Univerzita Pardubice

Fakulta ekonomicko-správní

Technické zabezpečení firmy

Jan Přibyl

Bakalářská práce
2015

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2014/2015**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan Přibyl**
Osobní číslo:	**E12671**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Technické zabezpečení firmy**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce je analýza současného zabezpečení firmy. Na základě této analýzy odhalit případné nedostatky v technickém zabezpečení firmy. Bude proveden nový návrh technického zabezpečení movitých věcí a technického zabezpečení vybraných dat.

Osnova:
- Základní pojmy a související legislativa.
- Vybrané technické prostředky zabezpečení movitého majetku a dat.
- Analýza stávajícího stavu zabezpečení majetku a dat ve vybrané firmě.
- Identifikace možných bezpečnostních rizik.
- Vlastní návrh technického zabezpečení firmy.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

SCHLOSSBERGER, O. Platební služby. Praha: Management press, 2012. ISBN 978-80-7261-238-3
DOUCEK, P. Řízení bezpečnosti a informací. Praha: Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7
ČANDÍK, M. Technické prostředky bezpečnostního průmyslu. Zlín: Univerzita Tomáše Baťi 2005. 117s. ISBN 80-7318-328-5
LAUCKÝ, V. Technologie komerční bezpečnosti II. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. ISBN ISBN 9788073182311
KINDL, J.: Projektování bezpečnostních systémů. [I. díl, EPS, EZS]. Zlín: Univerzita Tomáše Bati, 2007. 134s., ISBN 978-80-7318-554-1
Interní materiály
Zdroje na internetu

Vedoucí bakalářské práce: **Ing. Hana Jonášová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **29. září 2014**
Termín odevzdání bakalářské práce: **30. dubna 2015**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

prof. Ing. Jan Čapek, CSc.
vedoucí ústavu

V Pardubicích dne 29. září 2014

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Nesouhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 30. 6. 2015 Jan Přibyl

PODĚKOVÁNÍ:

Tímto bych rád poděkoval své vedoucí práce Ing. Haně Jonášové, Ph.D. za její odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

Děkuji také panu Milanu Bigošovi za velice cenné rady, spolupráci při získávání informací, trpělivost a ochotu, kterou mi v průběhu zpracování bakalářské práce věnoval. Poděkování patří i mé rodině a všem, kteří mě při práci podporovali.

ANOTACE

Tato bakalářská práce se zabývá technickým zabezpečením firmy (školy). Obsahem této práce je seznámení se základními prvky bezpečnostní techniky, analýza současného stavu zabezpečení a návrh nového technického zabezpečení.

KLÍČOVÁ SLOVA

Technické zabezpečení firmy, elektronické zabezpečovací systémy, současný stav zabezpečení, analýza rizik, metoda FMAE, nový návrh technického zabezpečení.

TITLE

A technical security of a company.

ANNOTATION

This Bachelor's thesis deals with technical security of a company (a school). The content of this work is to familiarize readers with basic elements of security technologies, the analysis of the current state of the security of the school. It also proposes a new motion of a technical security. The scope of the work corresponds with the syllabus of the subject.

KEYWORDS

A technical security of a company, electronic security systems, the current state of the security, an analysis of possible risks, the FMAE method, a new motion of a technical security.

OBSAH

SEZNAM TABULEK

SEZNAM ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

CCD	Druh kamerového čipu
CCTV	Kamerový systém
ČR	Česká republika
ČSN	Česká technická norma
FMAE	Metoda analýzy rizik
HDD	Hard disk
ID	Identifikátor
PC	Stolní počítač
PIR - US	PIR ultrazvukové
PIR- MW	PIR mikrovlnné
PIR	Pohybový detektor
RFID	Rádio frekvenční identifikátor
Sb.	Sbírka zákonů
SD.	Druh paměťové karty
TNI.	Technické normalizační informace
WC	Toalety

ÚVOD

Již od nepaměti byla vždy snaha lidí chránit jakýmkoliv způsobem svůj majetek. Ze začátku se jednalo pouze o mechanické zábrany, jako byly různé ploty, mříže, zámky, což bylo v té době postačující zabezpečení. Postupem času s příchodem elektrické energie přicházely i v tomto odvětví různé pokusy o zabezpečení pomocí tohoto média. Průkopníkem v této oblasti byl Edwin Holmes, který jako první navrhl elektronický zabezpečovací systém. Po nějaké době i jako první zprovoznil pult centralizované ochrany. Elektrické zabezpečení se neustále vyvíjelo a až postupem času se začalo vyrábět i jako samostatný systém pro zabezpečení a ne pouze, jako doplněk k mechanickému zabezpečení. Tento přelom nastal začátkem minulého století. Avšak ve většině případů byl tento systém vždy překonán, proto je velice důležité jeho neustálé zdokonalování.

V současné době, kdy je na prvním místě pokrok ve všech odvětvích elektroniky, se stává velice důležitým právě elektronické zabezpečení veškerého majetku, osob, dat a mnohého dalšího. Proto je technické zabezpečení nedílnou součástí každé firemní politiky. V této práci se jedná o technické zabezpečení střední školy, které je také velice důležité především v souvislosti s tím, co se poslední dobou děje ve světě a bohužel i u nás v oblasti osobní bezpečnosti žáků a studentů.

Cílem práce je seznámení se základními prostředky sloužícími k zabezpečení movitého i nemovitého majetku a zjistit současný stav vybrané firmy (školy). Dále pomocí vybrané metody analyzovat bezpečnostní rizika a v návaznosti na ně vypracovat vlastní návrh technického zabezpečení.

1 DRUHY OCHRANY

Druhy bezpečnostní ochrany se dělí obecně celkem do čtyř skupin. Rozdělení je odvozeno od toho, jakou ochranu objekt nebo subjekt potřebuje. Jedná se o klasickou ochranu, režimovou ochranu, fyzickou ochranu a nakonec technickou ochranu, která je v současné době nejvíce využívána.

1.1 Související legislativa

V evropských společenstvích je zabezpečovací technika pod působností směrnic evropských společenství. Povinností členských zemí je jejich zpracování do národní legislativy v termínu, který je uvedený přímo ve směrnicích. České republika od roku 2004 patří mezi členské země Evropské unie, a proto jsou technické směrnice přejímány formou vlády České republiky. Základní legislativa je tvořena zákonem 22/97 Sb. O technických požadavcích na výrobky. V souvislosti s tím, že se jedná o objekt školy je další část legislativy tvořena zákonem 262/2006 Sb. [29] [4]

V České republice je mnoho norem ČSN EN, které se problematikou zabezpečovacích systémů zabývají. Tabulka 1 uvádí některé příklady norem a technických normalizačních informací.

Tabulka 1: Příklady ČSN EN a TNI

ČSN EN 50131-1 ED.2	Poplachové systémy - Elektrické zabezpečovací systémy Část 1: Všeobecné požadavky
ČSN EN 50134-1	Poplachové systémy - Systémy přivolání pomoci Část 1: Systémové požadavky
ČSN EN 50134-3	Poplachové systémy - Systémy přivolání pomoci Část 3: Místní jednotka a kontrolér
ČSN EN 50130-4 ED.2	Poplachové systémy - Část 4: Elektromagnetická kompatibilita
ČSN EN 50130-5 ED.2	Poplachové systémy - Část 5: Metody zkoušek vlivu prostředí
ČSN EN 50131-3	Poplachové systémy - Elektrické zabezpečovací systémy - Část 3: Ústředny
ČSN EN 50131-6 ED.2	Poplachové systémy - Elektrické zabezpečovací systémy Část 6: Napájecí zdroje
TNI 33 4591-1	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy Část 1: Návrh systému PZTS
TNI 33 4591-2	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy Část 2: Montáž PZTS
TNI 33 4591-3	Poplachové systémy - Poplachové zabezpečovací a tísňové systémy Část 3: Uvedení PZTS do provozu a jeho následný provoz, údržba a servis

Zdroj: [29]

1.2 Klasická ochrana

Klasická ochrana představuje nejstarší typ ochrany. Jedná se především o vytváření různých zábran, znemožňující zpravidla odcizení nebo zničení cenných předmětů, výrobků, zařízení, zboží atd. [31]

Různé zábrany vždy odpovídají úrovni své doby, jako ploty, mříže, pancéřové pokladny, různé typy zámků apod. Přestože se s technickým pokrokem zábrany neustále zdokonalují, tak se objevují i prostředky a způsoby, jak tyto zábrany překonávat. Historický vývoj i nynější zkušenosti potvrzují, že tyto zábrany nejsou schopny zcela a bezezbytku zabezpečit chráněné objekty. [13] [31]

Vzhledem ke skutečnosti že klasická ochrana patří do širší problematiky bezpečnostního zabezpečení, můžeme jí rozdělit zhruba do tří oblastí podle toho, jaké problematiky zabezpečení se týkají [13]:

- prostředky obvodové ochrany,
- prostředky objektové ochrany,
- prostředky individuální ochrany.

Prostředky obvodové ochrany

Jedná se o skupinu vnějších mechanických zábran, které nejsou přímou součástí vlastního objektu (budova, místnost, dveře apod.), ale jsou od něho prostorově vzdálené. Jsou na volné ploše, většinou na parcele objektu, a mnohdy vytvářejí nejen fyzickou ale i právní ochranu. [13]

Hlavními představiteli těchto ochranných zábran jsou ochranné zdi a ploty. S oběma souvisí používání dalších prvků, které musí být zabezpečeny: vrata, branky a v některých případech i závory, průchody a turnikety. Průchozími prvky v ochranných plotech a zdech jsou dveře, vrata, branky. Všechny tyto prvky jsou stabilně uložené, ale mohou se použít i přenosné zábrany - zátarasy. Vrcholová ochrana představuje zabezpečení vršku zdí či plotů. Mezi prvky této ochrany patří pevné hroty na vrcholech plotů a zdí nebo ostnatý a žiletkový drát. [30] [13]

Prostředky objektové ochrany

Jedná se především o zabezpečení proti vniknutí vstupními otvory, jako jsou dveře, okna, garážová vrata, stavební otvory, vikýře.

Dveře se skládají ze dvou celků. První je zárubeň, která je vyrobena buď ze dřeva, nebo nejlépe z ocelových profilů, a tím je bezpečnější než dřevěný rám. Velmi důležité je usazení rámu do stěny a jedna jeho stojina musí být opatřena zapadacím plechem (tzv. protiplechem), což je přišroubovaný díl sloužící pro zasouvání závory včetně střelky uzamykacího zámku při zamykání. Z hlediska bezpečnosti jsou nejdůležitější vstupní dveře. Jejich bytelnost musí zaručovat, že plochu dveří nelze prokopnout či vyvrátit. [13] [30]

Okna, resp. všechny zasklené prostory stavebních otvorů, jsou hned na druhém místě zájmu ochran. Konstrukce oken může být otevíratelná nebo neotevíratelná. Z hlediska bezpečnosti musí být rám okna pevný a musí být do zdi (ostění) řádně ukotven. Také závěsy musí být pevné a bezpečně připevněné k rámu (musí odolávat páčení). [30]

V souvislosti s vniknutím do objektů je i velice důležitá tzv. minimální doba průlomové odolnosti otvorových výplní. Čím je tento čas delší, tím je daná překážka nebo zábrana hůře překonatelná.

Stanovení minimální doby průlomové odolnosti otvorových výplní

Jedná se o dveře, okna, balkonové dveře, mříže, vrata apod. Minimální čas potřebný pro překonání je uveden v tabulce 2. Tento čas je nutno 2-3 násobně navýšit (neboť se jedná) o zkušební čas), tím dostaneme reálný čas, za který lze otvorovou výplň zpravidla překonat. [13]

Tabulka 2 Bezpečnostní třídy a odporový čas otvorových výplní

Bezpečnostní třída	Kategorie nářadí	Předpokládaný způsob napadení	Odporový čas (min)
1	Nepoužívá se	Příležitostný zloděj zkouší rozbít okno, dveře nebo okenice užitím fyzického násilí, např. kopáním, naražením ramenem, zdviháním vytrháváním.	Neměřen
2	A	Příležitostný zloděj dále zkouší rozbít okno, dveře nebo okenice užitím jednoduchých nástrojů, např. šroubováků, kleští, klínu.	3
3	B	Zloděj zkouší zajistit přístup použitím dalšího šroubováku a páčidla.	5
4	C	Zkušený zloděj dále používá pily, kladiva, sekery, sekáče a přenosné akumulátorové vrtačky.	10
5	D	Zkušený zloděj dále používá elektrické nářadí, např. vrtačku, přímočarou pilu, úhlovou brusku o průmětu kotouče maximálně 125 mm	15
6	E	Zkušený zloděj dále používá výkonné elektrické nářadí např. vrtačku, přímočarou pilu, úhlovou brusku o průmětu kotouče maximálně 230 mm.	20

Zdroj: [13]

Prostředky individuální ochrany

Jedná se o prostředky, které mohou sloužit samostatně, převážně jako úschovné objekty, ale mohou být zařazeny i do předchozích ochranných systémů ochrany. Tyto prostředky jsou konečným místem pro úschovu finančních hotovostí, šperků, cenností, sbírek, cenných papírů a dokumentů. Musí být proto na nejvyšším stupni bezpečnosti. Patřím sem především mobilní a stabilní trezory, trezorové skříně, ohnivzdorné skříně, příruční pokladny, manipulační schránky, přenosné kontejnery a kufry. Samozřejmě všechny tyto prostředky musí být opatřeny zámkovou technikou vzhledem k účelu těchto prostředků. [30] [6]

Klíčové zámky se prezentují vysokou přesností výroby stavítek a montáže, tak aby se při otáčení klíče zasouval závorový kolík do výřezu stavítek s minimální vůlí. U heslových zámků mohou nastat dvě varianty. První z nich je heslový zámek mechanický, kde nastavení zvoleného kódu se provádí otáčením heslového kotouče umístěného na čelní stěně dveří trezoru. Druhou variantou je heslový zámek elektronický, kde se nastavení kódu provádí na klávesnici. Mnohdy se používají u trezorů i dva zámky. [31]

1.3 Režimová ochrana

Režimová ochrana je souhrnný název pro směrnice, která stanovuje pravidla pro vstup, výstup a pohyb osob po objektu. Jsou určeny, jak pro zaměstnance, tak i pro návštěvy. Pravidla jsou vytvořena pro manipulaci s informacemi nebo pro výkon služby ostrahy objektu. Je důležité, aby tyto směrnice byly prosazeny a každodenně používány. [3] [6]

Vnější režimová opatření

Vnější opatření se týkají vstupních a výstupních podmínek. Jedná se hlavně o osobní a nákladové brány. Tedy o místa, kde se dostávají osoby do objektu nebo z objektu. Tyto opatření určují kdo, kdy, kde a jak smí, popřípadě nesmí do objektu vstupovat. Konkrétní opatření bývají často řešena fyzickou ostrahou. [31] [2]

Vnitřní režimová opatření

Opatření se týkají omezení pohybu osob a vozidel ve stanovených oblastech v chráněném objektu. Omezení se může týkat i určitých prostorů, kam mají povolen vstup pouze prověření pracovníci. Směrnice dále mohou stanovit i zajištění osvětlení, vytvoření druhého vnitřního oplocení z důvodu možnosti vpuštění hlídacích psů. Úkolem směrnic je i zajištění režimu pohybu materiálu tak, aby bylo zamezeno úniku neevidovaných materiálů, či výrobků. [31]

1.4 Fyzická ochrana

Fyzická ochrana je prováděna strážnými, hlídači, hlídací službou nebo policisty. Vysoká přednost spočívá v reakci pracovníků na vzniklý problém. I když jsou zde poměrně nízké pořizovací náklady, stále se jedná o nejdražší typ ochrany, a to z důvodu režijních nákladů. Aby objekt byl efektivně zabezpečen proti vniknutí, je potřeba kombinovat fyzickou ochranu s ostatními druhy. Fyzické ochrana je jako jediná schopna v případě nutnosti provést zásah k odvrácení nebezpečí, je to dáno tím, že se aktivně podílí na zmaření záměrů narušitele a umožňuje bezprostřední opatření k jeho dopadení. [13]

1.5 Technická ochrana

Její hlavní funkce spočívá v tom, že velmi rychle reaguje na změny vyvolané pachatelem a na základě těchto změn, indikovaných i na značné vzdálenosti, uvádějí v činnosti síly (zásahové jednotky), schopné v další činnosti pachateli zabránit a dopadnout jej prakticky ještě před dokonáním jeho činu. [31]

Technická ochrana sama o sobě není ochranou v pravém slova smyslu, ale má směrem k pachateli bezprostředně jen odstrašující účinek. Zcela obecně jde o detekční systém, který zajišťuje a předává informace o situaci v chráněném prostoru. Situací v chráněném prostoru rozumíme souhrn fyzikálních, případně i jiných veličin, které jsou technickými prostředky vyhodnocovány z hlediska „jevů s charakterem nebezpečí“. [13]

Prvky technické ochrany lze považovat za nejspolehlivější a nejhůře překonatelné. Technická ochrana účinně podporuje klasickou ochranu tak, že jsou předávány informace o jejich napadení. Jednou z výhod je snížení počtu zaměstnanců fyzické ochrany. Označení o použití těchto prvků má na pachatele značně odstrašující účinek. [31] [2]

2 ELEKTRONICKÉ ZABEZPEČOVACÍ SYSTÉMY

Elektronické zabezpečovací systémy (EZS) jsou komplexem technických prostředků, které jsou schopné rozpoznat přítomnost nežádoucí osoby a tuto skutečnost určitým způsobem (opticky, akusticky) na definovaném místě signalizovat. Hlavním posláním EZS je informovat majitele objektu nebo určenou obsluhu o pokusu vniknutí cizí osoby do chráněného prostoru. Systém se skládá ze zabezpečovací ústředny, záložního zdroje, z detektorů (čidel v mnoho modifikacích - pasivních, aktivních i kombinovaných) a z koncových zařízení (venkovní a vnitřní sirény, telefonní komunikátory, atd.). Před uvedením na trh musí systém EZS projít zákonem stanovenými zkouškami v akreditované zkušebně. Potom je výrobek certifikován do určité kategorie, která umožňuje jeho využití v objektech s určitými riziky. [2]

V Evropě se rozlišují čtyři kategorie [13]:

- velmi vysoká rizika,
- vysoká rizika,
- průměrná rizika,
- nízká rizika.

Systémy EZS pracují obvykle ve dvou režimech [2]:

- v nočním režimu, kdy střeží zpravidla všemi detektory celý objekt
- v denním režimu, kdy je budova v normálním stavu, se střeží pouze instalace systému a vybrané předměty (trezory, vystavované předměty apod.).

Stupně zabezpečení

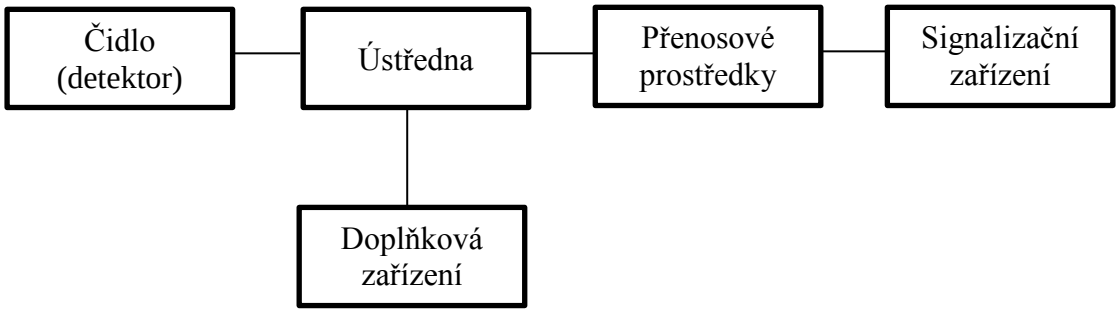
Nejdůležitějším kritériem pro zatřídění příslušného prvku EZS jsou tzv. stupně zabezpečení, které jsou definovány v ČSN EN 50131-1 ED.2. Stanovují kritéria na výbavu a funkci jednotlivých komponentů popř. i systému z hlediska: přístupové úrovně, provozování, vyhodnocení, napájení, zabezpečení proti sabotáži, monitorování, propojení, záznamu událostí. Jednotlivé stupně zabezpečení včetně popisu viz tabulka 3. [13]

Tabulka 3: Stupně zabezpečení

Stupeň	Míra rizika	Předpokládaný typ narušitele
1	Nízká	Narušitel má malou znalost EZS; omezený sortiment snadno dostupných nástrojů
2	Nízká a střední	Narušitel má určité znalosti o EZS; omezený sortiment základních přenosných přístrojů (například multimetr)
3	Střední a vysoká	Narušitel je obeznámen s EZS; úplný sortiment základních přenosných přístrojů a elektronických zařízení
4	Vysoká	Narušitel je schopen nebo má možnost zpracovat podrobný plán vniknutí; kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících prvků EZS

Zdroj: [13]

Za pomocí následujících prvků je vytvořen tzv. *zabezpečovací řetězec*, který znázorňuje správnou funkci prostředků technické ochrany. Tento řetězec je zobrazen na obrázku 1. [31]



Obrázek 1: Zabezpečovací řetězec

Zdroj: [31]

2.1 Čidla (detektory)

Jedná se o zařízení, která dokáží bezprostředně reagovat na fyzikální změny spojené s narušením střeženého prostoru nebo s pohybem střeženého předmětu. Pokud dojde k této reakci, vyšle čidlo následně poplachový signál nebo zprávu. Umístění se volí zejména do míst, kde pachatel překonává chráněný prostor. Jedná se o vnější otvorové výplně a stavební prvky budov. Čidla mohou být napájená nebo nenapájená. V případě napájených zařízení se dále rozlišují čidla aktivní, která jsou snadněji odhalitelná a čidla pasivní. [31]

Dělení napájení čidel podle dosahu pro vnitřní (vnější) použití [13]:

- čidla s krátkým dosahem – do 15 m (do 50 m),
- čidla se středním dosahem – do 50 m (do 150 m),
- čidla s dlouhým dosahem – nad 50 m (nad 150 m).

Nenapájená čidla mohou být formou poplachových fólií, tapet či skla. Jedná se o destrukční zařízení sloužící pouze do doby, než je činností pachatele zničeno. Při jejich narušení dochází k poplachu. [31]

Nevýhodou těchto detektorů může být ovlivnitelnost spolehlivosti rychlou změnou teploty ve střeženém prostoru (topení, tepelné zdroje) nebo dalšími aspekty, kterými mohou být např. rušení zdrojem světla, proudění vzduchu nebo pohyb zvířat. Jednou z velkých nevýhod čidel je omezenost detekční charakteristiky. Proto je velice důležité při montáži dbát na správné umístění čidel. V každém čidle je tzv. tamper, který slouží k okamžitému vyhlášení poplachu v případě, že se pachatel bude snažit odejmout nebo jinak poškodit kryt čidla. [2]

2.2 Ústředny elektronických zabezpečovacích systémů

Zásadní funkcí ústředen je sběr informací o stavu jednotlivých poplachových čidel a na základě rozhodovacího schématu, předem vytvořeného obsluhou, vyvolání poplachových signálů. Moderně vybavená ústředna dokáže oznámit, k čemu ve střeženém objektu došlo a poté přivolat posilu ve formě policie. Ústředny se mohou lišit vnitřním uspořádáním elektroniky, programovým vybavením, způsoby ovládání a také připojováním vstupů a výstupů. Všechny ale zajišťují napájení čidel nebo dalších prvků elektronických zabezpečovacích systémů elektrickou energií. Jejich umístění musí být v chráněném prostoru, aby byly mimo dohled neoprávněných osob, protože by pachatel mohl zničit středobod celého systému před včasným odesláním informací o napadení. [13] [7]

Napájecí obvody v ústřednách k napájení jednotlivých prvků (detektory, klávesnice atd.), a také hlavně k napájení samotné ústředny. K napájení se používá 12V DC. Systém EZS musí být schopen pracovat i při výpadku elektrického proudu, ať již v důsledku poruchy nebo narušení. Záloha elektrické energie je realizována pomocí bezúdržbových olověných akumulátorů. Zdroj ústředny musí být schopný dodávat elektrický proud, který je dán součtem všech proudových odběrů jednotlivých prvků. Zároveň musí být schopen dodávat elektrický proud pro dobíjení akumulátoru v daném čase, který je stanoven příslušnou normou. [2] [12]

Požadované minimální doby napájení náhradním napájecím zdrojem nabíjeným ústřednou EZS dle normy ČSN EN 50131-1 pro jednotlivé stupně jsou [7]:

Minimální doba pro napájení je uvedena v tabulce 4.

Tabulka 4: Minimální doba napájení

	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Doba v hod.	12		60	

Zdroj:[7]

Norma ČSN EN 50131-1 také stanovuje dobu nabíjení akumulátoru do hodnoty 80% nabití pro ústředny EZS. Hodnoty jsou uvedeny v následující tabulce 5.

Tabulka 5: Minimální doba pro dobití

	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Maximální doba pro dobití v min	12		60	

Zdroj:[7]

2.3 Přenosové prostředky

Cílem přenosových prostředků je přenést informace o poplachu ve střeženém místě do místa trvalé obsluhy. Může jim být pult centralizované ochrany, Policie ČR, Městské policie nebo soukromé bezpečnostní služby. [31]

K přenosu se využívají tyto druhy tras [31]:

- přímá (pevná) linka,
- sítě nízkého napětí,
- linka jednotné telekomunikační sítě,
- bezdrátový přenos (rádiový, optický).

Bezdrátový přenos je ve vlastnictví provozovatele, který musí vybudovat jednoúčelovou rádiovou síť. Pokud je přenos přerušen nebo dojde k výpadku, zjistí to centralizovaný pult ochrany. Nezjistí-li zda došlo k ohrožení objektu, vyšle jednotku k prozkoumání. [13] [3].

2.4 Signalizační zařízení

Signalizační zařízení signalizuje výstupní informace ústředny a to buď opticky, akusticky nebo jejich kombinací. Signalizační zařízení má za úkol zajistit převedení předaných informací na vhodný signál, který vyhlásí poplach nebo výstrahu. [7]

2.5 Doplňková zařízení

Ke klasické sestavě zabezpečovacího systému, která se skládá z čidla a ústředny, lze připojovat další zařízení, která zlepšují činnost, dokumentují místa narušení nebo usnadňují obsluhu. Mezi tato doplňková zařízení především patří akustická signalizace, optická signalizace, tiskárna a fotodokumentační zařízení. [7]

2.6 Prvky EZS

Umístění a směřování prvků EZS se provádí způsobem, umožňujícím detekovat charakteristické rysy nebezpečí právě v tom okamžiku, kdy pachatel překonává chráněný prostor nebo předmět. Podle toho, ve které části zabezpečovaného prostoru (zóny) může být pomocí prvků EZS detekováno nebezpečí, rozlišujeme střežené zóny podle prostorové orientace na [13] [31]:

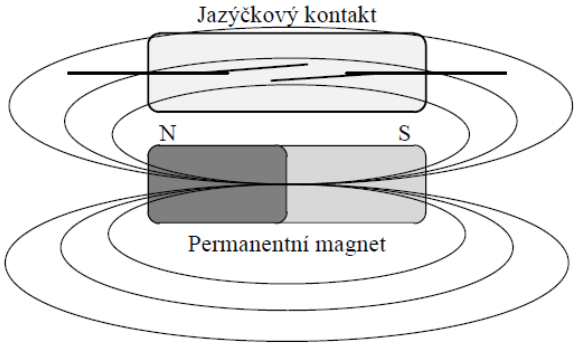
- prvky plášťové ochrany,
- prvky prostorové ochrany,
- prvky tísňové ochrany,
- prvky předmětové ochrany,
- prvky venkovní obvodové ochrany,
- signalizační zařízení.

2.6.1 Prvky plášťové ochrany

Úlohou prvků EZS v plášťové ochraně je včasná signalizace snahy pachatele o překonání klasické ochrany chráněného objektu. Jedná se především o vnější otvorové výplně (vstupní a balkónové dveře, okna), ale i často opomíjené stavební prvky budov (obvodové zdivo, podlahy, stropy a střechy). [3]

Magnetické kontakty

Magnetický kontakt tvoří vždy dvojce jazýčkový kontakt a permanentní magnet, kde jazýčkový kontakt je vytvořen skleněnou trubičkou naplněnou ochrannou atmosférou, v níž jsou dva feromagnetické kontakty, viz obrázek 2. Jsou vhodné pro střežení přístupových bodů a jejich otevření. Magnet se připevní na pohyblivou část a kontakt na rám. [13]



Obrázek 2:Princip magnetického kontaktu *Zdroj: [13]*

Čidla na ochranu prosklených ploch

Tříštění skla způsobuje charakteristický zvuk, který se hmotou skla šíří jako vlnění v pevném tělese. Toto vlnění zachycuje čidlo pevně spojené s plochou skla - přilepené s důrazem na co nejmenší ztráty při přenosu zvuku. Tato čidla se nazývají kontaktní. Při narušení skleněné plochy je vlnění vyhodnoceno elektronikou čidla a čidlo způsobí hlášení. Praktický dosah těchto čidel bývá 1,5 – 3 m dle typu. [23]

Vibrační čidla

K prvkům střežení pláště budov dále patří vibrační čidla pro hlídání průrazu stěn a stavebních konstrukcí. Osazují se podle konstrukčního provedení na riziková místa možného průchodu zdí, luxfery či na rámy dveří a oken. Vzhledem ke své konstrukci nejsou určena pro střežení trezorových skříní a komorových trezorů. [2]

Poplachové fólie, tapety, polepy a poplachová skla

Tato čidla pracují na principu přerušení vodivého média. Nejčastěji se jedná o jemný drátek uvnitř zmiňovaného nosiče (fólie, tapety, skla), či pásků fólie aplikovaných samostatně na povrch hlídané plochy (polepy). Podstatným problémem zůstává vysoká náročnost vlastního řemeslného provedení všech variant střežení pláště objektů uvedených v této části. [13]

Drátová čidla

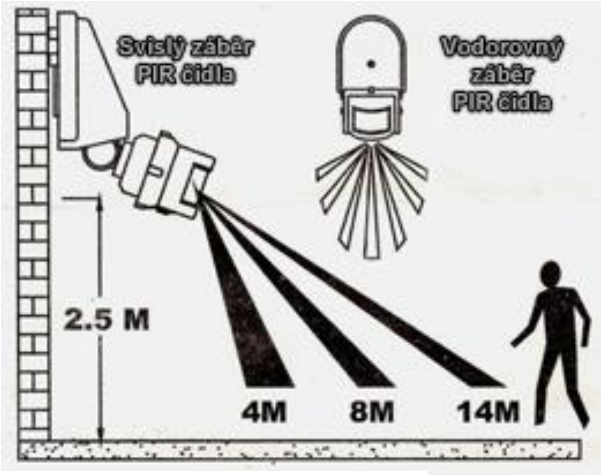
Jedná se o jemná ocelová lanka propojená s citlivým mikrospínačem. Jsou vhodná pro střežení velkých prostupů ventilace a prostupů inženýrských sítí do objektu. Správně instalovaná čidla reagují již na malé zvýšení mechanického napětí. [13] [31]

2.6.2 Prvky prostorové ochrany

Těžištěm prostorové ochrany jsou centrální body budovy tj. schodišťové přístupy či výstupy, haly, spojovací chodby a vnitřní komunikační uzly. Předností tohoto druhu ochrany jsou nižší náklady na instalaci a montáž, protože precizní zvládnutí montáže magnetických kontaktů a čidel na ochranu skleněných ploch je výrazně náročnější a nákladnější než montáž čidel pohybu. [30]

Pasivní infračervená čidla

Obvykle jsou tato čidla označována jako PIR čidla (Passive InfraRed sensor). Jsou založena na principu zachycení změn vyzařování v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění. Využívají skutečnosti, že každé těleso, jehož teplota je vyšší než -273 °C (absolutní nula) a nižší než 560 °C, je zdrojem vyzařování vlnění v infrapásmu odpovídajícím teplotě tělesa. Jako detektor je použit materiál, který vykazuje pyroelektrický jev – polovodičová součástka, která vyhodnocuje změny zařízení. Kvůli vyhodnocení se prostor, který čidlo zabírá, rozděluje pomocí speciální optiky na aktivní a neaktivní oblasti a právě přechod mezi těmito oblastmi je vyhodnocován. Nejčastějším typem optiky je tzv. Fresnelova čočka, kterou lze měnit typ detekční charakteristiky viz obrázek 3. [13]



Obrázek 3: Příklady detekčních charakteristik PIR čidel

Zdroj: [9]

Na obrázku 3 jsou zobrazeny standardní vlastnosti PIR čidla, které se týkají úhlu záběru a jeho dosahu. Úhel a dosah záběru různých typů PIR čidel, se může lišit. Avšak obecný zorný úhel běžného pohybového čidla je stejný jako na vyobrazení. Některá speciální PIR čidla pro zabezpečovací systémy, mají velmi plochou charakteristiku záběru (detekční plochu tvoří "úzký vějíř"). Tento typ čidel se používá především v prostorách, kde se pohybují malá domácí zvířata (psi, kočky apod.). Takový typ čidla - "plošné pohybové čidlo" registruje pohyb pouze v úzce vymezeném prostoru z hlediska "výšky" záběru. Detekční úhel (na výšku) takového čidla může být např. 15°. Kočku a psa pohybující se po zemi, takové čidlo nezachytí, protože registruje pohyb např. až od výšky 1,5 metrů. Každopádně obecně platí, že psi, kočky apod., do prostoru střeženého pohybovým čidlem nepatří. [9]

Kombinovaná (duální) čidla

V prostorách s obtížnými podmínkami nasazení, s výrazným negativním vlivem okolí prostředí, se nabízí využití kombinovaných čidel PIR – US či PIR – MW. Vlastní myšlenka pro vývoj kombinovaných (duálních) čidel vychází ze zásady, že je zanedbatelná pravděpodobnost současného vzniků jevů, které by mohly vyvolat planý poplach u více čidel pracujících na různých fyzikálních principech. [13]

2.6.3 Prvky tísňové ochrany

Slouží k ochraně zaměstnanců a veřejnosti v případě přímého ohrožení. Hlášení do místa, odkud může být poskytnuta pomoc, je vyvoláno buď přímým manuálním aktem, nebo zprostředkovaně při definovaném způsobu manipulace, popř. automaticky bez jakéhokoli přispění obsluhy či nositele [3] [2]

Veřejné tísňové hlásiče

Veřejné tísňové hlásiče jsou magnetokontakty či mikrospínače, zapouzdřené do žlutého nebo červeného tlačítka. Slouží veřejnosti (popř. klientele) k vyvolání tísňového hlášení. Aplikují se na viditelných místech objektů, při schodištích, v chodbách a halách (ve výšce 120 – 150 cm od podlahy) tak, aby je mohl použít každý, kdo je v nouzové situaci nebo je takové situace svědkem. [13] [31]

Speciální tísňové hlásiče

Speciální (skryté) tísňové hlásiče jsou určeny k nepozorovanému vyvolání tísňového hlášení v případě přímého ohrožení. Používají je osoby zaměstnané v chráněném objektu a seznámené s jejich účelem, funkcí a způsobem použití. Při jejich umisťování je nutno

pečlivě zvolit vhodné místo, protože nemají ochranu před nechtěným vyhlášením poplachu. [2]

2.6.4 Prvky předmětové ochrany

Prvky předmětové ochrany jsou především určeny ke střežení cenných, ať již volně stojících, samostatně nebo skupinově umístěných předmětů (obrazy, sochy, skříně, trezory apod.). Umožňují jejich trvalé střežení i v době, kdy prostorová čidla pohybu musí být z důvodu provozu v zájmovém prostoru vypnuta. [30]

Kapacitní čidla

Jsou určena k indikaci přiblížení se k chráněnému předmětu čí jeho doteku. Čidla mohou být užita k ochraně obrazů, volně stojících předmětů, skříní kovových i nekovových. Kapacitní čidla lze použít v místnostech i ve volném terénu. Principem je měnění parametrů vzduchu. [13]

2.6.5 Prvky venkovní obvodové ochrany

Jsou to čidla, která chrání, resp. signalizují narušení vnějších částí u rozlehlých objektů, komplexů budov nebo továren na samostatném pozemku. [23]

Infračervené závory a bariéry

Nejrozšířenějším druhem venkovních obvodových čidel jsou infračervené závor (infrazávory). Mezi přijímací a vysílací stranou probíhá jeden či více infračervených paprsků. Při přerušení některého z nich dochází na přijímací straně k vyhodnocení a k vyhlášení poplachu. Pro zvýšení odolnosti proti cizím zdrojům světla pracují infrazávory v pulsním režimu. [31] [10]

2.6.6 Signalizační zařízení

Zábleskový maják

Většinou je již součástí venkovních sirén, bývá zabudovaný. Jedná se o výkonovou žárovku buzenou přes přerušovač, ne o výbojku. Účelem je i po doznění sirény možnost určení místa poplachu. [7]

Sirény

Sirény jsou nejčastěji instalovaná doplňková zařízení. Jsou určeny, buď pro vnitřní nebo venkovní použití. Základem je akustický měnič vytvářející kolísavý tón. Doba činnosti sirény

musí být minimálně 90 sekund a maximálně 15 minut. Umisťuje se do vyššího místa, kvůli dostupnosti i šíření zvuku. V dnešní době má většina sirén svůj vlastní záložní zdroj. [7] [10]

2.6.7 Kamerové systémy

Vzhledem ke zlepšení zabezpečení různých objektů se v současné době stále využívají více systémy průmyslové televize, jsou to tzv. uzavřené televizní okruhy (Closed Circuit Television). Velice často se využívají společně s EZS. Výhodou systémů CCTV je efektivním způsobem monitorovat střežený prostor a kontrolovat i velmi rozsáhlé prostory v reálném čase. Systém CCTV umožňuje ukládat snímání obrazu na datové médium, a to v dnešní době především na HDD. Záznam následně slouží k vyhodnocení poplachových situací a k zpětnému dohledání zaznamenávaných informací apod. Systém CCTV lze vhodně využívat se systémem EZS nebo jej lze provozovat i jako samostatnou jednotku. Největší překážkou většího rozšíření je jejich vysoká pořizovací cena. [23] [11]

Systémy CCTV se vyznačují především těmito základními funkcemi [13]:

- Zdrojem informací v systému CCTV je kamera,
- v dnešní době se prakticky využívají pouze kamery s CCD čipem, který umožňuje dokonalé digitální zpracování obrazu,
- kamery mohou být černobílé nebo barevné,
- pro ochranu objektu se dá využít tzv. psychologického účinku imitací kamer.

2.6.8 Přístupové systémy

Jednou z hlavních částí bezpečnostních systémů jsou ty prvky (části), které slouží k ověření identifikace osob. V této souvislosti je významným parametrem autentizace, tj. ověření, že daná osoba je skutečně tou osobou, za kterou se vydává. Přístupové systémy neslouží pouze k otevírání elektrických dveřních zámků, ale také podle přístupových práv umožňují průchod jakoukoliv elektronickou zábranou. Ve výsledku tyto systémy umožňují v mnoha případech zmenšit náklady na ostrahu či zámkový systém, a přesto podstatně zvýšit úroveň bezpečnosti. Systémy bývají založeny na jednoznačné identifikaci osob pomocí bezkontaktních čipových karet, RFID karet, nebo na základě biometrické identifikace. [3] [24].

2.6.9 Čipové karty

Čipová karta je polovodičový čip, který byl speciálně vyroben pro konstrukci čipové karty nebo podobného zařízení (kryptografického předmětu). Pod čipovou kartou si lze představit miniaturní kryptografický počítač, jehož funkcí je komunikace s PC nebo s terminálem pomocí rádiového nebo kontaktního přenosu. Čipové karty se dělí na dva druhy, a to na kontaktní a bezkontaktní čipové karty. [24] [1]

Kontaktní čipové karty

Kontaktní čipové karty obsahují kontaktní pole, které se nejčastěji skládá z osmi kontaktů. Pomocí těchto kontaktů dochází k propojení do čtečky. Nevýhodou je omezená životnost mechanických částí, jak čipové karty a čtečky, která velice závisí na počtu uživatelů a jejich přístupu k zařízení. [1]

Bezkontaktní čipové karty

Bezkontaktní čipové karty nemají pevný kontakt se čtečkou. Komunikace karty a čtečky používá elektromagnetické vlny a probíhá pouhým přiblížením. Standartní vzdálenost je 5-10 cm. Díky tomu jsou používány pro identifikaci fyzického přístupu. Čtečka působí primárně v roli vysílače, které do okolí vysílá kmitočet, který je nejčastěji od výrobců stanoven na 125 kHz. [3] [24]

RFID karty

Jsou dnes mnohem více využívány v běžném provozu, než je tomu u čipových karet. RFID využívají bezkontaktní identifikace, která probíhá pomocí rádiového signálu bez nutnosti přímé viditelnosti. Prakticky se jedná o rádiovou náhradu za čárové kódy. Karty RFID se dělí do dvou skupin, a to na pasivní a aktivní RFID karty. [3]

Pasivní RFID karty

Karty pracují jako vysílače periodických pulsů do okolí. Blízká RFID karta využije signál k nabití svého napájecího kondenzátoru a odešle odpověď. Tento typ pasivních karet je nejrozšířenější, protože nemusí mít vlastní zdroj energie a jsou napájeny polem snímače. [24]

Aktivní RFID karty

Mají vlastní baterii a jsou schopny sami vyslat svoji identifikaci. Aktivní karty jsou používané méně než pasivní, protože jsou složitější, těžší a dražší. [1]

ZÁVĚR

V první části této bakalářské práce jsem se snažil o objasnění základních prostředků, které se používají k technickému zabezpečení. Jedná se zejména o prvky elektronických zabezpečovacích systémů společně s prvky mechanické ochrany. Nedá se ovšem říci, že se jedná o přesný výčet všech možných komponentů, které existují, jedná se spíše o uvedení do dané problematiky a porozumění základním funkcím těchto prvků.

V druhé části práce se zabývám konkrétním zabezpečením vybrané střední školy. Prostory se ovšem nachází společně v areálu více středních škol, proto je hned na začátku této části práce objasněno, o jaké pavilony střední školy se bude přesně jednat. Vybrané pavilony slouží především k odbornému výcviku studentů a nachází se zde mnoho vybavení, které je nezbytné pro výuku. V souvislosti s tím je na tyto pavilony kladen větší důraz z hlediska zabezpečení.

Po zjištění současného stavu zabezpečení jednotlivých pavilónů, jež jsem provedl společně s jedním z pedagogů, který má zabezpečení těchto prostor na starosti, jsem přistoupil k vlastnímu návrhu nového zabezpečení. Základy pro půdorysy, které jsou v práci použity, mi byly poskytnuty Střední školou spojů a informatiky. Tyto půdorysy vznikly již v roce 1985 a bylo je třeba celé překreslit. Sloužily spíše jako podklad pro mou práci, jelikož tuto školu detailně znám z předešlého studia. Návrh byl proveden pro všechny pavilony se zcela novým rozmístěním komponentů zabezpečení. V některých prostorech byla úroveň zabezpečení zvýšena tím, že zde byl přidán ještě jeden prvek, a tím byl detektor tříštění skla. V místnostech, kde se nenachází žádný detektor, byly použity pouze magnetické kontakty, které jsou v těchto místnostech zcela postačující.

Jedním z nejdůležitějších doplnění zabezpečení byla přístupová ochrana. Ta zde prakticky úplně chyběla. Jednalo se hlavně o to, aby se do těchto prostor nemohla dostat osoba, která nemá ke vstupu dostatečné oprávnění. Tento problém byl vyřešen navržením přístupového systému u vchodů v pavilonu A a v pavilonu C. U pavilonu B tento druh ochrany nebyl nutný, protože zde žádný vstup zvenku není. Přesný popis funkčnosti tohoto prvku zabezpečení je popsán v práci.

Střežení chodeb je v novém návrhu zajištěno pomocí kamer, které neslouží pouze ke snímání obrazu, ale také především jako prvky EZS, protože v sobě mají zabudovaný detektor pohybu, detektor tříštění skla a další.

Prvek, který zde zcela chyběl, bylo signalizační zařízení poplachového stavu. To je nyní zajištěno dvěma venkovními sirénami. První siréna je umístěna před vchodem do pavilonu A v dostatečné výšce, aby nebylo tak snadné se k ní dostat. Druhá siréna je u vchodu do pavilonu C a je umístěna velice podobným způsobem. Vnitřní signalizace poplachového stavu je zajištěna pomocí jedné vnitřní sirény umístěné v pavilonu B.

Velkou výhodou zabezpečovacích systémů od firmy JABLTRON ALARMS a.s. je, že nová řada produktů je kompatibilní s předchozí řadou. Díky tomu jsou všechny navržené prvky kompatibilní s nejnovější řadou i s řadou o generaci starší. Proto tento návrh nemusí sloužit pouze k zcela nové instalaci bezpečnostního systému, ale může sloužit i jako předloha k možnosti doplnění stávající bezpečnostního systému.

Jako poslední byly vyčísleny náklady na nové navrhnuté zabezpečení, které činí 160 140 Kč. Dle mého názoru se jedná o částku, která není tak vysoká, vezmeme-li v úvahu, že jde o zabezpečení tří velkých pavilonů.

Tato bakalářská práce může sloužit, jako dostatečně vhodný podklad pro možnou inovaci v zabezpečení středních škol podobného typu.

POUŽITÁ LITERATURA

[1] Bezhotovostní platební styk. In: Manažerka.cz [online]. 20. 3. 2012 [cit. 2015-04-27]. Dostupné z: http://www.managerka.cz/bezhotovostni-platebni-styk/.

[2] ČANDÍK, Marek. *Objektová bezpečnost II.* 1. vyd. Zlín: Univerzita Tomáše Bati, 2004. 100 s. ISBN 80-7318-217-3.

[3] ČANDÍK, Marek. *Technické prostředky bezpečnostního průmyslu*. Zlín: Univerzita Tomáše Bati, 2005. 117s. ISBN 80-7318-328-5

[4] ČESKO. Zákon č. 262/2006 Sb. ze dne 21. dubna 2006 zákoník práce. In: Sbírka zákonů České republiky. 2006, Dostupné také z: <http://www.zakonyprolidi.cz/cs/2006-262>

[5] *Dekonta*. Analýza rizik [online]. c2015 [cit. 2015-06-10]. Dostupné z: <http://www.dekonta.cz/sluzby-a-produkty/konzultacni-sluzby/rizikova-analyza.html>.

[6] DOUCEK, Petr. *Řízení bezpečnosti a informací*. Praha: Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7

[7] ELKOV elektro a.s. [online]. 28. 3. 2013 [cit. 2015-05-20]. Dostupné z: <http://www.ladinn.cz/ostatni/technika/princip-EZS.html>

[8] FMEA [online]. [cit. 2015-06-10] Dostupné z: <http://oprlz.lss.fd.cvut.cz/dokumenty/080523_6.2.FMEA.pdf>

[9] HNILICA, Pavel. *Deramax.cz* [online]. [cit. 2015-06-10]. Dostupné z: <http://www.deramax.cz/gsm-alarm-vyber-a-instalace-od-a-do-z>.

[10] HUSÁK, Miroslav, Úvod do EZS (přednáška), Praha, ČVÚT, [online]. [cit. 2015-06-3]. Dostupné z: <http://www.micro.feld.cvut.cz/home/X34EZS/prednasky/0%20Uvod%20do%20EZS_prednaska.pdf>

[11] HUSÁK, Miroslav, Základy CCTV (přednáška), Praha, ČVÚT, [online]. [cit. 2015-05-11]. Dostupné z: http://www.micro.feld.cvut.cz/home/X34EZS/prednasky/Zaklady%20CCTV.pdf

[12] HUSÁK, Miroslav. Ústředny EZS (přednáška), Praha, ČVÚT, [online]. [cit. 2015-05-12]. Dostupné z: <http://www.micro.feld.cvut.cz/home/x34ezs/prednasky/Zaklady%20EZS_2.pdf>

[13] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky.* Blatná, Cricetus, 3. vyd. 2006. 313 s. ISBN 80-902938-2-4

[14] *LB Quality*. FMEA [online]. [cit. 2015-06-10] Dostupné z: <http://www.lbquality.cz/fmea.php>

[15] *Managment mania*. Analýza pomocí kontrolního seznamu [online]. 26. 6. 2013 [cit. 2015-06-12]. Dostupné z: <https://managementmania.com/cs/analyza-kontrolni-seznam-cla-checklist-analysis>

[16] *Managment mania*. Co – když analýza [online]. 1. 5. 2013 [cit. 2015-06-13]. Dostupné z: <https://managementmania.com/cs/co-kdyz-analyza-what-if-analysis>

[17] Manuál firmy JABLOTRON ALARMS a.s., JS-22 Dvouzónový PIR detektor pohybu osob [online]. [cit. 2015-05-15]. Dostupné z: <http://www.jablotron.com/cz/katalog-produktu/alarmy/univerzalni-prvky/detektory/pohybove/js-22.aspx>

[18] Manuál firmy JABLOTRON ALARMS a.s., klávesnice JA-81E [online]. [cit.2015-06-05]. Dostupné z: <http://www.jablotron.com/cz/katalog-produktu/alarmy/jablotron-80/ovladaci-prvky/klavesnice-a-pristupove-m/ja-81e.aspx>

[19] Manuál firmy JABLOTRON ALARMS a.s., ústředna JS-82 [online]. [cit. 2015-06-04]. Dostupné z: <http://www.jablotron.com/cz/katalog-produktu/alarmy/jablotron-80/ustredny/ja-82k.aspx>

[20] Manuál firmy JABLOTRON ALARMS a.s., Uživatelský manuál [online]. [cit. 2015-06-07]. Dostupné z: <http://www.loucka.cz/_uploads/JA-8x%20u%C5%BEivatelsky%20man.pdf>

[21] MAPY.CZ. [online]. [cit. 2015-05-15]. Dostupné z: http://www.mapy.cz/zakladni?x=14.6792150&y=49.4051815&z=17&base=ophoto&source=muni&id=1031

[22] Metody analýzy rizik [online]. [cit. 2015-06-11]. Dostupné z: <www.jh.cz/filemanager/files/file.php?file=132160>

[23] Ochrana majetku systémy průmyslové televize In: pmpzlin.cz [online]. [cit. 2015-04-27]. Dostupné z: <http://www.pmpzlin.cz/data/file/jak-vybrat-kamerovy-system.pdf>

[24] SCHLOSSBERGER, Otakar. *Platební služby.* Praha: Management press, 2012. 325 s. 1. vyd. ISBN 978-80-7261-238-3

[25] SMEJKAL, Vladimír a Karel RAIS. *Co je to riziko a analýza rizik* [online]. 8. 2. 2011 [cit. 2015-06-10]. Dostupné z: <http://www.orsec.cz/cs/informacni-servis/komercni-zpravy/co-je-to-riziko-a-analyza-rizik_42-570/ >.

[26] Střední škola spojů a informatiky [online]. [cit. 2015-06-01]. Dostupné z: <http://www.sous.cz/index.php/skola/historie-skoly>

[27] ŠCUREK, Jaromír, *Studie analýzy rizika protiprávních činů na letišti*. [online]. [cit 2015-06-14]. Dostupné z: <www.fbi.vsb.cz/export/sites/fbi/040/.content/sys-cs/resource/PDF/analyzy_rizika_letisti.pdf>

[28] ŠNAJDR, Ivo. *Analýza stromu poruchových stavů* [online]. c2013 [cit. 2015-06-15]. Dostupné z: <http://www.snajdr.com/informujeme/snajdruv-slovnicek/fta-analyza-stromu-poruchovych-stavu-fault-tree-analysis/>

[29] *TECHNOR*. Technické normy [online]. [cit. 2015-04-28]. Dostupné z: <http://www.technicke-normy-csn.cz/technicke-normy/elektrotechnika-elektrotechnicke-predpisy-33/elektricka-ridici-zarizeni-3345/?do%5b%5d=setOffset&offset=0>

[30] UHLÁŘ, Jan. *Technická ochrana objektů: I. díl – Mechanické zábranné systémy II.* 1. vyd. Praha: Policejní akademie České republiky, 2004. 179 s. ISBN 80-7251-235-8.

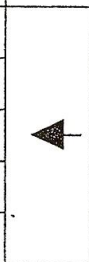
[31] UHLÁŘ, Jan. *Technická ochrana objektů: II.díl - Elektrické bezpečnostní systémy II.* 2. vyd. Praha: Policejní akademie České republiky, 2009. 232 s. ISBN 978-80-7251-313-0.

[32] Uživatelský manuál EYE-02 3G firmy JABLOTRON ALARMS a.s. [online]. [cit. 2015-06-14] Dostupné z: <http://www.jabloshop.cz/eye-02-3g-gsm-kamera-s-technologii-3g>

[33] Zapůjčené interní materiál Střední školy spojů a informatiky

SEZNAM PŘÍLOH

Příloha A – Schématické značky EZS

Sch. značka dle ČSN 50131	Zjednodušená sch. značka	Popis prvku
		Magnetický detektor
		Magnetický detektor - odolný
		Detektor tříštění skla
		Detektor tříštění skla - antimasking
		Kontaktní detektor piezo
		PIR vějíř
		PIR vějíř venkovní
		PIR vějíř antimasking
		PIR dlouhý dosah
		PIR s vlastní adresou
		PIR záclona
		PIR záclona antimasking
		PIR záclona dveřní
		Infrazávora
		Infrazávora vysílač
		Infrazávora přijímač
		Ultrazvukový detektor
		PIR stropní

Sch. značka dle ČSN 50131	Zjednodušená sch. značka	Popis prvku
		Kombinovaný detektor PIR stropní a GBS
		Kombinovaný detektor PIR a GBS (JS-25)
		Mikrovlnný detektor
		Duální detektor mikrovlna, PIR
		Duální stropní detek. mikrovlna, PIR
		Otřesový detektor
		Detektor poslední bankovky
		Tísňový hlásič PANIC tlačítko
		Tísňový hlásič PANIC lišta
		Technologický hlásič
		Detektor hořlavých plynů
		Požární hlásič
		Signalizace optická
		Signalizace optická a akustická
		Vnitřní siréna s blikačem
		Vnitřní siréna
		Venkovní siréna s blikačem
		Venkovní siréna

Sch. značka dle ČSN 50131	Zjednodušená sch. značka	Popis prvku
		Výstražné zařízení maják
		Ústředna EZS
		Napájecí zdroj
		Expandér, link. modul koncentrátor
		Tablo EZS
		Přenosové zařízení komunikátor
		Transformátor 220/18 V
		Záložní akumulátor
		Přijímač řady UC (216, 220, ...)
		Expandér řady UC 280
		Detektor kouře

Sch. značka dle ČSN 50131	Zjednodušená sch. značka	Popis prvku
		Bezdrátový vysílač, přijímač
		Klíčový spínač
		Propouštěcí zámek
		Ovladač, klávesnice
		Vstupně-výstupní modul
		Reléový modul
		Detektor kouře
		Vysílač GSM
		Vysílač PCO
		Záplavový detektor
		Vývod kabelu

Zdroj: [13]

Příloha B – Návrh zabezpečení pro pavilon A - utajené

Zdroj: vlastní zpracování

Příloha D – Návrh zabezpečení pro pavilon B - utajené

Zdroj: vlastní zpracování

Příloha D – Návrh zabezpečení pro pavilon C - utajené

Zdroj: vlastní zpracování