Univerzita Pardubice

Fakulta ekonomicko-správní

Zabezpečení firmy pomocí biometrických systémů

Bakalářská práce

2025 Lukáš Kulhánek

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Lukáš Kulhánek**
Osobní číslo:	**E21792**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Zabezpečení firmy pomocí biometrických systémů**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je navrhnout řešení pro zabezpečení firmy pomocí biometrických systémů v několika variantách podle typu oblasti, kterou je potřeba zabezpečit.

Osnova:

- Identifikovat potřeby firmy a prostředí, ve kterém bude biometrický systém implementován.
- Provést výběr oblasti, kterou bude chtít firma zabezpečit.
- Navrhnout a vyhodnotit použití vhodných biometrických technologií.

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

Seznam doporučené literatury:

BROOKS, Charles J.; GROW, Christopher; CRAIG, Philip a SHORT, Donald. *Cybersecurity essentials*. Indianapolis, Indiana: Sybex, John Wiley, [2018]. ISBN 978-1-119-36239-5.
DRAHANSKÝ, Martin a ORSÁG, Filip. *Biometrie*. [Brno: M. Drahanský], 2011. ISBN 978-80-254-8979-6.
PORADA, Viktor. *Bezpečnostní vědy: úvod do teorie, metodologie a bezpečnostní terminologie*. 2. aktualizované a rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-903-4.
RAK, Roman; MATYÁŠ, Vašek a ŘÍHA, Zdeněk. *Biometrie a identita člověka ve forenzních a komerčních aplikacích. Profesional*. Praha: Grada, 2008. ISBN 978-80-247-2365-5.

Vedoucí bakalářské práce: **RNDr. Ing. Oldřich Horák, 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:

Práci s názvem Zabezpečení firmy pomocí biometrických systémů jsem 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., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, 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 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 6. 2025

Lukáš Kulhánek v. r.

Poděkování

Tímto bych velice rád poděkoval svému vedoucímu bakalářské práce, panu RNDr. Ing. Oldřichu Horákovi, Ph.D., za jeho odborné vedení, cenné rady, vstřícný přístup a věcné připomínky, které mi významně pomohly při zpracování této práce.

ANOTACE

Tato bakalářská práce se věnuje návrhu zabezpečení firemního prostředí prostřednictvím biometrických technologií. Cílem je vytvořit funkční a bezpečné řešení přístupu do vybraných prostor společnosti KulhFik s.r.o., které bude odpovídat jejím provozním potřebám a zároveň splňovat platné legislativní požadavky. Práce obsahuje přehled nejčastěji používaných biometrických systémů, jejich výhod, nevýhod a technologických možností, dále pak popis právních a etických aspektů využívání biometrických údajů. Následně je navržen konkrétní systém zabezpečení pro vybrané oblasti firmy, přičemž jednotlivé technologie byly porovnány na základě vícekriteriálního hodnocení. Závěrečná část se zabývá ekonomickým vyhodnocením návrhu a porovnáním s alternativní variantou. Výstupem je doporučené řešení, které může sloužit jako model pro obdobné implementace v malých a středně velkých firmách.

KLÍČOVÁ SLOVA

biometrie, zabezpečení, přístupové systémy, identifikace, otisky prstů, rozpoznání obličeje, GDPR, firemní bezpečnost

TITLE

Proposal for Company Security Using Biometric Systems

ANNOTATION

This bachelor's thesis focuses on designing a security system for a corporate environment using biometric technologies. The aim is to develop a functional and secure access control solution for selected areas of the company KulhFik s.r.o., tailored to its operational needs and in compliance with applicable legal regulations. The thesis provides an overview of commonly used biometric systems, their advantages, limitations, and technological capabilities, as well as legal and ethical considerations related to the processing of biometric data. A specific security solution is proposed for selected areas of the company, with technologies evaluated through multicriteria assessment. The final section includes an economic evaluation of the proposed system and a comparison with an alternative option. The outcome is a recommended solution that can serve as a model for similar implementations in small and medium-sized enterprises.

KEYWORDS

biometrics, security, access systems, identification, fingerprint recognition, facial recognition, GDPR, corporate security

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek

AI	Artificial Intelligence
GDPR	General Data Protection Regulation
NAS	Network Attached Storage
PIN	Personal Identification Number
RFID	Radio Frequency Identification
IoT	Internet of Things
GV-ASManager	Software společnosti GeoVision pro správu přístupových práv
GV-VMS	Video Management System společnosti GeoVision

Úvod

V dnešní době rychle se vyvíjejících technologií a rostoucích hrozeb v oblasti kybernetické i fyzické bezpečnosti je pro firmy nezbytné hledat inovativní způsoby, jak efektivně chránit svá data, zaměstnance a majetek. Tradiční přístupy k zabezpečení, jako jsou hesla, PIN kódy či přístupové karty, se sice stále používají, ale čelí narůstajícímu počtu bezpečnostních incidentů. Jsou snadno zneužitelné, mohou být zapomenuty, ztraceny nebo odcizeny, a jejich samotná existence často neodpovídá současným požadavkům na vysokou míru ochrany v kritických firemních oblastech.

V tomto kontextu se do popředí stále více dostávají biometrické systémy, které využívají unikátní fyziologické nebo behaviorální vlastnosti jednotlivce pro jeho identifikaci či autentizaci. Tyto technologie nabízejí nejen vyšší úroveň bezpečnosti, ale také větší komfort pro uživatele, neboť nevyžadují nošení fyzických identifikátorů ani zapamatování přístupových údajů.

Cílem této bakalářské práce je navrhnout komplexní a variantní řešení zabezpečení firemního prostředí pomocí biometrických technologií. Práce se zaměří na různé oblasti podnikového provozu – od kanceláří, přes serverovny až po citlivá datová úložiště – a pro každou z nich vyhodnotí vhodnost konkrétních biometrických metod. Dále se bude věnovat posouzení nákladovosti, přínosů a potenciálních rizik spojených s implementací těchto systémů.

Teoretická část práce poskytne přehled hlavních typů biometrických identifikačních metod, jejich výhod a nevýhod, dále legislativní a etické aspekty využívání biometrie v pracovním prostředí a dostupné technologie na trhu. Praktická část se bude věnovat konkrétnímu návrhu zabezpečení fiktivní společnosti – KulhFik s.r.o. – včetně identifikace zabezpečovaných oblastí, výběru odpovídajících technologií a vyhodnocení ekonomických aspektů dvou variant řešení. Výběr konkrétních technologií bude podpořen vícekriteriálním hodnocením, které umožní objektivně posoudit vhodnost dostupných alternativ z hlediska bezpečnosti, technické realizovatelnosti a finanční efektivity.

Závěrem práce bude zhodnoceno, do jaké míry se nasazení biometrických technologií vyplatí nejen z hlediska zvýšení bezpečnosti, ale také z pohledu dlouhodobé návratnosti investice a provozní udržitelnosti. Práce si klade za cíl poskytnout jak odborný přehled v oblasti biometrického zabezpečení, tak i praktický návod, jak tyto technologie efektivně implementovat v reálném firemním prostředí.

1 Základní pojmy a definice biometrických systémů

Biometrické systémy představují specifickou kategorii bezpečnostních technologií, které využívají fyzické nebo behaviorální charakteristiky jednotlivce pro jeho jednoznačnou identifikaci nebo autentizaci. Využití biometrie v oblasti zabezpečení je stále rozšířenější, a to zejména díky zvyšujícím se nárokům na ochranu dat, majetku a osob (Drahanský a Orság, 2011; Kolář, 2019).

Pod pojmem biometrie rozumíme vědní obor zabývající se měřením a statistickým vyhodnocováním biologických vlastností živých organismů, zejména lidí. V kontextu informačních a bezpečnostních technologií se biometrie zaměřuje především na unikátní rysy, které lze spolehlivě změřit, uložit a následně využít pro ověření totožnosti (Rak, Matyáš a Říha, 2008).

Biometrický systém je souhrn hardwarových a softwarových komponent, které provádějí sběr, zpracování, uchovávání a porovnávání biometrických dat s cílem identifikace nebo autentizace osoby. Typický biometrický systém obsahuje následující funkční bloky (Drahanský a Orság, 2011):

- **Snímač** (zachycení charakteristiky) – zařízení, které získává fyzická nebo behaviorální data (např. snímání otisku prstu, obrazu obličeje, záznam hlasu).
- **Předzpracování dat** – fáze, kdy se ze zachycených údajů odstraní šum a data se normalizují pro další zpracování a porovnání.
- **Vytvoření biometrické šablony** – výběr klíčových rysů a jejich uložení v databázi ve formě digitální reprezentace.
- **Porovnání a rozhodování** – proces porovnání aktuálně nasnímaných údajů s uloženými šablonami a rozhodnutí o shodě nebo neshodě.

Pojmy identifikace a autentizace v rámci biometrických systémů je třeba odlišovat:

- **Identifikace (1:N)** znamená, že systém porovnává biometrický vzorek s celou databází šablon a určuje, zda existuje shoda. Tento proces se běžně používá například při kontrole vstupů (Brooks et al., 2018).
- **Autentizace (1:1)** spočívá v ověření, zda biometrický vzorek odpovídá konkrétní, předem deklarované identitě, například po zadání ID čísla a následném ověření otisku prstu.

Biometrické údaje jsou podle právní úpravy (zejména Nařízení (EU) 2016/679) považovány za zvláštní kategorii osobních údajů, protože umožňují jednoznačnou identifikaci osoby. Z tohoto důvodu podléhají přísným pravidlům ochrany a jejich zpracování je vázáno na dodržování zásad minimalizace, zákonnosti a transparentnosti (Nařízení (EU) 2016/679). V praxi se biometrické systémy používají zejména v následujících oblastech (Drahanský a Orság, 2011; Kolář, 2019):

- **Zabezpečení fyzických vstupů** – kontrola vstupu do budov, kanceláří, skladů a dalších prostor,
- **Informační bezpečnost** – autentizace přístupu k informačním systémům a zařízením,
- **Docházkové systémy** – evidence příchodů a odchodů zaměstnanců,
- **Bankovní a finanční sektor** – ověřování identity klientů při přístupu k finančním službám,
- **Veřejná správa a zdravotnictví** – správa citlivých dat, autentizace pacientů.

Výhodou biometrických systémů oproti tradičním metodám, jako jsou hesla, čipové karty nebo PIN kódy, je vyšší bezpečnost založená na unikátních vlastnostech osoby, které nelze snadno zkopírovat nebo zapomenout. Na druhé straně biometrie přináší také specifická rizika, zejména v oblasti ochrany soukromí, protože v případě ztráty biometrického údaje jej nelze "změnit" jako běžné heslo (Rak, Matyáš a Říha, 2008).

1.1 Historický vývoj a současné trendy v biometrickém zabezpečení

Biometrie, jakožto metoda rozpoznávání jednotlivců na základě jejich biologických charakteristik, má své kořeny hluboko v historii lidstva. Přestože moderní technologie umožňují automatizované a sofistikované biometrické systémy teprve v posledních desetiletích, samotný princip využívání unikátních tělesných znaků pro identifikaci lidí sahá až do starověku (Rak, Matyáš a Říha, 2008; Drahanský a Orság, 2011).

První známé příklady využití biometrických prvků lze nalézt ve starověké Číně, kde si obchodníci uchovávali otisky prstů dlužníků na hliněných destičkách jako důkaz uzavřeného obchodu. V 19. století se otisky prstů začaly systematicky používat při policejní identifikaci. Průkopníkem v této oblasti byl britský antropolog Francis Galton, který vědecky prokázal, že otisky prstů jsou pro každého člověka jedinečné a neměnné (Drahanský a Orság, 2011).

Dalším významným krokem ve vývoji biometrie bylo zavedení tzv. bertillonáže, systému identifikace na základě měření fyzických parametrů těla, který vyvinul francouzský kriminalista Alphonse Bertillon. Ačkoli byl tento systém později nahrazen daktyloskopií (otisky prstů), položil důležité základy pro rozvoj moderních metod identifikace (Rak, Matyáš a Říha, 2008).

Rozvoj elektroniky, výpočetní techniky a digitálního zpracování obrazu v druhé polovině 20. století umožnil vznik prvních automatizovaných biometrických systémů. Tyto systémy byly původně vyvíjeny pro potřeby armády, tajných služeb a vládních institucí, zejména v oblasti kontroly přístupu a ověřování identity (Kolář, 2019).

Na přelomu 20. a 21. století zažila biometrie dynamický rozmach i v civilní sféře. Rozšíření internetu, růst kyberkriminality a zvyšující se důraz na bezpečnost osobních dat vedly k hledání spolehlivějších metod autentizace než tradiční hesla či přístupové karty. Výsledkem je široké uplatnění biometrických technologií v komerčním sektoru, zejména v bankovnictví, zdravotnictví, školství, cestovním ruchu a mobilních technologiích (Brooks et al., 2018; Kolář, 2019). Mezi nejvýznamnější současné trendy v oblasti biometrického zabezpečení patří:

- **Multimodální biometrie** – kombinace více biometrických charakteristik (například otisku prstu a rozpoznání obličeje) za účelem zvýšení spolehlivosti autentizace. Tento přístup je obzvláště výhodný v prostředích s vyššími nároky na bezpečnost, nebo tam, kde může dojít k omezení funkčnosti jednoho typu biometrie (Brooks et al., 2018).

- **Mobilní biometrie** – implementace biometrických technologií do chytrých telefonů a tabletů (např. Face ID, Touch ID) umožňuje pohodlné a rychlé ověřování identity, a tím posiluje uživatelský komfort i bezpečnost (Kolář, 2019).

- **Bezpečná vzdálená identifikace** – využití biometrie v online prostředí, například při ověřování identity klientů při uzavírání smluv na dálku. Tento trend zesílil zejména během pandemie COVID-19, kdy bylo nutné provádět autentizaci bez fyzického kontaktu.

- **Behaviorální biometrie** – sledování dynamiky chování uživatele, jako je rychlost psaní na klávesnici, styl pohybu kurzoru nebo používání dotykové obrazovky. Tato metoda umožňuje nepřetržitou identifikaci uživatele během jeho činnosti, a tím přispívá k vyšší úrovni bezpečnosti (Brooks et al., 2018).

- **Biometrie s umělou inteligencí (AI)** – využití strojového učení a neuronových sítí ke zlepšení přesnosti rozpoznávání a detekce podvodů. Umělá inteligence dokáže lépe

rozpoznávat vzory v datech, přizpůsobit se změnám a rozlišovat skutečné vstupy od pokusů o podvodné napodobení (Kolář, 2019; Brooks et al., 2018).

Kromě těchto trendů se v poslední době klade stále větší důraz na ochranu biometrických dat. Vzhledem k tomu, že biometrické údaje jsou unikátní a nezměnitelné, představuje jejich zneužití vážné riziko pro ochranu soukromí jednotlivců. Proto se vyvíjejí technologie umožňující například bezpečné ukládání biometrických šablon v zašifrované podobě nebo použití rozptýleného uložení dat (Kolář, 2019).

Biometrie se dnes stává nedílnou součástí moderní společnosti. Přestože přináší řadu výhod v oblasti bezpečnosti a uživatelského komfortu, je nezbytné, aby její nasazování bylo provázeno důslednou ochranou práv jednotlivců a respektováním etických zásad (Rak, Matyáš a Říha, 2008; Drahanský a Orság, 2011).

1.2 Typy biometrických systémů a jejich využití

Biometrické systémy lze dělit podle toho, jakou charakteristiku člověka využívají k jeho identifikaci nebo autentizaci. V praxi existuje několik hlavních kategorií biometrických metod, přičemž každá z nich má své specifické vlastnosti, výhody i omezení. Výběr vhodné biometrické metody závisí na konkrétním použití, požadované úrovni zabezpečení, komfortu uživatele i nákladech na implementaci (Drahanský a Orság, 2011; Kolář, 2019).

Tabulka 1 - Typy biometrických systémů.

Typ biometrického systému	Princip ověřování	Výhody	Nevýhody
Otisk prstu	Snímaní papilárních linií prstu	Vysoká přesnost, rychlé ověření, nízké náklady	Citlivost na poškození kůže, možnost falšování
Rozpoznání obličeje	Analýza rysů a proporcí obličeje	Bezdotykové ověření, rychlá autentizace	Citlivost na změny vzhledu, světelné podmínky
Snímání duhovky	Skenování vzoru duhovky infračerveným světlem	Extrémní přesnost, neměnnost vzoru	Vyšší náklady, vyšší nároky na snímání

Typ biometrického systému	Princip ověřování	Výhody	Nevýhody
Hlasová biometrie	Analýza hlasového otisku a řečových vlastností	Vhodné pro vzdálenou autentizaci, pohodlí	Hluk v prostředí, změny hlasu při nemoci
Dynamika podpisu	Analýza způsobu psaní (rychlost, tlak, pořadí tahů)	Přirozenost pro uživatele, nízké náklady	Variabilita podpisu podle psychického stavu
Behaviorální biometrie	Analýza způsobu používání zařízení (psaní, klikání)	Vhodné pro online ověřování, detekce podvodů	Vyšší technologická náročnost, potřeba velkého vzorku dat

Zdroj: vlastní zpracování na základě autorů (Drahanský a Orság, 2011) a (Kolář, 2019).

1.2.1 Otisk prstu

Snímání otisku prstu patří mezi nejstarší a nejrozšířenější biometrické metody. Každý člověk má jedinečný vzor papilárních linií na prstech, který se nemění v průběhu života. Otisky prstů se využívají nejen v kriminalistice, ale také pro zabezpečení přístupu k mobilním zařízením, budovám, serverovnám nebo informačním systémům (Rak, Matyáš a Říha, 2008).

Biometrické systémy založené na otiscích prstů obvykle fungují ve třech krocích: snímání otisku pomocí optického, kapacitního nebo ultrazvukového senzoru, vytvoření digitální šablony charakteristických rysů a porovnání aktuálního otisku se šablonou uloženou v databázi.

Výhody této metody zahrnují vysokou přesnost, rychlost zpracování a relativně nízké pořizovací náklady. Otisk prstu je snadno snímatelný a uživatelé jsou na tuto technologii dobře zvyklí, zejména díky jejímu rozšíření v mobilních zařízeních (Kolář, 2019; Brooks et al., 2018).

Nevýhodou může být snížená spolehlivost v případě poranění prstu, opotřebení pokožky nebo znečištění snímače. Některé typy senzorů mohou být citlivé na falešné otisky, což klade důraz na využití pokročilých technologií životní detekce, například detekce teploty nebo průtoku krve.

Otisky prstů se hojně využívají například v docházkových systémech, přístupových terminálech firem, v mobilních telefonech a stále častěji i v elektronickém bankovnictví.

1.2.2 Rozpoznání obličeje

Rozpoznání obličeje je biometrická metoda, která využívá jedinečné rysy lidského obličeje k ověření identity osoby. Systémy pro rozpoznávání obličeje analyzují a vyhodnocují charakteristické znaky, jako je vzdálenost mezi očima, tvar nosu, linie čelisti nebo obrys rtů (Kolář, 2019; Brooks et al., 2018).

Moderní systémy využívají pokročilé algoritmy strojového učení a neuronových sítí, které umožňují velmi přesné rozpoznávání i v měnících se světelných podmínkách, při změnách účesu, použití brýlí či při stárnutí uživatele. Technologie jako 3D rozpoznávání obličeje nebo infračervené snímání výrazně zvyšují odolnost systémů proti podvodům, například použitím fotografie.

Výhody rozpoznání obličeje zahrnují pohodlí pro uživatele (bezdotyková autentizace), rychlost ověření a snadnou integraci do kamerových systémů. Díky možnosti identifikace na dálku se tato technologie stává stále populárnější, zejména v přístupových systémech, mobilních zařízeních (například Apple Face ID) a bezpečnostních aplikacích.

Nevýhodou je vyšší citlivost na kvalitu nasnímání obrazu, změny vzhledu uživatele a možnost snížení přesnosti v extrémních světelných podmínkách. Také otázky ochrany soukromí jsou u rozpoznání obličeje obzvláště citlivé, zejména při hromadném sledování veřejných prostor (Drahanský a Orság, 2011).

Rozpoznání obličeje se dnes uplatňuje například na letištích, v bankovnictví, v přístupových systémech firem a při zabezpečení mobilních zařízení.

1.2.3 Duhovka a sítnice

Biometrická identifikace na základě oční duhovky a sítnice patří k nejspolehlivějším metodám ověřování identity. Obě části oka vykazují extrémně složité a jedinečné vzory, které jsou stabilní po celý život jednotlivce (Drahanský a Orság, 2011; Rak, Matyáš a Říha, 2008).

Skenování duhovky využívá analýzu vzorů barevných a strukturálních prvků v oblasti duhovky. Systém nasnímá obraz duhovky pomocí speciální kamery v blízkém infračerveném spektru a vytvoří digitální šablonu pro porovnání. Výhodou této metody je vysoká odolnost vůči vnějším změnám a mimořádná přesnost, kdy míra chybné identifikace bývá extrémně nízká (Kolář, 2019).

Skenování sítnice je metoda, která zkoumá unikátní vzor krevních cév na vnitřní straně oka. Tato technologie vyžaduje aktivní spolupráci uživatele, protože snímání probíhá pomocí laserového paprsku, který zmapuje strukturu sítnice.

Obě technologie se vyznačují vysokou úrovní zabezpečení, ale také vyššími náklady na zařízení a vyšší náročností na uživatele. Proto jsou systémy na bázi duhovky a sítnice využívány především v prostředích s vysokými bezpečnostními požadavky, jako jsou vojenské objekty, vládní úřady nebo špičková výzkumná pracoviště (Drahanský a Orság, 2011).

1.2.4 Hlasová biometrie

Hlasová biometrie identifikuje jednotlivce na základě jejich hlasového otisku. Každý člověk má unikátní kombinaci fyziologických a behaviorálních charakteristik, které ovlivňují vlastnosti jeho hlasu – například tvar hlasivek, dutin v nosohltanu, intonaci, rytmus řeči a artikulaci (Brooks et al., 2018).

V hlasových biometrických systémech je hlas uživatele nahrán, analyzován a převeden na digitální šablonu. Systém poté porovnává aktuální hlasový vzorek se šablonou uloženou v databázi.

Výhodou hlasové biometrie je možnost vzdáleného ověřování bez nutnosti specializovaného hardwaru. Díky tomu je hlasová biometrie využívána například v bankovnictví, call centrech a při zabezpečení přístupu k online službám (Kolář, 2019).

Nevýhodou je vyšší citlivost na vnější podmínky (hluk v pozadí, kvalita spojení) a možnost ovlivnění hlasu například nemocí nebo stárnutím. Bezpečnostní hrozbou je i možnost napodobení hlasu nebo použití syntetického hlasu, proto moderní systémy využívají doplňkové metody životní detekce (Brooks et al., 2018).

1.2.5 Dynamika podpisu a pohybu

Tato biometrická metoda sleduje nejen výsledný tvar podpisu, ale také dynamiku jeho provedení – například rychlost pohybu, tlak na podložku, pořadí jednotlivých tahů a časování (Drahanský a Orság, 2011).

Systémy pro ověřování dynamiky podpisu využívají speciální tablety nebo dotykové obrazovky schopné zaznamenávat jemné nuance pohybu při psaní.

Výhodou je přirozenost této formy ověřování pro uživatele, nízké náklady na zařízení a možnost integrace do běžných workflow. Nevýhodou je určitá variabilita podpisu v závislosti

na psychickém stavu, spěchu nebo změně návyků uživatele, což může ovlivnit přesnost ověření (Rak, Matyáš a Říha, 2008).

1.2.6 Kombinované multimodální systémy

Kombinované neboli multimodální biometrické systémy využívají více než jednu biometrickou charakteristiku současně, aby zvýšily spolehlivost identifikace a odolnost vůči podvodům (Kolář, 2019).

Typickým příkladem je kombinace otisku prstu a rozpoznání obličeje, případně rozpoznání duhovky a hlasové biometrie. Výhody multimodálních systémů zahrnují vyšší přesnost a spolehlivost ověření, snížení rizika falešného přijetí a falešného odmítnutí, a vyšší odolnost proti pokusům o napadení nebo obejití systému. Na druhé straně multimodální systémy vyžadují vyšší investice do technologií, složitější správu a často i větší spolupráci uživatele při ověřování.

Multimodální biometrické systémy nacházejí uplatnění v oblastech s vysokými bezpečnostními požadavky, jako jsou vládní agentury, letiště, finanční instituce a datová centra (Brooks et al., 2018; Kolář, 2019).

1.3 Výhody a nevýhody biometrických systémů ve firemním prostředí

Biometrické systémy představují moderní způsob autentizace, který se stále častěji využívá nejen ve veřejných institucích, ale i v soukromém sektoru. Jejich zavádění přináší řadu výhod, avšak také určitá rizika a omezení, která je třeba při implementaci pečlivě zvážit (Drahanský a Orság, 2011; Brooks et al., 2018).

1.3.1 Výhody biometrických systémů

Jedinečnost a spolehlivost

Biometrické charakteristiky, jako jsou otisky prstů, struktura duhovky nebo rozpoznání obličeje, jsou pro každého jedince unikátní a během života se téměř nemění. Tento faktor přispívá k vysoké spolehlivosti biometrických systémů při autentizaci uživatele (Rak, Matyáš a Říha, 2008). Významným příkladem využití této technologie je systém Face ID společnosti Apple, který prostřednictvím 3D skenování obličeje umožňuje bezpečnou autentizaci uživatelů chytrých telefonů (Brooks et al., 2018).

Obtížná podvrhnutelnost

Na rozdíl od tradičních metod, jako jsou hesla nebo čipové karty, jsou biometrické údaje pevně spojeny s konkrétní osobou, což výrazně ztěžuje jejich podvržení. Moderní autentizační systémy navíc využívají technologie životní detekce k ověření, že biometrický údaj pochází od živého subjektu. Bankovní aplikace, které umožňují přihlašování pomocí otisku prstu, jsou dnes standardem, přičemž životní detekce brání pokusům o podvodné přihlášení (Kolář, 2019).

Komfort a uživatelská přívětivost

Biometrická autentizace eliminuje nutnost pamatovat si složitá hesla nebo nosit fyzické identifikační prostředky. Ověření je rychlé, intuitivní a často probíhá bez vědomé akce uživatele. Například chytré telefony značek Samsung a Huawei umožňují odemykání zařízení pomocí otisku prstu nebo rozpoznání obličeje, čímž významně zvyšují komfort uživatelů (Drahanský a Orság, 2011).

Zvýšení bezpečnosti firemních procesů

Implementace biometrických technologií přináší výrazné zvýšení zabezpečení kritických prostor a citlivých dat. Vládní agentury a bezpečnostní složky standardně využívají biometrické systémy ke kontrole přístupu do vysoce chráněných zón (Kolář, 2019).

Možnost integrace s dalšími systémy

Moderní biometrické systémy lze snadno propojit s docházkovými, přístupovými i informačními systémy správy identit (IAM). V logistických a výrobních firmách je běžné, že biometrická autentizace je integrována s evidencí pracovní doby, což snižuje riziko neoprávněných manipulací (Brooks et al., 2018).

1.3.2 Nevýhody biometrických systémů

Riziko zneužití biometrických dat

Biometrické údaje jsou považovány za zvláštní kategorii osobních údajů, jejichž únik nebo zneužití může mít vážné následky, neboť je nelze změnit jako běžné heslo (Rak, Matyáš a Říha, 2008). Příkladem je incident z roku 2015, kdy došlo k úniku biometrických údajů milionů zaměstnanců amerického Úřadu pro správu personálních záležitostí (Brooks et al., 2018).

Legislativní a etické otázky

Použití biometrie podléhá přísné legislativě, zejména obecnému nařízení GDPR, které omezuje zpracování biometrických údajů bez prokazatelné nezbytnosti. Evropská unie například zpřísnila pravidla pro využívání biometrie na pracovišti, což komplikuje některé implementace v komerčním sektoru (Nařízení (EU) 2016/679; Porada, 2022).

Náklady na implementaci a správu

Implementace biometrických systémů představuje významnou investici nejen na pořízení zařízení, ale také na instalaci, integraci, školení personálu a pravidelnou údržbu. Příkladem nákladné realizace je nasazení systémů rozpoznávání obličeje na mezinárodních letištích, kde byly nutné rozsáhlé modernizace (Kolář, 2019).

Technologická omezení

Výkon biometrických systémů může být ovlivněn vnějšími faktory, jako jsou světelné podmínky, fyzické změny uživatele nebo zdravotní stav. Například uživatelé Face ID hlásili sníženou funkčnost autentizace v zimním období při nošení šál či roušek (Brooks et al., 2018).

Akceptace uživatelů

Zavedení biometrie může vyvolávat u zaměstnanců obavy o soukromí a vést k odporu vůči novým opatřením. V některých call centrech v USA byla například implementace hlasové biometrie odmítnuta zaměstnanci právě z těchto důvodů (Drahanský a Orság, 2011).

1.3.3 Rizika při implementaci biometrických systémů

Všechny tyto faktory mohou negativně ovlivnit efektivitu biometrického zabezpečení a způsobit problémy v jeho praktickém nasazení. Při zavádění biometrických technologií je nutné pečlivě zvažovat následující rizika (Kolář, 2019; Rak, Matyáš a Říha, 2008):

- Nedostatečné zabezpečení databází biometrických údajů,
- Chyby v konfiguraci systémů,
- Omezené testování v reálných podmínkách,
- Nedostatečné proškolení zaměstnanců,
- Rychlé technologické zastarávání.

1.4 Právní a etické aspekty využívání biometrie

Zpracování biometrických údajů představuje specifickou oblast práva a etiky, která je charakteristická vysokými nároky na ochranu osobních údajů a respektování soukromí jednotlivce. Biometrie jako nástroj identifikace a autentizace je v moderní společnosti na vzestupu, což s sebou přináší řadu právních i etických výzev (Drahanský a Orság, 2011; Porada, 2022).

1.4.1 Definice biometrických údajů

Podle Nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR) jsou biometrické údaje zařazeny mezi zvláštní kategorie osobních údajů. Článek 4 odstavec 14 GDPR definuje biometrické údaje jako osobní údaje vzniklé specifickým technickým zpracováním fyzických, fyziologických nebo behaviorálních charakteristik osoby, umožňujících její jednoznačnou identifikaci (Nařízení (EU) 2016/679).

Patří sem například otisky prstů, rozpoznání obličeje, sken duhovky, hlasový otisk nebo dynamika podpisu (Rak, Matyáš a Říha, 2008).

Tato data jsou specifická svou nezměnitelností a trvalostí, což klade mimořádné nároky na jejich ochranu. Únik biometrických údajů může mít vážnější důsledky než ztráta běžných osobních údajů, protože biometrické znaky nelze změnit jako heslo či PIN (Brooks et al., 2018).

1.4.2 Právní zásady zpracování biometrických údajů

Zpracování biometrických údajů musí respektovat základní zásady stanovené GDPR, konkrétně zásadu zákonnosti, korektnosti a transparentnosti, podle které musí být subjekt údajů informován o účelu a způsobu zpracování jeho údajů. Dále je nutné dodržet zásadu účelového omezení, tedy shromažďovat biometrické údaje pouze pro konkrétní a legitimní účely, a zásadu minimalizace údajů, tedy sbírat pouze údaje nezbytné pro daný účel (Nařízení (EU) 2016/679).

Údaje musejí být přesné a aktuální v souladu se zásadou přesnosti a musí být uchovávány pouze po nezbytně nutnou dobu. Je třeba zavést vhodná technická a organizační opatření, která zajistí ochranu biometrických údajů v souladu se zásadou integrity a důvěrnosti (Porada, 2022). V českém právním prostředí tato pravidla dále rozvádí zákon č. 110/2019 Sb., o zpracování osobních údajů.

1.4.3 Význam souhlasu subjektu údajů

Jedním z klíčových právních základů umožňujících zpracování biometrických údajů je výslovný souhlas subjektu údajů. Tento souhlas musí být informovaný, svobodný, konkrétní

a jednoznačný (Formánková, 2021). Subjekt údajů musí být plně obeznámen se způsobem a účelem zpracování svých údajů a musí mít možnost svobodného rozhodnutí.

V pracovněprávních vztazích je otázka dobrovolnosti souhlasu problematická, neboť vztah mezi zaměstnavatelem a zaměstnancem je z podstaty věci nerovný. Proto je doporučeno, aby zaměstnavatelé upřednostnili jiné právní tituly zpracování biometrických údajů, například ochranu oprávněného zájmu na zabezpečení majetku nebo ochranu životně důležitých zájmů jiných osob (Porada, 2022).

1.4.4 Etické aspekty využívání biometrie

Vedle právních povinností musí být využívání biometrických systémů v souladu s etickými principy ochrany soukromí a osobní integrity. Zásadní je respektování soukromí jednotlivce, což znamená minimalizaci rozsahu sbíraných údajů a zajištění jejich ochrany proti zneužití (Kovařík, 2020).

Biometrické technologie by měly být navrhovány s ohledem na principy "privacy by design" a "privacy by default", tedy ochranu soukromí již při návrhu systému a jako výchozí nastavení. Dále je důležité zajistit dobrovolnost účasti na biometrických systémech a nabídnout alternativu k biometrickému ověřování. Transparentnost zpracování údajů a prevence diskriminace určitých skupin obyvatelstva, například osob se zdravotním postižením, jsou dalšími klíčovými etickými požadavky (Formánková, 2021).

1.4.5 Výzvy a budoucí trendy v oblasti práva a etiky biometrie

S rostoucím využíváním biometrie se očekává zpřísňování právních rámců. Evropská unie připravuje například Zákon o umělé inteligenci (AI Act), který upravuje podmínky pro využívání biometrického rozpoznávání v reálném čase ve veřejném prostoru (Porada, 2022).

V budoucnu se předpokládá posílení práv subjektů údajů, včetně práva na přístup k biometrickým údajům, jejich přenositelnosti a práva být zapomenut. Etické aspekty budou klást důraz na větší informovanost, respektování soukromí a zajištění rovného přístupu všech uživatelů k biometrickým technologiím (Kovařík, 2020).

2 Přehled současných technologií a jejich dostupnost

Vývoj biometrických technologií v posledních desetiletích významně ovlivnil způsob, jakým organizace zabezpečují přístup ke svým systémům, prostorám a citlivým datům. Biometrické systémy dnes nabízejí vysokou míru bezpečnosti, pohodlí a efektivity. Jejich dostupnost se rozšiřuje nejen ve státní správě a v sektoru kritické infrastruktury, ale také v běžném podnikatelském prostředí (Drahanský a Orság, 2011; Brooks et al., 2018).

V této kapitole jsou představeny hlavní typy biometrických technologií, jejich přednosti, omezení a dostupnost na trhu.

2.1 Technologie otisků prstů

Systémy pro snímání otisků prstů patří k nejstarším a zároveň nejrozšířenějším biometrickým metodám. Moderní zařízení využívají optické, kapacitní nebo ultrazvukové senzory. Optické senzory jsou levnější, kapacitní nabízejí vyšší odolnost proti falšování a ultrazvukové poskytují nejlepší spolehlivost i v náročných podmínkách (Rak, Matyáš a Říha, 2008).

Technologie snímání otisků je dnes běžně dostupná v mobilních telefonech, kancelářských přístupových systémech i docházkových evidencích. Výrobci jako Suprema, ZKTeco, Futronic nebo HID Global nabízejí široké portfolio produktů od základních zařízení po sofistikované systémy s možností integrace.

Pro malé a střední firmy představují systémy snímání otisků cenově dostupnou cestu k zavedení biometrického zabezpečení. Výhodou této technologie je rychlost ověření a nízká chybovost při správné implementaci. Nevýhodou může být snížená funkčnost v případě poškození kůže, znečištění snímače nebo extrémních povětrnostních podmínek.

2.2 Technologie rozpoznání obličeje

Rozpoznávání obličeje patří mezi nejdynamičtěji se rozvíjející oblasti biometrie. Systémy využívají buď analýzu dvourozměrného obrazu, nebo pokročilé 3D skenování, které poskytuje vyšší přesnost a odolnost vůči pokusům o podvod.

Významnou výhodou této technologie je bezkontaktní ověřování, což zvyšuje hygienu a uživatelský komfort. Moderní systémy dokážou rozpoznat osobu i při částečném zakrytí obličeje či při změnách vzhledu (Drahanský a Orság, 2011).

Hlavními výrobci v této oblasti jsou GeoVision, IDEMIA, VisionLabs a NEC Corporation. Například zařízení GV-FR2020 od společnosti GeoVision kombinuje vysokou přesnost, rychlost ověření a možnost integrace do přístupových systémů. Cenově se technologie rozpoznávání obličeje pohybuje od vyšších jednotek tisíc korun za základní modely až po desítky tisíc korun za pokročilá řešení.

2.3 Technologie snímání duhovky a sítnice

Snímání duhovky a sítnice představuje vrchol biometrického zabezpečení díky extrémní spolehlivosti a obtížnosti podvrhnutí. Technologie využívá infračervené záření ke zmapování vzoru duhovky, respektive krevních cév sítnice (Rak, Matyáš a Říha, 2008).

Významní výrobci v této oblasti zahrnují společnosti Iris ID, IriTech a Princeton Identity. Tato technologie nachází uplatnění v prostředích s extrémními požadavky na bezpečnost, jako jsou vládní instituce, datová centra či bankovní sektor. Hlavní nevýhodou je vysoká cena zařízení a náročnější provozní podmínky, což omezuje její běžné firemní nasazení.

2.4 Hlasová biometrie a behaviorální biometrie

Hlasová biometrie umožňuje identifikaci jednotlivce na základě unikátních akustických vlastností jeho hlasu. Výhodou je možnost vzdáleného ověřování bez nutnosti specializovaného hardwaru (Kovařík, 2020).

Významnými hráči v této oblasti jsou například Nuance Communications a Pindrop. Hlasová biometrie se hojně využívá ve finančních službách a call centrech.

Behaviorální biometrie analyzuje dynamiku uživatelova chování, například styl psaní na klávesnici, pohyb kurzoru či tlak při dotyku obrazovky. Tyto technologie posilují bezpečnost při online autentizaci a kybernetické bezpečnosti. Nasazení těchto technologií je zatím omezené převážně na specifické případy a pilotní projekty.

Tabulka 2 - Přehled hlavních výrobců biometrických technologií.

Výrobce	Zaměření	Typ produktů	Příklady použití
GeoVision	Rozpoznávání obličeje	Terminály přístupu, kamery	Kontrola vstupu ve firmách, školách
Suprema	Otisky prstů, multimodální systémy	Přístupové terminály, docházkové systémy	Firemní zabezpečení, evidence docházky
IDEMIA	Multimodální biometrie	Rozpoznávání obličeje, otisků, duhovky	Letiště, státní správa, banky
ZKTeco	Otisky prstů, rozpoznání obličeje	Docházkové terminály, čtečky	Malé a střední podniky
Iris ID	Snímání duhovky	Skenery duhovky	Kritická infrastruktura, vysoká bezpečnost
VisionLabs	Rozpoznávání obličeje	Softwarová řešení pro videoanalýzu	Městský dohled, retail

Zdroj: vlastní zpracování na základě webových stránek výrobců (GeoVision, Suprema, IDEMIA, ZKTeco, Iris ID, VisionLabs).

2.5 Dostupnost biometrických technologií pro firemní použití

Díky poklesu cen a technologickému pokroku se biometrické technologie rozšířily i mezi malé a střední podniky. Firmy mohou vybírat z širokého spektra zařízení – od jednoduchých čteček otisků prstů přes terminály pro rozpoznávání obličeje až po komplexní multimodální systémy.

Například produkty společnosti GeoVision nabízejí cenově dostupné a modulární řešení pro firmy, které potřebují zajistit kontrolu přístupu, evidenci docházky i ochranu citlivých dat. Při výběru biometrického řešení je třeba kromě ceny zohlednit také uživatelský komfort, rychlost ověření, kompatibilitu se stávajícími systémy a podporu bezpečnostních standardů.

2.6 Kybernetická bezpečnost biometrických systémů

Biometrické systémy jsou stále více využívány jako spolehlivý způsob autentizace osob díky své schopnosti identifikovat jedince na základě unikátních fyziologických či behaviorálních charakteristik. Nicméně, jejich rostoucí nasazení zároveň přináší i nové kybernetické hrozby a rizika, která mohou ohrozit nejen samotnou funkčnost systému, ale především ochranu citlivých biometrických dat. Tato data jsou navíc specifická tím, že jsou neměnná a neopravitelná – pokud jednou dojde k jejich kompromitaci, nelze je jednoduše změnit, jako například heslo či PIN.

2.6.1 Typy kybernetických hrozeb

Mezi nejčastější hrozby patří **spoofing** – pokus o podvržení falešných biometrických vzorků, kterými může být například umělý otisk prstu, fotografie nebo nahrávka hlasu. Tento typ útoku využívá slabiny v procesu snímání biometrických dat a snaží se oklamat systém, aby vydal přístup neoprávněné osobě (Galbally et al., 2014).

Dalším nebezpečím jsou **replay útoky**, kdy útočník zachytí autentizační data během přenosu mezi snímačem a serverem a následně je znovu použije ke získání přístupu. Takové útoky mohou být účinné zejména v systémech bez dostatečného šifrování komunikace.

Velkým rizikem je také **útok na datové úložiště** biometrických údajů, kde jsou tato data centralizovaně uchovávána. Únik biometrických dat ze serverů znamená trvalé ohrožení osobní identity uživatelů, protože biometrické údaje nelze změnit, na rozdíl od tradičních autentizačních prostředků (Ratha et al., 2007).

Dále nelze opomenout ani útoky na hardware a software biometrických systémů, včetně zneužití chyb v softwarových modulech nebo fyzické manipulace s hardwarem, což může vést k obejití bezpečnostních kontrol nebo narušení dostupnosti systému.

2.6.2 Ochranná opatření

Aby bylo možné tato rizika minimalizovat, je nutné implementovat různá bezpečnostní opatření. Jedním z nejúčinnějších je vícefaktorová autentizace (MFA), která kombinuje biometrická data s dalšími ověřovacími prvky, například PIN kódem nebo bezpečnostním tokenem. Takový přístup významně snižuje riziko úspěšného průniku (O'Gorman, 2003).

Důležitou součástí ochrany je také šifrování biometrických dat při jejich přenosu i uložení. Moderní kryptografické metody zajišťují, že zachycená data nejsou pro útočníka čitelná a nelze je jednoduše zneužít (Uludag et al., 2004).

Další technikou je detekce živosti (liveness detection), která zjišťuje, zda vzorek skutečně pochází od živé osoby. To výrazně omezuje možnosti spoofingu, protože systém dokáže rozpoznat například, že před snímačem není pouze fotografie nebo model umělého otisku (Galbally et al., 2014).

Nesmí být opomenuty ani pravidelné bezpečnostní audity a aktualizace softwaru, které pomáhají odhalit a odstranit potenciální zranitelnosti ještě před tím, než je útočníci mohou využít.

2.6.3 Příklady kybernetických incidentů

V České republice dochází stále častěji k různým kybernetickým incidentům, které ovlivňují i oblasti bezpečnostních a biometrických systémů. Přestože konkrétní útoky přímo na biometrické technologie nejsou veřejně často zveřejňovány kvůli citlivosti těchto dat, existují relevantní příklady útoků na přístupové a identifikační systémy ve firmách i veřejném sektoru.

Například v roce 2022 došlo k útoku na jednoho z významných českých poskytovatelů IT služeb, který spravoval zabezpečení přístupových systémů pro několik klientů. Útočníci využili zranitelnosti v softwaru, což vedlo k dočasnému narušení funkčnosti přístupových karet a částečné expozici dat o zaměstnancích (Český bezpečnostní portál, 2022).

Dalším příkladem je incident z roku 2023, kdy byla odhalena snaha o phishingový útok zaměřený na zaměstnance velké průmyslové firmy s využitím sociálního inženýrství. Útočníci se pokusili získat přístupové údaje k systému biometrické autentizace prostřednictvím podvržených e-mailů (Národní centrum kybernetické bezpečnosti, 2023).

2.7 Budoucí trendy a inovace v biometrických systémech

Biometrické technologie dnes procházejí bouřlivým vývojem, který určuje nejen technický pokrok, ale i rostoucí nároky na ochranu soukromí, kybernetickou bezpečnost a efektivní autentizaci uživatelů v reálném čase. Kombinace s umělou inteligencí, rozšiřování behaviorálních metod nebo zavádění blockchainu do správy dat ukazují směr, kterým se zabezpečení identity posouvá. Biometrie se tak stává klíčovou součástí bezpečnostní infrastruktury nejen ve

firmách, ale i ve veřejné správě, zdravotnictví, dopravě a běžném životě (Kolář, 2019; Jain et al., 2020).

2.7.1 Umělá inteligence a strojové učení

Integrace AI do biometrie patří k nejzásadnějším technologickým posunům posledního desetiletí. Dříve používané algoritmy založené na pevných pravidlech jsou dnes nahrazovány hlubokými neuronovými sítěmi schopnými „učit se“ a v čase se zlepšovat. Výsledkem je dramaticky vyšší přesnost rozpoznávání tváře, hlasu nebo otisků. Zatímco tradiční systémy se potýkaly s problémy u různých typů pleti, nasvícení nebo změn vzhledu (vousy, make-up, stárnutí), AI modely tyto proměny zvládají s větší robustností.

Strojové učení se uplatňuje i při detekci spoofingu – tedy podvodných pokusů o přihlášení pomocí napodobeniny biometrického znaku. Například deepfake videa nebo fotografie obličeje byly dříve pro některé systémy překážkou. Dnes již moderní systémy s využitím tzv. "liveness detection" dovedou analyzovat mikroexprese, teplotní rozložení obličeje nebo sledovat pohyb zorniček, což zvyšuje jejich odolnost proti útokům (Wang et al., 2021).

V České republice se této problematice věnuje například tým Fakulty informačních technologií VUT v Brně, který vyvíjí vlastní řešení rozpoznávání obličeje s využitím neuronových sítí. Tyto modely dokážou klasifikovat uživatele s vysokou přesností i za ztížených světelných podmínek nebo v pohybu, což je klíčové například pro bezpečnostní kamery na letištích nebo v metru (Drahanský a Orság, 2011).

2.7.2 Biometrie založená na behaviorálních vzorcích

Vedle fyziologických znaků jako jsou otisky prstů nebo tvar duhovky získávají stále větší popularitu tzv. behaviorální biometrie. Tyto technologie analyzují chování uživatele – například jeho způsob psaní na klávesnici (tzv. „keystroke dynamics“), držení mobilního zařízení, rytmus kroků či vzory pohybu myši.

Výhodou behaviorální biometrie je její nenápadnost – uživatel není nucen se nijak aktivně identifikovat, systém jej rozpoznává „na pozadí“ během běžného používání zařízení. Díky tomu lze detekovat i okamžiky, kdy se zařízení zmocní neoprávněná osoba – například v bankovní aplikaci může systém odhalit, že dotyčný drží telefon jinak nebo jinak gestikuluje. Tyto technologie nacházejí využití zejména v oblasti mobilního bankovnictví a tzv. „zero-trust“ architektur, kdy se neustále ověřuje, kdo se systémem pracuje (Jain et al., 2020; Kovář, 2020).

České banky jako Česká spořitelna nebo Air Bank už experimentují s behaviorálními profily v kombinaci s geolokací a mobilními daty pro detekci podezřelých transakcí, čímž se posouvají směrem k prediktivní bezpečnosti.

2.7.3 Blockchain a bezpečné uchovávání biometrických údajů

S rostoucím důrazem na ochranu osobních údajů a s nástupem GDPR se objevila nová výzva – kde a jak bezpečně ukládat biometrická data, která jsou považována za citlivá. V tomto ohledu se jako perspektivní technologie ukazuje blockchain, tedy decentralizovaná databáze záznamů, která je prakticky nemožná zfalšovat.

Přestože není vhodné ukládat samotná biometrická data přímo do blockchainu (např. z důvodu velikosti a práva na výmaz), existují přístupy, kdy se do blockchainu ukládá pouze hash (otisk) biometrického šablonu. To umožňuje ověření integrity údajů, aniž by došlo ke kompromitaci jejich obsahu. Systémy tohoto typu by mohly najít uplatnění například v digitálních občankách, očkovacích pasech či hlasovacích systémech (Ryan, 2020; Porada, 2022).

2.7.4 Biometrie pro internet věcí (IoT)

Internet věcí (IoT) přináší obrovský počet zařízení připojených k síti – od chytrých zámků, přes termostaty, až po zdravotnické přístroje. Každé z těchto zařízení může být potenciálním vstupním bodem pro kybernetický útok, a biometrická autentizace se tak jeví jako logický krok ke zvýšení jejich bezpečnosti.

Hlavní výzvou je však výpočetní a energetická náročnost klasických biometrických algoritmů, kterou drobná zařízení často nezvládají. V reakci na to vznikají optimalizované algoritmy s nízkými nároky, případně řešení založená na přenesení výpočtu na cloud. Zajímavý příklad představují chytré dveřní zámky dostupné i na českém trhu – například Nuki nebo Danalock, které umožňují odemykání pomocí otisků prstů nebo mobilního rozpoznání obličeje. Jejich popularita roste zejména v rezidenčním sektoru (Rak et al., 2008; Alza.cz, 2024).

2.7.5 Český výzkum a aplikace biometrických inovací

Také v České republice se biometrickému výzkumu věnuje několik institucí. Vedle zmíněného VUT v Brně je to například Fakulta elektrotechnická ČVUT, kde probíhá výzkum v oblasti zpracování obrazu a bezpečnostních aplikací. Česká asociace pro biometriku (CAB) pravidelně organizuje odborné konference a podporuje propojení výzkumu s praxí.

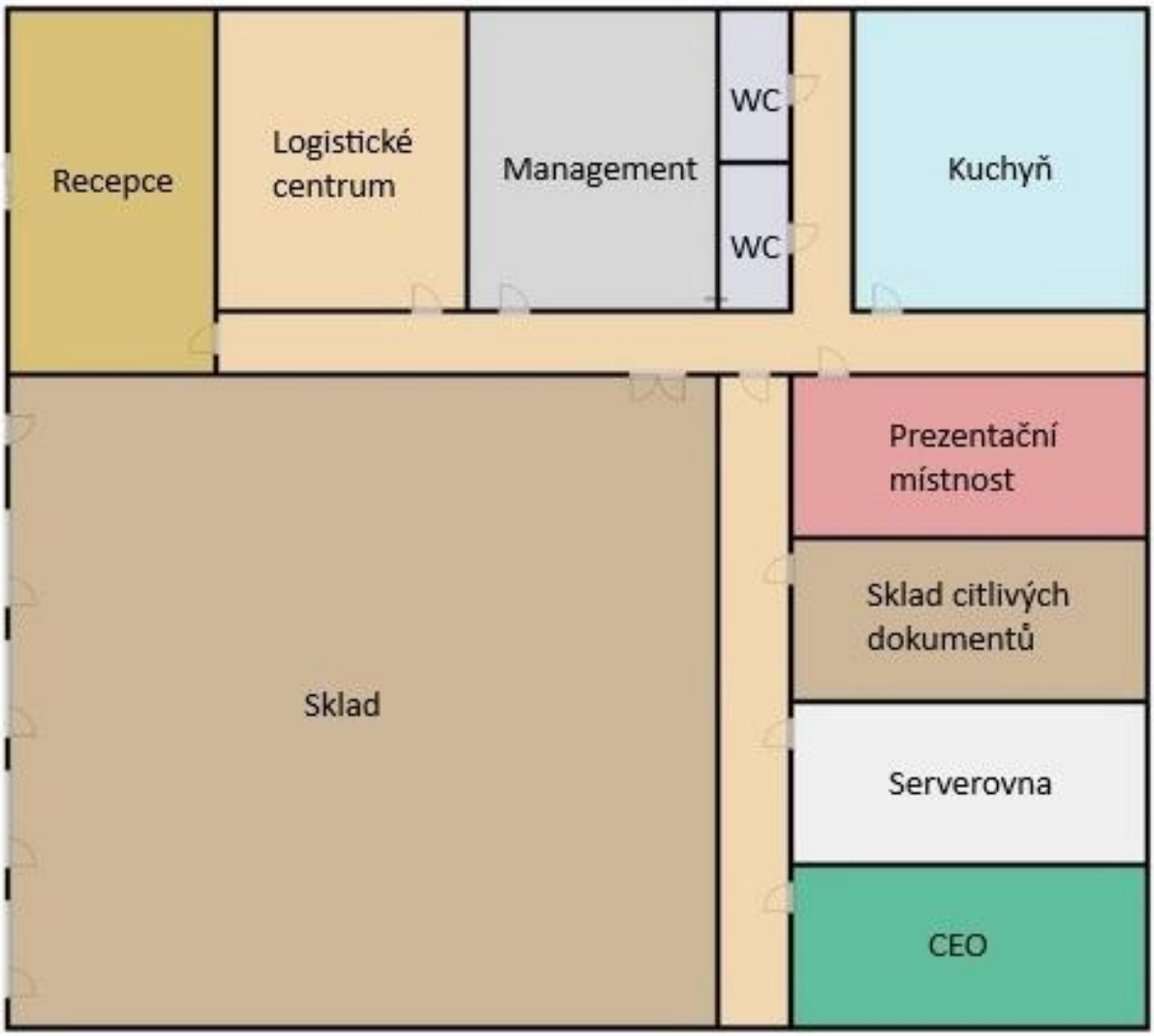
V komerčním sektoru se inovacím věnují firmy jako Kamartech, CED Systems nebo Zebra Systems. Tyto společnosti implementují pokročilé přístupové systémy kombinující otisky, rozpoznání obličeje i čipové karty do bank, nemocnic a státních institucí. V poslední době je patrný posun i k řešením určeným pro malé a střední firmy, kde je kladen důraz na poměr cena–výkon a snadnou správu (Drahanský a Orság, 2011; Kamartech.cz, 2024).

3 Popis zabezpečované firmy a její infrastruktury

V práci je použita smyšlená firma s názvem KulhFik s.r.o. Je postavena jako modelová společnost, která funguje v oblasti logistiky. Mezi hlavní činnosti patří skladování, balení zboží a jeho odesílání. Celkově má zhruba čtyřiceti zaměstnanců.

Nejvíc zaměstnanců pracuje ve skladu a na expedici. Ostatní dělají administrativu nebo vedou jednotlivé úseky. KulhFik s.r.o. spolupracuje hlavně s e-shopy, takže běžně přichází do kontaktu s osobními údaji zákazníků. Kvůli tomu je důležité, aby byly dobře zajištěné nejen prostory, ale taky data (Tichý, 2018; Novotný, 2020).

3.1 Prostory a jejich využití



Obrázek 1 - Schéma firmy.

Zdroj: vlastní zpracování v programu Floorplanner.

KulhFik s.r.o. sídlí v přízemní budově, kde má každý prostor své konkrétní využití. Díky tomu může firma fungovat bez zbytečného zdržení, což pomáhá plynulému chodu organizaci v každodenním provozu. Přesný půdorys objektu je součástí příloh této práce. Mezi hlavní části budovy patří:

- **Recepce** – vstup, kde se evidují návštěvy i pohyb zaměstnanců.
- **Skladová hala** – hlavní provozní prostor, kde dochází k manipulaci se zbožím.
- **Logistické centrum** – prostor, ve kterém se organizují zakázky a expedice.
- **Kanceláře vedení** – osoby, které zajišťují správné fungování společnosti
- **Kancelář ředitele (CEO)** – samostatná místnost určená pro vedení společnosti.
- **Serverovna** – technická místnost s uloženou IT infrastrukturou, servery a zálohovacím vybavením.
- **Archiv dokumentů** – místo, kde se uchovávají citlivé písemnosti, smlouvy nebo faktury.
- **Zasedací místnost** – slouží k poradám, školením nebo obchodním jednáním.
- **Kuchyňka** – prostor pro zaměstnance, využívaný při přestávkách.

Identifikace klíčových oblastí k zabezpečení

Na základě provozních potřeb a charakteru firemní infrastruktury byly identifikovány následující prostory jako klíčové z hlediska bezpečnosti:

Tabulka 3 - Přehled klíčových prostor a doporučeného zabezpečení.

Prostor	Typ rizika	Doporučené zabezpečení
Serverovna	Neoprávněný přístup, poškození dat, kybernetický útok	Vysoká úroveň – biometrie + PIN + kamera
Sklad dokumentů	Únik dat, ztráta dokumentů, vnitřní hrozba	Biometrie – otisk prstu nebo duhovka
Recepce / vstup	Vstup neoprávněných osob, sociální inženýrství	Obličejová biometrie + evidence vstupu
Kancelář CEO	Strategická data, důvěrné informace	Dvoufaktorová autentizace, biometrie

Prostor	Typ rizika	Doporučené zabezpečení
Sklad	Ztráta zboží, neoprávněná manipulace	Karty + biometrický záznam přístupů
Prezentační místnost	Pohyb návštěvníků, ochrana důvěrných dat	Časově omezený přístup, dohled kamerou
Serverovna	Neoprávněný přístup, poškození dat, kybernetický útok	Vysoká úroveň – biometrie + PIN + kamera

Zdroj: vlastní zpracování.

Cílem navrhovaného systému bude nastavit různé úrovně přístupu podle citlivosti a rizikovosti jednotlivých prostor, přičemž některé části budovy budou zcela neveřejné a přístupné pouze konkrétním osobám s příslušným oprávněním. Biometrické technologie budou hrát klíčovou roli v ověřování identity uživatelů, bez nutnosti fyzických klíčů nebo karet, které lze snadno ztratit nebo zneužít (Kolář, 2019; Jelínek, 2021).

3.2 Legislativní požadavky a právní omezení

Implementací biometrických systémů v podnikovém prostředí jsou aktivovány různé právní mechanismy, zejména v oblasti ochrany osobních údajů. Biometrické údaje jsou dle současné právní úpravy zařazeny do zvláštní kategorie osobních údajů, s nimiž je spojeno zvýšené riziko neoprávněných zásahů do soukromí jednotlivce. Proto musí být při jejich získávání a zpracování respektovány evropské i národní předpisy. Tato problematika je zároveň součástí širší bezpečnostní politiky a řízení rizik, kde jsou sledovány oprávněné zájmy jak zaměstnavatele, tak subjektů údajů (Porada, 2022; Nařízení (EU) 2016/679).

3.2.1 Regulace na úrovni EU: GDPR

Základním právním rámcem upravujícím zpracování biometrických údajů je Nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR). V článku 4 odst. 14 GDPR jsou biometrické údaje definovány jako osobní údaje, které vznikly specifickým technickým zpracováním a vztahují se k fyzickým, fyziologickým či behaviorálním charakteristikám, jež umožňují jednoznačnou identifikaci fyzické osoby. Typickými příklady jsou otisky prstů, charakteristiky obličeje, vzory duhovky nebo hlasový otisk.

V článku 9 GDPR je zakázáno zpracovávat biometrické údaje, pokud není splněna některá ze zákonných výjimek. Výjimky zahrnují výslovný souhlas subjektu údajů, ochranu životně důležitých zájmů, plnění pracovněprávních povinností nebo oprávněné zájmy zaměstnavatele (Nařízení (EU) 2016/679).

Zpracování biometrických údajů musí být prováděno s ohledem na zásady minimalizace údajů a omezení účelu, aby byl zaručen co nejmenší zásah do práv a svobod subjektů údajů. Součástí GDPR je rovněž požadavek na provedení posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment, DPIA) před nasazením biometrických systémů, zejména pokud jsou tato data zpracovávána ve velkém rozsahu nebo způsobem, který může vyvolat vysoké riziko pro práva subjektů údajů.

3.2.2 Národní právní úprava v ČR

V České republice je evropská regulace doplněna zákonem č. 110/2019 Sb., o zpracování osobních údajů. Podle tohoto zákona smí být biometrické údaje zaměstnanců zpracovávány pouze tehdy, pokud je prokázáno, že neexistuje méně invazivní řešení, které by dosáhlo stejného účelu. Musí být rovněž přesně stanoven účel zpracování, doba uchovávání a zajištěna technická i organizační opatření na ochranu těchto údajů. Pokud zpracování není zákonem či smluvně vyžadováno, musí být získán výslovný, informovaný a dobrovolný souhlas zaměstnance, což je v pracovněprávním prostředí problematické vzhledem k nerovnováze postavení stran (Formánková, 2021).

Důležitým aspektem české legislativy je také role Úřadu pro ochranu osobních údajů, který dohlíží na správné dodržování pravidel zpracování biometrických dat a může v případě zjištění porušení uložit sankce. Zaměstnavatel je povinen vést evidenci a dokumentaci o zpracování biometrických údajů a je mu ukládána povinnost informovat zaměstnance o jejich právech, způsobech ochrany a případném zpracování.

3.2.3 Etické aspekty

Vedle právních požadavků musí být zohledněna i etická dimenze zavádění biometrických systémů. Je zdůrazňována potřeba transparentnosti a informovanosti zaměstnanců o účelu, rozsahu a způsobu zpracování biometrických údajů. Minimalizace objemu sbíraných dat na nezbytné minimum a participace zaměstnanců či jejich zástupců v procesu zavádění jsou doporučovány, aby se předešlo vnímání biometrických systémů jako neadekvátního zásahu do soukromí (Kovařík, 2020; Drahanský a Orság, 2011).

Etická stránka zahrnuje i otázky rovného zacházení a ochrany proti diskriminaci, protože biometrická data mohou být zneužita k nespravedlivé selekci nebo sledování zaměstnanců. Proto je nutné zavádět mechanismy, které zamezí takovému zneužití a umožní kontrolu nad daty. V tomto směru může pomoci interní politika ochrany osobních údajů a pravidelný audit využití biometrických systémů.

3.2.4 Technické normy a standardy

Pro zajištění správného a bezpečného fungování biometrických systémů jsou využívány mezinárodní standardy, například normy řady ISO/IEC, které stanovují doporučené postupy pro zpracování biometrických údajů. Jejich aplikací je posilována důvěryhodnost, interoperabilita a bezpečnost nasazených řešení (Kolář, 2019).

Tyto normy definují mimo jiné požadavky na přesnost, integritu a ochranu biometrických dat, jakož i na bezpečnostní opatření zabraňující neoprávněnému přístupu. Dodržování těchto technických standardů významně přispívá ke zvýšení důvěry subjektů údajů a ke snížení rizika případných bezpečnostních incidentů.

3.2.5 Vývoj legislativy a aktuální trendy

S rychlým rozvojem technologií je legislativa týkající se biometrických dat stále podrobněji rozvíjena a zpřesňována. Evropské instituce i národní orgány se zaměřují na posílení ochrany osobních údajů v souvislosti s rostoucím nasazením umělé inteligence a automatizovaných rozhodovacích systémů, které často využívají biometrická data.

Mezinárodní společenství diskutuje o nutnosti zavedení přísnějších pravidel pro biometrickou identifikaci, zejména ve veřejném prostoru, a o zajištění lepší kontroly nad sběrem a využíváním biometrických údajů. V této souvislosti jsou prosazovány principy privacy by design a privacy by default, které vyžadují, aby ochrana osobních údajů byla integrována již ve fázi návrhu technologií a systémů.

3.3 Vyhodnocení rizik a hledání možných hrozeb

Dříve než se firma rozhodne zavádět nějaký bezpečnostní systém, měla by si nejdřív ujasnit, proč ho vlastně potřebuje. Není to jen o technice, ale taky o tom, co všechno je ve firmě zranitelné – a jaké hrozby jí reálně hrozí. Tyhle hrozby se přitom netýkají jen počítačů nebo sítí, ale i lidí, prostoru nebo třeba papírových dokumentů. Zjednodušeně se to dá rozdělit na tři hlavní skupiny: fyzické (třeba někdo vleze dovnitř bez povolení), personální (když zaměstnanec

udělá chybu nebo se zachová špatně) a technické, což je všechno kolem IT a dat. Každá tahle oblast může být slabým místem – a když se něco pokazí, může to ovlivnit celou firmu (Brooks et al., 2018; Porada, 2022).

Bezpečnostní systém by proto neměl spoléhat jen na technologie. Měl by také počítat s tím, že chyby dělají i lidé, nebo že může něco selhat v organizaci práce. Všechno je to propojené. Funguje-li technologie, ale zaměstnanci s ní špatně zachází, problém nastane stejně.

3.3.1 Rizika ve firemním prostředí

Ve společnosti KulhFik s.r.o. bývají identifikovány všechny tři základní typy bezpečnostních rizik, které byly popsány v předchozí části práce. Tato rizika se projevují v různých oblastech provozu a jejich konkrétní podoba může být charakterizována následovně:

- **Fyzická rizika:** Dochází k nim v případech neoprávněného vstupu do areálu, odcizení majetku nebo úmyslného poškození technického vybavení.
- **Personální rizika:** Tato rizika jsou spojena s nepozorností zaměstnanců, neoprávněným sdílením přístupových údajů nebo s neetickým jednáním pracovníků.
- **Technická a informační rizika:** Mezi nejčastější patří únik citlivých dat, napadení IT systémů nebo neoprávněná manipulace s důvěrnými dokumenty.

V prostředí společnosti KulhFik s.r.o. je navíc nutné klást důraz na tzv. vnitřní rizika, která vznikají přímo uvnitř organizace. Ta mohou být způsobena nejen zaměstnanci, ale také návštěvníky pohybujícími se po firemních prostorách bez adekvátní kontroly. Právě tato vnitřní rizika bývají podle odborné literatury často podceňována, přestože mohou mít zásadní dopad na celkovou bezpečnost podniku (Blažek, 2019).

3.3.2 Možné bezpečnostní incidenty

Při posuzovaní bezpečnostních hrozeb ve společnosti KulhFik s.r.o. byla věnována zvláštní pozornost možným typům incidentů, které by mohly ohrozit jak plynulost provozu, tak integritu dat a důvěryhodnost firmy. Tyto incidenty představují konkrétní situace, kdy by mohlo dojít k narušení ochrany majetku, informací nebo osob. Jejich správná identifikace je klíčová pro návrh účinných bezpečnostních opatření a prevenci budoucích škod. Mezi nejvýznamnější možné incidenty patří:

- **Vniknutí do serverovny:** I jednorázové selhání přístupového systému může znamenat ohrožení IT infrastruktury.

- **Ztráta nebo únik dokumentů:** Když se někdo dostane k fyzickým podkladům, hrozí zneužití důvěrných dat.
- **Volný pohyb osob:** Návštěvníci bez dozoru mohou vstoupit do prostor, kam nemají přístup.
- **Zneužití přístupových údajů:** Pokud někdo použije kartu nebo kód jiné osoby, může dojít ke zneužití oprávnění.
- **Neoprávněná manipulace se zbožím:** Zaměstnanec může něco poškodit nebo si přivlastnit bez povolení.

Tyto incidenty mohou ohrozit nejen samotný provoz firmy, ale i její důvěryhodnost. Jakmile se naruší bezpečnost, dopad může být rychlý a výrazný – a někdy i těžko napravitelný (Novotný, 2022).

3.3.3 Slabiny aktuálního zabezpečení

Při posouzení současného stavu zabezpečení ve středně velkých logistických firmách, mezi které patří i společnost KulhFik s.r.o., byly zjištěny některé opakující se nedostatky v oblasti ochrany osob, majetku a informací. Tyto slabiny zvyšují pravděpodobnost vzniku bezpečnostních incidentů a mohou vést k ohrožení provozní kontinuity nebo reputace podniku. Mezi nejčastěji identifikované slabé stránky patří následující:

- **Chybějící ověření identity:** Používání karet bez biometrie je snadno zneužitelné.
- **Volný pohyb návštěv:** Bez evidence se ztrácí přehled o tom, kdo se kde pohyboval.
- **Používání fyzických klíčů:** Ty lze zkopírovat nebo ztratit a zabezpečení se tím snižuje.
- **Absence logování:** Pokud se něco stane, není zpětně dohledatelné, kdo kam vstoupil a kdy.
- **Nedostatečná ochrana serverovny:** Bez fyzického zabezpečení se může ke klíčové infrastruktuře dostat kdokoli.

Z těchto bodů je vidět, že aktuální bezpečnostní opatření nestačí odpovídajícím způsobem reagovat na reálná rizika. Nový biometrický systém by měl pomoci tyto problémy odstranit – ideálně tak, aby přitom zůstal praktický a zvládnutelný i v běžném provozu.

3.4 Návrh biometrického zabezpečení pro jednotlivé oblasti

V některých firmách se už dneska místo klasických klíčů nebo čipových karet používají jiné způsoby, jak poznat, kdo má kam přístup. Může to být třeba otisk prstu nebo rozpoznání

obličeje. Tyto způsoby pomáhají líp ohlídat prostory, kde je uložená technika nebo důležité dokumenty. Výhodou je, že se těžko zneužívají, a proto se hodí na místa, kde je potřeba větší jistota (Drahanský a Orság, 2011; Kolář, 2019).

3.4.1 Serverovna

Z hlediska bezpečnosti patří serverovna k nejcitlivějším místům v celé firmě. Vevnitř se nachází servery, síťové prvky a další klíčová zařízení. Bez nich by firemní IT nemohlo fungovat. Do serverovny by proto měli chodit jen lidé s potřebným oprávněním – především IT personál a technické vedení.

Jako bezpečnostní řešení se hodí dvoufázové ověření. Nejprve pomocí biometrie – třeba otisk prstu – a následně třeba PINem nebo kartou. Pro tento účel se hodí čtečka GV-Fingerprint, nebo model GV-FR2020, který umí pracovat jak s otisky prstů, tak s obličejem. Přístupy se budou zapisovat v systému GV-ASManager. Ten zároveň zvládne sledovat události, spravovat přístupová práva a propojit se s kamerami (GeoVision, 2023).

IP kamera, která bude u vstupu, se může propojit s tímto systémem. S platformou GV-VMS pak bude možné zaznamenávat všechny přístupy a lépe hlídat, co se děje. Použité zařízení:

- Biometrická čtečka GeoVision GV-Fingerprint nebo GV-FR2020
- Software GV-ASManager pro správu přístupů
- IP kamera propojená s platformou GV-VMS

Obrázek 2 - Zařízení GV-FR2020.

Zdroj: GeoVision, 2023.

Návrh propojení přístupových zařízení, řídicí jednotky a serverové infrastruktury. Systém GeoVision využívá centrální správu přístupů pomocí platformy GV-ASManager, která eviduje a řídí všechny přístupové operace v reálném čase.

3.4.2 Sklad citlivých dokumentů

V této místnosti se ukládají smlouvy, osobní údaje, faktury a podobné dokumenty. Hrozbou může být nejen krádež nebo ztráta, ale taky to, že k nim získá přístup někdo nepovolaný.

K zabezpečení se navrhuje biometrická čtečka otisků prstů GeoVision GV-Fingerprint. Přístupy se evidují přes GV-ASManager, který umožňuje správu oprávnění i kontrolu vstupů. Povoleni budou mít jen někteří zaměstnanci – hlavně ti z administrativy nebo vedení. Výhodou je, že se systém snadno připojí ke stávající síti a může se propojit i s jinými zabezpečovacími zařízeními (GeoVision, 2023).

Je snadno ovladatelný a zároveň poskytuje přehled o tom, kdo a kdy vstoupil. Navíc dobře zabezpečuje důležité prostory. Použité zařízení:

- Biometrická čtečka GeoVision GV-Fingerprint
- Přístupový software GV-ASManager
- Propojení s interní sítí a docházkovým systémem

3.4.3 Kancelář vedení / generálního ředitele

Kancelář vedení bývá místem, kde jsou uložené důležité finanční a strategické dokumenty. Navíc tam často bývá přítomen sám ředitel, takže je potřeba řešit i jeho osobní bezpečí. Do této místnosti se hodí bezdotykové ověření obličeje. Takové řešení je komfortní, bezpečné a bezkontaktní, což je výhoda i z hygienického hlediska.

Pro tento účel je doporučeno použít terminál GV-FR2020, který funguje i za zhoršených světelných podmínek díky IR senzoru. Zařízení rozpozná obličej, ale zvládne i zadání PINu nebo použití RFID karty. Všechna přístupová oprávnění se pak nastavují v systému GV-ASManager, který se dá propojit s ostatními bezpečnostními prvky (GeoVision, 2023). Použité zařízení:

- Terminál GV-FR2020 s rozpoznáním obličeje a IR senzorem
- Správa přístupů pomocí GV-ASManager
- Možnost kombinace s PIN kódem nebo RFID kartou

3.4.4 Doporučení pro skladové prostory

Sklad sice není místo, kde se běžně pracuje s citlivými údaji, ale pořád jde o prostor, kde se skladuje zboží s vyšší hodnotou. Navíc se v něm často pohybují zaměstnanci. Není nutné sem zavádět biometrický přístup, ale určitě má smysl posílit dohled.

Ve skladu se doporučuje použít IP kamery napojené na systém GV-VMS. To umožní zpětně zkontrolovat, co se tam dělo – třeba při podezřelém pohybu nebo jiných událostech. Výhodou je, že to nijak nenaruší běžný provoz. Navíc získá vedení firmy lepší přehled o dění. Pokud by došlo k problému, záznamy poslouží jako důkaz (GeoVision, 2023). Použité zařízení:

- Kamery kompatibilní se systémem GeoVision
- Analytická a záznamová platforma GV-VMS
- Možnost doplnění o RFID čtečky pro evidenci vstupů

3.4.5 Metodika výběru zařízení

Při výběru konkrétních zařízení pro zabezpečení jednotlivých prostor bylo nutné přistoupit k tomuto kroku systematicky, a nikoliv pouze na základě subjektivních preferencí nebo dostupnosti. Výběr proto vycházel z principů vícekriteriálního rozhodování, a to formou zjednodušeného bodového hodnocení s využitím vážených kritérií. Tento přístup zvyšuje

transparentnost návrhu a umožňuje obhájit zvolená technická řešení z hlediska funkčnosti, ekonomiky i provozní udržitelnosti. Pro účely hodnocení byla zvolena pětice kritérií, z nichž každému byla přiřazena váha odrážející jeho důležitost v kontextu konkrétního použití. Kritéria a jejich popis uvádí následující tabulka:

Tabulka 4 - Použitá hodnoticí kritéria

Kritérium	Popis	Váha
Spolehlivost identifikace	Přesnost, odolnost proti chybám, ochrana proti spoofingu	30
Uživatelská přívětivost	Intuitivnost obsluhy, komfort a rychlost identifikace	20
Technická podpora a servis	Dostupnost technické podpory a možnost servisu v ČR	15
Cena zařízení a provozu	Pořizovací a provozní náklady	20
Rozšiřitelnost a integrace	Možnost integrace do docházky, systémů řízení přístupu a kamerových řešení	15

Zdroj: vlastní zpracování podle (Füller, 2003).

Každé kritérium bylo ohodnoceno vahou vyjadřující jeho důležitost (v procentech), a jednotlivé varianty byly bodově ohodnoceny na škále 1–5 (1 – nevyhovující, 5 – výborné). Celkové skóre bylo získáno součtem jednotlivých vážených bodů. Do porovnání byly zařazeny tři reálné alternativy (Füller, 2003):

- **GeoVision GV-FR2020** – AI terminál s rozpoznáním obličeje a možností integrace s docházkovými a kamerovými systémy
- **Suprema BioStation 2** – pokročilá čtečka otisků prstů s vysokou přesností a rychlostí,
- **ZKTeco MB20** – cenově dostupné zařízení kombinující čtečku otisku prstu a rozpoznání obličeje.

Tabulka 5 - Porovnání variant.

Kritérium	Váha	GeoVision	Suprema	ZKTeco
Spolehlivost identifikace	30	5	5	3
Uživatelská přívětivost	20	5	4	3
Technická podpora a servis	15	4	5	2
Cena zařízení a provozu	20	3	3	5
Rozšiřitelnost a integrace	15	5	4	3
Celkové skóre	—	**445**	**425**	**325**

Zdroj: vlastní výpočty dle metody (Füller, 2003).

Na základě celkového hodnocení vychází jako nejvhodnější varianta zařízení **GeoVision GV-FR2020**, které dosáhlo nejvyššího bodového skóre. Přestože jeho pořizovací náklady jsou vyšší než u konkurence, výborně obstálo v oblasti spolehlivosti, uživatelské přívětivosti i možností integrace. Suprema BioStation 2 představuje solidní alternativu tam, kde je důraz kladen na kvalitu snímání otisku prstu, a zároveň je k dispozici spolehlivá technická podpora. ZKTeco MB20 pak nabízí nízkou pořizovací cenu, ale nedosahuje takové technické úrovně jako předchozí dvě varianty (Drahanský a Orság, 2011).

Hlavním přínosem tohoto porovnání není absolutní výběr „nejlepšího zařízení“, ale vytvoření transparentního postupu výběru, který může být dále upraven podle specifik jiných firem nebo prostředí. V praxi lze navíc výběr doplnit o testování zařízení v reálném provozu nebo konzultaci s odborníky na bezpečnostní systémy.

4 Celkové vyhodnocení

Ve společnosti KulhFik s.r.o. bylo posouzeno zavedení přístupového systému, který využívá biometrické technologie pro identifikaci osob. Tento krok byl zvažován zejména z důvodu zvýšení úrovně fyzické bezpečnosti a zajištění přesné evidence pohybu osob ve firemních prostorách. Zavedením systému založeného na biometrických údajích by se významně snížilo riziko neoprávněného vstupu a současně by se zlepšila dohledatelnost a odpovědnost jednotlivých zaměstnanců.

Jedním z hlavních přínosů použití biometrie je její jedinečnost – každý člověk disponuje unikátními znaky, jako je například otisk prstu, které nelze snadno zaměnit nebo zneužít. Oproti tradičním přístupovým prostředkům, jako jsou karty nebo hesla, poskytuje biometrie vyšší úroveň zabezpečení (Kolář, 2019). Přístupový systém navíc zaznamenává veškeré pohyby osob, což umožňuje zpětné dohledání a vyhodnocení událostí v případě vzniku bezpečnostního incidentu.

V navrženém řešení je počítáno s využitím zařízení a softwaru značky GeoVision. Systém GV-ASManager zajišťuje propojení jednotlivých komponent (např. čteček, kamer, přístupových terminálů) do jednoho uceleného prostředí, které umožňuje správu oprávnění, logování a přehledné řízení přístupů (GeoVision, 2023).

Je však nezbytné počítat i s potenciálními překážkami implementace. V některých provozních podmínkách, jako jsou prašná prostředí nebo výkyvy teplot, může docházet ke snížení přesnosti snímání. Současně je nutné věnovat pozornost postojům zaměstnanců, kteří mohou vnímat sběr biometrických údajů jako zásah do soukromí. Tyto obavy lze eliminovat prostřednictvím důkladné interní komunikace, školení a transparentního seznámení s účelem i způsobem fungování systému (Formánková, 2021).

Z hlediska právní regulace je implementace biometrických technologií podmíněna dodržením požadavků plynoucích z GDPR a zákona č. 110/2019 Sb. Biometrická data jsou považována za citlivou kategorii osobních údajů a jejich zpracování je povoleno pouze tehdy, pokud jsou splněny konkrétní podmínky – např. existence výslovného souhlasu subjektu údajů, nebo prokazatelná nezbytnost zpracování pro ochranu oprávněných zájmů. Firma je rovněž povinna určit účel zpracování, dobu uchování údajů a zajistit odpovídající technická i organizační opatření (Nařízení (EU) 2016/679).

Celkově lze konstatovat, že biometrický přístupový systém může přinést společnosti KulhFik s.r.o. výrazné zvýšení bezpečnostních standardů, a to při dodržení všech legislativních a etických požadavků. Klíčovým předpokladem úspěšné realizace je kvalitní plánování, informovanost uživatelů a průběžné vyhodnocování účinnosti zavedených opatření.

4.1 Odhad nákladů a přínosů navrženého řešení

Zavedení biometrického přístupového systému ve společnosti KulhFik s.r.o. není pouze technickým krokem směrem ke zvýšení úrovně zabezpečení, ale představuje rovněž důležité rozhodnutí z ekonomického hlediska. Z toho důvodu je vhodné posoudit nejen technologické možnosti, ale i ekonomickou efektivitu tohoto řešení. V této kapitole je uveden přehled hlavních nákladových a přínosových oblastí; konkrétní výpočty budou podrobně zpracovány v následující části práce.

Mezi hlavní položky investičních výdajů patří pořízení hardwarových komponent, jako jsou čtečky otisků prstů, kamerové jednotky, přístupové terminály či elektromagnetické zámky. Nedílnou součástí systému je také softwarové vybavení, které zajišťuje správu uživatelů, definici přístupových oprávnění a provozní monitoring. V případě, že již ve firmě existuje infrastruktura pro řízení přístupů, je třeba počítat s náklady na integraci nového systému do stávajícího prostředí. Do celkové částky vstupují také výdaje na odbornou instalaci, konfiguraci zařízení a školení personálu, jenž bude se systémem pracovat (Kolář, 2019).

Po implementaci systému nevznikají obvykle vysoké provozní náklady, nicméně je nutné zohlednit náklady na pravidelný servis, výměnu opotřebených komponent a softwarové aktualizace. Ve většině případů je možné tyto činnosti provádět v rámci interního IT oddělení, bez nutnosti externího poskytovatele (Ryan, 2020).

Z hlediska přínosů systém umožňuje výrazné zvýšení bezpečnosti firemních prostor. Díky biometrické autentizaci je zajištěno, že do vymezených prostor vstupují pouze osoby s odpovídajícím oprávněním. Veškeré přístupy jsou systémem zaznamenávány, což umožňuje zpětnou kontrolu událostí a identifikaci odpovědných osob v případě bezpečnostního incidentu (Kolář, 2019).

Kromě přímých přínosů existují také nepřímé efekty, které se projeví například snížením závislosti na fyzické ostraze, odstraněním problémů spojených se ztrátou přístupových karet nebo minimalizací chyb způsobených lidským faktorem. Díky automatizaci dochází ke zjednodušení správy systému a zvýšení provozní efektivity. V konečném důsledku může být biometrie

vnímána nejen jako bezpečnostní nástroj, ale i jako prostředek ke zlepšení organizace práce, zvýšení odpovědnosti zaměstnanců a snížení administrativní zátěže (Formánková, 2021).

Přesto je nezbytné, aby bylo rozhodnutí o implementaci podloženo relevantními informacemi a posouzením, které zohledňují specifické podmínky daného podniku. Při zpracování tohoto rozhodnutí je třeba dodržet i všechny právní a regulační požadavky související se zpracováním biometrických údajů (Nařízení (EU) 2016/679).

4.2 Ekonomické vyhodnocení návrhu

Pro účely posouzení efektivity zavedení biometrického přístupového systému ve společnosti KulhFik s.r.o. byl proveden odhad nákladů a přínosů, který zohledňuje celkové investiční i provozní výdaje v porovnání s očekávanými přínosy. Navržený systém je koncipován na bázi technologií společnosti GeoVision, která nabízí ucelené řešení zahrnující biometrické čtečky, software pro správu přístupových oprávnění i nástroje pro monitoring a dohled (GeoVision, 2023).

V rámci návrhu byly identifikovány tři klíčové přístupové body – vstup do serverovny, vstup do skladu citlivých dokumentů a vstup do kanceláře vedení. Každý z těchto prostor je chráněn odlišnou metodou ověření, přičemž je využívána autentizace pomocí otisku prstu, rozpoznání obličeje nebo jejich kombinace. Všechna zařízení jsou propojena a centrálně řízena prostřednictvím softwarového rozhraní GV-ASManager, které zajišťuje nejen správu uživatelů a přístupových práv, ale i evidenci vstupů a možnost vzdálené správy systému.

Z hlediska investičních nákladů je systém navržen tak, aby byl finančně přiměřený velikosti a potřebám středně velkého podniku. Klíčovým kritériem hodnocení je ekonomická únosnost řešení v pětiletém horizontu a potenciál návratnosti prostřednictvím zvýšení bezpečnosti, snížení provozních rizik a optimalizace řízení přístupů. Návrh proto vychází nejen z technologické efektivity, ale také z rovnováhy mezi pořizovací cenou a funkčním přínosem.

4.2.1 Odhad pořizovacích nákladů

Při stanovení pořizovacích nákladů byly zohledněny veřejně dostupné ceníky a nabídky českých dodavatelů bezpečnostních technologií. Uváděné ceny odpovídají standardní úrovni vybavení, které je považováno za vhodné pro středně velkou společnost, jakou je KulhFik s.r.o. (Kamartech, 2024; Alza.cz, 2024).

Tabulka 6 - Přehled použitých zařízení Geovision.

Položka	Model	Cena	Množství	Celkem
Biometrický terminál – otisk prstu (sklad dokumentů)	GV-Fingerprint Reader	7 500	1	7 500
Biometrický terminál – obličej + otisk (serverovna)	GV-FR2020	15 500	1	15 500
Biometrický terminál – obličej (kancelář vedení)	GV-FR2020	15 500	1	15 500
Elektromagnetické zámky, čtečky, kabeláž, montážní materiál	–	3 500	3	10 500
Software pro správu přístupů a záznamu (do 5 dveří)	GV-ASManager (základ)	12 000	1	12 000
Instalační a konfigurační práce, školení obsluhy	–	–	–	8 000
Celkové investiční náklady	–	–	–	**69 000**

Zdroj: vlastní zpracování na základě údajů výrobce (GeoVision, 2025).

Náklady na pořízení systému činí přibližně **69 000 Kč.** Tato částka zahrnuje jak hardware, tak software, instalační práce i základní školení pracovníků. Systém lze kdykoliv rozšířit o další přístupové body nebo kamerové jednotky díky modulárnímu licenčnímu modelu GV-ASManager.

4.2.2 Provozní náklady

V rámci navrženého řešení byly identifikovány rovněž provozní náklady, které se v tomto modelu jeví jako relativně nízké. Uvažuje se zejména s pravidelnou údržbou zařízení,

drobnými opravami, aktualizacemi softwaru a případnou výměnou opotřebovaných komponent v pětiletém provozním horizontu.

Tabulka 7 - Přehled provozních nákladů.

Položka	Roční odhad
Servisní prohlídky a údržba zařízení	3 000
Aktualizace softwaru a technická podpora	2 000
Opravy a výměny komponent	1 500
Celkem ročně	**6 500**

Zdroj: vlastní zpracování na základě odhadů dle dostupných ceníků a informací výrobce (GeoVision, 2025).

Při předpokládané pětileté životnosti systému lze celkové provozní náklady odhadnout na částku přibližně **32 500 Kč**. Tyto náklady zahrnují běžnou technickou podporu a servisní zásahy a lze je v rámci menšího podniku považovat za dlouhodobě udržitelné.

4.2.3 Celkové náklady a návratnost investice

Celkové náklady spojené s pořízením a provozem biometrického systému byly při zohlednění pětiletého období vyčísleny na přibližně **101 500 Kč.** Do této částky jsou zahrnuty náklady na hardwarové a softwarové vybavení, instalační práce, školení obsluhy, pravidelná údržba i technická podpora.

Z hlediska návratnosti investice lze uvažovat následující modelovou situaci: v případě narušení zabezpečené oblasti – například neoprávněného vstupu do serverovny – může dojít ke škodám přesahujícím **50 000 Kč**. Tyto ztráty mohou být způsobeny výpadkem informační infrastruktury, únikem nebo ztrátou dat, případně porušením legislativy (např. GDPR), což může vést i k udělení sankcí.

Za předpokladu, že biometrický systém přispěje k eliminaci alespoň dvou takových incidentů během pěti let, lze investici považovat za plně návratnou. Kromě toho však existují i přínosy, které nejsou přímo finančně vyjádřitelné, ale přesto mají výrazný dopad na chod

podniku. Mezi tyto přínosy patří například lepší kontrola pohybu osob v areálu, zvýšená odpovědnost zaměstnanců nebo zjednodušená správa přístupových práv. Tyto aspekty pozitivně ovlivňují stabilitu provozu a přispívají k vytvoření bezpečnějšího pracovního prostředí (Rak, Matyáš a Říha, 2008).

4.2.4 Alternativní varianta řešení a porovnání

Byla zvážena i druhá možnost, a to náročnější řešení zahrnující více přístupových bodů, kvalitnější kamery, záložní napájení a pokročilejší software (GV-VMS). V tomto systému by byla využita kombinovaná biometrie, síťové úložiště NAS a větší počet čteček (GeoVision, 2023).

Náklady na toto řešení by se však odhadovaly na přibližně 130 000 Kč. Roční provozní náklady by byly o několik tisíc korun vyšší než u původního návrhu. Přestože by byla zvýšena úroveň zabezpečení, bylo by toto řešení pro společnost KulhFik s.r.o. zbytečně složité a nákladné. Správa systému by vyžadovala více času, a ne všechny nové prvky by byly ve firmě efektivně využity. Z provedeného porovnání vyplývá, že původní návrh je výhodnější. Cena je rozumná, návratnost investice se odhaduje na tři až čtyři roky a celý systém je méně náročný na provoz. I když by rozšířená varianta působila moderněji, v podmínkách střední firmy by byla přínosem spíše komplikace než užitek.

Tabulka 8 - Porovnání variant (řešení).

Kritérium	Navržené řešení (A)	Rozšířená varianta (B)
Pořizovací náklady	cca 69 000	cca 130 000
Provozní náklady (roční)	cca 6 500	cca 10 000–12 000
Typ ověření	Biometrie (otisk, obličej), PIN, RFID	Multibiometrie + vizuální monitoring
Počet zabezpečených prostor	3	5–6
Softwarová správa	GV-ASManager (základ)	GV-ASManager + GV-VMS + NAS
Uživatelský komfort	Vysoký	Vysoký, ale náročnější

Kritérium	Navržené řešení (A)	Rozšířená varianta (B)
Reálný přínos pro firmu	Vysoký / odpovídající potřebám	Nadbytečný, náročný na správu
Návratnost investice	3–4 roky	5+ let, obtížně měřitelná
Ekonomická efektivita	Vyvážená	Nízká pro danou velikost firmy

Zdroj: vlastní zpracování na základě údajů výrobce (GeoVision, 2025) a odborné literatury (Kolář, 2019; Ryan, 2020).

Na základě uvedeného porovnání lze konstatovat, že ačkoli je rozšířená varianta nabízena s vyšší mírou zabezpečení a pokročilými technologickými možnostmi, její přínos není úměrný výrazně vyšším nákladům. V podmínkách středně velké firmy, jakou je KulhFik s.r.o., je navržené řešení považováno za ekonomicky efektivnější a provozně přiměřené, jelikož zajišťuje požadovanou úroveň ochrany bez zbytečného zatížení rozpočtu či personálu.

4.2.5 Vyhodnocení

V rámci práce byly obě varianty podrobeny komplexnímu srovnání, přičemž základní řešení (označované jako A) je možno považovat za ekonomicky výhodnější pro společnost KulhFik s.r.o. Biometrickým systémem, jenž byl navržen v této variantě, je firmě poskytována přiměřená ochrana objektu s rozumnými provozními náklady nepřesahujícími 6 500 Kč za rok. V porovnání s jinými možnostmi bylo toto řešení hodnoceno jako nejvíce vyhovující pro tento konkrétní subjekt, což ostatně bývá u podobných firem pravidlem (viz studie GeoVision, 2023).

Oproti tomu rozšířenou variantou B, ač technicky propracovanější, by byly firemní finance zatíženy neúměrně. Investice přesahující 130 tisíc korun společně s každoročními výdaji 10-12 tisíc by byla vzhledem k reálným potřebám společnosti KulhFik zbytečná. Dalšími kamerami a přídavnými přístupovými body, s nimiž je tato varianta vybavena, by za takových okolností nebylo dosaženo odpovídajícího zvýšení bezpečnosti. V těchto souvislostech je proto doporučováno přiklonit se k ekonomičtější variantě A, kterou je zajišťována adekvátní bezpečnost při zachování finanční udržitelnosti.

Závěr

Cílem této práce bylo posoudit potřeby zabezpečení ve firmě KulhFik s.r.o., navrhnout efektivní systém biometrického přístupu a provést jeho ekonomické zhodnocení. Návrh řešení zohledňoval jak technické, tak legislativní a ekonomické aspekty spojené s využíváním biometrických údajů ve firemním prostředí.

V rámci praktické části byly definovány klíčové prostory vyžadující zvýšenou ochranu – serverovna, sklad citlivých dokumentů a kancelář vedení. Současně byly zmapovány právní požadavky, zejména v oblasti ochrany osobních údajů dle nařízení GDPR a zákona č. 110/2019 Sb., které významně ovlivňují způsob zavádění biometrických systémů.

Na základě identifikovaných potřeb byl navržen systém založený na technologiích společnosti GeoVision, využívající kombinaci ověřování pomocí otisku prstu, rozpoznání obličeje a centrální správu přístupů prostřednictvím platformy GV-ASManager. Součástí návrhu bylo také doporučení na doplňkové zabezpečení skladových prostor prostřednictvím kamerového systému.

Ekonomické vyhodnocení potvrdilo, že zavedení navrženého biometrického systému je z finančního hlediska efektivní. Celkové pořizovací náklady ve výši přibližně 69 000 Kč a provozní náklady cca 6 500 Kč ročně odpovídají velikosti a potřebám firmy. Odhad nákladů a přínosů ukázal, že zamezení alespoň dvou závažných bezpečnostních incidentů během pěti let by zajistilo plnou návratnost investice. Ve srovnání s alternativní, nákladnější variantou rozšířeného zabezpečení byla navržená varianta vyhodnocena jako optimální kompromis mezi náklady a přínosy.

Práce rovněž upozornila na důležitost respektování etických a právních zásad při implementaci biometrických systémů a na potřebu transparentní komunikace se zaměstnanci, aby bylo zajištěno správné vnímání těchto opatření uvnitř firmy.

Z hlediska možností dalšího rozvoje lze do budoucna uvažovat o rozšíření systému o další přístupové body, integraci s docházkovými systémy nebo nasazení pokročilých analytických funkcí v rámci kamerového dohledu. Rozvoj technologií v oblasti biometrie nabízí v tomto směru značný potenciál.

Použité zdroje

ALZA.CZ. *Elektronické zámky a biometrické čtečky – katalogové ceny* [online]. Alza.cz, 2024 [cit. 12. 6. 2025]. Dostupné z: https://www.alza.cz

BLAŽEK, Radim. *Řízení rizik v bezpečnostních systémech*. Brno: Tribun EU, 2019. ISBN 978-80-263-1504-0.

BROOKS, Charles J.; GROW, Christopher; CRAIG, Philip a SHORT, Donald. *Cybersecurity essentials*. Indianapolis, Indiana: Sybex, John Wiley, 2018. ISBN 978-1-119-36239-5.

ČESKÝ BEZPEČNOSTNÍ PORTÁL. *Kybernetické hrozby a incidenty v ČR* [online]. 2022 [cit. 12. 6. 2025]. Dostupné z: https://www.securitymagazin.cz

ČSN ISO/IEC 19794. *Informační technologie – Formáty výměny biometrických dat*.

DRAHANSKÝ, Martin a ORSÁG, Filip. *Biometrie*. [Brno: M. Drahanský], 2011. ISBN 978-80-254-8979-6.

FORMÁNKOVÁ, Klára. *Pracovní právo a ochrana osobních údajů*. Praha: Wolters Kluwer, 2021. ISBN 978-80-7598-982-0.

FÜLLER, Jiří. *Vícekriteriální rozhodování v praxi*. Praha: Professional Publishing, 2003. ISBN 80-86419-40-6.

GALBALLY, Javier; ORTEGA-GARCÍA, Javier; FIERREZ, Julian a MARCEL, Sébastien. A high performance fingerprint liveness detection method based on quality related features. *Future Generation Computer Systems*, 2014, 28(1): 311–321. ISSN 0167-739X.

GEOVISION. *GV-EBL4702, GV-ASManager, GV-VMS – Produktová dokumentace* [online]. Taipei: GeoVision Inc., 2023 [cit. 12. 6. 2025]. Dostupné z: https://www.geovision.com.tw

GEOVISION. *GV-Fingerprint, GV-FR2020, GV-ASManager, GV-VMS – Produktová dokumentace* [online]. Taipei: GeoVision Inc., 2023 [cit. 12. 6. 2025]. Dostupné z: https://www.geovision.com.tw

GEOVISION. *Product Overview*. [online]. 2025 [cit. 30. 6. 2025]. Dostupné z: https://www.geovision.com.tw/

IDEMIA. Biometric Devices and Solutions. [online]. 2025 [cit. 30. 6. 2025]. Dostupné z: https://www.idemia.com/

IRIS ID Systems Inc. Iris Recognition Solutions. [online]. 2025 [cit. 30. 6. 2025]. Dostupné z: https://www.irisid.com/

JAIN, Anil K.; ROSS, Arun a NANDAKUMAR, Karthik. *Introduction to Biometrics*. 2nd ed. New York: Springer, 2020. ISBN 978-0-387-77326-1.

JELÍNEK, Lukáš. *Zabezpečení IT infrastruktury ve firmách*. Praha: Grada, 2021. ISBN 978-80-271-3126-8.

KAMARTECH. *Ceník přístupových systémů a biometrie* [online]. Praha: Kamartech s.r.o., 2024 [cit. 12. 6. 2025]. Dostupné z: https://www.kamartech.cz

KOLÁŘ, Petr. *Biometrické technologie: principy a praxe*. Plzeň: Západočeská univerzita, 2019. ISBN 978-80-261-0880-2.

KOVÁŘ, Jiří. *Analýza a management rizik*. Praha: Grada Publishing, 2020. ISBN 978-80-271-3001-8.

KOVAŘÍK, David. *Etické aspekty biometrie*. Brno: Masarykova univerzita, 2020.

NAŘÍZENÍ (EU) 2016/679 Evropského parlamentu a Rady ze dne 27. dubna 2016, obecné nařízení o ochraně osobních údajů (GDPR).

NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI. *Výroční zpráva NÚKIB* [online]. Brno: NÚKIB, 2023 [cit. 12. 6. 2025]. Dostupné z: https://www.nukib.cz

NOVOTNÝ, Marek. *Bezpečnostní strategie podniku*. Ostrava: SPU, 2022.

NOVOTNÝ, Michal. *Ochrana dat a bezpečnostní politika*. Brno: VUT Brno, 2020.

O'GORMAN, Lawrence. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 2003, 91(12): 2021–2040. ISSN 0018-9219.

PORADA, Viktor. *Bezpečnostní vědy: úvod do teorie, metodologie a bezpečnostní terminologie*. 2. vyd. Plzeň: Aleš Čeněk, 2022. ISBN 978-80-7380-903-4.

RAK, Roman; MATYÁŠ, Vašek a ŘÍHA, Zdeněk. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. ISBN 978-80-247-2365-5.

RYAN, Patrick. *Cost Benefit Analysis for Security Projects*. Springer, 2020. ISBN 978-3-030-46800-1.

SUPREMA Inc. Suprema Products. [online]. 2025 [cit. 30. 6. 2025]. Dostupné z: https://www.supremainc.com/

TICHÝ, Radim. *Bezpečnost informací v praxi*. Praha: Computer Press, 2018. ISBN 978-80-251-4856-3.

ULUDAĞ, Umut; POHLMANN, Norbert; JAIN, Anil K. Biometric cryptosystems: Issues and challenges. *Proceedings of the IEEE*, 2004, 92(6): 948–960. ISSN 0018-9219.

VISIONLABS. Face Recognition Software. [online]. 2025 [cit. 30. 6. 2025]. Dostupné z: https://visionlabs.ai/

WANG, Yu; YU, Zhiwen; HUANG, Shijian a LIU, Yang. Deep learning for biometric recognition: A survey. *Pattern Recognition Letters*, 2021, 136: 1–16. ISSN 0167-8655.

ZÁKON č. 110/2019 Sb. o zpracování osobních údajů. In: *Sbírka zákonů České republiky*. 2019.

ZKTECO Co., Ltd. ZKTeco Biometric Solutions. [online]. 2025 [cit. 30. 6. 2025]. Dostupné z: https://www.zkteco.com/