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

BAKALÁŘSKÁ PRÁCE

KOMPLEXNÍ ZABEZPEČENÍ OBJEKTU POMOCÍ ELEKTRONICKÝCH A BIOMETRICKÝCH ZABEZPEČOVACÍCH SYSTÉMŮ

Autor práce: Dominik Vaněček, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: Mgr. Bc. Radovan Sládek

Katedra: Katedra právních oborů a bezpečnostních studií

2022

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Dominik Vaněček DiS.

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

Název bakalářské práce: Komplexní zabezpečení objektu pomocí elektronických a biometrických zabezpečovacích systémů

Název bakalářské práce v anglickém jazyce: Comprehensive Security of the Building by using Electronic and Biometric Security Systems

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

Datum zadání bakalářské práce: Listopad 2021

Cíl bakalářské práce:

Hlavní cíl: Obecně charakterizovat aktuální technologie zabezpečovacích systémů, jejich metody a aplikace.

Vedlejší cíl: V rámci užšího praxeologického postihu vytvořit komplexní projekt zabezpečení pro vybraný objekt.

Student: Dominik Vaněček, DiS.	18.11.2021 *datum*	*podpis*
Vedoucí práce: Mgr. Bc. Radovan Sládek	18.11.2021 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	6.12.2021 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	8.12.2021 *datum*	*podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	14.12.2021 *datum*	*podpis*

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

Prohlašuji, že jsem bakalářskou práci vypracoval 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 vedoucího 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. Zároveň děkuji své rodině a přátelům, kteří mě podporovali po celou dobu studia.

ABSTRAKT

VANĚČEK, D. *Komplexní zabezpečení objektu pomocí elektronických a biometrických zabezpečovacích systémů: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2022. 69 s. Vedoucí bakalářské práce: Mgr. Bc. Radovan Sládek

Klíčová slova: zabezpečovací systémy, biometrie, zabezpečení objektu,

Tato bakalářská práce se zabývá teorií, funkcemi a možnostmi dostupných elektronických zabezpečovacích systémů a bezpečnostních systémů s prvky biometrie. Cílem práce je charakterizovat jednotlivé metody a funkce vybraných zabezpečovacích systémů a jejich komponentů. Druhým cílem práce je na vybraném objektu vytvořit bezpečnostní analýzu poukazující na nedostatky v ochraně objektu a na základě zjištěných informací vytvořit návrhy na zabezpečení a kontrolování pohybu osob. Tyto následně budou komparovány za účelem vydání doporučení pro instalaci.

ABSTRACT

VANĚČEK, D. *Comprehensive Security of the Building by using Electronic and Biometric Security Systems: Bachelor Thesis.* České Budějovice: The College of European and Regional Studies, 2022. 69 pp. Supervisor: Mgr. Bc. Radovan Sládek

Key words: security systems, biometrics, object security

This bachelor thesis deals with the theories, the functions and options of available electronics security systems and security systems with biometrics elements. The aim of the bachelor thesis is to characterize individual methods and functions of selected security systems and their components. The second aim of the thesis is to create a security analysis pointing to shortcomings in the protection on a selected object and make concepts of security and movement control systems based on the obtained information. These will then be compared in order to issue installation recommendations.

Obsah

Úvod

Každý člověk si v dnešní době chce zabezpečit svůj majetek a informace před zneužitím či odcizením. Samozřejmě tyto věci chce zabezpečit tím nejlepším a nejdostupnějším způsobem, a to dalo důvod, obzvlášť v posledních desítkách let pro rapidní vývoj elektronických zabezpečovacích systémů.

Dříve bylo možné svůj majetek chránit pouze mechanickými zábrannými systémy jako jsou zámky, ale tyto bezpečnostní prvky bylo a je možné s trochou nácviku a jednoduchým nářadím prolomit. Kvůli tomu se prvky zabezpečení zaměřily i na to, aby byl pachatel detekován a zadržen dříve než se k majetku, popřípadě informaci dostane.

Pro takové zabezpečení objektu, které dokáže detekovat pachatele a pošle majiteli zprávu, popřípadě rovnou zalarmuje bezpečnostní službu či policii, je potřeba zhotovit bezpečnostní analýzu objektu, ve které se vyhodnocuje rizikovost místa, slabé stránky objektu a podobné atributy. Na základě této analýzy lze vytvořit návrh bezpečnostního systému, který efektivně dokáže detekovat nepovolanou osobu.

Tato bakalářská práce si klade za cíl v první části charakterizovat nejnovější trendy a funkce elektronických zabezpečovacích systémů, způsoby používání systému kontroly vstupu a jeden z posledních milníků bezpečnostních systémů, a tím je zakomponování biometrie v těchto systémech. Závěrečná část práce obsahuje zhotovenou bezpečnostní analýzu vybraného objektu na základě, které jsou vypracovány návrhy bezpečnostního systému.

1 Cíl a metodika bakalářské práce

Bakalářská práce se zaobírá využitím elektronických zabezpečovacích systémů a bezpečnostních systémů s prvky biometrie. Jejím cílem je charakterizovat aktuální technologie těchto systémů, jejich metody a aplikaci. Dílčím cílem je, na vybraném objektu, vytvořit projekty zabezpečení, které by efektivně odradily útočníka od napadení objektu a zároveň kontrolovaly vstup osob. Tyto návrhy budou v závěrečné části komparovány s cílem doporučit jeden z nich pro vybraný objekt.

Samotná bakalářská práce je rozdělena do dvou částí. První část práce začíná kapitolou dva, která charakterizuje technologie elektronických zabezpečovacích systémů a definuje vybrané komponenty. Třetí kapitola má za cíl vysvětlit systém kontroly vstupu a poukázat na možnosti prostředků identifikace. Kapitola čtyři ukazuje možnosti použití biometrických prvků jako identifikátoru v bezpečnostních systémech.

V druhé části práce autor v kapitole pět na základě vlastního pozorování vytvoří bezpečnostní analýzu, díky které lze zjistit nedostatky v mechanickém a elektronickém zabezpečení objektu. V šesté kapitole je na základě analýzy vytvořen souhrn doporučení na zabezpečení objektu mechanickými zábrannými systémy, které jsou velice důležité pro správnou funkci elektronického zabezpečovacího systému a systému kontroly vstupu. Sedmá kapitola obsahuje dva návrhy s cenovou relací a podrobným popisem jednotlivých komponentů, které lze použít pro zabezpečení objektu. Závěrem je provedena komparace na základě, které autor jeden z návrhů doporučí.

2 Elektronické zabezpečovací systémy

Elektronické zabezpečovací systémy, dále jen EZS, patří do okruhu integrovaného bezpečnostního systému. Jedná se o systém skládající se z řady technických prvků, které jsou spolu navzájem propojeny. Struktura integrovaného bezpečnostního systému je tvořena z:

- mechanických zábranných systémů
- signalizačních prostředků a monitorovacích zařízení
- organizačních opatření a ostrahy[1]

Pokud mluvíme o druhém bodě, tedy o signalizačních prostředcích a monitorovacích zařízeních, mluvíme právě o EZS. Tyto prostředky monitorují prostředí a detekují možnosti narušení střeženého prostoru. V případě detekce narušitele systém zašle signál do řídícího centra a tím vyvolá poplach.

Je jasné, že EZS, jakožto technická ochrana nedokáže objekt samostatně ochránit, a proto musí být zakomponována do ostatních dvou systémů a má pouze podpůrnou funkci pro mechanické zábranné systémy a zvyšuje efektivnost fyzické ostrahy.[2]

Vytváření zabezpečovacího systému je pro každý objekt odlišné. Výběr technických prostředků pro zabezpečení závisí zejména na rizikovosti objektu a na tom, co investor od zabezpečovacího systému očekává. Stupně rizikovosti objektu se rozdělují do čtyř kategorií, jimiž jsou nízká, průměrná, vysoká a nejvyšší.

- nízká – V této kategorii jsou zahrnuty obytné budovy, malé provozovny a veškeré prostory s nízkou chráněnou hodnotou.
- průměrná – Zde se nacházejí větší provozovny, sklady, obchody a zařazení objektu do této kategorie je minimální podmínkou pro připojení EZS k pultu centralizované ochrany PČR.
- vysoká – Zde se jedná o objekty s vysokou chráněnou hodnotou jako jsou peněžní ústavy, sklady a výrobny zbraní, výrobny opiátů a galerie.
- nejvyšší – V poslední kategorii jsou objekty, které jsou buďto státní anebo jejich ochrana je pro stát a celkovou bezpečnost velice významná. Jedná se například o centrální úložny, atomové elektrárny nebo státní pokladny.[3]

[1] UHLÁŘ, Jan. *Technická ochrana objektů I. díl: Mechanické zábranné systémy* Praha, 2004. str. 13
[2] ČANDÍK, Marek. Objektová bezpečnost II. Zlín, 2004. str. 7-9

Očekávání investora jsou zejména znemožnit vniknutí do objektu a zabránit odcizení, poškození či zničení hodnot uschovaných uvnitř. Další doplňující požadavky jsou takové, které dokáží urychlit a zefektivnit odhalování trestné činnosti. Jedná se o:

- Preventivní funkci systému.
- Dokázat narušitele na místě zdržet dostatečně dlouhou dobu kvůli jeho dopadení.
- Poskytnutí důkazů pro usvědčení narušitele.

2.1 Legislativa elektronických zabezpečovacích systémů

EZS se podle aktuálních norem označují jako poplachové zabezpečovací a tísňové systémy. Existuje několik norem upravujících postup při projektování a následnou montáž EZS, avšak nejdůležitější jsou tyto dvě.

ČSN EN 50131-1 ed. 2 (334591) Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky

Tato norma specifikuje požadavky na provedení a vlastnosti instalovaných systémů.

V obsahu této normy jsou uvedeny:

- Termíny a definice
- Zkratky
- Systémové požadavky
- Propojování systémů
- Požadavky na funkčnost
- Ovládání
- Stupně zabezpečení
- Třídy prostředí[4]

ČSN CLC/TS 50131-7 (334591) Poplachové systémy - Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace

Obsahem normy jsou uvedeny:

---

[3] UHLÁŘ, Jan. *Technická ochrana objektů II. díl: Elektrické zabezpečovací systémy II*. Praha, 2005 str. 20-21

[4] ČSN EN 50131-1 ed. 2*: Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2015. Třídící znak. *334591*

- Termíny a definice
- Zkratky
- Návrh systému
- Montáž systému
- Prohlídky
- Funkční zkoušky
- Dokumentace a záznamy o provozu
- Údržba systému
- Opravy[5]

2.2 Struktura elektronických zabezpečovacích systémů

EZS je soubor prvků schopný dálkově opticky nebo akusticky signalizovat na určeném místě přítomnost, vstup nebo pokus o vstup narušitele do střežených objektů nebo prostorů.[6]

Plnohodnotný EZS se skládá z pěti základních komponentů, které jsou propojeny a vytváří tzv. zabezpečovací řetězec. Těmito komponenty jsou čidlo, ústředna, přenosové prostředky, signalizační zařízení a doplňková zařízení.

1. **Čidlo (detektor)** – jedná se o nejvíce rozmanitý komponent celého EZS. Dokáže detekovat narušení pomocí fyzikálních změn v prostředí. Příkladem mohou být otřesy při přelézání plotu nebo změna teploty ve sledovaném prostoru.
2. **Ústředna** – je jádro a mozek celého EZS, řídí celý systém a vyhodnocuje informace získané z ostatních komponentů. Po vyhodnocení stavu vysílá signál o poplachu.
3. **Přenosové prostředky –** zajišťují přenos informací mezi jednotlivými komponenty.
4. **Signalizační zařízení** – informují o detekci narušení. Nejčastěji se jedná o sirény či majáky.
5. **Doplňková zařízení –** jsou komponenty, kterými lze ovládat a nastavovat celý systém EZS např. klávesnice, dotykové displeje a počítače.

[5] ČSN CLC/TS 50131-7*:* Poplachové systémy - Poplachové zabezpečovací a tísňové systémy – Část 7. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Třídící znak. *334591*
[6] UHLÁŘ, Jan. *Technická ochrana objektů II. díl: Elektrické zabezpečovací systémy II*. Praha, 2005 str. 24

Bez těchto komponentů by systém EZS nemohl stoprocentně fungovat. Množství a propracovanost se odvíjí od velikosti chráněného prostoru a rizikovosti.[7]

2.3 Čidla

Jak již bylo psáno, čidla jsou komponenty, které reagují na fyzikální změny v chráněném prostoru. Dělení čidel je velice rozmanité, jak podle technických parametrů, tak podle místa a způsobu použití. Základním rozdělením podle technických parametrů je na napájená a nenapájená. Podle způsobu použití na vnitřní a vnější.[8]

2.3.1 Napájená čidla

Tato čidla ke své funkci potřebují napájení elektrickou energií a dělí se do dvou podkategorií.

a) **Aktivní** – vyzařují do prostoru aktivně energii, nejčastěji rádiové či infračervené vlny, které se přímo nebo odrazem dostávají k přijímači. Pokud je tato energie narušena fyzikální změnou, přijímač toto vyhodnotí jako důvod poplachu.
b) **Pasivní** – čidla pasivního charakteru pouze registrují fyzikální změny a přijímají energii právě z těchto změn. Nejčastějšími příklady jsou vyzařování tepla z těla narušitele, otřesy či zvuk rozbitého skla.

2.3.2 Nenapájená čidla

Nenapájenými čidly elektrická energie pouze proudí a v případě přerušení energetického toku se vyšle signál o narušení. Tato čidla lze také rozdělit do dvou podkategorií.

a) **Destrukční** – jedná se o jednorázová čidla, která jsou v případě aktivace zničena. Příkladem jsou poplachové folie na skla či bezpečnostní skla.
b) **Nedestrukční** – tato čidla lze použít opakovaně, jedná se o mikrospínače, vibrační a magnetický kontakt.

[7] BURDA, Karel. *Základy elektronických zabezpečovacích sytému*. Brno, 2017. str. 6-8 a 14
[8] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha, 2014, str. 203

2.3.3 **Vnější a vnitřní čidla**

Rozdíl mezi těmito čidly je zejména ve způsobu provedení ochranné schránky. Pro vnější použití je vždy potřeba, aby čidlo dokázalo odolávat povětrnostním podmínkám a případným vandalům.[9] [10]

2.4 Vybrané druhy čidel

2.4.1 **Magnetická čidla**

Magnetická čidla se nejčastěji používají na ochranu vstupních výplní (dveře, okna). Fungují na principu spínání a rozepínání jazýčkových kontaktů pomocí magnetu. V klidovém stavu, když jsou dveře zavřené, síla magnetu přitahuje a spíná jazýčky k sobě. Při otevření dveří dojde k oddálení magnetu a tím přestává magnetická síla působit na jazýčky, což způsobí jejich rozepnutí. Tento stav je vyhodnocen jako poplach a čidlo vyšle signál do ústředny EZS. Magnetická čidla bývají zapouzdřena v plastových či hliníkových krytech, které zabraňují jejich sabotáži. U rizikovějších míst se využívají čidla s ochranou proti cizímu magnetickému poli, díky tomu jakýkoliv pokus o sabotáž pomocí jiného magnetu vede k vyvolání poplachu.[11]

2.4.2 **Čidla rozbití skla**

K ochraně skleněných výplní se používají dva druhy čidel, a to akustické a bezpečnostní skla či fólie. Akustické čidlo využívá charakteristického zvuku, které vydává tříštění skla. Tento zvuk vydává specifické vlnění, které čidlo dokáže rozeznat. Pro co nejvyšší efektivnost je potřeba, aby bylo čidlo umístěné co nejblíže skleněné výplni. Dosah těchto čidel bývá 1,5 – 3 m. Principem fungování akustického čidla je: při přijmutí vlnění ze zvuku tříštění skla elektronika v čidle rozepne kontakty a tím vyvolá poplach. U modernějších čidel dojde ke spuštění poplachu prudkým vzrůstem odběru energie.

Bezpečnostní skla či fólie mají zcela odlišný princip fungování. V zabezpečovacím prvku jsou zabudovány jemné vodivé dráty nebo vodivá fólie, přes

[9] UHLÁŘ, Jan. *Technická ochrana objektů II. díl: Elektrické zabezpečovací systémy II*. Praha, 2005. str. 25-26
[10] BURDA, Karel. *Základy elektronických zabezpečovacích sytému*. Brno, 2017. str. 14-15
[11] PETRUZZELLIS, Thomas. *The Alarm, Sensor & Security Circuit Cookbook*. New York, 1994. str. 134-135

které proudí energie. V případě porušení celistvosti skla dojde k jejich porušení a přerušení toku energie, což má za následek vyvolání poplachu.[12]

2.4.3 **Pasivní infračervená čidla (PIR)**

PIR čidla (Passive infra red sensor) patří k nejrozšířenějším pohybovým čidlům dnešní doby, a to díky jejich snadné montáži a nízké spotřebě energie. Nevýhodou je lehká ovlivnitelnost okolním prostředím (náhlá změna teplot, zvířata, proudění teplého vzduchu atd.). Principem fungování PIR čidla je detekce infračerveného záření, které vyzařuje narušitel. Toto záření dokáže detekovat součástka zvaná pyroelement. Ta reaguje na změny teplotních hodnot oproti okolnímu prostředí. Pokud by na čidlo dopadalo infračervené záření z celého prostoru, tak by narušitel způsobil pouze nepatrnou změnu záření, proto je v senzoru zabudovaná speciální optika, která kontrolovaný prostor rozděluje do sektorů. Díky tomu čidlo vyhodnocuje změny teploty mezi jednotlivými sektory. Tato čidla se umísťují tak, aby pokryla co nevětší plochu kontrolovaného prostoru. Nejčastěji v rohu místnosti a v případě čidel snímající plochu 360° na strop uprostřed místnosti.

2.4.4 **Aktivní infračervená čidla (AIR)**

AIR čidla (active infra red sensor) na rozdíl od PIR čidel vysílají do prostoru infračervené paprsky a využívají jejich odrazu pro detekování narušitele. Díky tomu dokáže detekovat i předměty, které nevyzařují teplo a pohybují se libovolně nízkou rychlostí. Při uvedení do provozu si čidlo do paměti zapíše rozložení kontrolovaného prostoru a v případě změny od uloženého rozložení vyvolá poplach. Umisťování těchto čidel je stejné jako u PIR čidel, ale pokud je potřeba umístit dvě AIR čidla v jedné místnosti, musí se sesynchronizovat.

2.4.5 **Ultrazvuková čidla**

Ultrazvuková čidla vysílají do prostoru vlnění o stálém kmitočtu, které lidské ucho nedokáže zaznamenat. Toto vlnění se odráží od stěn ve stejné frekvenci jako vyslané vlnění. V případě, že se v prostoru pohybuje narušitel, odražené vlnění změní frekvenci a přijímač čidla toto vyhodnotí jako poplach. Tato čidla se moc nepoužívají, protože musí být instalována tak, aby pohyb narušitele směřoval k čidlu a v místnosti, která

[12] HORN, Delton. T. *Electronic Alarm and Security Systems: A Technician's Guide*. New York City, 1995. str. 32-34

nemá rušivé spotřebiče pracující s širokým kmitočtovým spektrem (telefon) a předměty se zvukově absorpčními schopnostmi (koberec).[13]

2.4.6 **Mikrovlnná čidla**

Princip fungování je stejný jako u předchozích ultrazvukových čidel, ale v kmitočtovém pásmu elektromagnetického vlnění. Díky jejich delšímu dosahu se používají ke kontrolování prostorů velkých objektů jako jsou pracovní haly či sklady.

2.4.7 **Duální čidla**

Pro zvýšení zabezpečení a efektivnosti pohybových čidel, obzvláště v rizikových místech, se používají čidla, která v sobě mají zabudované dvě technologie. Nejčastěji se jedná o kombinaci PIR a ultrazvukového čidla nebo PIR a mikrovlnného čidla.[14]

2.5 Ústředny

Ústředna je jádrem a mozkem celého zabezpečovacího systému. Sbírá a zároveň vyhodnocuje informace od ostatních komponentů EZS. Při potřebě vyhlášení poplachového stavu ústředna vyšle signál do signalizačního zařízení, které upozorní opticky či akusticky na incident v objektu. Ústředny se mohou nacházet v několika stavech, avšak nejdůležitější jsou stavy zastřeženo a odstřeženo. Při prvním stavu je objekt prázdný a čidla reagují na jakoukoliv změnu, zatímco v druhém stavu vysílají poplach jen určitá čidla např. čidlo požáru.[15]

2.5.1 **Dělení ústředen podle stupně vybavenosti**

Stupeň vybavenosti závisí na odolnosti proti překonání zabezpečení ústředny a komfortu jejich ovládání obsluhou. Podle typu rizikovosti objektu se instaluje i odpovídající ústředna.

- 1. stupeň zabezpečení
- 2. stupeň zabezpečení
- 3. stupeň zabezpečení
- 4. stupeň zabezpečení

[13] UHLÁŘ, Jan. *Technická ochrana objektů II. díl: Elektrické zabezpečovací systémy II*. Praha, 2005. str. 57 - 69
[14] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. Blatná, 2006. str. 85 a 88
[15] BURDA, Karel. *Základy elektronických zabezpečovacích sytému*. Brno, 2017. str. 5-6

U čtvrtého stupně se používají dvě ústředny, přičemž jedna musí být v kategorii stupně 3 a druhá minimálně kategorie stupně 2.

2.5.2 **Dělení ústředen podle počtu smyček**

Smyčka je skupina čidel či hlásičů nebo jiných komponentů EZS, které jsou napojeny na společné vedení do ústředny. Podle velikosti objektu se instaluje ústředna, která dokáže pojmout veškerá čidla či jiné zabezpečovací prvky, které budou v objektu nainstalovány.

- malé ústředny (1 – 5 smyček)
- střední ústředny (6 – 12 smyček)
- velké ústředny (nad 12 smyček)
- pult centralizované ochrany (několik set vstupních míst)

2.5.3 **Dělení ústředen podle způsobu připojení smyček**

Analogové ústředny (smyčkové ústředny) se vyznačují tím, že jedna smyčka čidel je připojena na samostatný vyhodnocovací obvod v ústředně. Tento obvod vyhodnocuje klidový proud smyčky, který jím protéká a při jeho změně vyhlásí poplach. Nevýhodou takovýchto ústředen je velmi rozsáhlá kabeláž, jelikož ke každému čidlu musí vést po dvou vodičích napájení, poplachový kontakt, sabotážní kontakt, kontakt dodatkové funkce. Tato ústředna také nedokáže určit, které čidlo bylo přesně aktivováno, zjistí pouze celou smyčku.

Sběrnicové ústředny využívají přímé adresace čidel na ústřednu pomocí datového vedení. Díky tomu je kabeláž minimální stačí přivést k čidlům pouze dva vodiče napájení a dva datové vodiče. Na rozdíl od analogových ústředen, sběrnicové dokáží určit, které přesně čidlo spustilo poplach a i o jaký poplach jde (klasický poplach, sabotáž, zkrat či jiné funkce). Nevýhodou je naopak malý počet přímo adresovaných čidel.

Koncentrátorové ústředny jsou kombinací dvou předchozích typů. Jednotlivá čidla jsou připojena na tzv. koncentrátory, které slouží jako malé analogové podústředny a komunikace mezi koncentrátory a hlavní ústřednou probíhá jako u sběrnicových ústředen.

Bezdrátové ústředny využívají rádiové komunikace mezi ústřednou a čidlem. Výhodou je jednoduchost montáže, flexibilita a možnost dočasného použití. Naopak nevýhodou je nutnost výměny baterií v komponentech (systém sám na nízký stav baterie upozorní). Tyto ústředny se využívají na místech, kde nelze ve stěnách objektů vést kabeláž (historické objekty, galerie).

Hybridní ústředny jsou nejmladší skupinou a kombinují veškeré výhody a nevýhody předchozích ústředen. Vhodné je jejich umístění do objektu, ve kterém z části lze zabudovat kabeláž a z části nikoliv.[16]

2.6 Signalizační zařízení

Úkolem signalizačního zařízení je upozornit na narušení objektu a v nejlepším případě i ukázat přesnou polohu pachatele. Základní prostředky pro signalizaci narušení jsou sirény, majáky a mapy či tabla.

- Majáky tvoří tzv. optickou signalizaci, která upozorňuje zpravidla silným oranžovým světlem na narušitele. Tyto majáky se umísťují na dobře viditelná a zároveň těžko dosažitelná místa.
- Sirény vytváří akustickou signalizaci, která má účinně upozornit na pachatele a zároveň ho vystrašit a donutit k opuštění místa. V obydlených místech je výhodou, že siréna zalarmuje okolní obyvatelstvo, které může zavolat policejní složky a tím dopadnout pachatele.
- Mapy a tabla se používají pro budovy, které nejsou v centru dění a zvuková či optická signalizace by nemusela fungovat, nebo pro budovy, které jsou chráněny pultem centralizované ochrany. Principem je, že pachatel nemusí vůbec vědět, že byl odhalen a obsluha mapy může na místo vyslat zásahovou jednotku a pachatele zadržet.[17]

[16] UHLÁŘ, Jan. *Technická ochrana objektů II. díl: Elektrické zabezpečovací systémy II*. Praha:, 2005. str. 122 - 128
[17] Tamtéž - s. 136 - 137

3 Systém kontroly vstupu

Systém kontroly vstupu, dále jen SKV, je bezpečnostní systém využívaný pro zamezení přístupu nepovolaným osobám do objektu, a to pomocí přidělených přístupových práv. Tato přístupová práva jsou zakódována ve specifickém identifikačním prvku, kterým osoba disponuje. SKV se využívá zejména u objektů či u části objektu, kde se uschovává citlivý obsah. Jedná se zejména o výpočetní centra, kanceláře, trezorové místnosti nebo podobná důležitá místa. SKV se nevyužívá pouze u velkých objektů, ale dá se použít i na malé soukromé objekty.

Principem SKV je přidělení přístupových práv osobě podle stupňů oprávnění, personální či časové dispozice. Pokud osoba nedisponuje přístupovým právem, systém jí neumožní přístup. Pokud je osobě vstup povolen, tak systém dokáže sledovat její pohyb, průchod, popřípadě její polohu.

3.1 Legislativa systémů kontroly vstupu

V současné době jsou veškeré systémové, technické a aplikační požadavky systému kontroly vstupu upraveny ve dvou technických normách.

ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – požadavky na systém a komponenty

Tato norma řeší problematiku funkčnosti a požadavků pro elektronické systémy kontroly vstupu a jejich zkoušení.

V obsahu této normy jsou uvedeny:

- Termíny a definice
- Zkratky
- Koncepční modely a architektura systému
- Požadavky na funkčnost
- Požadavky na odolnost proti vlivům prostředí a elektromagnetickou kompatibilitu
- Způsob zkoušek
- Dokumentace a značení[18]

[18] ČSN EN 60839-11-1: *Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak. *334593*

ČSN EN 60839-11-2 Poplachové a elektronické bezpečnostní systémy – část 11-2: Elektronické systémy kontroly vstupu – Pokyny pro aplikace

Tato norma definuje minimální požadavky pro montáž a provoz elektronických systémů kontroly vstupu.

Jejím obsahem je:

- Termíny a definice
- Zkratky
- Architektura systému
- Požadavky na odolnost proti vlivům prostředí
- Plánování systému
- Montáž systému
- Uvedení do provozu a předání systému
- Provoz a údržba systému
- Dokumentace[19]

3.2 Třídy identifikace systému kontroly vstupu

Podle důležitosti objektu se používají propracovanější metody a kombinace metod SKV. Pro tyto účely lze přiřadit SKV do určité třídy podle identifikace.

- 0. třída. U této třídy není přímá identifikace, postačuje zde pouhé tlačítko či detektor pohybu, zároveň je po vstupu možnost namátkové kontroly fyzickou ostrahou.
- 1. třída. Zde je k identifikaci využito dat uložených v paměti osoby. Jedná se například o heslo či číslo zaměstnance.
- 2. třída. Tato třída používá identifikační prvek nebo biometrickou vlastnost. Příkladem jsou identifikační karty, čipy, otisky prstů nebo snímání oční duhovky.
- 3. třída. Kombinace 1. a 2. třídy. Jedná se o nejvyšší stupeň.[20]

[19] ČSN EN 60839-11-2: *Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 334593

[20] *IDB Journal.* Bratislava: HMH, 2012, č. 5. str. 32

3.3 Identifikační prvky

Každý systém kontroly vstupu potřebuje ke svému správnému fungování identifikační prvek. Tento identifikační prvek slouží jako klíč ke vstupu do objektu chráněným SKV. Existuje mnoho druhů a provedení těchto identifikačních prvků, avšak pokud chceme docílit co nejvyšší bezpečnosti, tak tyto prvky kombinujeme. Základní rozdělení je podle toho, jak osoba prvkem disponuje.[21]

3.3.1 **Paměťové identifikační prvky**

Z názvu vyplývá, že osoba užívající tento prvek si jej musí zapamatovat. Jedná se o nejběžnější a nejjednodušší prvek, zároveň i nejméně bezpečný. Používají se dvě varianty, kterými jsou heslo nebo PIN (z anglického personal identification number) kód. Při vstupu do zabezpečeného objektu osoba zadá identifikační prvek přes kódovou klávesnici do systému a systém správnost prvku potvrdí nebo vyvrátí. Pro zvýšení bezpečnostního stupně je zde možnost využití speciální klávesnice s proměnlivým rozložením číslic a znaků. Díky této modifikaci je znemožněno odhadnutí zadávaného kódu a znaky na klávesnici nepodléhají opotřebení, ze kterého lze zjistit znaky kódu.

Rozdíl mezi heslem a PIN kódem

- Heslo – jedná se o řetězec 8-12 znaků v kombinaci číslic, velkých a malých písmen. Při vytváření hesla je třeba dbát na složitost a zároveň snadnou zapamatovatelnost. Počítačové systémy mohou pomoci při výběru a zjištění bezpečnosti hesla, popřípadě sami bezpečné heslo vygenerují. Heslo se zadává spolu s identifikačními údaji. Pokud se heslo a identifikační prvek neshodují v systému, přístup je zamítnut.
- PIN kód – zde je uplatněna kombinace pouze čísel, a to v délce 4-8 znaků. Jedná se o jednodušší, a proto méně bezpečný prvek, proto je při zadávání omezen počet pokusů. Pokud se přesáhne počet nesprávných pokusů, systém se zablokuje a je nutno použít složitější mechanismus pro odblokování nebo vyčkat určitou dobu, než se systém sám odblokuje.

[21] UHLÁŘ, Jan. *Technická ochrana objektů III. díl: Ostatní zabezpečovací systémy*. Praha, 2006. str. 64

Rozdělení podle přidělení

- Identifikační prvek je přidělen skupině lidí – lze využít u zaměstnanců, kdy skupina s jedním identifikačním prvkem má možnost vstoupit pouze do určité části objektu. Při potřebě vstupu do zakázaných částí objektu musí zaměstnanec jít s oprávněnou osobou. Dalším příkladem je vstup do společných prostor obytného domu, kde identifikační prvek znají obyvatelé tohoto domu. Nevýhodou je, že nelze zpětně vyhledat totožnost osoby, která do objektu či prostor objektu vstoupila.
- Identifikační prvek je přidělen každé osobě zvlášť – zde přibyla možnost zpětně vyhledat totožnost a čas osoby, která do objektu vstoupila.

Nevýhody paměťových identifikačních prvků jsou těžká zapamatovatelnost, neidentifikovatelnost osoby, zda je ta, za kterou se vydává, manuální zadávání a lehkost vynucení či úmyslné sdělení. Naopak výhody: nelze jej ztratit, jednoduchost změny a přidělení, kód může signalizovat různé stavy.[22]

3.3.2 Vlastnění identifikačního prvku

Jedná se o fyzický předmět, nejčastěji nazývaný token, který udává nebo potvrzuje identitu vlastníka. Tento token je jedinečný a je přiřazen dané osobě. Při vybírání tokenu je důležité držet se několika aspektů, zejména z hlediska bezpečnosti. Jedním z hlavních aspektů je zabezpečení tokenu před padělaním. Dalšími aspekty jsou bezpečnost přenosu informace mezi tokenem a snímacím zařízením, spolehlivost identifikace, trvanlivost, spolehlivost tokenu a jeho kapacita. Zabezpečení proti padělání a krádeži se nejlépe zvýší kombinací s jinou metodou identifikace, např. heslem nebo biometrickou vlastností.[23]

Magnetické identifikační karty

Jedná se o jednoduchý systém, kdy tokenem je plastová karta, rovnající se velikosti klasické kreditní karty, která je opatřena magnetickým proužkem. Na tento magnetický proužek jsou pomocí nahrávacího zařízení naneseny informace a údaje o osobě. Díky těmto informacím je možnost kontrolovat danou osobu, kdy a kam šla, popřípadě

[22] UHLÁŘ, Jan. *Technická ochrana objektů III. díl: Ostatní zabezpečovací systémy*. Praha, 2006. str. 70-74
[23] Tamtéž, str. 64-65

omezit její přístup do určité oblasti. Při použití musí být karta fyzicky protažena štěrbinou snímacího zařízení.

- Výhodami magnetické karty jsou nízká cena, snadné přepisování informací a možnost využití jedné karty k více systémům.
- Nevýhody jsou snadná duplikace, rychlé opotřebení karty, snadná krádež nebo zapůjčení karty.

Tento token již bývá zaměňován za modernější a bezpečnější technologii.

Optické identifikační karty

Optický systém využívá čárový kód jako identifikační prvek. V čárovém kódu je zaznamenána informace, kterou snímací zařízení naskenuje a vyhledá v databázi. V dnešní době se používá mnoho čárových kódů, jako jsou např. EAN 8, EAN 13, CODE 39, CODE 128, CODEBAR. Zabezpečení tohoto tokenu je velice nízké a jeho padělání postačí fotoaparát či okopírování karty. Pro zlepšení bezpečnosti je možno kartu zapouzdřit v bezpečnostní fólii nebo ji opatřit bezpečnostním černým lakem, kterým snímací zařízení projde. U použití lze kartu přiložit k čtecímu zařízení nebo lze kód snímat ze vzdálenosti několika centimetrů.

- Výhodami jsou velice nízká cena karty a snadná úprava informací v systému.
- Nevýhodou je vysoké nebezpečí zfalšování karty.

Indukční identifikační karty

U tohoto druhu tokenu se využívá princip elektromagnetické indukce. Karta připomíná klasickou plastovou kartu, avšak uvnitř je zabudována kovová destička s jedinečným vzorem nebo přesně umístěné vodivé plochy, ve kterých je zakódována informace. Pro použití se karta zasune do snímače a ten informaci převede do systému.

- Výhodami je těžké zfalšování a odolnost karty.
- Nevýhodou je krádež karty.

Identifikační čipy

Identifikační čipy jsou využívány zejména v podobách karet či přívěšků. Jedná se o mikročip, který v sobě nese informace potřebné k identifikaci. Tento čip je nalisován do karty rovnající se velikosti klasické platební karty, popřípadě je upevněn v plastovém

pouzdře, které se dá připevnit na klíče nebo se dá nosit jako náramek. Tento token z hlediska způsobu použití rozdělujeme na:

- Kontaktní – zde je potřeba identifikační čip přiložit nebo vložit do čtečky, aby vzniklo elektrické propojení a systém získal potřebné informace k poskytnutí přístupu,

- Bezkontaktní – tato metoda využívá radiofrekvenčních vln k přenosu informací, tudíž lze kartu použít několik centimetrů od čtečky. Bezkontaktní čipy mají rozdělení na aktivní a pasivní, kdy aktivní mají zabudovanou baterii a vysílají signál neustále, naopak u pasivních čtečka vysílá do okolí elektromagnetické impulzy a čip tuto energii využije k vlastnímu napájení.

Identifikační čipy nahrazují starší technologie zejména kvůli bezpečnosti a možnosti nahrát do tokenu více informací a aplikací, díky čemuž se dá karta použít například i k bezhotovostní platbě.

- Výhodami jsou bezpečnost, multifunkčnost a u pasivních čipů nízká cena.
- Nevýhoda u aktivních čipu je vysoká cena a složitost.[24]

3.3.3 **Biometrické identifikační prvky**

Jedná se o poslední a nejmladší skupinu identifikačních prvků v SKV, která je vyznačená svojí bezpečností a uplatňuje se v systémech zajišťujících vyšší stupeň zabezpečení. Princip biometrického identifikačního prvku spočívá ve využití biometrické vlastnosti člověka k identifikaci či verifikaci osoby.[25]

3.4 Snímací zařízení identifikačního prvku

Jedná se zařízení, které po zapsání, vložení nebo přiložení identifikačního prvku, získá informace o osobě. Tyto informace snímací zařízení elektronicky pošle do řídící jednotky, kde je systém vyhodnotí. Na základě tohoto procesu a správnosti informací je osobě povolen či zamítnut přístup do chráněného objektu. Jelikož se snímací zařízení

[24] UHLÁŘ, Jan. *Technická ochrana objektů III. díl: Ostatní zabezpečovací systémy*. Praha, 2006. str. 65-69
[25] Tamtéž, str. 70-71

nachází před vchodem do chráněného objektu a jde o zařízení povolující vstup, je potřeba, aby splňoval dva základní atributy.

- Jednoduchost a otevřenost pro uživatele.
- Vysoká odolnost proti sabotáži a jiným vnějším vlivům.

Snímací zařízení paměťových identifikačních prvků

Jde o veškeré klávesnice sloužící k zanesení hesla či PIN kódu do systému. Ve většině případů se jedná o numerické klávesnice, ale je zde možnost použití klávesnice abecední či kombinované. Tato snímací zařízení se pro zvýšení bezpečnosti využívají v kombinaci s jinými snímači, například s čtečkou karet.

Čtečky magnetických karet

Pro použití magnetické karty je potřeba ji nejprve nahrát neboli zmagnetizovat. Po tomto procesu se na kartě vytvoří trvale zmagnetizované malé magnety, jejichž rozložení tvoří soustavu pro binární rozhodování, kde zmagnetizované pole je chápáno jako 1 a nezmagnetizované pole jako 0. Po protažení karty čtečkou systém přečte informace na kartě a vyhodnotí jejich správnost.

Optická čtečka karet

Jedná se o čtečku čárových kódů, kde je principem použití laserového paprsku. Tento paprsek je vyslán na čárový kód, kde černé proužky laserový paprsek pohltí a bílý podklad mezi proužky paprsek odrazí zpět do čtečky, která podle informací získaných z odraženého paprsku vyhledá v databázi informace o osobě, zda má oprávnění vstoupit do chráněného objektu.

Indukční čtečka

Čtečka má v sobě pevně zabudované magnetické pole, které je po vložení karty propojeno s jejími vodivými plochami. Vodivé plochy udávají vzor binárního rozhodování, kdy vodivá plocha má hodnotu 1 a její absence 0. Tyto informace jsou vyslány do řídící jednotky a vyhodnoceny.

Čipové čtečky

Jelikož elektronické čipy mají veškeré informace nahrané v paměti, tak čipové čtečky fungují jako nástroj propojení mezi systémem a čipem. Podle způsobu použití, stejně jako u identifikace čipem, rozdělujeme tyto čtečky na kontaktní a bezkontaktní.

- Kontaktní čtečky – Zde musí být čip přiložen nebo vložen do čtečky, aby se propojily elektronické kontakty a systém získal přístup k informacím.
- Bezkontaktní čtečky – tento způsob je rozšířenější díky tomu, že není potřeba čip přikládat do těsné blízkosti čtečky. Podle způsobu získávání informací bezkontaktní čtečky lze rozdělit na čtečky aktivních a pasivních čipů. U pasivních čipů čtečka vysílá elektromagnetické impulzy, které napájí čip a ten poté vyšle signál s informacemi do čtečky. Naopak u aktivních čipů, které mají vlastní napájení a signál vysílají neustále, tak čtečka pouze signál s informacemi přijímá.

3.5 Snímače biometrických identifikačních prvků

Jde o velice složité systémy, které se stále vyvíjí a zajišťují vysokou bezpečnost. Jejich složitost spočívá v druhu snímaného biometrického prvku a velikosti databáze systému.[26]

[26] UHLÁŘ, Jan. *Technická ochrana objektů III. díl: Ostatní zabezpečovací systémy*. Praha, 2006. str. 72-74

4 Biometrie a její využití u systému kontroly vstupu

Pod pojmem biometrie je vědní obor, jehož zkoumání je zaměřeno na měření fyziologických a behaviorálních vlastností živého organismu (nejčastěji člověka) a jeho následné a jednoznačné identifikování. Každá fyziologická a behaviorální biometrická vlastnost musí být *jedinečná, stálá, měřitelná, zpracovatelná a vyhodnotitelná.*

Jak již bylo psáno, biometrické vlastnosti se dají rozdělit do dvou skupin, fyziologické a behaviorální. U fyziologické (tělesné) skupiny se jedná o vlastnosti, které má naše tělo, jako jsou například: *otisk prstu, oční sítnice, geometrie ruky, tvar oka nebo geometrie obličeje*. U druhé skupiny, tzv. behaviorální (biometrie chování) je hlavní cíl zkoumání osobnostních vlastností člověka, ty mohou být například: *styl chůze, dynamika písma, styl psaní na klávesnici nebo hlas*

Hlavní myšlenka biometrie se zakládá na principu biometrické identifikace, to znamená, že každá osoba je identická jen pouze sama se sebou. Fyziologické a behaviorální vlastnosti člověka jsou prokazatelně jedinečné a lze je tedy použít k efektivní identifikaci, nadále tyto vlastnosti je téměř nemožné pozměnit či napodobit. Biologickou identitu nelze odcizit, protože fyzické vlastnosti člověka jsou s ním bezprostředně spojeny, a to již od narození.[27]

4.1 Obecné využití biometrie

Prvotně byla biometrie využívána zejména v kriminalistickém sektoru pro identifikaci pachatelů, ale časem se začala dostávat i do běžného života. Dnes ji používáme skoro denně jak u velkých firem, kde zastává bezpečnostní funkci pro kontrolu pohybu osob v objektu nebo v soukromém životě, kde její funkce využíváme pro ochranu soukromí a osobních dat. Základní využití dnešní biometrie spočívá v rozpoznání osob díky jejich fyziologickým vlastnostem. Tento postup je obecně znám jako biometrická identifikace nebo verifikace.[28]

[27] RAK, Roman., MATYÁŠ, Václav., a ŘÍHA, Zdeněk., *Biometrie a identita člověka*. Praha, 2008. str. 104-105

[28] Tamtéž str. 33-34

Identita a identifikace

Zatímco **identita** (totožnost) je pojem, který znázorňuje totožnost něčeho s něčím nebo se sebou samým, tak **identifikace** (ztotožnění) je proces, který se využívá při zjištění identity osoby. Při tomto procesu se porovnává předložená biometrická vlastnost s databází a ve výsledku dojde k zjištění identity, pokud se v databázi najde shodná biometrická vlastnost. Délka identifikace závisí na množství biometrických vlastností v databázi. Čím obsáhlejší databáze, tím delší bude proces porovnávání.[29]

Verifikace

Na rozdíl od **identifikace** je **verifikace** proces mnohem rychlejší. Důvodem toho je, že proces verifikace prověřuje, zdali je osoba tou, za kterou se vydává. Zde se porovnává jedna biometrická vlastnost pouze s jednou vlastností uloženou v databázi. U procesu verifikace nejprve osoba sdělí svoji identitu, např. heslem, čipem či kartou, následně předloží svou biometrickou vlastnost a výsledkem je potvrzení či vyvrácení identity. Verifikace je nejčastěji používaná k povolení vstupu do objektů, popřípadě části objektu.[30]

4.2 Biometrické metody identifikace

Biometrie má mnoho metod sloužících k identifikování či verifikování osoby. Rozdíly v těchto metodách jsou v jejich získání, přesnosti a využitelnosti. Tyto metody lze rozdělit do tří skupin.

Forenzní skupina

Jedná se o dlouhodobě a vědecky podložené metody, které vyžadují vysokou náročnost a jsou nejefektivnější. Jelikož se jedná o metody používající se v policejní a soudní identifikaci, je jim věnována vysoká pozornost, aby nedošlo k chybě. Výsledkem forenzních metod je většinou důkaz, který jednoznačně určuje totožnost osoby. Při zpracovávání je použito speciální laboratorní a technické vybavení, které zaručuje nejvyšší možnou správnost výsledku. Každý výsledek poté zhodnotí specialista v oboru a případně metodu obhájí u soudu. Forenzní metody zahrnují daktyloskopii, analýzu DNA a fonetiku lidského hlasu. Častěji se zde uplatňuje identifikace než verifikace.

[29] RAK, Roman., MATYÁŠ, Václav., a ŘÍHA, Zdeněk., *Biometrie a identita člověka*. Praha, 2008. Str. 39-40
[30] Tamtéž, str. 130-131

Bezpečnostně-komerční skupina

Tyto metody se vyvíjely od metod forenzních a za účelem použití v civilním životě se zjednodušovaly. Jejich využití je zejména pro ochranu soukromých, bankovních a počítačových dat. Dalším rozdílem je plná automatizace metod a vyšší chybovost na rozdíl od forenzní skupiny. Bezpečnostně-komerční metody využívají daktyloskopii, oční duhovku, anatomii lidského těla, geometrii obličeje či dlaní, fonetiku lidského hlasu a dynamiku psaní.

Ezoterická skupina

Metody ezoterické skupiny jsou nejméně rozšířené a využívají je experti v oborech. Jedná se o metody, které se stále vyvíjí a zkoumají. Postupem času a výzkumem mohou být tyto metody přiřazeny k některé ze dvou předchozích skupin, nyní jsou využívány minimálně. Mezi tyto metody patří dynamika chůze, otisk rtů, tvar vnějšího ucha, topografie žil, pach lidského těla, obsah solí v lidském těle apod.[31]

Využití biometrie v zabezpečovacích systémech je vcelku nové. První využití biometrie bylo aplikováno v 80. letech 19. století. Jako biometrická verifikace byla použita metoda otisku prstu, kde se kombinovala s identifikačními kartami či zadáváním PIN kódu. K většímu rozmachu došlo v 90. letech díky levným optickým snímačům a inovaci bezpečnostních systémů. V dnešní době se s bezpečnostním využitím biometrie setkáme kdekoliv od vstupu do budovy, přes kontroly na letištích až po zabezpečení mobilního telefonu nebo jako ověření při manipulaci s účtem v bance.

Dnešní bezpečnostní systémy využívající biometrie nepracují pouze s otiskem prstu. Ke zvýšení bezpečnosti používají více biometrických vlastností člověka, nejčastěji geometrie tváře, geometrie ruky, struktura žil, duhovka oka, oční sítnice a struktura žil. Cílem zabezpečení pomocí biometrických vlastností je vytvořit komplexní systém, který měří více charakteristik, díky čemuž se mnohonásobně zvyšuje stupeň zabezpečení a spolehlivost.

Na rozdíl od identifikace heslem či PIN kódem nebo identifikace tokenem, které se používají od nejnižšího po vyšší stupeň zabezpečení v závislosti na propracovanosti systému, se identifikace biometrickým prvkem používá u nejvyššího stupně

[31] RAK, Roman., MATYÁŠ, Václav., a ŘÍHA, Zdeněk., *Biometrie a identita člověka*. Praha, 2008. str. 107-112

zabezpečení. Proto se od tohoto systému očekává několik zásadních vlastností, jimiž jsou: vysoká spolehlivost, rychlost, efektivnost, odolnost a jednoduchost použití.

4.3 Rozdíly biometrických identifikačních systémů

Existují dvě skupiny biometrických identifikačních systémů, jimiž jsou forenzní skupina a soukromá skupina. Rozdíl mezi skupinami je v principu fungování. Forenzní skupina, používající se v soudní, kriminalistické a vyšetřovací sféře, má za úkol identifikovat osobu, o které nemáme žádné jiné informace nebo velice málo. K tomu potřebuje systém rozsáhlou databázi k porovnávání biometrické vlastnosti se šablonami. Samozřejmě tyto systémy jsou nepřijatelné pro soukromou sféru zejména kvůli jejich ceně pohybující se v miliónových částkách. Proto bylo potřeba systém upravit a tím změnit princip a snížit cenu. Na rozdíl od forenzní skupiny v soukromé skupině není potřeba obsáhlá databáze a ani vysoký operační výkon. Databází je myšleno jak databáze osob, kde postačuje kapacita pro několik stovek až tisíc osob nebo databáze biometrických prvků, u které není potřeba například u otisků prstů snímat všech deset, ale pouze jeden. Díky tomuto odpadá i potřeba vysokého výkonu operačního systému, který má hlavní vliv na cenu.[32]

4.4 Princip fungování biometrických systémů kontroly vstupu

SKV využívající biometrie používají proces verifikace, který vyžaduje nejprve zadat svoji identitu a posléze ji potvrdit. Pro fungování je potřeba, aby biometrickou vlastnost měla osoba zapsanou v databázi. Samotný zápis se musí odehrávat v bezpečném prostředí, aby se snížila možnost neoprávněného získání dat či neoprávněného zadání biometrických vlastností do systému. Při procesu zapisování je dbáno na opatrnost a kvalitu snímání vlastnosti, na níž závisí následný proces verifikace.

Proces použití biometrického systému funguje následovně:

- Snímání biometrické vlastnosti za pomoci vhodného snímače.

[32] ŠČUREK, Radomír. *Biometrické technologie: Technické prostředky bezpečnostních služeb* [online]. Ostrava. 2015, [cit. 2022-04-07]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/BiometrickeTechnologie.pdf str. 12-13

- Zjištění kvality vzorku, při špatné kvalitě okamžité zamítnutí a žádost o opakování snímání.
- Vytvoření referenční šablony.
- Zápis referenční šablony do archívu.
- Porovnání referenční šablony na základě algoritmu určujícím shodu se šablonou vyžadovanou z databáze.
- Při dostatečné shodě šablon povolení přístupu, v opačném případě zamítnutí.

Důležitým aspektem při procesu povolení přístupu je počet přihlašovacích pokusů. Díky tomuto omezení se sníží čas, který nepovolaná osoba potřebuje k získání dostatku informací k překonání systému. Po využití všech pokusů systém natrvalo zabrání přístupu identifikující se osobě. Podle stupně zabezpečení je třeba vybrat správný počet pokusů a brát v úvahu to, že čím je menší počet pokusů, tím se zvýší pravděpodobnost falešných poplachů. V těchto systémech by měla být zabudována paměť, do které se zapisují výsledky verifikace. To vytváří možnost zpětně nahlížet do systému pro zjištění pracovní docházky, kontrolu pohybu zaměstnanců nebo zjištění neoprávněného manipulování s přístupem.[33]

Možnosti zapisování výsledku verifikace.

- Zápis do snímacího zařízení – tato možnost není příliš bezpečná vzhledem k snadnému přístupu nepovolané osoby k paměti, kde jsou tato data uložena. Další nevýhodou je omezená paměť, tudíž hrozí přepsání starých dat novými.
- Zápis do vzdáleného počítače – zde odpadají nevýhody snadného přístupu a omezené paměti. Hrozbou pro tuto metodu je napadení systému zvnějšku, proto je potřeba komunikaci s počítačem a samotnou paměť dostatečně zabezpečit.
- Zápis do tokenu – celkově nevýhodný způsob, který vyžaduje složitou elektroniku v tokenu, což se odráží na vysoké ceně, další nevýhodou je možnost ztráty nebo odcizení tokenu, tudíž možnost vytěžení dat.[34]

[33] ŠČUREK, Radomír. *Biometrické technologie: Technické prostředky bezpečnostních služeb* [online]. Ostrava. 2015, [cit. 2022-04-07]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/BiometrickeTechnologie.pdf str. 15-16
[34] Tamtéž str. 14

4.5 Bezpečnost a komfort biometrických systémů kontroly vstupu

Nejzákladnějšími aspekty pro uživatele biometrických systémů kontroly vstupu jsou bezpečnost a komfort. Tyto dvě veličiny lze změřit pomocí koeficientů.

False Acceptance Rate (FAR)

Jedná se o koeficient chybného přijetí, tedy z hlediska bezpečnosti jde o velice důležitou veličinu v procesu identifikace. Udává statistický údaj o tom, jaká je pravděpodobnost, že neoprávněná osoba bude systémem vyhodnocena jako oprávněná. Jedná se o velice závažnou bezpečnostní chybu.

False Rejection Rate (FRR)

Koeficient chybného odmítnutí, který je veličinou komfortu systému. Představuje údaj, kdy oprávněná osoba je systémem vyhodnocena jako neoprávněná, tudíž musí opakovat pokus o přístup do objektu. Tato chyba nemá žádný význam z hlediska bezpečnosti, ale pro marketing je nevýhodná.

Equal Eror Rate (ERR)

Pro efektivnost biometrických systémů vstupu je důležitý křížový EER koeficient neboli koeficient vyrovnaných chyb. Jeho funkce spočívá v nastavení citlivosti systému, kde se vyrovnává FAR a FRR koeficient pro co nejvyšší bezpečnost a komfort. Pokud budeme chtít posunout hranici bezpečnosti na vyšší úroveň, tak hranice komfortu nám naopak klesne.[35]

4.6 Jednotlivé snímače biometrických vlastností a jejich chybovost

Biometrická identifikace a verifikace využívá mnoho metod v závislosti na dostupnosti a umístění biometrických vlastností na lidském těle. Tyto vlastnosti lze snímat pouze určitými snímači, které jsou k tomu přizpůsobeny. Nejčastěji používanými biometrickými vlastnostmi jsou otisk prstu, geometrie obličeje, geometrie dlaně, krevní řečiště ruky, oční duhovka, oční sítnice a hlas.[36]

[35] ŠČUREK, Radomír. *Biometrické technologie: Technické prostředky bezpečnostních služeb* [online]. Ostrava. 2015, [cit. 2022-04-07]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/BiometrickeTechnologie.pdf str. 20-24

[36] UHLÁŘ, J. *Technická ochrana objektů III. díl: Ostatní zabezpečovací systémy*. Praha: Policejní akademie české republiky, 2006. str. 75-76

4.6.1 Snímače otisku prstu

Operační systém pro snímače otisku prstu využívá určité algoritmy ke srovnání snímaného otisku se šablonou uloženou v databázi. Tyto algoritmy využívají zejména markanty v papilárních liniích prstu.

- Algoritmus polohy markantu porovnává jeho umístění a směr s šablonou v databázi.
- Algoritmus sčítání rýh využívá konkrétních dvou markantů a sečte počet rýh mezi nimi.
- Algoritmus markantografický vytvoří spojnice mezi markanty a následný obrazec porovná se šablonou.

Je mnoho snímačů otisků prstů využívající rozdílné technologie, avšak nejpoužívanější je využití optických senzorů. Tyto snímače rozdělujeme podle principu použití na reflexní statické, reflexní se skládáním obrazu, bezdotykové a transmisní. Dalšími používanými snímači jsou kapacitní, tepelné, tlakové a ultrazvukové.

Reflexní statické snímače

Je to klasický způsob snímání otisku prstu, kdy osoba přiloží svůj prst na skleněný podsvícený senzor, který zachytí odrážející se světlo od prstu a vytvoří obraz, který následně porovnává. Jeho nevýhodou je vysoké množství chyb, které jsou zapříčiněny nečistotami na prstě, popřípadě na snímači.

Reflexní snímače se skládáním obrazu

Tento snímač má zabudovaný úzký rolovací senzor, přes který osoba prstem přejíždí. Při každém pohybu, za použití principu odrážení světla jako u předchozího snímače, senzor vytváří pruhy snímaného prstu, následně pruhy složí a vytvoří celkový obraz, který porovnává šablonou. Oproti statickému snímači, díky posouvání prstu přes senzor, zde nezůstávají nečistoty a staré otisky.

Bezdotykové optické snímače

U tohoto druhu snímače není potřeba kontaktního senzoru pro přímé snímání otisku. Prst stačí nastavit nad snímač, ten následně vyšle světelné paprsky, které se odrazí od papilárních linií prstu zpět do snímače. Snímač poté vytvoří porovnávací obraz. Zde senzor chybně odepře přístup, pokud jsou na prstě nečistoty.

Transmisní snímače

Na rozdíl od předchozích senzorů vytvářejících obraz pomocí odražených paprsků, u transmisního snímače senzory zachycují paprsky procházející prstem. Následující proces vytváření a porovnávání obrazu je stejný jako u předchozích.

Kapacitní snímače

Jedná se o kondenzátorovou destičku pokrytou silikonovou vrstvou, která měří napětí mezi prstem a samotnou destičkou. U hřebenu papilární linie je jiné než v rýze mezi nimi, díky tomu snímač získá obraz otisku a potřebné informace k identifikování osoby. Nevýhodou je potřeba časté údržby od nečistot.

Tepelné snímače

Tepelný snímač měří rozdíly teplot mezi papilární linií a vzduchem v rýhách mezi nimi. Samotný senzor je vyroben z křemíku a pokryt speciálním materiálem citlivým na teplo. Teplotní rozdíly se převedou na elektronický náboj a vytvoří obraz otisku. Nevýhoda je nízká kvalita obrazu.

Tlakové snímače

Zjišťují rozdíly tlaku papilárních linií a rýh, díky čemuž vytváří jejich obraz. Snímač je vytvořen z pružného materiálu, který se přizpůsobí tvaru otisku. Nevýhodou je nízká citlivost.

Ultrazvukové snímače

Tyto snímače vysílají ultrazvukové vlny, které se odráží od povrchu prstu do přijímače a ten vyhodnotí obraz otisku. Obrovskou výhodou tohoto snímače oproti ostatním je odolnost vůči nečistotám, naopak nevýhodou je vysoká cena a velikost snímače.

Chybovost při této biometrické vlastnosti je velice variabilní z důvodu možnosti nastavení citlivosti sytému. Objektivně je udáváno FAR 0,01 % a FFR 5 %, z toho vyplývá, že identifikace či verifikace pomocí otisku prstu je velmi přesná, zato méně komfortní. [37]

[37] ŠČUREK, Radomír. *Biometrické technologie: Technické prostředky bezpečnostních služeb* [online]. Ostrava. 2015, [cit. 2022-04-07]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/BiometrickeTechnologie.pdf str. 58-64

4.6.2 Snímače geometrie obličeje

Tato snímací zařízení rozpoznávají osoby podle tvaru obličeje a jeho významných částí jako jsou tvary a vzdálenosti očí, úst, nosu či obočí. Pro samotné snímání je použita klasická kamera, avšak pro zpracování obrazu a jeho přiřazení k osobě je použit speciální program. Programy vyhodnocující geometrii obličeje používají určité algoritmy pro měření.

Algoritmus analýzy hlavních částí (PCA – Principal Components Analysis)

Tento algoritmus používá jednorozměrný vektor a kovariační matici pro vytvoření tzv. eigenfaces. Tyto eigenfaces jsou rozdílné svým jasem a dají se složit do jedné šablony. S touto šablonou se poté porovnává obraz identifikující se osoby.

Algoritmus Lineární diskriminační analýzy (LDA – Linear Discriminant Analysis)

Zde se obrazy tváře s různými mimickými výrazy řadí do skupiny, díky čemuž rozdíly v jedné skupině minimalizuje, a naopak rozdíly mezi jednotlivými skupinami maximalizuje.

Elastický srovnávací diagram (EBGM - Elastic Bunch Graph Matching)

Díky špatnému fungování předchozích algoritmů se změnou světla nebo pozicí hlavy byl vyvinut EBGM algoritmus. Ten vytvoří na obličeji uzlové body, které jsou propojeny a díky tomu vytvoří obličejovou síť. Tato obličejová síť je posléze porovnávána s databází šablon. Problémem je, že samotný algoritmus obtížně vyhledává uzlové body, proto je používán v kombinaci s předchozími metodami.[38]

3D model obličeje

Při tomto druhu snímání obličeje se používá 3D laserový skener. Díky tomu lze vytvořit přesný tvar i strukturu obličeje, která je porovnávána se šablonami v databázi. Jedná se o jeden z nejpřesnějších systémů identifikace pomocí geometrie obličeje. Velkou výhodou kromě přesnosti je i fakt, že laser nelze oklamat fotografií.

Chybovost této metody se může pohybovat i v několika procentech. To se děje v důsledku proměny obličeje v čase nebo změnou osvětlení. Tento problém se částečně

[38] ŠČUREK, Radomír. *Biometrické technologie: Technické prostředky bezpečnostních služeb* [online]. Ostrava. 2015, [cit. 2022-04-07]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/BiometrickeTechnologie.pdf str. str. 32-36

vyřešil spojením EBGM algoritmu s LDA nebo PCA algoritmem, díky čemuž je FAR 0,1 % a FRR okolo 1 %.[39]

4.6.3 **Snímače geometrie ruky**

Principem je snímání geometrie ruky ve třech dimenzích, kterými jsou délka, šířka, tloušťka ruky a prstů. Ruka je přiložena na snímací desku, na níž je pět polohovacích kolíků, díky kterým je umístěna ve správné poloze. Systém dokáže určit přes 31 000 polohových bodů a provede 90 druhů měření vzdálenosti. Snímání je prováděno díky klasické kameře a infračervenému světlu. V řádu jedné sekundy snímač provede řadu měření a porovná snímaný obraz s databází.

Jelikož geometrie ruky není příliš unikátní biometrickou vlastností, tak je zde vysoká míra chybovosti. Chybovost také zapříčiňuje špatná poloha dlaně na snímači. FAR a FRR se zde pohybuje okolo 5 %, díky tomu lze použít snímání geometrie ruky pouze pro verifikaci a pouze do určitého stupně zabezpečení.[40]

4.6.4 **Snímače krevního řečiště ruky**

Snímání probíhá pomocí speciální kamery a infračerveného světla. Toto světlo prosvítí ruku a veškeré její cévy či tkáně. Po nasnímání získáme černobílý obraz, na kterém je zvýrazněná mapa krevního řečiště. Zvýraznění cév je způsobeno odkysličeným hemoglobinem, který pohlcuje infračervené světlo. Snímat krevní řečiště lze ze hřbetu ruky, zápěstí ruky či dlaně. Jejich snímání funguje na stejném principu.

Po sejmutí obrazu místa krevního řečiště následuje postup tvořený ze čtyř fází, který nás dovede k vytvoření finální šablony a následnému porovnání s databází.

- Fáze segmentace rozdělí obraz na dvě části, jimiž jsou část ruky, která je důležitá pro následné fáze. Druhá je část pozadí, kterou systém vyhodnocovat nebude.
- Fáze vyhlazení a redukce šumu zkvalitňuje a vyhlazuje obraz řečiště. Dále redukuje vliv tvaru ruky na obraz.
- Fáze lokálního prahování oddělí mapu krevního řečiště od ruky.

[39] ŠURKALA, Milan. *Digimanie: Detekce a rozpoznání tváří: vím, kdo jsi!* [online]. Příbram: oXyShop, 19. 3. 2014, [cit. 2022-04-07]. Dostupné z: https://www.digimanie.cz/detekce-a-rozpoznani-tvari-vim-kdo-jsi/5500-2

[40] ŠČUREK, Radomír. *Biometrické technologie: Technické prostředky bezpečnostních služeb* [online]. Ostrava. 2015, [cit. 2022-04-07]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/BiometrickeTechnologie.pdf str. 30-32

- Fáze postprocessingu upravuje obraz do finální podoby a vytváří šablonu porovnávanou s databází šablon. [41]

Chybovost tohoto snímání je velice nízká a jde o jeden z nejbezpečnějších systémů, a to i díky špatné možnosti falšování. FAR činí méně než 0,00008 % a FFR okolo 0,01 %.[42]

4.6.5 **Snímač oční duhovky**

Další velice bezpečná možnost identifikace či verifikace pracující na principu snímání mapy oční duhovky. Snímání je bezkontaktní a probíhá ze vzdálenosti několika desítek centimetrů, proto je potřeba kvalitní digitální kamery a infračerveného osvícení. Zbarvení duhovky není pro tento proces důležité, jelikož snímač pořizuje černobílý obraz, který poté převádí do tzv. IrisCode, ve kterém jsou uloženy veškeré informace o vzoru duhovky. Nasnímaný IrisCode je následně porovnáván se šablonou uloženou v databázi.

Chybovost a bezpečnost snímání oční duhovky je téměř nulová díky její jedinečnosti a nemožnosti oklamat. FAR 0,00066 % FFR 0,00078 %[43]

4.6.6 **Snímání sítnice oka**

U této biometrické vlastnosti je snímán obraz cév z okolí slepé skvrny oční sítnice, nacházející se na zadní straně oka. Snímání je prováděno použitím infračervené led diody, která osvítí sítnici a získá mapu cév. Tuto mapu následně porovná s databází šablon. Jelikož se jedná o vnitřní orgán, není zde možnost zanechání stop pro vytvoření falešné sítnice. Nevýhodou je potřeba vysoké spolupráce osoby se snímačem, kdy osoba musí nahlédnout do snímače a zaostřit na určitý bod. Poté proběhne snímání po dobu až 2 sekund.

Chybovost u FAR je 0 %, avšak kvůli nepříjemnosti a potřebě dodržovat určitý postup u snímání FFR se pohybuje okolo 12 %, proto sítnice snímá vícekrát a tím sníží FFR na 0,4 %[44]

---

[41] ŠČUREK, Radomír. *Biometrické technologie: Technické prostředky bezpečnostních služeb* [online]. Ostrava. 2015, [cit. 2022-04-07]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/BiometrickeTechnologie.pdf str. 42-46

[42] GRYGAŘÍKOVÁ, Michaela. *MasterDC: Datacentra Masteru jako nedobytný hrad. I díky biometrické autentizaci* [online]. Praha: MasterDC, 28. 09. 2019 [cit. 2022-04-07]. Dostupné z: https://www.master.cz/blog/biometricka-autentizace-v-datacentru/

[43] ŠČUREK, Radomír. *Biometrické technologie: Technické prostředky bezpečnostních služeb* [online]. Ostrava. 2015, [cit. 2022-04-07]. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/BiometrickeTechnologie.pdf str. 36-37

5 Bezpečnostní analýza vybraného objektu

5.1 Popis objektu

Pro účely vytvoření návrhu na zabezpečení je použit objekt tělocvičny SAWADE GYM & SHOP, dále jen „objekt“ nacházející se ve Strakonicích. Objekt slouží k poskytování tělovýchovných a sportovních služeb v oblasti fitness a jako maloobchod s fitness příslušenstvím a doplňky stravy. Jedná se o malý přízemní objekt, který je situován ve společném prostoru komplexu soukromých budov s bytovými jednotkami a jednou příjezdovou cestou.

Samotný objekt je rozdělen do čtyř místností, kterými jsou kancelář, převlékárna, toaleta a tělocvična. Vchod je rozdělen dvěma dveřmi, které mají mezi sebou prostor 1 metr. Následující místnost slouží jako kancelář a prodejna fitness příslušenství. Po levé straně je vchod do převlékárny, ve které je situováno stropní celistvé plastové okno a vchod na toaletu. Po pravé straně kanceláře leží vchod do tělocvičny, ve které je umístěno fitness vybavení. V místnosti tělocvičny se nacházejí tři dvojitě zasklená plastová okna a únikový východ.

5.2 Bezpečnostní analýza objektu

Celkové zabezpečení společných prostor komplexu je velice dobré, a to díky tomu, že zdi okolních budov tvoří obvodovou ochranu a zamezují výhledu do prostor. Vjezd do komplexu je chráněn ocelovou dvoukřídlou bránou pro průjezd vozidel, jejíž součástí je i menší branka pro průchod osob. Brána pro vozidla je ovládána elektronicky pomocí dálkového ovladače a průchod pro osoby je zabezpečen bezpečnostním mechanickým zámkem a elektronickým zámkem ovládaným pomocí tlačítka uvnitř komplexu. Společné prostory jsou volně přístupné každý den pouze od 8:00 do 20:00, mimo tento čas je brána zavřená a zamčená, tudíž vstup do těchto prostor je umožněn pouze osobám vlastnícím klíč či dálkový ovladač nebo v doprovodu těchto osob. Za bezpečnostní faktor lze považovat i fakt, že z okolních budov komplexu je dobrý výhled na společné prostory, tudíž obyvatelé komplexu mohou zareagovat na podezřelou činnost.

[44] *ABBAS: Biometrie oka* [online]. Brno: © 2011–2021 ABBAS [cit. 2021-03-18]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/oko/

Ochranu objektu lze označit za nedostačující, a to díky absenci řádných bezpečnostních prvků. Hlavním nedostatkem objektu jsou vstupní a únikové dveře. Jedná se o starý typ skleněných dveří s železným rámem, díky čemuž lze jednoduše nahlížet do vnitřních prostor objektu. Zámky dveří jsou opatřeny jednoduchou cylindrickou vložkou, kterou pro zkušenější osobu není problém překonat. Dalším nedostatkem jsou okna, kterými lze ze společných prostor komplexu nahlížet na dění v objektu. V denní době má do objektu povolen přístup pouze majitel a jakákoliv osoba, které byl svěřen klíč nebo v doprovodu této osoby, za účelem vykonávat činnost související s poskytováním tělovýchovných a sportovních služeb v oblasti fitness. V nočních hodinách má do objektu přístup pouze majitel, který disponuje klíčem a elektronickým dálkovým ovladačem od vstupní brány komplexu.

5.3 Možnosti proniknutí do objektu

Možnosti proniknutí lze díky umístění objektu v komplexu rozdělit do dvou částí, jimiž jsou **proniknutí do komplexu** a **proniknutí do objektu**.

Proniknutí do komplexu

- Narušitel vnikne do komplexu ještě před tím, než se brána uzamkne.
- Odcizí či nalezne klíč nebo dálkový ovladač.
- Je vpuštěn do komplexu osobou.

Proniknutí do objektu

- Narušitel vnikne do objektu odcizením či nalezením klíče od objektu.
- Získáním klíče od osoby, které byl svěřen.
- Rozbitím či vypáčením dveří.
- Rozbitím či vypáčením oken.
- Vyháčkováním či odvrtáním cylindrické vložky.

Shrnutí

Z bezpečnostní analýzy a možností průniku lze usoudit, že objekt nedisponuje kvalitními mechanickými zábrannými systémy a EZS, které by zamezily vniknutí.

6 Prostředky pro zvýšení základního zabezpečení objektu

Aby do objektu mohla být nainstalována elektronická zabezpečovací zařízení, která by efektivně dokázala chránit prostor, musí být objekt nejprve vybaven kvalitními mechanickými zábrannými systémy. Nejslabšími prvky v zabezpečení objektu jsou dveře a okna.

Vchodové dveře

Pro zvýšení zabezpečení je třeba alespoň jedny ze dvou prosklených dveří zaměnit za dveře bezpečnostní s kvalitními zárubněmi, díky čemuž se značně zvýší doba pro průnik.

Únikové dveře

Únikový východ je třeba také vybavit bezpečnostními dveřmi a zárubněmi, avšak tyto dveře by měly být otevíratelné pouze z vnitřní strany a vybaveny panikovým zámkem a bezpečnostním kováním.

Okna

Zvýšení zabezpečení oken lze docílit několika způsoby, které se odlišují zejména cenou. Prvním a zároveň nejlevnějším způsobem je použití bezpečnostní folie, která zabrání vysypání skla po násilném zacházení. Tím také zvyšuje dobu pro průnik. Druhým způsobem je opatření oken mříží, která zabrání neoprávněné osobě proniknout do objektu. Posledním způsobem je vybavení oken bezpečnostními roletami. Výhodou rolet je zamezení proniknutí neoprávněné osoby a zároveň zamezení náhledu do vnitřních prostor objektu.

Orientační ceny základního zabezpečení

Vlastním šetřením jsem zjistil orientační ceny doporučených zabezpečovacích prvků včetně ceny montáže.

Tabulka č. 1 – Cenová relace zabezpečení dveří

Bezpečnostní prvek	**Cena bezpečnostního prvku**	**Cena montáže**
2x bezpečnostní dveře	19 700 Kč	3 600 Kč
2x bezpečnostní zárubně	6 000 Kč	7 000 Kč
Panikové kování a zámek	3 000 Kč	600 Kč
celkem	28 700 Kč	11 200 Kč

Zdroj: vlastní šetření

Závěrečná cena zabezpečení dveří včetně prací se pohybuje okolo 39 795 Kč

Tabulka č. 2 – Cenová relace zabezpečení oken

Bezpečnostní prvek	**Cena bezpečnostního prvku**	**Cena montáže**	**Celková cena i s montáží**
6 m^2 Bezpečnostní fólie	4 200 Kč	1 200 Kč	5 400 Kč
3x Okenní mříže	14 520 Kč	6 600 Kč	21 120 Kč
3x Bezpečnostní rolety	21 000 Kč	2 700 Kč	23 700 Kč

Zdroj: vlastní šetření

Dle výběru způsobu zabezpečení se závěrečná cena s montáží liší.

7 Návrh pro zabezpečení elektronickými a biometrickými bezpečnostními systémy

V této kapitole jsou vybrány a charakterizovány základní komponenty pro elektronický zabezpečovací systém a systém kontroly vstupu s prvky biometrie. Dílčím úkolem kapitoly je vytvořit nadstandardní možnosti či modifikace, které budou v závěru kapitoly komparovány.

7.1 Základní elektronický zabezpečovací systém

Ústředna JA-103KRY

Jedná se o mozek EZS, přes který lze programovat a nastavovat celý systém zabezpečení. Programování probíhá prostřednictvím počítačového softwaru F-link a dokáže pojmout až 50 sběrnicových nebo bezdrátových zón. Ústředna je vybavena jedním rádiovým modulem s názvem JA-111R, který je určen pro komunikaci s bezdrátovým prostředím systému, jako jsou detektory či klávesnice, a jedním modulem s názvem JA-192Y. Díky tomuto modulu probíhá komunikace mezi samotným systémem a obsluhou pomocí již zmíněnému programu F-link nebo mobilní aplikace MyJablotron. Dále modul dokáže předávat poplachové SMS zprávy, hlasové zprávy a poplachové zprávy pro pult centralizované ochrany. Veškeré zprávy a události jsou uchovány v paměťové kartě o velikosti 1 GB. Ústředna je dodávána v ochranném boxu, který lze připevnit na zeď.

Souhrn vlastností

- Nastavování pomocí softwaru
- Nastavování pomocí mobilní aplikace
- 50 sběrnicových nebo bezdrátových zón
- Bezdrátová komunikace s příslušenstvím
- Propojení s PCO
- Poplachové zprávy
- Paměťová karta na události

Ovládací klávesnice JA-153E

Prvek sloužící k zakódování či odkódování zabezpečovacího systému. Jedná se o bezdrátovou verzi napájenou dvěma alkalickými bateriemi AA 1,5 V. Obsahuje

číselnou klávesnici a čtečku RFID čipů pro snadnější obsluhu. Samostatné ovládání je zprostředkováno pomocí ovládacího segmentu v horní části zařízení.

Souhrn vlastností

- Bezdrátová komunikace
- Číselná klávesnice
- Čtečka RFID

Detektor JA-150P

Bezdrátový detektor používající technologii PIR určený pro vnitřní prostředí. Detekční úhel tohoto detektoru činí 110° a 12 m se základní čočkou. Napájení je provedeno dvěma alkalickými bateriemi AA 1,5 V a díky funkci smartwatch je životnost baterie prodloužena až na dva roky. Detektor je možno modifikovat pomocí čoček a tím zlepšit jeho detekční vlastnosti.

Souhrn vlastností

- Bezdrátová komunikace
- PIR detekce
- Detekční pokrytí 110°/12 m
- Funkce smartwatch
- Možnost modifikace čoček

Siréna JA-150A

Tato siréna je určena pro vnitřní prostředí, proto je hlasitost sirény nastavena na 85 dB/1 m. Jedná se o bezdrátový prvek s vlastním specifickým dobíjecím akumulátorem, jehož životnost činí 3 roky.

Souhrn vlastností

- Bezdrátová komunikace
- Hlasitost 85 dB/1 m

Akumulátor SA214-2.6 Jablotron

Jedná se o záložní bezúdržbový zdroj pro ústřednu JA-103KRY, který dokáže udržet systém EZS v aktivním režimu i při výpadku elektrické energie.

Souhrn vlastností

- Bezúdržbovost
- Přesné rozměry pro ústřednu JA-103KRY

Instalace a umístění komponentů EZS v objektu.

Ochranný box s ústřednou je třeba umístit na místo, které není na první pohled vidět. Důvodem umístění ústředny na skryté místo je snížení rizika pro neoprávněnou manipulaci a případnou sabotáž. Nejvýhodnější místo pro umístění komponentu je proto na stěně kancelářské místnosti, kde díky vhodně umístěnému nábytku bude box ústředny skrytý před zraky osob. Do boxu bude poté nainstalován akumulátor.

Klávesnice musí být umístěna na dobře přístupném místě, aby po vstupu do objektu mohlo dojít včas k odkódování systému. Vhodné místo pro umístění klávesnice je na stěně u pracovního stolu v kancelářské místnosti.

Detektory musí být umístěny tak, aby využily co nejvíce svého detekčního pokrytí, proto se nejčastěji umísťují do rohů místností. V tomto případě by byl jeden detektor umístěn v pravém horním rohu kancelářské místnosti a druhý detektor v pravém horním rohu tělocvičny.

Siréna bude z důvodu těžké přístupnosti umístěna co nejvýše na stěnu v místnosti tělocvičny.

Veškerá montáž musí být provedena certifikovaným pracovníkem, který následně systém podrobí zkoušce funkčnosti a uvede jej do provozu.

7.2 Základní systém kontroly vstupu s prvky biometrie

Snímací zařízení Sebury sPress (SF01)

Jedná se o biometrické snímací zařízení otisku prstu, které dokáže pracovat autonomně. Tělo čtečky se skládá z kvalitního kovu, čímž zvyšuje odolnost proti nástrojům, vandalizmu a lze jej použít i ve venkovním prostředí. Obsah paměti je 1000

uživatelů a jejich nastavování probíhá pomocí ovladače nebo po naskenování manažerského otisku. Díky režimu spánku šetří energii a zvyšuje životnost čtečky. Probuzení proběhne velmi rychle po přiblížení k senzoru umístěného na kovovém těle. Čtení otisku probíhá statickým reflexním snímáním s rychlostí 1 vteřinu. Chybovost čtečky je FAR 0,0000256 % a FRR 0,0198 %.

Shrnutí vlastností:

- Kovové provedení těla
- Použití vnitřní i venkovní (u venkovního je doporučeno použít ochrannou stříšku)
- Paměť 1000 uživatelů
- Doba čtení otisku 1 vteřina

Elektromechanický samozamykací zámek ERBI SAM EL 7255

Pro objekt jsem vybral právě tento zámek z důvodu, že při poruše SKV nebo výpadku proudu lze zámek odemknout pomocí klíče. Další výhodou je možnost nastavení zámku do panikové funkce, tudíž není potřeba objekt vybavovat odchodovým tlačítkem. Rozměry zámku jsou srovnatelné s klasickým mechanickým zadlabávacím zámkem, a proto není potřeba složitých úprav při instalaci do dveří. Zámek je také možno nainstalovat na levou či pravou stranu dveří a má funkci samozamykání. Veškeré kritické díly jsou z nerezové oceli a tím vytváří vysokou odolnost vůči poškození a vandalizmu.

Shrnutí vlastností:

- Možnost odemknutí pomocí klíče
- Oboustranná instalace
- Paniková funkce
- Rozměry klasického zámku
- Kovové provedení
- Samozamykací funkce

Napájecí zdroj SEBURY BPS-09

Posledním důležitým komponentem je napájecí zdroj, který zásobuje elektřinou celý SKV. SEBURY BPS-09 má vestavěný ochranný modul, který chrání zařízení proti přepětí a snižuje zatížení přístupové jednotky.

Souhrn vlastností:

- Napájení SKV
- Ochranný modul proti přepětí

Kabely a příslušenství

- Přívod energie do napájecího zdroje bude proveden kabelem CYKY – J 3x1,5.
- Z napájecího zdroje bude pro napájení snímacího zařízení zaveden kabel H05VV-F 2x1.
- Pro přenos signálu mezi komponenty bude použit kabel FI-HX08/02.
- Veškerá kabeláž bude vedena kabelovými žlaby nebo podlahovými lištami.
- Ochranný box SEZ P-BOX 2030 pro napájecí zdroj, který lze připevnit na stěnu.

Tabulka č. 3 – Cenová relace standardního návrhu

Komponent	Cena
Ústředna JA-103KRY	12 700 Kč
Ovládací klávesnice JA-153E	2 600 Kč
Detektor JA-150P	3 600 Kč
Siréna JA-150A	1 400 Kč
Akumulátor SA214-2.6 Jablotron	400 Kč
Snímací zařízení Sebury sPress (SF01)	2 600 Kč
Elektromechanický samozamykací zámek ERBI SAM EL 7255	6 800 Kč
Napájecí zdroj SEBURY BPS-09	600 Kč
Kabely a příslušenství	600 Kč
Ochranný SEZ P-BOX 2030	700 Kč
Montáž (cca 4 hodiny)	2 500 Kč
Celkem	**34 500 Kč**

Zdroj: vlastní šetření

Závěrečná cena komponentů základního návrhu včetně montáže je 34 500 Kč.

Instalace a umístění komponentů SKV v objektu

Box se zdrojem napájení bude umístěn na skrytém místě vedle ústředny EZS, aby se předešlo sabotáži či neoprávněnému manipulování.

Nejvhodnější místo pro umístění snímacího zařízení je na stěně v prostoru mezi prvními a druhými vchodovými dveřmi. Toto místo bylo vybráno, protože prostor mezi dveřmi je zcela bez využití a dokáže vytvořit přirozenou ochranu proti přírodním vlivům, popřípadě vandalizmu.

Díky rozměru a tvaru elektronického zámku není potřeba žádných speciálních úprav bezpečnostních dveří pro jeho zadlabání.

Vedení kabelů bude realizováno od boxu se zdrojem napájení po stěnách pomocí kabelových žlabů, v podlaze pomocí podlahových lišt a přivedení ke čtečce skrze stěnu u vchodových dveří. Veškeré příslušenství pro propojení kabelů se zámkem je součástí balení elektronického zámku.

Závěrem instalace je kontrola a vyzkoušení systému montážním pracovníkem a následné uvedení do provozu.

7.3 Nadstandardní možnosti a modifikace

Pokud by byl investor ochoten uvolnit více finančních prostředků pro zvýšení zabezpečení objektu, tak tato podkapitola nabízí nadstandardní možnosti komponentů.

Detektor JA-160PC (90)

Tento bezdrátový detektor využívající technologii PIR dokáže detekovat zónu 90°/12 m a je navíc obohacen o kameru, která slouží k vizuálnímu potvrzení poplachu. Při zaznamenání poplachu detektor pořídí barevný snímek o rozlišení 640x480 bodů. Detektor je vybaven bleskem, díky kterému je lepší kvalita snímku i za tmy. Napájení je prováděno dvěma alkalickými bateriemi AA 1,5 V. Typická životnost baterie je 2 roky.

Souhrn vlastností

- Bezdrátová komunikace
- Kamera
- PIR technologie

- Detekční pokrytí 90°/12 m

Kompletní set ACB-001 s řídící jednotkou SEBURY BC800NT1

Set se skládá z řídící jednotky se zabudovaným zdrojem napájení a plechového boxu, ve kterém je tento komponent připevněn. Řídící jednotka využívá ke komunikaci se snímacími zařízeními rozhraní wiegand 26-34. Dokáže spojit jeden elektronický zámek až se dvěma snímacími zařízeními. Disponuje pamětí až pro 20 000 uživatelů a dokáže zaznamenat maximálně 100 000 událostí. Díky paměti pro zaznamenání událostí lze zpětně vyhledat, který uživatel a ve kterém čase použil čtecí zařízení, tudíž vstoupil do objektu. Pokud řídící jednotka vyhodnotí neoprávněné manipulování se čtecím zařízením, ihned spustí alarm. K řídící jednotce je dodáván sofistikovaný ovládací program, kterým lze po nainstalování do počítače spravovat veškeré nastavení řídící jednotky. Mezi toto nastavení spadá: povolení vstupu uživatelům, a to včetně povolení jen v určité době, nastavení časového intervalu, po který mohou být dveře otevřené, monitorování uživatelů v reálném čase a spravování veškerých uživatelů. Řídící jednotku lze připojit k počítači pomocí TCP/IP rozhraní a díky tomu lze celý systém ovládat a nastavovat vzdáleně. Veškeré tyto programové možnosti vytvářejí plnohodnotný docházkový systém, který dokáže události uživatelů přetransformovat do přehledného MS Excel formátu. Řídící jednotku lze propojit s ústřednou JA-103KRY a díky tomu lze nastavit dva módy SKV. V prvním módu u dlouho otevřených dveří řídící jednotka vyšle signál do ústředny a tím spustí alarm. V druhém tzv. TOGGLE módu řídící jednotka po správné identifikaci odemkne zámek a následné zamknutí provede až po další správné identifikaci. K připojení řídící jednotky je potřeba vybavit ústřednu sběrnicovým modulem JA-111H-AD, který tyto dva komponenty dokáže propojit.

Souhrn vlastností:

- Nastavování pomocí počítače
- Vzdálený přístup
- Speciální program pro nastavení
- Paměť pro 20 000 uživatelů
- Zaznamenání max. 100 000 událostí
- Propojí 2 snímače s 1 zámkem
- Možnost propojení s EZS
- Rozhraní wiegand 26-34 pro komunikaci se snímacím zařízením
- Rozhraní TCP/IP pro komunikaci s počítačem

- Události lze přetransformovat do MS Excel tabulky

Snímací zařízení Zoneway T501

Jedná se o snímací zařízení, které kombinuje 4 možnosti identifikace, jimiž jsou: otisk prstu, rozpoznání obličeje, RFID čtečka karet a čipů, PIN kód. Zabudovaný snímač otisku prstů využívá k získání vzorku otisku prstu kapacitní technologie a dokáže uložit až 10 000 šablon otisků prstů. Rozpoznání obličeje je zprostředkováno pomocí kamer a technologií 3D snímání. Systém rozpozná obličej i přes brýle, čepici, make-up a vousy. Kapacita paměti pro šablony obličeje činí 1 000. Stejná kapacita je i pro množství PIN kódů, které zařízení dokáže pojmout. Číselná klávesnice je tvořena jednotlivou kapacitní dotykovou vrstvou, tudíž je zde snížené opotřebení. RFID čtečka dokáže pojmout také 1 000 jednotlivých karet či čipů. Jednotlivé možnosti identifikace lze používat samostatně nebo v kombinacích. U kombinací není žádné omezení v počtu či druhu. Tělo snímacího zařízení má kovové provedení z duralové slitiny a vysokou odolnost proti vandalizmu. Součástí těla je i 2,8 palcový display. Přenosové rozhraní wiegand lze nastavit na hodnotu 26 nebo 34. I když se jedná o snímací zařízení jiného výrobce než je řídící jednotka, oba dva komponenty jsou spolu zcela kompatibilní. Součástí balení je i bezdrátový zvonek s dosahem 50 m od snímacího zařízení. Chybovost Zoneway T501 je udávána FAR 0,0001 % FRR 0,1 %.

Souhrn vlastností:

- 4 možnosti identifikace
- Neomezené kombinace identifikace
- Paměť pro uživatele 1000
- Paměť pro otisky 10 000
- Paměť RFID 1000
- Paměť PIN kódů 1000
- Paměť rozpoznání obličejů 1000
- Kapacitní snímač otisků prstů
- 3D technologie rozpoznání obličeje
- Kovové tělo
- Kapacitní povrch dotykové klávesnice
- 2,8 palcový display
- Rozhraní wiegand 26 nebo 34
- Bezdrátový zvonek

Instalace nadstandardních komponentů v objektu

Ochranný box s řídící jednotkou a zdrojem napájení bude umístěn na skrytém místě vedle ústředny EZS a propojen pomocí modulu JA-111H-AD.

Ostatní umístění a postupy při instalaci komponentů jsou stejné jako u předchozích návrhů s rozdílem záměny snímacího zařízení Sebury sPress (SF01) za snímací zařízení Zoneway T501 a záměny detektorů JA-150P za detektory JA-160PC (90).

Tabulka č. 4 – Cenová relace nadstandardního návrhu

Komponent	Cena
Ústředna JA-103KRY	12 700 Kč
Ovládací klávesnice JA-153E	2 600 Kč
2x Detektor JA-160PC (90)	6 600 Kč
Siréna JA-150A	1 400 Kč
Akumulátor SA214-2.6 Jablotron	400 Kč
Snímací zařízení Zoneway T501	5 800 Kč
JA-111H-AD	800 Kč
Kompletní set ACB-001 s řídící jednotkou SEBURY BC800NT1	3 800 Kč
Elektromechanický samozamykací zámek ERBI SAM EL 7255	6 800 Kč
Kabely a příslušenství	600 Kč
Montáž (cca 5 hodin)	2 500 Kč
Celkem	**44 000 Kč**

Zdroj: vlastní šetření

Závěrečná cena komponentů nadstandardního návrhu včetně montáže je 44 000 Kč, což činí cenový rozdíl mezi návrhy 9 500 Kč.

7.4 Doporučení a komparace vlastností návrhů

Investorovi je doporučen výběr nadstandardního návrhu. Hlavními důvody výběru jsou: vyšší ochrana před sabotáží, detektory se záznamovou kamerou, možnost víceúrovňové identifikace, kompatibilita EZS s SKV, docházkový systém, databáze o uživatelích. Veškeré rozdíly mezi návrhy jsou rozepsané v následující tabulce.

Tabulka č. 5 – Komparace návrhů

Porovnávaná vlastnost	Základní návrh	Nadstandardní návrh
Možnosti identifikace	Otisk prstu	Otisk prstu, rozpoznání obličeje, PIN kód, RFID karta/čip
Ovládání SKV	Pomocí dálkového ovladače	Skrze počítačový program
Paměť na uživatele	1 000	20 000
Paměť na události	Ne	Max. 100 000 událostí
Vizuální potvrzení poplachu	Ne	Ano
Zvýšená ochrana proti sabotáži	Ne	Ano
Databáze o uživatelích	Ne	Ano
Docházkový systém	Ne	Ano
Propojení EZS a SKV	Ne	Ano
Cena	34 500 Kč	44 000 Kč

Zdroj: vlastní šetření

Závěr

Cílem bakalářské práce bylo teoreticky charakterizovat základní pojmy oboru elektronických zabezpečovacích systémů a systémů kontroly vstupu. Zároveň poukázat na možnost aplikace biometrických prvků do těchto systémů. Dílčím cílem bylo na předem vybraném objektu vytvořit analýzu zabezpečení, od které se odvíjela doporučení pro zvýšení zabezpečení mechanickými zábrannými systémy a návrhy na zabezpečení elektronickými zabezpečovacími systémy a systémy kontroly vstupu s prvky biometrie. Samotné návrhy byly komparovány díky čemuž bylo možné jeden z těchto návrhů doporučit investorovi.

První část práce se zaobírá teorií elektronických zabezpečovacích systémů, jelikož se jedná o jeden z prvků použitých v návrzích zabezpečovacích systémů v závěru práce. Jsou zde uvedeny základní definice, používané normy a základní komponenty struktury elektronických zabezpečovacích systémů. Další část práce definuje druhý použitý prvek, což je systém kontroly vstupu, kde je poukázáno na možnosti identifikace osob pomocí jednotlivých identifikačních prvků a jejich samotné čtení pomocí čtecích zařízení. Závěrem první části práce jsou možnosti aplikace biometrie v systému kontroly vstupu.

Druhá část práce je zaměřena na objekt SAWADE GYM & SHOP, pro který je vytvořena bezpečnostní analýza, z níž lze vyhodnotit, že objekt nedisponuje dostatečně kvalitními mechanickými zábrannými systémy a elektronické zabezpečovací systémy zde zcela chybí. Na základě této analýzy bylo investorovi doporučeno modifikovat mechanické zábranné systémy, jelikož jsou základním stavebním kamenem pro správné fungování pozdějších návrhů elektronického zabezpečení. Závěrem práce jsou vytvořeny dva návrhy obsahující elektronický zabezpečovací systém a systém kontroly vstupu. Jedná se o základní návrh a návrh s nadstandardními možnostmi. V obou návrzích jsou detailně charakterizovány funkce a možnosti jednotlivých komponentů, včetně jejich cenové relace. Dále díky komparaci je doporučen návrh, který má jednoznačně více možností, je efektivnější a jednodušší na obsluhu.

Přínosem bakalářské práce je jednoznačně rozšíření znalostí bezpečnostních systémů jak pro samotného autora, tak pro případné čtenáře. Dále práce poukazuje na nutnost vytvoření alespoň základní bezpečnostní analýzy, bez které by byla vysoká pravděpodobnost vytvoření zcela neadekvátního systému zabezpečení. Poznatkem

bakalářské práce je i celkově přívětivá cenová dostupnost bezpečnostních systémů, které lze použít nejen na zabezpečení provozoven, ale i rodinných domů či bytů.

Seznam použitých zdrojů

Literární zdroje

1. BURDA, Karel. *Základy elektronických zabezpečovacích sytému*. Brno: CERM, 2017, 123 s. ISBN 978-80-7204-967-7.

2. ČANDÍK, Marek. *Objektová bezpečnost II.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 100 s. ISBN 80-7318-217-3.

3. ČSN CLC/TS 50131-7: *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy – Část 7*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. 48 s. Třídící znak. 334591

4. ČSN EN 50131-1 ed. 2: *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2015. 40 s. Třídící znak. 334591

5. ČSN EN 60839-11-1: *Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 56 s. Třídící znak. 334593

6. ČSN EN 60839-11-2: *Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 34 s. Třídící znak 334593

7. HORN, Delton. T. *Electronic Alarm and Security Systems: A Technician's Guide*. New York City: McGraw-Hill, 1995, 272 s. ISBN 9780070305298.

8. IDB Journal. Bratislava: HMH, 2012, č. 5. ISSN 1338-3379

9. KŘEČEK, Stanislav. *Příručka zabezpečovací techniky. 3*. Blatná: Cricetus, 2006. 313 s. ISBN 80-902938-2-4.

10. KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti ČR, 2014, 390 s. ISBN 978-80-260-7115-0.

11. PETRUZZELLIS, Thomas. *The Alarm, Sensor & Security Circuit Cookbook*. New York: TAB Books, 1994. 286 s. ISBN 0-8306-4314-1.

12. RAK, Roman, MATYÁŠ, Václav, a ŘÍHA, Zdeněk., *Biometrie a identita člověka*. Praha: Grada, 2008. 631s. ISBN 978-80-247-2365-5.

13. UHLÁŘ, Jan. *Technická ochrana objektů I. díl: Mechanické zábranné systémy* Praha: Vydavatelství Policejní akademie České republiky, 2004. 179 s. ISBN 80-7251-172-6.

14. UHLÁŘ, Jan. *Technická ochrana objektů II. díl: Elektrické zabezpečovací systémy II.* Praha: Policejní akademie České republiky, 2005. 229 s. ISBN 80-7251-189-0.

15. UHLÁŘ, Jan. Technická *ochrana objektů III. díl: Ostatní zabezpečovací systémy*. Praha: Policejní akademie české republiky, 2006. 246 s. ISBN 80-7251-235-8.

Elektronické zdroje

1. ŠČUREK, Radomír. *Biometrické technologie: Technické prostředky bezpečnostních služeb* [online]. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava, 2015, 115 s. [cit. 2022-04-07]. ISBN 978-80-248-3786-4. Dostupné z: https://www.fbi.vsb.cz/export/sites/fbi/060/.content/galerie-souboru/studijni-materialy/BiometrickeTechnologie.pdf

2. ŠURKALA, Milan. *Digimanie: Detekce a rozpoznání tváří: vím, kdo jsi!* [online]. Příbram: oXyShop, 19. 3. 2014, [cit. 2022-04-07]. Dostupné z: https://www.digimanie.cz/detekce-a-rozpoznani-tvari-vim-kdo-jsi/5500-2

3. GRYGAŘÍKOVÁ, Michaela. *MasterDC: Datacentra Masteru jako nedobytný hrad. I díky biometrické autentizaci* [online]. Praha: MasterDC, 28. 09. 2019 [cit. 2022-04-07]. Dostupné z: https://www.master.cz/blog/biometricka-autentizace-v-datacentru/

Seznam zkratek

SKV – systém kontroly vstupu

EZS – elektronické zabezpečovací systémy

PIN – personal identification number

EAN – european article number

FRR – false rejection rate

FAR – false acceptance rate

ERR – equal error rate

PCA – principal components analysis

LDA – linear discriminant analysis

EBGM – elastic bunch graph matching

TCP/IP – Transmission Control Protocol/Internet Protocol

RFID – Radio Frequency Identification

Seznam tabulek a grafů

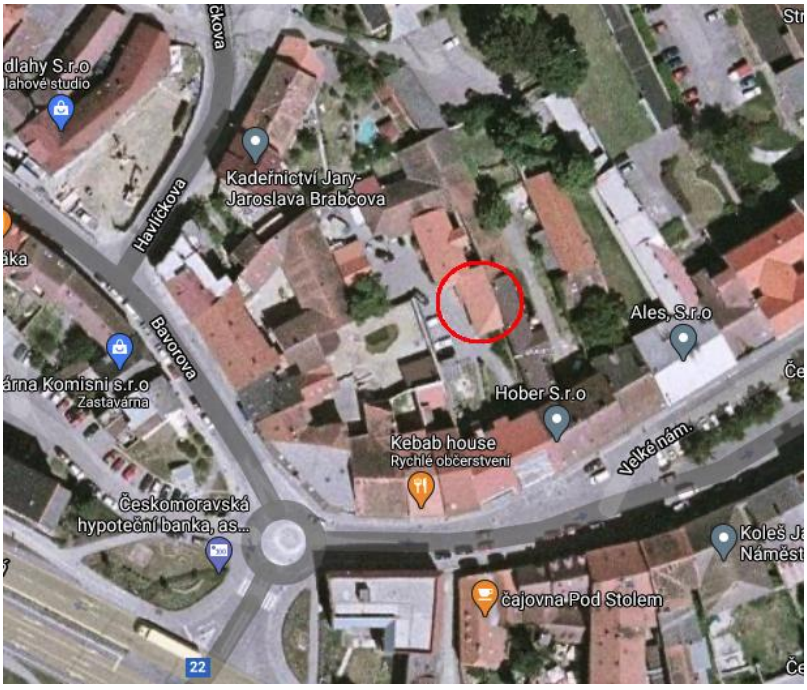
Přílohy

Příloha č. I – obrázky

Obrázek č. 1 – Komplex, ve kterém se objekt nachází

Zdroj: https://www.google.com/maps/@49.2609513,13.9004203,153m/data=!3m1!1e3
+ vlastní zakreslení

Obrázek č. 2 – Vyznačení objektu



Zdroj: https://www.google.com/maps/@49.2609513,13.9004203,153m/data=!3m1!1e3
+ vlastní zakreslení

Obrázek č. 3 – Vchod do objektu

Zdroj: Vlastní

Obrázek č. 4 – Kancelářská místnost

Zdroj: Vlastní

Obrázek č. 5 – Hlavní vchod z vnitřní strany objektu

Zdroj: Vlastní

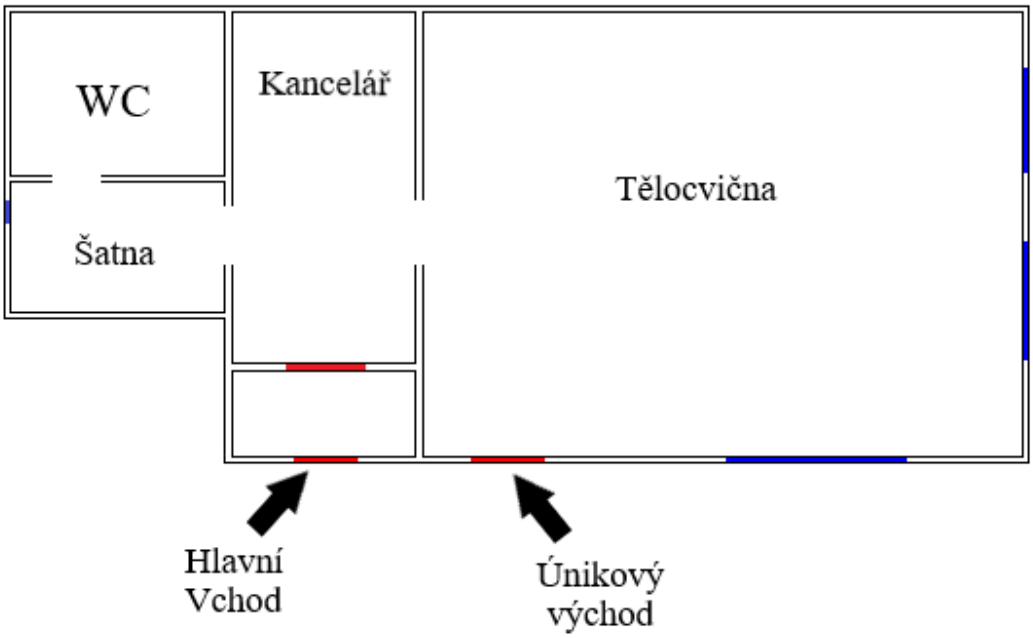
Obrázek č. 6 – Šatna

Zdroj: Vlastní

Obrázek č. 7 – Pohled z kancelářské místnosti do tělocvičny

Zdroj: Vlastní

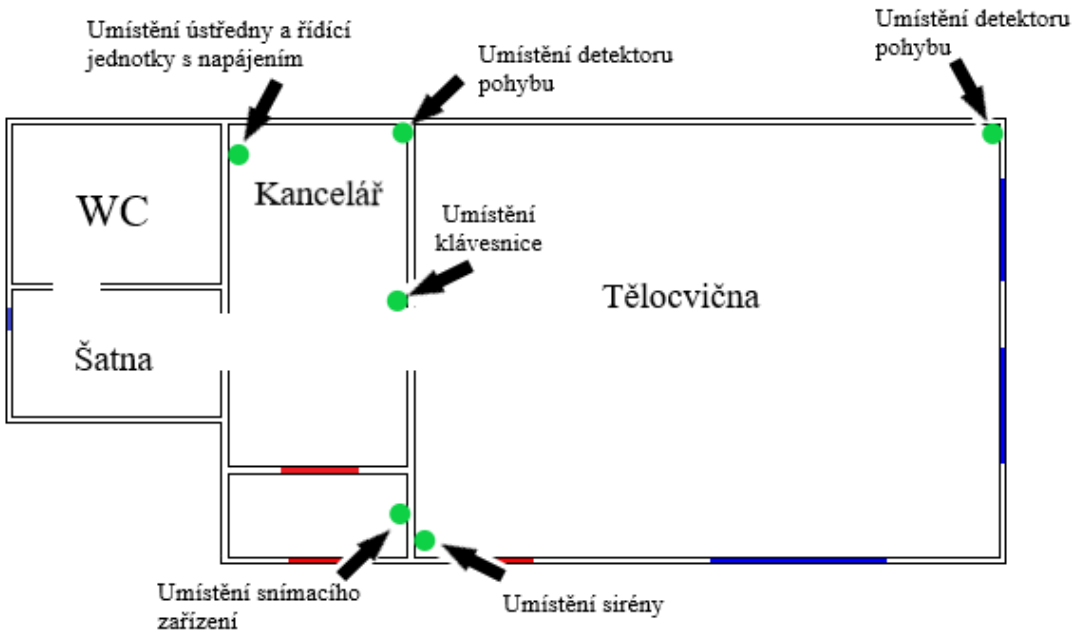
Obrázek č. 8 – Plánek budovy



Červeně zvýrazněné jsou vchody. Modře zvýrazněná jsou okna.

Zdroj: Vlastní

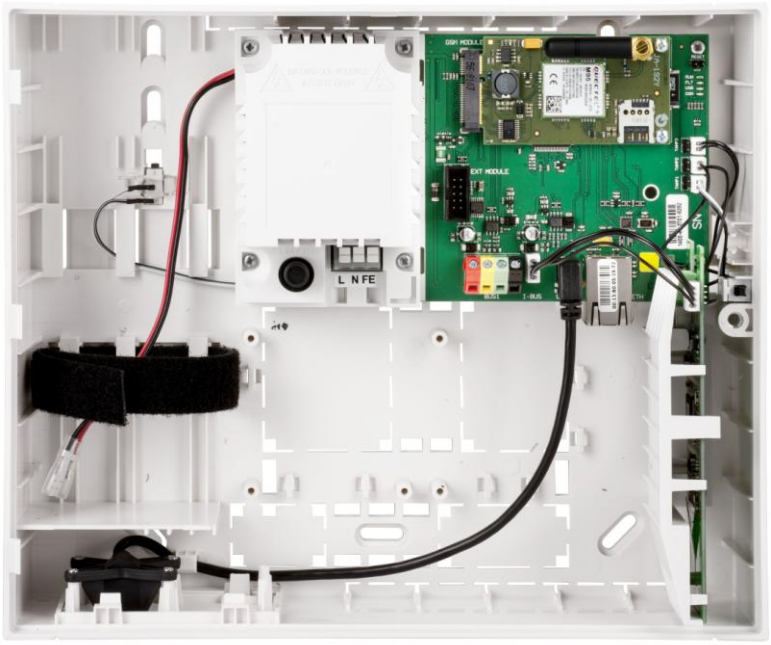
Obrázek č. 9 – Plánek s umístěním komponentů



Červeně zvýrazněné jsou vchody. Modře zvýrazněná jsou okna. Zeleně označená jsou místa umístění komponentů.

Zdroj: Vlastní

Obrázek č. 10 – Ústředna JA-103KRY



Zdroj: https://eshop.eurosat.cz/product/99796/351/JA-103KRY

Obrázek č. 11 - Ovládací klávesnice JA-153E

Zdroj: https://eshop.eurosat.cz/product/48123/10637/JA-153E

Obrázek č. 12 – Detektor JA-150P

Zdroj: https://eshop.eurosat.cz/product/45373/10369/JA-150P

Obrázek č. 13 – Siréna JA-150A

Zdroj: https://eshop.eurosat.cz/product/48124/10609/JA-150A

Obrázek č. 14 - Akumulátor SA214-2.6 Jablotron

Zdroj:https://www.jabloshop.cz/sa214-2-6-bezudrzbove-akumulatory?gclid=EAIaIQobChMIjYvknqmE9wIV5pBoCR0MWgl_EAQYASABEgJpdvD_BwE#444

Obrázek č. 15 - Snímací zařízení Sebury sPress (SF01)

Zdroj: https://sebury.com.cz/Biometricka-ctecka-otisku-prstu-Sebury-sPress-S-200-SF01

Obrázek č. 16 - Elektromechanický samozamykací zámek ERBI SAM EL 7255

Zdroj: https://www.euroalarm.cz/eshop-zabezpecovaci-technika/pristup-a-dochazka/samozamykaci-zamky/elektromechanicke/72-55-interierove/sam-el-7255/?gclid=EAIaIQobChMI75Wp9qmE9wIVBNN3Ch2hKQqfEAQYASABEgKrI_D_BwE

Obrázek č. 17 - Napájecí zdroj SEBURY BPS-09

Zdroj: https://sebury.com.cz/zdroj-bps-09?search=Nap%C3%A1jec%C3%AD%20zdroj%20SEBURY%20BPS-09&description=1

Obrázek č. 18 - Detektor JA-160PC (90)

Zdroj: https://eshop.eurosat.cz/product/48159/351/JA-160PC

Obrázek č. 19 - Kompletní set ACB-001 s řídící jednotkou SEBURY BC800NT1

Zdroj: https://sebury.com.cz/SEBURY-BC800NT1-ridici-jednotka-pro-1-dvere-IP-komunikace-cesky-SW-v-cene?search=ACB-001%20&description=1

Obrázek č. 20 - sběrnicový modul JA-111H-AD

Zdroj: https://www.jabloshop.cz/ja-111h-ad-trb-sbernicovy-modul-ovladani-systemu?gclid=EAIaIQobChMIhrmN9ayE9wIVielRCh0ZMg15EAAYASAAEgJFnvD_BwE

Obrázek č. 21 - Snímací zařízení Zoneway T501

Zdroj: https://zoneway.cz/acs-zoneway/pristupovy-system-s-funkci-3dfcr-rozpoznani-obliceje-t501