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

BAKALÁŘSKÁ PRÁCE

VYUŽITÍ ELEKTRICKÝCH ZABEZPEČOVACÍCH SYSTÉMŮ PŘI ZABEZPEČENÍ OBJEKTŮ A VOZIDEL

Autor práce: Stanislav Ptáčník, DiS.

Studijní obor: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: Mgr. Bc. Radovan Sládek

Katedra: Katedra právních oborů a bezpečnostních studií 2018

Prohlašuji, že jsem bakalářskou práci vypracoval (a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci. Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění

.....

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

ABSTRAKT

Bakalářská práce se zaobírá problematikou zabezpečení majetku a motorových vozidel, jejich možnosti a využití. Tato práce se skládá ze dvou částí, první z nich je teoretická, seznamuje čtenáře s úplnými základy zabezpečení, rozdělením jednotlivých druhů dle možnosti využití ochrany. Druhá část je praktická část zaměřená na zkušenosti z praxe, statistiky a cenovou nabídku na konkrétní objekt. Tento objekt je vybrán záměrně, aby ukázal snadnou finanční dostupnost a tím získání velké ochrany svého majetku, a tak ho i bránit jak před samotnou trestnou činností, tak jí i předcházet pomocí zastrašování v podobě různých signálů, to vše upevní a zvýší nedobytnost objektu nebo vozidla a znemožní nebo alespoň ztíží poškození a sníží tak finanční ztráty.

Klíčová slova: Bezpečnost, objekt, střežení, zabezpečen

ABSTRACT

The bachelor thesis deals with issues of property and motor vehicle security, their possibilities and utilization. This thesis consists of two parts, the first of which is theoretical, introduces readers with complete security bases, division of individual species according to the possibility of protection. The second part is a practical part focused on the experience from the practice, the statistics and the pricing on a particular object. This object is deliberately chosen to show easy financial availability and thus to gain a great deal of protection of its property, thus preventing it from both criminal activity itself and preventing it from using intimidation in the form of various signals, all of which will consolidate and increase impracticability of an object or vehicle and obviate or at least reduce the damage and reduce financial losses.

Keywords: Security, Object, Guard, Security

Obsah

Úvod

Elektrický zabezpečovací systém chrání objekt před narušením. Nainstalované snímače pohybu, rozbití skla, snímače zámků ve dveřích apod. sledují objekt a v případě narušení spustí minimálně sirénu.

Elektrické zabezpečovací systémy jsou mnohem levnější než se řada lidí domnívá. Pořizovací cena těch jednodušších systémů je srovnatelná např. s cenou elektrospotřebičů, které se v našich domácnostech běžně nachází. Celková cena však bude závislá na individuálních požadavcích majitele nemovitosti.

Klasické prvky EZS jsou navzájem propojeny kabely, oproti tomu bezdrátové systémy mezi sebou komunikují rádiově a snímače jsou napájeny bateriemi. Klasické EZS jsou zpravidla levnější než ty bezdrátové. Oproti tomu instalace bezdrátového systému se obejde bez zbytečného vrtání a sekání, vlastní instalace je velmi rychlá a levná. Takovýto systém je možné nechat do bytu nainstalovat například pouze po dobu dovolené. Klasické systémy vyžadují větší zásahy při instalaci a hodí se tedy spíše k trvalému užití.

Jaký systém a jaké komponenty zvolíte závisí samozřejmě na individuálních požadavcích na bezpečnost. Alarm může mít různé podoby a formy - od složitých zařízení až po ty jednoduché, ale přesto účinné. Samotný alarm může mít podobu zvonku, sirény nebo se například rozsvítí celý dům. Alarm může být nastaven tak, že se automaticky po jedné, či dvou minutách vypne. Tento čas je však plně dostačující k tomu, aby zalarmoval policii, bezpečnostní agenturu či sousedy. Komfortnější zabezpečovací systémy také signalizují poplach přes GSM bránu přímo majiteli, případně policii. Většina zlodějů při spuštění alarmu zpanikaří a dále se domu nepokouší dostat.

Jednodužší než vloupání řešit, je samozřejmě mu předcházet. Při odchodu z domu lze nastavit zapnutí funkce simulace přítomnosti, kdy se večer náhodně zapne osvětlení, stáhnou se žaluzie apod.

Historie EZS

Historie zabezpečovacích systémů

V rámci historie se lze setkat s rozsáhlou paletou postupně zdokonalujících se systémů zajišťujících bezpečí.

Z nejstarších dob se až do dneška dochoval vynález zámků na klíč a prosté mříže blokující přístup. Tyto dva prosté vynálezy ovšem prošly postupných vývojem, kdy se z mříží stal estetický doplněk oken i dveří a zámek postupně procházel zpřesňováním klíčového mechanismus a miniaturizací.

Prvním výrazným posunem je vynález mechanického kódového mechanismu známého ze starých sejfů a vysoce zabezpečených prostor (například bank). Podobné zámky fungovaly na mechanicky zadané sekvenci čísel či znaků, které odemykaly daný zámek.

Další výrazný posun přichází s objevem elektrického proudu, který se používal jako prevence proti vniknutí (nabití kovové konstrukce elektřinou). Po objevení elektromagnetismu se dokonce na některých místech používají i elektromagnetické zámky, které se otvírají poté, co do nich přestane proudit elektřina – konkrétně na místech, které musí být otevřené v případě, že vypadne elektřina, například únikové východy.

Poslední posun nadchází s příchodem moderní elektroniky, která je brzy zapracována do bezpečnostních systémů. V tomto bodě lze již mluvit o první generaci EZS (Elektrických Zabezpečovacích Systémů).

První generace EZS se vyznačuje tím, že je mechanická a analogická, spíše než optická či chemická digitální. Je poměrně neohrabaná a špatně se integruje do interiérů, které nejsou již dopředu postaveny se záměrem ji v sobě obsahovat. Přes tyto nevýhody je již první generace EZS přijata s mohutnou vlnou pozitivních reakcí od všech lidí, které trápí ochrana svého majetku a blízkých.

Druhou generací se rozumí EZS, které již fungují na principu raných počítačových sítí. Ty zajišťovaly lepší kontrolu a monitorování toho, jak má síť reagovat. Bohužel i tato generaci trpěla nedostatky generace minulé, byť v menší míře díky větší ovladatelnosti a pokračující miniaturizaci.[1]

[1] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. s.15

Dnešní EZS lze definovat jako třetí generaci, která aplikuje základní principy generací minulých na dnešní technologie. Díky tomu je velmi flexibilní, nenápadná, praktická, energeticky i prostorově nenáročná a nabízí excelentní kontrolu a osobní nastavení každému dle jeho potřeb.[2]

[2] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. s 15

1. CÍLE A METODIKA BAKALÁŘSKÉ PRÁCE

Hlavním cílem bakalářské práce je seznámit čtenáře s možnostmi ochrany majetku, zmírnit tak dopady trestného činu, znepříjemnit vandalům jejich úmysl, nebo zapříčinit samotnému aktu trestného činu, kde je navázáno i na statistiky PČR. V neposlední řadě zlepšit podvědomí o finanční náročnosti při základním pořízení zabezpečení v plnohodnotném rozsahu u rodinného domu. Poukázat na způsoby zabezpečení a k čemu jsou určeny, popř. jak je kombinovat pro jejich nejlepší účinnost.

U motorových vozidel pak stejně tak jako u rodinných domů tak i v bytě se zaobíráme možnostmi zabezpečení od těch úplně základních přes ty v nejdokonalejší.

Cílem praktické části je konkrétní cenová nabídka zabezpečení rodinného domu. Nabídka obsahuje cenovou nabídku pro standardní rodinný domek. Dům je umístěn u řeky a ze dvou stran jej obklopují sousedi. Co se bezpečnostních opatření týká, bylo to vhodné řešení, které doplnilo standardní bezpečnostní opatření jakým byl jen plot. Chrání tak objekt před násilným vniknutím do přízemí domu. Je určena převážně pro podobné objekty, které mají celkem jednoduché překonatelné klasické překážky pro případného pachatele. Velkou výhodou tohoto zabezpečení je velká bezpečnostní jistota a tím zdokonalení zabezpečení objektu. Finanční stránka celého projektu není nikterak závratná a nenáročná. Zabezpečit (zakódovat) objekt zvládnou díky jednoduchému provedení i děti nebo se dá dům zajistit i přes mobilní telefon.

.

2. ZABEZPEČOVACÍ SYSTÉMY

Typy bezpečnostních systémů dle způsobu ochrany:

Řešení nastalých problémů ochrany se musí vždy provádět současně. Zabezpečovací systémy se skládají ze 4 základních druhů ochrany:

2.1. Klasická ochrana

2.2. Režimová ochrana

2.3. Fyzická ochrana

2.4. Technická ochrana

2.1. Klasická ochrana

Klasická ochrana je podle vývoje nejstarším typem ochrany. K zajištění příslušných objektů je dobré použít takové mechanické zařízení, které objekt umožní spolehlivě ochránit. Ať už se jedná o různé zábrany, které znemožňují odcizení nebo zničení cenných předmětů zboží, výrobků, případně vytvářejí takové překážky, které pachatelům ztíží dosažení jejich cílů. Tyto zábrany se dobou vyvíjely a to ať už se jednalo o mříže, ploty pancéřové pokladny, kované truhlice, zámky apod. Se vzrůstajícím technických pokrokem se zároveň objevují i prostředky jak tyto zábrany překonávat. Ukazuje se, že tyto zábrany nikdy nebudou 100% dokonalé zabezpečit chráněné objekty. Klasická ochrana je součástí každého zabezpečovacího systému. Někdy může být relativně postačující proti vloupání. Důležitým hlediskem je výdrž odolávání. Z tohoto důvodu se objevuje pojem zdržovací faktor. Jedná se o hodnotu, jak dlouho je daný prostředek schopen čelit jeho překonávání. Proto je dobré prostředky klasické ochrany kombinovat a doplňovat jinými druhy.[3]

2.2. Režimová ochrana

[3] UHLÁŘ Jan, *Technická ochrana objektů, II.díl – Elektrické zabezpečovací systémy II,* Praha: PA ČR, 2005. s. 12

Režimová ochrana je souhrnem ať už administrativních nebo organizačních opatření a postupů sloužících ke zdokonalení ochrany chráněných objektů. Snižuje zranitelnost chráněných zájmů, jako jsou loupeže, výtržnost, vandalismus, přepadení, rozkrádání, drobných krádeží, sabotáží, žhářství, průmyslových sabotáží. Jedná se o specifikace pro vstup, odchod a pohyb zaměstnanců v objektech. Nutností je jejich prosazování a zavádění do každodenní praxe v objektech. Je zapotřebí, aby se tato opatření stala součástí organizace podniku. Režimová opatření dělíme na vnější a vnitřní. Vnější opatření se týkají vstupních a výstupních míst chráněných objektů, neboli míst, kterými se osoby, vozidla do objektu dostávají a opouští ho. Příkladem mohou být brány, vrata, kanalizace, potoky, říčky, lanovky, kabinové šachty, otvory pro příjem paliv a výtahy.

Vnitřní opatření se většinou týká dodržování technických směrnic, režimu pohybu materiálu, skladovacích režimů (způsob výdaje a příjmu materiálu), omezení pohybu vozidel a osob v objektu zvláštního režimu. Zejména v dodržování perfektního stavu ohrazení, osvětlení.

2.3. Fyzická ochrana

Tak jako klasická ochrana je součástí každého systému ochrany. Dá se říci, že je dost podstatná. Obvykle jí provádí hlídači vrátní, strážní, policisté, hlídací služby. Na jejich způsobu provedení závisí spolehlivost všech ostatních druhů ochrany. Právě fyzická ochrana je finančně nejnáročnější. Značné finanční prostředky jsou na tzv. pořizovací náklady na výstroj, výcvik, výzbroj a v neposlední řadě i na platy zaměstnanců. Z tohoto důvodu je důležité tuto ochranu kombinovat s ostatními prostředky ochrany.[4]

2.4. Technická ochrana

Tato ochrana je poměrně nový druh v zabezpečování objektů, Je to dáno tím, že jsou na překonávání nejspolehlivější a nejhůře překonavatelné. Z těchto důvodů značně doplňují dosavadní systémy klasické ochrany. Jejich výhoda spočívá v tom, že rychle reagují na změny způsobené pachatelem, ty pak následně uvedou v činnost zásahovou jednotku, která zamezí pachateli v páchání další trestné činnosti. Leckdy se dokonce povede pachatele dopadnout dokonce před vniknutím

[4] UHLÁŘ Jan, *Technická ochrana objektů, II.díl – Elektrické zabezpečovací systémy II,* Praha: PA ČR, 2005. s. 16

do samotného objektu. Úkolem technické ochrany je zejména oddálit, nebo zcela odolat vniknutí narušitele do střeženého objektu. Úkoly technické ochrany:

- Podporovat klasickou ochranu (zajišťovat a předávat informaci o napadení, urychlení fyzické ochrany k včasnému zásahu)

- Zvyšovat efektivnost fyzické ochrany (obvykle postačí menší zásahová jednotka, která zvládne reagovat na signál o poplachu).

V dnešní době jsou prostředky technické ochrany leckdy pokládány za jediný způsob zabezpečení. Doporučuje se ale kombinovat s napojením objektu na PCO.

Montáž EZS v objektech a zkušební provoz

Montáž EZS v objektech je realizována na základě smlouvy mezi majitelem objektu a provozovatelem EZS. Ten musí mít koncesovanou živnost. Tuto montáž může provádět ať už pracovník PCO nebo osoba oprávněná a přezkoušená na tuto činnost provádět. Před samotnou montáží je důležité provést bezpečnostní posouzení objektu, režimovou studii objektu, topografii střežení. To vše bude posléze sloužit jako podklad pro zpracování EZS a vyhotovení projektové dokumentace.

Další nedílnou součástí by mělo být i mechanické zabezpečení. Na základě projektu je třeba určit i nejvhodnější komponenty EZS.

Po montáži EZS se provede předání EZS k napojení na PCO. Nesmí se opomenout ani režimová studie objektu s domluvenou ostrahou objektu. Další důležitou věcí je poučení a seznámení osob s obsluhou EZS. Obsluha musí být poučená o povinnostech k provozu PCO.[5]

3. Technická ochrana a EZS v objektech

3.1. Pojem EZS, rozdělení podle zón instalace

[5] UHLÁŘ Jan, *Technická ochrana objektů, II.díl – Elektrické zabezpečovací systémy II,* Praha: PA ČR, 2005. s. 25

Čidla EZS je nutné umisťovat tak, aby co nejlépe splňovala svůj účel. Dbáme pokynů výrobce. Umístění a směřování čidel EZS může být pomocí čidel detekováno nebezpečí, rozlišujeme střeženou zónu.

Technická ochrana objektů se dělí na:

a) Plášťová

b) Prostorová

c) Obvodová

d) Předmětová

e) Klíčová

a) Plášťová ochrana

signalizuje narušení pláště objektu. V tomto případě se zabýváme stavebním objektem nebo celým komplexem objektů.

b) Prostorová ochrana

signalizuje nebezpečí v daném chráněném prostoru a to v případě, že pachatel již vnikl do daného objektu a zachytily ho čidla detekující pohyb.

c) Obvodová ochrana

signalizuje narušení obvodu objektu. Obvykle se jedná o venkovní prostředky vyráběné pro tento účel. [6]

d) Předmětová ochrana

signalizuje bezprostřední přítomnost pachatele u chráněného předmětu a to ať už v případě napadení či neoprávněné manipulaci s daným předmětem na daném místě. Typickým příkladem může být trezor.

e) **Klíčová ochrana**

[6] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti ČR, 2014. s. 35

signalizuje narušení klíčových míst (schodiště, haly, chodby). Velkou výhodou je kombinace těchto typů ochrany, pak vytváříme tzv. vícestupňovou ochranu

3.2. Zabezpečovací řetězec EZS

3.2.1. Základní kritéria

Mezi základní kritéria patří:

- Zabezpečení proti záměně (objektová stanice)
- Doba přenosu (poplachu)
- Zabezpečení informací (šifrování zpráv)
- Doba hlášení zprávy (kontrolní spojení)
- Dosažitelnost (navázání spojení) Tyto PCO se od sebe především liší přenosem signálu ze zabezpečených systémů na dispečerskou stanici.

Z pravidla se jedná o přenos:

- Bezdrátový - veřejná rádiová sít (GSM), oba přenosy se využívají v místech, kde není telefonní linka - Vlastní rádiová sít (PCO securiton)
- Linkový - Po telefonních linkách - Po počítačových sítích (internet, intranet)
- Kombinovaný – kombinace předchozích variant, tím zvyšujeme jejich spolehlivost

3.2.2.Čidlo

- neboli senzor, snímač je obecně zdroj informací pro nějaký řídicí systém v užším slova smyslu technické zařízení, které měří určitou fyzikální nebo technickou veličinu a převádí ji na signál, který lze dálkově přenášet a dále zpracovat v měřicích a řídicích systémech. Nejčastěji jde o elektrický signál.[7]

Dělení čidel:

- *Čidla napájena* – se dělí z hlediska toho, zda do zabezpečovaného prostotu vyzařují nebo nevyzařují využitelnou energii na:

[7] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti ČR, 2014. s. 35

- **Aktivní čidla** – při zjišťování charakteristických rysů nebezpečí vytvářejí sví pracovní prostředí aktivním zásahem do okolního prostoru (např. vysíláním elektromagnetického nebo ultrazvukového vlnění), proto je možné tato čidla poměrně snadno detekovat a určovat jejich mrtvé zóny.
- **Pasivní čidla** – reagují pouze na fyzikální změny ve svém okolí např. pasivní infračervené čidlo registruje jen změnu teplotního gradientu. Na rozdíl od aktivních čidel jsou tato obtížně identifikovatelná běžným technickými prostředky.

- *Čidla nenapájená* – vzhledem k úzkému sortimentu čidel nenapájených, používaných v zabezpečovacích systémech, lez tato čidla rozdělit podle aktivační činnosti pouze na:
  - Destrukční čidla . jsou schopna pouze jednorázové funkce – při vyhlášení poplachu dojde k jejich zničení
  - Nedestrukční čidla – u kterých při aktivaci dochází ke vratným změnám

a) Čidla kontaktní

- Kontaktní čidla jsou vždy určitou konstrukční variantou kontaktu, který je vřazen do zabezpečovací smyčky. Pracují na principu přerušení nebo uzavření proudového okruhu zabezpečovací smyčky.
- Kontaktní čidla jsou ekonomicky výhodná, avšak vyžadují poměrně složitou instalaci a z hlediska poskytované ochrany je lze zařadit na nejnižší stupeň.
- Nejčastěji se umisťují tak, aby bylo detekováno otevření dveří nebo oken při oddálení maximálně 30 mm, u vrat a brán pracujících na principu otevření křídel nebo posuvu jejich částí max. 50 mm. Proto jsou také nazývaná jako čidla otevření. [8]

Podle způsobu, kterým se uvádějí v činnost, rozeznáváme obvykle následující druhy kontaktních čidel:

- Mikrospínače

[8] KYNCL, Jaromír. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti ČR, 2014. s.37

- Dveřní a přechodové kontakty
- Smykové kontakty
- Nášlapné kontakty
- Rozpěrné tyče
- Závěsné kontakty
- Koncové spínače
- Magnetické kontakty

b) Čidla destrukční

- Jedná se o skupinu čidel, která odvozují svoji funkci destrukce (rozbití) určité fyzické překážky, kterou musí narušitel překonat. Hlavní odlišností od čidel kontaktních je jejich nezvratná funkce. Znamená to, že po vyvolání poplachu se čidlo musí vyměnit nebo opravit. Destrukční čidla lze rozdělit na:

Poplachové fólie, tapety a skla

- Jsou konstruována na principu přerušení vodivého média, nejčastěji jemného drátku uvnitř zmiňovaného nosiče nebo napařeného vodivého meandru.

Fóliové polepy

- Používají se u křehkých a tříštivých ploch (okna, výkladní skříně, skleněné výplně dveří nebo i tenké neskleněné plochy).
- Jsou to pásky z vodivé hliníkové fólie, které se lepí pomocí lodního laku na skleněnou plochu na okraj rámu.

Vodičové sítě a zátarasy

- Používaly se při budování trezorových místností, depozitářů zvláště cenných předmětů, archivů, dokumentů zvláštní důležitosti apod.
- Vychází se z předpokladu, že takový objekt napadá kvalifikovaný a technicky vybavený pachatel, který ví, že předměty jsou chráněny kvalitním zabezpečovacím systémem.[9]
- Vodičové sítě sestávají ze slabého vodiče, kterým se pokryje celá chráněná stěna. Vodiče se umisťují nepřerušovaně cca 15 mm od sebe. Potom se stěna nahodí cementovou nebo tvrdou omítkou.

[9] LAUCKÝ, Vladimír, DRGA, Rudolf: *Speciální technologie komerční bezpečnosti.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. s. 20

Světlovodné zábranné sítě

- Lze využít k zabezpečení pláště budovy, trezorových místností a všude tam, kde je předpoklad, že pachatel se bude snažit tímto pláštěm probourat.
- Síť je tvořena z tenkého světlovodného kabelu (optických vláken) pro infračervenou oblast. Optická vláka jsou vyrobena z ultračistého skla, obaleného umělou pryskyřicí nebo plasty.[10]

c) Čidla destrukčních projevů

- Další velkou skupinou prvků plášťové ochrany jsou čidla reagující na otřesy (vibrace), které vznikají při pokusech o narušení chráněných ploch. Je vhodné je rozdělit do následujících skupin:

Čidla otřesová s mechanickým měničem

- Fungují na principu setrvačnosti pružně uchyceného závaží, které při dostatečném rozkmitu podložky se vychýlí a tím se rozpojí zabezpečovací smyčka. Citlivost čidla se nastavuje pomocí justačního šroubku.
- Otřesová čidla se umisťují tam, kde předpokládáme, že k narušení klasického zabezpečení dojde destrukcí provázenou vibracemi. Používají se na ochranu skleněných ploch výkladních skříní, skleněné i neskleněné výplně dveří, oken apod.

Čidla otřesová s akusticko-elektrickým měničem

- Instalují se na pevný podklad, jehož vibrace snímají prostřednictvím vhodného akustického měniče a elektricky vyhodnocují charakteristiky přijatého frekvenčního spektra.
- Osazují se podle konstrukčního provedení na riziková místa možného průchodu pláštěm budov, např. zdi, luxfery či rámy dveří a oken.
-

Čidla na ochranu skleněných ploch

- Užívají se převážně ke střežení skleněných ploch pláště zabezpečeného prostoru. Jsou známa jako čidla rozbití skla. Čidla rozbití skla určení pro stupeň

[10] LAUCKÝ, Vladimír, DRGA, Rudolf: *Speciální technologie komerční bezpečnosti.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. s. 26

zabezpečení navíc monitorují funkci senzoru a s ním spojených obvodů pro zpravování signálu.

Mikrofonní kabely

- Podle způsobu snímání poplachové informace můžeme rozdělit do dvou základních skupin na:
    - Mikrofonní kabely s diskrétními snímacími prvky- jsou aplikována na místech předpokládaného průniku pachatele (např. zdi, podlahy, stropy budov, trezorových místností) nebo jednotlivě při předmětové ochraně trezorů apod.
    - Mikrofonní koaxiální kabely s rozloženými snímacími parametry

Mechanické zábrany s detekcí narušení

- Jedná se o elektrický systém s metalickými nebo optickými vlákny, doplňující mechanické zábranné bariéry určené k ochraně objektů a budov či jejich specifických částí (oken, vstupních jednotek,…).

Čidla tlaková akustická (ultrazvuková)

- Používá se jeden typ těchto čidel.
- Jedná se prakticky o citlivý snímač a zesilovač akustických frekvencí radu jednotek, vznikajících při pohybu velkých ploch nebo při změně objemových charakteristik chráněného uzavřeného prostoru (otevřením dveří, destrukcí oken a dveří apod.).[11]

Čidla bariérová

Bariérová čidla aplikována v plášťové ochraně slouží k vytvoření umělé překážky (bariéry) v chráněných prostorách. Jde zejména o:

- **Světelná čidla** – obecně dělíme světelná čidla především podle oblasti elektromagnetického spektra, ve kterém pracují na:
    - Viditelné světelné závory
    - Neviditelné světelné závory

[11] LAUCKÝ, Vladimír, DRGA, Rudolf: *Speciální technologie komerční bezpečnosti.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. s. 30

- **Laserové aktivní záclony**
- **Pasivní a aktivní infračervená čidla** s charakteristickou záclony

Čidla pohybu

- Každý druh čidla pohybu má určité vlastnosti, jež jsou výsledkem úrovně vývoje zpracování signálu a technologie použité daným výrobcem.[12]
- Z hlediska aplikace nabízejí některé typy čidel pohyb další doplňkoví funkce:
    - Dálkové odpojení indikační LED diody, které montážní organizace i uživateli usnadní testování funkce a dosahu čidel v provozu, při servisních zásazích a při pravidelných kontrolách a revizích
    - Odpojení mikrovlnné či ultrazvukové vysílací části čidel, neboť u citlivějších osob může při dlouhodobém pohybu v prostorách s ultrazvukovým nebo mikrovlnným polem dojít ke zdravotním potížím
    - Paměť poplachu a dálkové nulování této paměti, které umožní identifikaci narušení prostoru či poruchu čidla v případech, je-li na jedinou smyčku připojeno více těchto čidel
    - Další doplňkovou funkcí, která oproti předcházejícím přináší vyšší úroveň bezpečnosti, je funkce aktivní ochrany proti zakrytí a přestříkání čidla, tzv. antimasking.

Antimasking

- Čidla s antimaskingem jsou používána v prostorách s vyšším rizikem napadení a veřejně přístupných, kde hrozí nebezpečí sabotáže systému s cílem připravit si objekt ve stavu střežení na vloupání.
- Funkce antimasking u čidel znamená, že při jejich provozu v době střežení i mimo něj je na výstup čidla vyvedena informace o snaze ho vyřadit z činnosti nebo podstatně snížit jeho dosah a citlivost.

[12] LAUCKÝ, Vladimír, DRGA, Rudolf: *Speciální technologie komerční bezpečnosti.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. s. 38

- Vyřazení čidla je v praxi prováděno částečným nebo celým zakrytím, či přestříkáním vhodným aerosolovým přípravkem, který nepropouští infračervení, ultrazvukové nebo mikrovlnné záření a tím je detekční schopnost čidla značně snížena.
- Důvody pro nasazení čidel s funkcí atimasking mohou být:
    - V objektu se strážní (stálou či denní) službou – požadavek okamžitě indikace zakrytí nebo přestříkání čidla
    - V objektu bez strážní služby, nemožnosti uvedení EZS do stavu střežení, je-li některé z čidel vybavené antimaskingem zamaskováno.
    -

3.2.3. Hledisko způsobu předání poplachového signálu

Podle způsobu předání poplachového signálu můžeme dělit elektrické zabezpečovací

systémy na:

a) Lokální

Lokální alarmy určené pro hlídání objektů a jednoduché zabezpečovací zařízení pro ochranu menších objektů a místností. Poplach je vyhlašován pouze akusticky interiérovou nebo exteriérovou sirénou. Poplach není přenášen na mobilní telefon nebo pult centrální ochrany.

Lokální alarmy jsou vhodné pro hlídání zahradních domků, sklepních kójí a všude tam kde způsobí akustický poplach dostatečný rozruch v okolí, aby upozornil na zloděje. Největší výhodou lokálních alarmů je zajímavý poměr cena/výkon a žádné měsíční náklady na telefonní služby operátorů.[13]

b) Autonomní požární hlásiče

Stále oblíbenější autonomní hlásiče požáru zajišťují ochranu vašeho domova proti vzniku požáru nebo úniku jedovatých a hořlavých plynů. Hlavní výhodou autonomních požárních hlásičů je jejich velmi jednoduchá instalace a uvedení do chodu. Obsahují totiž vše nutné k provozu a vyhlášení poplachu již uvnitř hlásiče.

[13] MACEK, Pavel a NOVÁK, František. *Privátní bezpečnostní služby.* Vyd. 1. Praha: Police history, 2005. s 236

Proto stačí pouze vložit baterii nebo je zasunout do zásuvky a upevnit na nejvhodnější místo. Tím je celá instalace a zprovoznění hotové.

Jak fungují:

Autonomní hlásič požáru nepřetržitě testuje okolní vzduch na přítomnost kouře nebo plynu, podle toho na co je určen. Pokud se některý z těchto podnětů objeví v jeho okolí, okamžitě spustí hlasitý poplach pomocí vestavěné sirény a bude houkat, dokud nepomine příčina poplachu.

Pokud je požární hlásič napájen baterií, provádí automaticky její pravidelný test. V případě, že zjistí slábnutí napětí na baterii, začne vydávat zvukový signál většinou ve formě krátkého pípnutí jednou za několik desítek sekund. Upozorní vás tak na nutnost výměny baterie.[14]

c) dálkové - PCO (pulty centralizované ochrany)

PCO neboli pult centrální ochrany značí přímé napojení elektrických monitorovacích systémů a svedení získaných dat elektrickou cestou do jednoho centralizovaného střediska – dohledového centra PCO**.**

Toto spojení umožňuje přenos plného rozsahu událostí generovaných monitorovacími systémy nebo formou předávání stavových signálů. Případně využitím kombinace obou možností.

A) Elektronické zabezpečovací systémy s lokální signalizací

Dojde-li ke stavu „poplach“ spustí se akustická nebo optická signalizace, případně obě. Tato opatření může EZS s lokální signalizací plnit:

- preventivní funkci
- informační funkci :

a)preventivní funkce u tohoto systému není k dispozici žádná služba ani zásahová služba, slouží akustická signalizace k odrazení pachatele k nepokračování napadení objektu případně k upozornění sousedů ke kontaktování policie.

[14] MACEK, Pavel a NOVÁK, František. *Privátní bezpečnostní služby.* Vyd. 1. Praha: Police history, 2005. s. 240

b)informační funkce lokální signalizace je založená k možnosti aby oprávněná osoba nebo náhodná osoba pozorovala páchání trestné činnosti [15]

B). Elektronické zabezpečovací systémy s autonomní signalizací

Případný poplach se objeví u stálé služby, která vyhodnotí zmíněný signál a zákrok.

1) Elektronické zabezpečovací systémy s dálkovou signalizací

Případný poplach se objeví u stálé služby, se kterou má majitel objektu smluvní vztah a vyhodnotí provedení zákroku. Příkladem jsou pulty centralizované ochrany.

2) Elektronické zabezpečovací systémy

Elektronické zabezpečovací systémy je soubor prvků, které jsou schopny dálkově, opticky případně akusticky v daném místě vstup nebo pokus o narušení do střežených objektů nebo prostorů. Každý EZS je složen z pěti prvků, které mají specifické funkce a tvoří zabezpečovací řetězec. [16]

Patří sem:

- čidlo (detektor)
- přenosové prostředky
- ústředna
- signalizační zařízení (PCO)
- doplňková zařízení

a) Čidlo je zařízení, které reaguje na fyzické změny související s narušením prostoru či objektu. Při detekci narušení vysílá čidlo poplachový signál nebo zprávu.

b) Přenosové prostředky zajišťují přenos vstupní informace z ústředny do místa signalizace.

[15] MACEK, Pavel a NOVÁK, František. *Privátní bezpečnostní služby.* Vyd. 1. Praha: Police history, 2005. s. 257
[16] ŘÍHA, Milan, SIEGER, Ladislav a PIKOLA, Pavel. *Bezpečnostní systémy* I. Vyd. 4. Praha: Námořní akademie České republiky, 2011. s 76

c) Ústředna přijímá a zpracovává informace s čidel. Umožnuje ovládání zabezpečovacího systému jeho napájení a přenos informací.

d) Signalizační zařízení zajištuje, vyhlašuje poplach případně výstrahu.

e) Doplňková zařízení napomáhají ovládání systému.

S těmito prvky se v různých obměnách často setkáváme ve vzájemných kombinacích a složitostech. Daná spojení elektronického zabezpečovacího systému jsou průběžně nebo občasně kontrolována. Průběžná kontrola správné funkce EZS je důležitým faktorem ovlivňující zranitelnost systému jako celku. Důležité je výběr kvalitních druhů technických prostředků.

3.3. Obecná pravidla montáže

a) Vnitřní detekce

Detektory pro vnitřní použití jsou určeny pro instalaci uvnitř budov a v místech bez vlivu povětrnostních podmínek. Tomuto způsobu použití odpovídá jejich krytí a odolnost proti falešným poplachům, kde se předpokládá výskyt rušivých vlivů přibližně na úrovni uzavřených vnitřních prostor. Základ nabídky tvoří detektory, které se vyznačují výbornou citlivostí a odolností proti rušení. Nabídka je dále doplněna o kompletní sortiment nejčastěji používaných detektorů (magnetické kontakty, požární detektory, detektor zaplavení, detektory otřesu, tísňové hlásiče). Sortiment umožňuje zajištění prostorové detekce uvnitř objektu, vytvoření plášťové ochrany pomocí magnetů a detektorů tříštění skla, ochrana proti požáru atd.[17]

b) Venkovní detekce

Detektory pro vnější prostředí mají vyšší stupeň krytí proti vlhkosti a způsob jejich konstrukce a metody vyhodnocování musí počítat s výrazně vyšším výskytem rušení než u detektorů pro prostředí vnitřní (přímý vliv slunce, vítr, déšť, mlha). Další odlišností proti vnitřní detekci je plocha, kterou je potřeba hlídat a ta bývá výrazně větší. Z toho důvodu se u rozsáhlejších instalací volí obvodová ochrana detekující průnik do střeženého prostoru s následnou obrazovou kontrolou pomocí prvků CCTV.

[17] ŘÍHA, Milan, SIEGER, Ladislav a PIKOLA, Pavel. *Bezpečnostní systémy* I. Vyd. 4. Praha: Námořní akademie České republiky, 2011. s.76

c) Systém pro menší objekty

Řada ústředen pro menší a střední objekty nabízí až 32 zóny a 2 podsystémy. Ústředny - drátové a bezdrátové mají jednotné programování, filozofii instalace, jednotnou nabídku klávesnic a modulů. [18]Tato jednotnost výrazně usnadňuje práci instalačním firmám, kdy je celá řada ústředen velmi přehledná a pro instalaci i návrh jednoduchá. Instalaci ulehčuje i kompletní sortiment pro drátové a bezdrátové řešení, široká nabídka klávesnic a nabídka moderní komunikace na PCO i uživateli. Komunikace je možná přes IP (internet) nebo GSM (mobil).

d) **Systém pro větší objekty**

Ústředna pro větší a rozsáhlé objekty má 8 podsystémů a 192 zón. Jedná se o plně sběrnicový systém, který nabízí vysoký stupeň variability při vytváření topologie objektu. Čtyř vodičová sběrnice s vysokou odolností proti rušení umožňuje vytvářet i velmi dlouhé větve od základní ústředny a tím je možné instalovat i značně vzdálené zabezpečení v rozsáhlých objektech. Lze použít klasické drátové zóny připojené přes expandéry, detektory a bezdrátové detektory. Uživatel může systém ovládat klasickým způsobem přes klávesnici, pomocí bezdrátových klíčenek, přes čtečku kartami a celou řadou čteček včetně otisků prstu. Kromě zabezpečení je integrovaná nadstavba přístupu, která umožňuje pomocí čteček a karet povolit nebo omezit pohyb osob po objektu. Systém má širokou nabídku pro drátové a bezdrátové řešení, širokou nabídku klávesnic a nabídku moderní komunikace na PCO i uživateli. Komunikace je možná přes IP (internet) nebo GSM (mobil).[19]

e) Systém pro integraci

Velká ústředna určená pro projekty a integraci. Systém dokáže zabezpečit objekty s počtem podsystémů do 32 a počtem zón do 520.

f) Komunikace

Komunikační moduly zajišťují přenos informace o poplachu, nebo stavu systému z hlídaného objektu. Informace se přenáší na bezpečnostní agenturu nebo přímo uživateli. Pro přenos se používá klasická telefonní linka a ta je součástí ústředny. Pro využití přenosu IP (internet - data, email) nebo GSM/GPRS (mobil - SMS,

[18] LAUCKÝ, Vladimír, DRGA, Rudolf: *Speciální technologie komerční bezpečnosti.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. s 48

hlas) se musí systém osadit příslušným modulem. Na bezpečnostní agenturu se používají klasické GSM brány, které běžné formáty 4/2 nebo CID přenášejí přes GSM síť na PCO. Datový přenos na PCO umožňuje nadstavbový přijímač, který zajišťuje příjem zpráv přes internet nebo GPRS. Zpráva uživateli je předávána přes GSM v hlasové podobě nebo jako SMS. Přes internet je uživateli nejčastěji poslán email.

g) Signalizace

Signalizace ve formě sirén slouží pro signalizaci poplachu, kdy akustický výkon je velký a slouží pro maximální možné znepříjemnění pobytu v místnosti, nebo výrazné upozornění na poplach. Signalizace ve formě signálek slouží pro světelné nebo akustické upozornění na vzniklý stav. Upozornění nemá být nepříjemné, ale pouze dostatečně nepřehlédnutelné.

h) Zdroje

Napájecí zdroje slouží pro napájení zabezpečovacích zařízení, posílení základních zdrojů ústředen EZS nebo pro napájení různých elektro zařízení. V nabídce najdete různé typy napájecích zdrojů, od jednoduchých bez zálohování až po zdroje se zálohováním a vyhodnocováním poruchových stavů, které splňují podmínky homologace pro stupeň zabezpečení 3.[20]

ch) Kabely

Stíněné kabely pro slaboproudé instalace v provedení lanko nebo drát. V nabídce najdete kabely s počty žil 4 až 10, s posílenými vodiči, kabely se zdvojenou izolací pro venkovní použití. Kabely mají platnou CPR certifikaci a je na ně vydáno prohlášení o vlastnostech.

i) **Doplňky**

[20] LAUCKÝ, Vladimír, DRGA, Rudolf: *Speciální technologie komerční bezpečnosti.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. s. 83

Široký sortiment doplňkových zařízení pro montáž EZS tvoří elektrické doplňky (propouštěcí zámky, reléové prvky, bleskojistky,…), instalační krabice, řada mechanických doplňků (zejména boxy pro ústředny, klávesnice a přídavné moduly), transformátory a doplňkové zdroje.[21]

Rozvod kabelů pro EZS

Každý výrobce, resp. každá technologie umožňuje jiné způsoby tažení kabelů. Navíc každá montážní firma má svůj "rukopis", kterým kabely rozvádí. Pokud víte, který systém budete instalovat, je vhodné rozvést kabely přesně pro daný systém s využitím systémového kabelu (např. pro Jablotron 100 se využívá systémový kabel CC-01, nebo CC-02 a jiná metoda rozvodu kabelů).

Konvence

- Většina kabelů se táhne od detektoru rovnou do ústředny. Kabely se nikdy **nesmí napojit!** Nepoužívají se ani žádné instalační krabice pro napojení kabelů.
- Kabely se popisují tak, aby bylo zřejmé kam kabel vede a čím má být osazen (PIR obývák, KLAV zádveří atp.)
- Je nutné myslet na to, že na vyvedený kabel bude potřeba přidělat detektor, který se přivrtává. Takže před vyústěním kabelů neděláme žádné „vlny“ smyčky a podobné zákruty, které by zvýšily riziko navrtání kabelu. Kabel se tedy vede nejlépe shora nebo zdola.[22]
- Každé vyústění kabelu ze zdi je cca 1m dlouhé (necháváme si dostatečnou rezervu).

Kabely se musí rozvádět s péčí! Vyhne se tak dodatečným nákladům.

3.4. Jak zabezpečit objekty a prostory

Stále se rozšiřují možnosti přístupu k sofistikovaným technologiím i aktivity osob s protispolečenskými úmysly. Od vandalismu přes záměrné poškozování

[21] LAUCKÝ, Vladimír, DRGA, Rudolf: *Speciální technologie komerční bezpečnosti.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. s 199

materiálů a zařízení až po terorismus. Akce mohou být náhodné, individuální i projektově připravené. Nebezpečí hrozí nejen ze země, ale i ze vzdušného prostoru (rogala, bezpilotní letadla a rádiem naváděná létací zařízení). Ohroženy jsou sklady, sklady nebezpečných látek nebo zařízení infrastruktury. Mnohá složitá a členitá, prostorově rozsáhlá zařízení není prakticky možné zabezpečit ostrahou pomocí živé síly. Pro komplexní ochranu je nutno nasadit i elektronické zabezpečovací systémy. Funkčnost a úspěšnost EZS závisí na kombinaci různých principů a opatření.[23] Pro eliminaci slabin optických čidel (kamerových systémů) se nabízí monitoring zájmového prostoru dálkově ovládanými radarovými čidly nebo perimetrickými detekčními systémy.[24]

A) PRO ZABEZPEČENI OBJEKTŮ A PROSTOR

- monitoring zájmového prostoru malými, levnými a dálkově ovládanými radarovými čidly. Monitoring může být proveden jedním radarem i množinou čidel pracujících selektivně v aktivním nebo pasivním režimu, což prakticky zcela znemožňuje lokalizaci jednotlivého radaru. Díky tomu mohou být radary zapojeny i do vojenských aplikací. K typickým aplikacím patří ostraha okolí průmyslových podniků, zabezpečení letišť, hlídání hraničních pásem, ostraha vojenských objektů, monitorování oblastí se zákazem vstupu nebo průzkum zájmového prostoru. Je to dopplerovský radar se stálou nosnou vlnou (LFM) a nízkým vyzařovacím výkonem. Uplatní se jako elektronický zabezpečovací monitorovací systém, lze jej použít jako průzkumný vojenský prostředek nebo může tvořit nadstavbu stávajícího neradarového (např. optického) systému. Struktura radaru obsahuje plně polovodičový vysílač a sofistikovaný přijímač využívající lineární frekvenční modulace. Vysílač a přijímač používají automatickou digitální kalibraci a diagnostiku. Můžou být použity jako stacionární (k dlouhodobému zabezpečení prostor) i jako mobilní radar instalovaný na dopravním prostředku nebo ve speciální odlehčené verzi nesené 2-3 osobami. Promyšlené signálové zpracování poskytuje maximum informací o sledované oblasti. Propracovaný software umožňuje činnosti v různých módech (předledávání, alarm při detekci v předem definované oblasti, rozpoznávání cílů atd.). V systému je např. možno

[24] LAUCKÝ, Vladimír, DRGA, Rudolf: *Speciální technologie komerční bezpečnosti.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. s. 199

sledovat odrazy s různými dopplerovskými rychlostmi a provádět filtraci zobrazené interference, poskytovat operátorům doplňkový popis cíle (na základě charakteru spektra odrazu) nebo provádět automatizovanou detekci typu cíle (korelací spektra s databází charakteristik známých cílů) a rozhodnout, zda se jedná o cíl typu člověk, vozidlo, vrtulník. Sledovat různé sektory s různým rozlišením, dosahem a rychlostí obnovy informace, např. rychle přehledat celý okolní prostor (360°) a detailněji sledovat místa potenciálního nebezpečí, připojit více radarových čidel a sdružovat jejich výstupy v komplexnější a detailnější informaci. Díky použití principu s nízkým vyzařovacím výkonem a rozprostření spektra je velmi obtížné radar zaměřit - detekovat. [25]

Možnost technického parametru: Kmitočtové pásmo 9 až 10 GHz, modulace LFM-CW, solid-state transmitter Výkon: max. 2 W podle zvoleného rozsahu Pohyb antény: azimut 360° (základní 3 ot/min, zrychlený 6 ot/min, zpomalený 1 ot/min), sektorový (základní 20°/s, zrychlený 35°/s, zpomalený 5°/s) Elevace antény je nastavitelná v rozsahu -10 až +15° Dosah 15 km. Předdefinovatelné dosahy 1,5 km, 3 km, 6 km, 12 km, 24 km Dálková přesnost (RMS) 2 m. Dálkové rozlišení (RMS) 5 m. Úhlová přesnost (RMS) 0,25°. Úhlové rozlišení (RMS) 3°. Napájení ss 20-30 V DC. Příkon 90 W Rozhraní standardní 100 Mbit LAN pro ovládání, diagnostiku a přenos radarové informace Radar lze rozložit na dvě části: stacionární základnu a rotační část s anténou. Výška sestavy 182 cm, hmotnost sestavy 42 kg.

B) PERIMETRICKY DETEKČNI SYSTÉM

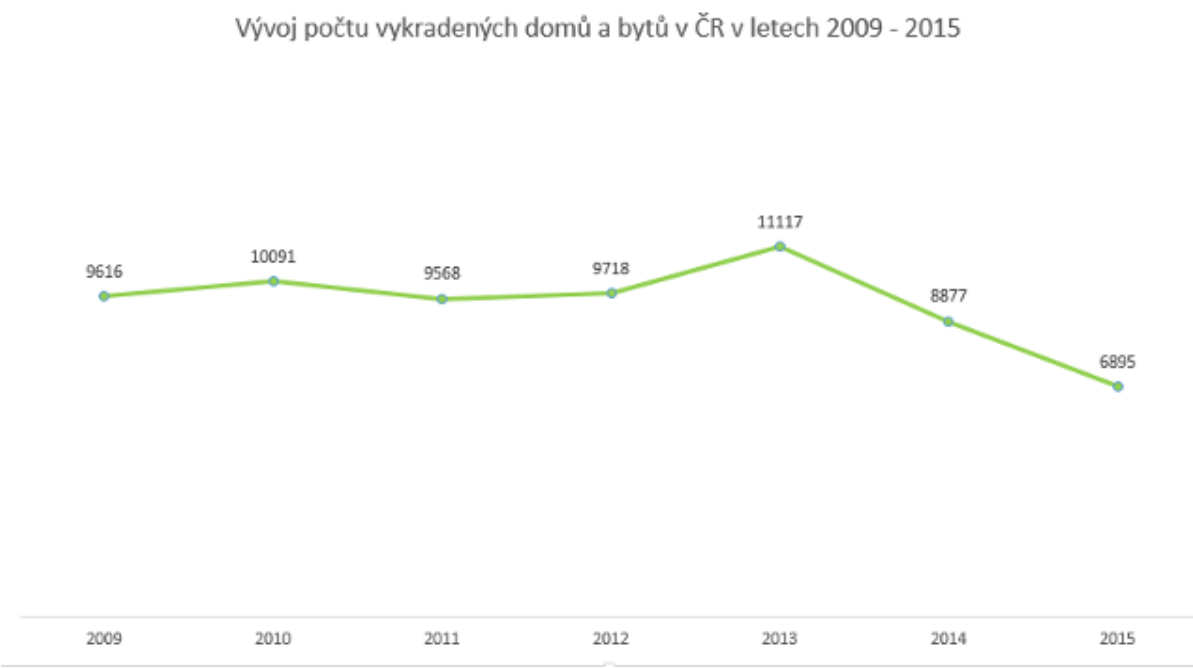
je určen hlavně k uchycení na běžné typy oplocení. Detekuje vibrace způsobené mechanickými podněty (přelezení, prostřižení, nadzvednutí). K detekci využívá senzory s piezoelektrickým prvkem doplněný mikroprocesorovým zpracováním signálu. Použitím diferenční logiky systém výrazně potlačuje plané poplachy. Přesnost detekce systému je s rozlišením na každý jednotlivý detekční senzor PDS, při čemž lze nastavovat nezávisle parametry libovolného senzoru. Typické

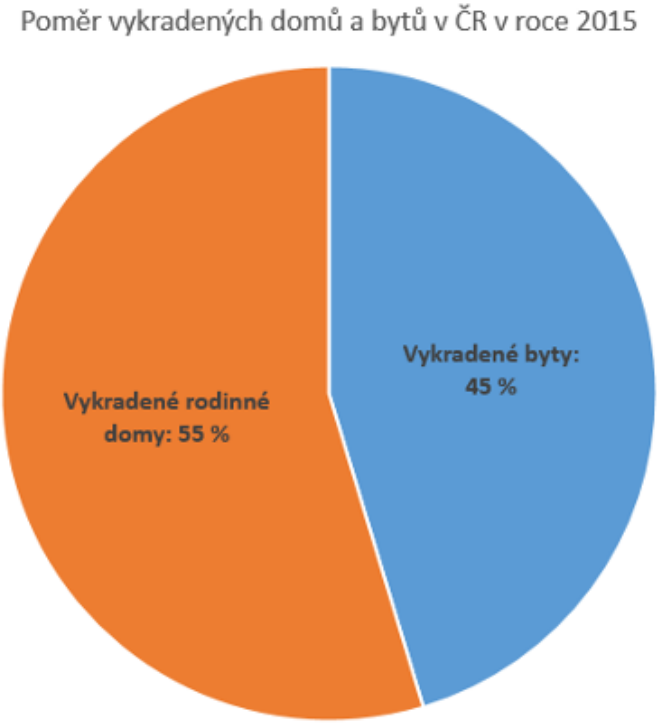
[25] ŘÍHA, Milan, SIEGER, Ladislav a PIKOLA, Pavel. *Bezpečnostní systémy* I. Vyd. 4. Praha: Námořní akademie České republiky, 2011. s. 46

zabezpečení jednou vyhodnocovací jednotkou je linie o délce cca 600 m s rozlišením průniku po 2,5 m. Systém je zcela autonomní zařízení s plně konfigurovatelnými vlastnostmi a s poplachovými výstupy, které umožňují jednoduše připojit systém do všech EZS systémů jako běžný detektor. Větší komfort obsluhy poskytuje jeho připojení k vizualizačnímu programu pro integraci bezpečnostních a řídicích systémů. Je možno zobrazit přímo zabezpečenou oblast graficky, a to i se stavem jednotlivých komponentů zařízení. Systém umí navíc být vybaven vstupními/ výstupními moduly, které umožňují kdekoli na trase perimetru jednoduché připojení jiných zařízení (např. kontaktu) do systému a zároveň ovládání dalších zařízení (např. reflektor).Systémy tvoří vyhodnocovací jednotka (PVJ), ke které jsou datovým kabelem připojeny detekční senzory (PDS), případně vstupně/výstupní moduly (PIO). Kapacita jedné vyhodnocovací jednotky umožňuje připojení až 246 detekčních senzorů PDS a 8 vstupních/výstupních modulů PIO. Systém je již z výroby standardně přednastaven. [26]

Pro využití všech jeho funkcí a k maximálnímu přizpůsobení konkrétní situaci je možno provést pomocí konfiguračního programu individuální nastavení. Lze nastavit např. počet a adresu PDS a PIO modulů, citlivost jednotlivých senzorů podle druhu oplocení a lokality, funkci vazeb programovatelných výstupů a stahovat deník událostí. Systém vyhodnocuje poplach nejenom podle amplitudy vzruchů, ale i podle počtu vzruchů během určité doby a vazby se sousedními detekčními senzory. Pomocí vizualizačních programů lze poplachové či poruchové stavy graficky a textově zobrazit na podkladových půdorysech a lokalizovat tak přehledně jejich umístění. Systémy umožňují i integraci bezpečnostních, CCTV, požárních, přístupových a dalších systémů včetně přehledné vizualizace. Propojení systému s webovým serverem umožňuje zobrazování grafických nebo textových informací přímo v internetových prohlížečích klientské sítě. Taková podobná zařízení vyhovuje požadavkům pro použití v objektech Armády ČR a lze je využít k zabezpečení objektů stupně 4 vysoké riziko. Prostředek lze použít k ochraně utajovaných skutečností do a včetně stupně utajení „PT“.[27]

[26] ŘÍHA, Milan, SIEGER, Ladislav a PIKOLA, Pavel. *Bezpečnostní systémy* I. Vyd. 4. Praha: Námořní akademie České republiky, 2011. s 89





[28]

[28] *Počet vykradených domů a bytů v ČR: Počet vykradených domů a bytů v ČR v letech 2009-2015* [online]. 2015 [cit. 2018-03-25]. Dostupné z: https://www.srovnator.cz/pocet-vykradenych-domu-a-bytu-v-cr

3.5.Jaké systémy dále využít?

- Jednodušší systémy reagují například na násilné otevření oken či dveří. Tyto systémy lze ještě doplnit o senzory reagující na zvuk tříštivého skla, jestli-že dojde k rozbití skleněné tabulky, spustí se alarm.
- Dům lze vybavit vnějším i vnitřním kamerovým systémem. Videokamery mohou být umístěny kdekoliv v okolí a uvnitř domu, nebo pouze na místech, kde je hrozba potencionálního nebezpečí vyšší, např. u dveří, oken či prosklených ploch.
- Kamery mohou okolí monitorovat 24 hodin denně, 7 dní v týdnu, nebo je možné využít systémy, které spustí nahrávání v případě, že senzory zachytí nějaký pohyb. V případě venkovních senzorů pak mohou přímo spustit alarm, nebo lze využít nasimulování vaší přítomnosti.[29]
- Kamerové systémy lze také většinou propojit s jakýmkoliv počítačem, takže můžete sledovat co se během vaší nepřítomnosti v domě děje.
- Zabezpečovací systém může také poskytovat informace o přítomnosti a pohybu osob v jednotlivých místnostech

Při výběru systému je třeba především vycházet z toho, že systém EZS má za úkol chránit váš majetek v řádově vyšších hodnotách. Proto musíte mít jistotu, že se na váš zabezpečovací systém můžete spolehnout. Asi by nikoho nenapadlo kupovat poplachovou ústřednu na tržišti, ale ani nákup v supermarketech není tím nejlepším řešením. Při poptávce systému EZS se ujistěte, zda je výrobek atestován dle normy pro systémy EZS ČSN EN 50131-1 případně i schválen Českou asociací pojišťoven. Pokud systém používá některá rádiová nebo telekomunikační zařízení, potom musí mít zároveň i atest ČTÚ. Tato schválení jsou určitou zárukou kvality EZS a výrazně Vám usnadní jednání s pojišťovnami o akceptaci zabezpečení objektu.[30]

[29] ŘÍHA, Milan, SIEGER, Ladislav a PIKOLA, Pavel. *Bezpečnostní systémy* I. Vyd. 4. Praha: Námořní akademie České republiky, 2011. s 39

3.6. Technické normy

Přehled nejdůležitějších zákonů a norem, které definují způsob návrhu, montáže a servisu slaboproudých technologii, které se používají pro tento typ technologií.

A) Poplachové zabezpečovací a tísňové systémy (PZTS), elektronická zabezpečovací signalizace (EZS)

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

ČSN CLC/TS 50131-7 - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 7: Pokyny pro aplikace[31]

TNI 33 4591-1: část 1 návrh systému PZTS
návrh systému, bezpečnostní posouzení, obsah projektové dokumentace, značky a zkratky pro projektování, vzorové zabezpečení objektu

TNI 33 4591-2: část 2 montáž PZTS
montáž systému – ústředny, napájecí zdroj, ovládací zařízení, detektory, signalizační zařízení, kabeláž

TNI 33 4591-3: část 3 uvedení PZTS do provozu a jeho následný provoz, údržba a servis
prohlídka systému, funkční zkouška, revize elektrického zařízení, proškolení obsluhy, zkušební provoz, pravidelná kontrola a údržba

ČSN EN 50131-6 ed. 2 - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 6: Napájecí zdroje

ČSN EN 50131-3 - Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 3: Ústředny

B) **CCTV** sledovací systémy pro použití v bezpečnostních aplikacích

[31] *Technické normy: Technické normy* [online]. 2018 [cit. 2018-03-25]. Dostupné z: https://seznam.normy.biz/

ČSN EN 50132-1 - Poplachové systémy - CCTV sledovací systémy pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky

ČSN EN 50132-7 ed. 2 - Poplachové systémy - CCTV dohledové systémy pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace

ČSN EN 50132-5-1 - Poplachové systémy - CCTV dohledové systémy pro použití v bezpečnostních aplikacích - Část 5-1: Video přenosy - obecné provozní požadavky

ČSN EN 50132-5-2 - Poplachové systémy - CCTV dohledové systémy pro použití v bezpečnostních aplikacích - Část 5-2: IP video přenosové protokoly

ČSN EN 50132-5-3 - Poplachové systémy - CCTV dohledové systémy pro použití v bezpečnostních aplikacích - Část 5-3: Video přenosy - Analogový a digitální video přenos[32]

C) Poplachové systémy – systémy kontroly vstupů pro použití v bezpečnostních aplikacích (ACCESS)

ČSN EN 60839-11-1 - Poplachové a elektrické bezpečnostní systémy - Část 11-1: Elektrické systémy kontroly vstupu - Požadavky na systém a komponenty

ČSN EN 50133-1- Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky

ČSN EN 50133-2-1 - Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 2-1: Všeobecné požadavky na komponenty

ČSN EN 50133-7 - Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 7: Pokyny pro aplikace

D) Elektronická požární signalizace (EPS)

ZÁKON č. 133/1985 Sb. o požární ochraně ze dne 17. prosince 1985 - Vytváří podmínky pro ochranu života a zdraví před požáry

[32] *Technické normy: Technické normy* [online]. 2018 [cit. 2018-03-25]. Dostupné z: https://seznam.normy.biz/

VYHLÁŠKA 246/2001 Sb. o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci) ze dne 29. června 2001 (určuje množství, druhy a způsob vybavení prostor a zařízení požárně bezpečnostními zařízeními a jeho provozování)

VYHLÁŠKA 23/2008 o technických podmínkách požární ochrany staveb ze dne 29. ledna 2008, doplněna Vyhláška 286/2011 ze 9/2011 (změny) - Technické podmínky pro navrhování, provádění a užívání staveb

ČSN 730875 - Požární bezpečnost staveb - Stanovení podmínek pro navrhování elektronické požární signalizace v rámci požárně bezpečnostního řešení (norma je určena pro projektanty stupně UP (požárně bezpečnostní řešení – systém jaké funkce, jaké rozhraní s jinými PB systémy)[33]

ČSN 342710 „Elektronická požární signalizace - Projektování, montáž, užívání, provoz, kontrola, servis a údržba k tomu Změna Z1 8/2013 (norma je určena pro projektanty DKPS)

ČSN EN 60332 - Zkoušky elektrických a optických kabelů v podmínkách požáru

IEC 60331 - řada norem definuje celistvost obvodu při požáru

B2ca – Klasifikace dle reakce na oheň CPD 2006/751/EC - označení pro kabel:

- S1 - množství kouře při hoření v rozsahu 1 až 3 (1 = nejméně)
- D1 – možnost odkapávání hořících částeček izolace (1 = malé)

VDE 4102-12 - definuje funkční schopnost celého nosného systému (včetně kabelu)

ZP 27/2008 - zkušební předpis PAVUS pro zkoušky funkční schopnosti

ČSN EN 54-1 - Elektrická požární signalizace - Část 1: Úvod

ČSN EN 54-2 - Elektrická požární signalizace - Část 2: Ústředna

[33] *Technické normy: Technické normy* [online]. 2018 [cit. 2018-03-25]. Dostupné z: https://seznam.normy.biz/

ČSN EN 54-3 - Elektrická požární signalizace - Část 3: Požární poplachová zařízení – Sirény

ČSN EN 54-4 - Elektrická požární signalizace - Část 4: Napájecí zdroj

ČSN EN 54-5 - Elektrická požární signalizace - Část 5: Hlásiče teplot - Bodové hlásiče

ČSN EN 54-7 - Elektrická požární signalizace - Část 7: Hlásiče kouře - Hlásiče bodové využívající rozptýleného světla, vysílaného světla a ionizace

ČSN EN 54-10 - Elektrická požární signalizace - Část 10: Hlásiče plamene - Bodové hlásiče

ČSN EN 54-11 - Elektrická požární signalizace - Část 11: Tlačítkové hlásiče

ČSN EN 54-12 - Elektrická požární signalizace - Část 21: Poplachová a poruchová přenosová zařízení[34]

ČSN EN 54-13 - Elektrická požární signalizace - Část 13: Posouzení kompatibility komponentů systému

ČSN EN 54-16 - Elektrická požární signalizace - Část 16: Ústředny pro hlasová výstražná zařízení

ČSN EN 54-17 - Elektrická požární signalizace - Část 17: Izolátory

ČSN EN 54-18 - Elektrická požární signalizace - Část 18: Vstupní/výstupní zařízení

ČSN EN 54-24 - Elektrická požární signalizace - Část 24: Komponenty pro hlasové výstražné systémy – Reproduktory

E) Informační technologie - Univerzální kabelážní systémy (Strukturovaný kabelážní systém)

ČSN EN 50173-1 ed. 3 - Informační technologie - Univerzální kabelážní systémy - Část 1: Všeobecné požadavky

[34] *Technické normy: Technické normy* [online]. 2018 [cit. 2018-03-25]. Dostupné z: https://seznam.normy.biz/

ČSN EN 50173-2 - Informační technologie - Univerzální kabelážní systémy - Část 2: Kancelářské prostory

ČSN EN 50173-3 - Informační technologie - Univerzální kabelážní systémy - Část 3: Průmyslové prostory

ČSN EN 50173-4 - Informační technologie - Univerzální kabelážní systémy - Část 4: Obytné prostory

ČSN EN 50173-5 - Informační technologie - Univerzální kabelážní systémy - Část 5: Datová centra

ČSN EN 50174-1 ed. 2 - Informační technologie - Instalace kabelových rozvodů - Část 1: Specifikace a zabezpečení kvality

ČSN EN 50174-2 ed. 2 - Informační technologie - Instalace kabelových rozvodů - Část 2: Projektová příprava a výstavba v budovách

ČSN EN 50174-3 - Informační technologie - Kabelová vedení - Část 3: Projektová příprava a výstavba vně budov

F) **Poplachové systémy** – Kombinované a integrované systémy (integrace bezpečných systémů)

ČSN CLC/TS 50398 - Poplachové systémy - Kombinované a integrované systémy - Všeobecné požadavky[35]

3.7. PULTY CENTRALIZOVANÉ OCHRANY

Pult centralizované ochrany (dále jen PCO) je zařízení, které je nainstalované v objektech provozovatele nebo ve vybraných objektech umožňujících přenos, příjem a vyhodnocení signálů ze zabezpečených objektů (EZS) a kontrolu a ovládání technického stavu použitých zařízení a přenosových cest. Zmíněné signály můžou být přenášeny jednotnou telekomunikační sítí (JTS), elektrickou rozvodovou sítí, rádiovým přenosem, GSM/GPRS, LAN sítí nebo internetem mají získat k přenosu informací nutných k odvrácení útoků proti objektům chráněných tímto systémem. První centralizace poplachu se začala prosazovat již se vznikem

[35] *Technické normy: Technické normy* [online]. 2018 [cit. 2018-03-25]. Dostupné z: https://seznam.normy.biz/

prvních elektrických zabezpečovacích zařízení (r. 1858). Vynutila si to nezbytnost zřídit poplachový signál do míst trvalé kvalifikované obsluhy, která tyto údaje vyhodnotí a zařídí okamžitě další akci. Obecně je PCO vnímán jako dispečerské zařízení, které zhodnotí poplachové a informační sestavy z EZS zapojené stavby, jež jsou na toto zařízení přenášeny prostřednictvím přenosového objektového zařízení. Aplikace můžou obsahovat skupinu dvou a více dispečerských nebo přidaných zařízení, poskytující přenos souhrnné informace ze vzdáleného objektu na centrální monitorovací pracoviště, se záměrem co nejúčinněji vyhodnocovat všechny dostupné informace a následně přijmout vhodné rozhodnutí a opatření. Jedná se tedy o ústředí, odtud název pult centralizované ochrany, který odpovídá i všem zahraničním pojmenováním, např. anglickému Central Board Station. V tomto centru se soustřeďují všechny poplachové i servisní data ze všech chráněných objektů náležitého území.[36] Kromě dat dosažených ze sdělovacích cest přiřazuje PCO automaticky informace potřebné k zajištění. V minulosti se pouze používali náčrtky chráněných objektů únikových cest a příjezdových tras. Většina pultů centralizované ochrany se dělí na autonomní systémy a systémy integrované do PC.

a) **Autonomní systémy**

Autonomní systémy dokáží plnohodnotného provozu bez dalších přístrojů. Jsou vybaveny displejem a tiskárnou. Jestliže dojde k výpadku napájení, dokáží reagovat bez připojení až na dobu 30 hodin.

b) Systémy integrované do PC

K jejich provozu je nutné, aby fungovaly všechny části počítače. Pakliže dojde k poruše pevného disku, znamená to totální výpadek funkce PCO. U těchto systémů je tedy obtížnější zajistit jejich chod při výpadku elektrického napájení. V současné době je v ČR poměrně velké množství typu PCO. [37]

3.7.1.Střežení

[36] *Statistické přehledy kriminality* [online]. 2015 [cit. 2018-03-25]. Dostupné z: http://www.policie.cz/statistiky-kriminalita.aspx

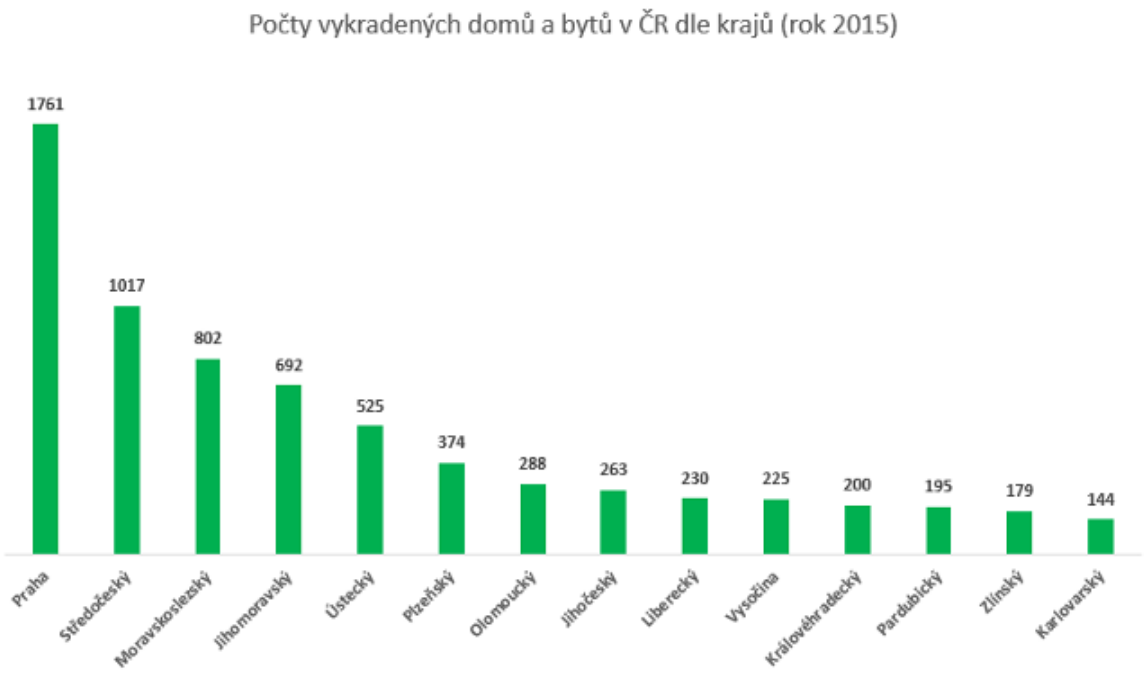
1) V případě přijetí poplachového signálu z objektu poskytovatel kontaktuje zákazníka, případně vysílá zásahové jednotce k fyzickému dohledání objektu, a to podle požadavků sjednaných se zákazníkem při uzavírání smlouvy či později, v průběhu její účinnosti.
2) Poskytovatel nekontaktuje zákazníka v případě, že do jedné (1) minuty po přijetí poplachového signálu z objektu dojde k přijetí zprávy o odjištění objektu. V takovém případě je signál považován za planý poplach a zásahová jednotka neprovádí výjezd.
3) Poskytovatel provádí fyzický zásah pouze na nepohybující se objekty. V případě, že se objekt pohybuje, tísňová linka telefonicky vyrozumí Policii ČR a spolupracuje na dohledání objektu.
4) Zjistí-li poskytovatel v průběhu zásahu, že objekt nelze lokalizovat nebo ten se nachází mimo území České republiky, Informuje zákazníka. Dle požadavku zákazníka poskytovatel předá Policii ČR poslední známou polohu objektu.
5) Zásahová jednotka není oprávněna při zásahu násilně překonat jakoukoliv překážku, zejména nesmí vnikat do uzamčených prostor či vstupovat na soukromé pozemky.
6) Zjistí-li zásahová jednotka osobu, která způsobila vyslání poplachového signálu, vyzve takovou osobu k prokázání totožnosti předložením odpovídajícího dokladu a zaznamená jméno, příjmení, číslo dokladu a datum narození osoby. Pokud zjištěná osoba nebude ochotna prokázat svoji totožnost, zásahová jednotka vyrozumí Policii ČR.
7) V případě zjištění narušení objektu tísňová linka kontaktuje Zákazníka, který rozhodne o dalším postupu. Nepodaří-li se kontaktovat Zákazníka, tísňová linka vyrozumí Policii ČR a zásahová jednotka vyčká do příjezdu Policie ČR.
8) Zásahová jednotka provede podle pokynů tísňové linky zajištění narušeného objektu až do příchodu zákazníka nebo kontaktní osoby event. do příjezdu Policie ČR, a to formou fyzické ostrahy po dobu dvou (2) hodin v ceně výjezdu. Každá další hodina fyzické ostrahy bývá účtován.
9) V případě, že objekt je vizuálně bez fyzického narušení, tísňová linka informuje zákazníka.[38]

[38] [38] *Zabezpečení vozidel* [online]. 2018 [cit. 2018-03-25]. Dostupné z: https://www.lokatory.cz/

10) O každém výjezdu je tísňová linka povinna Informovat zákazníka.
11) Veškerá komunikace mezi tísňovou linkou a systémem, jakožto i komunikace mezi tísňovou linkou a zásahovou jednotkou nebo tísňovou linkou a zákazníkem je monitorována (nahrávána).
12) Zákazník uděluje poskytovateli souhlas ohledně oznamování informací týkajících se narušení objektu Policii ČR či orgánům činným v trestním řízení, zejména za účelem koordinace zásahu Policie ČR.

Poskytování služby jako takové nemůže zabránit případnému spáchání trestného činu třetí osobou či podobnému jednání a v jejich důsledku ani případnému vzniku újmy na straně zákazníka. Poskytovatel nenese odpovědnost za skutečnost, že ke spáchání trestného činu či podobného jednání nebo ke vzniku škody v jejich důsledku dojde.[39]

To jsou tedy možnosti jak zloději znepříjemnit jeho práci. Pokud ke krádeži dojde, máme pojišťovny, aby ztráta nebyla tak bolestivá. Každé sjednané havarijní pojištění v sobě obsahuje i pojištění vozu proti krádeži. V případě krádeže pojišťovna vyplatí cenu obvyklou v době krádeže, po odečtení spoluúčasti (1, 5 nebo 10%).[40]



[39] *Zabezpečení vozidel* [online]. 2018 [cit. 2018-03-25]. Dostupné z: https://www.lokatory.cz/

41

4. Zabezpečení vozidel

4.1. Ochrana Vašeho automobilu

Podle statistik jsou v České republice ukradeny každou hodinu dvě vozidla.

Všichni výrobci používají jako základní ochranu takzvaný imobilizér, což je zjednodušeně řečeno elektrický kód v klíčku, bez nějž se nepovede vůz nastartovat. Zloděj se však dostane do auta, může ho vykrást, může ho odtáhnout. Z toho důvodu se používají i další ochrany proti krádeži:

a) Mechanické zabezpečení

Jedná se o přídavný zámek řadicí páky. Když opouštíme vozidlo, zařadíme zpátečku a zamkneme polohu řadicí páky. Když se zloděj vloupá do vozidla, je mu prakticky znemožněno vozidlo přemístit. Pokud by nastartoval, může odjet pouze couváním, nemůže vůz odtáhnout a je výrazně ztíženo i například natažení vozu na odtahovou službu.

Cena zámku řadicí páky včetně montáže je cca 7 000 Kč dle typu vozu a při této ochraně poskytují pojišťovny slevu na havarijní pojištění.

b) Leptání VIN kódu na skla vozu

vyleptání VIN kód vozu na všechna autoskla.

Ukradenému vozidlu se vždy musí změnit identita, tedy číslo karoserie. Pokud je ale na sklech vyleptán originál kód, musí zloděj všechna skla vyměnit a starých se zbavit. To je pro něj komplikace aproto se takto označeným vozidlům raději vyhne.

Tato ochrana vychází na **800 Kč** [42]

c) Alarm

Téměř jediná možnost, která chrání vůz nejen před ukradnutím, ale i před vykradením vozu. Alarm díky čidlům (kontakty dveří, ale i čidlo rozbití skla, pohybové čidlo) zjistí nestandardní vniknutí do vozu a spustí sirénu. Ta odradí zloděje a

[41] *Zabezpečení vozidel* [online]. 2018 [cit. 2018-03-25]. Dostupné z: https://www.lokatory.cz/

přiláká pozornost okolí, některé alarmy odešlou varovnou SMS majiteli, nebo zabrání nastartování vozu.

Dle sofistikovanosti můžeme alarm včetně montáže pořídit **od 5 000 Kč**[43]

d) Sledování polohy vozu

Dostali jsme se k nejdokonalejším zařízením na trhu, které nám díky GPS přijímači nahlásí aktuální polohu vozu**.**

e) GPS lokátor

Voděodolná přenosná krabička s příjmem GPS signálu umožňující sledování prakticky čehokoli. Informace o poloze můžeme získávat každých 5 minut, nebo je zařízení v pohotovosti a probudí se až při opuštění předem definovaného prostoru.

V případě nestandardního vniknutí do vozu odešle varovnou zprávu SMS a jeho GPS souřadnice. Na základě souřadnic se můžeme podívat do mapy, kde se vůz nachází. Aktuální pozice nám z vozu přijde vždy na základě SMS příkazu.

Cena včetně montáže je cca **6 000 Kč.**

To jsou tedy možnosti jak zloději znepříjemnit jeho práci. Pokud ke krádeži dojde, máme pojišťovny, aby ztráta nebyla tak bolestivá. Každé sjednané havarijní pojištění v sobě obsahuje i pojištění vozu proti krádeži. V případě krádeže pojišťovna vyplatí cenu obvyklou v době krádeže, po odečtení spoluúčasti (1, 5 nebo 10%).

Je také možné domluvit si střežení vozidel jako komplexní službu dle požadavků:

1) **služba pro logistické jednotky, která zahrnuje:**

a) Ol-line monitoring objektu v mapovém podkladu s historií tras
b) Elektronickou knihu jízd pro měsíční vyúčtování

[43] *Zabezpečení vozidel* [online]. 2018 [cit. 2018-03-25]. Dostupné z: https://www.lokatory.cz/

c) Sledování najetých kilometrů, stavu tachometru a spotřeby
d) Správu více objektů a řidičů
e) Komunikaci systému zákazníka s cloudem prostřednictvím bezpečností SIM karty za podmínek platných pro provozování cloudu
f) Administraci bezpečnostní SIM karty a dohled nad její provozuschopností
g) Informační servis o novinkách a změnách v oblasti zabezpečovací techniky a služeb komerční bezpečnosti[44]

2) pro mobilní jednotky je služba pro autoalarmy, která zahrnuje:

a) Možnost zjišťovat stav systému
b) Možnost notifikace vybraných událostí ze systému
c) Sledování historie událostí ze systému
d) Komunikaci systému zákazníka s cloudem prostřednictvím bezpečnostní SIM karty za podmínek platných pro provozování cloudu
e) Administraci bezpečnostní SIM karty a dohled nad její provozuschopností
f) Informační servis o novinkách a změnách v oblasti zabezpečovací techniky a služeb komerční bezpečnosti

3) služba pro autoalarmy

- která oproti službě pro mobilní jednotky zahrnuje:

a) Online monitoring objektu v mapovém podkladu s historii tras
b) Elektrickou knihu jízd pro měsíční vyúčtování
c) Sledování najetých kilometrů, stavu tachometru a spotřeby
d) Správu více objektů a řidičů[45]

4.2. Střežení

Díky mnoha čidlům varuje majitele pomocí sms nejen o vniknutí, ale například i o havárii nebo při pokusu o odtažení. Pohyb vozidla je sledován na pultu centrální ochrany a můžeme se na něj kdykoli podívat na internetu. Díky online datům se

[44] *Rok zabezpečení vozidel*. Praha: Asociace technických bezpečnostních služeb Grémium Alarm, 2010. s. 16
[45] *Zabezpečení vozidel* [online]. 2018 [cit. 2018-03-25]. Dostupné z: https://www.lokatory.cz/

podnikatelům automaticky vypisuje kniha jízd a můžeme vyhodnocovat i jízdní návyky řidičů (dodržování rychlosti, kritické brždění, rychlá akcelerace, spotřeba).

Pořizovací cena je od 7 500 korun s měsíčním paušálem od 200 Kč.

4) služba pro autoalarmy, která oproti službě Vozidlo online zahrnuje:

a) Vyhodnocování signálů přenesených z objektů na tísňovou linku
b) Informování zákazníka při přijetí poplachového signálu z objektu
c) Vyslání výjezdu při přijetí poplachového signálu nebo na vyžádání

d) Bezplatné odvolání výjezdu zásahové jednotky, pokud byl vyvolán nedopatřením

4.3. STATISTIKY

Zjištěno krádeží	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
dvoustopých motorových vozidel	18 011	13 954	12 349	11 647	10 403	10 736	8 720	6 292	4 920	3594
jednostopých motorových vozidel	782	816	760	746	724	905	741	594	427	428
věcí z automobilů	49 430	46 613	39 455	33 230	28 751	30 899	22 976	18 457	14 513	13121
Součástek motorových vozidel	6 450	7 099	8 794	9 967	9 577	10 761	8 641	5 036	3 814	4191

Důvody snížení trestné činnosti na motorových vozidlech v posledních letech

Na snížení kriminality páchané na motorových vozidlech v určitých regionech či lokalitách se podílí i zajištění organizované skupiny pachatelů, kteří svoji trestnou činnost situovali do této lokality. Velkým přínosem v tomto směru je i spolupráce vyšetřovacích týmů kriminalistů jednotlivých krajských ředitelství Policie ČR, přeshraniční spolupráce nebo činnost mezinárodních vyšetřovacích týmů.[46]

[46] *Rok zabezpečení vozidel*. Praha: Asociace technických bezpečnostních služeb Grémium Alarm, 2010. s. 17

Důležitým nástrojem pro odhalení kriminality na motorových vozidlech je i výměna informací z informačních systémů jak České republiky (např. mezi systémem Ministerstva životního prostředí pro vyřazená vozidla a pátrací evidencí Policie ČR), tak mezinárodní výměna informací – především policejních orgánů, ale i orgánů registračních.

K zúžení prostoru pro páchání tohoto druhu kriminality došlo rovněž v souvislosti s některými legislativními změnami (zrušení polopřevodů a společná žádost nového a původního majitele při převodu vozidla, zpřísnění kontrol vozidel a fotodokumentace jejich přítomnosti a identifikačních údajů ve Stanicích technické kontroly a nově i ve Stanicích emisní kontroly, zvýšení nároků na kontrolní techniky, pravidla pro nakládání s vyřazenými vozidly apod.)[47]

K odhalení legalizace odcizených motorových vozidel na některých registračních místech, k odhalení padělaných, pozměněných či zneužitých dokladů či omlazování vozidel přispěla i rozsáhlá kontrolní akce Čistka zaměřená na kontrolu dokladů, zejména k dovozovým vozidlům, na níž se významným způsobem podílela služba cizinecké policie.

Nemalou zásluhu na snížení kriminality, zejména pokud se týká odcizení věcí z automobilů, ale i krádeží vozidel, mají také preventivní aktivity – ať již se jedná o lepší technické zabezpečení vozidel nebo preventivně informační aktivity ze strany Policie ČR. Při prevenci používá Policie ČR i mapy kriminality - do rizikových lokalit a v době zvýšené trestné činnosti je situována hlídková činnost Policie ČR nebo městské policie.

Na druhou stranu se pachatelé specializovaní na motorová vozidla snaží najít i jiné cesty k zajištění finančních zisků - v roce 2016 byl např. zaznamenán nárůst případů daňových deliktů spojených s odpočty DPH, pojišťovacích a úvěrových podvodů, v roce 2017 se organizované skupiny pachatelů ve větší míře zaměřily na krádeže zboží ze zaparkovaných kamionů.

[47] *Krádeže motorových vozidel* [online]. 2017 [cit. 2018-03-25]. Dostupné z: http://www.mvcr.cz/clanek/bezpecnost-a-prevence-kradeze-motorovych-vozidel.aspx

4.4. Nejčastěji zcizená vozidla

K odcizení dochází především u těch typů vozidel, která jsou nejčastěji v provozu – vozidla zn. Škoda (přes 30 % vozového parku osobních automobilů České republiky) a další vozidla koncernu VW (téměř 10 % vozového parku osobních automobilů České republiky). Naopak běžné typy vozidel japonské a korejské výroby a vozidla méně rozšířených továrních značek, např. americké vozy, jsou dle statistických přehledů odcizovány méně.[48]

typ	2011	2012	2013	2014	2015	2016	2017
ŠKODA	4 092	3 926	3809	4 131	2978	2 107	1 511
VW	698	584	566	635	737	634	512
Ford	542	560	414	685	450	361	312
Renault	500	431	353	463	349	244	268
Peugeot	279	326	258	396	260	206	172
AUDI	276	215	191	279	241	261	266
Mercedes	199	239	180	271	232	221	226
BMW	213	226	177	229	201	218	174
Opel	235	228	157	259	195	164	109
Fiat	204	234	150	278	176	141	110
Citroen	139	151	120	194	121	91	94

z toho	2011	2012	2013	2014	2015
Octavia	1 905	2 038	2157	2 311	1682
Fabia	971	823	811	759	509
Felicia	282	273	260	376	291
Superb	117	157	160	195	165
Roomster	51	50	74	59	51
Š - Rapid					49
Yeti	9	21	27	37	39
Š-120	86	87	38	51	25
Š- Favorit	375	275	151	28	19
Š-105	59	42	20	29	8
Š-110	3	4	3	9	8
Š-Forman	145	93	55	10	4

Klesá také počet odcizených starších typů škodovek, které se používaly zejména na náhradní díly.

V roce 2017 také stoupla dosud nízká **objasněnost u krádeží motorových vozidel.** [49]

[48] *Rok zabezpečení vozidel*. Praha: Asociace technických bezpečnostních služeb Grémium Alarm, 2010. s. 13

[49] *Krádeže motorových vozidel* [online]. 2017 [cit. 2018-03-25]. Dostupné z: http://www.mvcr.cz/clanek/bezpecnost-a-prevence-kradeze-motorovych-vozidel.aspx

Objasněnost v %	Dvoustopá vozidla	Jednostopá vozidla	Věci z vozidel	Součástky vozidel
2007	14 %	26 %	8 %	10 %
2008	15 %	26 %	7 %	9 %
2009	16 %	22 %	8 %	10 %
2010	15 %	17 %	8 %	9 %
2011	17 %	16 %	7 %	10 %
2012	16 %	20 %	8 %	10 %
2013	18 %	21 %	8 %	8 %
2014	19 %	25 %	9 %	10 %
2015	20 %	23 %	9 %	10 %
2016	23 %	24 %	12 %	12 %
2017	29 %	30 %	12 %	9 %

4.5. Rizikové faktory

Krádeže motorových vozidel dvoustopých

Mezi nejrizikovější kraje České republiky v roce 2017 patřily:

- hlavní město Praha (v Praze je odcizena 27 % dvoustopých vozidel odcizených v České republice),
- Středočeský kraj (zejména Kladno – 17 % dvoustopých vozidel odcizených ve Středočeském kraji; Mělník, Mladá Boleslav),
- Liberecký kraj (zejména Liberec – 66 % dvoustopých vozidel odcizených v Libereckém kraji),
- Moravskoslezský kraj (zejména Ostrava – 39 % dvoustopých vozidel odcizených v Moravskoslezském kraji; Karviná)
- Ústecký kraj (zejména Děčín – 24 % dvoustopých vozidel odcizených v Ústeckém kraji; Teplice) [50]
- Jihomoravský (zejména Brno-město – 32 % dvoustopých vozidel odcizených v Jihomoravském kraji). Nutno ovšem zdůraznit, že ve všech výše jmenovaných krajích došlo meziročně k poklesu krádeží motorových vozidel dvoustopých (v Praze o 42 %, ve

[50] *Krádeže motorových vozidel* [online]. 2017 [cit. 2018-03-25]. Dostupné z: http://www.mvcr.cz/clanek/bezpecnost-a-prevence-kradeze-motorovych-vozidel.aspx

Středočeském kraji o 20 %, v Moravskoslezském kraji o 7 %, v Ústeckém kraji o 24 % a v Libereckém o 32 %).

Krádeže věcí z automobilů

Mezi nejrizikovější kraje České republiky v roce 2017 patřily:

- hlavní město Praha (v Praze bylo v roce 2017 evidováno 41 % z celkového počtu odcizených věcí z automobilů v České republice),
- Moravskoslezský kraj (17 % z celkového počtu v ČR odcizených věcí z vozidel; z toho nejvíce v Ostravě - 80 % všech věcí odcizených v Moravskoslezském kraji) a
- Jihomoravský kraj (nejvíce v Brně – 65 % všech věcí odcizených v Jihomoravském kraji).[51]

Krádeže součástek automobilů

Mezi nejrizikovější kraje České republiky v roce 2017 patřily:

- hlavní město Praha (v Praze bylo v roce 2017 odcizena 60 % všech odcizených součástek motorových vozidel v České republice),
- Středočeský kraj (nejvíce Praha – venkov jih) a
- Brno – město.

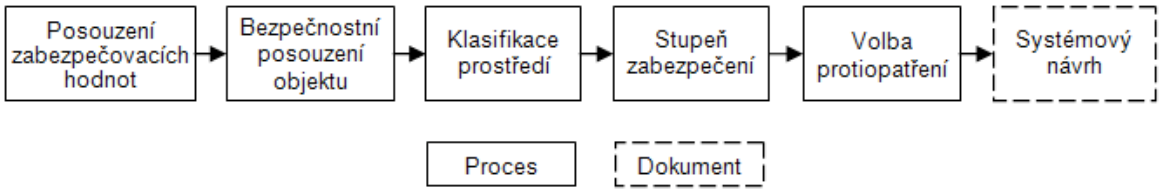
K dalšímu okruhu rizikových faktorů lze zařadit i **chování vlastníků, resp. provozovatelů vozidel**. Jde například o opomenutí uzamčení vozidla, ponechání klíčků ve vozidle nebo ponechání věcí ve vozidle na viditelném místě (mobilní telefony, notebooky, navigace, autorádia, oděvy, zavazadla), lyže či jízdní kola na střeše vozidla apod.

[51] *Krádeže motorových vozidel* [online]. 2017 [cit. 2018-03-25]. Dostupné z: http://www.mvcr.cz/clanek/bezpecnost-a-prevence-kradeze-motorovych-vozidel.aspx

5. Návrh EZS

Návrh systému EZS je proces, při němž se stanovuje rozsah systému, stupeň zabezpečení, komponenty odpovídajícího stupně zabezpečení, volby protiopatření, třídy prostředí. Při tomto procesu dochází k výběru vhodné ústředny a způsobu provedení kabeláže, ke stanovení počtu a typu detektorů, typu ovládacích a indikačních zařízení a dalších doplňkových zařízení. Návrh systému EZS většinou také slouží pro přibližný odhad ceny navrhovaného systému.[52]

Na následujícím obrázku je znázorněn sled událostí při návrhu EZS.



5.1. Posouzení zabezpečovacích hodnot

Při stanovení bezpečnostního stupně EZS objektu je nutné brát v úvahu tyto faktory:

- Druh majetku, snadnost zpeněžení, atraktivnost pro pachatele
- Hodnota majetku, maximální hodnota ztráty, výdaje související se ztrátou, osobní ztráty[53]
- Objem nebo velikost majetku, snadnost krádeže a transportu
- Historie krádeží, počet předešlých krádeží ve střežených objektech, způsob vloupání při předchozích krádežích
- Nebezpečí pro okolní prostředí, zneužití střeženého majetku
- Poškození vandalizmem na střeženém majetku, riziko žhářství

5.2. Bezpečnostní posouzení objektu

Prověrka lokality budovy

Při systémovém posuzování hlavních rizik projektu EZS bude při jeho zpracování hlavním určujícím faktorem struktura střežených objektů.

Je nutné posoudit následující faktory:

- Konstrukce stěn, střech, podlah, sklepení,

[52] JELÍNEK, Josef. *Jak zabezpečit byt, dům, chatu, automobil*. Vyd. 1. Praha: Grada, 2000. s .66
[53] JELÍNEK, Josef. *Jak zabezpečit byt, dům, chatu, automobil*. Vyd. 1. Praha: Grada, 2000. s .69

• Otevírané části dveří, oken, střešních světlíků, ventilačních kanálů, ostatních otevíraných částí pláště budovy,

• Provoz (veřejná budova, přítomnost ostrahy),

• Lokalita (míra kriminality, okolní budovy, rychlost reakce na signalizaci, informace o sousedních objektech),

• Stávající zabezpečení (kvalita a rozsah),

• Historie krádeží (počet předchozích krádeží, způsoby vloupání),

• Místní legislativy, předpisy (bezpečnostní požadavky, požární předpisy, konstrukce budovy),[54]

• Poloha střeženého objektu (městská zástavba, venkov).

5.3. Faktory mající původ uvnitř střežených objektů

Uvnitř střežených objektů existuje řada faktorů, které mohou ovlivnit správnou funkci EZS. Při volbě typu zařízení, zvláště čidel a jejich umístění, je nutno tyto faktory posoudit.

Faktory, které mají původ uvnitř střežených objektů lze považovat za ovlivnitelné uživatelem objektu. Pokud by dané podmínky mohly negativně ovlivnit provoz nějakého komponentu systému nebo celý systém, je nutno tyto podmínky změnit. *Mezi takové podmínky patří:*

• Vodovodní potrubí (vliv pohybu vody v plastových potrubích na MW čidla),

• Tepelné, ventilační a klimatizační systémy (vliv turbulence na US čidla),

• Závěsné tabule a ostatní předměty (vliv pohyblivých částí na čidla),

• Výtahy (vliv vibrací způsobené výtahy a strojními zařízeními na čidla),

• Světla (vliv zářivek na MW čidla, vliv halogenových světel na PIR čidla),

• Elektromagnetické rušení (všechna elektrická zařízení mohou být zdrojem elektromagnetického rušení, které může ovlivnit provoz zařízení EZS – běžné jsou mobilní telefony),

• Vnější zvuky (vlivy zařízení generující zvuky ve stejném frekvenčním rozsahu na US čidla – telefonní zvonky, letadla, kompresory),

• Domácí zvířata a škůdci (vliv na čidla pohybu i otřesová čidla),

• Průvan (vliv proudění vzduchu na PIR a US čidla – vznikají v důsledku

[54] JELÍNEK, Josef. *Jak zabezpečit byt, dům, chatu, automobil*. Vyd. 1. Praha: Grada, 2000. s.55

špatně utěsněných otvorů),

• Uspořádání skladových předmětů (možnost zastínění průzoru čidel, možnost přemisťování skladovaných předmětů, zařízení interiéru v průzoru čidla),

• Struktura střežených objektů (při volbě umístění čidel nutnost posoudit strukturu střežených objektů a stav a usazení dveří a oken),[55]

• Speciální pozornost (nutné odborné posouzení – hořlaviny, výbušniny, skelné podklady).

5.4. Faktory mající původ vně střežených objektů

Také vně střežených objektů se vyskytuje řada faktorů, které mohou ovlivnit provoz EZS. Rovněž tyto faktory je nutné posoudit při volbě typů zařízení a při rozmísťování těchto zařízení.[56]

Za ovlivňující faktory mimo střežené objekty se považují takové, které uživatel nemůže ovlivnit. Pokud by dané podmínky mohly negativně ovlivnit provoz nějakého komponentu systému nebo celý systém, je nutno tyto podmínky změnit. Mezi takové podmínky patří*:*

• Dlouhodobé faktory (silnice, železnice, podzemní dopravní systémy, letecká doprava, parkoviště podzemní i nadzemní, zemětřesení a chvění půdy),

• Krátkodobé faktory (vliv konstrukce sousedících budov),

• Vlivy počasí (místa s výskytem silných větrů a dešťů, časté blesky),

• Vysokofrekvenční rušení (vliv blízkosti stožárů vysílačů, civilních antén, vojenských radarů, antén amatérských vysílačů na bezdrátové EZS),

• Sousední objekty (vliv činností, procesů a zařízení provozovaným nebo přepravovaným v těchto objektech na střežený objekt – vibrace, zařízení generující vysoké hladiny elektromagnetického rušení),

• Vlivy klimatických podmínek (nutné použít pouze zařízení vhodná pro dané klimatické podmínky – teplotní rozsah, relativní vlhkost nebo vlhko),

• Ostatní podmínky (aktivity v okolí).

[55] JELÍNEK, Josef. *Jak zabezpečit byt, dům, chatu, automobil*. Vyd. 1. Praha: Grada, 2000. s.57
[56] UHLÁŘ Jan, *Technická ochrana objektů, II.díl – Elektrické zabezpečovací systémy II,* Praha: PA ČR, 2005 .s. 99

5.5. Klasifikace prostředí pro zařízení

Při výběru je nutné zvážit prostředí, ve kterém budou jednotlivé komponenty systému EZS umístěny a ve kterém budou schopny správného a spolehlivého provozu. Toto rozdělení je znázorněno v následující tabulce.[57]

5.6. Stupeň zabezpečení

Ke stanovení stupně zabezpečení je zapotřebí posouzení zabezpečovacích hodnot a bezpečnostního posouzení objektu. Toto posouzení se provádí vždy za účasti zákazníka, případně za účasti dalších zainteresovaných subjektů (policie, bezpečnostní agentura, pojišťovna). Orgánem, který toto posouzení provádí, bývá zpravidla zástupce organizace, která zajišťuje návrh systému EZS. Rozdělení stupňů zabezpečení je znázorněno v následující tabulce.

Ve všech stupních zabezpečení termín útočník zahrnuje i ostatní typy ohrožení (například loupežné přepadení nebo vyhrožování fyzickým násilím), což může ovlivnit návrh EZS.

5.7. Volba protiopatření (volba čidel)

Pro každý stupeň zabezpečení je charakteristická konkrétní volba protiopatření. Pomůcka pro správný výběr protiopatření je znázorněna v následující tabulce.

Detekce otevření je nutné u okna nebo jiného otevíratelného prostoru, jehož rozměry jsou větší než 900cm2 a jenže je umístěn ve vzdálenosti menší než 5,5m ve všech směrech od míst, z nichž by bylo možné vniknout do střeženého prostoru (balkon, lodžie, střecha, otevřený terén). Je realizováno většinou magnetickým či mechanickým kontaktem.
Detekce průnikem je nutná u otvorů větších než 900cm2. Je realizováno většinou detektorem tříštění skla GBS nebo otřesovým čidlem.
U *nástrahy* je nutná detekce průchodu útočníka. Je realizováno většinou detektorem pohybu.
Potřeba speciální detekce je dána specifiky chráněných aktiv, kterými mohou být například umělecká díla.

[57] JELÍNEK, Josef. *Jak zabezpečit byt, dům, chatu, automobil*. Vyd. 1. Praha: Grada, 2000. s. 69

5.7. Systémový návrh

Je to dokument, který je výsledkem návrhu systému EZS. Zpracovává se jako podklad pro zadavatele nebo kupujícího. Tento návrh obsahuje všechny informace, podle kterých se zadavatel nebo kupující může přesvědčit o vhodnosti vybraného typu EZS pro danou aplikaci, účel a lokalitu.

V tomto dokumentu musí být uvedeny následující informace:

- Údaje o zákazníkovi (údaje nutné pro identifikaci zákazníka),
- Údaje o střežených objektech (název a adresa, popis – typ konstrukce, účel objektu – např. rodinný dům),
- Stupeň zabezpečení navrženého EZS,
- Třída prostředí každého komponentu EZS,
- Přehled komponentů (přehled typů, rozmístění, očekávané pokrytí),
- Konfigurace systému (programování smyček),
- Ohlašování (typ a umístění signalizačních zařízení, zařízení dálkového přenosu poplachu a název PCO),
- Legislativa (údaje o shodě komponentů systému s požadavky místní nebo národní legislativy),
- Normy (údaje o shodě prvků systému s požadavky národní nebo evr. normy),
- Další předpisy (podrobnosti o shodě komponentů systému s dalšími předpisy – směrnice, kódy publikované pojišťovnami nebo příslušnými inspektoráty),
- Certifikace (údaje o uplatnění nároku na certifikaci prvků i EZS systémů),
- Odezva (plánované odezvy na signalizaci poplachů nebo poruch – PČR, majitel, bezpečnostní agentura),[58]
- Údržba a Opravy (údaje o plánované údržbě EZS a firmě poskytující servis).

5.8. Z praxe

Při instalaci a užívání Elektronických Zabezpečovacích Systémů (EZS) vás může potkat množství nečekaných situací, které by ani sebelepší analytik ne-

[58] ŘÍHA, Milan, SIEGER, Ladislav a PIKOLA, Pavel. *Bezpečnostní systémy* I. Vyd. 4. Praha: Námořní akademie České republiky, 2011. s. 83

předpokládal a prostě a jednoduše by ho ani ve snu nenapadly. Tyto nepříjemnosti a problémy čítají vše možné – od rozmarů přírody až po zlomyslné sousedy, kteří vám z nějakého prapodivného důvodu závidí dokonce i váš EZS.

Jako první můžeme uvést kuriózní zkušenosti s používáním EZS v odlehlých lokalitách – například chata v horách. Může se například stát, že při nedostatečném zakrytí kabeláže vašeho EZS si místní divoká zvěř splete vaše drátování s nějakou místní rostlinou – především v zimě či po tmě. Poté může nastat poměrně komická situace, kdy uprostřed silvestrovské noci vyrazíte velkou rychlostí na vaši chatu, protože systém hlásí vloupání a po příjezdu objevíte přehryzaný drát od vaší kamery, střežící hlavní přístupovou cestu.

Podobně nepříjemná situace může vzniknout i v případě, že máte domácí mazlíčky, kteří rádi ohryzávají (především králíci) nebo škrábou všemožné části vašeho pokoje. I v tomto případě doporučujeme dostatečně zakrýt všechnu vaši kabeláž, aby náhodou nedošlo k poškození vašeho EZS díky hloupé náhodě.

Další nepříjemné poškození vašeho EZS může způsobit lidská hloupost a závist. Asi každý se někdy setkal se sousedem, který postával v okně nebo u plotu a závistivě pokukoval po vašich životních úspěších – ať už to bylo nové auto, krásný dům nebo váš skvělý EZS. V takových případech se může stát, že podobná nevraživost přeroste do přímo nelidských rozměrů a vás žárlivý soused (či někdo jiný) se rozhodne, že se vám daří až příliš.

Vaše auto bude pravděpodobně v garáži, vašeho domu se podobný vandal ani nedováží dotknout, protože je chráněn vašim EZS. Ale co samotný zabezpečovací systém, speciálně pokud máte venkovní kamery?

Pro podobný případ pro vás mámě několik typů a triků jak se vyvarovat podobným nepříjemnostem:

1. Vandal si dvakrát rozmyslí, jestli zkusí poškodit váš EZS, pokud bude vaše drátování dobře zakryto a vaše případné kamery budou umístěny na špatně přístupných místech.

2. Navíc je velmi efektivní vaše kamery obložit bariérou z plexiskla či jiného, podobného materiálu. Díky tomu znemožníte poškození například vrženým kamenem.

3. Dále je velice efektivní jakékoliv senzory umísťovat tak, aby měli co nejmenší slepý úhel a aby byly schopny pokrýt co největší prostor.

4. Pokud se přece jen nemůžete vyvarovat slepých úhlů, tak vždycky můžete přistoupit k systému kamer, které se hlídají navzájem. To znamená, že minimálně v rohu každého záběru z libovolné kamery je pokryt slepý úhel aspoň jedné další kamery.

5. Nakonec pak ještě můžete umístit skryté kamery na neobvyklá místa, které budou mít za cíl snímat prostor, v kterém jsou umístěné vaše další kamery. V případě poškození budete mít pak jasný důkazní materiál o tom, kdo se snažil poškodit vaši nemovitost – ideální je pak kamera s nočním viděním, aby vám neuniklo opravdu nic!

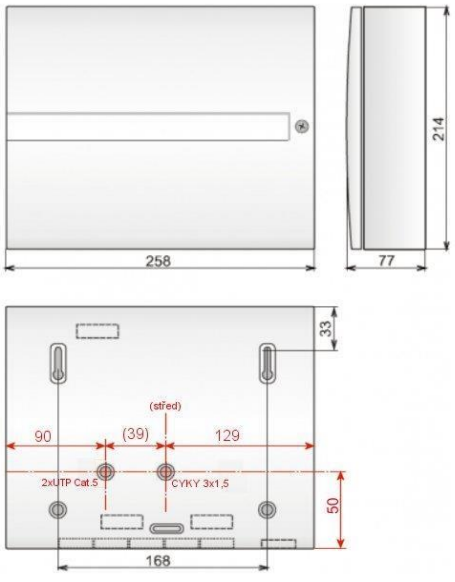
6. KONKRÉTNÍ CENOVÁ NABÍDKA NA ZABEZPEČENÍ PATROVÉHO RODINNÉHO DOMU

Alarm JABLOTRON 100
nabídka: p. Ptáčník, Lhota

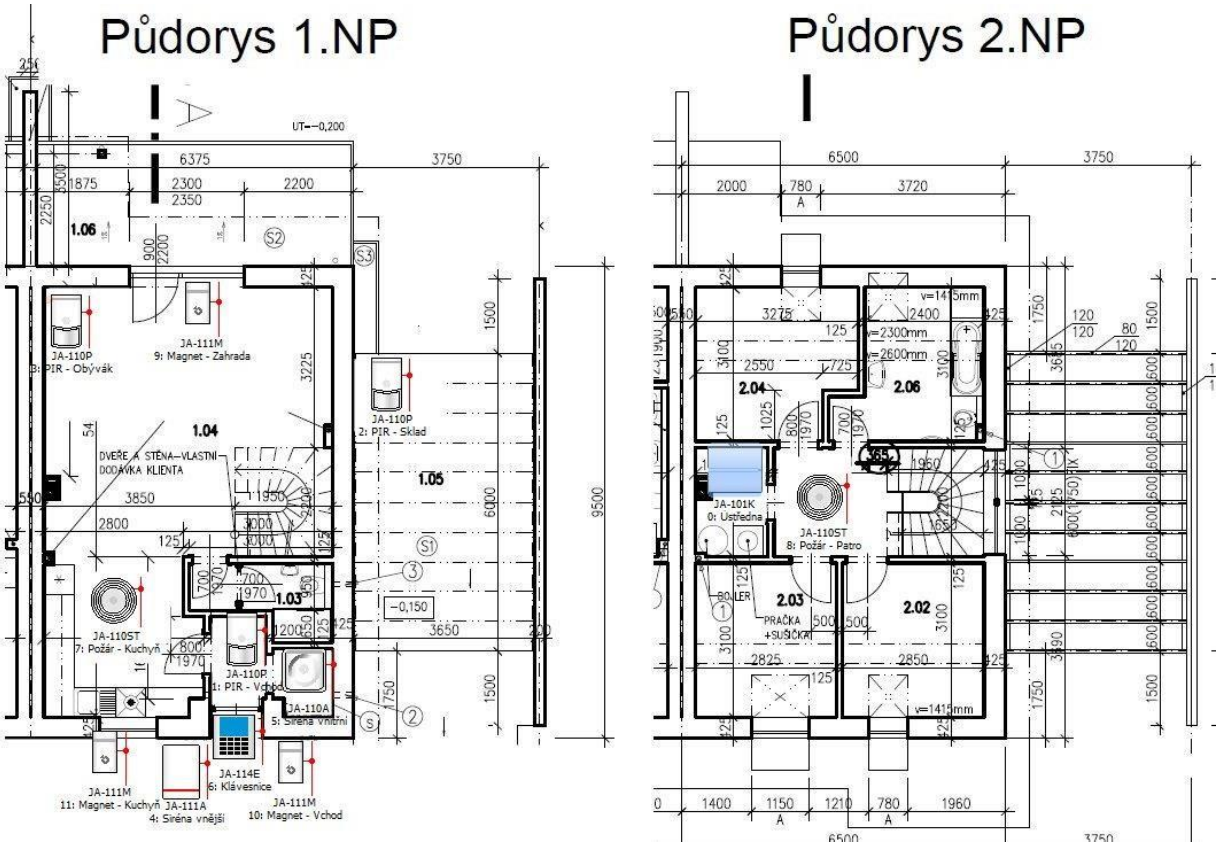
		ks	cena/ks	cena
JA-101K	Ústředna vč. GSM komunikátoru	1	7343,00 Kč	7343,00 Kč
JA-114E	Přístup. modul - kláv, displ., RFID	1	1730,00 Kč	1730,00 Kč
JA192-E	Ovládací segment přístup. modulu	2	82,00 Kč	164,00 Kč
JA-110P	Sběrnicový PIR det. pohybu	3	472,00 Kč	416,00 Kč
JA-111A-BASE	Vnější siréna sběrnicová – zákl. s elektronikou	1	1070,00 Kč	1070,00 Kč
JA-1X1A-C-WH	Plastový kryt sirény bílý, červený blikač			

		1	353,00 Kč	353,00 Kč
JA-110A	Vnitřní siréna sběrnicová	1	464,00 Kč	464,00 Kč
JA-111M	Sběrnicový magnet. detektor mini	3	303,00 Kč	909,00 Kč
SA214-2.6	Akumulátor	1	350,00 Kč	350,00 Kč
JA-110ST	Sběrnicový komb. detektor kouře a teploty	2	796,00 Kč	1592,00 Kč
JA-190J	Přístupová karta RFID (1ks je součástí ústředny)	1	64,00 Kč	64,00 Kč
JA-191J	RFID přívěsek	1	54,00 Kč	54,00 Kč
materiál celkem před slevou			15509,00 Kč	
Sleva 12,5%			1938,63 Kč	
materiál po slevě			13570,38 Kč	
doprava + drobný instal. materiál			400,00 Kč	
montáž, nastavení, přezkoušení		1	2480,00 Kč	2480,00 Kč
Celkem bez DPH			16450,38 Kč	
DPH 15 %			2467,56 Kč	
Celkem s DPH			18917,93 Kč	
Alternativně:				
JA-1X1A-C-ST	Nerezový kryt vnější sirény	1	1297,00 Kč	
PC 04 B	RFID přívěsek kožený - černý	1	72,00 Kč	
PC 04 G	RFID přívěsek kožený – zelený	1	72,00 Kč	

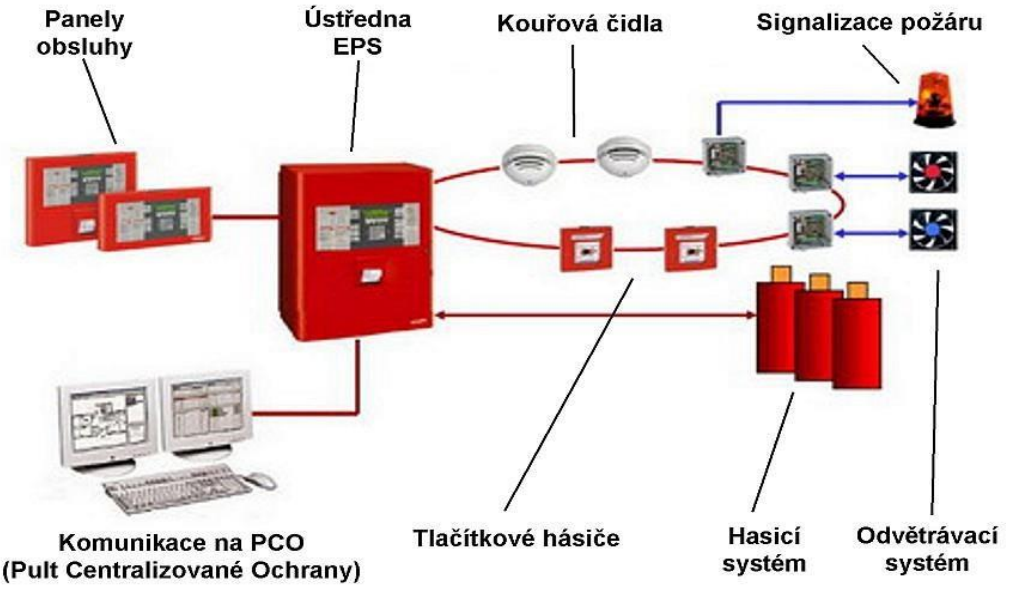
Ústředna



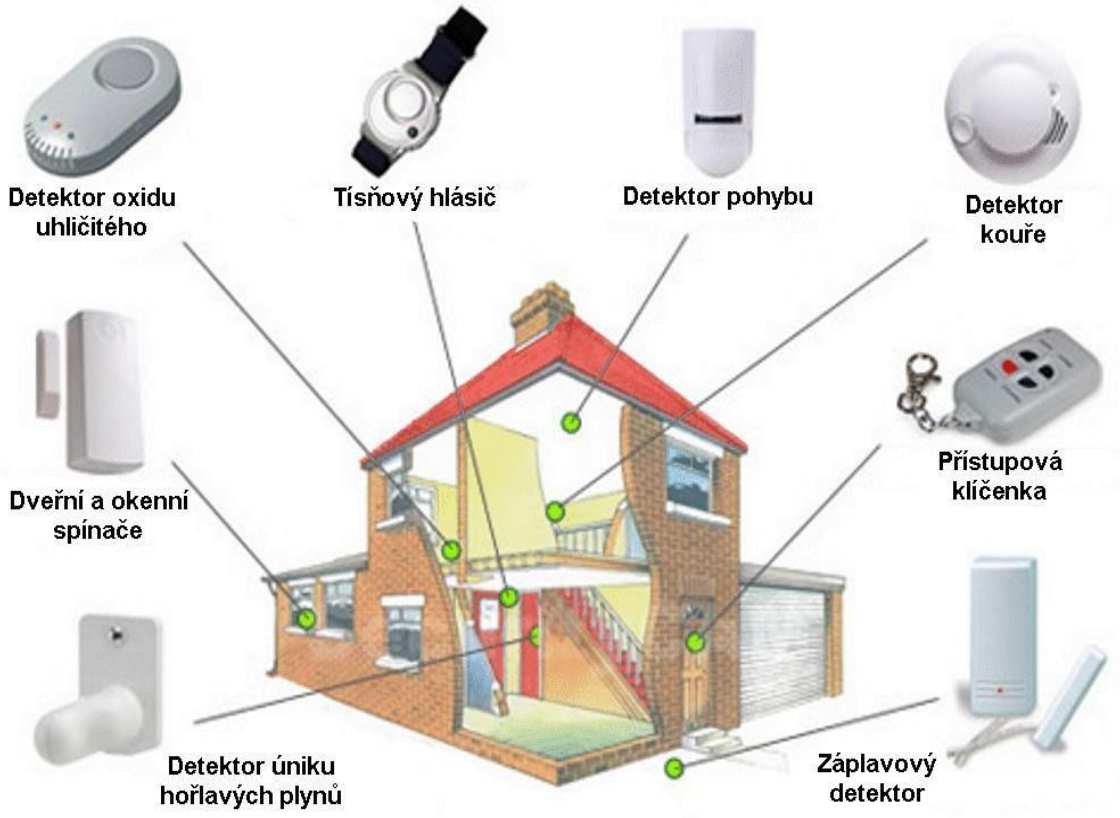
Jablotron JA-101K



Půdorysy objektu



Prvky sloužící k propojení na PCO



Soustava prvků k zabezpečení objektu

6.1. Ukázka prvků EZS

Vnitřní siréna – hlásič požáru

Bezdrátový detektor pochybu

Venkovní siréna

Vnitřní siréna – hlásič narušení objektu

ZÁVĚR

Cílem bakalářské práce je seznámit odbornou i laickou veřejnost o výhodách ochrany, způsobů zabezpečení majetku napojením rodinného domu, bytového domu, komerčních prostor a motorových vozidel. Čtenář by si měl uvědomit, že všechna tato zařízení nejsou nepřekonatelné, ale mají za úkol vyplašení, znepříjemnění, znesnadnění nebo alespoň prodloužení času k páchání trestného činu a s tím spojenou možnost využití zásahové jednotky v případě narušení. Ani finanční hledisko by nemělo hrát žádnou významnou roli v rozhodování, zda si zabezpečení svého majetku pořídit či nikoli.

Jsou zde popsány možnosti zabezpečení, tak aby si každý našel své jak v možnostech obrany, tak i ve finančním rozpětí, která jsou příznivější než o jaké je většina veřejnosti myslí.

Slovník použitých termínů a zkratek

ČSN – České technické normy

EZS – Elektronické zabezpečovací systémy

GPRS – Datová služba GSM (General Packet Radio Service)

GSM – Globální systém pro mobilní komunikaci, (Groupe Spécial Mobile)

IAS – Systémy kombinované nebo integrované

LCD – Displej z tekutých krystalů (Liquid crystal display)

PCO – Pult centrální ochrany

SAS – Systémy přivolání pomoci

SIM – Karta pro identifikaci účastníka v mobilní síti (Subscriber identity module)

SMS – Služba krátkých textových zpráv (Short message service)

VTS – Veřejná telefonní síť

ZS – Zabezpečovací systémy

Seznam použitých zdrojů

Literární zdroje:

ŘÍHA, Milan, SIEGER, Ladislav a PIKOLA, Pavel. *Bezpečnostní systémy* I. Vyd. 4. Praha: Námořní akademie České republiky, 2011. 153 s. ISBN 978-80-87103-32-6

LAUCKÝ, Vladimír, DRGA, Rudolf: *Speciální technologie komerční bezpečnosti*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. 293 s. ISBN 978-80-7454-146-9.

JELÍNEK, Josef. *Jak zabezpečit byt, dům, chatu, automobil*. Vyd. 1. Praha: Grada, 2000. 80 s. ISBN 80-7169-931-4.

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

UHLÁŘ Jan, *Technická ochrana objektů, II.díl – Elektrické zabezpečovací systémy II,* Praha: PA ČR, 2005. 229 s. ISBN 80-7251-189 - 0

Rok zabezpečení vozidel. Praha: Asociace technických bezpečnostních služeb Grémium Alarm, 2010. 20 s. ISBN 978-80-254-8783-9.

KŘEČEK, Stanislav. *Rok zabezpečení vozidel*. 3. aktualizované. Praha: Cricetus, 201l. 351 s. ISBN 80-902938-2-4.

Elektronické zdroje:

Pult centralizované ochrany [online]. 2017 [cit. 2018-03-25]. Dostupné z: http://sis-tel.cz/sluzby/pult-centralizovane-ochrany/

Krádeže motorových vozidel [online]. 2017 [cit. 2018-03-25]. Dostupné z: http://www.mvcr.cz/clanek/bezpecnost-a-prevence-kradeze-motorovych-vozidel.aspx

Krádeže motorových vozidel [online]. 2017 [cit. 2018-03-25]. Dostupné z: http://www.mvcr.cz/clanek/bezpecnost-a-prevence-kradeze-motorovych-vozidel.aspx

Rok zabezpečení vozidel. Praha: Asociace technických bezpečnostních služeb Grémium Alarm, 2010. ISBN 978-80-254-8783-9.

Statistické přehledy kriminality [online]. 2015 [cit. 2018-03-25]. Dostupné z: http://www.policie.cz/statistiky-kriminalita.aspx

Statistické přehledy kriminality [online]. 2015 [cit. 2018-03-25]. Dostupné z: http://www.policie.cz/statistiky-kriminalita.aspx

Příloha 1:

Pult centralizované ochrany