Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Technologie elektronických zabezpečovacích systémů

Bc. Michal Dvořák

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Michal Dvořák

Systémové inženýrství a informatika
Informatika

Název práce

Technologie elektronických zabezpečovacích systémů

Název anglicky

Electronic Security Systems Technologies

Cíle práce

Práce je tematicky zaměřena na elektronické zabezpečovací systémy. Hlavní cíl DP je analýza současného trhu s řešeními pro elektronické zabezpečovací systémy včetně kvalitativního srovnání jednotlivých řešení a výběr nejlepší varianty dle stanovených kritérií. Dílčí cíle práce jsou:
- návrh pilotního nasazení vybrané varianty pro reálný rodinný dům a
- vypracování přehledu technologií elektronických zabezpečovacích systémů.

Metodika

Metodika řešené problematiky diplomové práce je založena na studiu a analýze odborných informačních zdrojů. Vlastní práce spočívá v objektivních analýze současného trhu s řešením pro elektronické zabezpečovací systémy, jejich hodnocení, srovnání včetně možností návaznosti na chytrou domácnost a výběr nejlepší varianty dle stanovených kritérií s návrhem reálného pilotního nasazení. Na základě syntézy teoretických poznatků a výsledků praktické části budou formulovány závěry diplomové práce.

Doporučený rozsah práce

60 – 80 stran textu.

Klíčová slova

Elektronický zabezpečovací systém, EZS, detektory, kamery, alarm, bezpečnost.

Doporučené zdroje informací

BROŽOVÁ, Helena a Milan HOUŠKA. Základní metody operační analýzy. Praha: Credit, 2002. ISBN 978-80-213-0951-7.

BURDA, Karel. Základy elektronických zabezpečovacích systémů. Brno: Akademické nakladatelství CERM, 2017. ISBN 978-80-7204-967-7.

CARLSEN, John. Everything You Need to Know about Home Security. SafeWise [online]. c2021, May 27, 2021. Dostupné z: https://www.safewise.com/everything-you-need-to-know-about-home-security/

KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 2. S.l.: Cricetus, 2003. ISBN 80-902-9382-4.

Předběžný termín obhajoby

2021/22 LS – PEF

Vedoucí práce

Ing. Pavel Šimek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 10. 8. 2021

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2021

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 19. 10. 2021

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Technologie elektronických zabezpečovacích systémů" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 21.03.2022 _____

Poděkování

Rád bych touto cestou poděkoval doc. Ing. Pavlu Šimkovi, Ph.D. za ochotu, vstřícnost a odborné rady na konzultacích, které mi pomohli při zpracování této diplomové práce.

Technologie elektronických zabezpečovacích systémů

Abstrakt

Tato diplomová práce se zaměřuje na výběr elektronického zabezpečovacího systému pro reálný rodinný dům. Hlavním cílem této práce je průzkum nabídky elektronických zabezpečovacích systémů na českém trhu a následný výběr kompromisní varianty na základě stanovených kritérií. Dílčím cílem práce je zpracování přehledu technologií, které se v těchto systémech využívají a vytvořit návrh pilotního nasazení vybraného systému. Rešeršní část práce je věnována právě již zmíněným technologiím používaných u ústředen, detektorů, kamer a také normám, které s elektronickými zabezpečovacími systémy souvisí. Praktická část se zabývá výběrem kompromisní varianty elektronického zabezpečovacího systému z nabídky od třech největších výrobců působících na českém trhu. Výběr je prováděn pomocí metody TOPSIS, metody váženého součtu a na základě jedenácti hodnoticích kritérií, pro které jsou stanoveny váhy pomocí Saatyho metody párového porovnání. Vítězná varianta je použita pro zpracování návrhu pilotního nasazení systému a cenové kalkulace pro daný objekt.

Klíčová slova: Elektronický zabezpečovací systém, EZS, ústředna, detektor, kamera, alarm, bezpečnost, vícekriteriální analýza variant, porovnání

Electronic Security Systems Technologies

Abstract

This diploma thesis focuses on the selection of the electronic security system for a real detached house. The main aim of the thesis is the research of the electronic security systems' offers on the Czech market and the subsequent choice of the compromise options based on the set criteria. The partial aim of the thesis is to compile an overview of technologies that are used in given systems and to create a draft for the pilot deployment of the selected system. The research part of the thesis is dedicated to the already mentioned technologies which are used in control panels, detectors, camcorders and also the standards related to electronic security systems. The empirical part deals with the selection of the compromise variant of the electronic security system from the offers from the three greatest producers operating on the Czech market. The selection is carried out using the TOPSIS method, the weighted sum method and on the basis of the eleven evaluation criteria, for which weights are set using the Saaty pairwise comparison method. The winning variant is employed for the processing of a draft for the pilot deployment of the system and the price calculation for the given building.

Keywords: Electronic security system, ESS, control panel, detector, camera, alarm, security, multiple-criteria decision analysis, comparison

Obsah

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam použitých zkratek

EZS – Elektronický zabezpečovací systém

PZTS – Poplachový zabezpečovací a tísňový systém

PZS – Poplachový zabezpečovací systém

PCO – Pult centrální ochrany

PIR – Pasivní infračervený detektor (Pasive infrared)

MW – Mikrovlnný detektor (Microwave)

US – Ultrazvukový detektor (Ultrasonic)

IP – Internet protokol

CCTV – Uzavřený televizní okruh (Closed Circuit Televison)

RFID – Identifikace na rádiové frekvenci (Radio Frequency Identification)

POE – Napájení pomocí ethernetu (Power Over Ethernet)

1 Úvod

Bezpečnost a s tím spojená ochrana majetku a osob je téma, o kterém se hlavně v dnešní době stále více mluví. Dle Českého statistického úřadu bylo v České republice jen za rok 2020 spácháno přes pět a půl tisíc trestných činů spojených s vloupáním do rodinných domů, bytů či rekreačních objektů. I proto v dnešní době stále více lidí investuje do zabezpečení jejich majetku.

Zabezpečovací systémy se postupem času staly dostupnější a díky tomu je tak možné na trhu narazit, jak na jednoduché systémy pro zabezpečení malých prostor jako jsou například garáže či chatky tak velké komplexní systémy, které nabízejí možnost připojení velkého množství prvků pro maximální střežení daného objektu.

Je nutné konstatovat, že tyto systémy jsou především orientovány na zmírnění následků případného vloupání a informování majitele objektu či bezpečnostní agentury, která na základě spuštěného poplachu může vyslat na místo zásahovou jednotku. Elektronické zabezpečovací systémy ve většině případů přímo nezabraňují pachateli vstoupit do objektu, jen detekují jeho narušení. S tím souvisí správné nastavení a spolehlivost systému, aby zbytečně nedocházelo k nahodilým a planým poplachům.

Některé systémy nabízí také kromě běžné funkce zabezpečení možnost propojení s prvky chytré domácnosti. O prvky chytré domácnosti a automatizaci rutinních činností je stále větší zájem a díky tomuto propojení je tak možné ovládat například stínící techniku, osvětlení, vytápění, garážová a vjezdová vrata a mnoho dalšího pomocí jednoho systému.

2 Cíl práce a metodika

2.1 Cíl práce

Práce je tematicky zaměřena na elektronické zabezpečovací systémy. Hlavní cíl diplomové práce je analýza současného trhu s řešeními pro elektronické zabezpečovací systémy včetně kvalitativního srovnání jednotlivých řešení a výběr kompromisní varianty dle stanovených kritérií.

Dílčí cíle práce jsou:

- návrh pilotního nasazení vybrané varianty pro reálný rodinný dům
- vypracování přehledu technologií elektronických zabezpečovacích systémů.

2.2 Metodika

Rešerše této diplomové práce bude založena na studiu a analýze odborných informačních zdrojů. Zabývat se bude především technologiemi, které jsou využívané u elektronických zabezpečovacích systémů a také normami, které s nimi souvisí. Získané poznatky budou dále využity při zpracování praktické části.

Praktická část bude věnována výběru elektronického zabezpečovacího systému pro reálny rodinný dům. Nejprve bude popsán objekt pro, který bude systém vybírán. Součástí tohoto popisu bude stručná charakteristika objektu, jeho umístění, jednotlivých prostor v objektu včetně plánovaného zabezpečení a identifikace silných a slabých míst. Na základě tohoto popisu bude určen doporučený stupeň zabezpečení a klasifikace prostředí dle norem ČSN. Následně bude proveden průzkum nabídky komplexních elektronických zabezpečovacích systémů na českém trhu. Dostupné varianty budou podrobeny vícekriteriální analýze variant, s využitím metody TOPSIS a metody váženého součtu, ze které bude na základě stanovených kritérií a vypočtení jejich vah pomocí Saatyho metody párového porovnání, vybrána kompromisní varianta pro daný objekt. Pro tuto kompromisní variantu bude vytvořen návrh pilotního nasazení včetně blokového schéma, půdorysného schéma, popisu nastavení systému a cenové kalkulace.

3 Teoretická východiska

3.1 Předpisy a normy v ČR

V České republice jsou Evropské technické směrnice převzaty skrze Nařízení vlády ČR. Evropské směrnice jsou pak vydávány Evropskou komisí (dříve Evropská hospodářská komise). Tyto směrnice stanovují základní požadavky na elektronické zabezpečovací systémy. Členské země pak mají povinnost zapracovat tyto požadavky do národní legislativy. Jako podpora ke splnění požadavků pro výrobce, dovozce a distributory jsou vyhlašovány v Úředním věstníku Evropské Unie tzv. Evropské harmonizované normy, které slouží jako právní precedent. Tyto normy jsou zpracovávány organizacemi CEN – Evropský výbor pro normalizaci a CENELEC – Evropský výbor pro normalizaci v elektrotechnice. Normy pro poplachové systémy má na starost technická komise CENELEC/TC79 a pro elektronickou požární signalizaci pak technická komise CEN/TC72. [1]

Základní zákonem, který udává legislativní rámec v České republice je Zákon 22/97 Sb., o technických požadavcích na výrobky, účinný od 1. 9. 1997. Samotné zpracování evropských norem do ČSN (Českých technických norem) má za úkol Český normalizační institut. [1]

3.1.1 Norma ČSN EN 50131

Elektronické zabezpečovací systémy (EZS) jsou v České republice zařazeny pod soubor norem a technických specifikací ČSN EN 50131. Kromě těchto norem byli vydány také tři Technické normalizační informace (TNI) jakožto návod k jejich aplikaci. [1]

Dílčí části souboru norem ČSN EN 50131 a jednotlivé TNI jsou popsány v následujících tabulkách:

Tabulka 1 – Skupina norem pro elektronické zabezpečovací systémy

Označení	Popis
EN 50131-1	Systémové požadavky
CLC/TS 50131-2-2	Pasivní infračervené detektory (PIR)
CLC/TS 50131-2-3	Mikrovlnné detektory (MW)

CLC/TS 50131-2-4	Kombinované detektory (PIR/MW)
CLC/TS 50131-2-5	Kombinované detektory (UZ/PIR)
EN 50131-2-6	Detektory otevření
CLC/TS 50131-3	Ústředny
EN 50131-4	Výstražná zařízení
EN 50131-5-3	Prvky využívající bezdrátové propojení
EN 50131-6	Napájecí zdroje
CLC/TS 50131-7	Pokyny pro aplikace

Zdroj: zpracováno dle [1]

Tabulka 2 – Technické normalizační informace

Označení	Popis
TNI 334590-1	Návrh EZS
TNI 334590-2	Montáž EZS
TNI 334590-3	Kontrola a údržba EZS

Zdroj: zpracováno dle [1]

3.1.1.1 Bezpečnost

Jedním z velmi důležitých kritérií, které jsou definovány normou ČSN EN 50131-1 jsou tzv. stupně bezpečnosti. Ty následně stanovují doporučené požadavky na systém z hlediska úrovně přístupu, vyhodnocení, provozování, detekce, napájení, ochrany proti sabotáži, monitorování, propojení a záznamu. [1]

Tabulka 3 – Stupně zabezpečení dle ČSN EN 50131-1

Stupeň	Riziko	Typ narušitele
1	nízké	malé znalosti EZS, velmi malá výbava nástrojů
2	nízké / střední	určité znalosti EZS, omezená výbava nástrojů
3	střední / vysoké	disponuje znalostmi ohledně EZS a základními přístroji a elektronickými zařízeními
4	vysoké	detailní znalost daného EZS, kompletní výbava včetně prvků pro náhradu rozhodujících prvků EZS

Zdroj: zpracováno dle [1]

3.1.1.2 Prostředí

Podobně jako stupně bezpečnosti, definuje norma ČSN EN 50131-1 také čtyři třídy prostředí. Ty určují, do jakého prostředí lze detektory umisťovat s ohledem na odolnost a konstrukci. [2]

Tabulka 4 – Třídy prostředí dle ČSN EN 50131-1

Třída	Prostředí	Popis	Rozsah teplot
I	vnitřní	vytápěné obytné nebo obchodní místa	MIN +5 °C MAX +40 °C
II	vnitřní všeobecné	vytápěné přerušovaně, nevytápěné	MIN -10 °C MAX +40 °C
III	venkovní chráněné	bez trvalého vystavení vlivům počasí	MIN -25 °C MAX +50 °C
IV	venkovní všeobecné	trvalé vystavení vlivům počasí	MIN -25 °C MAX +60 °C

Zdroj: zpracováno dle [2]

Pro kamerové a dohledové systémy jsou tyto parametry jako stupeň zabezpečení a třída prostředí definovány normou ČSN EN 62676-1-1. [4]

S prostředím je také úzce spjatá odolnost zařízení proti vniknutí cizích pevných předmětů a vody do krytu zařízení označována jako stupeň krytí IP. Jednotlivé stupně jsou definovány normou ČSN EN 60529 z roku 1991. Samotné označení obsahuje písmena IP a následně dvě číslice za kterými se mohou objevit ještě přídavná či doplňková písmena. První číslo udává stupeň ochrany před vniknutím cizích pevných předmětů a druhé stupeň ochrany před vniknutím vody do krytu zařízení. [3]

Stupně ochrany před vniknutím cizích pevných předmětů:

- **IP 0x** – žádná ochrana;
- **IP 1x** – ochrana před předměty větší než 50 mm;
- **IP 2x** – ochrana před předměty větší než 12,5 mm;
- **IP 3x** – ochrana před předměty větší než 2,5 mm;
- **IP 4x** – ochrana před předměty větší než 1 mm;
- **IP 5x** – ochrana před prachem (vniknutý prach nenaruší funkčnost);
- **IP 6x** – prachotěsné. [3]

Stupně ochrany před vniknutím vody:

- **IP x0** – nechráněno;
- **IP x1** – ochrana před svisle kapající vodou;
- **IP x2** – ochrana před kapající vodou ve sklonu 15°;
- **IP x3** – ochrana před kropením a deštěm do sklonu 60°;
- **IP x4** – ochrana před stříkající vodou;
- **IP x5** – ochrana před tryskající vodou;
- **IP x6** – ochrana před intenzivně tryskající vodou;
- **IP x7** – ochrana při ponoření zařízení až do 1 m po dobu 30 min;
- **IP x8** – ochrana při trvalém ponoření. [3]

Přídavná nepovinná písmena značící ochranu před dotykem nebezpečných částí:

- **A** – ochrana před dotykem hřbetem ruky;
- **B** – ochrana před dotykem prstem;
- **C** – ochrana před dotykem nástrojem;
- **D** – ochrana před dotykem drátem. [3]

Doplňková písmena:

- **H** – označení pro zařízení vysokého napětí;
- **M** – označení pro pohyb během zkoušky s vodou;
- **S** – označení pro klidový stav během zkoušky s vodou;
- **W** – označení pro použití za stanovených povětrnostních podmínek. [3]

3.2 Elektronické zabezpečovací systémy

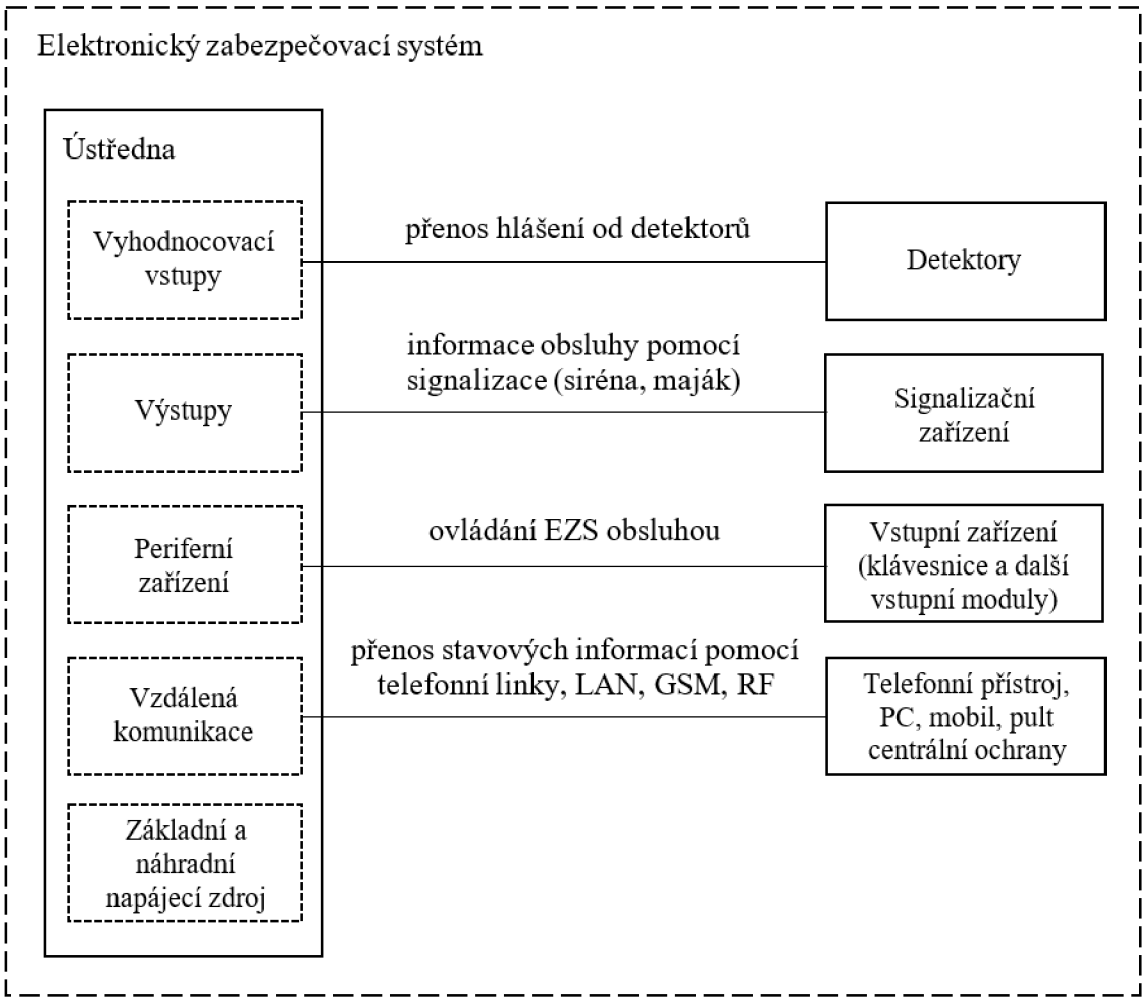
Elektronický zabezpečovací systém (EZS) označován také jako poplachový zabezpečovací a tísňový systém (PZTS) či jen poplachový zabezpečovací systém (PZS) je elektronický systém, který slouží k detekování a signalizaci nežádoucích stavů a událostí v dané oblasti. Touto událostí či stavem může být například vniknutí neoprávněné osoby do objektu, pokus o únik ze střežené oblasti či nedovolená manipulace se sledovaným předmětem. Dalším příkladem pak může být detekce požáru, uniku vody či nebezpečných látek. [4]

Pravděpodobně první jednoduchý bezpečností systém proti vniknutí neoprávněné osoby do objektu byl použit již v polovině 19. století. Princip spočíval v sepnutí kontaktu u dveří nebo oken a následným rozezněním bzučáku. S příchodem procesorů a dalších typů senzorů se začali objevovat nové typy detektorů a dalších prvků což vedlo k vyšší úrovni zabezpečení a spolehlivosti díky čemu došlo k rozšíření těchto systémů. [4]

3.2.1 Architektura

Základem elektronického zabezpečovacího systému je ústředna, která je pomocí různých rozhraních propojena s detektory, signalizačními zařízeními, vstupními zařízeními a dalšími moduly. Informace a stavy získané z jednotlivých prvků vyhodnocuje a na základě toho provádí danou operaci jako například spuštění poplachu. Komunikace mezi prvky může být zajištěna kabelově, bezdrátově nebo kombinovaně tzn., že jeden prvek je připojen pomocí kabelu a druhý bezdrátovým způsobem. Následně můžou být tyto informace pomocí modulu vzdálené komunikace odesílány na pult centrální ochrany (PCO), což jsou místa se stálou službou, ze kterých se realizují bezpečnostní zásahy. Další možností je přenos informací na mobilní telefon. [5]

Obrázek 1 – Schéma elektronického zabezpečovacího systému



Zdroj: vlastní zpracování dle[4][5]

3.2.2 Základní prvky a rozdělení

Mezi základní prvky, které tvoří tzv. zabezpečovací řetězec elektronického zabezpečovacího systému patří zejména:

- **Detektory (čidla)** – zařízení, které reagují na změny fyzikálních vlastností ve střeženém prostředí a při zjištění stavu narušení odesílají poplachový signál.
- **Ústředna** – přijímá a vyhodnocuje informace od detektorů, umožňuje ovládat systém a stará se o jeho napájení.
- **Přenosové technologie** – umožňují přenos signálu a zpráv mezi jednotlivými prvky sytému.
- **Signalizační zařízení** – převádí přijaté informace z ústředny na vhodný optický či akustický signál (poplach či siréna).

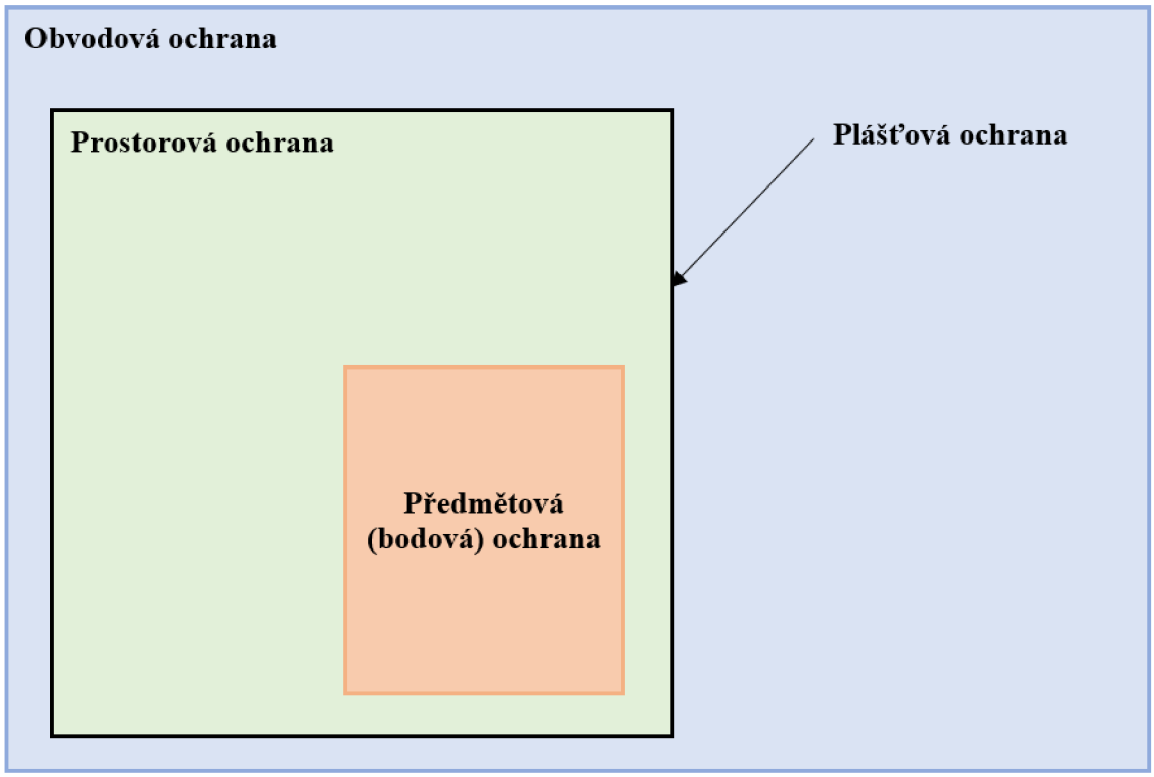
- **Vstupní zařízení** – umožňují ovládat systém či vykonávat některé speciální funkce.
- **Napájecí zdroj** – je nezbytnou součástí pro správný chod bezpečnostního systému. Jedná se především o základní a následně náhradní napájecí zdroj v případě výpadku.

Z hlediska prostoru je pak možné rozdělit zaměření ochrany elektronického zabezpečovacího systému na pět druhů jejíž kombinací lze vytvořit tzv. systém s vícestupňovou ochranou. [6]

Rozdělení prostorového zaměření ochrany:

- obvodové;
- plášťové;
- prostorové;
- předmětové (bodové);
- klíčové. [6]

Obrázek 2 – Znázornění prostorového zaměření ochrany



Zdroj: vlastní zpracování

3.2.2.1 Obvodová ochrana

Obvodová ochrana je zaměřena na signalizaci narušení obvodu střeženého objektu dříve, než se narušitel dostane k objektu blíže. Tímto obvodem bývají většinou katastrální hranice, které jsou vymezeny například vodními toky, ploty či zdmi. Ve většině případů se jedná o venkovní prvky ochrany, které jsou speciálně uzpůsobené pro tento typ účelu. [1][6]

Příklady používaných bezpečnostních prvků:

- infračervené závory;
- mikrovlnné bariéry;
- tlakové hadice;
- štěrbinové kabely. [1]

3.2.2.2 Plášťová ochrana

Plášťová ochrana má za cíl detekovat narušení pláště, tedy nějaké mechanické překážky (např. vstupní dveře) střeženého objektu. [6]

Příklady používaných bezpečnostních prvků:

- magnetické kontakty;
- prvky pro ochranu skleněných ploch;
- vibrační detektory. [1]

3.2.2.3 Prostorová ochrana

Prostorová ochrana, někdy označována jako objemová, je navržena tak aby detekovala narušení vnitřního prostoru chráněného objektu. Používané detektory odhalí pohyb narušitele až v prostoru nikoliv před vstupem do něj. [6]

Příklady používaných bezpečnostních prvků:

- pasivní a aktivní infračervené detektory;
- ultrazvukové detektory;
- mikrovlnné detektory;
- kombinované detektory. [1]

3.2.2.4 Předmětová (bodová) ochrana

Označení předmětová neboli bodová ochrana se používá pro detekci narušitele v bezprostřední blízkosti u střeženého předmětu a následnou manipulaci s tímto předmětem. V praxi s tímto typem nejčastěji setkáváme při ochraně trezorů nebo sběratelských předmětů. [6]

3.2.2.5 Klíčová ochrana

Klíčová ochrana se využívá v souvislosti s detekcí narušitele v klíčových prostorech střeženého objektu jako jsou například chodby či schodiště. Využívají se stejné prvky jako u plášťové a prostorové ochrany. [6]

3.2.3 Vzdálená komunikace

Aby mohl elektronický zabezpečovací systém efektivně fungovat je nutné nejen využívat lokální signalizaci poplachu ale také přenášet tyto informace o narušení střeženého objektu na PCO případně na mobilní telefon oprávněné osoby. Pro vzdálený přenos těchto informací se používají různé přenosové technologie jako je jednotná telefonní síť (JTS), GSM, LAN sítě a další. [6]

3.2.3.1 Jednotná telefonní síť (JTS)

Jednotná telefonní síť využívá modul, který se nazývá telefonní komunikátor, který je součástí základní desky ústředny. Princip přenosu spočívá ve vytočení telefonního čísla provázaného s PCO a po předání informací a potvrzení přijetí se přenos ukončí. Při obsazené lince musí být komunikátor schopný toto spojení přerušit, aby mohlo být navázáno nové spojení s PCO. Pro přenos se využívá několik přenosových formátů. Nevýhodou tohoto přenosu je, že mohou být účtovány poplatky za přenos a dále velký interval pro testování spojení, který bývá většinou jednou za 12 či 24 hodin. [6][7]

3.2.3.2 GSM

Podobně jako telefonní komunikátor u jednotné telefonní sítě funguje také GSM modul. Ten bývá také přímo integrován do základní desky ústředny či připojen pomocí sběrnice. K přenosu informací se využívá mobilní síť GSM (Global System Mobile Comunication). Tento způsob poskytuje rychlý přenos ve vysokém stupni zabezpečení,

avšak bez odpovídající spolehlivosti. To je způsobeno tím, že provozovatel negarantuje dokonalou propustnost sítě. K přenosu informací se využívají krátké textové zprávy (SMS), které ale při přetížení sítě mohou mít enormní zpoždění až desítky hodin. [6][8]

O něco lépe je na tom služba GPRS (General Packet Radio Service), která díky datovému přenosu umožňuje trvalou kontrolu přenosu a obousměrný přenos. Moduly podporující tento typ přenosu při odeslání informace vyžadují potvrzení druhé strany. Pokud potvrzení nezískají tak se přenos několikrát zopakuje a případně se pomocí záložního spojení informuje PCO o neúspěchu komunikace. [8][9]

3.2.3.3 LAN

Jednou z nejpoužívanějších přenosových technologií pro přenos informací k PCO je využití moderního internetu s pomocí LAN komunikačního modulu. Instalace tohoto modulu je velmi snadná a připojuje se na lokální internetovou síť v objektu, což ovšem může způsobovat komplikace, pokud je připojení nestabilní. Komunikace je podobně jako GPRS obousměrná s využitím protokolů TCP a UDP. Hlavní nevýhodou je, že jednotlivé aktivní prvky v síti (switch, router a podobně) nemají v případě výpadku elektrické energie záložní zdroj napájení. Proto je nutné využívat záložní komunikaci. [7][8]

3.2.3.4 Rádiový přenos

Bezdrátový rádiový přenos je další přenosovou technologií, která se využívá pro přenos informací na PCO. Přenos je jednosměrný, velmi spolehlivý a probíhá skrze speciální jednoúčelové rádiové sítě s vyhrazeným frekvenčním pásmem. Výhodou je, že bezpečnostní agentury provozující PCO mají často tyto sítě ve vlastní správě a mají tak přehled o provozu a propustnosti sítě. Nevýhodou je, že rádiový přenos lze poměrně snad rušit. [6]

3.2.4 Pult centrální ochrany (PCO)

Pulty centrální ochrany, někdy nazývané jako dohledová centra jsou specializované pracoviště, pracující 24 hodin denně 7 dní v týdnu, na které jsou zasílány informace z ústředen jednotlivých střežených objektů. Ty jsou následně pracovníky vyhodnoceny a v případě narušení je základě smlouvy o střežení aktivován bezpečnostní protokol což může znamenat například vyslání výjezdové skupiny, která objekt zkontroluje. Kromě

vyhodnocení přijatých hlášení se také monitoruje, zda nedošlo k výpadku sítě či přenosové trasy pomocí automatických testů. [11]

Obrázek 3 – Dohledové centrum společnosti M2C

Zdroj: [12]

3.3 Ústředny

Hlavním prvkem elektronického zabezpečovacího systému je ústředna jejíž základní funkcí je sběr informací od jednotlivých detektorů a následně tyto informace vyhodnotit a případně vyhlásit poplach. [6]

Obrázek 4 – Ústředna elektronického zabezpečovacího systému

Zdroj: [10]

Běžně se můžeme setkat s různými typy ústředen, které se liší jak vnitřní elektronikou, programovým vybavením, způsobem oznámení, typem ovládání, připojením vstupních a výstupních prvků a podobně. [6] I přesto, že existuje celá řada různých ústředen platí pro všechny tyto základní charakteristiky:

- příjem a vyhodnocení signálu a informací od detektorů;
- signalizace a přenos informací o vnitřním stavu například na PCO;

- ovládání poplachových, signalizačních a dalších prvků pro indikaci narušení střeženého objektu;
- napájení připojených prvků;
- ovládání celého systému pomocí ovládacích prvků a následné uvedení do stavu střežení nebo klidu;
- diagnostika systému. [6]

Jednotlivé typy ústředen pak dále můžeme dělit do skupin podle stupně vybavenosti, počtu smyček nebo způsobu připojení těchto smyček.

3.3.1 Stupeň vybavenosti

Stupeň vybavenosti ústředny si můžeme představit nejen jako prvky pro komfortní obsluhu ale především jako odolnost oproti možnému překonání zabezpečovacího systému a tím také vyřazení jeho částí či systému jako celku. Tento stupeň vychází z rizika střeženého objektu a s tím spojeným stupněm zabezpečení. Rozlišujeme následující stupně vybavenosti:

- nízký – stupeň zabezpečení 1;
- nízký až střední – stupeň zabezpečení 2;
- střední až vysoký – stupeň zabezpečení 3;
- vysoký – stupeň zabezpečení 4. [6]

Pro ústřednu se 4. stupněm zabezpečení (vysokým) musí být realizovány dvě samostatné ústředny s vlastním záložním zdrojem, a to jedna minimálně pro 3. stupeň a druhá minimálně pro 2. stupeň zabezpečení. [6]

3.3.2 Způsob připojení

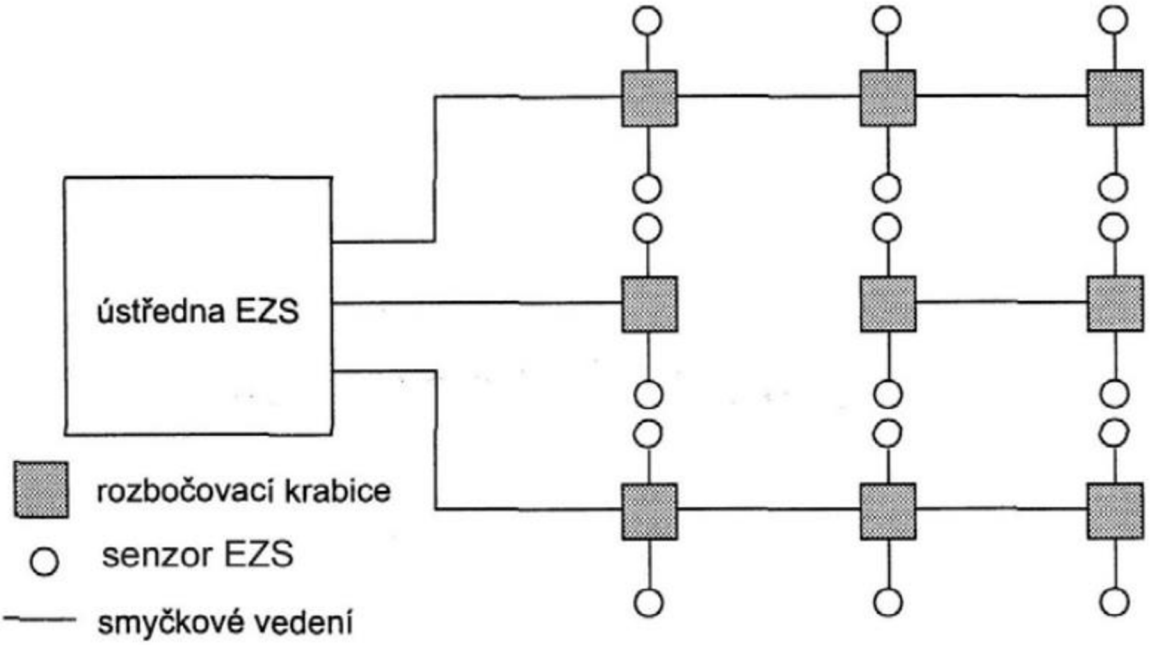
Dalším způsobem, jak lze ústředny rozdělit, bez ohledu na stupeň zabezpečení je dle způsobu připojení zabezpečovacích smyček. Ústředny dělíme na:

- smyčkové (analogové);
- s přímou adresací čidel (sběrnicové);
- smíšené;
- využívající bezdrátovou komunikaci čidel;
- hybridní. [6]

3.3.3 Smyčkové (analogové)

Smyčková neboli analogová ústředna disponuje vstupními vyhodnocovacími obvody pro každou smyčku a komunikace probíhá pouze ve směru od detektorů. Každá smyčka je pak zakončena odporem s předepsanou hodnotou pro daný typ ústředny. Stavy jednotlivých detektorů se signalizují zařazením odporu do smyčky a tím změnou celkového odporu dané smyčky. Tento odpor ústředna neustále měří a na základě hodnot jednotlivých odporů smyček vyhodnocuje vyhlášení poplachu. [1][4]

Obrázek 5 – Schéma zapojení smyčkové ústředny



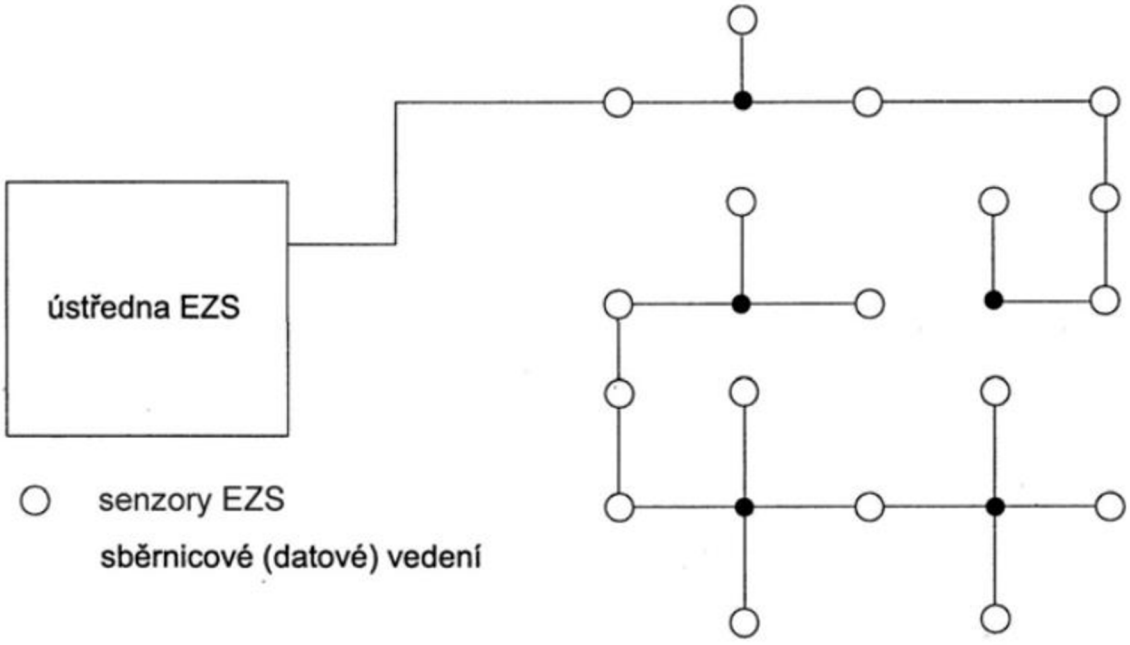
Zdroj: [1]

Komunikace ústředny se signalizačními prvky probíhá taktéž pouze v jednom směru, ale tentokrát od ústředny směrem k danému signalizačními prvku. Oproti tomu komunikace s ovládacími prvky (například klávesnice) je oboustranná a realizována pomocí sběrnice. O napájení jednotlivých prvků se stará ústředna skrze vodiče, které jsou umístněné v kabelu vedoucímu ke každému detektoru. Nevýhodou tohoto řešení je právě velké množství kabeláže potřebné na propojení všech detektorů. [4]

3.3.4 S přímou adresací čidel (sběrnicové)

Dalším typem jsou ústředny s přímou adresací čidel někdy označované jako sběrnicové. Sběrnicové se označují, jelikož tento typ ústředny využívá pro komunikaci mezi jednotlivými detektory právě datovou sběrnici. [1]

Obrázek 6 – Schéma zapojení ústředny s přímou adresací čidel



Zdroj: [1]

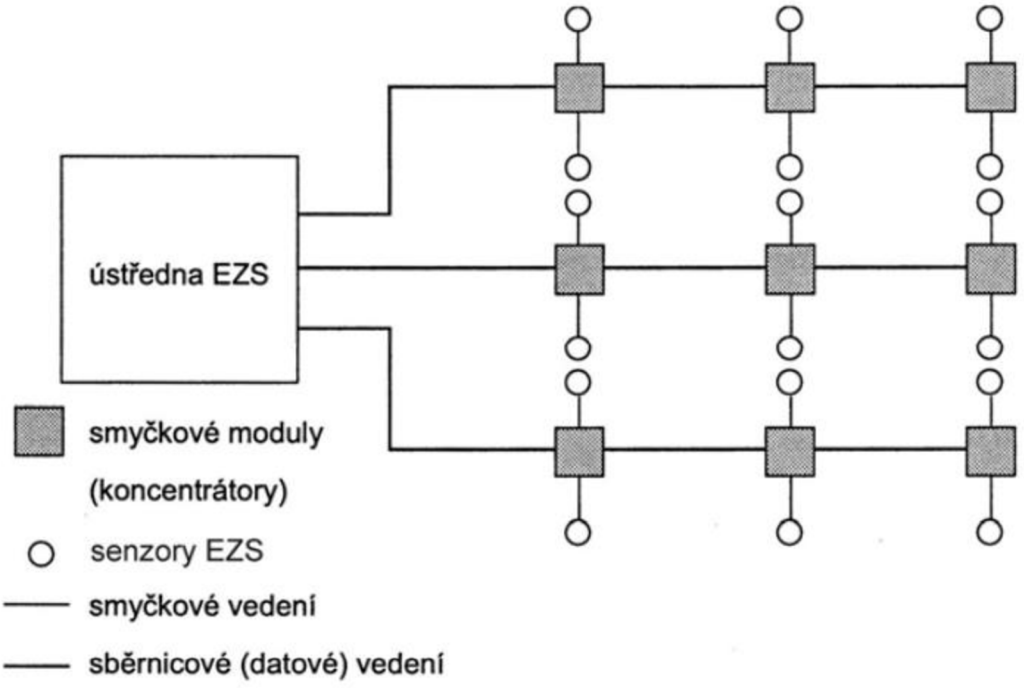
Principem je periodická výměna datových rámců mezi ústřednou a jednotlivými detektory. Samotné datové rámce si můžeme představit jako tři skupiny bitů. První skupina bitů reprezentuje unikátní adresu každého detektoru. Následuje skupina bitů, které definují příkaz ústředny či hlášení od daného zařízení. Tyto příkazy závisí na typu zařízení, kterému jsou posílány. U detektorů jsou to zpravidla požadavky na hlášení stavu. Poslední skupinou jsou bity, které slouží ke kontrole úspěšnosti přenosu celého datového rámce. [4]

Výhodou tohoto řešení je, že při vniku do střeženého objektu dokáže ústředna oznámit konkrétní detektor, který byl aktivovaný včetně typu narušení jako je poplach, sabotáž, zkrat a podobně. Další výhodou je pak jednoduchost kabelové sítě. To ovšem přináší také omezení v podobě nemožnosti realizace dodatkových funkcí detektorů jako například paměť poplachů. Další nevýhodou je nutnost využívat pouze určitý druh detektorů, které jsou schopné s tímto typem ústředny komunikovat. [6]

3.3.5 Smíšené (koncentrátorové)

Smíšené ústředny jsou kombinací smyčkových a sběrnicových typů. Často také bývají označovány jako koncentrátorové a to z toho důvodu, že využívají smyčkové moduly, které se označují jako koncentrátory. Komunikace je zde zajištěna přes datovou sběrnici a smyčkové vedení. Samotné detektory jsou na jednotlivé koncentrátory připojeny přes smyčky jako u analogové ústředny a koncentrátory pak přes datovou sběrnici jako u sběrnicové ústředny. [1][6]

Obrázek 7 – Schéma zapojení smíšené ústředny



Zdroj: [1]

Vyhodnocení stavů detektorů může probíhat přes analogový multiplex, kdy jsou na sběrnici připojeny jednotlivé smyčky a vyhodnocuje se impedance smyčky nebo případně

pomocí vyhodnocovací logiky a vyrovnávací paměti, která je integrována přímo do jednotlivých koncentrátorů a komunikace probíhá pouze datově. [1][6]

3.3.6 Využívající bezdrátovou komunikaci čidel

Ústředny využívající bezdrátové sítě pro komunikaci s detektory se stávají stále více populárními, a to především z důvodu minimálního vedení kabeláže. Pro přenos informací se využívá pásmo 433 MHz nebo 868 MHz. Přenášené rámce jsou velmi podobné těm, které se využívají u sběrnicových ústředen včetně struktury komunikace ve tvaru příkazu od ústředny či hlášení od detektoru. Jelikož se nevyužívá kabelové propojení je nutné dbát na maximální vzdálenost čidel od ústředny, tak aby byla zajištěna spolehlivá komunikace. Napájení jednotlivých čidel je pomocí lithiových baterií či 9 V článků a samotné detektory disponují akustickou signalizací nebo předávají informace o poklesu napětí baterie ústředně, aby mohla být zajištěna včasná výměna a neohrožen chod systému. [1][6]

3.3.6.1 Jednosměrná komunikace (simplex)

Jednodušší systémy využívají tzv. jednosměrnou komunikaci. Jednosměrné se označují z toho důvodu, že detektor je v roli vysílače a ústředna naopak v roli přijímače. Problém starších systému založených na tomto principu byl v chybějící kontrole funkčnosti detektorů mimo již zmíněnou indikaci poklesu napětí. Modernější systémy již kontrolují stavy jednotlivých detektorů, ale jelikož by vysoká četnost kontrol měla negativní dopad na životnost baterií, využívají se tyto kontroly s frekvencí několika hodin. To v praxi znamená, že případnou poruchu detektoru lze zjistit často s velkou odezvou. Další nevýhodou těchto systémů je, že mohou vznikat plané poplachy z důvodu přerušení signálu. Aby došlo ke správnému vyhodnocení poplachu, vyhodnocuje se stav jako poplachový až ve chvíli, kdy nedorazí alespoň dvě kontrolní relace. Nebezpečí také spočívá v poměrné velkém riziku možného rušení, jelikož lze snadno zjistit kmitočet a druh modulace. [1][6]

3.3.6.2 Obousměrná komunikace (duplex)

Novější systémy již pracují duplexně to znamená, že každý prvek může zastávat roli vysílače i přijímače. Spojení je trvale monitorováno což značně zvyšuje spolehlivost daného systému. K dispozici je přibližně 100 adres a je možné tento systém dále dělit na nezávislé podsystémy. Výhodou těchto systémů je také, že v případě rušení kanálů jsou schopny

automaticky vyhledat jiné kanály a na ty se přeladit. Samotný přenos mezi jednotlivými zařízeními uvnitř systému je digitální a zabezpečen proti odposlechu. [1][6]

3.3.7 Hybridní

Hybridní ústředny umožňují kombinovat jednotlivé zabezpečovací prvky bez ohledu na druh připojení (kabelové, bezdrátové). Oproti klasickým drátovým ústřednám jsou vybaveny speciálním komunikátorem, který zajišťuje přenos informací mezi bezdrátovými prvky a ústřednou. Tento typ ústředen nachází využití v objektech, ve kterých nelze ve všech místnostech využít kabelové rozvody. Výhodou je také, že v budoucnu je možné systém jednoduše rozšířit o další bezdrátové prvky. [6]

3.4 Ovládací zařízení

Nedílnou součástí elektronického zabezpečovacího systému je jeho ovládání, tak aby mohl být uváděn do stavu střežení či klidu. Většinou se můžeme setkat s kódovými klávesnicemi, které jsou umístěny ve vnitřním prostoru střeženého objektu v blízkosti vstupu. Při vstupu do objektu je při zapnutém střežení nutné zadat kód, po kterém se systém uvede do stavu klidu. Každý uživatel může mít přidělený vlastní kód. V závislosti na nastavení systému je po špatném zadaní tohoto kódu vyhlášen poplach. Tyto zařízení jsou zaměřeny především na snadnou obsluhu EZS. [1]

Obrázek 8 – Ovládací klávesnice s displejem Jablotron JA-150E

Zdroj: [13]

3.5 Detektory

Detektory jsou nejdůležitějšími prvky zabezpečovacího systému. Jedná se o elektrická zařízení, která detekují incidenty, které jsou způsobeny narušením střeženého objektu či prostoru. Princip detekce je založen na skutečnosti, že každý incident (například přelezení plotu) má svůj určitý fyzikální děj (otřesy plotu). Pokud detektor zaznamená výskyt tohoto určitého příznaku tak je vyhlášen poplach. Detektory rozlišujeme dle chování na aktivní a pasivní, ty se dále dělí dle typu střeženého prostoru a typu použité technologie. [4]

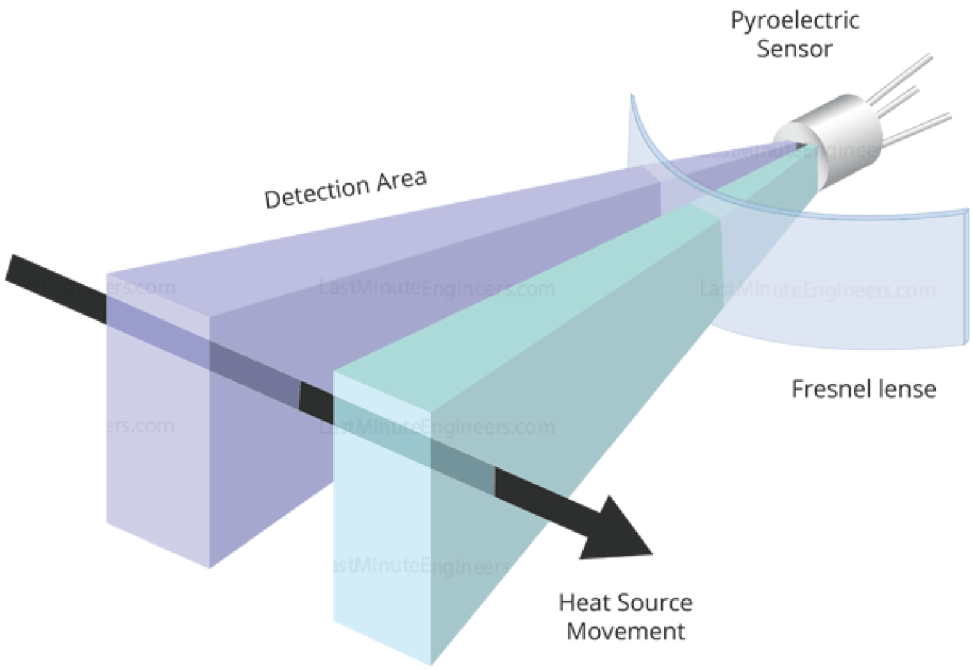
3.5.1 Pasivní infračervené detektory (PIR)

Pasivní infračervené detektory fungují na principu detekce tepelného záření osob. Infračervené detektory se nazývají z toho důvodu, že nejintenzivnější tepelná složka lidského těla je vyzařována na vlnové délce okolo 10 μm, což spadá do infračerveného pásma záření. [4]

Základním prvkem těchto detektorů je tzv. PIR snímač. Jedná se o elektronickou součástku podobnou fototranzistoru, která je vyrobena materiálu na bázi lithia a tantalu. Oproti fototranzistoru má však PIR snímač posunutou citlivost směrem do oblasti infračerveného záření. To však neznamená, že je citlivý pouze infračervené záření. Typickým zdrojem rušivého záření je sluneční světlo, které také obsahuje tyto vlnové délky. Jednoduché PIR snímače detekují objekty, které se pohybují v jeho zorném poli nebo nepohyblivé zdroje záření, které jsou schopny rychle změnit svoji teplotu. Kvalitnější PIR detektory sčítají signály ze dvou PIR snímačů zapojených sériově a s opačnou polaritou a využívají tak dvě detekční zóny. [6]

Před PIR snímače jsou umístěny soustavy čoček, které napomáhají přizpůsobit zaměření samotného detektoru tak aby detekční zóny co nejvíce pokrývaly dané oblasti použití (dlouhé chodby, záclonové čočky apod.). Tyto čočky jsou vyrobeny z teflonu a nazývají se Fresnelovy čočky. Díky svému specifickému tvaru disponují malým útlumem záření. [4]

Obrázek 9 – Princip funkčnosti PIR detektoru



Zdroj: [14][1]

Při nečinnosti detekují obě zóny (na obrázku znázorněné fialově a zeleně) stejné množství infračerveného záření což generuje nulový vstupní signál. Pokud však skrze tyto zóny projde těleso s jinou teplotou, než je teplota okolí, čidlo tyto změny zachytí a dojde k vyhlášení poplachu. [14]

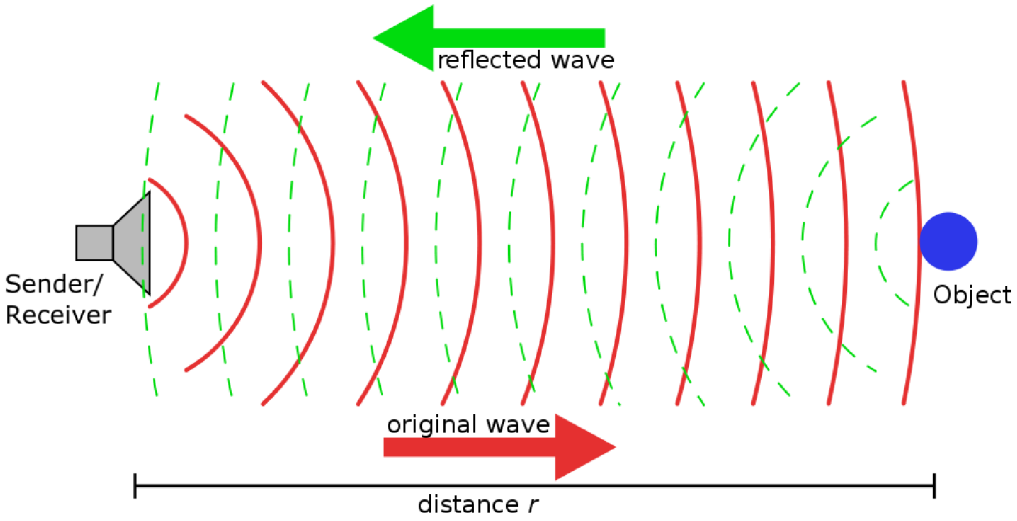
Výhodou těchto senzorů je malá spotřeba energie, snadná montáž, spolehlivost a odolnost proti planým poplachům. Další výhodou je možnost instalace více PIR detektorů do jednoho střeženého prostoru tak aby byla jeho plocha co nejvíce pokryta. Jelikož PIR detektory nevyzařují žádnou energii nedochází tak k jejich vzájemnému rušení. [6] Oproti tomu u jednodušších PIR detektorů je nevýhodou relativně jednoduchá sabotáž zacloněním. Kvalitnější detektory jsou na tento typ sabotáže připraveny a jsou vybaveny zabudovanou detekcí zaclonění označovanou jako antimasking. [4]

3.5.2 Mikrovlnné detektory (MW)

Mikrovlnné detektory spadají do třídy takzvaných reflexních detektorů. Principem činnosti je praktické využití Dopplerova jevu. Ten je aplikován na mikrovlnném pásmu, které se pohybuje v rozmezí 300 MHz až 300 GHz. Dopplerův jev je jev při kterém

se frekvence a vlnová délka vlnění generovaného vysílačem liší od té přijaté přijímačem z důvodu vzájemné nenulové rychlosti. V praxi to znamená, že pokud detektor vyzařuje do střeženého prostoru rádiový signál o určité frekvenci a v prostoru nejsou žádná pohyblivá tělesa, vysílaná a přijatá frekvence si budou rovny a rozdílová frekvence bude rovna nule. Pokud se však ve střeženém prostoru objeví pohybující se těleso, bude přijatá frekvence odlišná od odeslané a což znamená, že rozdílová frekvence bude nenulová. Nenulová hodnota rozdílové frekvence je vyhodnocena jako narušení a je vyhlášen poplach. [4][15]

Obrázek 10 – Princip činnosti mikrovlnného detektoru



Zdroj: [16]

Pro správnou funkci mikrovlnných detektoru je nutné si při instalaci dát pozor na několik aspektů. V první řadě by tyto detektory neměli být instalovány poblíž velkých kovových předmětů. Dalším předpokladem je instalace v prostorách bez využívání zářivkového osvětlení. Podobně jako u PIR detektorů je možné použit více mikrovlnných detektorů v jednom střeženém prostoru, avšak za předpokladu, že pracují každý na jiné frekvenci či jsou od sebe umístněné tak, aby nebylo možné jejich vzájemné rušení. [4]

3.5.3 Ultrazvukové detektory (US)

Ultrazvukové nebo ultrasonické detektory (US) pracují na podobném principu jako mikrovlnné detektory, tedy na principu Dopplerova jevu. Oproti mikrovlnným detektorům ovšem využívají ultrazvukového pole v pásmu 20–45 kHz. Hlavním prvkem těchto detektorů je akustický zářič neboli vysílač, který si lze představit jako obdobu reproduktoru. Pomocí tohoto vysílače je do střeženého prostoru vysíláno vlnění se stálým kmitočtem,

které mohou slyšet například psi. V prostoru se vytvoří tzv. stojaté vlnění, které značí klidový stav ve střeženém prostoru. Bude-li se v prostoru pohybovat nějaké těleso, dojde ke změně fáze přijímaného vlnění což vede k vyhlášení poplachu. [6]

Stejně jako u mikrovlnných detektorů existuje řada instalačních předpokladů pro zajištění správné funkčnosti detektoru. Jedním z těchto předpokladů je, že detektor by měl být instalován tak, aby pohyb případného narušitele směřoval směrem k detektoru případně směrem od něj. Dosah těchto detektorů bývá maximálně 10 m, jelikož dochází k velkému útlumu ultrazvuku ve vzduchu. V prostoru je také možné instalovat více ultrazvukových detektorů ale jen pokud jsou vysílače synchronizovány, aby nedocházelo k vzájemnému rušení. Oproti tomu by se tyto detektory neměli instalovat v prostorech s volně zavěšenými předměty, pohybujícími zvířaty či nad topná tělesa. [6]

3.5.4 Kombinované detektory

Kombinované detektory bývají často označovány jako duální, a to z důvodu, že kombinují funkci dvou detektorů v jednom. Výhodou těchto detektorů je velmi malá pravděpodobnost, že některý z fyzikálních jevů, by vyvolal planý poplach u obou senzorů zároveň. Uhlář toto demonstruje na příkladu, kdy uvažujeme, že planý poplach u samostatných detektorů vzniká jednou za 100 h, což nám dává hodinovou pravděpodobnost planého poplachu 0,01. U kombinovaného čidla je tato pravděpodobnost pouze 0,0001 (přibližně jednou za 417 dnů). [4][6]

Tabulka 5 – Citlivost detektorů na zdroje planého poplachu

Zdroj planého poplachu	**Typ detektoru**		
	pasivní infračervený	**mikrovlnný**	**ultrazvukový**
Proudění teplého vzduchu	X		X
Vibrace a otřesy		X	X
Světelné zdroje	X		

Zdroj: zpracováno dle [6]

Pro vyhodnocení, zda se jedná o planý či skutečný poplach se využívá součinová logika. To znamená, že je nutné, aby poplach byl vyhlášen oběma senzory a až poté je informována ústředna. U bezdrátových detektorů kombinující princip PIR-MW se také často můžeme setkat s tím, že mikrovlnný detektor je po celou dobu vypnutý a zapíná se pouze pokud PIR zaznamená poplach. To je z toho důvodu, že MW, neustále vysílá do okolí, což značně zvyšuje spotřebu akumulátoru. [4]

Nejčastěji se můžeme setkat s kombinovanými detektory sdružující technologie pasivních infračervených a mikrovlnných detektorů. Druhou častou variantou je kombinace pasivních infračervených a ultrazvukových detektorů. [6]

3.5.5 Magnetické kontakty

Magnetické kontakty patří mezi nejpoužívanější kontaktní detektory. Díky velké oblibě se vyrábějí v několika variantách v závislosti na konstrukci, funkci či úrovni odolnosti. Lze je na základě těchto vlastností rozdělit do následujících skupin:

- s jedním či více jazýčkovými kontakty;
- s ochranným odporem;
- s funkcí spínání či rozpínání;
- s nebo bez ochranné smyčky;
- s předmagnetizací (označováno jako BIASED). [6]

Tento typ detektorů je určen pro střežení otvírání dveří a oken proto bývají označovány také jako vstupní nebo okenní detektory a je tvořen dvěma hlavními částmi. Jednou z nich je jazýčkový spínač. Ten se skládá ze dvou feromagnetických kontaktů (jazýčků) umístěných uvnitř malé skleněné kapsle. Jednotlivé kontakty jsou od sebe nepatrně vzdáleny což znamená, že elektřina nemůže spínačem proudit. Druhou částí je magnet. Pokud se jazýčky dostanou do kontaktu s magnetickým polem, přitáhnou se k sobě, čímž se obvod uzavře a umožní se proudění elektřiny. Při opuštění magnetického pole se od sebe opět odtáhnou a obvod se otevře. [18]

Montáž dveřních či okenních detektorů spočívá v umístění jazýčkového spínače na rám dveří a magnetu na samotné dveře případně naopak. Je nutné dbát na správné výškové vyrovnání tak aby byli jednotlivé částí umístěni přesně proti sobě. Při otevření dveří je pak

do ústředny vyslán signál a na základě nastavení je provedena požadovaná operace například v podobě zvukového signálu či odeslání SMS s upozorněním. [18]

Obrázek 11 – Ukázka instalace magnetického kontaktu na okně

Zdroj: [19]

Výhodou těchto detektorů je velká spolehlivost a odolnost proti planým poplachům. Dále pak jednoduchá montáž a relativně přijatelná cena. Nevýhodou je, že pro odpovídající zabezpečení je často nutné tyto detektory instalovat na každé okno a dveře. [18]

3.5.6 Detektory rozbití skla

Někdy si nevystačíme pouze s magnetickými kontakty na dveřích a oknech. Pokud by totiž narušitel okno rozbil, magnetické kontakty logicky žádné narušení nezaznamenají. Zde nacházejí uplatnění právě detektory rozbití skla nebo také označované jako detektory pro ochranu skleněných ploch, které monitorují zvuky a vibrace způsobené rozbitím skla. Výhodou těchto detektorů je, že je možné je mít neustále aktivované i pokud se v prostoru pohybují lidé. Tyto detektory je vhodné používat v prostorech, které disponují velkými okny či prosklenými plochami. Samotné zařízení se umisťuje buď přímo na okna nebo vedle nich z důvodu malého dosahu. [17]

Můžeme se setkat s dvěma typy detekce. Jedním z nich je monitorování vibrací, které způsobuje rozbité sklo, pomocí vibračních senzorů. Nevýhodou tohoto typu je, že mohou být náchylné na plané poplachy v případě větších otřesů způsobené například bouchnutím dveří. Druhý typ funguje na principu rozeznání akustické frekvence při tříštění skla. Zde existuje riziko planého poplachu v případě rozbití skleněného nádobí či jiných skleněných předmětů. Pro eliminaci planých poplachů je proto vhodné nastavit odpovídající úroveň citlivosti. [17]

3.5.7 Destrukční detektory

Pod označení destrukční detektory řadíme speciální typy detektorů, které fungují na principu rozbití překážky, na které jsou aplikovány. Patří do skupiny plášťové ochrany a hlavní odlišnost od ostatních detektorů je, že pokud dojde k vyvolání poplachu, znamená to, že detekční prvek byl zničen a bude muset být vyměněn nebo opraven. Mezi tyto detektor se řadí:

- Poplachové fólie, tapety a skla
- Fóliové polepy
- Vodičové sítě a zátarasy
- Světlovodné sítě [1]

3.5.7.1 Poplachové fólie, tapety, skla a polepy

Konstrukce těchto detektorů je založena na principu přerušení vodivého média. Tímto médiem bývá nejčastěji velmi jemný drátek zabudovaný uvnitř fólie, tapety či skla. Dříve se používali pro ochranu velkých skleněných ploch jako jsou například výlohy obchodů. Při instalaci fóliového polepu se na střežené ploše vytvoří tenká vodivá vrstva. Ta je součástí zabezpečující smyčky. Pokud narušitel rozbije střeženou plochu (výlohu) dojde k přerušení polepu a klidového proudu na smyčce což vede k vyhlášení poplachu. Dnes je použití těchto prvků na ústupu a jsou nahrazovány spíše detektory rozbití skla. [1][6]

3.5.7.2 Vodičové sítě a zátarasy

Tento typ detektorů se dříve používali jako ochrana trezorových prostorů, depozitářů s velmi cennými předměty a podobně. Jsou založeny na předpokladu, že narušitel má značné znalosti bezpečnostních systému, patřičné technické vybavení. Vodičová síť využívá slabý

vodič, kterým je nepřerušovaně cca v 15 cm odstupech pokryta celá stěna, která je následně nahozena omítkou. Aby bylo možné detekovat, kde došlo k narušení, tvoří jedna stěna samostatnou smyčku. [6]

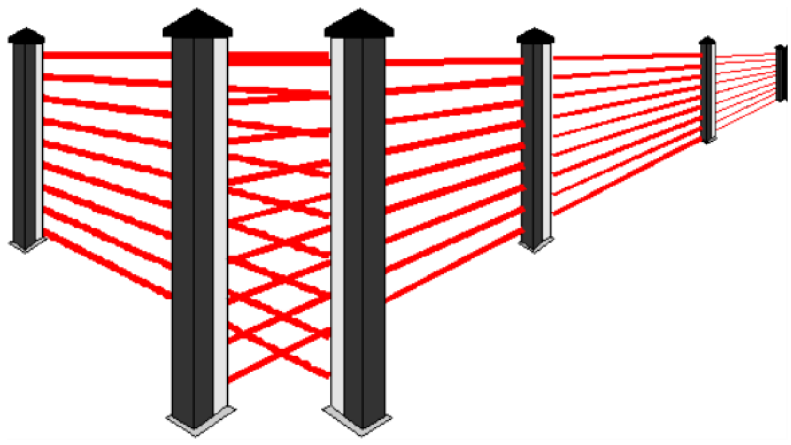
3.5.7.3 Světlovodné sítě

Podobně jako vodičové sítě lze světlovodné využít k ochraně trezorových místností a ve všech prostorech, kde hrozí možné probourání pláštěm ať už se jedná o zeď či skleněnou plochu. Původně byl tento typ detektorů vyvinut pro střežení podvodních prostorů jako jsou vjezdy do přístavů či hranice řek. Obrovskou výhodou je, že zde nevznikají plané poplachy. Hlavním rozdílem oproti vodičovým sítím je, že se nevyužívá drátového vodiče nýbrž optických vláken. [6]

3.5.8 Infračervené závory a bariéry

Infračervené závory či bariéry jsou typem detektorů, které lze využít interně tak externě. Tyto aktivní detektory se skládají ze dvou částí. Jedná se o vysílač a přijímač infračerveného paprsku. Narušení střeženého objektu se vyhodnocuje na základě přerušení infračerveného paprsku mezi přijímačem a vysílačem. V praxi se lze setkat s různými typy těchto detektorů, a to zejména s vyhřívanými či nevyhřívanými infračervenými závorami. Nevýhodou nevyhřívaných infrazávor je malá odolnost proti sněhu a námraze což logicky vede k negativnímu ovlivnění správné funkčnosti. Dále se rozlišuje, zda vysílají modulovaný případně nemodulovaný paprsek. Modulovaný paprsek se od nemodulovaného liší tím, že neruší ostatní přijímače, jelikož vysílaný infračervený signál je kódovaný a určený pro jeden přijímač. [20]

Obrázek 12 – Vizualizace infračervených bariér



Zdroj: [20]

3.5.9 Detektory CO

Oxid uhelnatý (CO) je velmi jedovatý plyn, který vzniká spalováním fosilních paliv jako je například zemní plyn, a u kterého i malá dávka může způsobit velmi vážné zdravotní komplikace. Tento plyn je velmi obtížné detekovat, jelikož je bezbarvý bez zápachu. Proto byly vynalezeny detektory, díky kterým se možné rychle tento plyn detekovat a předejít tak otravě. Existují různé druhy senzorů v závislosti na principu činnosti. Jednou z varianty je využití biomimetrického senzoru, u kterého je vyhlášen poplach na základě změny barvy gelu, jež absorbuje oxid uhelnatý. Další variantou je detektor, jehož funkce spočívá ve snížení elektrického odporu či detekující změny elektrického proudu při kontaktu s CO. [21]

3.5.10 Požární detektory

Detektory požáru pracují na principu detekce určitých jevů (fyzikálních či chemických), jež jsou spojené s požárem. Těmito jevy jsou nejčastěji kouř, rostoucí teplota, plameny či jejich kombinace. Při instalaci těchto detektorů je nutné dbát na instalační pokyny, které jsou dány normami a výrobcem. Nejvíce používaným typem požárního hlásiče jsou tzv. bodové hlásiče, které se připevňují na strop. Detektor je pak možné projit s ústřednou bezpečnostního systému nebo využít autonomní detektory, které pracují samostatně ale disponují pouze s lokální zvukovou signalizací. Napájení těchto detektorů bývá z pravidla pomocí 9 V článků případně ze sítě. Jednotlivé typy detektorů pracují na různých principech detekce požáru. [1]

Mezi nejčastější typy požárních detektorů patří:

- teplotní;
- kouřové;
- ionizační;
- optické a další. [1]

3.5.10.1 Teplotní detektory

Principem činnosti tohoto typu, je v identifikaci požáru na základě rostoucí okolní teploty. Detektor při překročení určité teploty vyhlásí poplach či předá informace ústředně, která je vyhodnotí. Bývají také označovány jako statické detektory teploty, jelikož jsou vyráběny pro určité poplachové teploty, přibližně v rozmezí od 60 °C do 100 °C. Nevýhodou tohoto řešení, je skutečnost, že při příliš nízké poplachové teplotě mohou vznikat plané

poplachy. Naopak při příliš vysoké může dojít k pozdnímu vyhlášení požáru. Řešení tohoto problému nabízí diferenciální detektory teploty, které se nezaměřují na určitou teplotu ale na rychlost změny teploty. Nejlepší variantou jsou pak kombinované detektory teploty, jež kombinují funkci obou předchozích. [20]

3.5.10.2 Kouřové detektory

Kouřové detektory požáru patří k nejpoužívanějším detektorům požáru. Pro svoji činnost využívají pulzní infračervenou diodu (IRED) a fotodiodu. Ty se nacházejí v komoře bez přístupu světla, do které může proniknout kouř a jeho částice. To způsobí pokles intenzity paprsku vyzařovaného infračervenou diodou. Pokud fotodioda detekuje dvakrát po sobě pokles intenzity vyhodnocuje tento stav jako poplachový. Výhodou oproti teplotním detektorům je včasnější varování již při vznikajícím požáru. [1]

3.5.10.3 Ionizační detektory

Při hoření se do vzduchu uvolňuje celá řada plynů a kouř na bázi uhlíku. Této skutečnosti využívají právě ionizační požární detektory. Ty jsou vybaveny dvěma komorami tzv. vnější otevřenou a vnitřní referenční. Uvnitř komory je fólie, kterou prochází elektrický proud a velmi malé množství radioaktivního prvku Americium. Detekce je založena na porovnávání rozdílového napětí mezi jednotlivými komorami. Pokud je překročena určitá hodnota je vyhlášen poplach. Výhodou je, že detektor dokáže reagovat již při velmi malém množství částic ve vzduchu. Za nevýhodu lze označit přítomnost radioaktivního prvku. [20]

3.5.10.4 Multisenzorové detektory

Tento druh detektoru požáru, kombinuje vlastnosti a technologie ostatní detektorů požáru. Jedná se především o optický, teplotní a chemický senzory, které jsou doplněny inteligentní elektronikou pro vyhodnocení. Vyznačující se velmi vysokou odolností oproti falešným poplachům, nízkou spotřebou energie a rychlou detekcí požáru již při jeho vzniku. [1]

3.6 Kamerové systémy

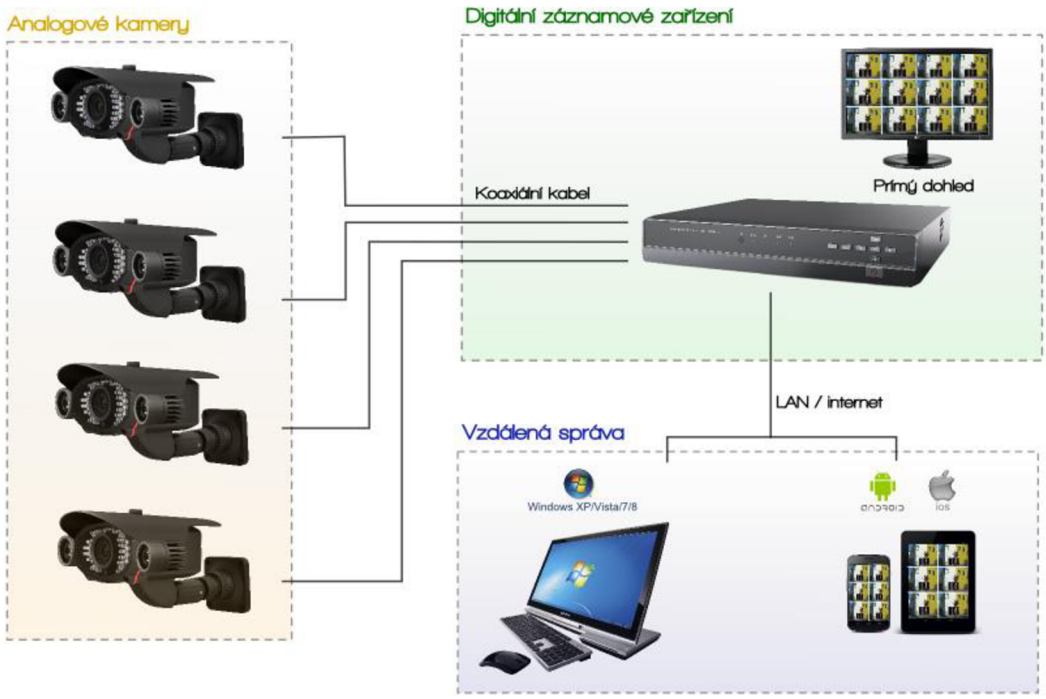
Kamerový systém, bývá označován jako uzavřený televizní okruh či anglickou zkratkou CCTV (Closed Circuit Televison) a tvoří další velmi důležitou a oblíbenou součást elektronického zabezpečovacího systému. Jedním z hlavních důvodu je možná identifikace narušitele a pořizování důkazních materiálů. Běžně se s nimi setkáváme každý den, ať už se jedná o dopravní kamerové systémy či jsou součástí interiérové a exteriérové ochrany objektů. Mezi nejrozšířenější druhy kamerových systému patří analogové a digitální, někdy označované jako IP kamerové systémy, pokud využívají právě IP kamery. Samotné kamerové zařízení lze rozdělit do dvou typů dle tvaru konstrukce. První typ je označován jako DOME a jedná se o kamery s kopulovitým tvarem. Druhou skupinou jsou kamery označované jako BULLET, které mají tvar tubusu. Velkou výhodou, kterou tyto systémy poskytují je vzdálený dohled v reálném čase, díky čemuž je možné střežený objekt monitorovat odkudkoliv pomocí chytrého telefonu, tabletu nebo PC a to nonstop 24 hodin denně. [22]

3.6.1 Analogový kamerový systém

Tyto kamerové systémy pracují s analogovým výstupem v rozlišení 720x576 (případně 960x576) obrazových bodů v poměru stran 4:3. Přenos signálu se nejčastěji provádí přes obyčejné koaxiální kabely s BNC konektory. Délka takového kabelového vedení je závislá na kvalitě použitého koaxiálního kabelu ovšem maximálně 100 m. Pokud je vedení delší dochází k tlumení signálu což způsobuje zhoršení kvality obrazového záznamu. Pro delší vzdálenosti je nutné využít zesilovač signálu. [23]

Modernější analogovou technologii představuje AHD kamerový systém, který disponuje vysokým rozlišením až 1920x1080 (Full HD). Výhodou tohoto systému je, že pomocí převodu digitálního signálu do analogového je prodloužena přenosová vzdálenost a uspořena kapacita zálohových úložišť. I zde se pro přenos signálu využívají koaxiální kabely s maximální délkou 500 metrů. Nevýhodou je právě omezená délka kabelového vedení a riziko rušení signálu. [23]

Obrázek 13 – Schéma analogového kamerového systému



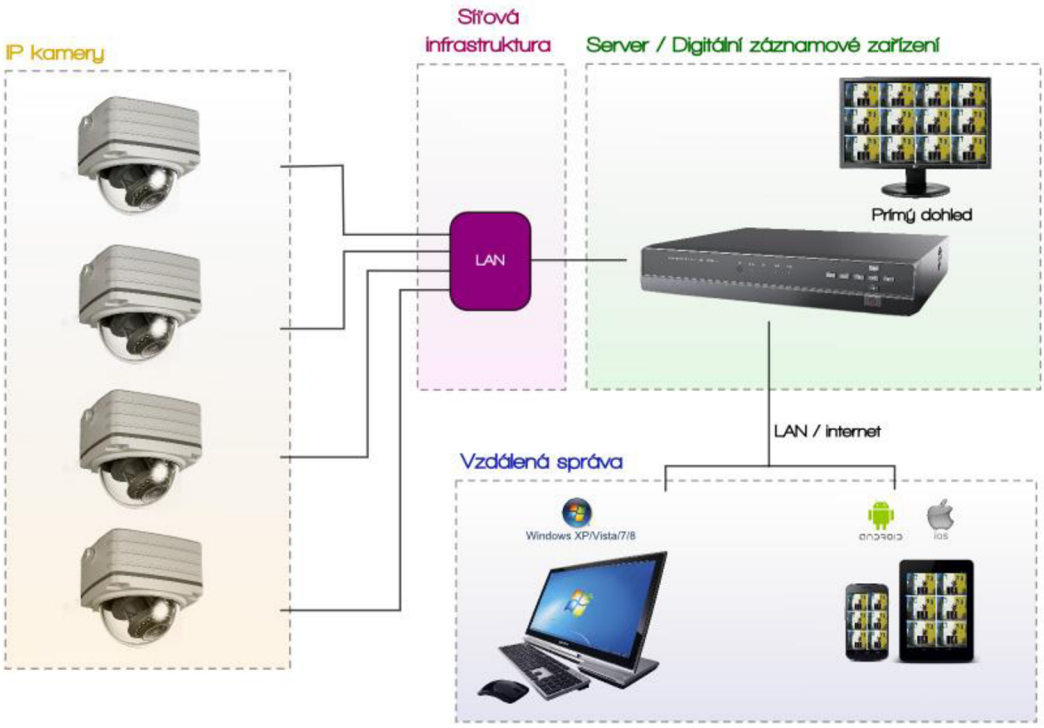
Zdroj: [23]

Tyto systémy jsou poměrně jednoduché na obsluhu a instalaci. Vzdálený dohled u těchto systému je zajišťován tzv. DVR rekordérem, který je připojen do sítě LAN a skrze router je obraz přenášen na různá zařízení. [23]

3.6.2 Digitální kamerový systém

Tento typ kamerového sytému vznikl na základě požadavků na větší rozlišení obrazu, které nejsou analogové typy kamerových systému schopné dosáhnout. Tyto systémy nemají díky digitálnímu signálu žádné omezení ze strany maximální rozlišení obrazu. To je dáno pouze typem použitých kamer, uložištěm a propustností dané sítě. U těchto systému se pro přenos signálu používají datové kabely označované jako UTP, které zároveň zařízení napájejí a protokol TCP/IP. Od jednotlivých IP kamer, z nichž každá má standartní konektor (RJ45) pro připojení do sítě LAN, jsou pak kabely svedeny do aktivního síťového prvku (switch). [24]

Obrázek 14 – Schéma digitálního kamerového systému



Zdroj: [23]

Z důvodu velkého objemu dat, které se přenášejí a zálohují se využívají kompresní formáty. Nejčastěji se jedná o formáty M-JPEG, MPEG-4, H.264 a H.265. U IP kamer se nejčastěji využívá formát H.264. Tento formát disponuje velkou kompresní činností výsledného souboru, a to až o 80 % oproti M-JPEG a až o 50 % oproti MPEG-4. [24]

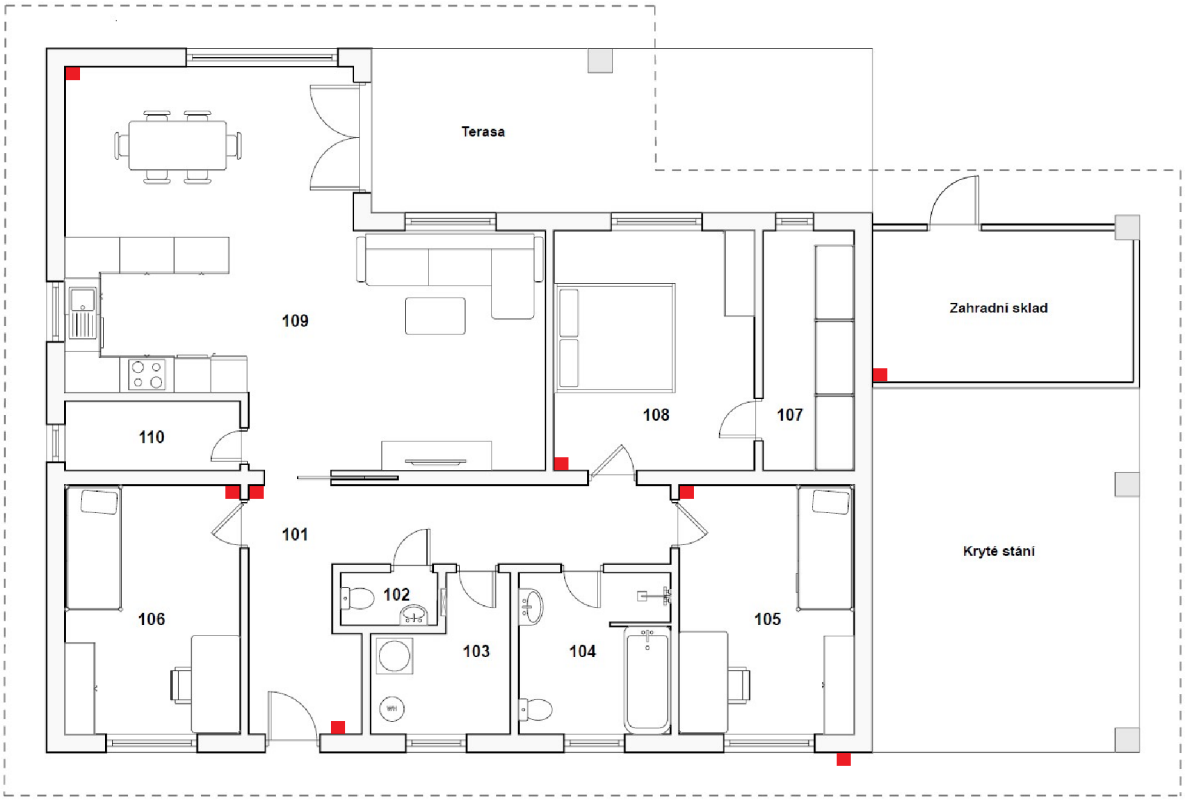
Výhodou digitálního kamerového systému, je snadná instalace a udržovatelnost při základní znalosti počítačových sítí. V případě potřeby je možné velmi snadno rozšířit kamerovou síť o další zařízení. A také možnost vzdáleného přístupu odkudkoliv a velmi vysoká kvalita obrazu až ve 4K (3840x2160 obrazových bodů). [24]

4 Vlastní práce

4.1 Popis objektu

Elektronický zabezpečovací systém byl vybírán pro rodinný dům autora práce, který byl v době psaní práce ve výstavbě. Dům se nachází na okraji obce Sedlčany ve Středočeském kraji asi 60 km jižně od Prahy. Jedná se o přízemní bungalov o dispozici 4+kk a užitou plochou 110 metrů čtverečních. Při realizaci rozvodů elektřiny byly připraveny slaboproudé rozvody pro hlavní prvky zabezpečovacího systému jako jsou pohybové detektory, venkovní siréna a ovládací klávesnice. Tyto rozvody byly realizovány pomocí kabelu UTP CAT5e a jejich vyústění je znázorněno červenými čtverečky v půdorysu budovy viz obrázek č.15. Kabelové rozvody pro kamery nejsou v půdorysu zakresleny, jelikož budou dodělávány následně skrze půdní prostor a podbití. Případné další prvky, pro které nebyla připravena kabeláž, budou realizovány bezdrátově. Předpokládá se tedy využití hybridního zabezpečovacího systému.

Obrázek 15 – Půdorys rodinného domu



Zdroj: vlastní zpracování

Budova se nachází na pozemku s výměrou 926 metrů čtverečních, kdy přední strana budovy je situována směrem ke komunikaci a ostatní strany jsou situovány k sousedním parcelám. Vytápění objektu bude realizováno teplovodním podlahovým topením pomocí zemního plynu, který je přiveden na hranici pozemku. Samotný plynový kondenzační kotel bude taktéž využíván k ohřevu vody. Internetové připojení bude řešeno pomocí venkovní antény umístěné na střeše objektu.

Objekt disponuje 9 otevíratelnými okny a jedním velkým, 2,5 metrů širokým fixním oknem umístěným v jídelně. Vstup do objektu je možný skrze dvoje dveře. První a primární možností je vstup přes hlavní vchodové dveře s pěti bodovým zámkem, vedoucí do zádveří. Druhou variantou je vstup přes balkónové dveře z terasy objektu. V domě jsou dva pokoje, ložnice s šatnou, koupelna s WC, technická místnost, samostatné WC, spíž a kuchyň spojená s obývacím pokojem a jídelnou. Samotná konstrukce domu je z keramického zdiva, sádrokartonových stropů a betonové střešní krytiny. Součástí domu je také dřevěný zahradní sklad.

4.1.1 Silná a slabá místa objektu

Za silné místo, z pohledu samotného domu, byla označena pravá (jižní) strana budovy, kde se nenacházejí žádné stavební otvory jako okna či dveře, a to z důvodu umístění krytého stání pro automobil a zahradního skladu. Naopak jako slabé místo, byla označena zadní (východní) strana budovy. Nachází se zde velké prosklené balkonové dveře, velké fixní okno a tři běžná okna, také nebylo uvažováno použití venkovních rolet či žaluzií, které by plnily funkci částečné ochrany před vniknutím. Samotný zahradní sklad byl určen jako další slabé místo. Dalším důvodem je špatná viditelnost do zadní části z přilehlé komunikace a sousedních parcel.

4.1.2 Specifikace střežených prostor

4.1.2.1 Zádveří s chodbou

Společná podlahová plocha zádveří s chodbou, označené v půdorysu jako 101, činí necelých 14 metrů čtverečních. Šířka samotné chodby je 1,3 metrů a zádveří 2 metry. V těchto prostorách bude umístěna ovládací klávesnice, požární hlásič, vnitřní siréna, magnetické kontakty a pohybový detektor.

4.1.2.2 Pokoje

Pokoje jsou v půdorysu označené čísly 105 a 106. Jejich podlahová plocha se shodná a činí necelých 12 metrů čtverečních. Jsou situovány na západní stranu směrem k přilehlé komunikaci. V každém pokoji bude použit jeden pohybový detektor PIR.

4.1.2.3 Ložnice

Ložnice, označená jako 108, disponuje podlahovou plochou 12 metrů čtverečních a je spojená s přilehlou šatnou označenou jako 107. V této místnosti bude použit jeden pohybový detektor. Samotná šatna zůstane bez střežení.

4.1.2.4 Obývací část s kuchyní a jídelnou

Největší místnost domu je označena jako 109 a jedná se o spojení obývacího pokoje, kuchyňského koutu a jídelny. Podlahová plocha této místností činí přibližně 40 metrů čtverečních. Střežení tohoto prostoru bude zajištěno pomocí magnetických kontaktů, detektoru kouře a detektoru tříštění skla v kombinaci s PIR z důvodu větších skleněných ploch v podobě fixního okna a balkonových dveří.

4.1.2.5 Technická místnost

Technická místnost má podlahovou plochu 4,8 metrů čtverečních a je označena číslem 103. Je zde elektrický rozvaděč, plynový kondenzační kotel se zásobníkem vody a pračka se sušičkou. V této místnosti bude kromě požárního hlásiče, detektoru pohybu a detektoru CO umístěna ústředna samotného zabezpečovacího a případně záznamové zařízení.

4.1.2.6 Venkovní prostory

Co se týče venkovních prostor, zde budou umístěné dvě IP kamery, konkrétně na severozápadní a jihovýchodní straně objektu. Na přední, tedy západní straně, bude umístěna venkovní siréna.

4.1.2.7 Zahradní sklad

Posledním střeženým prostorem, je venkovní zahradní sklad. Celý sklad, který je včetně dveří tvořen dřevěnou konstrukcí a palubkovým pobitím, disponuje rozlohou

přibližně 10 metrů čtverečních. Sklad je uzamykán pomocí petlice a bezpečnostního visacího zámku. V tomto prostoru bude umístěn jeden pohybový detektor.

4.1.3 Výčet požadovaných prvků

Následující tabulka č. 6 zobrazuje výčet požadovaných prvků včetně způsobu připojení, počtů a specifikace místnosti, ve které budou použity.

Tabulka 6 – Požadované prvky EZS, vlastní zpracování

Prvek	Typ	Počet	Místnost
Ústředna	-	1	103
Ovládací klávesnice	drátové	1	101
Vnitřní siréna	bezdrátové	1	101
Detektor kouře	bezdrátové	3	101, 103, 109
Magnetické kontakty	bezdrátové	2	101, 109
PIR detektor	drátové	6	101, 103, 105, 106, 108, Sklad
Kombinovaný detektor PIR + sklo	drátové	1	109
Detektor CO	bezdrátové	1	103
Venkovní siréna	drátové	1	exteriér

Zdroj: vlastní zpracování

4.2 Zhodnocení objektu dle norem ČSN

Před samotným výběrem zabezpečovacího systému bylo nutné určit požadovaný stupeň zabezpečení dle normy ČSN EN 50131-1. Stupně zabezpečení jsou rozděleny do čtyř tříd dle míry rizika a jsou popsány v teoretické části práce. Jelikož se objekt nachází na klidném okraji města, jedná se o standartní přízemní rodinný dům a nepředpokládá se výskyt velmi drahých a cenných předmětů či trezorů, byl zvolen stupeň zabezpečení 1, tedy nízké riziko. Tento stupeň udává, že v objektu by měli být zabezpečeny obvodové dveře proti otevření a v ostatních místnostech, kde se předpokládá možný pohyb narušitele, by měla být zajištěna prostorová ochrana například pomocí PIR detektorů.

Aby byla zajištěna správná funkčnost systému a jednotlivých komponent bylo také nutné správně určit klasifikaci prostředí opět dle ČSN EN 50131-1. Ta je podobně jako stupeň zabezpečení rozdělena do čtyř kategorií. Zde byla pro zabezpečovací systém zvolena třída prostředí II., tzn. vnitřní všeobecné prostředí s rozsahem teplot od -10 °C do +40 °C.

Podobně je tomu i u kamerového systému, ovšem zde se řídíme normou ČSN EN 62676-1-1. Po zvážení všech faktorů byl zvolen taktéž stupeň zabezpečení 1 tzn. nízké riziko. Třída prostředí byla s ohledem na plánované umístění kamer, tedy venku na přesahu střechy, zvolena s rozsahem teplot -25 °C až +50 °C což odpovídá třídě III. – venkovní chráněné prostředí.

4.3 Analýza českého trhu

Na českém trhu je v současné době možné pořídit řada zabezpečovacích systémů od různých výrobců, různého rozsahu, technologie a určení. Pro koncového uživatele to tak může být velmi složitý výběr. Nabídka začíná od jednoduchých systému určených pro zabezpečení malých prostor jako jsou například chaty či volně stojící garáže až po velmi komplexní systémy určené pro velké prostory jako jsou například výrobní haly a podobně. Mezi největší hráče na tomto trhu patří jednoznačně česká společnost Jablotron a.s. Velká část firem, které nabízejí odborné instalace bezpečnostních systému má ve své nabídce také systémy právě od společnosti Jablotron. Jedním z důvodů je to, že díky tomu, že se jedná o českou společnost je zde velmi kvalitní partnerský program pro firmy či jednotlivce včetně pravidelné nabídky školení či kvalitní nonstop technické podpory. Další systémy, které

se často vyskytují v nabídkách firem, jsou od polské společnosti Satel a kanadské společnosti Paradox. Dále můžeme narazit na výrobky či systémy od dalších firem jako DSC, AJAX, iGET a dalších, které často mají omezenou nabídku jednotlivých prvků a nejedná se o tak komplexní systémy. Z toho důvodu je v práci uvažováno použití právě jedno z nabízených systémů od společnosti Jablotron, Satel či Paradox, které budou následně podrobeny vícekriteriálnímu srovnání na základě stanovených hodnotících kritérií a požadavků.

4.3.1 Jablotron

Jak již bylo zmíněno, Jablotron a.s. je česká firma, která byla založena v roce 1990 v Jablonci nad Nisou. Již od založení se věnuje bezpečnostním systémům a postupem času se propracovala na pozici jedno z nejvýznamnějších dodavatelů bezpečnostních systému v České republice i ve světě a aktuálně své produkty vyváží do 73 zemí. [25]

Hlavním produktem v oblasti zabezpečovacích systémů společnosti Jablotron je systém Jablotron-100, někdy označován jako JA-100. Jedná se o velmi komplexní bezpečnostní systém, jenž má v nabídce celou řadu drátových či bezdrátových prvků, komunikačních modulů nebo například vlastní kamerový systém. Celý systém je navíc možné ovládat pomocí mobilního zařízení či počítače skrze aplikaci MyJablotron. Díky tomu je možné vytvořit zabezpečení objektu přesně na míru požadavkům investora.

4.3.2 Satel

Satel je polská společnost se sídlem v Gdaňsku (od roku 2014), která byla založena v roce 1990 a zabývá se výrobou zabezpečovacích systémů. Hlavním distributorem pro Českou republiku je společnost Euroalarm s.r.o. Oproti společnosti Jablotron, nalezneme v nabídce společnosti Satel několik různých systémů, konkrétně se jedná o systémy Versa, Perfecta, Integra a Micra. [26]

Systémy Versa a Perfecta jsou moderní a komplexní zabezpečovací systémy vhodné pro zabezpečení menších objektů jako jsou například byty, domy nebo malé obchodní prostory. Systémy je možné využívat s drátovými či bezdrátovými prvky a vytvořit tak v případě potřeby hybridní systém. Vzdálené ovládání je možné pomocí aplikace Versa Control respektive Perfecta Control. Systémy Integra disponují nejvýkonnějšími ústřednami,

které firma nabízí a jsou certifikované 3 stupněm úrovně zabezpečení. Správa systému se provádí pomocí aplikace Integra Control. Posledním systémem v nabídce je bezdrátový systém Micra, který jak už název napovídá je určený především pro ochranu malých prostorů jako jsou například chaty, garáže či mobilní prodejny, a proto nebude do srovnání zařazen.

4.3.3 Paradox

Společnost Paradox byla založena v roce 1989 v kanadském Montrealu a současnosti patří mezi jednoho z největších výrobců zabezpečovacích systémů na světě. Distribuci pro Českou republiku zajišťuje firma Eurosat CS s.r.o. V produktové nabídce můžeme v současné době nalézt především výrobky ze série Spectra, Magellan či Digiplex Evo. [27]

Systém Spectra SP se skvěle hodí k zabezpečení menších a středních objektů jako jsou byty či rodinné domy. Oproti tomu řada Digiplex Evo je určena hlavně pro velké prostory jako jsou firmy nebo výrobní haly, jelikož podporují až 192 zón a 999 uživatelů a z tohoto důvodu nebude podobně jako systém Satel Micra do vícekriteriálního srovnání zařazen.

4.4 Vícekriteriální analýza variant

Tato kapitola se zabývá výběrem kompromisní varianty EZS pomocí vícekriteriální analýzy variant, které byly pro srovnání vybrány na základě průzkumu trhu. Celkem se bylo srovnáváno devět ústředen od třech největších výrobců. Ústředny byly zvoleny, jelikož představují tzv. srdce elektronického zabezpečovacího systému a definují jeho parametry. Pro určení vah kritérií byla použita Saatyho metoda a pro samotné určení kompromisní varianty byla využita metoda TOPSIS. Jelikož různé metody mohou vést k různým řešením byla následně použita navíc metoda váženého součtu, a to z důvodu ověření výsledků. Varianty byly hodnoceny jedním rozhodovatelem, a to autorem práce, jelikož se jedná o budoucího uživatele vybíraného systému.

4.4.1 Saatyho metoda

Saatyho metoda, označována také jako metoda kvantitativního párového porovnání se využívá, pokud je pouze jeden hodnotitel. Při párovém porovnání se využívá tzv. Saatyho bodovací stupnice, která má 9 stupňů od 1 do 9, přičemž není potřeba využívat všechny ale lze například používat pouze liché mezistupně. Zkrácená podoba stupnice je uvedena v tabulce č.7.

Tabulka 7 – Saatyho bodovací stupnice

Body	Preference *i*-tého kritéria před *j*-tým
1	žádná, rovnocenná kritéria
3	slabá preference
5	silná preference
7	velmi silná preference
9	absolutní preference

Zdroj: [28]

Jednotlivá ohodnocení preferencí se zapisují do Saatyho matice, která má na hlavní diagonále jedničky, což značí rovnocennost kritéria se sebou samým. Pokud je řádkové (i-té) kritérium preferováno před sloupcovým (j-tým) je do pole zapsána příslušná bodová hodnota odpovídající síle preference. V opačném případě, tedy pokud je preferováno sloupcové kritérium před řádkovým, se zapíše do pole převrácená hodnota.

V dalším kroku se pro každé kritérium stanový geometrický průměr dle následujícího vzorce:

$$b_i = \sqrt[k]{\prod_{j=1}^{k} s_{ij}} \tag{1}$$

kde s_{ij} jsou hodnoty preferencí a k znační celkový počet kritérií. [28]

Poslední krok spočívá ve výpočtu vah samotných kritérií, které se vypočítají pomocí tohoto vztahu:

$$v_i = \frac{b_i}{\sum_{i=1}^{k} b_i} \tag{2}$$

tedy vydělením vlastním součtem, jelikož součet vah musí být roven 1. [28]

4.4.2 Metoda TOPSIS

Metoda TOPSIS využívá k posouzení variant výpočet vzdáleností od ideální a bazální, tedy nejhorší varianty. Šubrt a kolektiv popisuje postup této metody v následujících čtyřech krocích:

1. Vytvoření normalizované kriteriální matice R podle vzorce

$$r_{ij} = \frac{y_{ij}}{\sqrt{\sum_{i=1}^{p} y_{ij}^2}} \tag{3}$$

2. Určení normalizované vážené kriteriální matice W podle vztahu

$$w_{ij} = v_j r_{ij} \tag{4}$$

a stanovení ideální (H) a bazální (D) varianty.

3. Výpočet vzdáleností od ideální (di^+) a bazální (di^-) varianty

$$d_i^+ = \sqrt{\sum_{j=1}^{k} (w_{ij} - H_j)^2} \quad d_i^- = \sqrt{\sum_{j=1}^{k} (w_{ij} - D_j)^2} \tag{5,6}$$

4. Výpočet relativních ukazatelů vzdáleností podle vzorce

$$c_i = \frac{d_i^-}{d_i^+ + d_i^-} \tag{7}$$

a následné seřazení variant podle vypočtených hodnot c_i, kde varianta s nejvyšší hodnotnou je považována za kompromisní řešení. [29]

4.4.3 Metoda váženého součtu

Metoda váženého součtu je založena na principu maximálního užitku. Tento užitek je možné vyjádřit pomocí užitkové funkce jejíž hodnoty se nacházejí v uzavřeném intervalu 0 až 1. Čím je hodnota funkce pro danou variantu blíže k jedné tím je varianta lepší. Postup pro výpočet užitku variant je následující:

1. Stanovení ideální (H) a bazální (D) varianty

2. Vytvoření standardizované kriteriální matice R podle vzorce

$$r_{ij} = \frac{y_{ij} - d_j}{h_j - d_j} \tag{8}$$

3. Výpočet funkce užitku pro každou variantu podle vztahu

$$u(a_i) = \sum_{j=1}^{k} v_j \, r_{ij} \tag{9}$$

4. Sestupné seřazení všech variant dle vypočtené funkce užitku $u(a_i)$, kde kompromisní varianta je ta s nejvyšším užitkem. [28]

4.4.4 Varianty

Od společnosti Jablotron byly předmětem srovnání ústředny z řady Jablotron-100 viz tabulka číslo 8. Konkrétně se jedná o ústředny s označením JA-101KR-LAN-3G, JA-103KR a JA-106K-3G. Všechny tyto ústředny podporují připojení bezdrátových prvků a jsou kompatibilní s prvky z řady JA-100. Jablotron také poskytuje mobilní MyJablotron, která je dostupná jak pro iOS, tak Android a slouží pro vzdálenou správu systému.

Tabulka 8 – Údaje o ústřednách Jablotron

JABLOTRON	JA-101KR-LAN-3G	JA-103KR	JA-106K-3G
Max. počet zón	50	50	120
Max. počet prog. výstupů	16	32	32
Max. počet uživatelů	50	50	300
Vzdálený přístup	GSM a LAN součástí	LAN součástí + podpora GSM	GSM a LAN součástí
Podpora RFID čipů	Ano		
Počet čísel pro SMS	8	8	30
Podpora bezdrát. prvků	Ano, modul je součástí	Ano, modul je součástí	Ano, modul **není** součástí
Mobilní aplikace	Ano		
Certifikace	Stupeň zabezpečení 2 / Třída prostředí 2		
Cena ústředny	12 449 Kč	8 549 Kč	12 520 Kč

Zdroj: vlastní zpracování dle [25]

Společnost Satel má ve své nabídce, jak bylo uvedeno v kapitole 4.3.2, systémy Versa, Perfecta, Integra a Micra, který je ovšem určen pouze do malých prostor. Do srovnání byly proto zařazeny pouze ústředny ze systému Versa, Perfecta, Integra. Konkrétně Versa Plus, Perfecta 32-WRL a Integra 32 jejichž základní údaje jsou uvedeny v tabulce č. 9. Také tyto ústředny mohou být vzdáleně spravovány skrze mobilní aplikaci, ale pro každý systém existuje samostatná aplikace Versa Control, Integra Control a Perfecta Control.

Tabulka 9 – Údaje o ústřednách Satel

SATEL	VERSA Plus	PERFECTA 32-WRL	INTEGRA 32
Max. počet zón	30	32	32
Max. počet prog. výstupů	12	12	32
Max. počet uživatelů	30	15	64
Vzdálený přístup	GSM a LAN součástí	GSM součástí, bez podpory LAN	podpora GSM a LAN
Počet čísel pro SMS	16	8	8
Podpora RFID čipů	Ano	Ne	Ano
Podpora bezdrát. prvků	Ano, modul **není** součástí	Ano, modul je součástí	Ano, modul **není** součástí
Mobilní aplikace	Ano		
Certifikace	Stupeň zabezpečení 2 / Třída prostředí 2		
Cena ústředny	11 263 Kč	7 079 Kč	3 588 Kč

Zdroj: vlastní zpracování dle [26]

Tabulka číslo 10, obsahuje základní informace o ústřednách od společnosti Paradox, které byly předmětem srovnání. Jedná se o ústředny s označením MG5050, SP6000 a EVO192 z řad Magellan, Spectra a Digiplex Evo.

Tabulka 10 – Údaje o ústřednách Paradox

PARADOX	MG5050	SP6000	EVO192
Max. počet zón	32	32	192
Max. počet prog. výstupů	16	16	250
Max. počet uživatelů	32	64	999
Vzdálený přístup	podpora GSM a LAN, nejsou součástí		
Počet čísel pro SMS	8		
Podpora RFID čipů	Ne		Ano
Podpora bezdrát. prvků	Ano, modul je součástí	Ano, modul **není** součástí	Ano, modul **není** součástí
Mobilní aplikace	Ano		
Certifikace	Stupeň zabezpečení 2 / Třída prostředí 2		
Cena ústředny	3 355 Kč	2 683 Kč	4 172 Kč

Zdroj: vlastní zpracování dle [27]

Všech devět výše uvedených ústředen disponuje certifikací pro druhý stupeň zabezpečení a druhou třídu prostředí což odpovídá požadavků na tyto certifikace, které byly stanoveny v kapitole 4.2.

4.4.5 Kritéria

Pro hodnocení jednotlivých variant bylo stanoveno jedenáct hodnotících kritérií na základě, kterých byla určena kompromisní varianta pro daný rodinný dům. Aby bylo možné využít metodu TOPSIS a metodu váženého součtu bylo zapotřebí nejdříve slovně vyjádřená kritéria vhodně kvantifikovat. K tomu bylo využito bodové stupnice s rozsahem od 1 do 3.

4.4.5.1 Maximální počet zón

Počet zón je základním a dalo by se říct nejdůležitějším parametrem pro výběr ústředny elektronického zabezpečovacího sytému. Tento parametr udává, kolik zón je možné střežit, přičemž jednu zónu tvoří obvykle jeden detektor, jehož stavy jsou vyhodnocovány. Jedná se o maximalizační kritérium vyjádřené kvantitativně.

4.4.5.2 Maximální počet programovatelných výstupů

Toto kritérium stanovuje, jaký maximální počet dalších zařízení je možné ovládat pomocí ústředny. Mezi tyto zařízení patří především prvky pro automatizaci jako například ovládání světel, klimatizace, garáže, vrat, topení a další. Zde se také jedná o maximalizační kritérium, které je vyjádřené kvantitativně.

4.4.5.3 Maximální počet uživatelů

Maximální počet uživatelů je číslo, které nám říká kolik je maximálně možné nastavit uživatelských kódů (případně klíčenek a čipů) v jednom systému. I toto kritérium je vyjádřeno kvantitativně a má maximalizační povahu.

4.4.5.4 Vzdálený přístup

Vzdálený přístup je maximalizační kritérium, které zahrnuje více požadavků do jednoho. Konkrétně se jedná o podporu GSM a LAN komunikace. Není rozlišováno, zda jsou jednotlivé moduly přímo integrovány na základní desce ústředny či je nutné

je připojit samostatně. Protože je kritérium vyjádřeno kvalitativně, pro další výpočty jej bylo nutné kvantifikovat viz tabulka č. 11.

Tabulka 11 – Kvantifikace kritéria – Vzdálený přístup

Popis	Ohodnocení
Podpora GSM a LAN (součástí či možnost rozšíření)	3
Pouze GSM bez LAN modulu	2
Bez podpory GSM a LAN	1

Zdroj: vlastní zpracování

4.4.5.5 Mobilní aplikace

Dalším kritériem, na základě, kterého byl vybírán zabezpečovací systém, byla mobilní aplikace sloužící k jeho obsluze. Jelikož nebylo možné všechny mobilní aplikace vyzkoušet v reálném provozu, byla data pro hodnocení čerpána z technických dokumentací, návodů a videí k těmto aplikacím. Získaná data byla následně hodnocena pomocí hodnotící stupnice uvedené v tabulce č. 12. Pokud některý z aspektů nebyl splněn či podporován byl ohodnocen 0 body. Při částečném splnění byl přiřazen 1 bod, v případě, že byl aspekt splněn nebo podporován v požadovaném rozsahu, byl ohodnocen 2 body, případně 3 body, při splnění požadavku nad očekávání.

Tabulka 12 – Hodnotící škála pro aspekty mobilních aplikací

Popis	Ohodnocení
Splněno nad rámec	3
Splněno / Podporováno	2
Částečně splněno / Částečně podporováno	1
Nesplněno / Nepodporováno	0

Zdroj: vlastní zpracování

Tabulka 13 – Kvantifikace kritéria – Mobilní aplikace

	Hodnocený aspekt				
Název aplikace	**Android + iOS**	**Přehlednost**	**Funkce**	**Video verifikace**	**Celkem**
MyJablotron	2	2	2	2	**8**
VERSA Control	2	2	2	3	**9**
PERFECTA Control	2	2	2	3	**9**
INTEGRA Control	2	2	3	3	**10**
Insite GOLD	2	1	2	1	**6**

Zdroj: vlastní zpracování

Při kvantifikaci tohoto kritéria byly hodnoceny následující aspekty mobilní aplikace. V první řadě se jednalo o dostupnost aplikace na obou nejpoužívanějších mobilních platformách Android a iOS, dále přehlednost aplikace, její funkce a možnost video verifikace včetně integrace kamer do aplikace samotné. Společnost Jablotron nabízí pro všechny své systémy jednu aplikaci MyJablotron, ta disponuje základními funkcemi pro ovládání bezpečnostního sytému, kontrolu stavu jednotlivých prvků, nastavení notifikací či možnost změny přístupového kódu. Dále je také možnost zobrazit obraz z kamer, a to i od jiných výrobců ale samotné přidání kamery v aplikaci není možné. To se provádí pomocí aplikace MyCompany, kterou disponují montážní partneři.

Satel má pro každý systém samostatnou aplikaci. Tyto aplikace jsou si velmi podobné a na první pohled se odlišují pouze vzhledem. Versa Control a Perfecta Control nabízejí, podobně jako aplikace MyJablotron, základní funkce pro správu zabezpečovacího systému včetně možnosti zobrazení videa z kamer. Navíc však umožňují přidávat kamery do aplikace přímo. Aplikace Integra Control je na tom ještě o trochu lépe, kromě základních funkcí nabízí ještě možnost vytvářet makro funkce pro domácí automatizaci.

Společnost Paradox nabízí pro správu svých systémů aplikaci Insite Gold. Tato aplikace je stejně jako všechny ostatní dostupná jak pro Android tak pro iOS nicméně zaostává za ostatními v přehlednosti. Aplikace působí zastarale a nepřehledně. Funkčně je na tom podobně jako ostatní aplikace s tím, rozdílem, že podporuje video verifikaci pouze ze svých zařízeních HD78F a HD88, což jsou detektory pohybu s kamerou.

4.4.5.6 Počet telefonních čísel pro SMS

Další maximalizační kritérium, které bylo při výběru uplatněno je počet telefonních čísel pro zasílání informativních SMS z ústředny. Tyto informativní SMS mohou být zasílány na různá telefonní čísla například při spuštění alarmu. Kritérium je vyjádřeno kvantitativně.

4.4.5.7 Podpora RFID čipů

Možnost využívat RFID čipy k odblokování systému namísto kódu bylo jedním z dalších kritérií s maximalizační povahou. Tento požadavek byl stanoven z důvodu snazší obsluhy bez nutnosti zadávání kódu. V tabulce č. 14 je uvedena kvantifikace tohoto kritéria.

Tabulka 14 – Kvantifikace kritéria – Podpora RFID čipů

Popis	Ohodnocení
Podpora RFID	1
Bez podpory RFID	0

Zdroj: vlastní zpracování

4.4.5.8 Nabídka prvků

Toto kritérium vychází z požadovaných prvků uvedených v tabulce č. 6 v kapitole 4.1.3. Bylo zjišťováno, zda se daný prvek s požadovaným typem připojení v nabídce výrobce nachází v požadovaném, jiném či žádném provedení. Jelikož tyto základní prvky od jednotlivých výrobců jsou kompatibilní napříč s jejich ústřednami, byli pro zjednodušení hodnoceny samotní výrobci a získané ohodnocení bylo následně zapsáno k ústřednám od těchto výrobců. V tabulce č. 16 je pomocí „X“ označeno, že prvek se v nabídce výrobce nachází v požadovaném provedení. Lomítko „/“ udává, že se prvek v nabídce nachází v jiném než požadovaném provedení a pomlčka „-“ říká, že výrobce prvek nenabízí. Tabulka č. 15 popisuje kvantifikaci tohoto kritéria.

Tabulka 15 – Kvantifikace kritéria – Nabídka prvků

Popis	Ohodnocení
V nabídce jsou všechny požadované prvky v požadovaném provedení	3
V nabídce jsou všechny požadované prvky ale některé pouze v jiném provedení	2
V nabídce chybí některý z požadovaných prvků nebo není podporován	1

Zdroj: vlastní zpracování

Tabulka 16 – Nabídka výrobců s ohledem na požadované prvky a technologie

Prvek	Připojení	Výrobce		
		Jablotron	Satel	Paradox
Ovládací klávesnice	drátové	X	X	X
Vnitřní siréna	bezdrátové	X	X	X
Detektor kouře	bezdrátové	X	X	X
Magnetické kontakty	bezdrátové	X	X	X
PIR	drátové	X	X	X
PIR + sklo	drátové	X	X	-
Detektor CO	bezdrátové	/ (autonomní + modul)	X	X
Venkovní siréna	drátové	X	X	X
Ohodnocení dle tabulky č. 15		**2**	**3**	**1**

Zdroj: vlastní zpracování

Jablotronu chybí v nabídce bezdrátový detektor oxidu uhelnatého, který by přímo komunikoval s ústřednou. Nabízí pouze autonomní provedení tohoto detektoru s možností bezdrátového propojení s ústřednou pomocí speciálního modulu, který se instaluje přímo do detektoru. Společnost Satel má v nabídce všechny požadované prvky v požadovaném provedení. Oproti tomu Paradox nenabízí kombinovaný PIR detektor s detektorem tříštění skla. Ten by bylo nutné nahradit dvěma samostatnými detektory.

4.4.5.9 Estetika prvků

Kromě technický parametrů byla také hodnocena estetika prvků elektronického zabezpečovacího systému. Důvodem pro zahrnutí tohoto kritéria do srovnávání je především fakt, že se jedná o novostavbu rodinného domu, a proto je zde také požadavek na to, aby jednotlivé prvky nepůsobili zastarale, nemoderně či příliš výrazně. Hodnocení probíhalo na základě subjektivního názoru autora práce, jakožto rozhodovatele a budoucího uživatele sytému.

Tabulka 17 – Kvantifikace kritéria – Estetika prvků

Popis	Ohodnocení
Moderní, estetické	3
Průměrné	2
Nemoderní, neestetické	1

Zdroj: vlastní zpracování

4.4.5.10 Rozšiřitelnost s ohledem na chytrou domácnost

Předposledním kritériem, které bylo hodnoceno byla rozšiřitelnost systému o prvky chytré domácnosti. Nejlépe si v této oblasti vedly ústředny od společnosti Satel. Konkrétně ústředna z řady Integra, kterou je možné rozšířit o systém Satel KNX což je systém pro kompletní automatizaci budov. Díky tomuto systému je možné řídit vytápění, stínění, osvětlení včetně stmívání, detekovat unik kapalin či vzdáleně ovládat různá zařízení jako například vjezdové brány a garážová vrata. Satel navíc oproti ostatním výrobcům nabízí také chytré zásuvky. Na druhém místě je společnost Jablotron, která udělala v oblasti automatizace značný pokrok nicméně na společnost Satel to stále nestačí. Jedná se například o zmíněné chytré zásuvky, které sice jednu dobu v nabídce Jablotronu byly ale jejich prodej byl ukončen. Oproti konkurenci také nenabízí dotykové panely na ovládání systému. Na posledním místě, ale pouze s drobným odstupem, je společnost Paradox, jejíž nabídka je ještě o trochu omezenější než u Jablotronu.

Tabulka 18 – Kvantifikace kritéria – Rozšiřitelnost s ohledem na chytrou domácnost

Popis	Ohodnocení
Široká rozšiřitelnost	3
Omezená rozšiřitelnost	2
Velmi malá či žádná možnost rozšíření	1

Zdroj: vlastní zpracování

4.4.5.11 Cena systému

Posledním kritériem, které bylo hodnoceno je cena systému, která byla určena jako součet ceny ústředny včetně potřebných modulů, záložního napájecího zdroje a cen jednotlivých prvků dle požadovaného množství. Prvky, které v nabídce daných výrobců chybí úplně byly nahrazeny odpovídající alternativou.

U ústředen od výrobce Jablotron bylo počítáno s cenou autonomního bezdrátového detektoru oxidu uhelnatého doplněného o komunikační modul. Firma Paradox nemá v nabídce kombinovaný infračervený detektor s detektorem tříštění skla. Proto bylo pro určení celkové ceny ústředen Paradox počítáno s cenou samostatného drátového PIR detektoru a detektoru tříštění skla.

Pro toto kritérium byla stanovena aspirační úroveň v podobě maximální celkové ceny systému bez kamerového systému ve výši 45 000 Kč včetně. Systémy, jejichž cena toto kritérium překročila, byly z analýzy vyřazeny. Tabulky s určením cen jednotlivých variant jsou uvedeny v příloze této práce.

4.4.6 Stanovení vah kritérií

Váhy hodnotících kritérií byly stanoveny pomocí Saatyho metody párového porovnání. Pro hodnocení bylo využito bodovací stupnice dle tabulky č. 7 v kapitole 4.4.1. Preference kritérií znázorňuje níže uvedená tabulka č. 19. Pro větší přehlednost tabulky byly kritériím přiřazeny následující zkratky:

- **CS** – Cena systému (MIN);
- **PZ** – Maximální počet zón (MAX);
- **PG** – Maximální počet programovatelných výstupů (MAX);

- **PU** – Maximální počet uživatelů (MAX);
- **PC** – Počet telefonních čísel pro SMS hlášení (MAX);
- **E** – Estetika prvků (MAX);
- **VP** – Vzdálený přístup (MAX);
- **MA** – Mobilní aplikace (MAX);
- **RFID** – Podpora RFID čipů (MAX);
- **NP** – Nabídka prvků výrobce (MAX);
- **SH** – Rozšiřitelnost systému s ohledem na chytrou domácnost (MAX).

Tabulka 19 – Saatyho matice

	CS	PZ	PG	PU	PC	E	VP	MA	RFID	NP	SH
CS	1	5	7	7	9	9	3	9	7	3	7
PZ	0,2	1	5	7	7	7	5	7	7	3	7
PG	0,14	0,2	1	0,33	7	5	0,2	7	5	0,2	5
PU	0,14	0,14	3	1	3	5	0,14	5	3	0,14	0,33
PC	0,11	0,14	0,14	0,33	1	5	0,14	5	3	9	3
E	0,11	0,14	0,2	0,2	0,2	1	0,14	0,2	3	0,11	0,2
VP	0,33	0,2	5	7	7	7	1	7	7	0,2	7
MA	0,11	0,14	0,14	0,2	0,2	5	0,14	1	5	0,14	3
RFID	0,14	0,14	0,2	0,33	0,33	0,33	0,14	0,2	1	0,14	3
NP	0,33	0,33	5	7	0,11	9	5	7	7	1	7
SH	0,14	0,14	0,2	3	0,33	5	0,14	0,33	0,33	0,14	1

Zdroj: vlastní zpracování

Následující tabulka č. 20 obsahuje vypočtené váhy jednotlivých kritérií. Největší váhu při rozhodování mělo kritérium ceny systému (CS), následuje maximální počet zón (PZ), vzdálený přístup (VP) a nabídka prvků (NP), jejichž váhy se od sebe odlišují pouze v malé míře. Naopak nejméně důležitým kritériem byla estetika (E), podpora RFID čipů (RFID) a rozšiřitelnost systému s ohledem na chytrou domácnost (SH).

Tabulka 20 – Vypočtené váhy kritérií

Kritérium	Váha
CS	0,2973
PZ	0,2105
PG	0,0615
PU	0,0459
PC	0,0496
E	0,0143
VP	0,1287
MA	0,0254
RFID	0,0171
NP	0,1268
SH	0,0230
∑	**1**

Zdroj: vlastní zpracování

4.4.7 Výběr kompromisní varianty

Aby i zde byla zachována přehlednost, bylo z důvodu redukce velikosti tabulek zavedeno nové označení, konkrétně v podobě velkých písmen, které nahrazují dosavadní dlouhá označení jednotlivých variant. Nové označení variant znázorňuje níže uvedená tabulka č. 21.

Tabulka 21 – Varianty a jejich označení

Označení	Varianta
A	JA-101KR-LAN-3G
B	JA-103KR
C	JA-106K-3G
D	VERSA Plus
E	PERFECTA 32-WRL
F	INTEGRA 32
G	MG5050
H	SP6000
I	EVO192

Zdroj: vlastní zpracování

Před samotným výběrem kompromisní varianty bylo nutné nejdříve prozkoumat, zda všechny varianty splňují nastavenou aspirační úroveň u kritéria celkové ceny s hranicí 45 000 Kč včetně. Z tabulky č. 22 je vidět, že tuto aspirační úroveň nesplnili hned dvě varianty od firmy Paradox. Konkrétně se jednalo o variantu H (SP6000) a I (EVO192), které byly pro další postup z tabulky vyřazeny.

Tabulka 22 – Výchozí matice

	CS	PZ	PG	PU	PC	E	VP	MA	RFID	NP	SH
A	32732	50	16	50	8	3	3	8	1	2	2
B	32331	50	32	50	8	3	3	8	1	2	2
C	35847	120	32	300	30	3	3	8	1	2	2
D	36343	30	12	30	16	2	3	9	1	2	3
E	25946	32	12	15	8	2	1	9	0	2	3
F	37346	32	32	64	8	2	3	10	1	2	3
G	44860	32	16	32	8	1	3	6	0	1	1
H	**47242**	32	16	64	8	1	3	6	0	1	1
I	**49947**	192	250	999	8	1	3	6	1	1	3
	MIN	MAX	MAX	MAX	MAX	MAX	MAX	MAX	MAX	MAX	MAX

Zdroj: vlastní zpracování

4.4.7.1 Metoda TOPSIS

Po redukci výchozí matice o neefektivní varianty, které nesplňují stanovenou aspirační úroveň byla aplikována metoda TOPSIS viz kapitola 4.4.2. V prvním kroku bylo nutné stanovit normalizovanou matici R, podle vzorce (3). Vypočtené hodnoty jsou uvedené v tabulce č. 23.

Tabulka 23 – Normalizovaná matice R

	CS	PZ	PG	PU	PC	E	VP	MA	RFID	NP	SH
A	0,349	0,327	0,257	0,157	0,208	0,474	0,405	0,361	0,447	0,316	0,316
B	0,345	0,327	0,514	0,157	0,208	0,474	0,405	0,361	0,447	0,316	0,316
C	0,382	0,785	0,514	0,943	0,781	0,474	0,405	0,361	0,447	0,316	0,316
D	0,387	0,196	0,193	0,094	0,416	0,316	0,405	0,407	0,447	0,474	0,474
E	0,277	0,209	0,193	0,047	0,208	0,316	0,135	0,407	0	0,474	0,474
F	0,398	0,209	0,514	0,201	0,208	0,316	0,405	0,452	0,447	0,474	0,474
G	0,478	0,209	0,257	0,101	0,208	0,158	0,405	0,271	0	0,158	0,158

Zdroj: vlastní zpracování

Následně byla pomocí hodnot z normalizované matice R spočtena vážená kriteriální matice W. Její hodnoty byly spočteny dle vzorce (4), tedy součinu normalizované hodnoty z matice R a váhy daného kritéria a zaznamenány do tabulky č. 24.

Tabulka 24 – Vážená kriteriální matice W

	CS	PZ	PG	PU	PC	E	VP	MA	RFID	NP	SH
A	0,104	0,069	0,016	0,007	0,010	0,007	0,052	0,009	0,008	0,040	0,007
B	0,102	0,069	0,032	0,007	0,010	0,007	0,052	0,009	0,008	0,040	0,007
C	0,114	0,165	0,032	0,043	0,039	0,007	0,052	0,009	0,008	0,040	0,007
D	0,115	0,041	0,012	0,004	0,021	0,005	0,052	0,010	0,008	0,060	0,011
E	0,082	0,044	0,012	0,002	0,010	0,005	0,017	0,010	0	0,060	0,011
F	0,118	0,044	0,032	0,009	0,010	0,005	0,052	0,011	0,008	0,060	0,011
G	0,142	0,044	0,016	0,005	0,010	0,002	0,052	0,007	0	0,020	0,004

Zdroj: vlastní zpracování

Níže uvedená tabulka č. 25 zobrazuje ideální a bazální variantu pro tuto metodu, které byly určeny z vážené kriteriální matice W. Ideální variantu tvoří nejnižší vážená kriteriální hodnota pro celkovou cenu a nejvyšší vážené kriteriální hodnoty všech ostatních kritérií bez ohledu na variantu. Naopak bazální varianta je tvořena přesně opačně.

Tabulka 25 – Ideální a bazální varianta pro metodu TOPSIS

	CS	PZ	PG	PU	PC	E	VP	MA	RFID	NP	SH
ideální	0,082	0,165	0,032	0,043	0,039	0,007	0,052	0,011	0,008	0,060	0,011
bazální	0,142	0,041	0,012	0,002	0,010	0,002	0,017	0,007	0,000	0,020	0,004

Zdroj: vlastní zpracování

V posledním kroku byly vypočteny hodnoty vzdáleností jednotlivých variant od ideální a bazální varianty dle vzorců (5,6) a následně určeny relativní vzdálenosti od bazální varianty označovány jako c_i. Tyto hodnoty byly zapsány do tabulky č. 26.

Jak vyplívá z tabulky č. 26, nejlepších hodnot dosáhla varianta C (JA-106K-3G) od firmy Jablotron. Druhé a třetí místo obsadily také varianty společnosti Jablotron. Na druhém místě to byla varianta B (JA-103KR) a na třetím varianta A (JA-101KR-LAN-3G). Naopak nejhorších hodnot dosáhla varianta G (MG5050) od společnosti Paradox.

Tabulka 26 – Výsledky metody TOPSIS

	di^+	di^-	c_i	Pořadí
A	0,112	0,063	0,3604	3.
B	0,111	0,067	0,3764	2.
C	**0,037**	**0,144**	**0,7936**	**1.**
D	0,137	0,061	0,3102	6.
E	0,137	0,073	0,3461	4.
F	0,134	0,063	0,3196	5.
G	0,150	0,035	0,1894	7.

Zdroj: vlastní zpracování

4.4.7.2 Metoda váženého součtu

Pro ověření citlivosti výsledků metody TOPSIS byla použita metoda váženého součtu. V prvním kroku byla stanovena ideální a bazální varianta dle výchozí tabulky č. 20, opět bez variant, které nesplňují stanovenou aspirační úroveň kritéria celkové ceny s hodnotou 45 000 Kč včetně. Hodnoty kritérií pro ideální a bazální variantu jsou uvedeny v následující tabulce č. 27.

Tabulka 27 – Ideální a bazální varianta pro metodu váženého součtu

	CS	PZ	PG	PU	PC	E	VP	MA	RFID	NP	SH
ideální	25946	120	32	300	30	3	3	10	1	3	3
bazální	44860	30	12	15	8	1	1	6	0	1	1

Zdroj: vlastní zpracování

V dalším kroku byla s využitím ideální a bazální varianty stanovena standardizovaná kriteriální matice R. Hodnoty pro jednotlivé varianty byly vypočteny pomocí vzorce (8) uvedeného v kapitole 4.4.3 a jsou zobrazeny v tabulce č. 28.

Tabulka 28 - Standardizovaná kriteriální matice R

	CS	PZ	PG	PU	PC	E	VP	MA	RFID	NP	SH
A	0,641	0,222	0,200	0,123	0	1	1	0,5	1	0,5	0,5
B	0,662	0,222	1	0,123	0	1	1	0,5	1	0,5	0,5
C	0,477	1	1	1	1	1	1	0,5	1	0,5	0,5
D	0,450	0	0	0,053	0,364	0,5	1	0,75	1	1	1
E	1	0,022	0	0	0	0,5	0	0,75	0	1	1
F	0,397	0,022	1	0,172	0	0,5	1	1	1	1	1
G	0	0,022	0,200	0,060	0	0	1	0	0	0	0

Zdroj: vlastní zpracování

Nakonec byl pro každou variantu vypočten užitek podle vzorce (9) a určeno pořadí variant. Výsledky metody váženého součtu jsou zaznamenány v tabulce č. 29. Z těchto výsledků je patrné, že nejvyššího užitku dosáhla varianta C (JA-106K-3G). Druhé a třetí místo obsadily varianty B (JA-103KR) a varianta F (INTEGRA 32). Nejmenší užitek byl vypočten opět pro variantu G (MG5050).

Tabulka 29 – Výsledky metody váženého součtu

	Užitek	**Pořadí**
A	0,5030	4.
B	0,5585	2.
C	**0,7568**	**1.**
D	0,4760	6.
E	0,4779	5.
F	0,5202	3.
G	0,1484	7.

Zdroj: vlastní zpracování

4.4.7.3 Souhrnné výsledky

Na základě výsledků metody TOPSIS a metody váženého součtu byla zvolena kompromisní varianta JA-106K-3G, která po aplikaci obou metod dosáhla nejlepších výsledků. Tato varianta byla použita pro návrh pilotního nasazení elektronického zabezpečovacího systému.

Tabulka 30 – Výsledky metody TOPSIS a váženého součtu

	c_i	**Užitek**	**Pořadí**
JA-101KR-LAN-3G	0,3604	0,5030	3.
JA-103KR	0,3764	0,5585	2.
JA-106K-3G	**0,7936**	**0,7568**	**1.**
VERSA Plus	0,3102	0,4760	6.
PERFECTA 32-WRL	0,3461	0,4779	5.
INTEGRA 32	0,3196	0,5202	4.
MG5050	0,1894	0,1484	7.

Zdroj: vlastní zpracování

4.5 Návrh pilotního nasazení

V této kapitole bylo vytvořen návrh pilotní nasazení elektronického zabezpečovacího systému, který byl vybrán na základě výsledků vícekriteriální analýzy variant. Navrhovaným zabezpečovacím systémem byl systém od společnosti Jablotron s označením JA-100 a ústřednou JA-106K-3G.

4.5.1 Kamerový systém

Zde se nabízela možnost využít IP kamery právě od výrobce Jablotron, které, oproti kamerám ostatních výrobců, je možné připojit na bezpečnostní centrum Jablotronu. Další výhodou je přenášení záznamu přímo na cloud díky čemuž není nutné pořizovat videorekordér s diskem a předejít tak ztrátě záznamu při zničení zařízení. Nicméně tato služba je v závislosti na počtu kamer a délce záznamu zpoplatněna od 60 do 250 Kč za jednu kameru měsíčně což může být vhodné využít při použití jedné kamery, ale při větším počtu kamer v objektu bude lepší volbou pořízení videorekordéru. Hlavní parametry kamer Jablotron se i přes poměrně vysokou cenu neliší od kamer konkurenčních značek a přidaná hodnota je tak pouze ve výše zmíněných službách.

Z tohoto důvodu byly pro realizaci zvoleny IP kamery od renomovaného výrobce Hikvision, které disponují stejnými parametry za méně než poloviční cenu. Hodnoty hlavních parametrů IP kamer jsou uvedeny v tabulce č. 31.

Tabulka 31 – Srovnání hlavních parametrů IP kamer Jablotron a Hikvision

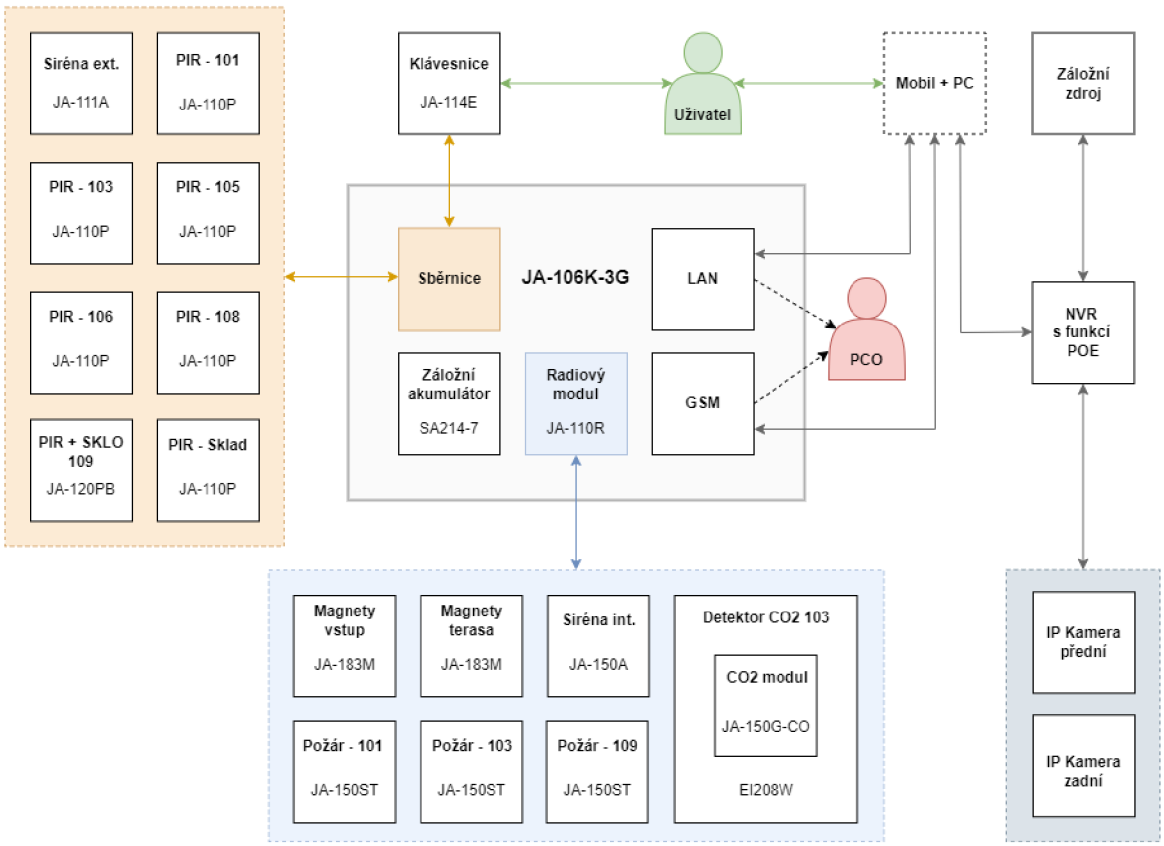
	Jablotron JI-111C	**Hikvision HWI-D121H 2,8mm**
Rozlišení	1920x1080 (Full HD)	1920x1080 (Full HD)
Úhel záběru	115 stupňů	114,8 stupňů
Noční režim	Ano, s IR přísvitem do 30 m	Ano, s IR přísvitem do 30 m
Snímková frekvence	8 fps	25 fps
Komprese videa	H.264, MJPEG	H.264, H.264+, H.265, H.265+, MJPEG
Stupeň krytí	IP67	IP67
Třída prostředí	4. venkovní všeobecné	4. venkovní všeobecné
Cena	5 620 Kč	2 359 Kč

Zdroj: vlastní zpracování (ceny dle elcar.cz a czc.cz ke dni 11.01.2022)

4.5.2 Blokové schéma

Pro lepší orientaci a představu bylo vytvořeno blokové schéma znázorňující komunikační vazby mezi jednotlivými prvky systému. Uprostřed schématu je umístěna ústředna zabezpečovacího systému. Prvky propojené oranžovými vazbami jsou připojeny pomocí drátového vedení přes sběrnici. Modře označená sekce, pak znázorňuje prvky, které komunikují s ústřednou bezdrátově pomocí rádiového modulu. Další komunikační moduly jako jsou LAN a GSM pak umožňují přenášet informace směrem k pultu centrální ochrany a uživateli. Pomocí těchto modulů je také prováděna vzdálená správa systému uživatelem. Uživatel má také přístup k obrazu z kamer pomocí síťového videorekordéru (NVR), který se stará o napájení kamer.

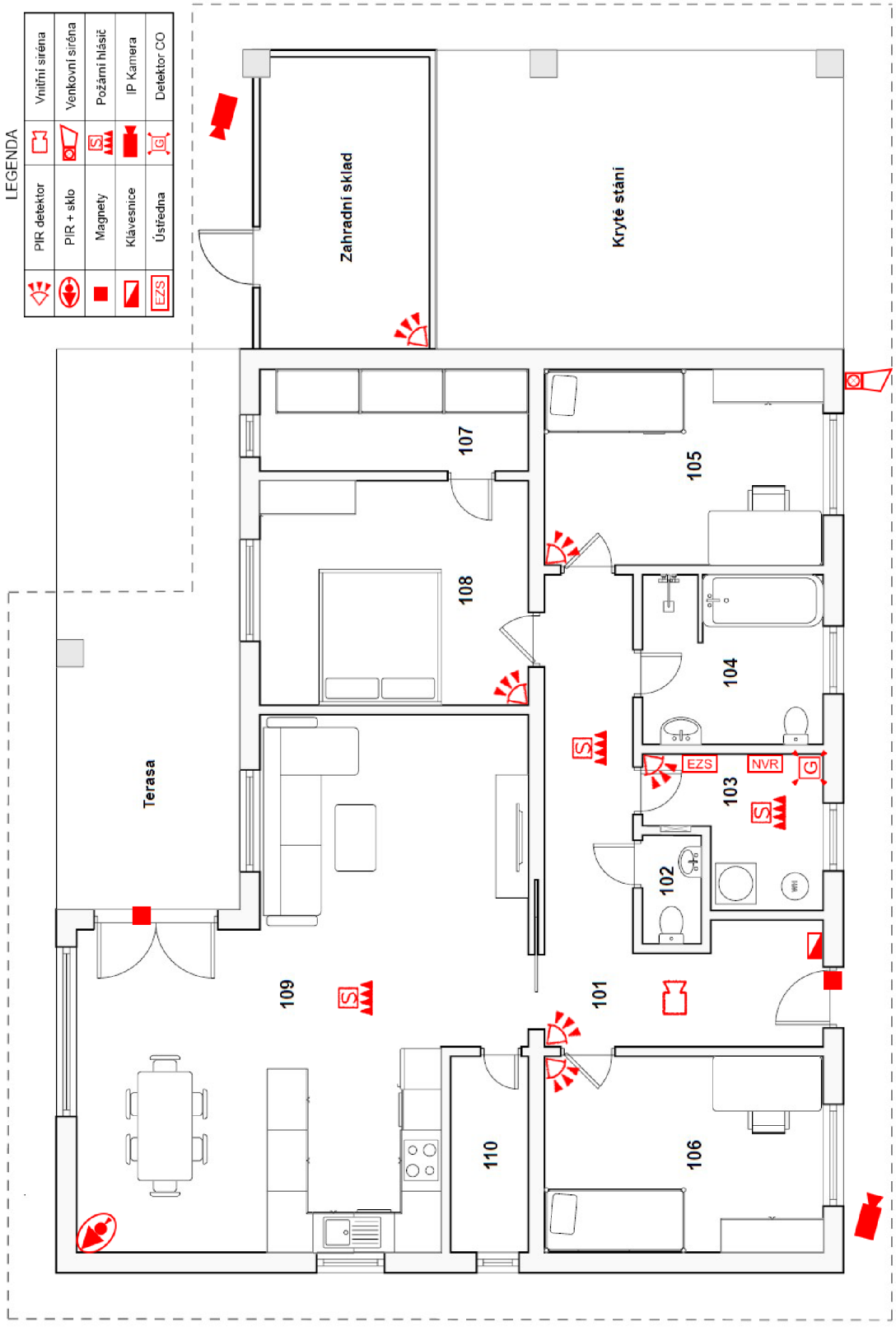
Obrázek 16 – Blokové schéma návrhu



Zdroj: vlastní zpracování

4.5.3 Návrh rozmístění prvků

Obrázek 17 – Návrh rozmístění prvků v půdorysu



Zdroj: vlastní zpracování

Na Obrázku č. 17 je znázorněn půdorys objektu a rozmístění jednotlivých prvků elektronického zabezpečovacího systému. Záznamové zařízení, které bude kromě nahrávání zajišťovat napájení kamer skrze síťový kabel pomocí funkce POE (Power Over Ethernet), bude navíc připojeno na záložní zdroj a spolu s ústřednou zabezpečovacího sytému a budou umístěny v technické místnosti označené jako 103.

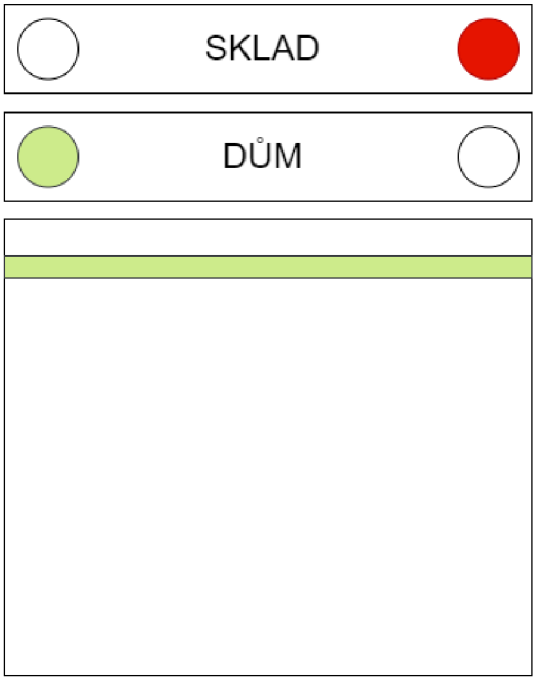
4.5.4 Nastavení systému

Následující kapitola byla zaměřena na nastavení samotného systému. Jednalo se především o rozdělení systému do sekcí, určení zpožděných a okamžitých zón a nastavení nočního režimu.

4.5.4.1 Rozdělení sekcí

Navrhovaný zabezpečovací systém byl rozdělen do dvou samostatně zajistitelných sekcí. Konkrétně se jedná o sekci „DŮM“ a sekci „SKLAD“, z nichž pro každou tuto sekci bude samostatný segment na ovládací klávesnici u vstupu. Sekci „SKLAD“ tvoří pouze samostatný pohybový detektor umístěný v zahradním skladu.

Obrázek 18 – Znázornění segmentů ovládací klávesnice JA-114E



Zdroj: vlastní zpracování

4.5.4.2 Zpožděné a okamžité zóny

Zpožděná zóna, někdy označována jako příchodové zpoždění, byla navrhnuta pro pohybový detektor v chodbě (101) a pro magnetické kontakty na hlavních vchodových dveřích. Toto zpoždění zajišťuje při vstupu do sekce dostatečný čas pro její odjištění. Ostatní detektory budou při detekci spouštět alarm okamžitě.

4.5.4.3 Noční režim

Noční režim byl navrhnut pouze pro sekci „DŮM“. Při aktivaci nočního režimu zůstanou v režimu střežení pouze magnetické kontakty na hlavních a balkónových dveřích. Pohybové detektory uvnitř domu nereagují, aby bylo možné se volně po objektu pohybovat například při cestě na toaletu.

4.5.5 Kapacita záznamového média

Dalším krokem při návrhu pilotního nasazení bylo určení kapacity disku pro kamerový záznam. Dle dostupných informací bylo zjištěno, že velikost 24hodinového záznamu z jedné kamery při střední kvalitě, rozlišení 1920x1080, 25 snímcích za vteřinu, střední aktivitě v obrazu a při využití kompresního formátu H.265+, které využívají právě kamery od společnosti Hikvison, je přibližně 15 GB tedy 0,015 TB. To znamená, že při využití disku s kapacitou 1 TB a 24hodinvého záznamu z dvou kamer, je možné uchovávat 30denní záznam s celkovou velikostí cca 0,9 TB.

4.5.6 Připojení na pult centrální ochrany

Pro zvýšení bezpečnosti a efektivity systému je možné celý systém připojit na pult centrální ochrany. Tuto službu běžně poskytují různé bezpečnostní agentury. Pro tento návrh systému se uvažuje připojení přímo na bezpečnostní centrum Jablotron. Výhodou tohoto bezpečnostní centra je, že dohled realizují přímo bezpečnostní pracovníci společnosti Jablotron ale samotné výjezdy jsou prováděny nejbližší smluvní bezpečnostní agenturou.

Tato služba je nabízena ve třech různých tarifech v závislosti na rozsahu služeb. Výhodou je také, že pro nové instalace systému Jablotron je nejvyšší tarif služby poskytován na 3 měsíce zcela zdarma.

4.5.7 Cenová kalkulace

V tabulce č. 32 byly zaznamenány položky s cenovými údaji, které souvisejí s instalací vybraného bezpečnostního sytému. Ceny prvků zabezpečovacího systému odpovídají cenám hodnotícího kritéria.

Tabulka 32 – Cenová kalkulace elektronického zabezpečovacího systému

Název	Označení	Cena (Kč/ks)	Počet	Celkem (Kč)
Ústředna	JA-106K-3G	12 520	1	**12 520**
Radiový modul	JA-110R	2 933	1	**2 933**
Detektor pohybu	JA-110P	635	6	**3 810**
Detektor pohybu a tříštění skla	JA-120PB	1 461	1	**1 461**
Magnetické kontakty	JA-183M	950	2	**1 900**
Detektor kouře	JA-150ST	1 359	3	**4 077**
Detektor CO	EI208W	1 254	1	**1 254**
Modul pro detektor CO	JA-150G-CO	890	1	**890**
Vnitřní siréna	JA-150A II	1 563	1	**1 563**
Venkovní siréna	JA-111A	2 460	1	**2 460**
Klávesnice	JA-114E	2 090	1	**2 090**
Záložní akumulátor ústředny	SA214-7	515	1	**515**
Baterie pro 183M	CR123A	67	2	**134**
Baterie pro JA-150A II	BAT-3V2-CR2	105	1	**105**
Baterie pro JA-150ST	AA	15	9	**135**
Celkem včetně DPH		**35 847 Kč**		

Zdroj: vlastní zpracování (ceny dle elcar.cz a czc.cz ke dni 11.01.2022)

Tabulka č. 33 obsahuje položky, které se týkají kamerového systému. Kromě samotných IP kamer se jedná o NVR rekordér s funkcí POE, pevný disk s kapacitou 1 TB pro ukládání záznamu, záložní zdroj napájení a náklady na dodatečnou kabeláž pro kamerový systém. Ceny byly určeny na základě cen uvedených na e-shopech CZC.cz a DEK.cz.

Tabulka 33 – Cenová kalkulace kamerového systému

Název	Označení	Cena (Kč/ks)	Počet	Celkem (Kč)
IP kamera	Hikvision HWI-D121H 2,8mm	2 360	2	**4 720**
NVR s funkcí POE	Dahua Imou N14P	1 589	1	**1 589**
Pevný disk 1TB	Seagate SkyHawk, 3,5"	1 099	1	**1 099**
Záložní zdroj	Fortron FSP Nano 800	1 599	1	**1 599**
Dodatečná kabeláž	Solarix CAT5E UTP	7,65	30	**230**
Konektory	RJ45	6	4	**24**
Celkem včetně DPH		**9 261 Kč**		

Zdroj: vlastní zpracování (ceny dle czc.cz a dek.cz ke dni 11.01.2022)

Kalkulace celkové předpokládané ceny za bezpečnostní a kamerový systém včetně odborných prací je uvedena v tabulce č. 34. Sazby za odborné práce v podobě montáže a programování systému byly určeny na základě zjištěných průměrný hodinových sazeb dostupných na internetu a subjektivního odhadu pracnosti.

Tabulka 34 – Kompletní cenová kalkulace

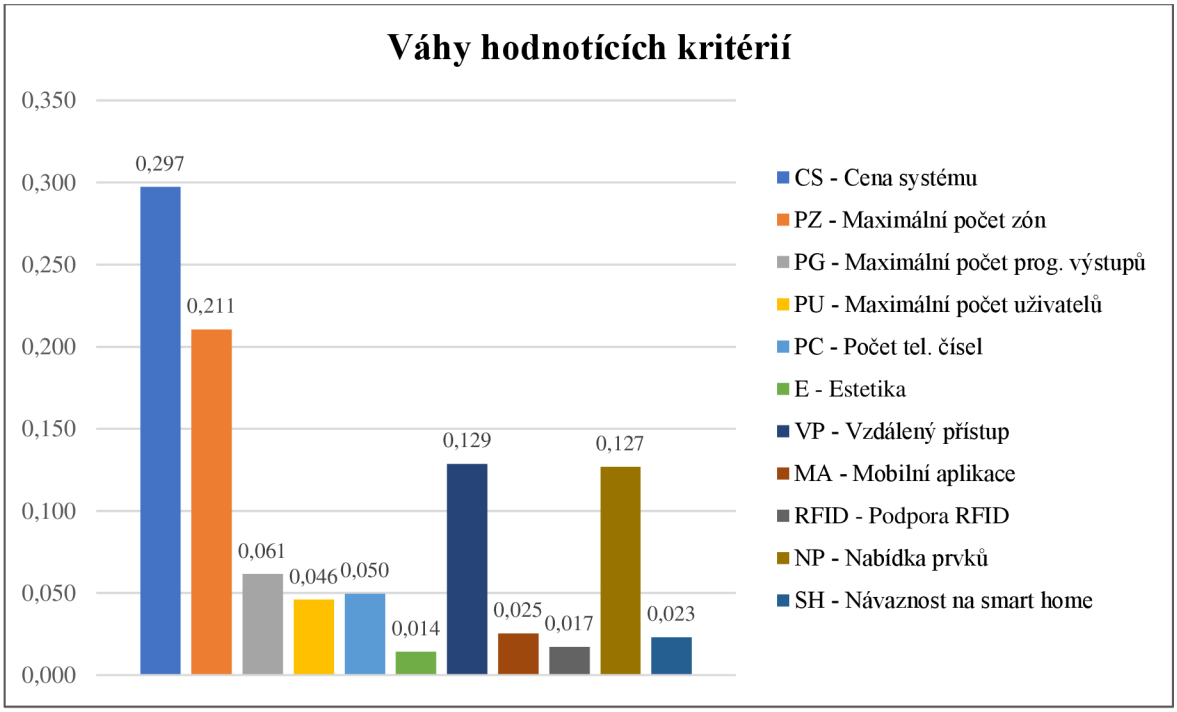
Název	Cena (Kč)	Počet	Celkem (Kč)
Zabezpečovací systém	35 847	1	**35 847**
Kamerový systém	9 261	1	**9 261**
Spojovací materiál	300	1	**300**
Příprava a montáž	400	8	**3 200**
Programování sytému	400	3	**1 200**
Celkem včetně DPH	**49 808 Kč**		

Zdroj: vlastní zpracování

5 Výsledky a diskuse

Výběr elektronické zabezpečovacího systému pomocí vícekriteriální analýzy variant byl prováděn s za pomoci metody TOPSIS a metody váženého součtu. Nedílnou součástí tohoto postupu je také stanovení kritérií a jejich vah, což bylo provedeno pomocí Saatyho metody párového porovnání. Hodnoty vah jednotlivých kritérií jsou zaznamenány v následujícím grafu č. 1.

Graf č. 1 – Váhy hodnotících kritérií



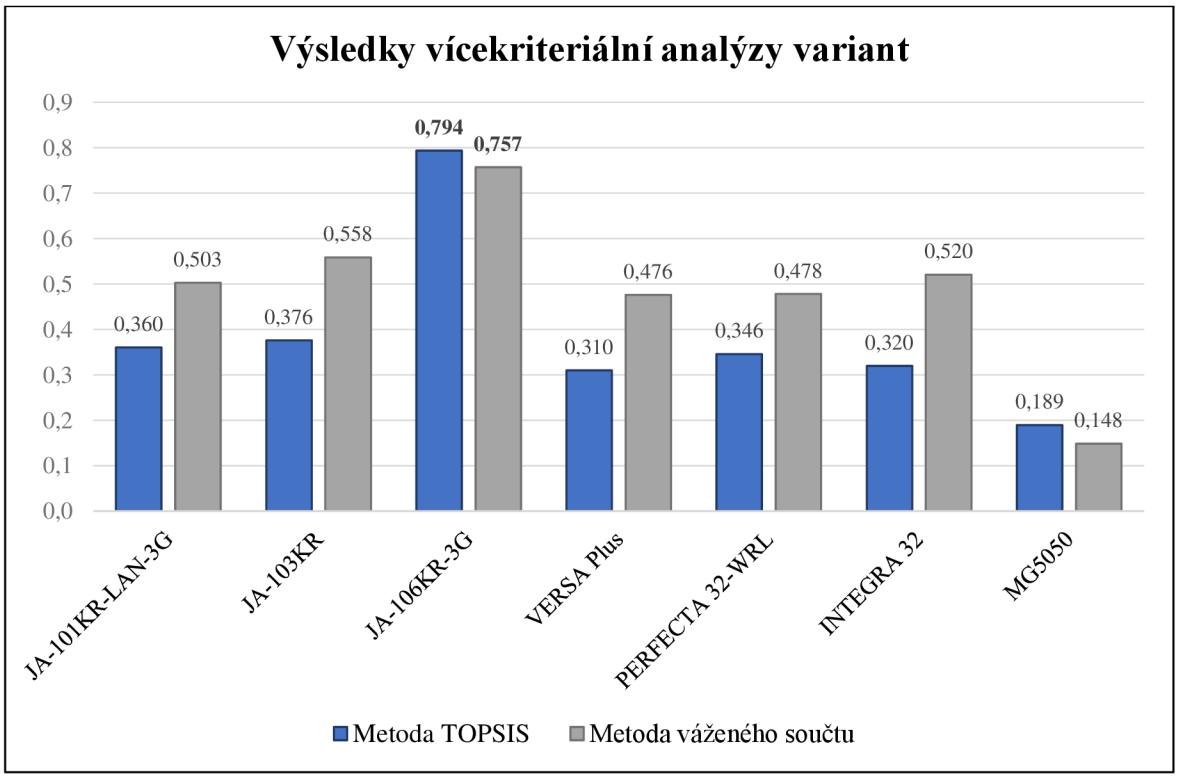
Zdroj: vlastní zpracování

Na základě získaných výsledků, které byly zaznamenány do grafu č. 2, byla určena kompromisní varianta elektronického zabezpečovacího systému pro daný rodinný dům. Konkrétně se jedná o variantu od společnosti Jablotron s ústřednou JA-106KR-3G. Tato varianta dosáhla nejlepších hodnot jak při použití metody TOPSIS, tak také ve výsledcích metody váženého součtu. A to i přes vyšší celkovou cenu, která byla kritériem s nejvyšší váhou. Nicméně v dalších aspektech jako je maximální počet zón, maximální počet programovatelných výstupů či maximální počet uživatelů dosahuje velmi dobrých hodnot. Druhých nejlepších výsledků dosáhl systém Jablotron s ústřednou JA-103KR a na třetím místě to byl systém s ústřednou JA-101KR-LAN-3G. Tyto systémy dopadly v celkové ceně lepé než předchozí JA-106KR-3G, nicméně v ostatních kritériích více či méně zaostávají.

Těsně za produkty společnosti Jablotron, následovaly systémy s ústřednami od polské společnosti Satel. Na čtvrtém místě to byl systém s ústřednou INTEGRA 32, který u metody váženého součtu dosáhl třetích nejlepších hodnot, nicméně metoda TOPSIS tak dobré výsledky neposkytla. Velmi těsně za sebou, na pátém a šestém místě, skončily systémy s ústřednami PERFECTA 32-WRL a VERSA PLUS, které dosáhli u metody váženého součtu velmi podobných hodnot. Systémy Satel dosáhly nejlepších hodnot při hodnocení nabídky prvků, mobilní aplikace a návaznosti systému na chytrou domácnost. Samotný systém s ústřednou PERFECTA 32-WRL pak v celkové ceně dopadl nejlépe ze všech.

Na posledním místě se s větším odstupem umístil systém společnosti Paradox s ústřednou MG5050. Hlavním důvodem je oproti ostatním systémům vyšší cena sytému, chybějící požadované prvky v nabídce společnosti nebo například chybějící podpora RFID prvků. Systém taktéž působí poměrně zastarale, a to nejen co se týče estetiky prvků ale také prostředí a funkcí mobilní aplikace.

Graf č. 2 – Výsledky vícekriteriální analýzy variant



Zdroj: vlastní zpracování

6 Závěr

Tato práce byla tematicky zaměřena na výběr elektronického zabezpečovacího systému pro reálny rodinný dům, a to na základě průzkumu českého trhu, stanovených kritérií a využitím metod vícekriteriální analýzy. Tomu předcházelo studium a analýza informačních zdrojů v rešeršní části práce, kde byla věnována pozornost předpisům a normám v České republice, které souvisejí s návrhem elektronických zabezpečovacích systémů. Dále byly tyto systémy charakterizovány z pohledu architektury, prvků a využívaných technologií.

Praktická část práce byla zaměřena na již zmíněný výběr elektronického zabezpečovacího systému a následný návrh pilotního nasazení vybrané varianty. Nejprve byl popsán objekt, pro který byl systém vybírán, včetně popisu silných a slabých míst, určení stupně zabezpečení a třídy prostředí a popisu prostor s požadavky na jejich zabezpečení. Dalším krokem bylo provedení průzkumu českého trhu s elektronickými zabezpečovacími systémy na základě, kterého byly určeny varianty pro srovnání a hodnotící kritéria včetně vah stanovených pomocí Saatyho metody.

Výběr kompromisní varianty byl proveden pomocí vícekriteriální analýzy variant s využitím metod TOPSIS a metody váženého součtu. Výsledky obou metod byly následně porovnány a na základě výsledků určena kompromisní varianta. Tou se stala varianta od společnosti Jablotron s označením JA-106KR-3G. Vítězná varianta byla dále použita pro návrh pilotního nasazení, kde bylo vytvořeno blokové schéma systému a schéma rozmístění prvků v půdorysu objektu. Také byly určeny kamery pro návrh, velikost použitého záznamového disku a popsáno nastavení systému. Posledním krokem bylo zpracování cenové kalkulace návrhu, kde celková předpokládaná cena činí 49 808 Kč.

Závěry práce mohou být dále využity při reálné instalaci vybraného zabezpečovacího sytému v daném objektu případně při výběru či návrhu nasazení elektronického zabezpečovacího systému pro jiný objekt.

7 Seznam použitých zdrojů

[1] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 3. S.l.: Cricetus, 2006. ISBN 80-902-9382-4.

[2] Poplachové systémy - Pravidla zřizování poplachových zabezpečovacích a tísňových systémů objektů (PZTS) [online]. *JABLOTRON ALARMS*, 21. září 2011 [cit. 2021-8-3]. Dostupné z: https://www.souepl.cz/wp-content/ucitele/hladik/opvk2009/dokumentace%20ke%20z%C5%99%C3%ADzen%C3%AD%20EZS/dokumentace_jablotron.pdf

[3] Krytí IP kód dle ČSN EN 60529 (33 0330). *Elektroprůmysl.cz* [online]. 9. duben 2011 [cit. 2021-8-3]. Dostupné z: https://www.elektroprumysl.cz/legislativa/kryti-ip-kod-dle-csn-en-60529-33-0330

[4] BURDA, Karel. *Základy elektronických zabezpečovacích systémů*. Brno: Akademické nakladatelství CERM, 2017. ISBN 978-80-7204-967-7.

[5] Elektrická zabezpečovací signalizace (EZS). *Zbyněk Fryč - Aret* [online]. [cit. 2021-8-4]. Dostupné z: https://www.aret.info/zabezpecovaci-systemy.html

[6] UHLÁŘ, Jan. *Technická ochrana objektů: Elektronické zabezpečovací systémy II*. Praha: Vydavatelství PA ČR, 2005. ISBN 80-725-1189-0.

[7] Alarm receiving centre, ARC/PCO monitoring. *Fenix international* [online]. FENIX INTERNATIONAL [cit. 2021-8-6]. Dostupné z: http://www.fenix-international.cz/sluzby/alarm-receiving-centre-arc-pco-monitoring.html

[8] Způsoby připojení. *CENTR PCO* [online]. CENTR PCO, c2021 [cit. 2021-8-6]. Dostupné z: https://www.centrpco.cz/index.php/zpusoby-pripojeni

[9] Objektový vysílač GPRS na PCO. *JJTrend* [online]. Náchod: JJTrend s.r.o [cit. 2021-8-8]. Dostupné z: http://www.jjtrend.com/files/dokumenty/popis_-_vysilac_gprs_online.pdf

[10] Satel OPU-4 PW. *Satel.eu* [online]. [cit. 2021-8-8]. Dostupné z: https://www.satel.eu/cz/produktid/605

[11] Pult Centrální Ochrany. *CENTR PCO* [online]. c2021 [cit. 2021-8-10]. Dostupné z: https://www.centrpco.cz/index.php/nase-sluzby/pult-centralni-ochrany

[12] M2C Space – řešení pro vaše komfortní podnikání. *COMPUTERWORLD* [online]. 23.5.2019 [cit. 2021-8-10]. Dostupné z: https://computerworld.cz/securityworld/m2c-space-reseni-pro-vase-komfortni-podnikani-55399

[13] JA-150E Bezdrátová klávesnice s displejem, klávesnicí a RFID čtečkou. *Jablotron* [online]. c2021 [cit. 2021-8-14]. Dostupné z: https://www.jablotron.com/cz/produkt/bezdratova-klavesnice-s-displejem-klavesnici-a-rfid-cteckou-756/

[14] How HC-SR501 PIR Sensor Works & Interface It With Arduino. *Last Minute Engineers* [online]. c2021 [cit. 2021-8-10]. Dostupné z: https://lastminuteengineers.com/pir-sensor-arduino-tutorial/

[15] SLADE, Lauren. What is a Microwave Motion Detector? *Brinkshome.com* [online]. c2021, September 3, 2020 [cit. 2021-8-10]. Dostupné z: https://brinkshome.com/smartcenter/what-is-a-microwave-motion-detector

[16] Microwave and PIR Sensors: A Small Investment For Big Savings. *SmartWorld* [online]. c2020, March 8, 2018 [cit. 2021-8-10]. Dostupné z: https://smart.electronicsforu.com/microwave-pir-motion-sensor/

[17] THOLEN, Celeste. How Does a Glass Break Detector Work? *Safewise.com* [online]. c2021, April 12, 2021 [cit. 2021-8-11]. Dostupné z: https://www.safewise.com/home-security-faq/how-glass-break-detectors-work/

[18] VIGDERMAN, Aliza a Gabe TURNER. How Do Door Sensors Work?: Find out just how these simple little devices make you safer. *Security.org* [online]. c2021 [cit. 2021-8-12]. Dostupné z: https://www.security.org/home-security-systems/door-sensors/

[19] MCGRATH, Jenny. They ain't pretty, but these sensors helped me feel safe in my smart apartment. *DigitalTrends* [online]. c2021, September 7, 2018 [cit. 2021-8-12]. Dostupné z: https://www.digitaltrends.com/home/wink-gocontrol-security-sensor-smart-apartment/

[20] HLADÍK, Drahoslav. Elektronické zabezpečovací systémy a elektronická požární signalizace. *Souepl.cz* [online]. Plzeň: SOUE Plzeň, 2011 [cit. 2021-8-13]. Dostupné z: https://www.souepl.cz/wp-content/uploads/2020/09/elektronické-zabezpečovací-systémy-a-elektronická-požární-signalizace.pdf

[21] CARLSEN, John. What Does a Carbon Monoxide Detector Do and How Does it Work? *Safewise.com* [online]. c2021, August 12, 2021 [cit. 2021-8-13]. Dostupné z: https://www.safewise.com/home-security-faq/carbon-monoxide-detector/

[22] RASTOČNÝ, Jakub. Kamerové systémy (CCTV). *Tvůjalarm.cz* [online]. c2021 [cit. 2021-8-14]. Dostupné z: https://www.tvujalarm.cz/kamerove-systemy-cctv

[23] Jakou technologii vybrat AHD vs. IP. *Nejkam.cz: Specialisté na kamerové systémy* [online]. c2021 [cit. 2021-8-14]. Dostupné z: https://www.nejkam.cz/jak-vybrat/jakou-technologii-vybrat-ahd-vs--ip/

[24] Základní rozdělení kamerových systémů - rozdíly mezi AHD a IP. *SecuriaPro.cz* [online]. c2021, 24.9.2020 [cit. 2021-8-14]. Dostupné z: https://www.securiapro.cz/clanek/zakladni-rozdeleni-kamerovych-systemu/

[25] *Jablotron* [online]. c2021 [cit. 2021-11-04]. Dostupné z: https://www.jablotron.com/cz/

[26] *Satel: Inteligentní zabezpečovací systémy* [online]. c2021 [cit. 2021-11-04]. Dostupné z: https://www.satel.eu/cz/

[27] *Paradox: zabezpečení vašeho majetku* [online]. c2021 [cit. 2021-11-04]. Dostupné z: https://www.paradox.cz/

[28] BROŽOVÁ, Helena a Milan HOUŠKA. *Základní metody operační analýzy*. Praha: Credit, 2002. ISBN 978-80-213-0951-7.

[29] ŠUBRT, Tomáš. *Ekonomicko-matematické metody*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011. ISBN 978-80-7380-345-2.

8 Přílohy

Příloha 1 – Tabulky s výpočtem hodnot pro kritérium cena systému (CS)

Prvek	Počet	JABLOTRON		
Ústředna	1	*JA-101KR-LAN-3G*	*JA-103KR*	*JA-106K-3G*
		12 449 Kč	8 549 Kč	12 520 Kč
GSM modul	1	-	*JA-192Y*	-
		0 Kč	3 499 Kč	0 Kč
LAN modul	1	*součástí ceny*		
		0 Kč	0 Kč	0 Kč
Radiový modul	1	*součástí ceny*		*JA-110R*
		0 Kč	0 Kč	2 933 Kč
PIR	6	*JA-110P*		
		3 810 Kč	3 810 Kč	3 810 Kč
PIR + Sklo	1	*JA-120PB*		
		1 461 Kč	1 461 Kč	1 461 Kč
Magnetické kontakty	2	*JA-183M*		
		1 900 Kč	1 900 Kč	1 900 Kč
Detektor kouře	3	*JA-150ST*		
		4 077 Kč	4 077 Kč	4 077 Kč
Detektor CO	1	*EI208W + modul JA-150G-CO*		
		2 144 Kč	2 144 Kč	2 144 Kč
Vnitřní siréna	1	*JA-150A*		
		1 563 Kč	1 563 Kč	1 563 Kč
Venkovní siréna	1	*JA-111A*		
		2 460 Kč	2 460 Kč	2 460 Kč
Klávesnice	1	*JA-114E*		
		2 090 Kč	2 090 Kč	2 090 Kč
Záložní akumulátor	1	*Alarmguard 2.6Ah*		*Alarmguard 7Ah*
		404 Kč	404 Kč	515 Kč
Baterie pro magnetické kontakty		2x CR123A		
		134 Kč	134 Kč	134 Kč
Baterie pro vnitřní sirénu		1x BAT-3V2-CR2		
		105 Kč	105 Kč	105 Kč
Baterie pro detektory požáru		9x AA		
		135 Kč	135 Kč	135 Kč
Celková cena systému		**32 732 Kč**	**32 331 Kč**	**35 847 Kč**

Zdroj: vlastní zpracování (ceny dle elcar.cz ke dni 11.01.2022)

Prvek	Počet	SATEL		
Ústředna	1	*VERSA Plus*	*PERFECTA 32-WRL*	*INTEGRA 32*
		11 263 Kč	7 079 Kč	3 588 Kč
GSM modul	1	*součástí ceny*		*INT-GSM*
		0 Kč	0 Kč	3 887 Kč
LAN modul	1	*součástí ceny*	*x*	*ETHM-1 Plus*
		0 Kč	x	3 960 Kč
Radiový modul	1	*ACU-280*	*součástí ceny*	*ACU-280*
		2 758 Kč	0 Kč	2 758 Kč
PIR	6	*SLIM-PIR*		
		2 772 Kč	2 772 Kč	2 772 Kč
PIR + Sklo	1	*NAVY*		
		963 Kč	963 Kč	963 Kč
Magnetické kontakty	2	*AXD-200*	*MMD-300*	*AXD-200*
		3 228 Kč	1 764 Kč	3 228 Kč
Detektor kouře	3	*ASD-250*	*MSD-300*	*ASD-250*
		5 355 Kč	4 215 Kč	5 355 Kč
Detektor CO	1	*ACMD-200*		
		1 868 Kč	1 868 Kč	1 868 Kč
Vnitřní siréna	1	*ASP-215 R*		
		2 280 Kč	2 280 Kč	2 280 Kč
Venkovní siréna	1	*SP-4006 R*		
		1 831 Kč	1 831 Kč	1 831 Kč
Klávesnice	1	*VERSA-LCDR-WH*	*PRF-LCD*	*INT-KLFR-WSW*
		3 108 Kč	2 257 Kč	3 939 Kč
Záložní akumulátor	1	*Alarmguard 7Ah*		
		515 Kč	515 Kč	515 Kč
Baterie pro magnetické kontakty		2x CR123A		
		134 Kč	134 Kč	134 Kč
Baterie pro vnitřní sirénu		1x CR123A		
		67 Kč	67 Kč	67 Kč
Baterie pro detektory požáru		3x CR123A		
		201 Kč	201 Kč	201 Kč
Celková cena systému		**36 343 Kč**	**25 946 Kč**	**37 346 Kč**

Zdroj: vlastní zpracování (ceny dle euroalarm.cz ke dni 11.01.2022)

Prvek	Počet	PARADOX		
Ústředna	1	*MG5050*	*SP6000*	*EVO192*
		3 355 Kč	2 683 Kč	4 172 Kč
GSM modul	1	*PCS250*		
		6 991 Kč	6 991 Kč	6 991 Kč
LAN modul	1	*IP 150+*		
		5 346 Kč	5 346 Kč	5 346 Kč
Radiový modul	1	*součástí ceny*	*RTX3*	
		0 Kč	3 054 Kč	3 054 Kč
PIR	6	*NV5M*		
		3 294 Kč	3 294 Kč	3 294 Kč
PIR + Sklo	1	*NV5M + DG457*		
		1 484 Kč	1 484 Kč	1 484 Kč
Magnetické kontakty	2	*DCT2*		
		3 444 Kč	3 444 Kč	3 444 Kč
Detektor kouře	3	*SD360*		
		7 152 Kč	7 152 Kč	7 152 Kč
Detektor CO	1	*WC588P*		
		3 461 Kč	3 461 Kč	3 461 Kč
Vnitřní siréna	1	*SR120*		
		2 637 Kč	2 637 Kč	2 637 Kč
Venkovní siréna	1	*SR230*		
		3 300 Kč	3 300 Kč	3 300 Kč
Klávesnice	1	*K32 LCD+*		*K641R*
		3 423 Kč	3 423 Kč	4 639 Kč
Záložní akumulátor	1	*Alarmguard 7Ah*		
		515 Kč	515 Kč	515 Kč
Baterie pro magnetické kontakty		2x CR2450		
		138 Kč	138 Kč	138 Kč
Baterie pro vnitřní sirénu		3x LR14-C		
		119 Kč	119 Kč	119 Kč
Baterie pro detektory požáru		3x CR123A		
		201 Kč	201 Kč	201 Kč
Celková cena systému		**44 860 Kč**	**47 242 Kč**	**49 947 Kč**

Zdroj: vlastní zpracování (ceny dle alarmmax.cz a abalarm.cz ke dni 11.01.2022)