelze však tvrdit, že kapacitní senzor je automaticky lepší volbou než senzor optický. Výběr vhodné varianty závisí na dalších faktorech, jako jsou například certifikace daného terminálu o jeho bezpečnosti, odolnost snímací plochy senzoru vůči mechanickému poškození, přítomnost algoritmů či funkcí pro detekci živé tkáně. Zatímco kapacitní senzory obecně nabízejí vyšší přesnost snímání, levné kapacitní senzory v nižších cenových kategoriích nemusí nutně překonat optický senzor integrovaný v kvalitním a certifikovaném terminálu. Terminály ve vyšších cenových kategoriích totiž mohou využívat senzory vyšší kvality, účinnější algoritmy a komplexnější zabezpečení, což může mít na výslednou spolehlivost a bezpečnost znatelný vliv než pouze samotný typ použitého senzoru. Výběr nebude tedy zvolen pouze dle typu senzoru, ale i podle technického a softwarového řešení a existenci certifikace terminálu či senzoru samotného.

Jedná se o bodové hodnocení, kde hodnota „1“ představuje nejhorší variantu a hodnota „10“ nejlepší variantu.

**Způsob správy systému**

Toto kritérium hodnotí úroveň komfortu a efektivity při správě přístupového systému. Přednost mají varianty umožňující centrální správu více terminálů prostřednictvím softwarového či webového rozhraní, ideálně s možností vzdálené správy přes internet. Správa v rámci lokální sítě je stále považována za dobré řešení, avšak s nižší efektivitou oproti vzdálené správě přes internet. Lokální správa přímo na terminálu, tedy individuální nastavování každé čtečky bez centrálního řízení, je z hlediska provozní náročnosti hodnocena nejhůře. V kontextu velikosti firmy XY je stále považována za akceptovatelnou variantu.

Jedná se o bodové hodnocení, kde hodnota „1“ představuje nejhorší variantu a hodnota „10“ nejlepší variantu.

**Maximální kapacita zaznamenávání vstupů**

Kapacita záznamů určuje, kolik jednotlivých událostí o průchodu může zařízení uchovat v paměti. Vyšší kapacita umožňuje delší dobu uchovávání informací o přístupech bez nutnosti častého stahování nebo mazání záznamů, což je důležité pro případy kdy by byla nutná zpětná

kontrola, audit nebo vyšetřování nějakého incidentu. Přednost mají řešení s vyšší kapacitou paměti pro záznamy, přičemž kapacity nižší jsou hodnoceny hůře.

Jedná se o kritérium kvantitativní maximalizační.

**Tamper ochrana (ochrana zařízení proti neoprávněné manipulaci a fyzické poškození)**

Toto kritérium se zaměřuje na schopnost zařízení odolat pokusům o násilné vniknutí nebo manipulaci. Tamper ochrana slouží k detekci snahy o otevření krytu nebo fyzické poškození zařízení, čímž pomáhá zabránit neoprávněným zásahům do systému. Preferována jsou zařízení, která kontrolují co nejvíce typů fyzické manipulace, například otevření krytu, přerušení napájení, odpojení ze sítě nebo odšroubování montážní desky. Je důležité zmínit, že ne všechny typy tohoto zabezpečení poskytují stejnou úroveň ochrany, některé terminály reagují například pouze pokud je terminál ze stěny násilně stržen.

Jedná se o bodové hodnocení, kde hodnota „1“ představuje nejhorší variantu a hodnota „5“ nejlepší variantu.

## 5.5. Varianty terminálů

V této části práce je uveden přehled jednotlivých variant, které splnily všechna stanovená omezující kritéria a byly proto zařazeny do rozhodovacího procesu. Následně budou tyto varianty porovnány a vyhodnoceny použitím Saatyho metody.

**Varianta 1**

**ZKTeco – MA 300**

MA 300 je autonomní čtečka otisků prstů (dále jen „terminál“), která je navržena pro firemní použití. Terminál využívá základní optickou čtečku otisků prstů a je rovněž vybaven RFID čtečkou, která však nebude v rámci tohoto návrhu využívána. Software umožňuje deaktivaci této RFID čtečky, čímž lze terminál provozovat výhradně na bázi biometrické autentizace.[41]

k1 – Pořizovací cena všech terminálů

Terminál MA 300 představuje nejdostupnější řešení z hodnocených variant. Jeho pořizovací cena činí 9 900 Kč bez DPH na jeden kus, tedy 49 500 Kč celkem za pět terminálů, což je nejnižší cena mezi všemi porovnávanými možnostmi. Cena vychází z nabídky zveřejněné na stránkách „DSTECHNIK.CZ“. Co se týče tohoto kritéria, jedná se o **nejlepší** variantu. [41]

k2 – Technologie snímače otisku prstů

MA 300 využívá základní optický snímač otisků prstů bez podpory pokročilých funkcí, jako je detekce živé tkáně nebo rozeznávání falešných otisků. Terminál rovněž postrádá bezpečnostní certifikace, jako je například FBI PIV, které by garantovaly jeho účinnost a odolnost proti neoprávněnému použití. Z hlediska technologické úrovně se proto jedná o nejméně pokročilou variantu ze všech hodnocených terminálů. Dle těchto vlastností je MA 300 hodnocen **3 body**. [41]

k3 – Způsob správy systému

Terminál je možné spravovat centrálně pomocí softwaru, který je součástí balení a komunikuje s terminály přes lokální síť LAN. Tento způsob správy je sice efektivnější v porovnání s lokální správou přímo na zařízení, ale neposkytuje možnost vzdáleného přístupu. Vzhledem k tomu, že dvě další varianty nabízejí centrální správu i vzdálený přístup, je tato varianta, v této kategorii ohodnocena **5 body**. [41]

k4 – Maximální kapacita zaznamenávání vstupů

MA 300 umožňuje uložení až 100 000 záznamů událostí, což je společně s jednou další variantou nejvyšší hodnota (jedná se o variantu IXM Mycro FP1). Tato kapacita umožňuje provoz bez nutnosti častého zálohování nebo mazání záznamů a terminál proto získává, společně s jednou další variantou, hodnocena jako **nejlepší** volba v tomto kritériu. [41]

k5 – Tamper ochrana

Terminál je vybaven základní mechanickou Tamper ochranou, která detekuje odejmutí zařízení ze stěny pomocí spínače umístěného na zadní straně. Tato ochrana je funkční pouze při fyzickém sejmutí zařízení, v případě otevření krytu bez demontáže se neaktivuje. Po narušení je spuštěn výstupní signál, která lze připojit k externímu zabezpečovacímu systému. V porovnání s dalšími dvěma variantami, které disponují pokročilejší detekcí neoprávněné manipulace, získává MA 300, společně s jednou další variantou, **2 body**. [41]

**Varianta 2**

**2N – Access Unit Fingerprint Reader**

2N Acces Unit Fingerprint je autonomní čtečka otisků prstů, navržená pro firemní použití v prostředí s vyššími požadavky na bezpečnost a spolehlivost.[42]

k1 – Pořizovací cena všech terminálů

Cena terminálu činí 20 145 Kč bez DPH za kus, tedy přibližně 100 725 Kč za pět terminálů. Tato hodnota je nejvyšší ze všech hodnocených variant, což variantu v rámci tohoto kritéria se

řadí jako **nejhorší** možnou. Cena vychází z aktuální nabídky na e-shopu „LANCOMAT.CZ“. [42]

k2 – Technologie snímače otisků prstů

Terminál je vybaven optickým snímačem vyšší třídy, který je chráněn tvrzeným sklem a dále disponuje algoritmy pro detekci falešných otisků i rozpoznávání živé tkáně. Zároveň je certifikován dle normy FBI PIV, což potvrzuje vysokou úroveň zabezpečení a splnění přísných standardů pro biometrická zařízení. Senzor je navíc schopen spolehlivě snímat i poškozené nebo suché otisky prstů, což zajišťuje vyšší komfort a spolehlivost v provozu. Dle těchto vlastností byl terminál hodnocen **10 body**, stejně jako terminál Invixium Inc. – IXM Mycro FP 1. [42]

k3 – Způsob správy systému

Správa zařízení probíhá prostřednictvím webového rozhraní nebo pomocí softwaru 2N Access Commander, který umožňuje efektivní správu více terminálů a export záznamů. Základní verze tohoto softwaru je bezplatná a nabízí podporu až pro 5 terminálů, 50 uživatelů, 1 administrátorský účet a základní správu přístupových práv a logování. Přestože je tato verze funkčně omezená ve srovnání s placenou verzí, pro aktuální provozní potřeby firmy je plně dostačující. [42]

V případě budoucího rozšíření firemního systému by bylo nutné přejít na placenou licenci, jejíž cena začíná přibližně na 16 700 Kč bez DPH. Vzhledem k tomu, že tato rozšířená verze není v současné chvíli nezbytná, není její cena započítávána do celkového hodnocení. Kvůli funkčním omezením základní verze získává tento terminál **8 bodů**. [42]

k4 – Maximální kapacita zaznamenávání vstupů

Terminál umožňuje uložení pouze 500 záznamů událostí, což je druhá nejnižší hodnota mezi všemi hodnocenými varianty. Jedna z variant (BIO C3S) tuto funkci vůbec samostatně neobsahuje, resp. neumožňuje uchovávat záznamy bez připojení k externí jednotce. Přestože u 2N Access Unit Fingerprint Reader existuje možnost jednoduchého exportu záznamů ve formátu CSV prostřednictvím softwaru nebo webového rozhraní, nízká interní kapacita omezuje možnost delšího uchovávání dat bez zásahu správce. Tento limit ale nevyplývá z technických omezení samotného terminálu, ale z omezení bezplatné verze SW 2N Access Commander. Z tohoto důvodu je varianta hodnocena jako **třetí** nejlepší možnost. [42]

k5 – Tamper ochrana

Terminál je vybaven kvalitní mechanickou Tamper ochranou, která detekuje jak sejmutí zařízení ze stěny, tak otevření jeho krytu. V případě narušení je aktivován výstupní signál a událost je zaznamenána do systému. Samotné zařízení nevydává žádný poplach, ale výstup je možné připojit k externímu zabezpečovacímu systému nebo alarmu. V porovnání s dvěma dalšími variantami se jedná o pokročilejší verzi Tamper ochrany, a proto, společně s jednou další variantou, získává **5 bodů**. [42]

**Varianta 3**

**Invixium Inc. - IXM Mycro FP 1**

Mycro FP 1 je autonomní čtečka otisků prstů (dále jen „terminál“) určená pro firemní potřeby. Využívá optický senzor od kvalitní značky SecuGen s technologií SEIR, který disponuje vysokou přesností a rychlostí rozpoznání. Technologie SEIR (Surface Enhanced Irregular Reflection), je pokročilou optickou metodou, která umožňuje vytvářet obraz s vysokým kontrastem a minimálním zkreslením.[41]

k1 – Pořizovací cena všech terminálů

Cena terminálu činí 16 999 Kč bez DPH za kus, což odpovídá částce 84 995 Kč za všech pět terminálů. Cena je vyšší než u MA 300 a BIO C3S, ale nižší než u terminálu 2N Access Unit Fingeprint Reader. Z toho důvodu se jedná **druhou nejdražší** variantu. Cena vychází z nabídky e-shopu „DSHTECHNIK.CZ“. [41]

K2 – Technologie snímače otisku prstů

Terminál využívá senzor vyšší třídy značky SecuGen který je vybavený technologií SEIR a chráněný tvrzeným sklem. Kromě skvělé přesnosti snímání je terminál vybaven také algoritmy pro detekci falešných otisků a rozpoznání živé tkáně, které zvyšují odolnost systému proti neoprávněným vstupům, a také disponuje certifikací FBI PIV. Díky těmto vlastnostem je tento terminál hodnocen **10 body**, stejně jako 2N – Access Unit Fingerpring Scanner. [41]

k3 – Způsob správy systému

Terminál je spravován prostřednictvím webového rozhraní IXM WEB, které je zcela zdarma bez funkčních omezení. Umožňuje kompletní nastavení terminálu, správu uživatelů, export dat i sledování historie přístupů. Výhodou oproti variantám MA 300 a BIO C3S, je možnost vzdálené správy odkudkoli přes internet, bez nutnosti připojení v rámci lokální sítě. Díky tomu je varianta hodnocena jako nejlepší s **10 body**. [41]

K4 – Maximální kapacita zaznamenávání vstupů

Zařízení disponuje interní pamětí až pro 100 000 záznamů událostí, což je nejvyšší hodnota, společně s variantou MA 300, mezi všemi hodnocenými zařízeními a umožňuje dlouhodobé uchovávání přístupových záznamů, bez nutnosti častého zásahu správce. Z toho důvodu je tedy společně s MA 300 hodnocena jako **nejlepší** varianta v této kategorii. [41]

k5 – Tamper ochrana

Tamper ochrana je u této varianty řešena také mechanickým spínačem, který reaguje, jak na otevření krytu, tak na násilné sejmutí terminálu. Událost je zaznamenána a aktivuje výstupní signál. Terminál nedisponuje alarmem vlastním, ale lze jej připojit k externímu zabezpečovacímu systému nebo alarmu. Úroveň ochrany je na stejné úrovni s terminálem 2N Access Unit Fingerprint Reader a získává **5 bodů**. [41]

**Varianta 4**

**XPR S.A. - BIO C3S**

BIO C3S je autonomní čtečka otisků prstů (dále jen „terminál“) určená pro firemní použití. Využívá kapacitní senzor, který je obecně známý vyšší výdrží proti mechanickému poškození, bez nutnosti dalších ochranných prvků senzoru. Jedná se o jeden z lepších terminálů, co se týče poměru cena/výkon.[42]

k1 – Pořizovací cena všech terminálů

Cena modelu činí 11 561,98 Kč bez DPH za kus, a tedy 57 809,90 Kč za pět všech kusů. Jedná se o **druhou nejlevnější** možnost mezi všemi varianty. Cena vychází z nabídky e-shopu „LANCOMAT.CZ“. [42]

k2 – Technologie snímače otisku prstů

BIO C3S využívá kapacitní senzor značky XPR, který oproti základním optickým senzorům nabízí vyšší přesnost snímání, schopnost lépe rozlišovat živou tkáň bez složitých algoritmů, větší odolnosti vůči poškrábáním, bez nutnosti další externí ochrany senzoru. Jedná se však o senzor nižší třídy, který není doplněn o pokročilé algoritmy ani certifikace, jako jsou přítomny u některých ze zmíněných variant. Ačkoli kapacitní senzory bývají obecně přesnější než některé optické senzory, v tomto případě je tento konkrétní překonán modely 2N Access Unit Fingerprint Reader a IXM Mycro FP 1, které kombinují kvalitní optický snímač s pokročilými algoritmy pro vyšší bezpečnost a certifikací FBI PIV. Senzor může mít rovněž potíže se snímáním suché nebo poškozené pokožky a vyžaduje stabilní kontakt s prstem. Díky těmto vlastnostem je terminál hodnocen **6 body**, které odráží lepší technologickou úroveň ve srovnání

s MA 300, ale nižší úroveň oproti 2N – Access Unit Fingerprint Scanner a Invixium Inc. – IXM Mycro FP 1. [41][42]

k3 – Způsob správy systému

Správa probíhá pomocí softwaru PROS CS, který je zdarma, ale vyžaduje fyzické propojení terminálu k počítači. Vzdálený přístup je možný pouze při dokoupení dalšího zařízení, který jej umožní. Varianta je tedy hodnocena jako nejhorší možnost s **2 body**. [42]

k4 – Maximální kapacita zaznamenávání vstupů

Terminál neumožňuje uchovávání záznamů událostí ve své interní paměti. Aby bylo možné záznamy o přístupech ukládat, je nutné terminál připojit k externímu kontroléru nebo počítači s potřebným softwarem, který tuto funkci zajistí. V takovém případě by už BIO C3S nebyl využíván jako autonomní jednotka, protože veškeré zpracování přístupů, vyhodnocování oprávnění i ukládání dat by přebírala externí jednotka. Vzhledem k absenci vlastního ukládání vstupů, je varianta v rámci tohoto kritéria **nejhorší**. [42]

k5 – Tamper ochrana

BIO C3S je vybaven mechanickou Tamper ochranou, která reaguje pouze na odstranění terminálu z povrchu kde je připevněn. Po přerušení kontaktu je aktivován výstupní signál, který lze připojit k externímu zabezpečovacímu systému. Terminál sám o sobě nevydává žádný poplach. V porovnání s varianty 2N Access Unit Fingerprint Reader a IXM Mycro FP 1 jde o nižší úroveň ochrany, a proto terminál v rámci tohoto kritéria získává **2 body**. [42]

**Kriteriální tabulka**

Tabulka 3 znázorňuje předběžné srovnání jednotlivých variant biometrických přístupových terminálů vůči zvoleným kritériím. [43]

Pořadí preferencí jednotlivých kritérií bylo stanoveno subjektivně a na základě úvahy o jejich významu pro potřeby firmy. Výsledkem je porovnání, které neslouží jako finální rozhodnutí, ale jako vstupní rámec pro další rozhodovací metodu, konkrétně Saatyho metodu, která pracuje s vahami jednotlivých kritérií a pomáhá kvantifikovat celkové pořadí variant. [43]

Na základě tohoto předběžného hodnocení vychází jako nejvhodnější varianta terminál IXM Mycro FP 1, které dosahuje nejlepších výsledků ve více kritériích zároveň.

**Tabulka 3:** Kriteriální tabulka

| | Kritéria | k1 | k2 | k3 | k4 | k5 |
|---|---|---|---|---|---|---|
| | Pořadí preferencí | 3 | 1 | 2 | 4 | 5 |
| alternativy | Název produktu | Pořizovací cena všech terminálů [Kč] | Technologie snímače otisku prstů [body] | Způsob správy systému [body] | Maximální kapacita zaznamenávání vstupů [počet] | Tamper ochrana [body] |
| a1 | MA 300 | 49 500 | 3 | 5 | 100 000 | 2 |
| a2 | 2N Access Unit Fingerprint Reader | 100 725 | 10 | 8 | 500 | 5 |
| a3 | IXM Mycro FP 1 | 84 995 | 10 | 10 | 100 000 | 5 |
| a4 | BIO C3S | 57 809 | 6 | 2 | 0 | 2 |

*Zdroj: vlastní zpracování*

## 5.6. Průběh a výsledek Saatyho metody

Prvním krokem rozhodovacího procesu bylo sestavení Saatyho porovnávací matice, v které byla jednotlivá kritéria mezi sebou ohodnocena dle jejich důležitosti **(výpočet v Příloze B)**. Výsledkem této matice bylo stanovení vah jednotlivých kritérií:

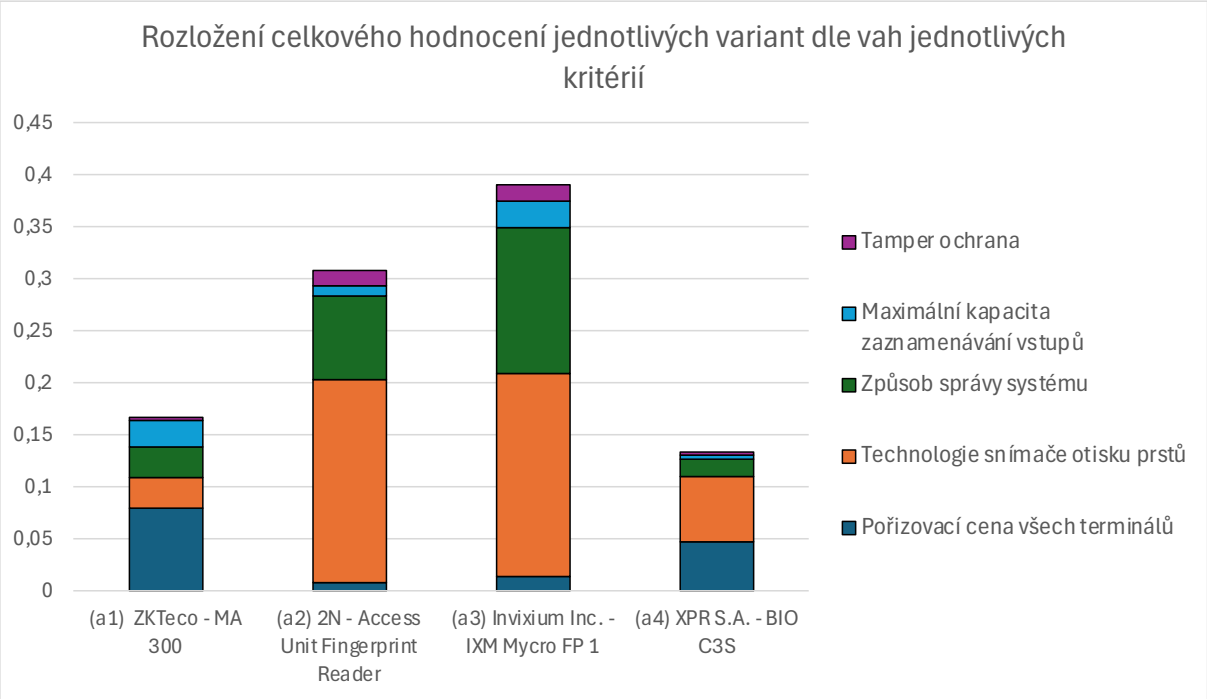
- k1 – 0,0819,
- k2 – 0,4806,
- k3 – 0,2662,
- k4 – 0,1132,
- k5 – 0,0581.

Následně bylo třeba ověřit konzistenci rozdělení hodnot mezi jednotlivá kritéria, a to pomocí výpočtu poměru konzistence (CR). Výpočet proběhl s využitím softwaru MATLAB, kde byla určena hodnota λmax (lambda max) a zbývající část výpočtu byla provedena v programu Excel **(výpočet poměru konzistence v Příloze B)**. [43]

Dalším krokem bylo sestavení matice pro každé z hodnotících kritérií, ve kterých byly navzájem porovnávány jednotlivé varianty čteček otisků prstů (a1 až a4) na základě jejich

vhodnosti vzhledem ke konkrétnímu kritériu. Z těchto matic byla následně pomocí geometrických průměrů a jejich normalizace určena dílčí ohodnocení variant, které vyjadřují míru preference jednotlivých variant vzhledem k danému kritériu. Tato dílčí ohodnocení byla následně vynásobena váhami těch kritérií, ke kterým byly jednotlivé varianty porovnávány, čímž byly získány vážené hodnoty pro každou variantu. Tyto hodnoty jednotlivých variant byly následně sečteny, čímž vznikl výsledný součet reprezentující celkovou míru vhodnosti každé z variant s ohledem na stanovená kritéria **(výpočet ohodnocení variant v Příloze B)**. [43]

Výsledný vážený součet dílčích ohodnocení variant byl následně převeden do podoby sloupcového grafu [43]:




**Obrázek 2:** Grafické porovnání variant terminálů

*Zdroj: vlastní zpracování*

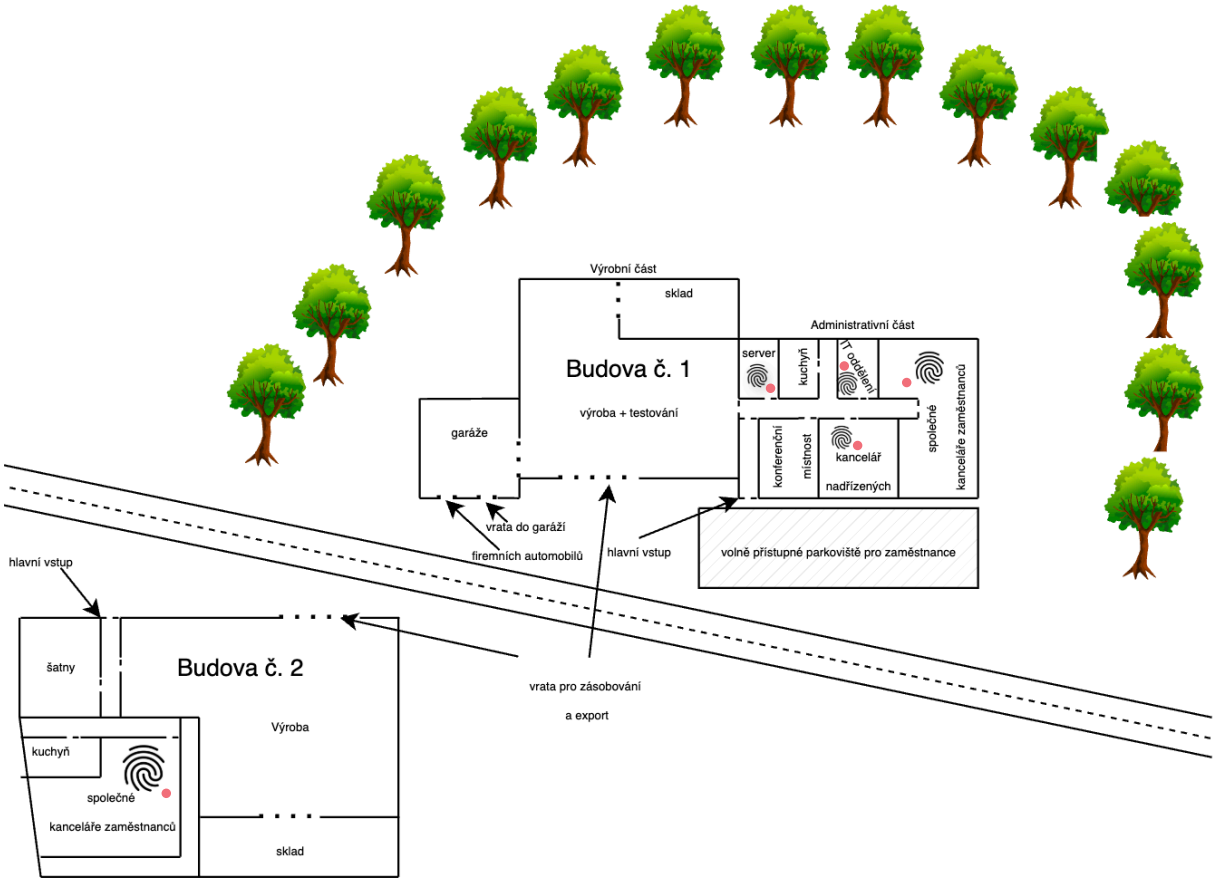
Obrázek 2 ukazuje ohodnocení jednotlivých variant, přičemž nejvhodnější je dle výsledků varianta **a3** neboli **Invixium Inc. – IXM Mycro FP 1**. Tato varianta vyniká především vysokým hodnocením ve třech nejdůležitějších kritériích: technologie snímače otisku prstů, způsob správy systému a maximální kapacita zaznamenávání vstupů. Tato varianta navíc nabízí technologicky pokročilou tamper ochranu, a přestože její pořizovací cena není nejnižší, zůstává stále přijatelná. Výsledné hodnocení pomocí Saatyho metody tak potvrzuje její vhodnost.[43]

## 5.7. Návrh nového přístupového systému s integrací čtečky otisku prstů

Na základě výsledku rozhodovacího procesu provedeného pomocí Saatyho metody vícekriteriálního rozhodování, ve kterém byla jako nejvhodnější varianta vyhodnocena varianta Invixium Inc. – IXM Mycro FP 1, byl vytvořen návrh nového přístupového systému pro vybrané prostory firmy.

Tyto prostory byly již předem určeny na základě toho, že obsahují citlivé informace nebo se v nich s těmito informace pracuje. Pro tyto prostory byla vyhotovena analýza rizik za účelem zjištění nedostatků současných RFID čteček (viz. Tabulka 1), které by navržený systém byl schopen ve značné míře eliminovat.

Prostory, kterých se návrh týká, jsou znázorněny ve vizuálním vyobrazením objektu (viz. Obrázek 3). Prostory jsou vyznačeny černým symbolem otisku prstu, vedle kterého je umístěna červená tečka, která slouží pro lepší vyobrazení míst, kde má být v rámci návrhu umístěna čtečka otisku prstu umožňující přístup do dané místnosti:




**Obrázek 3:** Plán areálu firmy s vyznačenými čtečky otisky prstů

*Zdroj: vlastní zpracování*

Návrh použití čteček otisku prstu se tedy týká následujících místností:

- serverovna (na Obrázek 3 jako „server“),
- IT oddělení,
- kancelář vedení,
- společné kanceláře zaměstnanců v budově č. 1,
- společné kanceláře zaměstnanců v budově č. 2.

Navržený systém by přinesl možnost detailního nastavení přístupových oprávnění pro jednotlivé místnosti, bez nutnosti externích nosičů. Přístup by byl povolen pouze konkrétním osobám na základě jejich pracovních potřeb. Majitel společnosti by měl přístup do všech prostor, stejně jako další osoby, u kterých je takový přístup nezbytný. Ostatním zaměstnancům by byla přístupová oprávnění přidělena pouze do prostor, které souvisejí s jejich pracovním zařazením. Uživatelům by navíc mohla být přístupová oprávnění nastavena i pouze na určitou dobu (např. konkrétním datovém rozmezí) nebo jen v přesně vymezených hodinách, pokud by bylo potřeba zavést důkladnější bezpečnostní opatření.

V případě selhání autentizace pomocí otisku prstu, například po několika neúspěšných pokusech, má správce možnost provést reset limitu prostřednictvím administrátorského softwaru. Tento software umožňuje vzdálený přístup, tudíž není nutná fyzická přítomnost správce v budově, pokud by tato skutečnost nastala. Dále je možné znovu zaregistrovat otisk nebo přidat alternativní prst v případě potřeby.

Díky tomu, že otisk prstu nelze zapomenout, ztratit nebo předat jiné osobě, odpadá potřeba používat dvou faktorovou autentizaci v místnosti se serverem. V případě budoucí potřeby zvýšení zabezpečení v určitých prostorech, jako je serverovna, je možné čtečku otisku prstu doplnit o další autentizační prvek.

Navržený biometrický přístupový systém tak odpovídá potřebám daných prostor a přináší praktické a bezpečné řešení, které reaguje na konkrétní slabiny současného způsobu zabezpečení.

# ZÁVĚR

Tato bakalářská práce se zaměřila na problematiku přístupových systémů, biometrických prvků a jejich využití v rámci přístupových systémů firmy. Součástí práce bylo také popsání současného stavu přístupového systému ve vybrané firmě a hlavním cílem byl návrh nového přístupového systému s integrací biometrických prvků.

V úvodní části práce byla představena související legislativa upravující podmínky pro zavádění a využívání přístupových systémů, včetně biometrických údajů ve firemním prostředí. Následně byly popsány různé druhy přístupových systémů, jejich princip fungování, výhody, nevýhody a možnosti praktického využití. Systémy byly rozděleny do dvou hlavních kategorií, mechanické a elektronické přístupové systémy, a dále biometrické přístupové systémy. Každá z těchto kategorií byla dále členěna na dvě podskupiny podle typu řešení a způsobu ověřování identity.

Druhá část práce začala popisem současného stavu přístupového systému ve vybrané firmě, se zaměřením na způsob zabezpečení jednotlivých prostor. Následně byla provedena analýza rizik, která poukázala na nedostatky současného přístupového systému, mezi ně patřil patřili rizika jako je například ztráta RFID.

Na základě této analýzy se biometrická autentizace osvědčila jako vhodné řešení, které může většinu identifikovaných nedostatků účinně eliminovat. Následně bylo přistoupeno k výběru konkrétní metody biometrického přístupu, kterou se staly otisky prstů. Další částí bylo vymezení rozhodovacího procesu, stanovení omezujících a hodnotících kritérií, definování variant řešení a aplikování Saatyho metody, která umožnila určit nejvhodnější variantu.

Na základě výsledků Saatyho metody, byl zpracován návrh nového přístupového systému s integrací biometrických prvků, přičemž bylo popsáno rozmístění čteček, správa přístupových oprávnění a možnost vzdálené administrace.

Téma této bakalářské práce přispělo k rozšíření znalostí v oblasti přístupových systémů a biometrické autentizace. Přínosem této práce je získání hlubší orientace v technologiích ověřování identity a v problematice implementace těchto systémů v podnikovém prostředí. Výsledné poznatky mohou sloužit jako východisko pro budoucí návrhy zabezpečení a praktické využití biometrických technologií v oblasti kontroly přístupu.

# POUŽITÁ LITERATURA


[1] EVROPSKÝ PARLAMENT A RADA EU. Nařízení evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů o volném pohybu těchto údajů a o zrušení směrnice 65/46/ES (obecné nařízení o ochraně osobních údajů). V *Zákony pro lidi.cz* [online]. [cit. 22.4.2025]. Dostupné z: https://www.zakonyprolidi.cz/pravoeu/dokument?celex=32016R0679.

[2] ČESKÁ REPUBLIKA. Zákon č. 110/2019 Sb., o zpracování osobních údajů. V: *Zákony pro lidi.cz* [online]. [cit. 22.4.2025]. Dostupné z: https://www.zakonyprolidi.cz/pravoeu/dokument?celex=32016R0679.

[3] ČESKÁ REPUBLIKA. Zákon č. 262/2006 Sb., zákoník práce. V *Zákony pro lidi.cz* [online]. [cit. 22.4.2025]. Dostupné z: https://www.zakonyprolidi.cz/pravoeu/dokument?celex=32016R0679.

[4] AVIGILON. *Benefits and use cases for wireless door access control systems.* [online]. [cit. 2024-11-23]. Dostupné z: https://www.avigilon.com/blog/wireless-access-control-system.

[5] BENANTAR, *Messaoud. Access Control Systems: Security, Identity Management and Trust Models.* 1. Vyd. New York: Springer US, 2006. ISBN 978-0-387-00445-7.

[6] SINGH, Neeraj K. *Near-field Communication (NFC). Information Technology and Libraries* [online]. 2020, roč 39, č. 2. [cit. 2024-11-24]. Dostupné z: https://www.researchgate.net/publication/342209942_Near-field_Communication_NFC. ISSN 0730-9295

[7] BURDA, Karel. *Universal description of access control systems. IJCSNS International Journal of Computer Science and Network Security* [online]. 30. srpen 2024, roč. 24, č. 8, s. 43-53 [cit. 2024-11-24]. Dostupné z: http://search.ijcsns.org/02_search/02_search_03.php?number=202408005. ISSN 1738-7906. ISSN 1738-7906.

[8] HUSÁK, Miroslav; VÍTEK, Tomáš; TEPLÝ, Tomáš. *Přístupové systémy (1). APT Journal* [online]. 26. března 2012, poslední revize 26.3.2012 [cit. 2024-11-24]. Dostupné z: https://www.atpjournal.sk/budovy/rubriky/prehladove-clanky/pristupove-systemy-1.html?page_id=14430.

[9] LOCKWIKI. *Combination* [online]. 19.10.2024. [cit. 2024-11-24]. Dostupné z: https://www.lockwiki.com/index.php?title=Combination&action=history.

[10] **SELIMIS, Georgios, Nicolas SKLAVOS a Odysseas G. KOUFOPAVLOU.** Crypto processor for contactless smart cards. In *Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference (MELECON 2004).* Dubrovník, Chorvatsko: IEEE, 2004. Svazek 2, s. 803–806. [online]. [cit. 2024-11-24]. Dostupné z: https://ieeexplore.ieee.org/document/1347053.

[11] SOUKALOVÁ, *Iveta. Přístupové čipy a karty: Jak fungují, výhody a kde je využít* [online]. c2024, poslední revize 10.3.2025 [cit. 2024-11-24]. Dostupné z: https://www.clockan.cz/pristupove-cipy-a-karty-jak-funguji-vyhody/.

[12] CLARK, ROGER. *Introduction to Chip-Cards and Smart Cards* [online]. c1998, poslední revize 23.5.1998 [cit. 2024-11-24]. Dostupné z: https://www.rogerclarke.com/EC/ChipIntro.html.

[13] BOSSUET, Lilian; GRAND, Michael; GASPAR, Lubos; FISCHER, Viktor; GOGNIAT, Guy. *Architecutres of flexible symmetric key crypto engines-a survey: From hardware coprocessor to multi-crypto-processor systém on chip. ACM Computing Surveys* [online]. 30.8.2013, roč. 45, č. 4, čl. č. 41, s. 1-32. [cit. 2024-11-24]. Dostupné z: https://dl.acm.org/doi/10.1145/2501654.2501655. ISSN 0360-0300.

[14] SECUREPASS. *Magnetic Strip Card Reader Access Control System* [online]. Leden 2021 [cit. 2024-11-24]. Dostupné z: https://thesecurepass.com/blog/magentic-strip-card-reader-access-control-system.

[15] WU, Chi-Che; HSU, Chiung-Wen; CHENG, Rung-Shiang. *The digital signature technology for access control system of mobile.* In *Proceedings of the 2018 IEEE International Conference on Applied System Innovation (ICASI)* [online]. IEEE, ed. Chiba, Japonsko: IEEE, 2018 [cit. 2024-11-24]. Dostupné z: https://ieeexplore.ieee.org/document/8394410.

[16] WANG, Xiaoxu; WANG, Yuesheng. *An office intelligent access control system based on RFID.* In *Proceedings of the 2018 Chinese Control And Decision Conference (CCDC)* [online]. Shenyang, Čína: IEEE, 9.-11.6.2018. [cit. 2023-11-24]. Dostupné z: https://ieeexplore.ieee.org/document/8407206.

[17] https://sci-hub.se/10.1109/MITP.2005.69WEINSTEIN, Ron. *RFID: a technical overview and its application to the enterprise. IT Professional I* [online]. 30.6.2005, roč. 7, č. 3, s.

27-33. ISSN 1803-7232. [cit. 2024-11-24]. Dostupné z: https://ieeexplore.ieee.org/document/1490473?arnumber=1490473. ISSN 1520-9202.

[18] FAROOQ, Umar; HASAN, Mahmood ul; AMAR, Muhammad; HANIF, Athar; ASAD, Muhammad Usman. *RFID Based Security and Access Control System. IACSIT International Journal of Engineering and Technology* [online]. 2014, roč. 6, č. 4, s. 309-314. [cit. 2024-11-24]. Dostupné z: https://www.researchgate.net/publication/275685766_RFID_Based_Security_and_Access_Control_System. ISSN 1793-8236.

[19] ISO/IEC 7813 [online]. Wikipedia: The Free Encyclopedia, poslední revize 15. října 2024 [cit. 24-11-2024]. Dostupné z: https://en.wikipedia.org/wiki/ISO/IEC_7813.

WIKIPEDIA. *ISO/IEC 7813* [online]. *Wikipedia, The Free Encyclopedia,* poslední úprava 18. března 2024 [cit. 2024-11-24]. Dostupné z: https://en.wikipedia.org/wiki/ISO/IEC_7813.

[20] MAYES, Keith; MARKANTONAKIS, Konstantinos. *Smart Cards, Tokens, Security and Applications.* Berlín: Springer Science & Business Media, 2007. ISBN 978-0387721989.

[21] STANEKOVÁ, L'ubica; STANEK, Martin. *Analysis of dictionary methods for PIN selection. Computers & Security* [online]. 1.11.2013, roč. 39, s. 289-298. ISSN 0167-4048. [cit. 2024-11-24]. Dostupné z: https://dblp.org/rec/journals/compsec/StanekovaS13.html?view=bibtex.

[22] CALOTA, Daniela-lulia; PASCA, Sever. *Presentation of Several Secure Access Systems and Implementations.* In *Proceedings of the 2019 11th International Symposium on Advanced Topics in Electrical Engineering (ATEE)* [online]. Bukurešť, Rumunsko: IEEE, 2019. s. 1-6. [cit. 2024-11-24]. Dostupné z: https://ieeexplore.ieee.org/document/8724986.

[23] RAHUL, Anusha; KRISHNAN, Gokul; H, Unni Krishnan; RAO, Sethuraman. Near Field Communication (NFC) Technology: A Survey [online]. Vyd. International Journal on Cybernetics & Informatics, 2015 [cit. 2025-02-10]. Dostupné z: https://sci-hub.se/10.5121/ijci.2015.4213. DOI: 10.5121/ijci.2015.4213.

[24] JAIN, A. K.; ROSS, A.; PRABHAKAR, S. *An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology* [online]. 30.1.2004, roč. 14, č. 1, s. 4-20. [cit. 2025-02-10]. Dostupné z: https://ieeexplore.ieee.org/document/1262027. ISSN 1558-2205.

[25] SINJINI, Mitra; GOFMAN, Mikhail. *Biometrics in a data driven world: trends, technologies, and challanges.* 1. vyd. Boca Raton: CRC Press, Taylor & Francis, 2017. ISBN 978-1498737647.

[26] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií.* Vyd. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. ISBN 978-8026071150.

[27] KIM, Hyun-Jung. *Biometrics, Is It a Viable Proposition for Identity Authentication and Access Control? Computers & Security* [online]. 1.1995, roč. 14, č. 3, s. 205-214. [cit. 2025-02-10]. Dostupné z: https://doi.org/10.1016/0167-4048(95)97054-E. ISSN 0167-4048.

[28] MITTAL, Y.; VARSHNEY, A.; AGGARWAL, P.; MATANI, K.; MITTAL, V.K. *Fingerprint biometric based Access Control and Classroom Attendance Management Systém. In Proceedings of the 2015 Annual IEEE India Conference (INDICON)* [online]. New Delhi, Indie: IEEE, 2015. s. 1-6. [cit. 2025-02-18]. Dostupné z: https://ieeexplore.ieee.org/document/7443699. ISSN 2325-9418.

[29] JAYARAMAN, Umarani; GUPTA, Phalguni; GUPTA, Sandesh; ARORA, Geetika; TIWARI, Kamlesh. *Recent development in face recognition. Neurocomputing* [online]. 2020, roč. 408, s. 231-245. [cit. 2025-02-20]. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S0925231220304951?via%3Dihub. ISSN 1872-8286.

[30] CHANG, K.I.; BOWYER, K. W.; FLYNN, P. J. *An evaluation of multimodal 2D+3D face biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence* [online]. 7.3.2005, roč. 27, č. 4, s. 619-624. [cit. 2025-02-20]. Dostupné z: https://ieeexplore.ieee.org/abstract/document/1401913. ISSN 0162-8828.

[31] KOVACS, L.; ZIMMERMANN, Alexander; BROCKMANN, Gernot; GÜHRING, M.; BAURECHT, H.; PAPADOPOULOS, N. A.; SCHWENZER-ZIMMERER, K.; SADER, R.; BIEMER, E.; ZEILHOFER, H. F. *Three-dimensional recording of the human face with a 3D laser scanner. Journal of Plastic, Reconstructive & Aesthetic Surgery* [online]. 2006, roč. 59, č. 11, s. 1193-1202. [cit. 2025-02-20]. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S1748681506000970. ISSN 1748-6815.

[32] HÁJEK, J; DRAHANSKÝ, M. *Recognition-Based on Eye Biometrics: Iris and Retina.* In *Biometric-Based Physical and Cybersecurity Systems.* 1. vyd. Obaidat, M., Traore, I.

a Woungang, I., vyd. Cham: Springer, 2019. Kapitola 3, s. 37-102. ISBN 978-3-319-98733-0.

[33] BAHMED, Farah; OULD MAMMAR, Madani. *Assessment of Finger Geometry Features for Multibiometric Authentication.* In *ICWIP 2019: Proceedings of the 2019 2nd International Conference on Watermarking and Image Processing* [online]. 1. vyd. New York: Association for Computing Machinery 2020. s. 1-5. [cit. 2025-02-27] ISBN 978-1-4503-7280-0. Dostupné z: https://dl.acm.org/doi/10.1145/3369973.3369974.

[34] SANCHEZ-REILLO, Raul; SANCHEZ-AVILA, Carmen; GONZALEZ-MARCOS, Ana Pilar. *Biometric identification through hand geometry measurements. IEEE Transactions on Pattern Analysis and Machine Intelligence* [online]. 2000, roč. 22, č. 10, s. 1168-1171. [cit. 2025-02-27]. Dostupné z: https://ieeexplore.ieee.org/document/879796. ISSN 1939-3539.

[35] DAPPURI, Bhasker; SRIJA, Vidadala; DHANNE, Basava. *Palm print Biometric Authentication Systém for Security Applications.* In *IOP Conference Series: Materials Science and Engineering* [online]. 1. vyd. Warangal, Indie: IOP Publishing, 2020. *International Conference on Recent Advancements in Engineering and Management (ICRAEM-2020),* 9.-10.10.2020, Warangal, Indie. [cit. 2025-03-02]. Dostupné z: https://iopscience.iop.org/article/10.1088/1757-899X/981/4/042083. ISSN 1757-899X.

[36] WU, Wei; ELLIOTT, Stephen John; LIN, Sen; SUN, Shenshen; TANG, Yandong. *Review of palm vein recognition. IET Biometrics* [online]. 2019, roč. 8 č. 6, s. 1-10. [cit. 2025-03-06]. Dostupné z: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-bmt.2019.0034. ISSN 2047-4938.

[37] WANG, Y.; XIE, W.; YU, X.; SHARK, L.-K. *An automatic physical access control systém based on hand vein biometric identification. IEEE Transactions on Consumer Electronics* [online]. 2015, roč. 61, č. 3, s. 320-327. [cit. 2025-03-06]. Dostupné z: https://ieeexplore.ieee.org/document/7298091. ISSN 1558-4127.

[38] ŠILHÁNKOVÁ, Vladimíra a NETÍKOVÁ, Květa. *Komparace metod analýzy rizik pro hodnocení bezpečnostních hrozeb lokalit brownfields.*V XXIII. Mezinárodní kolokvium o regionálních vědách. Sborník příspěvků. Brno: Masarykova univerzita, 2020. s. 489-496. DOI: 10.5817/CZ.MUNI.P210-9610-2020-62.

[39] HFSecurity. *Check Accuracy of Fingeprint Scanner* [online]. HFSecurity [cit. 2025-03-26]. Dostupné z: https://hfsecurity.cn/check-accuracy-of-fingerprint-scanner/.

[40] INFORDATA. *What is FAR and what is FRR?* [online]. Infordata Shop [cit. 2025-04-26]. Dostupné z: https://en.infordata-shop.com/aw_faq/faq_fingerprint/what_is_far_and_what_is_frr_/.

[41] DS Technik. *Oficiální web společnosti DS Technik s.r.o.* [online]. [cit. 2025-04-29]. Dostupné z: https://www.dstechnik.cz/

[42] Lancomat. *Oficiální web společnosti LANCOMAT s.r.o.* [online]. [cit. 2025-04-29]. Dostupné z: https://www.lancomat.cz/

[43] KRUPKA, Jiří, KAŠPAROVÁ Miloslava a MÁCHOVÁ Renata. *Rozhodovací procesy.* 1. vydání. Pardubice: Univerzita Pardubice, 2012. ISBN 978-80-7395-478-9

# SEZNAM PŘÍLOH

## Příloha A: Výpočet analýzy rizik

| Místnosti | | Data a informace v jednotlivých prostorách | N |
|---|---|---|---|
| A1 | Server | Zálohy firemních dat, osobní údaje zaměstnanců konfigurace systémmů a další důležitá data | 5 |
| A2 | Kancelář vedení | Finanční dokumenty, smlouvy, smlouvy s dodavateli, citlivé firemní údaje, trezor | 4 |
| A3 | Společné kanceláře zaměstnanců (Budova č. 1 a 2) | Počítače s technickou a finanční dokumentací, výkresy | 3 |
| A4 | IT oddělení | Správa přístupových systémů, přihlašovací údaje, IT insfrastruktura | 4 |

**Obrázek 4:** Výše citlivosti dat v jednotlivých místnostech

*Zdroj: vlastní zpracování*

| | | | Místnosti | | | |
|---|---|---|---|---|---|---|
| | | P | Server | Kancelář vedení | Společné kanceláře zaměstnanců (Budova č. 1 a 2) | IT Oddělení |
| Hrozby | | | A1 | A2 | A3 | A4 |
| H1 | Ztráta RFID karty | 4 | X | X | X | X |
| H2 | Krádež RFID karty | 2 | X | X | X | X |
| H3 | Klonování RFID karet | 1 | X | X | X | X |
| H4 | Odposlech/Odpozorování PIN kódu | 2 | X | | | |
| H5 | Fyzická manipulace s přístupovým systémem | 2 | X | X | X | X |
| H6 | Lidská chyba | 5 | X | X | X | X |

**Obrázek 5:** Pravděpodobnost vzniku hrozeb

*Zdroj: vlastní zpracování*

| | | | Místnosti | | | |
|---|---|---|---|---|---|---|
| | | H | Server | Kancelář vedení | Společné kanceláře zaměstnanců (Budova č. 1 a 2) | IT Oddělení |
| Hrozby | | | A1 | A2 | A3 | A4 |
| H1 | Ztráta RFID karty | 2 | X | X | X | X |
| H2 | Krádež RFID karty | 4 | X | X | X | X |
| H3 | Klonování RFID karet | 5 | X | X | X | X |
| H4 | Odposlech/Odpozorování PIN kódu | 3 | X | | | |
| H5 | Fyzická manipulace s přístupovým systémem | 4 | X | X | X | X |
| H6 | Lidská chyba | 3 | X | X | X | X |

**Obrázek 6:** Dopad hrozeb při jejich vzniku

*Zdroj: vlastní zpracování*

| Místnost (N) | Hrozba (P) | Hrozba (H) | Získané body | Stupneň rizika |
|---|---|---|---|---|
| Server (5) | Lidská chyba (5) | Lidská chyba (3) | 75 | I. |
| Server (5) | Ztráta RFID karty (4) | Ztráta RFID karty (3) | 60 | I. |
| Kancelář vedení (4) | Lidská chyba (5) | Lidská chyba (3) | 60 | I. |
| IT oddělení (4) | Lidská chyba (5) | Lidská chyba (3) | 60 | I. |
| Kancelář vedení (4) | Ztráta RFID karty (4) | Ztráta RFID karty (3) | 48 | II. |
| IT oddělení (4) | Ztráta RFID karty (4) | Ztráta RFID karty (3) | 48 | II. |
| Společné kanceláře zaměstnanců v budově č.1 a 2 | Lidská chyba (5) | Lidská chyba (3) | 45 | II. |
| Server (5) | Krádež RFID karty (2) | Krádež RFID karty (4) | 40 | III. |
| Server (5) | Fyzická manipulace s přístupovým systémem (2) | Fyzická manipulace s přístupovým systémem (4) | 40 | III. |
| Společné kanceláře zaměstnanců v budově č.1 a 2 | Ztráta RFID karty (4) | Ztráta RFID karty (3) | 36 | III. |
| Kancelář vedení (4) | Krádež RFID karty (2) | Krádež RFID karty (4) | 32 | III. |
| Kancelář vedení (4) | Fyzická manipulace s přístupovým systémem (2) | Fyzická manipulace s přístupovým systémem (4) | 32 | III. |
| IT oddělení (4) | Krádež RFID karty (2) | Krádež RFID karty (4) | 32 | III. |
| IT oddělení (4) | Fyzická manipulace s přístupovým systémem (2) | Fyzická manipulace s přístupovým systémem (4) | 32 | III. |
| Server (5) | Odposlech/Odpozorování PIN kódu (2) | Odposlech/Odpozorování PIN kódu (3) | 30 | III. |
| Server (5) | Klonování RFID karet (1) | Klonování RFID karet (5) | 25 | IV. |
| Společné kanceláře zaměstnanců v budově č.1 a 2 | Krádež RFID karty (2) | Krádež RFID karty (4) | 24 | IV. |
| Společné kanceláře zaměstnanců v budově č.1 a 2 | Fyzická manipulace s přístupovým systémem (2) | Fyzická manipulace s přístupovým systémem (4) | 24 | IV. |
| Kancelář vedení (4) | Klonování RFID karet (1) | Klonování RFID karet (5) | 20 | IV. |
| IT oddělení (4) | Klonování RFID karet (1) | Klonování RFID karet (5) | 20 | IV. |
| Společné kanceláře zaměstnanců v budově č.1 a 2 | Klonování RFID karet (1) | Klonování RFID karet (5) | 15 | V. |

**Obrázek 7:** Kompletní tabulka výsledků analýzy rizik

Zdroj: vlastní zpracování

## Příloha B: Výpočet Saatyho metody

| Váhy kritérií | | | | | | | |
|---|---|---|---|---|---|---|---|
| Kritéria | k1 | k2 | k3 | k4 | k5 | geometrický průměr | vi |
| k1 | 1 | 1/4 | 1/3 | 4 | 5 | 1,10756634 | 0,14980182 |
| k2 | 4 | 1 | 3 | 6 | 8 | 3,56520492 | 0,48220513 |
| k3 | 3 | 1/3 | 1 | 5 | 6 | 1,97435049 | 0,26703709 |
| k4 | 1/4 | 1/6 | 1/5 | 1 | 3 | 0,47817625 | **0,06467484** |
| k5 | 1/5 | 1/8 | 1/6 | 1/3 | 1 | 0,26824615 | 0,03628113 |
| | | | | | Suma: | 7,39354415 | 1 |

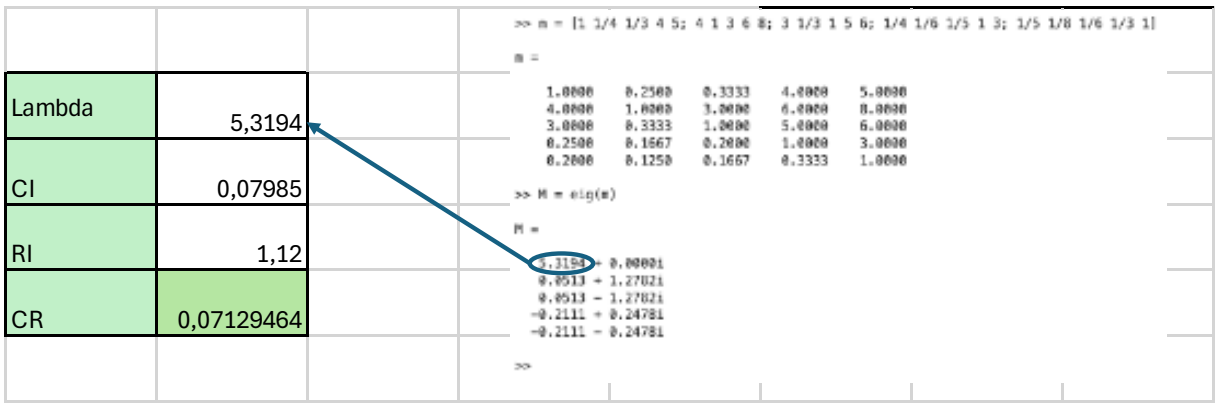
**Obrázek 8:** Výpočet vah kritérií metodou párového porovnávání

*Zdroj: vlastní zpracování*

| Hodnota | Význam |
|---|---|
| 1 | Obě kritéria jsou stejně důležitá |
| 3 | Mírná přednost jednoho kritéria |
| 5 | Silná přednost |
| 7 | Velmi silná přednost |
| 9 | Extrémní přednost |
| 2, 4, 6, 8 | Mezi úrovně |

**Obrázek 9:** Tabulka bodové významnosti

*Zdroj: vlastní zpracování*



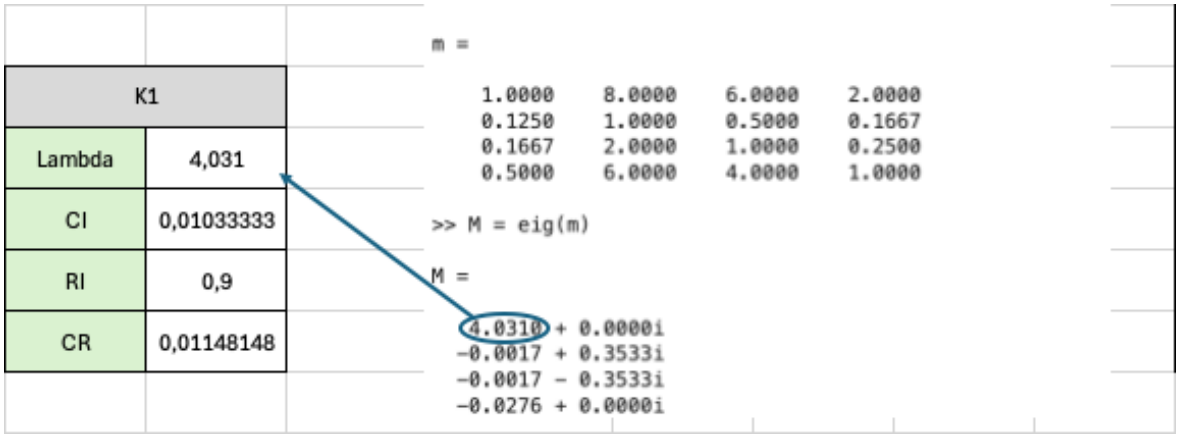

**Obrázek 10:** Ověření konzistence párového porovnávání kritérií

*Zdroj: vlastní zpracování*

| Výběr varianty | | | | | | |
|---|---|---|---|---|---|---|
| k1 | a1 | a2 | a3 | a4 | geometrický průměr | **h1j** |
| a1 | 1 | 8 | 6 | 2 | 3,13016916 | **0,53524225** |
| a2 | 1/8 | 1 | 1/2 | 1/6 | 0,31947155 | 0,05462793 |
| a3 | 1/6 | 2 | 1 | 1/4 | 0,53728497 | 0,09187287 |
| a4 | 1/2 | 6 | 4 | 1 | 1,86120972 | 0,31825695 |
| | | | | Suma: | 5,8481354 | 1 |

**Obrázek 11:** Obodování variant dle k1

*Zdroj: vlastní zpracování*



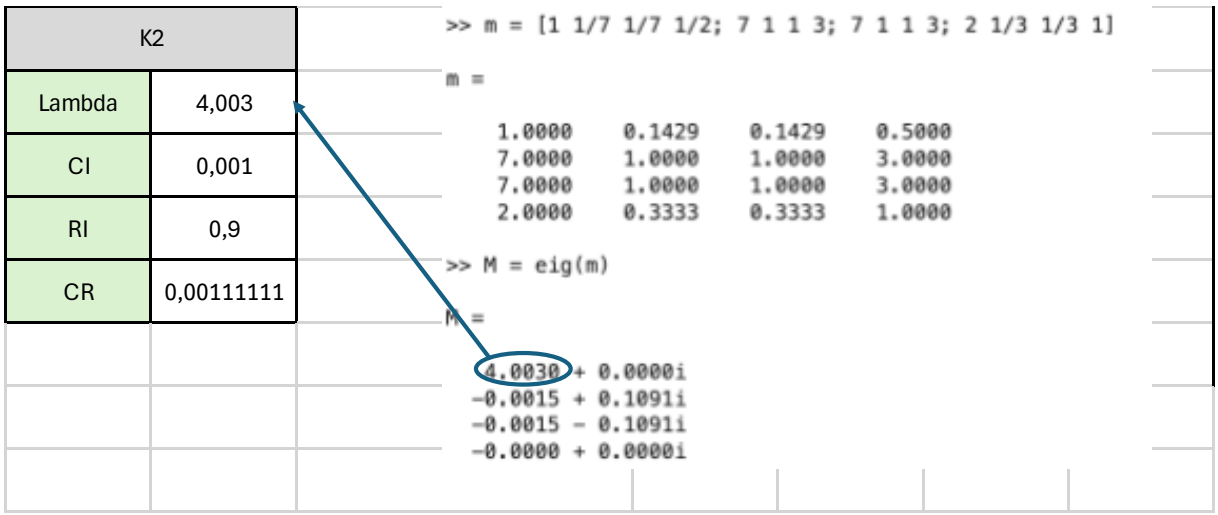

**Obrázek 12:** Ověření konzistence párového porovnávání variant dle k1

*Zdroj: vlastní zpracování*

| Výběr varianty | | | | | | |
|---|---|---|---|---|---|---|
| k2 | a1 | a2 | a3 | a4 | geometrický průměr | **h2j** |
| a1 | 1 | 1/7 | 1/7 | 1/2 | 0,31782897 | 0,06012874 |
| a2 | 7 | 1 | 1 | 3 | 2,14069514 | **0,40498917** |
| a3 | 7 | 1 | 1 | 3 | 2,14069514 | **0,40498917** |
| a4 | 2 | 1/3 | 1/3 | 1 | 0,68658905 | 0,12989291 |
| | | | | Suma: | 5,2858083 | 1 |

**Obrázek 13:** Obodování variant dle k2

*Zdroj: vlastní zpracování*




**Obrázek 14:** Ověření konzistence párového porovnávání variant dle k2

*Zdroj: vlastní zpracování*

| Výběr varianty | | | | | | |
|---|---|---|---|---|---|---|
| k3 | a1 | a2 | a3 | a4 | geometrický průměr | **h3J** |
| a1 | 1 | 1/3 | 1/5 | 2 | 0,60427508 | 0,10992058 |
| a2 | 3 | 1 | 1/2 | 5 | 1,65487546 | 0,30102991 |
| a3 | 5 | 2 | 1 | 7 | 2,89250761 | **0,5261612** |
| a4 | 1/2 | 1/5 | 1/7 | 1 | 0,34572078 | 0,06288829 |
| | | | | Suma: | 5,49737893 | 1 |

**Obrázek 15:** Obodování variant dle k3

*Zdroj: vlastní zpracování*

| K3 | |
|---|---|
| Lambda | 4,0201 |
| CI | 0,0067 |
| RI | 0,9 |
| CR | 0,00744444 |

```
>> m = [ 1 1/3 1/5 2; 3 1 1/2 5; 5 2 1 7; 1/2 1/5 1/7 1]

m =

    1.0000    0.3333    0.2000    2.0000
    3.0000    1.0000    0.5000    5.0000
    5.0000    2.0000    1.0000    7.0000
    0.5000    0.2000    0.1429    1.0000

>> M = eig(m)

M =

  4.0201 + 0.0000i
 -0.0132 + 0.0000i
 -0.0034 + 0.2841i
 -0.0034 - 0.2841i
```

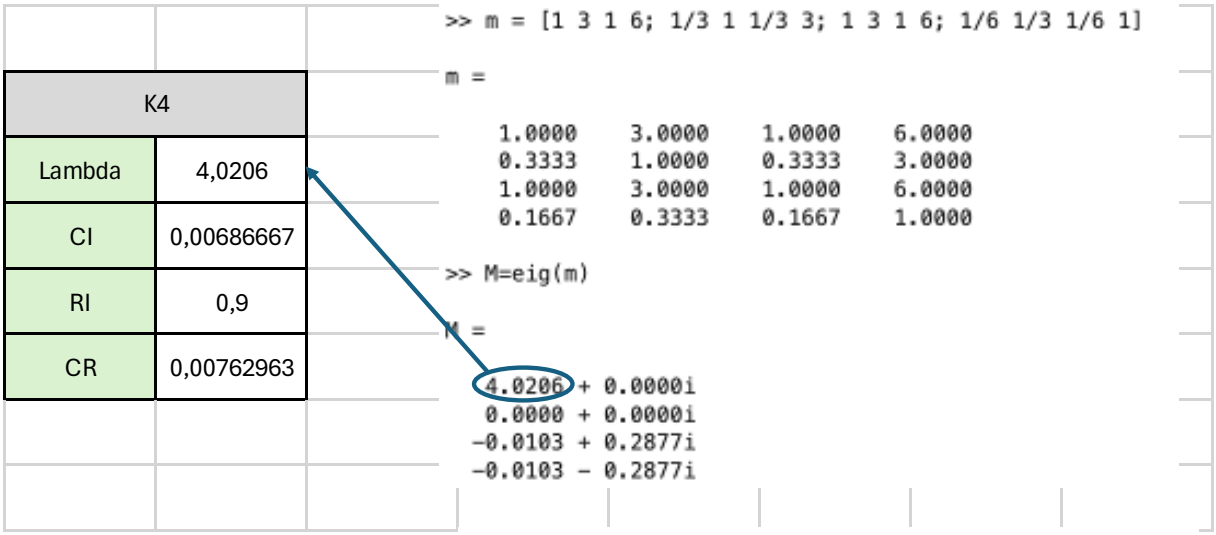
**Obrázek 16:** Ověření konzistence párového porovnávání variant dle k3

*Zdroj: vlastní zpracování*

| Výběr varianty | | | | | | |
|---|---|---|---|---|---|---|
| k4 | a1 | a2 | a3 | a4 | geometrický průměr | **h4j** |
| a1 | 1 | 3 | 1 | 6 | 2,05976714 | **0,39690504** |
| a2 | 1/3 | 1 | 1/3 | 3 | 0,75983569 | 0,14641588 |
| a3 | 1 | 3 | 1 | 6 | 2,05976714 | **0,39690504** |
| a4 | 1/6 | 1/3 | 1/6 | 1 | 0,31020162 | 0,05977403 |
| | | | | Suma: | 5,18957159 | 1 |

**Obrázek 17:** Obodování variant dle k4

*Zdroj: vlastní zpracování*



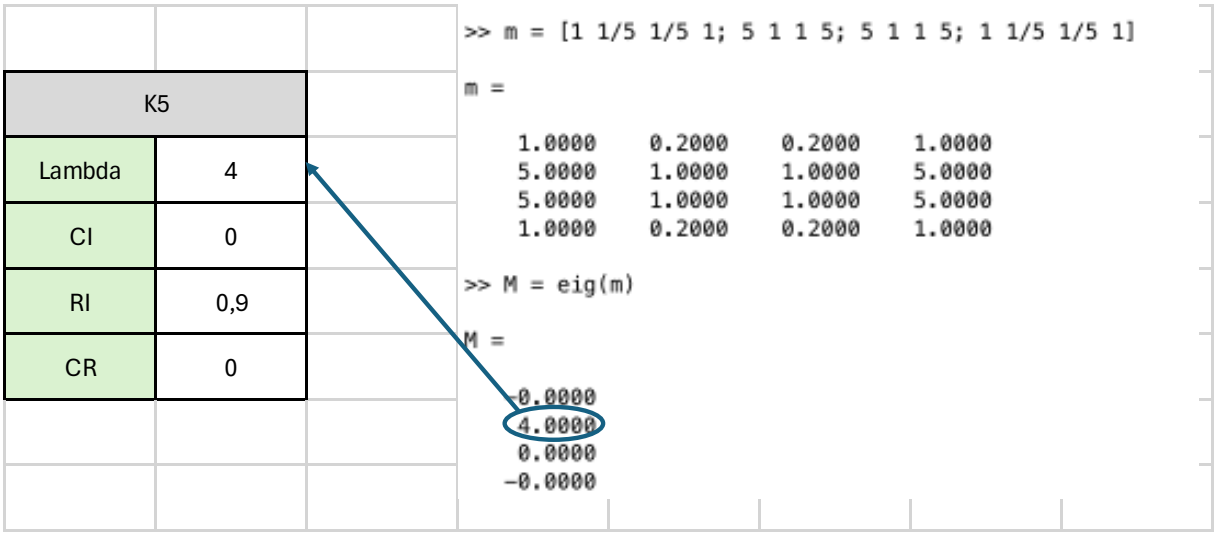

**Obrázek 18:** Ověření konzistence párového porovnávání variant dle k4

*Zdroj: vlastní zpracování*

| Výběr varianty | | | | | | |
|---|---|---|---|---|---|---|
| k5 | a1 | a2 | a3 | a4 | geometrický průměr | **h5j** |
| a1 | 1 | 1/5 | 1/5 | 1 | 0,4472136 | 0,08333333 |
| a2 | 5 | 1 | 1 | 5 | 2,23606798 | **0,41666667** |
| a3 | 5 | 1 | 1 | 5 | 2,23606798 | **0,41666667** |
| a4 | 1 | 1/5 | 1/5 | 1 | 0,4472136 | 0,08333333 |
| | | | | Suma: | 5,36656315 | 1 |

**Obrázek 19:** Obodování variant dle k5

*Zdroj: vlastní zpracování*




**Obrázek 20:** Ověření konzistence párového porovnávání variant dle k5

*Zdroj: vlastní zpracování*

| Výsledná normalizovaná váha variant | | | | | | | |
|---|---|---|---|---|---|---|---|
| | kritéria | k1 | k2 | k3 | k4 | k5 | **Suma vah** |
| varianty | a1 | 0,08018026 | 0,02899438 | 0,02935287 | 0,02566977 | 0,00302343 | 0,16722071 |
| | a2 | 0,00818336 | 0,19528786 | 0,08038615 | 0,00946942 | 0,01511714 | 0,30844393 |
| | a3 | 0,01376272 | 0,19528786 | 0,14050456 | 0,02566977 | 0,01511714 | **0,39034205** |
| | a4 | 0,04767547 | 0,06263503 | 0,01679351 | 0,00386588 | 0,00302343 | 0,13399331 |
| | | | | | | Suma: | 1 |

**Obrázek 21:** Výsledná normalizace vah jednotlivých variant

*Zdroj: vlastní zpracování*