VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

SYSTÉM KONTROLY VSTUPU

Autor práce: Pavel Peták, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: Mgr. Bc. Radovan Sládek

Katedra: Katedra právních oborů a bezpečnostních studií

2021

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Pavel Peták, DiS.

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Systém kontroly vstupu

Název bakalářské práce v anglickém jazyce: Systems for acces control

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce: Mgr. Bc. Radovan Sládek

Datum zadání bakalářské práce: Říjen 2020

Cíl bakalářské práce:

Cílem bakalářské práce je vytvořit zpracovaný a ucelený přehled, jak funguje systém kontroly vstupu, shrnutí jeho hlavních částí a jeho spolupráce s mechanickými zábrannými systémy. Podrobně rozvést nosiče informací a jejich snímače s uvedením jejich výhod a nevýhod. Dalším cílem je vytvořit model objektu malé firmy využívající systém kontroly vstupu.

Student: Pavel Peták, DiS.	*Datum* *5.11.2020*	*podpis*
Vedoucí práce: Mgr. Bc. Radovan Sládek	*Datum* *5.11.2020*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	23. 11. 20 *datum*	*podpis*
Prorektorka pro studium a vnitřní záležitosti: RNDr. Růžena Ferebauerová	1. 12. 20 *datum*	*podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	1. 12. 20 *datum*	*podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce Mgr. Bc. Radovanu Sládkovi za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

PETÁK, P. *Systém kontroly vstupu: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2021. 55 s. Vedoucí bakalářské práce: Mgr. Bc. Radovan Sládek.

Klíčová slova: Systém kontroly vstupu, identifikace, snímače, biometrie, čtečka

Bakalářská práce popisuje systém kontroly vstupu do zabezpečených objektů nebo předmětů. V této práci je detailně rozebrána celá struktura tohoto systému, jeho požadavky, používané komponenty, jeho úkoly a komunikace mezi dalšími prvky systému a dalších zabezpečovacích prvků. Nedílnou součástí systému kontroly vstupu jsou mechanické zábranné systémy, bez kterých by byl systém neefektivní. V další části této práce je vytvořen návrh zabezpečení malé firmy obsahující systém kontroly vstupu, jeho umístění a jeho celkovou kalkulací použitých komponentů tohoto zabezpečení v uvedené fiktivní firmě.

ABSTRACT

PETÁK, P. *Systems for access control: Bachelor Thesis.* České Budějovice: The College of European and Regional Studies, 2021. 55 p. Supervisor: Mgr. Bc. Radovan Sládek.

Key words: Systems for access control, identifications, sensors, biometrics, reader

Bachelor's thesis describes a system of access control to secured compounds and objects. The whole structure of this system, its requirements, used components, tasks and communication with other elements and other security components is covered in detail in this work. Integral part of systems of access control is physical obstruction system. Without it, it would be ineffective. In other part of this thesis is created a proposal of security measures for a small company. Proposal includes system of access control, its placement and overall list of used components with price calculation.

Obsah

Úvod

Systém kontroly vstupu vznikl na základě potřeby společnosti chránit svoji bezpečnost, zdraví či majetek. Jedná se o instinktivní reakci člověka na hrozbu ze strany třetí osoby. Tuto skutečnost již vnímali naši předkové v prvopočátcích civilizace, kdy mezi sebe nechtějí pouštět cizince, aby chránili svůj majetek. Postupem času, ač si více uvědomovali cenu svého majetku, nevěnovali dostatečnou pozornost jeho zabezpečení.

Systém kontroly vstupu majetek přímo nechrání, ale umožňuje kontrolovaný vstup do prostor na základě udělených práv konkrétním osobám, nebo skupinám. Tyto prostory je ale třeba stále hlídat i fyzicky, nebo je hlídat za použití kamerového systému, či jinými prvky EZS, které můžou být sepnuty, až na základě vstupu osoby do hlídaného prostoru. Systémy dokážou samy rozhodnout o umožnění vstupu, nebo jeho odmítnutí.

Tato práce pojednává o tom, co je to vlastně systém kontroly vstupu, jak funguje a jaké má hlavní části. Systém kontroly vstupu spolupracuje s mnohými dalšími systémy a je často součástí komplexního celku bezpečnosti. Je tedy často propojen s kamerovým systém, docházkovým systémem nebo s pultem centralizované ochrany, který při pokusu o neoprávněný vstup vyhlásí poplach.

Uvedené systémy jsou ještě relativně mladé a náročné co se týče instalace, provozu nebo údržby. Ale každý, ať už fyzická osoba nebo právnická osoba, by si měl uvědomit, že čím větší má majetek, tím více je třeba jej chránit. Uvědomit si, že instalace systému pro kontrolu vstupu není zbytečná, ale účinně pomáhá k poklesu krádeží, úniku důležitých dat, nebo neoprávněnému vstupu jiným osobám.

1 Cíl a metodika bakalářské práce

Hlavním cílem této bakalářské práce je charakterizovat co je systém kontroly vstupu, jeho úkoly a důležitost kombinace s dalšími prvky zabezpečení.

Teoretická část, pojednává o hlavním cíli práce. Představuje čtenáři strukturu celého systému pro kontrolu vstupu a podrobněji se zabývá identifikačními metodami a prostředky identifikace osob, zejména biometrické metody identifikace, kde jsou popsány nejčastější používané způsoby, jejich výhody a nevýhody. V práci jsou dále podrobněji představené mechanické zábranné systémy, které jsou pro systém nezbytnou součástí. Za pomoci odborné technické literatury od autora Jana Uhláře: *Technická ochrana objektů 3. díl*, Radomíra Ščurka: *Biometrické metody identifikace osob v bezpečnostní praxi* a Jána Ivanky: *Mechanické zábranné systémy*. Práce dále pojednává o tom, jak důležitá je spolupráce s dalšími systémy jako jsou elektronické zabezpečovací systémy, připojení na pult centralizované ochrany nebo požární signalizace. V této část se čtenář dozví, že se systémem pro kontrolu vstupu se setkává prakticky každý den u svého počítače nebo chytrého telefonu

V návaznosti na uvedenou problematiku je v druhé části práce popsán praktický příklad možného zabezpečení fiktivní firmy. Cílem této části je návrh možného zabezpečení malé firmy se zakomponovaným systémem pro kontrolu vstupu a dalšími prvky mechanických zábranných systémů, elektronických zabezpečovacích systému a požární ochrany. Zabezpečení bude provedeno za využití standardních zařízení dostupných na trhu, používaných pro vyšší stupeň zabezpečení objektu a v poslední řadě bude vytvořen finanční návrh řešení.

2 Systém kontroly vstupu

Systém kontroly vstupu je určen primárně k ochraně objektů, pozemků nebo jiných zařízeních před neoprávněným přístupem osob. Má primárně bezpečnostní charakter a je nedílnou součástí bezpečnostních systémů a zařízení. Největší rozkvět v oblasti je zaznamenán v 90. letech 20. století, a to příčinou začleněním moderních informačních technologií a posílen tak lidský faktor při kontrole osob vstupujících do chráněného objektu nebo prostoru.

Definice bezpečnosti vychází z latinského slova Securitas /sine cura + tutus/, který v Českém jazyce znamená bezstarostnost, bezpečnost, jistotu ale i duševní pokoj, ochranu či zabezpečení. Mezi základní pojmy k bezpečnosti však patří bezpečnost, hrozba a riziko. Přesnou definici je těžké určit, protože ji každý jedinec vnímá subjektivně. [1, 2]

Bezpečnostní definice podle Hofreitera zní: *„Z hlediska reálného (a realistického) hodnocení bezpečnosti můžeme bezpečnost definovat jako takový stav bezpečnostní situace, činitelů a procesů tento stav ovlivňujících, jenž zajišťuje příznivé podmínky pro existenci, přetrvání, plnění požadovaných funkcí a rozvoj každého referenčního objektu.“*[3]

Systém kontroly vstupu je používán zpravidla tam, kde je zapotřebí zabránit přístupu nepovolaným osobám k citlivým informacím, prostorům či předmětům. K těmto se řadí hlavně objekty policie, vězeňské služby, armády, celní správy, určených prostor nemocnic, ale také trezorové prostory, kanceláře managementu firem apod., nemusí však vždy jít o tak důležité objekty. Systém kontroly vstupu, který je spolehlivý, a přesto levný si dnes může zajistit například bytový nebo rodinný dům, který povolí vstup jen jejich majitelům či nájemníkům. Dále různá sportoviště, kdy je povolen vstup jen v různých časových intervalech na základě členství. Systém kontroly vstupu dnes zajišťuje i prostý přístup do moderních chytrých telefonů nebo počítačů. Kontrolou vstupu je tedy snaha docílit přístupu pouze oprávněným osobám k chráněným objektům, prostorům, zařízením nebo informacím na základě jednoznačně přidělených přístupových práv. Systém kontroly vstupu může být dále využit i jako docházkový systém, který je schopen sbírat informace o časovém úseku, případně i o důvodu průchodu místem kontroly k dalšímu

[1] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 63.
[2] HOFREITER, Ladislav. *MANAŽMENT OCHRANY OBJEKTOV*. vydavateľstvo Žilinskej univerzity: vydavateľské centrum ŽU, 2015, s. 13.
[3] LUKÁŠ, Luděk. Teorie bezpečnosti I. Zlín: Radim Bučavčík – VeRBuM, 2017, s 19.

zpracování nebo zpětné kontrole. Oba systémy bývají často propojeny a vytvářejí tímto integrovaný identifikační systém kontroly vstupu. Podobné systémy se například využívají v mateřských nebo základních školách, kde na základě přiložení čipu systém rozpozná, že jde o rodiče konkrétního dítěte, které učitel následně pošle ke vchodu do školy, nebo rodiče vpustí do prostoru školy. Jedná se o tzv. Bellhop systém.

V dnešním světě již dominují ve funkci kontroly vstupu automatické elektronické vstupní systémy, které nahradily klasické metody, které jsou prováděny za pomoci lidského faktoru, tedy strážných, vrátných, policistů apod., kteří kontrolují identifikační prvky s nositelem identifikátoru. Automatické elektronické systémy a klasické metody se dají však kombinovat a tím zlepšit bezpečnost. Podstatnou výhodou automatizovaného systému oproti lidskému faktoru je pravidelná finanční náročnost. Automatizovaný systém je třeba udržovat a má větší počáteční náklady, ale člověka je nutné vyškolit, vycvičit, pořídit vhodnou výstroj, výzbroj a pravidelně platit. Přesto se oba faktory vyplatí kombinovat a tím docílit maximální efektivity.

Běžné metody kontroly identity nedokážou zajistit bezpečnou identifikaci uživatelů v dostatečné míře z důvodu, že existuje možnost použití odcizeného průkazu, násilím vynuceného bezpečnostního kódu k neoprávněnému přístupu do prostoru, nebo k informacím, které umožní elektronické systémy obejít.

Podstatným prvkem pro bezpečný vstup je přidělení oprávnění ke vstupu podle prostorových, časových a personálních dispozic ve vztahu ke konkrétní osobě, jež je vybavena svým identifikačním prvkem. Systém tímto umožňuje sledování pohybu osob po objektu, vyhledávání současné polohy osob a další aplikace od nejjednoduššího snímacího zařízení bez evidence, až po ucelený, propracovaný systém evidence s vyhodnocením, analýzou a napojením na další bezpečnostní systémy[4, 5, 6]

Základními normami pro systém kontroly vstupu jsou:

[4] UHLÁŘ, Jan. *Technická ochrana objektů*. Praha: Vydavatelství PA ČR, 2005, s. 16-17.
[5] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 63.
[6] HOFREITER, Ladislav. *MANAŽMENT OCHRANY OBJEKTOV*. vydavateľstvo Žilinskej univerzity: vydavateľské centrum ŽU, 2015, s. 188.

1. ČSN EN 60839–11-1 Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty. [7]

2. ČSN EN 60839–11-2 Poplachové a elektronické bezpečnostní systémy – Část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace. [8]

3. ČSN EN 60839–11-5 Poplachové a elektronické bezpečnostní systémy – Část 11-5: Elektronické systémy kontroly vstupu – komunikační protokol řízení přístupu (OSDP)[9]

4. ČSN EN 60839–11-31 Poplachové a elektronické bezpečnostní systémy – Část 11-31: Elektronické systémy kontroly vstupu – Implementace IP interoperability na základě webových služeb – Základní specifikace[10]

5. ČSN EN 60839–11-32 Poplachové a elektronické bezpečnostní systémy – Část 11-32: Elektronické systémy kontroly vstupu – Implementace IP interoperability na základě webových služeb – Specifikace systému kontroly vstupu [11]

[7] *ČSN EN 60839-11-1 (334593) Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty* [online]. Česká republika, 2014 [cit. 2021-03-07]. Dostupné z: http://www.technicke-normy-csn.cz/334593-csn-en-60839-11-1_4_94585.html.

[8] *ČSN EN 60839-11-2 (334593) Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace* [online]. Česká Republika, 2016 [cit. 2021-03-07]. Dostupné z: http://www.technicke-normy-csn.cz/334593-csn-en-60839-11-2_4_99323.html.

[9] *ČSN EN IEC 60839-11-5 (334593) Poplachové a elektronické bezpečnostní systémy - Část 11-5: Elektronické systémy kontroly vstupu - Komunikační protokol řízení přístupu (OSDP)* [online]. Česká Republika, 2021 [cit. 2021-03-07]. Dostupné z: http://www.technicke-normy-csn.cz/334593-csn-en-iec-60839-11-5_4_511317.html.

[10] *ČSN EN 60839-11-31 Poplachové a elektronické bezpečnostní systémy - Část 11-31: Elektronické systémy kontroly vstupu - Implementace IP interoperability na základě webových služeb - Základní specifikace* [online]. Česká republika, 2017 [cit. 2021-03-14]. Dostupné z: http://www.technicke-normy-csn.cz/334593-csn-en-60839-11-31_4_502234.html.

[11] *ČSN EN 60839-11-32 Poplachové a elektronické bezpečnostní systémy - Část 11-32: Elektronické systémy kontroly vstupu - Implementace IP interoperability na základě webových služeb - Specifikace systému kontroly vstupu* [online]. Česká republika, 2017 [cit. 2021-03-14]. Dostupné z: http://www.technicke-normy-csn.cz/334593-csn-en-60839-11-32_4_502235.html.

6. ČSN EN 50130-4 ED. 2 Poplachové systémy – část 4: Elektronická kompatibilita – Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, poplachových zabezpečovacích a tísňových systémů a systémů CCTV, kontroly vstupu a přivolání pomoci.[12]

7. ČSN EN 50130–5 ED.2 Poplachové systémy – Část 5: Metody zkoušek vlivu prostředí.[13]

Základními prvky automatizované identifikace systému pro kontrolu vstupu do objektu je sestaven z následujících částí:

1) Identifikační prvek

2) Snímací zařízení

3) Řídící jednotka

4) Centrální jednotka

5) Blokovací zařízení

6) Jednotka zápisu [14]

[12] *ČSN EN 50130-4 ED.2 Poplachové systémy - Část 4: Elektromagnetická kompatibilita - Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, poplachových zabezpečovacích a tísňových systémů a systémů CCTV, kontroly vstupu a přivolání pomoci* [online]. Česká republika, 2012 [cit. 2021-03-14]. Dostupné z: http://www.technicke-normy-csn.cz/334590-csn-en-50130-4-ed-2_4_90572.html.

[13] *ČSN EN 50130-5 ED.2 Poplachové systémy - Část 5: Metody zkoušek vlivu prostředí* [online]. Česká republika, 2012 [cit. 2021-03-14]. Dostupné z: http://www.technicke-normy-csn.cz/334590-csn-en-50130-5-ed-2_4_90570.html.

[14] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 63-64.

2.1 Identifikační prvek

Identifikační prvek je nosič určité informace, která je důležitá pro oprávněný vstup po jejím předložení nebo jejím rozpoznáním. Identifikačních prvků je velké množství typů, které dělíme na kontaktní a nekontaktní. Nosičem informace může být cokoliv od biometrických rysů, jako je otisk prstu, oční sítnice, hlas nebo jiný nosič informace, jako čipová karta, magnetická karta apod. Nosič informace musí odpovídat zvolené identifikační technologii podle konkrétních podmínek. Identifikační prvek je obvykle přímo provázán k objektu identifikace. Objekty identifikace dále dělíme na následující:

1) Osoba vlastní identifikační prvek

2) Osoba disponuje znalostí kódu

3) Osoba disponuje biometrickými rysy [15, 16]

2.1.1 Osoba vlastní identifikační prvek

Do této kategorie patří prvky typu karta, přívěsek apod., kterými se jednotlivé osoby prokazují elektronickému systému nebo vrátnému. Každý tento prvek je jedinečný a je vázán s konkrétní osobou. Podle principu nosiče je dělíme na magnetické identifikační karty, optické identifikační karty s čárovým kódem, indukční identifikační karty a čipové identifikační prvky.[17]

2.1.1.1. Magnetické identifikační karty

Klasický prvek ve formě plastové karty (kreditní karty), na které je nanesen proužek magnetického nosiče, který obsahuje všechny údaje včetně oprávnění. Informace jsou čteny pomocí nahrávací hlavy protažením karty štěrbinou. Bezpečnost u tohoto prvku není velká z důvodu snadné čitelnosti a možnosti vytvoření duplikátu.

Proto je bezpečnost doplněna o druhou identifikaci, zpravidla znalostí kódu PIN (Personal identification Number). Magnetický proužek karty je náchylný na rychlé mechanické opotřebení, či může dojít k poškození dat vystavením silnému magnetickému poli. Magnetický proužek obsahuje dvě nebo tři datové stopy.

[15] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. 4-5.
[16] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 64.
[17] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 64-65.

První dvě stopy slouží pouze pro čtení informací a na třetí stopu lze informace i zapisovat. Tuto třetí stopu využívají např. banky pro zaznamenání různých údajů[18, 19]

Obrázek č. 1 – *Karta s magnetickým proužkem*

zdroj: https://www.apluscard.cz/inpage/magneticke-karty/

2.1.1.2 Identifikační karty s čárovým kódem

Čárový kód je řada vertikálních čar o různé tloušťce a vzdálenostmi mezi nimi. Existuje mnoho kombinací čar a mezer. Funkčnost prvku spočívá v naskenování čárového kódu snímacím zařízením. V minulosti zařízení fungovala na základě vysílání infračervených paprsků. Infračervený paprsek funguje způsobem, kdy černé pruhy paprsek záření absorbují a bílé jej naopak odrazí zpět. Foto sensor přijímá zpět odražené světlo a převádí jej na elektrický signál. Signál je slabý pro mezery a silnější pro pruhy. Dekódováním skenerem se data přenesou ve standardním formátu do počítače. V dnešním světě stačí pro naskenování čárového kódu i klasický fotoaparát.

Každý čárový kód obsahuje spouštěcí znak, kontrolní součet, zadanou informaci a končící znak. Řazení těchto čar musí mít logickou posloupnost. V dnešní době se používá více než padesát druhů čárových kódů. Nejčastěji používaným čárovým kódem je osmi nebo třináctimístný kód. Proti zneužití může být čárový kód opatřen PVC folií s ochrannou maskovací vrstvou, nebo nanesením maskovacího laku, který propouští pravě jen paprsky infračerveného záření a tím je chráněn před okopírováním.

[18] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 65.
[19] Karty s magnetickým pruhem [online]. 2010 [cit. 2021-01-03]. Dostupné z WWW: http://pandatron.cz/?535&karty_s_magnetickym_pruhem.

Čárový kód je ze 40. let 20. století, a byl vynalezen Američanem Normanem Joseph Woodlandem na základě snahy urychlit fronty u pokladen velkého obchodního řetězce, kde se dosud čárový kód využívá nejvíce. Novější verzí čárového kódu je tzv. QR kód, nebo kruhový kód.[20, 21]

Obrázek č. 2 – *Karta s čárovým kódem*

zdroj: https://www.perfectcards.cz/nase-produkty/hlavni-typy/karty-s-carovym-kodem

2.1.1.3 Indukční identifikační karty

Jedná se zpravidla o kartu klasického rozměru kreditní karty, tedy 85,6 x 54 mm z plastového materiálu. Technologie karty funguje na základě elektromagnetické indukce. V tomto nosiči je informace zakódována v podobě přesně umístěných vodivých ploch, zabudovanými rezonančními obvody nebo děrovanými kovovými destičkami. Prvek reaguje na elektromagnetické pole snímače. Vzdálenost závisí na síle elektromagnetického pole. Reakcí se rozumí změna v elektromagnetickém poli, která je následně vyhodnocena snímačem a informace převedena do datové podoby ke zpracování.

2.1.1.4 Čipové identifikační prvky

Čipové identifikační prvky mají informaci uloženou v paměťovém čipu. Tento čip je zalisován do různých nosičů, jako je karta, štítek nebo přívěsek. Čip reaguje na blízkost nebo kontakt se snímačem, kdy tímto dojde k jeho přečtení nebo zápisu informací k dalšímu zpracování. Čipové nosiče postupně nahrazují nosiče indukční a magnetické a

[20] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, 65-66.
[21] Kodys-Čárový kód [online]. 2009 [cit. 2021-01-16]. Dostupné z WWW: http://www.kodys.cz/carovy-kod.html.

jsou v dnešním světě pro člověka nedílnou součástí každodenního života, ať už zaplacením pomocí debetní/kreditní karty, nebo nákupu jízdenky ve voze MHD. Čipové identifikační prvky jsou stále vylepšovány a jsou známy také svojí spolehlivostí a bezpečností. Čipové identifikační prvky dělíme na dotykové, které je nutné fyzicky přiložit ke snímači, a dají se kombinovat s jinými prvky, jako např. Magnetickým proužkem, a bezdotykové, které fungují na základě radiofrekvenční identifikaci a stačí je přiložit ke snímacímu zařízení na vzdálenost několika centimetrů až metrů. Výhodou u bezkontaktního nosiče je, že nemusí přijít k fyzickému kontaktu se snímačem a dá se použít třeba i skrytě. Dosah záleží na systému antén, zpravidla od 20 mm do 200 cm. Čip u kontaktního i bezkontaktního nosiče je založen na 64-bitovém kódu a používá se jako průkaz jednoznačné identifikace. [22]

Obrázek č. 3 – *Čipová identifikační karta*

https://cardhouse.cz/cs/eshop/plastove-karty/infineon-sle-5542-cipova-karta-smart

2.1.2 Osoba disponuje znalostí kódu

Osoba si zapamatuje zpravidla číselný kód/pin, který nosí v paměti. Při vstupu, např. do počítače nebo objektu, tento kód zadá pomocí klávesnice do vstupního systému. Systém následně porovná oprávněnost vstupu a při správném zadání hesla a dostatečném oprávnění odblokuje přístupové překážky, jako uzamčenou obrazovku či mechanické zábranné systémy. Přidělení kódu dělíme na skupinové, kdy v tomto případě existuje jen jeden kód, který zná jen určitá skupina lidí, např. ze zaměstnání nebo bytového domu. Nevýhoda skupinového kódu je, že nelze provést zpětnou kontrolu, který člověk vstoupil nebo vystoupil z objektu. Další skupinou znalostí kódu je individuální. Toto znamená, že každý jedinec má svůj vlastní unikátní kód. U tohoto způsobu je možné zpětně zjistit časový harmonogram příchodů a odchodů osoby.

[22] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 66-70.

Mezi výhody znalostí kódu patří, že jej nelze ztratit, lze snadno měnit, může být předán písemně i telefonicky a umožňuje signalizovat nátlakové stavy. Mezi nevýhody patří však fakt, že si jej musí osoba pamatovat, neidentifikuje jednoznačně oprávněnou osobu, vyžaduje ruční zadání, lze kód získat pod nátlakem. Z tohoto důvodu se tento prvek často kombinuje.[23]

2.1.3 Osoba disponuje biometrickými rysy

Biometrické rysy jsou unikátní na každé životní formě. Slovo biometrie je složeno ze dvou řeckých slov „BIOS“ a „METRON“. BIOS znamená „život“ a METRON znamená „měřit, měření“ Tento vědní obor se zabývá zkoumáním živých bytostí, primárně však člověka, a to jeho anatomických, fyziologických vlastností, ale také jeho chování.

Biometrika tedy využívá jedinečných tělesných znaků pro identifikaci osoby. Výhodou této identifikace je, že si oprávněná osoba nemusí pamatovat heslo, nebo s sebou nosit identifikační prvek. Biometrická identifikační metoda je jednou z nejmladších identifikačních systémů. Je rychlou a velmi přesnou metodou pro identifikaci jedince a není ani příliš nákladná. Její výhodou je, že se biometrické rysy během života nemění, nelze je ukrást, nebo velmi těžce a nelze je zapomenout.

Podstatou systému je porovnání již uloženého biometrického rysu s osobou, která se pokouší o vstup do chráněného objektu. Kombinací vícero rysů se zvyšuje bezpečnost daného systému. Systém pro vstup funguje zpravidla způsobem verifikace, což znamená ověření totožnosti, kdy při tomto se zpravidla používá identifikační prvek (např. čipová karta), nebo znalost kódu a následným sejmutím biometrického údaje se identita osoby potvrdí s předem uloženým vzorem. Toto samozřejmě platí i v kombinaci čipové karty a následným zadáním kódu pinu). Samotné systémy pracují s mnoha biometrickými rysy, nejběžnějšími jsou však otisky prstů, geometrie ruky, struktura žil na zápěstí ruky, oční sítnice, oční duhovka, geometrie tváře, lidský hlas, dynamika podpisu a lidská DNA.

Hlavní výhody používání biometrie jsou následující:

a) Univerzálnost – každá osoba je nositelem biometrických údajů.

b) Jedinečnost – neexistují dvě osoby, které by měli shodné biometrické údaje.

[23] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 70.

c) Permanence – biometrické údaje osoby jsou v průběhu jejího života takřka neměnné.

d) Jednoduchost – biometrické údaje jsou jednoduché a přesné.

e) Přijatelnost – snímání biometrických údajů je nenáročné a je uživatelsky jednoduché.

f) Vysoký podíl spolehlivosti – biometrické údaje lze jen těžko duplikovat.

g) Rychlost

h) Praktičnost – biometrické údaje nelze ztratit a nelze je přenášet. (vyjma násilí).

Nevýhody biometrie:

a) Uchovávání citlivých údajů o osobě.

b) Systém nemusí vpustit osobu, u které proběhly mírné změny biometrických údajů. [24, 25]

2.2 Snímací zařízení

Snímací zařízení, také známé jako čtecí zařízení, nebo zkráceně jen čtečky je hardware, který disponuje softwarem pro dekódování informací z identifikátoru. Snímací zařízení jsou rozdělena podle druhu použitého identifikátoru na:

- zařízení určená pro identifikátor – předmět (čtečka)
- pro identifikátor kódu – klávesnice
- pro identifikátor biometrie – snímač biometrického znaku

Snímací zařízení musí odpovídat danému typu nebo typům identifikačních prvků. Jedná se tedy např. o čtečky otisků prstů, klávesnice, mikrofony apod. V dnešní době může být použita klávesnice dotyková, u které je možné náhodné generování čísel, a tak je tedy možné zabránit opsání kódu ze strany nepovolané osoby. Základní zásadou pro snímací zařízení je odolnost proti vnějším vlivům a sabotážní odolnost proti vniknutí ze strany cizích osob. Zároveň by snímač měl být uživatelsky přívětivý. Vhodné je jednotlivé metody kombinovat, dobrým příkladem je bankomat, do kterého je po vložení nebo bezkontaktním předložením debetní nebo kreditní karty zadat pin kód karty. Prvek pin kódu v tomto případě znemožní pachateli kartu zneužít.

[24] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 71-72.
[25] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. 14-19.

Snímací zařízení jsou při vhodném systémovém nastavení a vybavení schopny mimo kontrolu vstupů a jiných událostí jako např. odmítnutí fungovat, jako docházkový systém. Dále umožňují úsporu času např. výpočtem pracovní doby jednotlivých zaměstnanců. Všechny uvedené informace mohou být zaneseny do celkové databáze a spolupracovat s účetními systémy.

Snímací zařízení mohou být propojeny i s počítačem s monitorem, na kterém se při každém vstupu může vygenerovat fotografie vlastníka identifikátoru a v případě pokusu o vstup neoprávněné osoby se zcizeným identifikátorem může obsluha na vrátnici zabránit vstupu neoprávněné osobě. Nejznámějšími identifikačními prvky s biometrií jsou otisky prstů, geometrie ruky, struktura žil na zápěstí ruky, oční sítnice, oční duhovka, geometrie tváře, lidský hlas, dynamika podpisu a lidská DNA.[26]

2.2.1 Otisky prstů

V anglickém jazyce tzv. fingerprinting. Jedná se o jednu z nejznámějších biometrických metod vůbec patřící do skupiny daktyloskopických identifikací. Tato metoda se pro identifikaci používá nejdéle ze všech. Snímače otisků prstů osoby jsou založeny na elektronickém snímání otisků prstů a jsou začleňovány do technických zařízení pomocí senzorů na fyzikální bázi. Snímače otisků prstů dělíme na kontaktní nebo bezkontaktní.

a) Kontaktní snímače zahrnují mnoho způsobů, jak otisk prstu sejmout. Nejstarší a klasickou metodou, která se také používá ve forenzní vědě, tedy používanou policií při vyšetřování, je obtisknutí prstů potřenými inkoustem na papír. Prst se na papíře roluje, aby se tímto získal obtisk celého prstu, nejlépe v rozmezí od jednoho kraje nehtu ke druhému kraji nehtu. Daktyloskopie jako taková představuje vědu – nauku o obrazcích papilárních linií na polštářcích dlaně nebo chodidel lidí. Papilární linie jsou u každého jedinečné, určité shodné vzorce však vyhledat, lze Dále se k sejmutí otisků prstů dají použít senzory optické nebo kapacitní. Optické fungují na základě laserového paprsku, který zespodu osvětluje povrch prstu, který je ve fyzickém kontaktu s průhlednou destičkou. Množství odráženého světla zpět záleží na četnosti a hloubce papilárních linií v 3D. Při snímání otisků formou 2D je zvýšené riziko přijetí falsifikátu. Rizikem optických metod může být špatná kvalita znečištěním otisku nebo sklíčka. Toto může

[26] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. 8.

vzniknout kvůli příliš vysoké nebo nízké vlhkosti rukou, nebo pozůstatkem kožních tukových výpotků po předchozí osobě. Dále může schopnost identifikace ztížit práce, tedy opotřebení papilárních linií, síla přitlačení, kterou lze dojít k tzv. „slití“ papilárních linií. Další faktor ovlivňující funkci snímače může mít i zrnko prachu nebo zranění, které papilární linie vyhladí. Kapacitní senzory fungují pomocí měření elektrické kapacity. Snímač je tvořen řádově 100 000 vodivých plošek, které jsou vůči sobě odizolovány. Dotykem kůže s papilárními liniemi se pojí jednotlivé plošky v závislosti na tvaru papilárních linií. Dále se měří napětí mezi jednotlivými vodivými ploškami a tímto vzniká obraz papilárních linií digitálně. Nevýhodou kapacitních senzorů můžou být různé nečistoty, zbytky potravin obsahující soli nebo cukry, které mění vodivost kůže. Stejně takto negativně v této metodě mohou fungovat krémy nebo balzámy.[27, 28]

Vstupy na principu otisků prstů fungují na základě předem uloženého vzoru v databázi. Tato metoda je zpravidla doprovázena vygenerováním a zadáním kódu PIN, nebo přiložením jiného nosiče např. čipové karty, a přiložený otisk prstů je pak porovnáván pouze s daným profilem, nikoliv s celou dostupnou databází. Tímto způsobem se celý proces urychluje. Pravděpodobnost, že by systém vpustil neregistrovanou osobu je menší než 0,0001 % a pravděpodobnost odmítnutí vstupu oprávněné osoby menší než 1 %. Tento systém je rozšířen v dnešní době na smartphonech, noteboocích, ovládání přístupu do objektů nebo parkovišť, vstup do počítače a ovládání trezorů. Může také sloužit k elektronickému podpisu.

[27] ČANDÍK, Marek. *Objektová bezpečnost II*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-217-3. s 44-47.
[28] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s 75-76.

b) Bezkontaktní snímače jsou oproti kontaktním oproštěny o fyzický kontakt se snímací plochou. Mezi bezkontaktní snímače patří optické a ultrazvukové. Optické snímače jsou podobné jako dotykové snímače. Světelný paprsek zvládne snímat otisk prstů na vzdálenost do 50 mm. Výhodou oproti kontaktnímu snímači je, že se tento neznečišťuje opakovaným používáním. Ultrazvukové snímače fungují na podobném principu jako optické, s tím rozdílem, že na povrch kůže dopadají zvukové vlny s vysokou frekvencí (MHz), které jsou následně vyhodnocovány. Tento princip lze přirovnat k lodním sonarům, který je však podstatně citlivější. Vysílaný zvuk má charakter velmi krátkých impulzů v řadě. Ty se následně odrazí od dlaně zpět a to se pak následně vyhodnocuje. Tento snímač má vysokou přesnost na 0,1 mm a je odolnější vůči falzifikátům. Tato metoda je dále vhodná i pro otisk celých dlaní. Systém snímače otisku prstu je velice uživatelsky přívětivý a není třeba žádného školení. Výskyt chyb je minimální a přesnost porovnání je vysoká. Bezpečnost prvku je vysoká a stabilita prvku dlouhodobá.[29, 30, 31]

Obrázek č. 4 – *otisk prstu*

Zdroj: https://fotky-foto.cz/fotobanka/fingerprintvector(4-2683823)

2.2.2 Geometrie ruky

Stejně jako jiné biometrické snímače identifikuje člověka přímo, bez žádného mezičlánku. V této metodě se vychází jako u předchozí metody z toho, že každý člověk má jedinečný tvar ruky, který se věkem nemění. Při snímání se detekují tři hlavní atributy a to délka, šířka a tloušťka ruky. Nevýhodou oproti snímači otisků prstů je jeho velikost a rychlost zpracovávaných dat. Snímač dlaně funguje na základě vložení dlaně do jednotlivých drážek (kolíků) a systém kontroluje správnou polohu ruky a při tomto ruku snímá digitální kamerou, která snímá trojrozměrně. Po měření ruky systém následně vyhodnotí s již uloženou šablonou, zpravidla do dvou vteřin. Tento snímač může fungovat

[29] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s 75.
[30] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. 34-40.
[31] Biometrie otisku prstu. *Biometrie otisku prstu* [online]. 2020, 2011–2020 [cit. 2021-02-28]. Dostupné z: WWW http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/.

i na principu, kdy nesnímá celou ruku, ale např. jen 2 prsty. Princip je jinak stejný jako u otisků prstů, to znamená, že zadáním kódu PIN se určí uživatelský profil, se kterým je následný sken porovnáván. Neporovnává tedy geometrii ruky s celou databází. Jedná se o jeden z nejbezpečnějších systémů kontroly vstupu. Systém je uživatelsky přívětivý jako u prvku otisku prstů. Chybovost u tohoto zařízení může nastat věkem, nebo úrazem nositele identifikátoru. Přesnost u tohoto systému je vysoká, obdobná jako u otisků prstů. Úroveň zabezpečení je však menší než u otisku prstů, drží se ve střední rovině.[32, 33, 34, 35]

2.2.3 Struktura žil na zápěstí

Jedná se o jednu z nejmladších metod k rozpoznání konkrétní osoby, datováno okolo roku 2000. Tato metoda je rovněž známá pro obtížnost falsifikace z důvodu, že jedna z podmínek může být teplá tekoucí krev a dále žilní řečiště není viditelné samotným okem bez podsvícení. Sama technologie je založena na prosvícení ruky speciální infračervenou kamerou, která vytvoří černobílý obraz struktury žil v zápěstí, který je opět jedinečným prvkem každého jednotlivce. Samotná struktura se s věkem prakticky nemění. Struktura žil v zápěstí byla vědecky testována i u jednovaječných dvojčat, kdy i zde byly rozdíly. Další výhodou tohoto identifikátoru je bezkontaktnost, tedy zachovává lepší hygienické podmínky pro užívání, a tedy i menší údržbu zařízení. Tato technologie opět zpravidla funguje na principu předem uloženého vzoru v databázi. Tento je zpravidla vygenerován zadáním kódu PIN, nebo přiložením jiného identifikátoru a žilní řečiště je pak porovnáváno pouze s daným profilem, nikoliv s celou databází. Tímto způsobem se celý proces urychluje. Samozřejmě je možné využít jen žilní řečiště ruky bez předem použitého identifikátoru, toto však identifikaci a vpuštění může zdržovat z důvodu velikosti dat či množství porovnávaných vzorků.

Po přiložení ruky nastávají čtyři fáze k dokončení obrazce k porovnání a to segmentace (tzn. ze snímaného zápěstí se vyselektuje jen ta část, která slouží k porovnávání v databázi). Druhá fáze je vyhlazení a redukce šumu (v této fázi probíhá vyhlazení obrazu a krevního řečiště v ní např. Gaussovským filtrem) další fází je tzv.

---

[32] HUSÁK, Miroslav, Tomáš TEPLÝ a Tomáš VÍTEK. Přístupové systémy (2). *Atp Journal* [online]. Praha, 2012, 31.5.2012, **2012**(3/2012) [cit. 2021-03-01]. Dostupné z: https://www.atpjournal.sk/budovy/rubriky/prehladove-clanky/pristupove-systemy-2.html?page_id=14878.

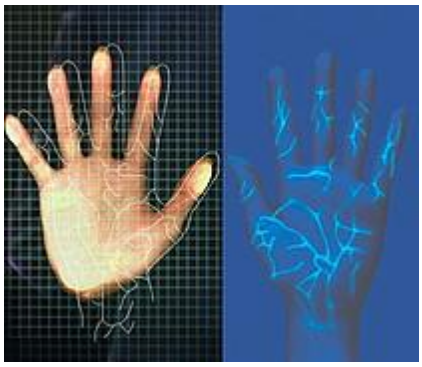
[33] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 78-79.

[34] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. 34-40.

[35] Biometrie krevního řečiště. Biometrie krevního řečiště [online]. 2020, 2011–2020 [cit. 2020-03-26]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/krevnireciste/.

Lokální pruhování (v této fázi dochází k oddělení vzoru řečiště z nasnímaného zápěstí k porovnání s databází). Poslední fází je postprocessing, kdy dochází k závěrečným úpravám pro verifikaci.[36, 37, 38]

Obrázek č. 5 *Geometrie ruky a struktura žil na zápěstí*



zdroj: http://www.biometricke-ctecky.cz/biometriky/krevni-reciste/

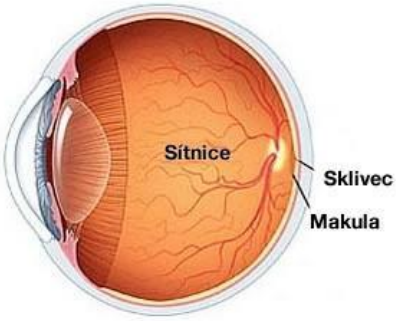
2.2.4 Oční sítnice

Snímač oční sítnice představuje jeden z nejbezpečnějších a nejpřesnějších systémů vůbec. Přesnost přijatého vzorku dosahuje 99,9999 %, výskyt chyby je tedy minimální. Svojí přesností a spolehlivostí předčí i například otisky prstů. Systém funguje podobně jako sken žilního řečiště ruky, tedy snímá řečiště cévek v oční sítnici, která nejsou pouhým okem viditelné. Pro zviditelnění se používá LED dioda s infračerveným zářením, které není pro oko závadné. Pro úspěšnou identifikaci je potřeba zaostřit na konkrétní bod ve čtečce. Obrázek je následně uložen do zpravidla 40bitového vzorku. Při snímání oční sítnice nevadí, když osoba nosí oční čočky, brýle je však nutno sundat. Tento systém je téměř nemožné obelstít. Falešné oči, transplantáty, kontaktní čočky nemohou narušit bezpečnost. Rychlost identifikace bývá kolem 1,5 vteřiny. Použitelnost snímače je složitější než u otisku prstů a proces identifikace může narušit mnoho faktorů od vlhkosti oka po nemoci.

[36] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 78.
[37] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. 26-30.
[38] Biometrie krevního řečiště. *Biometrie krevního řečiště* [online]. 2020, 2011–2020 [cit. 2021-02-28]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/krevni-reciste/.

Výskyt chyb je zpravidla způsoben nošením brýlí. Přesnost porovnání je vyšší než u otisku prstů. Úroveň zabezpečení je u tohoto prvku vysoká a vydrží dlouhodobě, tzn, sítnice se nemění[39, 40, 41, 42]

Obrázek č. 6 – *Oční sítnice*



Zdroj: https://www.neovize.cz/lecba-onemocneni-sitnice-a-sklivce/sitnice-makula-sklivec/

2.2.5 Oční Duhovky

Tento systém identifikace je založen na snímání viditelné barevné části oka, tedy oční duhovky a její jedinečnosti. Oblast duhovky se v oku nachází okolo oční panenky. Jedinečná informace v duhovce je stabilizována a konečně vytvořena již v prvním roce života člověka a po celý život zůstává neměnná, pokud nedojde k jejímu fyzickému poškozením např. úrazem. Šance nalezení dvou naprosto shodných očních duhovek je 1050krát menší než nalezení shodných otisků prstů. Vzor duhovky je tvořen více než 240 vektory, které se používá k identifikaci, a tedy ji nejde napodobit žádnou známou technologií. Jedná se o další z bezkontaktních prvků a disponuje stejnými výhodami jako předchozí. Snímači nevadí kontaktní čočky ani brýle pod podmínkou, že nejsou znečištěny. Hodnota chybného vyhodnocení činí 0,00076 %. Vytvoření vzoru oční duhovky trvá přibližně 2 minuty, identifikace trvá kolem 2 vteřin. Bezpečnost tohoto

[39] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. 24-25.
[40] Biometrie oka. Biometrie oka [online]. 2020, 2011–2020 [cit. 2021-02-26]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oko/.
[41] HUSÁK, Miroslav, Tomáš TEPLÝ a Tomáš VÍTEK. Přístupové systémy (2). *Atp Journal* [online]. Praha, 2012, 31.5.2012, **2012**(3/2012) [cit. 2021-03-01]. Dostupné z: https://www.atpjournal.sk/budovy/rubriky/prehladove-clanky/pristupove-systemy-2.html?page_id=14878.
[42] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 78-79.

systému je jedna z nejbezpečnějších. Použití snímače je snadnější než u skenu oční sítnice, ale o něco složitější než u otisku prstu.

Chybovost je častější při špatném osvětlení. Přesnost je srovnatelná s oční sítnicí. Systém poskytuje velmi vysokou úroveň zabezpečení i dlouhodobou stabilitu.[43, 44, 45, 46]

Obrázek č. 7 – *oční duhovka*

Zdroj: http://www.biometricke-ctecky.cz/biometriky/oko/

2.2.6 Geometrie obličeje

Již od roku 1960 byly získány pozitivní výsledky při automatizovaném rozpoznávání lidského obličeje. Největší vývoj tento systém zaznamenal po leteckém teroristickém útoku 11. září 2001 v USA. Přesto však má nižší identifikační jednoznačnost oproti otiskům prstů nebo oční duhovky z důvodu, že se obličej s časem mění, nebo jej může měnit i teplota okolí zabarvením pokožky. Naopak výhodou je, že tato metoda funguje i na poměrně velkou vzdálenost. Rozpoznávání je založeno na srovnání obrazu z kamery s obrazem z databáze. K identifikaci většinou dochází vyhodnocením tvaru obličeje, a významných, snadno rozpoznatelných částí obličeje – ústa, nos, oči, obočí. Dále využívá vzájemné polohy těchto bodů, jako např. vzdálenost očí od sebe, nebo úhel mezi okem a špičkou nosu. Systémy na rozpoznávání tváře omezují možnost správného výběru osoby na třetinu všech možných kandidátů v případě, je-li tvář

[43] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. 23-24.
[44] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 79.
[45] Biometrie oka. Biometrie oka [online]. 2020, 2011–2020 [cit. 2021-02-26]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oko/.
[46] HUSÁK, Miroslav, Tomáš TEPLÝ a Tomáš VÍTEK. Přístupové systémy (2). *Atp Journal* [online]. Praha, 2012, 31.5.2012, **2012**(3/2012) [cit. 2021-03-01]. Dostupné z: https://www.atpjournal.sk/budovy/rubriky/prehladove-clanky/pristupove-systemy-2.html?page_id=14878.

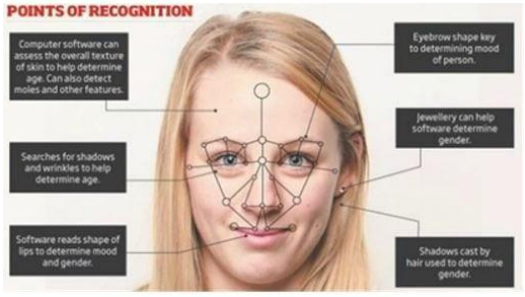
osoby sejmuta pod úhlem 45°. V tomto případě systém selhává až v 80 % případů. Vliv na spolehlivost mají i okolní podmínky jako osvětlení. První metodou snímaní obličeje je 2D metoda. Tato metoda využívá jen měření vzdálenosti v obličejové části. Tuto metodu je teoreticky možné obelstít dobře pořízenou fotografií. Další metodou je snímaní obličeje 3D. Tato funguje podobně jako metoda 2D, s tím rozdílem, že body jsou promítány do mřížky, která se promítá z jiného místa, než je umístěna samotná kamera. Tím dochází k měření vzdáleností obličejových bodů úhlově, ale také distančně (vzdáleností).

V praxi se systém rozpoznávání obličeje využívá na letištích a jiných frekventovaných místech. Systém vyhodnotí sejmutý obličej z kamery, která je zpravidla namířená přímo proti vchodu nebo východu objektu a vyhodnotí na kolik procent se podobá s osobou v databází, zpravidla s databází osob v pátrání. Následným porovnáním lidského faktoru fotografie z kamery s fotografií z databáze dojde k rozhodnutí, zda osobu fyzicky zkontrolovat, nebo zda se jedná o falešný poplach. V dnešní době je rozpoznávání obličeje nejvíce rozšířeno u moderních mobilních telefonů, kdy rozpoznání obličeje způsobí odemčení přístroje k používání. Tato metoda jde použít i u počítačů nebo notebooků, potřeba je však kamera, která zvládne obličej rozeznat a systém, který obličej porovná se šablonou. Systém rozpoznávání obličeje se dá kombinovat s jinými systémy a prvky systému kontroly vstupu do objektů.

Systém rozpoznávání obličeje bývá řazen do kategorie s umělou inteligencí. Při identifikaci systém dokáže rozeznat osobu s brýlemi i slunečními, nebo např. se třídenním strništěm nebo změnou účesu. Při dodržení ideálních podmínek je systém spolehlivý na 99,9 %. Použití systému je snadné, výskyt chyb se zvyšuje špatným osvětlením, věkem nebo brýlemi. Přesnost porovnání s uloženým vzorkem je vysoká. Úroveň zabezpečení průměrná, záleží na použití konkrétní technologie. Některé ze systémů jdou překonat za použití fotografie, ty se však již v dnešní době používají minimálně. Další výhodou je dlouhodobá stálost.[47, 48, 49]

[47] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 79-81.
[48] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. 20-23.
[49] Biometrie obličeje. *Biometrie obličeje* [online]. 2020, 2011–2020 [cit. 2021-02-28]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oblicej/.

Obrázek č. 8 – *geometrie obličeje*



Zdroj: https://www.svobodni.cz/clanky/hejduk-potrebujeme-biometricke-cestovni-doklady/

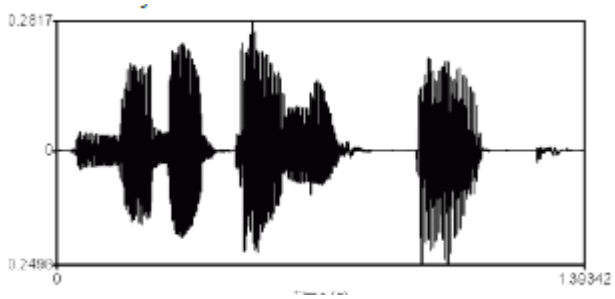
2.2.7 Lidský hlas

Tento systém je založen na bázi analýzy hlasu člověka, která je charakterizována akustickou strukturou (Amplitudově frekvenčním spektrem měnící se v čase), gramatikou a skladbou řeči. Pro vznik lidského hlasu jsou potřeba kmitající hlasivky, které jsou umístěny v hrtanu. Hlas je měnný, ale po delších časových úsecích. Technikou jsou následně měřeny základní složky hlasu, jako jsou hodnota frekvence, výška základního tónu, síla a doba tonace. Tento hlas přejde senzorem do digitální podoby, ve které jsou poté vidět markanty hlasu. Hlasové systémy následně porovnávají hlas s uloženou šablonou s tím, že se vybírá z celé databáze, nebo se osoba nejdříve identifikuje jiným identifikátorem např. čipovou kartou, kdy systém porovnává hlas jen s načteným profilem.

Hlasový systém pro identifikaci osob může být ovlivněn a nesprávně zamítnout přístup např. při nemoci, pozměněnými návyky. Proto se tento systém zpravidla používá jako druhotný – doplňkový. Přesto tento systém používají kriminalisté již několik desítek let pro detekci konkrétní osoby. Systém zpravidla funguje na definovaných slovech nebo větě, kterou člověk řekne do mikrofonu. Systém je uživatelsky přívětivý a není složité jej obsluhovat. Chybovost se zvyšuje s okolním hlukem, vlivem počasí nebo onemocněním uživatele např. nachlazením. Shoda se vzorkem v databázi je vysoká. Úroveň tohoto

zabezpečení je střední až vysoká, stále je horší než otisk prstu, oční duhovka nebo oční sítnice, časová stabilita je středně dlouhá.[50, 51, 52]

Obrázek č. 9 – *lidský hlas*



zdroj: https://is.muni.cz/elportal/estud/ff/ps09/fonetika/tisk_2009/ch06.html

2.2.8 Dynamika podpisu

Tato metoda se začala v praxi využívat už od roku 1977 a využívá kombinace jedinečného stylu a chování jednotlivce při podpisu. Zařízení na dynamický podpis se často zaměňuje se zařízením pro elektronický podpis. Z podpisu jako takového na papír lze zjistit, kde osoba více používá síly, nebo kde naopak přesahuje znaky, jeho tvar, jednotnost, což vše lze použít pro jednoznačnou identifikaci osoby. K digitalizaci se používají různé tablety, PDA nebo digitální tabulky. Základními dynamickými znaky jsou tlak, směr, síla, rychlost, čas a akcelerace. Při porovnání se systém zaměřuje na podobu podpisu podle vzoru a na dynamické vlastnosti jedince. Dle statistik je hodnota chybných přijetí 0,6 % a chybná odmítnutí na hodnotě 2 %. Identifikace zpravidla trvá do dvou vteřin. Vysoká snadnost použití, chybovost zpravidla při změně podpisu nebo nezvyku na dotykovou podložku. Přesnost porovnání se vzorkem je vysoká, úroveň zabezpečení je spíše střední, časová stabilita je spíše delší.[53, 54, 55]

---

[50]ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. 43-44.
[51] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 82.
[52] HUSÁK, Miroslav, Tomáš TEPLÝ a Tomáš VÍTEK. Přístupové systémy (2). *Atp Journal* [online]. Praha, 2012, 31.5.2012, **2012**(3/2012) [cit. 2021-03-01]. Dostupné z: https://www.atpjournal.sk/budovy/rubriky/prehladove-clanky/pristupove-systemy-2.html?page_id=14878.
[53] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 82-83.
[54] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. s.32.
[55] HUSÁK, Miroslav, Tomáš TEPLÝ a Tomáš VÍTEK. Přístupové systémy (2). *Atp Journal* [online]. Praha, 2012, 31.5.2012, **2012**(3/2012) [cit. 2021-03-01]. Dostupné z: https://www.atpjournal.sk/budovy/rubriky/prehladove-clanky/pristupove-systemy-2.html?page_id=14878.

2.2.9 DNA

Použití DNA (Deoxyribonukleová kyselina) při identifikaci osoby je používána zejména v policejní praxi, a to od doby druhé poloviny osmdesátých let 20 století. Její struktura je jedinečná pro každého jednotlivce kromě jednovaječných dvojčat. Vzorec DNA se s věkem nemění. Forma identifikace pomocí DNA je nejpřesnější metodou v dnešním světě. Jedná se však o metodu náročnou a zdlouhavou z důvodu, že k použitelnosti musí projít pěti fázemi, během kterých dochází k separaci celé spirály DNA, která je následně dále štěpena pomocí enzymu EcoR1, kdy po tomto jsou fragmenty prosévány do doby, než se získá použitelný řetězec vhodné a využitelné velikosti. Tento získaný fragment DNA je přenesen na nylonovou membránu a následně po přidání obarvených nebo radioaktivních genových sond je pořízen rentgenový snímek DNA, který je jeho otiskem. Tento otisk DNA se dá přirovnat např. k čárovému kódu a není tedy tolik složité jej převést do digitální podoby.

Informace DNA má široké spektrum využitelnosti, od testu otcovství po identifikaci těl. Do dnešní doby však nebyl vyvinut systém pro kontrolu přístupu v reálném čase z důvodu její náročnosti a časovému nároku. Metoda DNA má potenciál v 21. století, jako daktyloskopie ve 20. století. Reálné použití DNA pro systém kontroly vstupu není využitelný, neboť vyhodnocení trvá příliš dlouhou dobu, která je pro vstup podstatnou veličinou.[56, 57]

2.2.10 Ostatní biometrie

Biometrických metod, jak identifikovat člověka existuje samozřejmě více, ale nejsou již tak známé a rozšířené. Dalšími metodami může být např. způsob pohybu očí, povrchová topografie rohovky, tvaru článku prstu nebo tvaru pěsti, vrásnění článků prstů, behaviometriky, psaní na klávesnici, dynamiky chůze, pachu, ušního boltce, odrazem zvuku v ušním kanálku, tvaru a pohybu rtů apod...

Biometrie je v dnešním světě používána stále častěji, aniž by si to lidé uvědomovali. Biometrické údaje nebo vůbec systém kontroly vstupu do systémů používá každý člověk, který vlastní mobilní telefon nebo počítač. Již v dnešním světě je normální

[56] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 83.
[57] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. s.44.

odemykání mobilního telefonu pomocí otisku prstu nebo odemknutí za pomocí snímání obličeje.[58][59]

2.2.11 Kombinovaná biometrie

Pro zajištění maximální možné bezpečnosti proti vstupu neoprávněné osoby je vhodné kombinovat více metod biometrie zároveň. Zvýší se tak stupeň zabezpečení celého objektu a také kvalita vyhodnocení nosičů konkrétní osoby.

Jeden z možných procesů může být takový, že již při přiblížení k otvorové výplni a snímači, snímač zaznamená a porovná s databází obličej přibližující se osoby. Současně se na obrazovce snímače vygenerují čísla nebo písmena, ke kterým je v databázi vytvořen vzorek pro porovnání. Osoba následně heslo na obrazovce vysloví nahlas, a tímto se porovná hlasový vzorek a pohyb rtů. V tomto případě se se kombinují 3 metody identifikace a lze vyloučit cizí osobu s jistotou téměř 100 %.[60]

2.3 Řídící jednotka

Řídící jednotka je jedna ze základních pilířů moderních vstupních systémů. Tato jednotka třídí jednotlivé signály, která jsou vytvořeny snímači k identifikaci. Na základě dat (šablon) v paměti následně rozhoduje, zda se nosič informace dostatečně shoduje s uloženou šablonou a tímto porovnáním následně rozhodne o povolení ke vstupu nebo jeho odmítnutí. Odmítnutí zpravidla zablokuje vstup, tedy například neuvolní turniket, odmítne přístup k zabezpečeným datům, či dokonce dojde k vyhlášení skrytého nebo akustického poplachu. V opačném případě dojde k umožnění vstupu.

Dnešní řídící jednotky jsou ovládány mikroprocesory a díky svojí vlastní paměti následně rozhodují a vyhodnocují, zda osobu vpustit, či nikoliv. Tento automatizovaný postup je pro vstup klíčový.

Ze všech součástí kontroly vstupů je řídící jednotka tím nejdůležitějším. Řídící jednotka se konfiguruje za pomocí počítače a prověřuje oprávněnost vstupu, aktivuje ovládací prvky, zaznamenává narušení systému a zaznamenává jednotlivé identifikace a tím může zajistit případnou kontrolu docházky osob. Připojení PC však není vždy nezbytné,

[58] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 83-84.
[59] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. s. 25-50.
[60] Security magazín č.92.(listopad/prosinec 2009) Praha 1: Family media, ISSN 1210-8723 s. 12.

slouží hlavně k promazávání dat, přidávání a upravování šablon a rozsahu oprávnění do jednotlivých prostor.

Řídící jednotka je schopna ukládat údaje o počtu vstupů konkrétní osoby do konkrétních prostor. Proto je tento mechanismus praktický jako docházkový systém, případně i jako přehled zaměstnanců na pracovišti. Tento systém pro docházku je flexibilní a ve spolupráci s filtrací je možnost kontrolovat třeba jen jednoho zaměstnance, nebo kontrola jen jednoho vstupu.[61]

2.4 Centrální jednotka

Centrální jednotka řídí a monitoruje systém jako celek. Dále slouží k jeho programování, veškeré obsluze a jeho ovládání. V dnešní době moderní technologie ovládání centrální jednotky a její programování přebírají počítače se speciálním softwarem. Počítače také slouží k získávání dat z centrální jednotky, její diagnostice a opravě softwarových chyb, či k získání seznamu mechanických chyb.

Primárním úkolem centrální jednotky je sběr informací, jejich vyhodnocení a přiměřené reakce na ně v reálném čase. Sběr informací je prováděn formou online nebo offline. Výhoda online módu je permanentní sběr dat a možnost okamžité reakce systému nebo jeho obsluhy. Druhou formou je mód offline, kdy tento je řízen dálkově. V tomto módu jsou získané informace uloženy na místní paměťové zařízení. Data jsou velice variabilní s možností filtrace (osoba, konkrétní vstup). Další funkcí centrální jednotky by mělo být uživatelsky přívětivé a intuitivní ovládání i pro neodborné osoby[62]

2.5 Blokovací zařízení

Blokovací zařízení (mechanické zábranné systémy) jsou poslední nedílnou součástí všech vstupních systémů. Slouží k fyzickému zablokování osoby, která nemá oprávnění ke hlídanému vstupu, či se naopak uvolní, aby oprávněná osoba vstoupit mohla. Jedná se o prostředky chránící objekty anebo prostory před fyzickým vniknutím neoprávněných osob. Tyto prostředky mají za cíl odradit, znesnadnit nebo zabránit přístupu do chráněného objektu. Tomuto prostředku je třeba věnovat patřičnou pozornost, protože se jedná o hranici mezi chráněným objektem a volně přístupným terénem. Jedná se o různé typy motorických uvolňovačů, přídržných magnetů, elektromechanických uvolňovačů, turniketů apod. Blokovací zařízení jsou vybírána především podle objektu, do kterého mají být vsazena, podle stupně bezpečnosti, četnosti použití, funkčnosti a spolehlivosti.

[61] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 84.
[62] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 84-85.

Mezi blokovací zařízení patří hlavně brány, branky, závory, turnikety, a bezpečnostní propusti[63, 64, 65]

Každé blokovací zařízení je možno za nějaký čas překonat. Úkolem blokovacího zařízení je posunout tento čas na maximální možnou míru. Časový interval u blokovacího zařízení záleží na následujících faktorech:

- Kvalita
- Umístění
- Druh a kvalita použité techniky
- Preciznost
- Údržba[66]

2.5.1 Brány

Brány dělíme na otočné, výsuvné a posuvné. Posuvné dále na samonosné a brány pohybující se po kolejnici. Zpravidla se používá brána jedna, avšak u objektů, kde je vyžadována větší bezpečnost, jako jsou objekty Policie ČR, věznice, jaderné elektrárny apod., se využívá tzv. Dvoutaktní systém. Dvoutaktní systém funguje na principu překonání hranice objektu ve dvou taktech s kontrolovaným pohybem mezi bránami. V první řadě je povolenému vozidlu umožněn vjezd do prostoru mezi bránami. V tomto meziprostoru probíhá zvýšená kontrola ze strany personálu, kdy při splnění podmínek a požadavků pro vjezd, se otevře vnitřní brána do objektu. Brány v těchto případech bývají z důvodu bezpečnosti ovládány samostatným kontrolním systémem.

Brány se dále mohou dělit na automatické, či manuální. Veškeré součásti brány bývají přizpůsobeny vnějším vlivům např. materiálem, provedením a jejím umístěním. Povrchová úprava je zpravidla zinková s PVC povlakem, který může být v různém barevném provedení. Brána není vhodná u objektů, kde je hustý provoz, v tomto případě je vhodnější závora.[67, 68]

---

[63] IVANKA, Ján. *Mechanické zábranné systémy*. Univerzita Tomáše Bati ve Zlíně, 2014. ISBN 978-80-7454-427–9. s 63-64.
[64] UHLÁŘ, Jan. *Technická ochrana objektů 1. díl*. Praha: Vydavatelství PA ČR, 2004, s. 39.
[65] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II*. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, s. 92.
[66] ČERNÝ, Josef a Ján IVANKA. *Systemizace bezpečnostního průmyslu I*. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, s. 103.
[67] IVANKA, Ján. *Mechanické zábranné systémy*. Univerzita Tomáše Bati ve Zlíně, 2014, s. 128.
[68] UHLÁŘ, Jan. *Technická ochrana objektů 1. díl*. Praha: Vydavatelství PA ČR, 2004, s. 40.

2.5.2 Branky

Jedná se o jednokřídlý zábranný systém v obvodu plotu, který slouží k výstupu z a vstupu do objektu. Branka je zpravidla ze stejného materiálu, jako zbytek plotu. Bezpečnost musí být posílena prvky proti přelezení, např. navařenými ocelovými ostny, bodlovými doplňky nebo jinou vrcholovou zábranou. Rovněž musí být chráněna proti podhrabání vhodným materiálem.[69, 70]

2.5.3 Závory

Jedná se zpravidla o jednoramennou nebo dvouramennou páku, která je ovládána automaticky motorem, nebo manuálně klikou či za pomoci závaží. Páka může být jednou nebo vícekrát lomená. Závora má zejména kontrolní funkci, zpravidla nezabrání násilnému vniknutí do chráněného objektu. Proto jsou závory pod dohledem, protože u závory je možné ji podlézt, obejít nebo přeskočit. Její otevření obsluhuje osoba, nebo je otevření automatizováno, např. po přiložení čipové karty ke čtečce. Ke zvýšení bezpečnosti závory se používají další prvky např. hřebové ochrany, nebo jinými prvky zastavující vozidla.

Hřbetová bariéra slouží k zamezení vniknutí nebo úniku kolových vozidel z nebo do chráněného objektu. Vyskytuje se u vrat ve vnitřní části objektu. Tato ochrana představuje maximální zabezpečení v tomto směru. Mobilním řešením hřbetové ochrany jsou zastavovací pásy. Tento mobilní prostředek je používán v největší míře policií České republiky.[71, 72]

2.5.4 Turnikety

Turnikety patří do kategorie mechanické zábrany pro osoby, které oddělují zóny velkých i malých areálů. Turnikety mají za úkol přerušit nárazový proud lidí, tento rozmělnit a přeměnit jej na postupný. Tím že se proud osob stane postupným, stane se tak lépe kontrolovatelným. Turnikety dělíme na nízké (výška od 90 cm do 120 cm) a vysoké (výška nad 120 cm).

Nízké turnikety mají tu nevýhodu, že je lze přelézt. Proto se zpravidla umisťují na místa, kde se nachází vrátnice a turniket je tak ze strany vrátného kontrolovaný. U nízkého turniketu se používají zpravidla modely tříramenné zábrany, nízkého otočného kříže nebo

[69] IVANKA, Ján. *Mechanické zábranné systémy*. Univerzita Tomáše Bati ve Zlíně, 2014, s 128.
[70] UHLÁŘ, Jan. *Technická ochrana objektů 1. díl*. Praha: Vydavatelství PA ČR, 2004, s. 39-40.
[71] IVANKA, Ján. *Mechanické zábranné systémy*. Univerzita Tomáše Bati ve Zlíně, 2014, s. 129.
[72] UHLÁŘ, Jan. *Technická ochrana objektů 1. díl*. Praha: Vydavatelství PA ČR, 2004. s. 41-42.

nízké výsuvné zábrany. U nízkého turniketu se používají různé materiály, zpravidla se však jedná o kov, sklo, PVC, ale i dřevo. Materiál je závislý na okolním prostředí.

Vysoké turnikety jsou z bezpečnostního hlediska lepší, ale nákladnější než turnikety nízké. Další výhodou vysokých turniketů je jejich samostatnost, tedy nemusí být pod stálým dohledem, protože jsou samy o sobě neprůchozí. Vysoké turnikety jsou zpravidla tvořeny otočným křížem o takové hustotě, aby nešly prolézt skrz. Kříž je tvořen od dvou do čtyř segmentů, které však musí být tvořeny takovým způsobem, aby jím prošla jen jedna osoba najednou. Materiál je použit v kombinaci bezpečnosti (odolnost proti mechanickému poškození) a běžného opotřebení (odolnost vzhledem k častému používání a vlivům počasí).[73, 74]

2.5.5 Bezpečnostní propusti

Bezpečnostní propusti se používají u prostor s nutnou vysokou ochranou (trezor banky, trezor jaderných elektráren, výroba platebních karet apod.). Jedná se o kabinu, jejíž stěny jsou tvořeny silnostěnnými ocelovými panely se dveřmi kruhového tvaru, které jsou automatizované z důvodu jejich hmotnosti. Tyto dveře umožňují vstup zpravidla jen jedné osobě v daný okamžik díky váhovému detektoru a dvoutaktovému systému postupně se otevírajících dveří. Dveře mívají záložní zdroj energie pro případný výpadek elektrického proudu, který zajistí dalších až 200 vstupů.[75, 76]

2.5.6 Jiné vstupní jednotky

Do této kategorie spadají nekonvenční (nezvyklé) otvorové výplně sloužící pro vstup do objektu, jako jsou kolektory, větrací šachty, vzduchotechniky, kanalizace, stoky apod.). U těchto objektů je rovněž důležité, aby byly řádně zabezpečeny odpovídající otvorovou výplní (dveře, poklop) s možností kvalitního uzamčení. Podceněním bezpečnosti to může pro objekt znamenat slabý bod, který by mohl použít možný pachatel pro neoprávněný vstup do objektu, nebo způsobit zranitelnost objektu. V případě využití visacího zámku, musí tento být opatřen a chráněn speciálním krytem proti překonání. Důležité je, aby byl visací zámek vytvrzen třmeny s tloušťkou alespoň 12 mm. Samotný visací zámek, a vůbec celá otvorová výplň se musí pravidelně kontrolovat ze strany ostrahy fyzicky, nebo vhodně umístěným kamerovým systémem, zda nedošlo k jeho

[73] IVANKA, Ján. *Mechanické zábranné systémy*. Univerzita Tomáše Bati ve Zlíně, 2014, s. 129.
[74] UHLÁŘ, Jan. *Technická ochrana objektů 1. díl*. Praha: Vydavatelství PA ČR, 2004, s. 43-45.
[75] IVANKA, Ján. *Mechanické zábranné systémy*. Univerzita Tomáše Bati ve Zlíně, 2014, s. 120-128.
[76] UHLÁŘ, Jan. *Technická ochrana objektů 1. díl*. Praha: Vydavatelství PA ČR, 2004, s.45.

porušení. Otvorovou výplň je vhodné pojistit i vhodným elektrickým zabezpečovacím systémem, který každý pokus o narušení toto z detekuje a následně elektronickým systémem signalizuje na vyhodnocovací jednotku (velín ostrahy, vrátnice, mobilní telefon ostrahy apod.), a tímto docílí včasného zákroku ze strany ostrahy nebo policie a zabránit tak dokonání trestného činu.[77]

2.6 Odebírací zařízení

Na výjezdových nebo odchodových místech mohou být nainstalované tzv. „pohlcovače“ identifikačních karet, zpravidla návštěv. Jedná se o kryt, do kterého je umístěn bezkontaktní snímač, do jehož krytu osoba vloží svou kartu, která jím propadne do zásobníku a zajistí otevření mechanické zábrany pro výjezd nebo odchod. Osoba tak o kartu přijde, a nemůže ji tedy z budovy nebo parkoviště odnést. Často je toto zařízení instalováno u parkovišť.[78]

2.7 Jednotka zápisu

Jednotka zápisu je zařízení, které umožňuje zápis informací, jako jsou jméno, příjmení, rozsah oprávnění apod., do identifikačního prvku (čipové nebo jiné karty). Jednotka zápisu může, ale nemusí být, součástí celého systému pro kontrolu vstupu.[79]

[77] UHLÁŘ, Jan. *Technická ochrana objektů 1. díl*. Praha: Vydavatelství PA ČR, 2004, s. 46.
[78] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 85.
[79] UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, s. 85.

3 Zabezpečení objektu systémem pro kontrolu vstupu

3.1 Charakteristika objektu

Tato část bakalářské práce uvádí příklad možného zabezpečení objektu, který je vybaven systémem pro kontrolu vstupu s dalšími prvky ochrany a zabezpečení. Zabezpečení bude zaměřeno na mechanické zábranné systémy, systémem pro kontrolu vstupu a další elektronické zabezpečovací systémy pro plášťovou a prostorovou ochranu. Pro tento příklad byla vybrána fiktivní společnost zabývající se finančním plánováním a účetnictvím pro fyzické a právnické osoby se sídlem v Plzni, v klasické zástavbové oblasti. Výhodou sídla je, že v nejbližším okolí jsou složky IZS, které v případě zapnutí alarmu reagují s nízkým dojezdovým časem. Uvedené zabezpečení bude následně vyčísleno podle aktuální nabídky společnosti. Důvodem pro vytvoření zabezpečení se zakomponovaným systémem pro kontrolu vstupu je plánovaná celková rekonstrukce.

Obrázek č. 10 – *náhled budovy*

Zdroj: autor

V přízemí budovy se bude nacházet vrátnice s podatelnou, čekárna, toalety, posilovna, archiv a garáž pro tři osobní vozidla. V prvním patře se budou nacházet

3 kanceláře, kancelář sekretářky, kancelář ředitele, toalety, serverovna, zasedací místnost a kuchyňka. Kanceláře budou kompletně vybaveny nábytkem, počítači a dalším hardwarem. Důvodem pro zabudování systému pro kontrolu vstupu do budovy je omezení pohybu v horním patře a archivu v souvislosti s ochranou dat ve fyzické podobě a uložených elektronických dat v počítačích před případným odcizením, zneužitím, pozměněním či smazáním. V objektu vykonává pracovní činnost 20 osob, kdy pracovní doba je vytyčena pondělí–pátek od 07:00 do 15:00 hodin. Vstup do objektu bude možný hlavním vchodem nebo garážovými vraty. (viz. obr.)

Obrázek č. 11 – *vstupní dveře*

Zdroj autor

Obrázek č. 12 – *garážová vrata*

Zdroj: autor

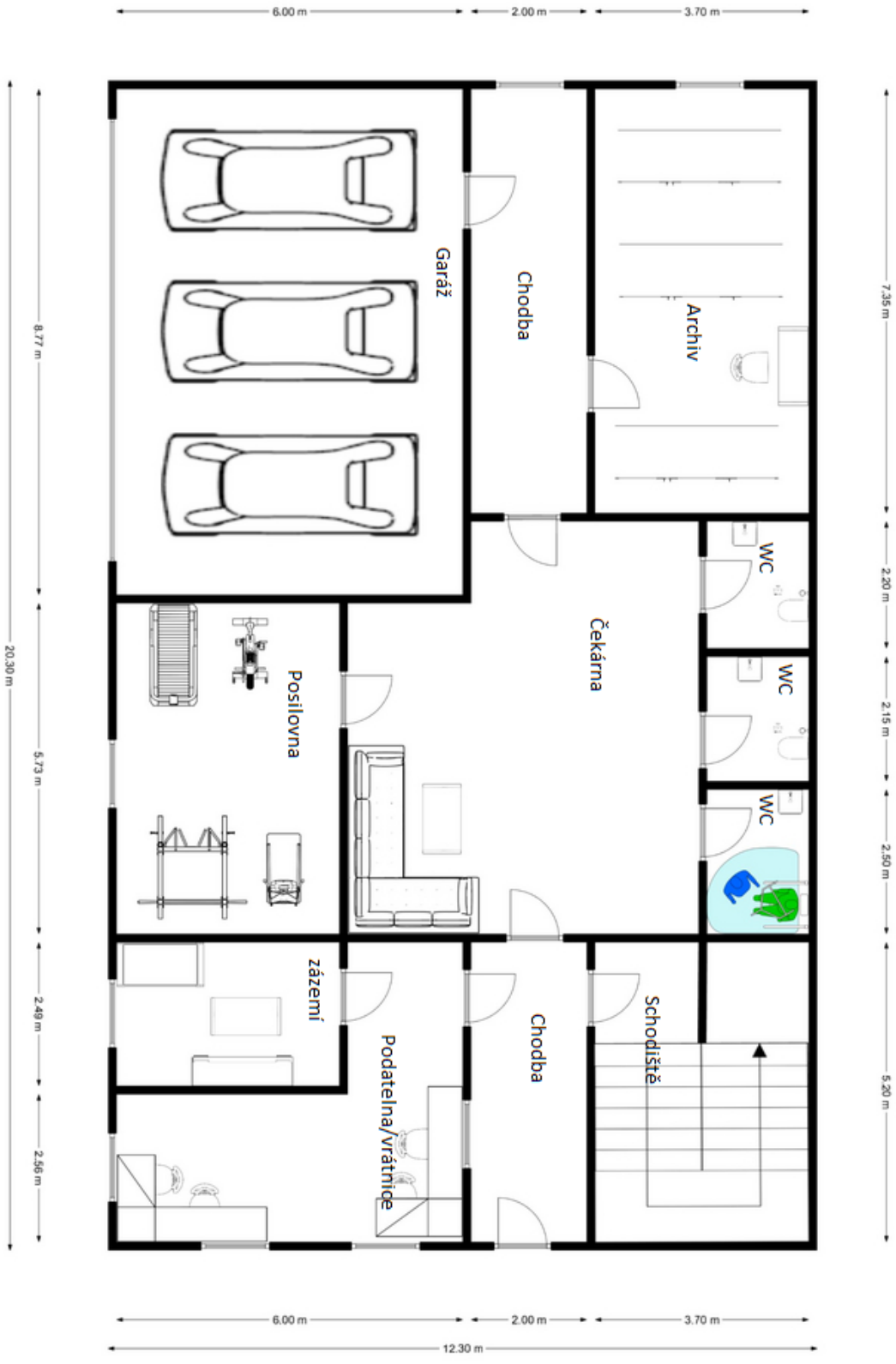
Návrh zabezpečení se systémem kontroly vstupu bude založen na použití kombinace mechanického zábranného systému, který slouží k zabránění vniknutí neoprávněné osoby do objektu. Systému kontroly vstupu v kombinaci elektrického zabezpečení zejména pohybu osob v objektu, indikace požáru a vyrozumění pultu centralizované ochrany, či majitele objektu.

Nejčastějšími cestami k vloupání do objektu jsou otvorové výplně objektu, tzn. Dveře, okna, vrata apod. Dveřní výplň lze překonat destruktivní formou odvrtáním nebo rozlomením cylindrické vložky, kde prevence před touto metodou je potřeba dveří s třídou bezpečnosti 4. Druhou formou překonání dveří může být vyháčkováním nebo tzv. Bumpingem. Jedná se o nedestruktivní metody pro překonání dveří. Při vyháčkování se pomocí planžet srovnávají stavítka tak, jak za normálních okolností srovná do roviny jen příslušný klíč. Při srovnání stavítek následně jde cylindrickou odemknout. Proti této metodě lze bránit pouze bezpečnostní cylindrickou vložkou třídy 3 a vyšší. Pro metodu Bumping je potřeba speciálního „klíče“ pro daný typ cylindrické vložky. Úderem do takového klíče kladívkem dojde ke srovnání stavítek, a tím potom zámek odemknout. Proti této metodě se lze bránit pouze bezpečnostní cylindrickou vložkou třídy 3 a vyšší.

Důležité je vědět, že v případě profesionála neodolají žádné dveře ani cylindrická vložka, a je jen otázkou času, než dveře pachatel překoná. Bezpečnostní dveře a kvalitní cylindrická vložka zastaví pouze pachatele, který není dostatečně zkušený a nemá k překonání potřebné nástroje. Proto je vhodné mít dveře zabezpečené tak, aby čidla tento pokus rozpoznala a předala informaci na pult centralizované ochrany nebo majiteli objektu, který zasáhne dříve, než pachatel dveře překoná.

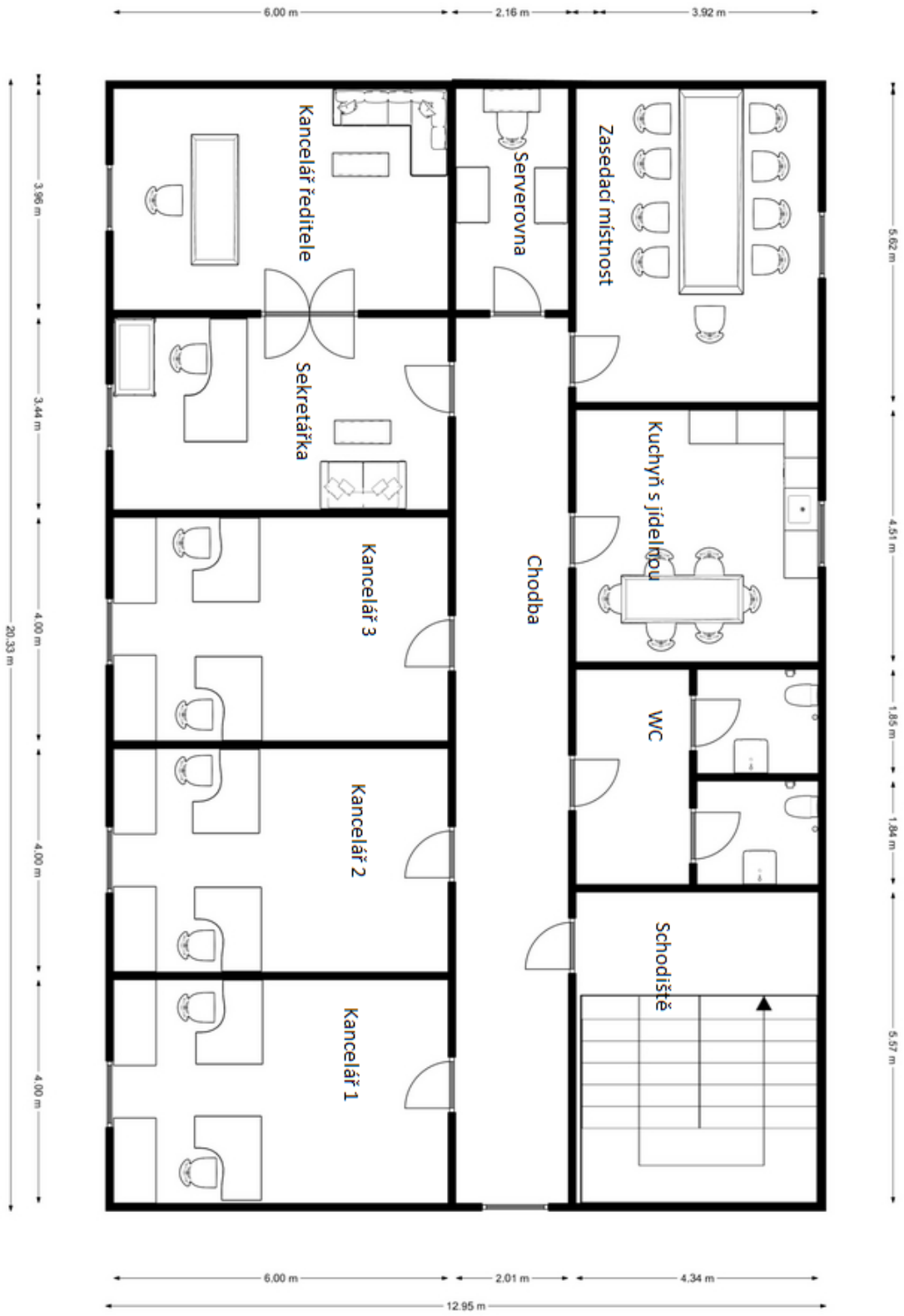
3.2 Půdorys objektu

Obrázek č. 13 -*Půdorys přízemí budovy:*



Zdroj: autor

Obrázek č. 14 - *Půdorys prvního patra.*



Zdroj: autor

3.3 Mechanický zábranný systém pláště budovy

3.3.1 Vchodové dveře

Pro příklad zabezpečení vchodu budou použity dveře od firmy D&L Mont, s.r.o. Dveře GERDA Star 60 RC4 jsou protipožární celokovové, bezpečnostní, vyztužené a zateplené dveře, které nabízejí bezpečnostní třídu 4 se zvýšenou odolností proti vloupání RC4. Dveře jsou opatřeny zadlabávacím zámkem značky SHERLOCK s elektrickým zámkem a bzučákem. Zámek je chráněný kovovým krytem zámku, který je přivařen k plášti dveřím. Naléhací lišta dveří je v prostoru zámku a v místě jistících bodů zpevněná kovovou výztuhou svařenou s oběma plášti dveří. Dveře jsou dále opatřeny třemi závěsy a třemi trny proti vloupání. Dveře mají celkem sedmnáct bezpečnostních čepů, z toho je čtrnáct aktivních a tři pasivní. Tloušťka dveřního křídla je 60 mm. Dveře jsou vsazeny do bezpečnostních zárubní značky Sherlock. Dveře splňují normu ČSN - EN 1627:2012 tedy jsou odolné proti vloupání. Dveře jsou dodávané s panoramatickým kukátkem a nerezovým prahem. Dveře jsou z vnitřní strany objektu dále jištěny nůžkovými mřížemi, které tak po překonání dveří tvoří další překážku.

Dveře jsou dále opatřeny terminálem JA-154E. Jedná se o přístupový modul s klávesnicí, LCD displejem a RFID přijímačem čipových karet pro identifikaci. Jedná se o bezdrátový modul, který je napájen čtyřmi kusy alkalických baterií. Typická životnost baterie se pohybuje mezi 1–2 roky, podle použitého nastavení. V tomto případě je však modul opatřen i síťovým zdrojem DE06-12, který zajišťuje stálý chod modulu i bez použití baterií, které potom slouží jako záložní zdroj. Snímač pracuje v komunikačním pásmu typické pro protokol Jablotronu, tedy 868,1 MHz. RFID se pohybuje na 125 KHz. Rozměry snímacího zařízení jsou 102 x 145 x 33 mm o hmotnosti 350 g. Modul splňuje klasifikace druhého stupně a splňuje normy dle ČSN EN 50131-1, ČSN EN 50131-3, ČSN EN 50131-5-3. Tento snímač je umístěn ve venkovním prostoru a zabudován ve stěně budovy.

Pro přístup do objektu je tedy třeba přiložit čipovou kartu nebo přívěsek ke čtečce a po načtení uživatele zadat osobní číselný kód, až po kterém se dveře automaticky odemknou a „odbzučí“ uživateli. V tomto případě byly použity čipové RFID přívěsky JA-194J-RE a bezkontaktní čipové karty JA-100. Oba tyto prvky operují na frekvenci 125 KHz a jsou opatřeny jedinečným kódováním firmy Jablotron. V případě výpadku elektrické energie lze dveře otevřít klíčem. Zamykání je možné nastavit se zpožděním 0/3/6/9 sekund po dovření dveří. Aby zámkový čep nevyjel ze zámku dříve, než dojde k

úplnému dovření dveří, jsou futra osazena kováním se zabudovaným magnetem, který pokud není proti druhému magnetickému kontaktu elektromechanického zámku, tak nedojde k zamčení a vyjetí zamykacího trnu.

3.3.2 Garážová vrata

Pro zabezpečení prostoru garáže budou vybrána sekční garážová vrata od firmy LOMAX & Co s.r.o. Tyto se skládají z několika panelů (sekcí), které se za pomoci torzních pružin pohybují vodicími kolejnicemi. ovládané pomocí elektropohonu. V případě výpadku elektrického proudu lze vrata ovládat i ručně. Mimo bezpečnosti, mají tato garážová vrata výhodu v jejich skladnosti. Přesto jsou vrata robustní a všechny motory brání proti vypáčení, a to i v případě výpadku elektrické energie. Při výpadku proudu se dá bezpečnost zvýšit dalšími mechanickými prvky jako je např. blokovací zarážka. Vrata jsou opatřena senzory, které při naražení do překážky tuto detekují a zasunou se automaticky zpět. Zabrání tím škodě na zdraví či majetku. Vrata jsou dále opatřena záložním zdrojem BACK UP 100, které umožní otevírat a zavírat vrata i při výpadku elektrického proudu.

3.3.3 Okna a mříže

Objekt je osazen klasickými plastovými okny, která jsou doplněná o cylindrickou vložku a jdou uzamykat v zavřené poloze i v poloze na ventilaci. Cylindrická vložka oken je třídy 2. Okna jsou z venku dále opatřena mříží, které jsou zabudovány přímo do budovy.

Okna jsou dále z vnitřní strany osazena čidly JA-182SH. Tento bezdrátový detektor otřesu nebo náklonu používá polovodičový tříosý akcelerometr s digitálním výstupem. Digitální zpracování v tomto případě předchází falešným poplachům. Detektor je napájen z lithiové baterie, která má životnost 2 roky. Detekovaný náklon je podle nastavení mezi 10° až 45°. Čidlo pracuje v komunikačním pásmu typické pro protokol Jablotronu, tedy 868,1 MHz. Rozměry čidla jsou 75 x 31 x 26 mm a splňuje druhý stupeň zabezpečení podle ČSN EN 50131-1 , ČSN EN 50131-5-3, ČSN CLC/TS 50131-2-8 a dále ČSN ETSI EN 300220, ČSN EN 50130-4, ČSN EN 55022, ČSN EN 60950-1.

3.3.4 Interiérové dveře do chráněných míst

V objektu se nacházejí místa, do kterých je striktně omezený přístup na základě udělených práv. Jedná se o archiv, serverovnu a dveře vedoucí ke schodišti v přízemí budovy. Tyto prostory jsou opatřeny dveřmi Bedex standard 2 od firmy D&L Mont, s.r.o.

Jedná se o dveře druhé bezpečnostní třídy RC2. Do konstrukce bezpečnostních dveří jsou použity pouze řádně certifikované komponenty a materiály tak, aby celkový výrobek uspěl v náročných zkouškách odolnosti proti vloupání. Tyto dveře jsou dále opatřeny terminálem JA-153E. Jedná se o přístupový modul s klávesnicí a RFID přijímačem čipových karet pro identifikaci. Jedná se o bezdrátový modul, který je napájen dvěma kusy alkalických baterií. Typická životnost baterie se pohybuje mezi 1–2 roky, a to podle použitého nastavení. V našem případě je však modul opatřen síťovým zdrojem DE06-12, který zajišťuje stálý chod modulu i bez použití baterií, které potom slouží jako záložní zdroj. Snímač pracuje v komunikačním pásmu typické pro protokol Jablotronu, tedy 868,1 MHz. RFID se pohybuje na 125 KHz. Rozměry snímacího zařízení je 102 x 96 x 33 mm o hmotnosti 200 g. Modul splňuje klasifikace druhého stupně a splňuje normy dle ČSN EN 50131-1, ČSN EN 50131-3, ČSN EN 50131-5-3.

Pro přístup do výše uvedených prostor je třeba přiložit čipovou kartu nebo přívěsek ke čtečce, která je zabudována do stěny budovy. Po načtení uživatele je třeba zadat osobní číselný kód, až po kterém se dveře automaticky odemknou a „odbzučí“ uživateli. V tomto případě byly použity čipové RFID přívěsky JA-194J-RE a bezkontaktní čipové karty JA-100. Oba tyto prvky operují na frekvenci 125 KHz a jsou opatřeny jedinečným kódováním firmy Jablotron.

3.3.5 Vnitřní ochrana

Ve vnitřním perimetru budovy, tedy ve všech místnostech a chodbách jsou zabudovaná bezdrátová pohybová čidla JA-150P. Tato jsou vhodná do chodeb i místností s funkcí smart watch pro potvrzování poplachů a následnému prodloužení životnosti baterie, která vydrží až dva roky. Čidlo je napájeno dvěma alkalickými bateriemi. Čidla pracují v komunikačním pásmu typické pro protokol Jablotronu, tedy 868,1 MHz. Z důvodu napájení z baterie jsou odolná vůči výpadku elektrické energie. V objektu se nachází celkem 18 čidel. Čidla splňují normy ČSN EN 50131-1 ed. 2+A1+A2, ČSN EN 50131-2-2, ČSN EN 50131-5-3+A1, ČSN EN 50131-6 ed. 2+A1, ČSN ETSI EN 300 220-1,-2, ČSN EN 50130-4 ed. 2+A1, ČSN EN 55032 ed. 2, ČSN EN 62368-1+A11, ČSN EN 50581, T 031.

Budova je dále vybavena detektory kouře a teplot se sirénou typu JA-151ST-A. Slouží k detekci požárního nebezpečí v interiéru obytných nebo komerčních budov. Jeho součástí je sirénka, která hlásí požární poplach jak z vlastního detektoru, tak z jiného požárního detektoru v systému. Detektor je napájen třemi alkalickými bateriemi a třemi

lithiovými bateriemi. Životnost baterií v detektoru je do tří let používání. V obejktu se nachází celkem 10 detektorů. Detektor splňuje normy ČSN EN 54-5, ČSN EN 54-7, ČSN EN 54-25, ČSN ETSI EN 300 220, ČSN EN 50130-4, ČSN EN 55022, ČSN EN 60950-1.

3.3.6 Ústředna

Komunikaci mezi čidly, detektory a dalšími moduly byla vybrána ústředna s LAN, GSM a rádiovým modulem typu JA-107KRY, která zároveň slouží jako řídící jednotka, centrální jednotka a jednotka zápisu objektu. Ústředna je napájena z elektrické sítě objektu a zároveň propojena s náhradním bezúdržbovým akumulátorem SA214-18, který v případě výpadku elektrické energie napájení převezme.

Popis Ústředny JA-107KRY

- až 120 bezdrátových a až 230 sběrnicových periferií
- až 600 uživatelů
- až 15 sekcí
- 64 vzájemně nezávislých kalendářních akcí
- 50 uživatelských SMS reportů
- 15 uživatelských hlasových reportů
- 5 nastavitelných PCO
- 5 volitelných protokolů pro PCO

Ústředna obsahuje:

- Rádiový modul JA-111R
- GSM/GPRS komunikátor JA-192Y

Ústředna dále nabízí funkce, např.:

- Údržba
- Režim den/noc

- Reakce zkrácený odchod
- Automatické zajištění
- Rozšířené funkce kalendáře

3.4 Použitý hardware

Pro návrh zabezpečení byly použity produkty firmy Jablotron alarms a. s., konkrétně systém s označením JABLOTRON 100+. Jedná se o nový produkt firmy s uživatelsky přívětivým rozhraním. Systém nabízí velké množství variant využití, vč. kontrolního či docházkového systému

Uvedený systém reaguje, pokud ve střeženém prostoru dojde k mechanickému narušení objektu (otřesu), naklonění hlídaného předmětu nebo pohyb osob v objektu. Systém se ovládá pomocí klávesnice výběrem příslušné volby a zadáním osobního kódu, nebo přiložením ovládacího RFID čipu či v kombinaci výše uvedeného. Kromě signalizace poplachu systém umožňuje ovládání dalších spotřebičů jako jsou el. brány, dveře, světlo, topení apod. Spolehlivost provozu zajišťuje záložní akumulátor, který vydrží překlenutí výpadku napájecího napětí dle použité kapacity po dobu v řádech hodin až dnů.

Certifikace Systému JABLOTRON 100+ je podle evropské normy EN 50131-1 zařazen do stupně zabezpečení č. 2. Údaje o stupni bezpečnosti jsou podstatné při jednání s pojišťovnou, kdy většina pojišťoven poskytuje při řádném zajištění objektu výhody na pojistném. Řádná certifikace systému a montáží je též podmínkou případné výplaty pojistné částky v plné výši, kdyby došlo ke škodě na majetku i přesto že je řádně zabezpečen. Připojení na pult centralizované ochrany nebo na mobilní telefon majitele je u tohoto systému doporučováno. Tento systém dále umožňuje mimo klasického elektronického zabezpečení také implementaci protipožární ochrany nebo systému chytré domácnosti.

RFID přívěsek nebo karta je přidělena každému zaměstnanci firmy, který má práva vstupu do firmy v době pracovní doby. Systém kontroly vstupu je spravován programem Vodasoft systém, který byl navržen pro malé a střední firmy, které využívají pro zabezpečení firmy EZS JABLOTRON 100 a vyšší s napojením na webovou samoobsluhu MyJABLOTRON. Kromě základní funkce střežení objektu lze díky možnostem nastavení PG výstupů rozšířit tento systém o sledování docházky zaměstnanců, což

umožní jednak kontrolu dodržování pracovní doby a zároveň slouží jako podklad pro splnění zákonné povinnosti o evidenci pracovní doby. Díky využití stávajícího systému JABLOTRON 100 jsou pořizovací náklady na docházkový systém minimální, na rozdíl od pořízení samostatného docházkového systému.

3.5 Kalkulace

Výše uvedené prvky mechanických zábranných systémů, elektrického zabezpečovacího systému a systém pro kontrolu vstupu je oceněn podle aktuálních ceníků pro rok 2021. Montážní práce v níže uvedené tabulce nejsou zohledněny.

Tabulka č. 1 – *kalkulace zabezpečení se systémem pro kontrolu vstupu*

Cenová kalkulace zabezpečení s SKV			
Název produktu	cena	množství	celkem
Ústředna s LAN, GSM a rádiovým modulem	11 320,00 Kč	1	11 320,00 Kč
Bezúdržbový akumulátor	1 150,00 Kč	1	1 150,00 Kč
Bezdrátový přístupový modul s displejem, klávesnicí a RFID	2 300,00 Kč	1	2 300,00 Kč
Síťový zdroj 12 V/0,5 A	266,00 Kč	4	1 064,00 Kč
Bezdrátový přístupový modul s klávesnicí a RFID	2 048,00 Kč	3	6 144,00 Kč
Bezdrátový detektor otřesu nebo náklonu	825,00 Kč	15	12 375,00 Kč
Lithiová baterie	52,00 Kč	15	780,00 Kč
Bezdrátový PIR detektor pohybu	1 419,00 Kč	18	25 542,00 Kč
Bezdrátový silový modul výstupů PG	1 121,00 Kč	3	3 363,00 Kč
Víceúčelová montážní krabice – střední velikost	307,00 Kč	3	921,00 Kč
Kombinovaný detektor kouře a teplot se sirénkou – bezdrátový	2 035,00 Kč	10	20 350,00 Kč
Alkalická baterie	11,00 Kč	128	1 408,00 Kč
El. zámek – bzučák	1 450,00 Kč	3	4 350,00 Kč
Mříž na okno	1 500,00 Kč	4	6 000,00 Kč
Nůžkové mříže – interiérové	3 400,00 Kč	1	3 400,00 Kč
GERDA Star 60 RC4 protipožární s novou bezpečnostní zárubní	27 223,00 Kč	1	27 223,00 Kč
Bedex Standard 2	15 013,00 Kč	3	45 039,00 Kč
Sekční garážová vrata Delta	29 900,00 Kč	1	29 900,00 Kč
RFID přívěsek červený	126,00 Kč	20	2 520,00 Kč
Přístupová karta RFID	81,00 Kč	10	810,00 Kč
Celkem bez DPH			205 959,00 Kč
DPH 21.00 %			43 251,39 Kč
Cena celkem s DPH			249 210,39 Kč

Zdroj: autor

4 Závěr

V dnešním světě je majetková trestná činnost nejrozšířenější ze všech trestných činností s nejmenším podílem objasněnosti. Metody pachatelů se stále rozvíjejí a proto je nutné se proti nim účinně bránit. Tato práce pojednává o možné prevenci proti takovým pachatelům, a to využitím systému pro kontrolu vstupu. Se systémem kontroly vstupu se setkáváme prakticky každý den, aniž bychom to vnímali. Systém je vhodný pro každé použití od zabezpečení mobilního telefonu po kontrolu pohybu osob v domě, nebo ve firmách všech velikostí. Systém kontroly vstupu umožňuje třídit pohyb osob v objektu a poskytovat informace, kde se zrovna nacházejí v reálném čase. Systém jako takový však nedokáže zabránit vstupu neoprávněné osoby samostatně. Nedílnou součástí systému kontroly vstupu jsou mechanické zábranné systémy a další systémy elektronického zabezpečení jako je alarm napojený na PCO nebo požární signalizace.

Práce představuje, co je systém pro kontrolu vstupu, jeho úkoly a důležitost kombinace s dalšími prvky zabezpečení. Cílem této práce bylo představit čtenáři strukturu systému pro kontrolu vstupu. Práce se podrobněji zabývá identifikačními metodami a prostředky identifikace osob, zejména biometrickou metodu identifikace, kterou jsou popsány nejčastější používané způsoby. V práci jsou dále podrobněji představené mechanické zábranné systémy, které jsou pro systém nezbytnou součástí.

V návaznosti na uvedenou problematiku bylo dalším cílem navrhnout možné zabezpečení malé firmy se zakomponovaným systémem pro kontrolu vstupu. Toto bylo provedeno za využití standardních zařízení dostupných na trhu, používaný pro vyšší stupeň zabezpečení. Objekt byl zabezpečen bezpečnostními dveřmi a vraty s mřížemi, ze kterých jsou tři opatřeny čtečkou RFID karty a klávesnicí pro zadání PIN. Všechna okna v objektu jsou hlídána detektory náklonu a otřesu. Dále je v objektu zabudováno celkem 18 pohybových čidel a 10 detektorů teploty a kouře. Všichni zaměstnanci firmy jsou vybaveni RFID prvkem, v tomto případě přívěskem nebo kartou. Celková kalkulace bez práce byla vyčíslena na 249 210,39,- Kč. Nejedná se o nejlevnější řešení, neboť je zde kladen důraz na maximální bezpečnost.

Cílem této práce bylo popsat systémy kontroly vstupů používané objekty a stanovit požadavky na tyto systémy. Problematika v této oblasti je dosti rozsáhlá. V práci je postupováno tak aby čtenář pochopil, jakým způsobem systém pracuje a jaké nabízí v současné době možnosti.

Seznam použitých zdrojů

Literární zdroje

1. ČANDÍK, Marek. *Objektová bezpečnost II*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 100 s. ISBN 80-7318-217-3.
2. ČERNÝ, Josef a Ján IVANKA. *Systemizace bezpečnostního průmyslu I*. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 135 s., ISBN 80-7318-402-8.
3. HOFREITER, Ladislav. *MANAŽMENT OCHRANY OBJEKTOV*. vydavateľstvo Žilinskej univerzity: vydavateľské centrum ŽU, 2015, 229 s., ISBN 978-80-554-1164-4.
4. IVANKA, Ján. *Mechanické zábranné systémy*. Univerzita Tomáše Bati ve Zlíně, 2014, 151 s., ISBN 978-80-7454-427–9.
5. LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II*. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s., ISBN 9788073186319.
6. LUKÁŠ, Luděk. Teorie bezpečnosti I. Zlín: Radim Bučavčík – VeRBuM, 2017, 220 s., ISBN 978-80-87500-89-7.
7. Security magazín č.92.(listopad/prosinec 2009) Praha 1: Family media, 68 s., ISSN 1210-8723
8. UHLÁŘ, Jan. *Technická ochrana objektů 1. díl*. Praha: Vydavatelství PA ČR, 2004, 179 s., ISBN 80-7251-172-6.
9. UHLÁŘ, Jan. *Technická ochrana objektů*. Praha: Vydavatelství PA ČR, 2005, 69 s., ISBN 8072511890.
10. UHLÁŘ, Jan. *Technická ochrana objektů 3.díl*. Praha: Vydavatelství PA ČR, 2006, 246 s., ISBN 80-7251-235-8.

Elektronické zdroje

1. Biometrie krevního řečiště. *Biometrie krevního řečiště* [online]. 2020, 2011–2020 [cit. 2021-02-28]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/krevni-reciste/

2. Biometrie obličeje. *Biometrie obličeje* [online]. 2020, 2011–2020 [cit. 2021-02-28]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oblicej/

3. Biometrie oka. *Biometrie oka* [online]. 2020, 2011–2020 [cit. 2021-02-28]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oko/

4. Biometrie otisku prstu. *Biometrie otisku prstu* [online]. 2020, 2011–2020 [cit. 2021-02-28]. Dostupné z: WWW http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/

5. *ČSN EN 60839-11-1 (334593) Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty* [online]. Česká republika, 2014 [cit. 2021-03-07]. Dostupné z: http://www.technicke-normy-csn.cz/334593-csn-en-60839-11-1_4_94585.html

6. *ČSN EN 60839-11-2 (334593) Poplachové a elektronické bezpečnostní systémy – Část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace* [online]. Česká republika, 2016 [cit. 2021-03-07]. Dostupné z: http://www.technicke-normy-csn.cz/334593-csn-en-60839-11-2_4_99323.html

7. ČSN EN IEC 60839-11-5 (334593) Poplachové a elektronické bezpečnostní systémy – Část 11-5: Elektronické systémy kontroly vstupu – Komunikační protokol řízení přístupu (OSDP) [online]. Česká republika, 2021 [cit. 2021-03-07]. Dostupné z: http://www.technicke-normy-csn.cz/334593-csn-en-iec-60839-11-5_4_511317.html

8. ČSN EN 60839-11-31 Poplachové a elektronické bezpečnostní systémy – Část 11-31: Elektronické systémy kontroly vstupu – Implementace IP interoperability na základě webových služeb – Základní specifikace [online]. Česká republika, 2017 [cit. 2021-03-14]. Dostupné z: http://www.technicke-normy-csn.cz/334593-

csn-en-60839-11-31_4_502234.html

9. ČSN EN 60839-11-32 Poplachové a elektronické bezpečnostní systémy – Část 11-32: Elektronické systémy kontroly vstupu – Implementace IP interoperability na základě webových služeb – Specifikace systému kontroly vstupu [online]. Česká republika, 2017 [cit. 2021-03-14]. Dostupné z: http://www.technicke-normy-csn.cz/334593-csn-en-60839-11-32_4_502235.html

10. ČSN EN 50130-4 ED.2 Poplachové systémy – Část 4: Elektromagnetická kompatibilita – Norma skupiny výrobků: Požadavky na odolnost komponentů požárních systémů, poplachových zabezpečovacích a tísňových systémů a systémů CCTV, kontroly vstupu a přivolání pomoci [online]. Česká republika, 2012 [cit. 2021-03-14]. Dostupné z: http://www.technicke-normy-csn.cz/334590-csn-en-50130-4-ed-2_4_90572.html

11. ČSN EN 50130-5 ED.2 Poplachové systémy – Část 5: Metody zkoušek vlivu prostředí [online]. Česká republika, 2012 [cit. 2021-03-14]. Dostupné z: http://www.technicke-normy-csn.cz/334590-csn-en-50130-5-ed-2_4_90570.html

12. HUSÁK, Miroslav, Tomáš TEPLÝ a Tomáš VÍTEK. Přístupové systémy (2). *Atp Journal* [online]. Praha, 2012, 31.5.2012, 2012(3/2012) [cit. 2021-03-01]. Dostupné z: https://www.atpjournal.sk/budovy/rubriky/prehladove-clanky/pristupove-systemy-2.html?page_id=14878

13. Karty s magnetickým pruhem [online]. 2010 [cit. 2021-01-03]. Dostupné z WWW: http://pandatron.cz/?535&karty_s_magnetickym_pruhem

14. Kodys-Čárový kód [online]. 2009 [cit. 2021-01-16]. Dostupné z WWW: http://www.kodys.cz/carovy-kod.html.

15. ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. 2008 [cit. 2021-01-22]. Dostupné z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf. Studijní text. VŠB TU Ostrava, Fakulta bezpečnostního inženýrství, Katedra bezpečnostního managementu, Oddělení bezpečnosti osob a majetku.

Seznam zkratek

EZS – Elektronický zabezpečovací systém

MZS – Mechanické zabezpečovací systémy

PC – Personal computer (osobní počítač)

PIN – Personal identification number (osobní identifikační číslo)

SKV – Systém kontroly vstupu

PCO – Pult centralizované ochrany

DNA – deoxyribonucleic acid

Seznam tabulek a grafů

Seznam obrázků