Technické zabezpečení firmy řešící pojistné události

Technical Security Company, that Resolves Insurance Events

Bc. Roman Zlocha

Diplomová práce 2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Roman Zlocha**
Osobní číslo:	**A11392**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Technické zabezpečení firmy, řešící pojistné události**

Zásady pro vypracování:

1. **Popište současný stav technického zabezpečení firmy, poskytující opravárenské služby a řešící pojistné události.**
2. **Proveďte analýnu bezpečnostních rizik při nakládání s osobními údaji pojištěnců, technického zabezpečení budovy.**
3. **Zpracujte normy a předpisy vztahující se k tématu.**
4. **Na konkrétním příkladu firmy, provádějící výměnu autoskel, zpracujte návrh technického zabezpečení budovy a režimová opatření.**
5. **Vyhodnoťte přínos navrhovaného řešení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BRABEC, František. Bezpečnost pro firmu, úřad, občana: velká kniha. 1.vyd. Praha: Public History, 2001, 400 s. ISBN 80-864-4504-6.**
2. **BRABEC, František. Ochrana bezpečnosti podniku: velká kniha. 1. vyd. Praha: Eurounion, 2005, 589 s. ISBN 80-858-5829-0.**
3. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-80-87500-05-7.**
4. **LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management II. 1. vyd. Zlín: VeRBuM, 2012, 386 s. ISBN 978-80-87500-19-4.**
5. **UHLÁŘ, Jan. Bezpečnost sítí: velká kniha. Vyd. 1. Brno: CP Books, 2005, 589 s. ISBN 80-251-0697-7.**
6. **UHLÁŘ, Jan. Technická ochrana objektů. 2. vyd. Praha: Policejní akademie České republiky v Praze, 2009, 229 s. ISBN 978-80-7251-313-0.**

Vedoucí diplomové práce:	**JUDr. Vladislav Štefka** Ústav bezpečnostního inženýrství
Konzultant:	**Ing. Rudolf Drga** Ústav bezpečnostního inženýrství
Datum zadání diplomové práce:	**8. února 2013**
Termín odevzdání diplomové práce:	**3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá zabezpečením sídla malé firmy zabývající se řešením a zpracováním pojistných událostí. V teoretické části práce se zabýváme požadavky na zpracování osobních údajů pojištěnců a tím i potřebné zabezpečení počítačů, na kterých jsou data zpracovávána, tak aby nedošlo k odcizení a zneužití těchto dat a dále pak aby se minimalizovalo riziko neoprávněného vniknutí do prostor firmy. Vzhledem k lokalitě, kde se budova nachází, bude provedena analýza rizika a shrnutí technických prostředku nyní použitých v dané budově. Praktická část obsahuje návrh optimalizace daného systému s poukázáním na současnou situaci, a možnosti jejich změn.

Klíčová slova:

Osobní údaje, Bezpečnost,, I&HAS, CCTV, Analýza rizik, Kamery, Ostraha

ABSTRACT

The master thesis deals with the security of the office of a small company which focuses on insure events solving and processing. In the theoretical part of this work we deal with demands on processing of insured persons personal data as well as demanding security of computers which are used for data processing in way that the data will not be stolen or misused and also to minimize the risk of non-authorized entry into the company office area. Considering the locality of the company building, there will be made an analysis and summary of technical means currently used in given building. The practical part contains a proposal of system optimization with emphasis on current situation and possible changes.

Keywords:

Personal data, security, I&HAS, CCTV, risk analysis, cameras, guarding

Poděkování

Nejdříve bych na tomto místě velmi rád poděkoval vedoucímu diplomové práce panu JUDr. Vladislavu Štefkovi za trpělivost, inspiraci, podporu a jeho pomoc při vedení během tvorby a trpělivost při konzultacích ohledně této práce.

Dále své rodině, za jejich trpělivost a podporu během celého studia na této škole.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Cílem této diplomové práce je zhodnotit současný stav firmy zabývající se opravou vozidel a následným zpracováním pojistných událostí. Zabezpečení uložených el. dat a následné zabezpečení sídla firmy. Jedná se převážně o všechny smluvní servisy, které pro pojišťovny provádějí opravy a samy likvidují pojistné události. Při tomto administrativním procesu dochází ke zpracování osobních údajů klientů pojišťoven třetí stranou a dále jsou tyto údaje posílány elektronickou cestou samotným pojišťovnám. Poté jsou tyto údaje zpracovány i v papírové podobě a jsou předány pojišťovně s tím, že kopie těchto dokumentů uchovává i firma provádějící samotnou likvidaci pojistné události. Provedeme analýzu současného zabezpečení konkrétní firmy zabývajícím se výše uvedenou problematikou, kdy se zaměříme na zhodnocení současného stavu s tím, zda je současný stav vyhovující v souvislosti se zákonem o ochraně osobních údajů č. 101/2000 sb. a s zda je také dostatečný s ohledem na lokalitu, kde se firma nachází. Tj. zvýšený nárůst kriminality v dané lokalitě a tím i zvýšeného rizika neoprávněného vniknutí do sídla firmy, kdy budeme předpokládat, že osobní údaje nebudou primární cíl takovéhoto útoku, ale při napadení objektu ve snaze získat majetkový prospěch může dojít i k odcizení a zneužití dat klientů firmy.

Dále cílem této práce bude navrhnout takové zabezpečení firmy, které bude vyhovovat nejenom firmě samotné, ale bude v souladu i s platnou legislativou. Například bych chtěl využít ustanovení § 10 zák.č.273/2008 Sb. zákona o polici ČR, kdy policie má povinnost konat v případě, že se dozví o možném protiprávním jednání. Jako určující faktor navrhovaného řešení bude finanční stránka celého zabezpečení s ohledem na finanční možnosti malé firmy. V práci se zaměřím nejenom na fyzické zabezpečení objektu a archivovaných dokumentů, ale i na elektronické zabezpečení archivovaných dokumentů v el. podobě a jejich uložení. Navrhnuté řešení by mělo sloužit jako vzor nejenom pro konkrétní firmu, ale jako řešení pro malé firmy zabývající se danou problematikou.

I. TEORETICKÁ ČÁST

1 OCHRANA DAT

Organizace a podniky v současné době si svůj chod bez informací uložených v elektronické podobě neumí představit. V podstatě všechny dokumenty, faktury jsou uloženy v elektronické podobě. Z toho plyne, že tyto data se musí náležitě chránit a zálohovat. Při ztrátě nebo poškození těchto dat, vznikají společnostem obrovské škody což samozřejmě může ve tvrdém konkurenčním boji znamenat velkou nevýhodu.

Ochrana dat nespočívá pouze v kvalitním antivirovém programu a firewallu, ale i v jejich zálohovaní a přijetím režimových opatření k tomu aby se snížilo riziko napadení dat např. virem nebo mechanickým poškozením PC. O data můžeme dojít například odcizením uložiště, kde jsou data uchována, hardwarovou poruchou, lidskou chybou, mechanickým poškozením počítače, napadením systému virem, systémovou poruchou.

1.1 VIRY

Jako základní ochranu počítače před napadením škodlivým programem považuji antivirový program, který by měl zabránit šíření škodlivého programu v síti a tím zabránit poškození uložených dat. V současné době je na trhu mnoho dostupných kvalitních antivirových programů, ale základní pravidlo spočívá v pravidelných aktualizacích a naplánovaných kontrolách. S tím také souvisí řádné proškolení personálu, který data zpracovává.

1.2 MECHANICKÉ POŠKOZENÍ

Každá mechanická součástka má svojí životnost a výjimkou nejsou ani počítačové komponenty. Mechanická závada např. pevného disku bývá nečastější důvodem ztráty uložených dat a z toho důvodu je nutné data zálohovat. Mít v povědomí provozní dobu a životnost uváděnou výrobcem.

1.3 LIDSKÝ FAKTOR

Jako druhou nejčastější příčinou ztráty uložených dat je lidská chyba, kdy dojde neodborným zásahem nebo nedbalostí ke ztrátě a poškození dat. Jako řešení se v této situaci jeví řádné proškolení obsluhy a využívání softwaru pro obnovu dat. Žádné zálohovaní nebude účinné pokud data obsluha z nedbalosti vymaže a na svou chybu přijde až dodatečně.

1.4 SELHÁNÍ SYSTÉMU

Tento problém spočívá v tom, že veškerá data jsou uložena na jednom disku společně s operačním systémem. Při poškození systému dochází k nutnosti pře instalaci tím i ke ztrátě uložených dat. V tomto případě je řešení jednoduché. Disk rozdělit na dvě části, kdy jednu část disku budeme využívat pro operační systém a druhou pro ukládání dat.

2 ZÁLOHOVÁNÍ DAT

V praxi používáme různé druhy zálohovaní dat, které se od sebe liší četnostní záloh a způsobem ukládání záloh. Důležité je zvolit si správný druh zálohování a to na základě našich potřeb. Především je zde bráno v potaz jak často budeme k datům přistupovat nebo jaká bude délka archivace. V praxi máme tři základní způsoby ukládání dat na různé datové uložiště..

2.1 DATOVÉ ULOŽIŠTĚ

V této kapitole bych chtěl vyjmenovat nejzákladnější datová uložiště jako je pevný disk, flash, DVD. SSD Disk,

2.1.1 Pevný disk

Pevný disk byl představen již v roce 1956 společností IBM. Jedná se o datové uložiště, které se používá k dočasnému nebo trvalému uložení dat. Jedná se o sekundární uložiště, na které se ukládají data pomocí magnetického záznamu. Disk obsahuje kovové nebo magnetické plotny, které jsou potáhnuty tenkou magnetickou vrstvou, hlav a elektroniky. Tyto plotny se otáčejí rychlostí 4.200 ot/min, 5.400 ot/min, 7.200 ot/min nebo 10.000 ot./min. což má velký vliv na rychlost a množství přenesených dat.

Důležitým faktorem je také tzv. hustota dat, kdy se jedná o množství bitů uložených na ploše jednoho palce čtverečného. Dalším důležitým údajem je množství plotem použitých u pevného disku. Data jsou na pevném disku organizována do soustředěných kružnic tzv. stop a povrch je rozdělen do zón a sektorů. Sektor má pevnou délku a to 512 byte.

Pevné disky mají výhodu v tom, že se na ně dá uložit velké množství dat a to v řádech až terabitů. Také jejich spolehlivost je na vysoké úrovni a data se na nich dají skladovat v řádu několika let. Jsou také dostatečně rychlé. Jejich nevýhodou je, že se skládají z mechanických součástek, které rotují vysokou rychlostí a tím může dojít k poškození a poruše disku. Jsou náchylné na případné otřesy a zacházení,

2.1.2 DVD

Jedná se druh optického datového uložiště. Je plně kompatibilní se starším a dnes již skoro nepoužívaným CD. Jedná se o plastový disk o průměru 120 mm a je 1,2 mm tlustý. Data se ukládají na povrch do jedné nebo dvou vrstev, kdy tyto data jsou následně čtena laserovým světlem o délce 660 mm. Nejčastěji je kapacita DVD 4,7 GB nebo 8,5 GB u

dvouvrstvého DVD. Nevýhodou zálohování na DVD je jeho malá kapacita a rychlost čtení a zápisu na DVD. Dávat si pozor musíme také na kvalitu, kdy má podstatný vliv na životnost uložených dat na DVD. Udává se řádově 3 roky a poté hrozí, že uložená data již nebudou použitelná.

2.1.3 FLASH Pamět

Jedná se o programovatelnou a vymazatelnou paměť. Největší výhodou je jeho velká kapacita, malé rozměry, přenosnost. Největší nevýhodou je životnost, která je omezena počtem přepsání části paměti a pomalý zápis. Flasch disk má kapacitu v řádu několika jednotek až desítek GB.

2.1.4 SD Karty

Tyto karty jsou v podstatě FLASCH paměti ve tvaru karty a používají se v zařízeních jako jsou kamery a fotoaparáty.

2.1.5 SSD Disk

Jedná se o stálou paměť s velkou kapacitou a v současné době pomalu nahrazuje pevné disky, kdy jeho největší výhoda je, že neobsahuje mechanické části, má malou spotřebu. Používá rozhraní Sata. A má vysoké přístupové rychlosti. Největší nevýhodou je životnost, kdy v podstatě základ SSD disku tvoří Flash pamět a tak i SSD disk má omezený počet přepsání, kdy se udává životnost reálně cca. 10.000 zápisů. Další nevýhodou je v současné době jeho pořizovací cena za 1 GB v porovnání s pevným diskem.

2.2 NESTRUKTUROVANÉ ZÁLOHOVÁNÍ

Jedná se o zálohování na CD nebo DVD, kdy se na zvolené médium uloží kompletní záloha. Jedná se o nejjednodušší typ zálohování, ale je nevhodný u větších firem, kde se ukládá větší množství rozdílných dat a záloha má tak velký objem a to především z toho důvodu, že chybí informace o uložené záloze.

2.3 PLNÉ ZÁLOHOVÁNÍ ROZDÍLOVÉ

V případě této metody jsou nejprve zálohovaná všechna data. Následně při každé další částečné záloze se porovnají změněné soubory oproti původní záloze a provede se plná záloha. Je to nejjednodušší způsob zálohování, ale má také nevýhody jako je časová náročnost. Má však výhodu v odolnosti. Výhodou je rychlost a jednoduchost obnovy dat po havárii. Plné zálohování se provádí obvykle jednou za týden nebo měsíc.

2.4 ZRCADLOVÉ - PŘÍRŮSTKOVÉ ZÁLOHOVÁNÍ

V tomto případě se nejprve provede úplná záloha dat, ale následně se zálohují ty, které se změnily od poslední zálohy. Tato metoda není tolik náročná na úložný prostor.

Je mnohem rychlejší variantou zálohování dat a také nejúspornější metodou z hlediska náročnosti na úložný prostor. Principem je vytvoření nejprve plné zálohy, poté se zálohují jen data, která se od poslední zálohy změnila. Po určité době se celý tento proces znovu opakuje. U této metody je potřeba mít údaje o provedených zálohách, aby bylo možné stanovit, která data jsou nová, nebo byla změněna. Navíc pokud by došlo k havárii systému a nutnosti obnovit data ze zálohy, je třeba se vrátit k poslední plné záloze, obnovit ji a následně i každou následující přírůstkovou zálohu, což znamená velkou časovou náročnost. Tímto způsobem můžeme obnovovat data až z několika zálohovacích médií. Jednou týdně se provádí plná záloha a poté se denně provádí záloha přírůstků.

2.5 RAID

Jedná se o záložní pole disků. Jde o seskupení více pevných disků do jednoho zdánlivého celku. Toto diskové pole se nám potom jeví jako souvislý disk, od kterého jsou požadovány určité vlastnosti, mezi které se řadí zejména rychlost, spolehlivost a velikost. RAID pole sebou však nese i nežádoucí "vlastnosti", kterými jsou cena, synchronizace hardwaru (ne každá karta a disk je vhodný na RAID) a také skutečnost, že nejlevnější řadiče nebývají právě nejspolehlivější. Doporučuje se sestavovat RAID pole jen z identických disků (výrobce, řada cache, otáčky, firmware), aby výsledný disk mohl dobře fungovat. Díky HOT-SWAP technologii, která je v dnešních moderních RAID polích již implementována, je možné jednotlivé disky za chodu systému vyjmout a měnit. Nevýhodou je, že tato záloha i originál zůstávají na jednom místě, což sebou přináší rizika. Rozlišuje se celkem 7 druhů RAID polí, kterými jsou RAID 0, RAID 1, RAID 2, RAID 3, RAID 4, RAID 5 a RAID 6, navíc ještě rozšíření těchto polí, které jsou kombinací základních.

2.6 ŠIFROVÁNÍ

Uložená data v počítači je potřeba chránit před zneužitím a to především data týkající se chodu firmy nebo citlivých údajů, jako jsou například osobní údaje. Neoprávněné nakládání s těmito daty by mohlo organizaci vystavit nebezpečí postihu nebo finanční ztráty. Z důvodu aby se k takto uloženým datům nedostala nepovolená osoba provedeme zašifrování těchto informací. V počítačových sítích je řešením omezený přístup a to omezení práv uživatelů a fyzické omezení přístupu k serverům. Zásluhou softwarových i hardwarových firewallů je intranet oddělen od internetu. Přístup uživatelů ke svým datům přes internet lze zajistit pomocí virtuální privátní sítě a technologií bezpečného webu.

Data šifrujeme dvěma základními způsoby a to symetricky a asymetricky.

2.6.1 Symetrické šifrování

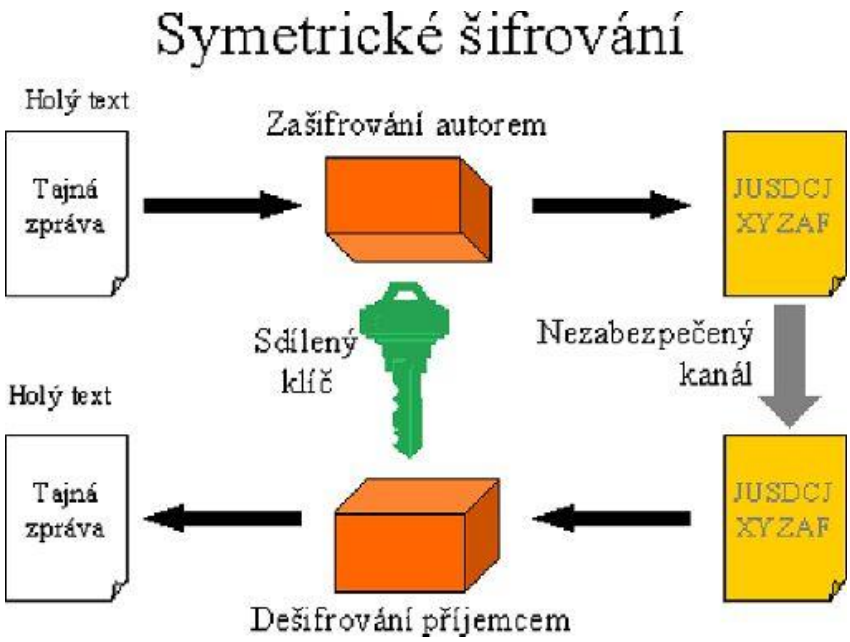
Symetrické šifrování používá pro šifrování i dešifrování stejný klíč. Tento stejný klíč musí mít k dispozici ten kdo data zašifroval i ten kdo data dešifruje. Největší slabinou tohoto řešení je nutnost klíč chránit před neoprávněný užíváním a zamezit přístupu ke klíči neoprávněným osobám. V případě, že klíč se dostane do rukou byť i jediné neoprávněné osobě, tak všechna data, která byla tímto klíčem zašifrována jsou prozrazena. Symetrická šifra tak v určitém smyslu splňuje i autorizační účinek, neboť v případě, že nedošlo k prozrazení klíče tak data mohla zašifrovat tímto klíčem pouze určená osoba.

Mezi nejvíce užívané symetrické algoritmy šifrování patří DES, 3DES, RC2,RC4, IDEA, AES, BlowFisch.

DES používá šifrovací klíč o délce 56 bitů, tento klíč se v současné době považuje již za nedostatečný. Výpočetní technika již pokročila, kdy se zvýšil i výpočetní výkon a tak tato šifra nesplňuje bezpečnostní požadavky, kdy tato šifra byla prolomena dokonce za pomocí hrubého útoku, což je vyzkoušení všech možných kombinací a z tohoto důvodu byl z něj vyvinut algoritmus 3DES, který k šifrování využívá klíč o délce 112 bitů nebo 168 bitů, záleží na tom, kolikrát budou data zašifrována pomocí DES 2x56 nebo 3x56. Oproti desu je pomalejší, ale bezpečnější.

Šifrovací algoritmy RC2,RC4, IDEA, využívají k šifrování algoritmy o délce 128 bitů. IDEA je oproti DES daleko rychlejší, ale v současné době je patentovaný, což brání jeho většímu rozmachu. Dnes je doporučován šifrovací algoritmus AES s délkou šifrovacího klíče až 256 bitů.

Další algoritmus BlowFish, který používá proměnnou délku šifrovacího klíče od 32 do 448 bitů. Nejčastěji se však používá klíč o délce 128bitovým. Je rychlý, bezpečný a není zatížen patentovými právy.



Obr. 1 Symetrické šifrování [22]

Proudové šifry - slouží ke zpracování otevřeného textu po bitech (RC4)

Blokové šifry - dochází k rozdělení otevřeného textu na bloky o stejných velikostech a poslední blok je vhodně doplněn na stejnou velikost (DES, 3DES, IDEA…)

ALGORITMUS DES a 3DES

Byly vytvořeny firmou IBM. Uvedené algoritmy bývají používány v bankovním sektoru s tím, že DES je možné prolomit s pomocí HW dekodérů během několika hodin. U 3DES je délka klíče 168 bitů a je založen na principu šifrování dat buď třikrát stejným klíčem, nebo dvěma či třemi. Tato šifra je dnes stále považována za bezpečnou.

2.6.2 Asymetrické šifrování

Na rozdíl od symetrického šifrování se při asymetrickém šifrování využívá takzvaný klíčový pár, který je tvořen dvojicí klíčů a to klíčem veřejným a klíčem soukromým. Kdy jeden klíč se využívá k šifrování a druhý k dešifrování. Nejznámější algoritmem pro asymetrické šifrování je RSA. Veřejný klíč je volně přístupný a je distribuován všem osobám, se kterými budu komunikovat. Na rozdíl od veřejného klíče musím klíč soukromí chránit.

Základní vlastností při asymetrickém šifrování je zašifrování dat veřejným klíčem, které lze naopak dešifrovat klíčem soukromým, kdy na základě znalosti veřejného klíče je velice obtížné dešifrovat tyto zašifrované data, co bylo zašifrováno veřejným klíčem, lze dešifrovat pouze soukromým a naopak. Jediný klíč nelze použít k zašifrování i opětovnému dešifrování.

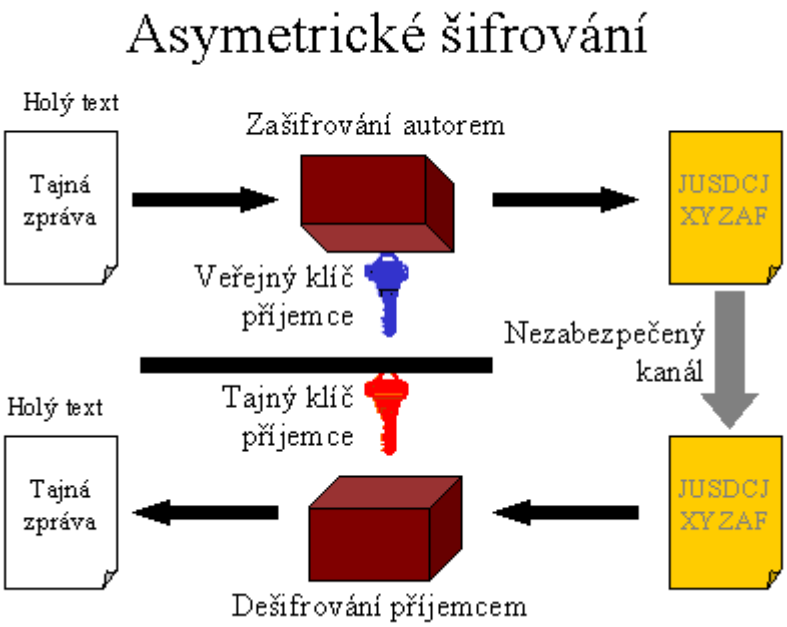
Asymetrické šifrování je v porovnání se symetrickými výrazně pomalejší. Nejčastěji používaný algoritmus je RSA a algoritmy na bázi eliptických křivek.

U RSA, který vznikl již v roce 1977 je pro jeho bezpečnost důležitá délka klíče. Pro vytváření elektronického podpisu se standardně používá klíč s minimální délkou 1024 bitů, kdy často se pro zvýšení zabezpečení používají klíče o velikosti 2048 nebo 4096 bitů.

Prolomení takového klíče závisí na schopnosti systému řešit úlohy faktorizace velkých čísel. Posledním trendem ve vývoji jsou algoritmy na bázi eliptických křivek ECC. Jedná se o algoritmy založené na řešení úlohy diskrétního logaritmu v grupách na eliptických křivkách. Výhodou je, že při dosažení stejné úrovně bezpečnosti jako u RSE o délce klíče 2048 bitů postačí u eliptického klíče 160 až 180 bitů, což přináší značné zrychlení.

V praxi se dále používají i hybridní šifry. Jedná se o kompromis mezi symetrickým šifrováním s jeho rychlostí a bezpečností asymetrických šifer. Pokud bychom totiž využívali pro šifrování bloku dat pouze asymetrický algoritmus, bylo by to pomalé.

Je tedy daleko výhodnější data zašifrovat symetrickým algoritmem a náhodným klíčem, který je vygenerován jako jedinečný pouze pro daný účel, ten následně zašifrovat pomocí asymetrického algoritmu a připojit k zašifrovaným datům. Celý soubor je pak odeslán příjemci, který nejprve dešifruje symetrický klíč a teprve s jeho pomocí samotná data. Takto funguje naprostá většina softwaru používajícího asymetrickou kryptografii.



Obr.2 Asymetrické šifrování [22]

3 SYSTÉM FYZICKÉ BEZPEČNOSTI

Důležitou součástí optimalizace systému objektu patří stanovení principů použitých při návrhu a realizaci. Jedním z nejdůležitějších principů je vícestupňová ochrana, kdy stanovíme stupně fyzické bezpečnosti, které představují určité hranice a oblast, které musí narušitel překonat při postupu k objektu a poté v objektu při cestě k předmětu jeho zájmu.[6]

Základní stupně ochrany jsou:

- perimetrická ochrana
- plášťová ochrana
- prostorová ochrana
- předmětová ochrana

3.1.1 Perimetrická ochrana

Jedná se o bezpečnostní opatření zajišťující bezpečí na obvodu pozemku chráněného objektu. Obvod pozemku je jeho katastrální hranice, která je vymezena přírodními nebo umělými barierami jako je plot, vodní tok, zeď atd.

Účelem perimetrické ochrany je zastrašení narušitele, jeho odhalení a zpomalení. Perimetrická ochrana by měla detekovat a následně signalizovat narušení obvodu ochrany. Detektory, které jsou použité v rámci perimetrické ochrany mají zpravidla delší dosah, jsou vyrobeny z trvanlivějších materiálů a jsou odolné proti přírodním živlům. Mají užší detekční charakteristiku a musí mít větší odolnost proti planým poplachům a to především z důvodu většího počtu pohybujících se předmětů, které se mohou ve volném prostoru pohybovat. Z toho samého důvodu je problematické tuto funkci zabezpečit. V současné době je snaha výrobců konstruovat technické prostředky s komplexnějším zajištěním perimetru. [1]

3.1.2 Plášťová ochrana

Jedná se o bezpečnostní opatření fyzické bezpečnosti na plášti chráněných objektů nejčastěji na chráněné budově. Cílem plášťové ochrany je stejná jako u ochrany perimetrické. Jedná se především o odstrašení narušitele, stižení přístupu do objektu, detekce narušení. Plášťovou ochranu tvoří stěny, okna, dveře, zámky, mříže, bezpečnostní fólie, kamerové systémy, detektory narušení. Detektory použité v rámci plášťové ochrany

se používají především zevnitř budovy. Detektory mají širší charakteristiku a kratší dosah a oproti detektorům používaných při perimetrické ochraně jsou méně odolné proti klimatickým jevům vyjma detektorů určených k použití na vnější straně objektu. Detektory jsou také méně odolné vůči planým poplachům. [1]

3.1.3 Prostorová ochrana

Účelem prostorové ochrany je především detekce narušení a následná signalizace. Dále má za úkol zpomalit narušitele. Instaluje se především uvnitř chráněných objektů a to především na přístupových chodbách, schodištích a na místech, kterým se narušitel při cestě k objektu svého zájmu nevyhne. Systému prostorové ochrany tvoří především systémy kontroly vstupu, poplachové zabezpečovací systémy, detektory narušení. Tyto detektory mají za úkol signalizovat vniknutí narušitele do vnitřních prostor chráněných objektů, jeho pohyb a přibližnou polohu. Tyto detektory mají zpravidla menší dosah a širší detekční zónu. Vzhledem k použití těchto detektorů ve vnitřních prostorách není u nich vyžadována velká klimatická odolnost a musí splňovat požadavky na použití ve vnitřních prostorách.[1]

3.1.4 Předmětová ochrana

Jedná se o soubor opatření mající za úkol přímou ochranu zájmového objektu, kdy se může jednat o cenné umělecké díla, cenné fyzické objekty, finanční hotovost atd. Detektory použité u plášťové ochrany mají zpravidla menší dosah a širokou a plochou detekční charakteristiku. Systém předmětové ochrany tvoří, skleněné vitríny, kamerové systémy, detektory narušení, trezory atd.

Není efektivní v rámci předmětové ochrany vynakládat finanční prostředky převyšující hodnotu chráněných objektů a měla by odpovídat této hodnotě. Také by měla odpovídat možnostem a schopnostem předpokládaného narušitele. [1]

3.2 STUPEŇ NEBEZPEČÍ

Vzhledem k stupni nebezpečí je definován jako schopnosti narušitele a jeho znalosti, dovednosti a technické vybavení,, kdy tyto znalosti může využit k překonání fyzické bezpečnosti. Stupeň zabezpečení včetně poplachového zabezpečovacího systému a detektorů narušení určuje stupeň zabezpečení celého systému, který je dán nejnižším stupněm použitých komponent. [1]

Dle ČSN 50131-1 poplachové systémy rozdělujeme systémy elektronické signalizace do 4 stupňů:

3.2.1 Nízké riziko

Narušitel má malou znalost poplachových zabezpečovacích systémů a velice omezené zdroje a omezenou dostupnost nástrojů, které potřebuje k překonání fyzického zabezpečení.

3.2.2 Nízké až střední riziko

Narušitel má omezené znalosti poplachových zabezpečovacích systémů a má omezené znalosti v používání běžného nářadí sloužící k překonání fyzického zabezpečení.

3.2.3 Střední až vysoké riziko

Narušitel je obeznámen s poplachovým zabezpečovacím systémem a disponuje rozsáhlým sortimentem nástrojů a přenosných elektronických zařízení [1]

3.2.4 Vysoké riziko

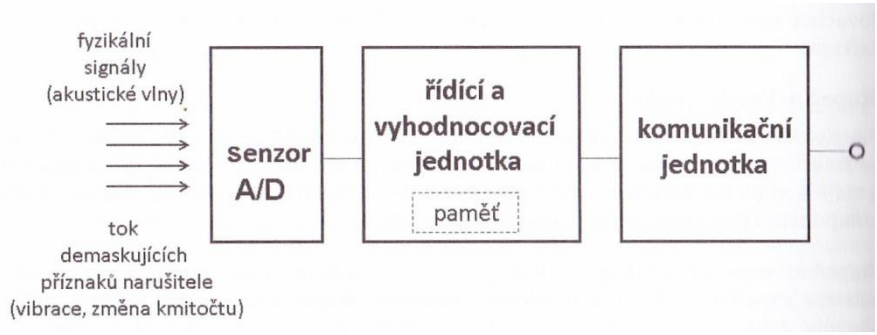
Narušitel má možnost vypracovat podrobný plán vniknutí do střeženého objektu. Je plně vybaven potřebným nářadím a to včetně komponentů potřebných k náhradě systémových částí poplachových zabezpečovacích systémů. [1]

3.3 DETEKTOR NARUŠENÍ

Hlavním úkolem detektoru narušení je zaznamenat a signalizovat neoprávněný vstup narušitele do střeženého prostoru. Jedná se o zařízení určené ke generování signálu nebo zprávy o narušení střeženého objektu, jako reakci na nenormální stav detekující přítomnost nebezpečí. Detektor dříve označován jako čidlo představuje zařízení reagující na změnu fyzikální veličiny jako např. teplota nebo zvukový signál. Změna fyzikální veličiny vyvolá v detektoru vyslání poplachové zprávy. Detektor trvale monitoruje vytyčený prostor a v případě jeho narušení generuje poplach. Úkolem vyvolání tohoto poplachu je informovat, že došlo k narušení objektu, bez dalších doplňujících informacích. K informaci může být doplněna poloha detektoru a tím i místo narušení. Další údaje se získávají jinými způsoby a to například kamerovým systémem. V současné době však jsou na trhu dostupné detektory, které mají v sobě integrované i kamerové systémy a při uvedení detektoru do stavu poplachu tento systém zapne automaticky i kamerový systém, kdy je následně na

ústřednu zaslán i obrazový výstup z tohoto detektoru. Schopnost detektoru rozpoznat narušení střeženého prostoru je dána fyzikálním jevem, který detektor monitoruje. Fyzikální měřená veličina může mít mechanickou, elektromagnetickou nebo akustickou povahu.

Například při snímání signálu, který může vzniknout i z jiných příčin než je narušení prostoru pachatelem dochází k častým planým poplachům. Takový systém je nespolehlivý a neúčinný.



Obr.3 Blokové schéma detektoru narušení. [1]

Detektor tvoří z pravidla senzorická část, řídící, hodnotící a komunikační jednotka. Senzorická část monitoruje snímanou fyzikální veličinu, kdy hodnotu této veličiny převádí na elektrický signál. Dle nastavených hodnot se velikost tohoto signálu vyhodnocuje řídící jednotkou. Součástí senzoru bývá A/D převodník, který zabezpečuje převod analogového signálu na digitální. Řídící jednotka vyhodnocuje charakter a průběh signálu. V případě, že nastane překročení stanovené meze je vyhlášen polach.

K vedení signálu se v současné době nejčastěji používá metalické vedení, rádiových signálů s elektromagnetickým šířením vln.

3.3.1 Rozdělení detektoru narušení

Detektory rozdělujeme dle napájení do základních dvou skupin:

- detektory napájené
- detektory nenapájené

Napájené detektory jak již název napovídá vyžadují ke své činnosti napájecí zdroj. Samotný napájecí zdroj může být zajištěn přímo lokálním zdrojem el. napětí jako je baterie nebo do detektoru může být elektrické napájení přivedeno dálkově z ústředny poplachového systému. Napájené detektory dále rozdělujeme dle způsobu přijímání signálu na:

- pasivní
- aktivní

Aktivní detektory samy vyzařují do prostoru elektromagnetické nebo akustické signály a na základě odrazu a změny kmitočtové charakteristiky tohoto signálu vyhodnocují změny ve střeženém prostoru. výhoda těchto detektorů je jednoznačnost snímaných fyzikálních projevů. Například signál se odrazí od těla narušitele. Nevýhodou těchto detektorů je jejich energetická náročnost a možnost rušení signálů druhých detektorů a tím ovlivnění jejich činnosti. Vzhledem k tomu, že detektor sám vysílá signál je tak snadno detekovatelný a tím i odhalitelný případným narušitelem.

Pasivní detektory na rozdíl od aktivních nevysílají žádný signál. Samy snímají požadovanou fyzikální veličinu jak například teplota nebo akustický signál. Detektory mají tu výhodu, že jsou méně energeticky náročné, hůře se detekují a tím je snížená jejich možnost odhalení. Ve střeženém prostoru může být umístěno více pasivních detektorů bez toho, aby se navzájem ovlivňovaly a rušily. Nevýhoda těchto detektorů spočívá v jejich náchylnosti k planým poplachům a nejednoznačnosti snímaného fyzikálního projevu.

Detektory narušení dále dělíme dle střežené oblasti na:

- prostorové – střeží celý vymezený prostor
- směrové – střežení se provádí v daném směru
- bariérové – snímá narušení nebo překonání bariéry
- polohové – snímá změnu polohy střeženého prostoru

Nenapájené detektory dělíme na:

- destrukční
- nedestrukční

Destrukční detektory jsou pouze na jedno použití, kdy po detekci narušení dojde k jejich zničení

Nedestruktivní detektory můžou provádět detekci opakovaně a nedochází k jejich zničení např. vibrační magnetický kontakt

Dle střežené zóny detektory dělíme na:

- perimetrické
- plášťové
- předmětové
- prostorové

Podle použité fyzikální veličiny dělíme detektory na:

- elektromechanické
- elektromagnetické
- elektroakustické

Elektromechanické detektory narušení využívají k detekci mechanickou změnu, jako je například mechanické chvění nebo vibrace způsobené pohybem narušitele. Tyto změny jsou převedeny na elektrický signál, který má stejný průběh jako snímané vibrace.

Obr.4 Venkovní detektor Risco. [2]

Elektromagnetické detektory využívají k detekci elektromagnetické vlny. Detektor snímá změnu elektromagnetického signálu, kdy detektor může pasivně snímat signál z okolí a poté vyhodnocovat jeho změnu nebo aktivně vysílat elektromagnetický signál a poté vyhodnocovat změnu odraženého signálu.

Obr.5 Bezdrátový magnetický detektor otevření JA-83M. [10]

Elektroakustické detektory využívají ke snímání akustické vlny, které vydává narušitel ve střeženém prostoru, tyto projevy jsou následně přeměněny na elektrický poplachový signál. V detektoru se vyhodnotí změna kmitočtu signálu na elektrický poplachový signál.[1]

Obr.6 Akustický detektor tříštění skla INDIGO [11]

3.3.2 Mechanické spínače

Jedná se o mikrospínače uzpůsobené k tomu aby mohli být zabudované např. do rámu dveří naproti západce nebo jako odpružený hrot, dosedající na vodivé plochy a uzavírající el. obvod.

Tyto spínače, tak střeží uzamčení a uzavření střeženého prostoru a při rozepnutí, které způsobí otevření dveří nebo okna se el. obvod přeruší a tím dojde k vyvolání poplachu.

Nevýhodou těchto detektorů je jejich nízká životnost a nutnost časté údržby. Z tohoto důvodu se již takřka nepoužívají.[1]

3.3.3 Magnetické spínače

Magnetické spínače slouží k bezdotykovému zjišťování polohy zabezpečovacího systému, kdy se nejčastěji využívají v plášťové ochraně jako jsou dveře a okna. V menší míře se využívají i jako předmětová ochrana sloužící zamezení sabotáží např. ústředen, ovládacích krabic atd.

Magnetické detektory jsou tvořeny dvojicí součástek a to jazýčkovými kontakty a permanentním magnetem. V nejjednodušší formě je tento kontakt založen na Reedově senzoru, který je tvořen dvěma vzájemně s překrývajícími se jazýčkovými kontakty, které jsou uloženy ve skleněné baňce o délce 15 až 20 mm a tloušťky 4 mm. V bance je inertní plyn nejčastěji dusík nebo argon.. Jazýčky kontaktu jsou z magneticky měkkého materiálu, které se působením magnetického pole se snadno zmagnetizují. Při umístění jazýčkového kontaktu do magnetického pole permanentního magnetu se oba jazýčky zmagnetizují opačnou magnetickou polaritou a dojde k vzájemnému přiblížení obou jazýčků a tím k sepnutí elektrického obvodu. V případě, že dojde k oddálení permanentního magnetu se magnetické pole oddálí a dojde k odmagnetizování obou jazýčků a jejich vlastní pružností dojde také k jejich oddálení. Tím se el. obvod přeruší a dojde k vyhlášení poplachového signálu. Magnetické detektory se zásadně instalují na nemagnetickém materiálu. Permanentní magnet se instaluje na pohyblivou část a spínací kontakt na pevnou část jako je například rám dveří. Instalace se provádí na křídlo proti závěsům. Při instalaci je také nutno dodržet vzdálenost permanentního magnetu od kontaktů, kdy tato vzdálenost se pohybuje v závislosti od typu mezi 10 až 50 mm. Důležité je také zachovat orientaci magnetu.[1]

3.3.4 Detektory destrukce skleněných ploch

Jedná se o zabezpečení skleněných ploch plášťové ochrany. Nejčastěji se využívají při ochraně oken, prosklených dveří a výkladních skříní. Jejich princip využívá vyhodnocení mechanických změn, které jsou přítomné při destrukci skla. Nejpoužívanější detektory rozbití skleněných ploch se využívají poplachové fólie, tapety a skla dále pak jsou to fóliové polepy a pasivní kontaktní detektory rozbité skla.[1]

Poplachové fólie, tapety a skla lze zařadit mezi pasivní kontaktní destrukční detektory. Princip detekce spočívá v přerušení vodivého prvku, kterým je buď jemný vodící drátek nebo meandr, pokrývající plochu skleněné výplně.

Fóliové polepy je pasivní destrukční detektor. Detekční prvek tvoří tenká hliníková fólie o tloušťce 0,08 mm a šířce 8 až 12 mm. Hliníková fólie je nalepena na postranní části skleněné výplně ve vzdálenosti 50 až 100 mm od okraje rámu. Detekční princip je spočívá v přerušení poplachové smyčky, tvořené hliníkovou fólii, v důsledku destrukce střežené skleněné plochy. Fólie se umisťují tak aby nebyly dostupné z prostoru předpokládaného napadení.

Pasivní kontaktní detektory rozbití skla lze zařadit mezi napájené elektromechanické detektory. Detekčním prvkem je piezoelektrický senzor naladěný na rezonanční kmitočet rozbíjejícího se skla a to na 40 kHz až 120 kHz. Pro vyhodnocování signálu ze senzoru detektoru se využívá porovnání frekvence kmitání piezosenzoru, vyvolaného mechanickým namáháním vyvolaným destrukcí střežené plochy. V detektoru senzoru se porovnává charakteristická frekvence řezání skla a tříštění skla, kdy tato je porovnána a v případě shody senzor vyvolá poplach. Detektor se instaluje 50 mm od spodního rámu okna nebo skleněné výplně a jeho dosah je až 1,5 až 3 m. Výhodou těchto detektorů je jejich nízká citlivost na rušivé zvuky ve střeženém prostoru a to z toho důvodu, že tyto zvuky mají většinou jinou frekvenci než výše popsané řezání a destrukce skla. Tato vlastnost umožnuje monitorování skleněných výplní i v době kdy jsou ostatní detektory ve střeženém prostoru v klidu.[1]

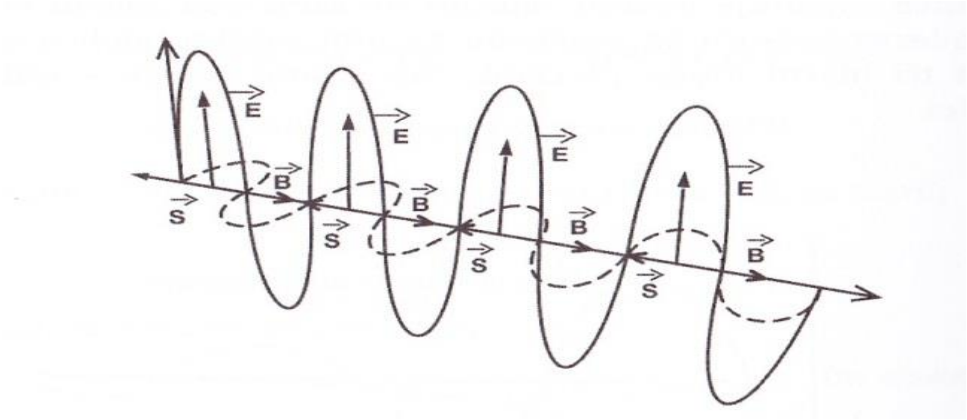
3.4 DETEKTORY POHYBU

Detektory pohybu slouží k detekování pohybu ve střeženém prostoru, kdy k tomuto využívají především elektromagnetického záření a to především oblast rádiovou, mikrovlnou a infračervenou. Dále se v oblasti pohybových detektorů využívají známé jevy jako piezoelektrický jev, pyroelektrický jev, Hallův jev a Dopplerův jev.

3.4.1 Elektromagnetické pole

Je vzájemné působení elektrického a magnetického pole.

Elektrické pole reprezentuje vektor elektrické intenzity E a magnetické pole vektor magnetické indukce B. Oba vektory jsou vzájemně kolmé na směr šíření vlny.[1]



Obr.7 Znázornění el. magnetického pole. [1]

3.4.2 Infračervené záření

Infračervené záření je záření o frekvenci 10^{11} Hz až 10^{14} Hz, což odpovídá vlnovým délkám o délce milimetrů až mikrometrů. Infračervené světlo lze rozdělit do čtyř základních druhů, tak jak je uvedeno v tabulce.

Infračervené světlo	**Vlnová délka**	**Zkratka**
Blízká infraoblast	0,75 μm – 3 μm	NWIR
Střední infraoblast	3 μm – 5 μm	MWIR
Vzdálená infraoblast	5 μm – 15 μm	LWIR
Velmi vzdálená infraoblast	15 μm – 1 mm	

Tab.1 Oblast infračerveného záření. Zdroj [1]

Infračervené záření produkujeme pomocí luminiscenčního, rádiového nebo tepelného zdroje. De- facto každé těleso, které má vyšší teplotu než je absolutní nula je zdrojem infračerveného záření. Těleso vyzařuje teplo.

Při využití infračerveného záření v detektoru pohybu rozdělujeme dvě základní rozdělení a to :

- metoda pasivního snímání
- metoda aktivního snímání

Při pasivním snímání detektor pohybu zaznamenává přítomnost infračerveného záření ve střeženém objektu, kdy toto záření produkuje pohybující se objekt. V tomto případě je detektor založen na principu pyroelektrického jevu. U aktivního detektoru pohybu založeném na infračerveném záření je infračervené záření emitován polovodičovou diodou a zaznamenávám fototranzistorem.[1]

3.4.3 Mikrovlnné záření

Mikrovlnné záření je záření o frekvenci 10^9 Hz až 10^{11} Hz, což je oblast decimetrových až milimetrových vln. Je podobné svými vlastnostmi viditelnému světlu. Tento typ záření se užívá například na ohřev látek, které obsahují vodu. Molekuly vody se při průchodu záření látkou rozkmitají a tření způsobí ohřev. Při detekci pohybu se především používá metoda Fresnerovy zóny a metoda Dopplerova jevu.[1]

3.4.4 Rádiové záření

Rádiové vlny mají frekvenci v rozmezí od 10^3 Hz až 10^{11} Hz. Rádiové vlny dělíme na základě vlnové dělky na

Označení rádiových vln	Frekvenční pásmo (Hz)	Pásmo vlnových délek (m)
Superdlouhé	$< 3.10^4$	> 10 000
Dlouhé	$3.10^4 – 3.10^5$	10 000 – 1 000
Střední	$3.10^5 – 3.10^6$	1 000 - 100
Krátké	$3.10^6 – 3.10^7$	100 – 10
Ultrakrátké	$3.10^7 – 3.10^9$	10 – 0,1

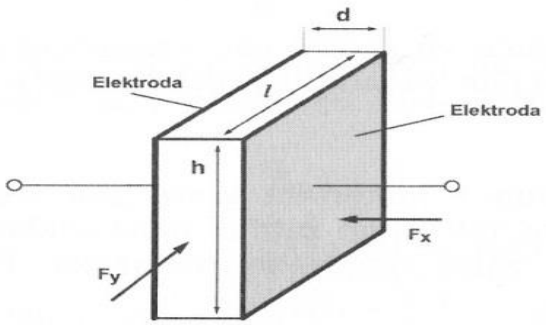
Tab.2 Označení rádiových vln zdroj [1]

3.4.5 Piezoelektrický jev

Piezoelektrický jev se vyskytuje především v důsledku mechanického namáhání, kdy u některých krystalických dielektrik vzniká elektrický náboj. Tento jev se vyskytuje především u krystalů, které jsou středově nesouměrné. Piezoelektrický element se získá vybroušením z krystalu, může být mechanicky namáhán ve směru osy x,y, nebo z.

Vektor polarizace Pe je rovnoběžný s osou x a je úměrný působícímu mechanickému tlaku, pro jeho velikost platí P_e=$k_p p_x$=$k_p \frac{Fx}{Sx}$.

Na každé stěně kolmé k elektrické ose vznikne elektrický náboj. $Q_x = P_e S_x = k_p F_x$

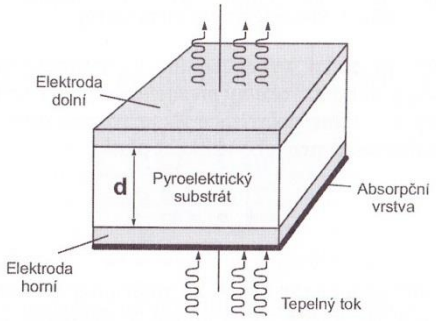


Obr.8 Piezoelektrický jev. [1]

Mechanické namáhaní krystalu ve směru osy z nezpůsobí přenos náboje. Dochází li k přenosu náboje, dochází i k posuvu látky, a proto dochází k deformaci elementu.[1]

3.4.6 Pyroelektrický jev

Pyroelektrický jev se vyskytuje u materiálů, které generují elektrický náboj při zahřátí nebo ochlazení protilehlých míst. Na ose se objeví plošný náboj opačného znaménka. Jako nejpoužívanější materiál je krystal turmalínu.

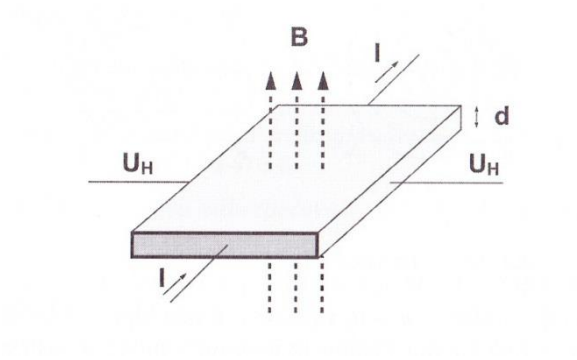


Obr.9 Pyroelektrický jev [1]

Jedná se nejčastěji o tenkou destičku s elektrodami ke snímání indukovaného náboje, který je indukovaný pyroelektrickým substrátem, což je velké množství elektrických dipólů, které jsou náhodně orientované. Pří působení teploty tyto částice ztrácejí dipólový efekt a pokud se tepelný tok šíří ve směru osy z, spodní elektroda bude teplejší a to způsobí rozpínání materiálu spodní elektrody a v materiálu se objeví mechanické pnutí a nastane změna dipólové orientace.[1]

3.4.7 Hallův jev

Hallův jev je založen na vzájemném působení pohybujícího se elektrického náboje a vnějšího magnetického pole. V případě, že se vodič, kterým protéká proud nachází v magnetickém poli jde o pohyb v magnetickém poli a na takovou částici působí Lorenzova síla ve tvaru $F = q.v.B$, kde q je jednotkový nádoj elektronu, v je rychlost pohybu a B udává magnetickou indukci.



Obr.10 Hallův jev [1]

Následkem Lorenzovy síly jsou elektrony vytlačovány k jedné straně vodiče a tím pádem to způsobí přebytek elektronů na jedné straně a na druhé straně nedostatek elektronů. Tím vodičem vznikne příčné tzv. Hallovo napětí, které je dáno vztahem: $U_H = \frac{R_H}{d} BI$, kde R_H

Je konstanta, B udává magnetickou indukci, d představuje tloušťku Hallova elementu a I vyjadřuje proud procházející Hallovým elementem [1]

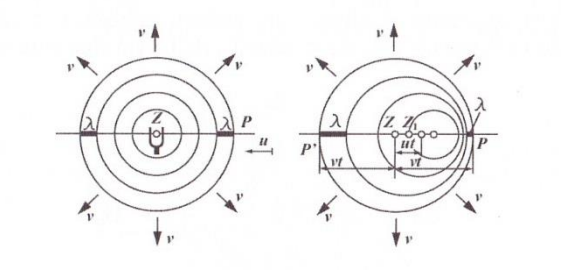
3.4.8 Dopplerův jev

Dopplerův jev popisuje změnu frekvence a vlnové délky přijímaného signálu oproti vysílanému signálu způsobenou nenulovou vzájemnou rychlostí vysílače a přijímače. Je-li zdroj signálu a přijímač v klidu, vlnová délka vysílaného signálu je dána vztahem

$$\lambda = \frac{v}{f_0} = vT.$$

Přijímač, který se pohybuje směrem ke zdroji rychlostí u > 0, přijme signál s frekvencí:

$$f_1 = f_0 + f'' = f_0 + f_0\frac{u}{v} = f_0(1 + \frac{u}{v})$$



Obr.11 Dopplerův jev [1]

3.5 PRVKY PŘEDMĚTOVÉ OCHRANY

Ceniny jako jsou peníze, cenné listiny, šperky se je nutno chránit. K tomuto se využívá především předmětová ochrana. Předmětová ochrana má za úkol zabránit neoprávněným osobám k přístupu k těmto dokumentům a ceninám a také má za úkol registrovat a předávat informace, pokud došlo k narušení střeženého předmětu.. Pro využití předmětové ochrany můžeme využít mechanické zábranné systémy, kdy se jedná nejčastěji o trezory.

Trezory mohou být pevně zabudované do stěny budovy, nebo do podlahy a nebo se může jednat o trezory volně uložené a přemístitelné. Nejčastěji se, ale využívá rozdělení trezorů podle účelu a konstrukce.

K ochraně předmětů se využívají úschovné objekty - úschovné schránky, domácí trezory. Podle určení je lze dělit na úschovné objekty ohnivzdorné a na úschovné objekty bezpečnostní. [19]

Zvláštním druhem trezorů jsou trezory komorové, kdy se jedná o jednu místnost. Trezory jsou bezpečnostní úschovné objekty, které chrání uložený obsah proti násilnému vniknutí a jejich vnitřní rozměry v uzavřeném stavu jsou větší než 1 metr ve všech směrech. Jedná se o samostatné části budov, které mají certifikovanou odolnost proti vniknutí.

Skříňové trezory jsou to úschovné objekty používané především v peněžnictví a bankovnictví. Od komorových trezorů se liší především konstrukcí a velikostí, kdy jedna strana je menší jak 1m. Trezorová skříň má dvouplášťovou konstrukci o různých tloušťkách. Tyto trezory dříve využívaly jako výplň mezi jednotlivými komorami písek nebo popel. Takovéto řešení již dnes neodpovídá bezpečnostním požadavkům. V současné době se jako výplň používá nejčastěji beton. Jednotlivé stěny komory jsou široké 5 až 10 mm a mezery, která je vyplněna je široká 120 až 150 mm. U trezoru s vysokým stupněm ochrany se využívá Relastan, což je směs železobetonu s kovovými prvky nebo pneumatikami. Tato směs zvyšuje odolnost vůči odvrtání a snižuje celkovou hmotnost trezoru. Dle odolnosti rozdělujeme trezory do 3 základních kategorií.

I. kategorie - stěny jsou z ocelového plechu tloušťky 2 až 4mm. Mezera mezi plášti o tloušťce 80mm bývá vyplněna dusaným popelem, nebo jinou výplní jako je písek, keramika nebo sádra. [19]

II. kategorie – stěny jsou z tlustého pancéřového plechu tloušťky 5 až 10mm. Mezera mezi plášti je asi 90 aţ 130mm a je vyplněna betonem nebo železobetonem. Jedná se o nejběžnější vyráběný typ trezorů. [19]

III. kategorie – vnější stěny jsou z plechu tlustého 6 až 8mm a vnitřní stěny mají 3mm. Mezera mezi stěnami je 60 až 100mm a je vyplněna RELASTANEM, Jako složka se může použít i textilie, která při použití hořáku vytváří dusíkaté plyny, které zhasnou plamen hořáku. [19]

Dveře trezoru jsou nejdůležitějším bezpečnostním prvkem. Dveře bývají nejčastěji napadanou část trezoru. Dveře jsou zavěšené v závěsech a mezera mezi stěnou trezoru a dveřmi nesmí přesahovat 0,5 mm a musí být ovládané jednou osobou. Tvoří vstupní část do prostoru trezoru, a proto musí být odolné proti násilnému průniku a odolat požáru. Ve dveřích je uchycen zámek trezoru a závorový systém. Rozměr a tloušťku ocelového plechu a kvality materiálu určujeme podle účelu a použití trezoru. Přední strana trezoru bývá ze železného plátu o tloušťce 8 až 10 mm, ale v prostoru umístění zámku bývá někdy zesílena a doplněna kalenou deskou, tak aby uchránila zámek a prodloužila dobu nutnou k odstranění zámku. Profil dveří může být schodišťový, rybinový nebo kaskádový. Uchycení dveří na skříni trezoru je realizováno dvěma závěsy. Nejlepší umístění závěsů je uvnitř skříně. Zámek se závorovým systémem bývá umístěn uvnitř dveří mimo vlastních zámků a tvoří komplikovaný systém. Závorový systém – kvalita závorového systému charakterizuje bezpečnost trezoru.

Trezor mívá jeden nebo více zámků – jsou to zařízení, která plní blokovací funkci závorového sytému dveří a plní blokovací funkci. V tom případě se využívá dvojice zámků, obvykle dvojice zámku klíčového a heslového, kdy je lze kombinovat. [19]

Klíčové zámky – jsou základním druhem uzamykání dveří trezoru. Nejčastěji se používají zámky s oboustrannými křídly, motýlkové, které mají na klíči po obou stranách zoubky. Dále se používají zámky planžetové, které mají zoubky směrem dopředu a zámky s praporky, které mají zoubky jenom z jedné strany. U trezorů o velké tloušťce dveří, kdy použitý klíč musí mít dlouhý nástavec se používá nastavovací klíč – skládá se ze dvou částí, a to z ovládací části s dlouhým dříkem, a klíče, který se před použitím upevňuje do úchytu na konci dříku. [19]

Ohnivzdorné trezory se zhotovují z ocelových a nehořlavých materiálů, které zaručují vysokou odolnost proti žáru a ohni. Stěny mají dvouplášťovou konstrukci složenou z ocelových plášťů silných 2 až 6mm. a výplň obsahuje ohnivzdorný materiál. Nejčastěji se používá popel, písek nebo Dekalit. Celková tloušťka stěn trezoru a dveří činí 40 až 150mm. Pro úschovu papírových materiálů – poskytují ochranu proti účinkům požáru po

dobu 60 a 120. Vnitřní teplota po tuto dobu nesmí překročit 175^{o}C, jinak by došlo k trvalému poškození uložených cenin.[19]

pro úschovu datových médií – tyto skříně musí vykazovat nejen odolnost proti požáru, ale také musí bránit účinkům magnetických polí. Vnitřní teplota nesmí překročit 55^{o}C a relativní vlhkost nesmí být vyšší než 85 %.[19]

Pro zvýšení bezpečnosti může být trezor vybaven otřesovým detektorem napojeným na bezpečností systém objektu. Takovýto detektor je schopný rozpoznat různé druhy napadení trezoru. Detektory mají široké pracovní pásmo frekvencí otřesů na třech nezávislých pásmech vyhodnocovacích kanálů. Detektor dokáže rozeznat a detekovat použití výbušnin, odvrtání, bourací kladiva, rozbrušovačky a některé dokážou reagovat i na tepelnou změnu způsobenou plamenem hořáku. V případě napadení trezoru vzniká vlnění o specifické frekvenci, které se šíří jako zvuková vlna. Tyto vlny jsou snímány piezoelektrickými snímači, které jsou instalovány uvnitř trezoru. Detektor dokáže vyhodnotit, zda se jedná o rušivé zvuky z prostředí nebo o zvuky, které vydává narušitel.

4 ZÁKONNÉ NORMY

V této kapitole bych chtěl seznámit se zákonnými normami se kterých budu vycházet. Jako nejdůležitější normou je zákon o ochraně osobních údajů, kdy stanovuje pravidla s nakládáním a ochranou osobních údajů. Také se dotýká v nakládání s kamerovým záznamem a to především v § 18, kdy při střežení objektu kamerovým systémem a ukládání takovéhoto záznamu je provozovatel povinen toto oznámit úřadu pro ochranu osobních údajů

Zákon o ochraně osobních údajů č.101/2000 Sb.

V § 3 jsou definovány povinnosti správce jak nakládat s osobními údaji, aby nedošlo k jejich zneužití nepovolanou osobou. Také vymezuje, které osobní údaje může zpracovávat. Je zde definováno jak má s těmito údaji následně nakládat.

Dále v § 13 jsou definovány opatření, které správce a zpracovatel mají za povinnost přijmout, aby nedošlo k neoprávněnému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, jakož i k jinému zneužití těchto údajů. Tato povinnost platí i po ukončení zpracování pojistných událostí.

V paragrafu 14 je uvedeno, aby osoby zpracující osobní údaje na základě plné moci od klientů je spravovali pouze za podmínek a v rozsahu správcem stanovené.

Paragraf 15 upřesňuje oprávnění a povinnosti zpracovatelů těchto údajů, kteří jsou povinni zachovávat mlčenlivost a tato opatření trvají i po skončení zaměstnání nebo příslušných prací.

Paragraf 16 se zabývá oznamovací povinností, kdy je zde upřesněna skutečnost písemného oznámení Úřadu před zpracováváním osobních údajů. Mimi jiné je zde upřesněna povinnost při zřízení kamerového systému uchovávající záznam toto oznámit úřadu pro ochranu osobních údajů. Pokud jsou splněny všechny náležitosti a je elektronicky odeslána žádost o povolení takovéhoto systému, tak Úřad ve lhůtě 30 dnů žadatele vyrozumí. Žádost mimo jiné musí obsahovat identifikační údaje správce, místo zpracování osobních údajů, účel zpracování informací. V § 18 jsou uvedeny výjimky, kterých se oznamovací povinnost dle § 16 nevztahuje.

Zákon o polici ČR č.273/2008 Sb.

Zde bych chtěl především upozornit na § 10, kde je policii ukládána povinnost jednat v případě, že se dozví o možném protiprávním jednání. Tento paragraf zde zmiňuji proto, abych poukázal na zbytečnost napojovat celý zabezpečovací systém na PCO, který by provozovala soukromá bezpečnostní služba. V případě vyhlášení poplachu, kdy uživateli bude doručena SMSka s textem o narušení objektu a uživatel nebude moc sám se na místo v požadovaném časovém horizontu dostavit postačí toto oznámit na linku 158, kde uvede, že objekt firmy byl neoprávněně napaden a z toho důvodu žádá o prověření, zda se nejedná o vloupání. Policie má povinnost na místo vyslat hlídku, která na místě celou věc prověří. Tato povinnost vyplívá z výše uvedeného § 10 odst.1

„*V případě ohrožení nebo porušení vnitřního pořádku a bezpečnosti, jehož odstranění spadá do úkolů policie, je policista ve službě nebo zaměstnanec policie v pracovní době povinen provést úkon v rámci své pravomoci (dále jen „úkon“) nebo přijmout jiné opatření, aby ohrožení nebo porušení odstranil*.“ [4]

PRAKTICKÁ ČÁST

5 ANALÝZA SOUČASNÉHO STAVU

Jako první bych chtěl analyzovat současné elektronické zabezpečení osobních údajů, které firma zpracovává při likvidaci pojistných událostí. Jedná se především o jména, rodné čísla a adresu trvalého bydliště, což jsou údaje upřesněné v zák.č.101/2000 Sb. a to především v § 4. Dále jsou to údaje, které nejsou upřesněné v tomto zákoně, ale také může dojít ke zneužití těchto údajů, kdy se jedná o tel. kontakty a emailové adresy klientů, které můžou být zneužity k odesílání např. nevyžádané reklamy a tím obtěžování klientů firmy a následné ztráty důvěry a porušení zákona o Regulaci reklamy zák. č. 40/1995 Sb.

V současné době je firemní síť zabezpečena firewallem a antivirem Avast. Což je vzhledem k možnostem firmy a charakteru zpracovaných dat dostačující.

Co není, ale dostačující, že osobní údaje uložené na počítači a se kterými se denně pracuje, nejsou chráněná žádným heslem. Jedná se řádově o tisíce klientů, které do současné doby firma zpracovala za 20 let své existence cca.10.000 pojistných událostí. Data jsou v počítači uložena pouze na pevném disku a při odcizení PC jsou tyto data volně dostupná pachateli, který je následně může zneužít ve svůj prospěch. Data nejsou nijak zálohovaná. Jsou uložené pouze v jedné kopii. V případě odcizení by firmě vznikla velká nemajetková újma a to především v tom, že data se denně využívají a jejich ztráta by vedla k průtahům a ztížení práce administrativního pracovníka.

Firma má čtyři administrativní kanceláře a jednu garáž sloužící jako dílna, kde se provádějí samotné opravy. Plastová okna budovy nejsou nijak chráněna a v celé firmě není žádné zabezpečovací zařízení, které by indikovalo případné narušení objektu.

Budova je chráně pouze mechanicky a to uzamykáním hlavních vstupních dveří zámkem FAB a oplocením o výšce 2 m. Do ulice Mrštíkova jsou okna skladu a ředitele vybavena mříží v oknech.

Vjezd do prostor firmy je řešen kovovou bránou, která se uzamyká pouze visacím zámkem.

Veškeré firemní dokumenty jsou ve firmě uloženy volně v dřevěné skříni bez toho, že by byly jakkoliv chráněny.

6 DISLOKACE STAVBY A TRESTNÁ ČINNOST V OKOLÍ

Objekt firmy je situován v obytné části města Hodonína v oblasti zvané Brandlovka, kde se jedná o průmyslový objekt. Tato část se nachází na vyvýšené části města a tak je zde minimalizováno nebezpečí povodní.

Obvodovou ochranu objektu tvoří cihlový plot o výšce 190 cm, který areál objektu odděluje od obytné zóny. Podél severní stěny plotu prochází ulice Nádražní řádek a dále se zde nachází frekventovaná železniční trať s blízkým vlakovým nádražím. Západní stěna cihlového plotu se nachází na ul. Mrštíková. V této části plotu se nachází i hlavní dvoukřídlá brána do objektu, kterou tvoří 190 cm vysoká kovová průhledná konstrukce se svislými tyčemi. Uzamykání brány je vyřešeno pouze nekvalitním visacím zámkem. V okolí objektu jsou především rodinné domy, kde však s jižní části objektu sousedí místní restaurace Jamajka a s tím i zvýšený pohyb osob. Samotný pozemek objektu je obdélník o velikosti 60 x 31 m. V severní části objektu se nachází parkoviště a u východní stěny se nachází dvě budovy garáží., kde samotná firma je umístěná do budovy o rozměru 25 x 14 m, kde stěna budovy je situována do ul. Mrštíkova.

Areál nemá žádné režimové opatření a to z toho důvodu, že garáže ve východní části pozemku má pronajatá firma zabývající se opravou vozidel a tak vzhledem k tomu, že firma má jinou otevírací dobu a jiné provozní nároky, je v objektu v denní době volný pohyb osob.

Samotná budova firmy je jednopodlažní stavba, která bude naším primárním objektem ochrany má jeden hlavní vstup do kanceláří firmy, který tvoří jedny dřevěné dveře se zámkem FAB a druhý hlavní vstup do prostor garáže. Celá budova je rozdělena na dvě části, kdy jižní část budovy je určena jako garáž a severní část budovy je tvořena kancelářemi a sociálním zařízením a šatnou. Kancelářský prostor má 3 okna směřující přímo do ulice Mrštíkova, které jsou chráněná plášťovou ochranou a to kovovými mřížemi. Tyto okna jsou situována do kanceláře majitele a do provizorního skladu materiálu, který se nachází v kancelářských prostorách.

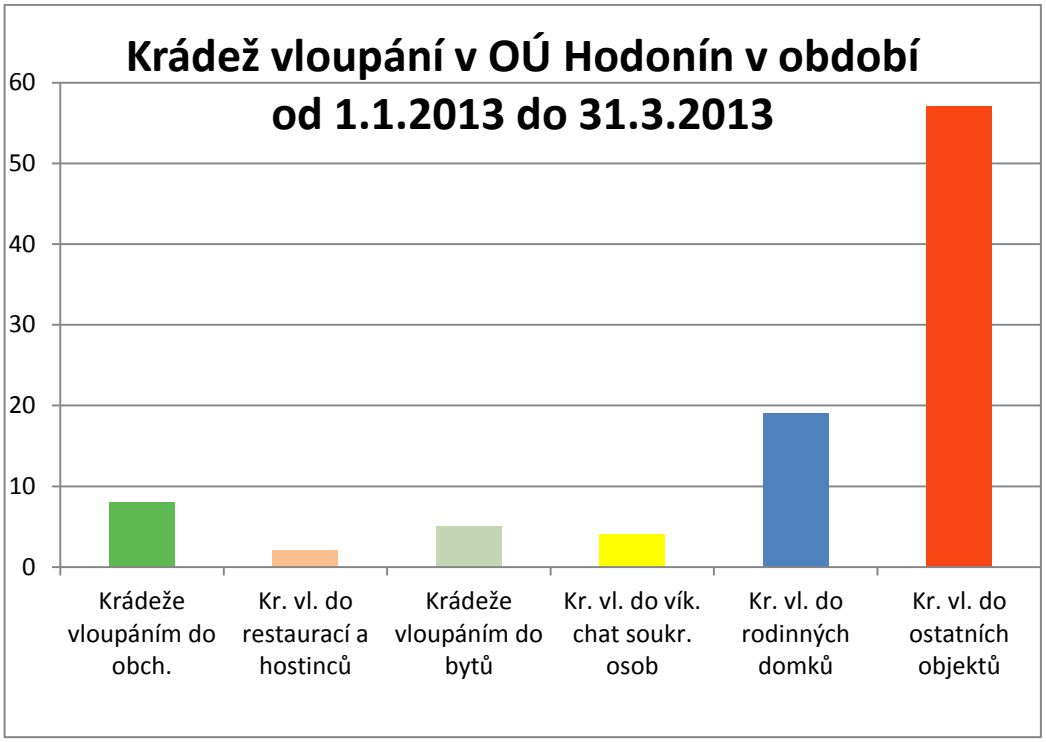
Další dvě okna jsou situována do dvora objektu firmy. Tyto okna nejsou vybavena mříží a jedná se o dvouvrstvá plastová okna, za kterými se nachází administrativní kancelář. V této místnosti bývá uložen počítač s programem, kde jsou uložené kopie pojistných smluv a také jsou zde skladované tyto smlouvy v papírové podobě, které jsou volně uložené v uzamčené dřevěné skříni.

Obr.12 Půdorys firmy [12]

Obr.13 Hlavní příjezdová brána. Zdroj. vlastní

6.1 NÁPAD TRESTNÉ ČINNOSTI

V okolí stavby je z důvodu dislokace takřka v centru města zvýšena majetková trestná činnost, kdy jsou zde zaznamenávány vloupání do firem a obytných budov. Většina vloupání, které jsou prováděná v této oblasti jsou provedena neklasifikovaným způsobem tzn. že pachatelé využívají daného momentu. K vloupání jsou pachatelé vybaveni pouze základním vybavením jako je páčidlo a kleště na odstranění zámků. Jejich primárním cílem vloupání je především finanční hotovost nebo elektronika jako jsou počítače nebo televizory. Takovéto zboží se lehce prodává. Provedení takového typu vloupání je většinou náhodné a pachatelé si svůj cíl typují náhodně, nebo na základě zevrubného ohledání jako zákazníci firmy při otevírací době. Při vloupání pachatelé využívají jenom výše uvedené nářadí, kdy nejsou vybaveni žádnou sofistikovanou technikou, jako je například elektronické vybavení k vyřazení zabezpečovacího systému nebo nástroje na odstranění zámků. Pachatel může být odrazen v takovém případě už jenom přítomností zabezpečovacího zařízení.. V těchto případech lze předpokládat, že primárním cílem vloupání je okamžité získání finanční hotovosti a to buď prodejem elektroniky nebo samotné finanční hotovosti. Jelikož ve firmě Autoglass se veškerá finanční hotovost kromě pracovní doby uschovává mimo prostor firmy a tato hotovost je uskladněna v trezoru na místě trvalého bydliště majitele, tak zde nehrozí finanční ztráta v podobě odcizení hotovosti. Získání elektroniky převážně PC pro firmu představuje ztrátu v řádech tisícikorun, kdy by tato ztráta nepředstavovala žádný výraznější problém. Problém by nastal ve ztrátě uložených osobních dat klientů, které by v tomto případě mohli být zneužity, kdy vzhledem k osobě pachatelů lze předpokládat, že naprostá většina je uživatelem drog a vloupání bylo provedeno jenom z důvodu okamžitého zisku toto PC by bylo obratem prodáno překupníkům a následně tyto data mohou být zneužita. Zde je zneužití dat již značně vysoké a to v případě, že by tyto data nebyla v PC nijak chráněna. Zde lze znovu předpokládat, že překupník, který vykupuje zboží není vybaven takovými znalostmi, aby dokázal svépomoci překonat zabezpečení šifrování a také lze předpokládat, že by nevynaložil neúměrné náklady na prolomení takovéhoto zabezpečení, kdy zisk z takto získaných údajů by nedosahoval samotných nákladů na překonání šifrování. Z toho vyplívá, že by došlo k formátování disků a následný prodej PC, kdy by takto data byla ochráněna před zneužitím. Sice by takovéto řešení nezabránilo samotné krádeži PC nebo NAS , ale spolehlivě by zabránilo zneužití těchto dat a to je hlavní cílem takovéhoto zabezpečení.



Tab.3 Nápad tr. činnosti. Zdroj [13]

Z grafu vyplývá, že počet vloupání do ostatních objektů představuje nejvyšší procento ze všech ostatních vloupání.

7 NÁVRH ZABEZPEČENÍ ELEKTRONICKÝCH DAT

Cílem zabezpečení a zálohování dat v malém podniku je, aby bylo co nejjednodušší a při tom splňovalo účel, který se vyžaduje. Jelikož data, která jsou archivována v elektronické podobě ve firmě Autoglass jsou zároveň uložena i v papírové podobě a firma je ukládá pouze z důvodu případné zpětné reklamace a jednodušší dohledatelnosti, tyto data nemají pro firmu strategický význam. Z tohoto důvodu navrhuji pouze jednoduché a levné řešení zabezpečení, spočívající v serveru NAS, kde budou data ukládána a poté šifrování dat pomocí programu TrueCrypt, který je volně dostupný na internetu. Cílem takovéhoto zabezpečení je, že v případě odcizení PC nebo NAS serveru nedojde k zneužití osobních údajů archivovaných v PC nebo NAS. Samotná ztráta těchto dat nebude mít pro firmu hlubší dopad, protože data se budou dát kdykoliv dohledat v papírové podobě.

Jako základ bych doporučil v podniku vybudovat malou lokální sít a to za pomocí bezdrátové Wi-Fi s routrem. Investice do takovéhoto zařízení je v řádech jednoho tisíce korun. Já osobně bych doporučil zakoupit Wi-Fi router TP-Link-WR1042ND. Tento router je vysoce ceněný i v nezávislých testech . Tento router podporuje standart IEEE 802.11n, rozhraní portů 4x RJ45 LAN, 1x RJ45 WLAN, 1X USB.

Obr.14 WiFi router 802.11b/g/n TP-LINK TL-WR1042ND [14]

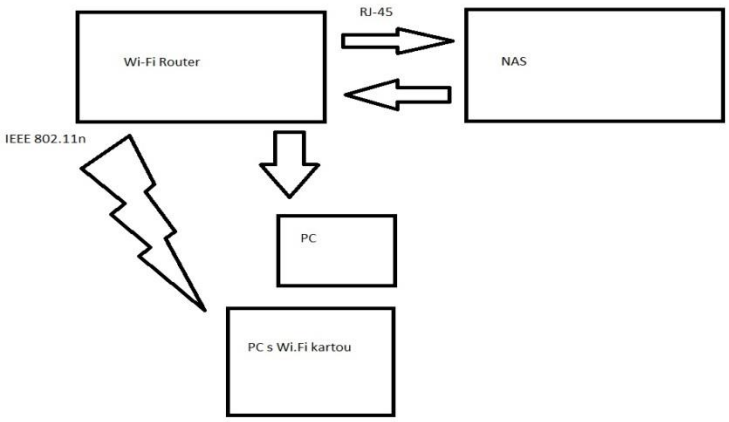
Při nastavení routeru doporučuji nastavit jako zabezpečení WPA 2. Základ domácí sítě je router, kdy vzhledem k malému množství ukládaných dat a jejich následný přenos může být realizován za pomocí bezdrátového přenosu. K routeru připojíme pes rozhraní NAS server QNAP TS-219P2, kdy tento má následující parametry uvedené v tabulece.

Procesor	Marvell 2 GHz (ARM)
Paměť	512 MB DDR3 RAM, 16 MB Flash
Podpora HDD, FS a RAID	2x 2,5“/3,5“ Serial ATA 3 Gbps (Hot-Swap) interní:EXT3,EXT4 externí: EXT3, EXT4, NTFS, FAT32, HFS+ Standard, JBOD, RAID 0 / 1, Online RAID
LAN	1x Gigabitový Ethernet (RJ-45)
USB, apod.	1x USB 2.0 vepředu 2x USB 2.0 vzadutiskový server, data, USB UPS
eSATA	2x eSATA vzadu
Rozměry	168,5 (V) x 102 (Š) x 225 (H) mm
Spotřeba	8 W ve spánkovém režimu 16 W v aktivním režimu (se dvěma disky)
Podpora standardů, apod.	CIFS/SMB (Plus DFS Support) AFP NFS (v3) FTP WebDAV IP Filter Network Access Protection s Auto-blocking HTTP/HTTPS FTP with SSL/TLS (Explicit) SFTP iSCSI Apple Time Machine Remote Replication Server DDNS SNMP (v2 & v3)

Tab.4: Technické parametry QNAP TS. Zdroj Vlastní

Obr. 15 NAS - QNAP TS-219P2 [15]

NAS server připojíme pomocí konektoru RJ-45 s routrem a nastavíme domácí síť. Jelikož tato práce nemá za úkol najít konkrétní řešení, ale jenom vytvořit návrh na řešení celkového zabezpečení a jednotlivé komponenty se mohou lišit, tak se nebudu zabývat jednotlivým nastavením a to z toho důvodu, že každé jednotlivé zařízení se může mírně lišit. NAS server doporučuji vybavit dvěma pevnými disky WD Red o kapacitě 1 TB, kdy tento je určen pro větší zatížení. Celková kapacitě 2 TB je plně postačující k uložení dat.



Obr. 16 Blokové schéma malé podnikové sítě. Zdroj: Vlastní

K šifrování dat uložených na discích NAS bych doporučil využít program TruCrypt.

TruCrypt je volně dostupný program, který využívá různé metody šifrování a může tak uchránit uložená data před zneužitím. K šifrování obsahu disků je možné použít několik algoritmů jako: AES (256-bit), Blowfish (448-bit key), ČÁST5, Serpent (256-bit key), Triple DES, Twofish (256-bit key), případně kaskády těchto algoritmů – například AES-Twofish-Serpent. tyto algoritmy mohou jako „klíč“ využít „klasického“ a různě dlouhého hesla, jako další klíč lze použít tzv. klíčové soubory (keyfiles).

Důležité je také použít dost silné heslo, které případný útočník ihned nevytypuje. Doporučil bych použít kombinaci velkých a malých písmen s číselnou řadou, při délce nejméně 8 znaků. Takové heslo bude dostatečně odolné proti případnému prolomení. Popřípadě může jako klíč posloužit jakýkoliv soubor, kdy zadáme cestu jeho uložení.

Program umožnuje různé také různé nastavení jako je vytvoření skrytého oddílu, který bude bez použití programu takřka neviditelný, ale TrueCrypt jej bude využívat jako datové uložiště.

Takto zabezpečené data jsou pro běžného útočníka nepřekonatelné a v tomto případě jsou data na discích v bezpečí a nehrozí jejich zneužití.

Obr. 17: Prostředí programu TrueCrypt. Zdroj. Vlastní

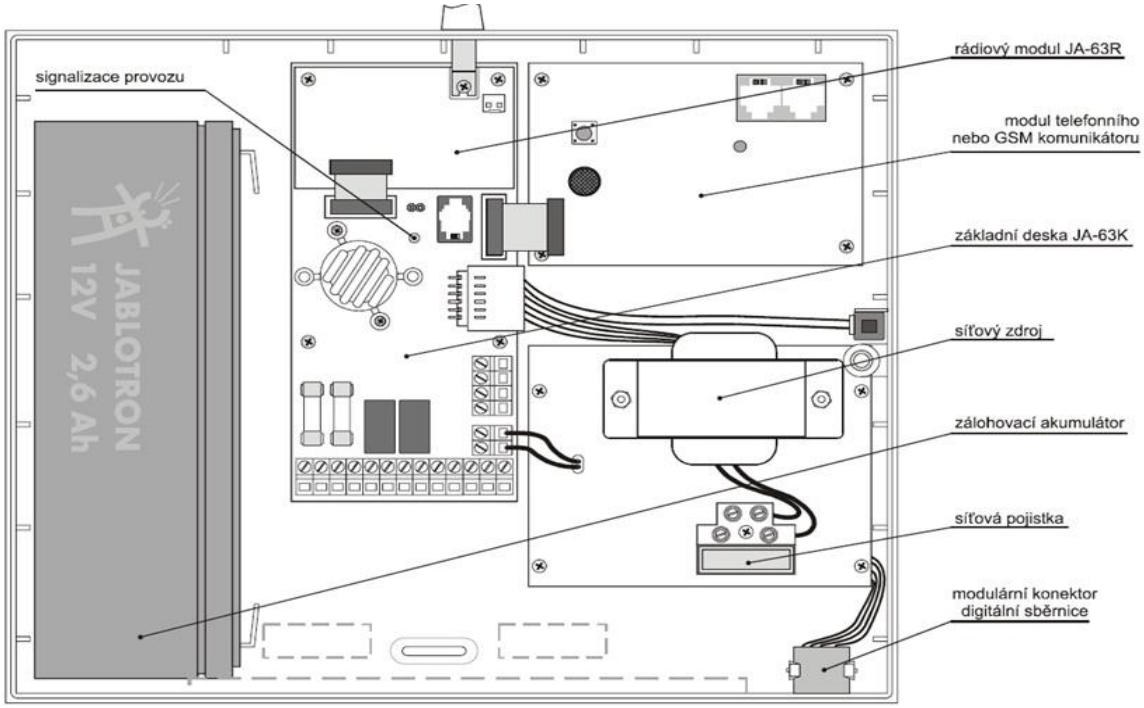
8 ZABEZPEČENÍ OBJEKTU

Jak jsem již popsal objekt je tvořen 5 místnostmi s okny a garáži. Okna, která vedou na ul. Mrštíkova jsou již v současné době vybavena mříží a tím se snižuje možnost jejich překonání. V práci se budu snažit snížit celkové náklady na zabezpečení na řádově několik desítek tisíc, což je částka, kterou je malý podnikatel ochoten investovat. Oslovil jsem 10 malých podnikatelů v mém okolí, kteří se zabývali různým druhem podnikání, kdy firmy měli situované v malých objektech podobných firmě Autoglass. Všichni byli ochotni investovat za EZS částku v rozsahu 30.000 až 50.000,-Kč za zabezpečení, kdy vyšší částka byla mimo jejich možnosti a hlavně se mi je nepodařilo přesvědčit o nutnosti investovat do dražšího zabezpečení, kdy v tomto neviděli návratnost takové investice.

8.1.1 Ústředna

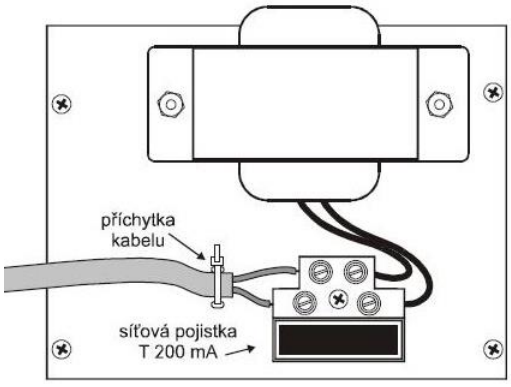
Jako základ pro EZS jsem se rozhodl se použít bezdrátovou ústřednu JA-63KR od společnosti Jablotron. JA-63KR, kdy se jedná čtyřsmyčkovou ústřednu s16 bezdrátovými zónami. Ústředna má čtyři vstupy pro drátové smyčky. Ústředna je v umístěná v plastovém krytu, kdy je zde vyčleněn prostor pro zálohový akumulátor. Ústředna má stavebnicovou koncepci, kdy s ní lze využít zálohový akumulátor o kapacitě 1,3 nebo 2,6 Ah. Ovládání ústředny je možné klávesnicí JA-60F. Ústřednu je možné programovat za pomocí programu ComLink. ComLink je software pro snadné nastavení ústředen JA-6X. V programu lze nastavit například tel. čísla na které má být odeslána hlášení nebo reakci celého systému. Pro propojení ústředny s PC slouží kabel JA-80T, který se zapojuje ke sběrnici ústředny a USB.

Obr.18 Prostředí programu ComLink [20]



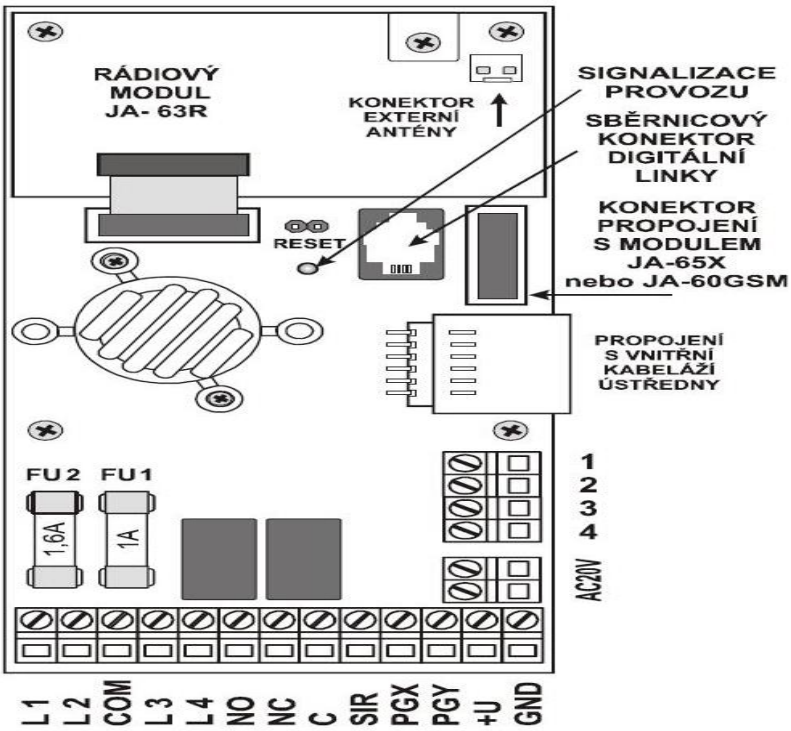
Obr.19 Popis ústředny JA-63KR [3]

Skříň ústředny se montuje na stěnu pomocí 3 vrutů, kdy pro přivedení kabelů jsou zde vylisované vylamovací otvory. Přívod elektřiny lze realizovat za pomocí dvoužilového kabelu s dvojitou izolací. Přívod by měl být zapojen na samostatný jistič s max.10A, který zajišťuje i funkci vypínače.



Obr. 20 Schéma zapojení k síti ústředny JA-63KR [3]

Konektor digitální sběrnice umožnuje připojit klávesnici JA-60 nebo počítač a to za pomocí standartního sdělovací sběrnice. K ústředně je možné připojit až 4 klávesnice. Kabel může být až 100 metrů dlouhý. Kabely delší než 10 m však musí být vedeny kabelem s kroucenými páry.



Obr.21 Schéma zapojení komunikátoru [3]

L1, L2, L3, L4. Vstupům lze v programovacím režimu nastavit způsob aktivace (rozpínací, vyvažovaný 2k2 nebo dvojitě vyvažovaný, vypnutý). Nastavit lze též druh reakce systému

Z výroby nebo po resetu je nastaveno na jednoduché vyvážení a reakce: L1=zpožděná, L2=následně zpožděná, L3=okamžitá a L4=24hodinová.

COM společná svorka pro uzavírání (vyvažování) vstupních smyček

NO spínací kontakt výstupního poplachového relé.

NC rozpínací kontakt výstupního poplachového relé.

C pohyblivý kontakt výstupního poplachového relé, zatížitelnost max. 60V=/1A, relé spíná na nastavenou dobu poplachu (při každém typu poplachu)

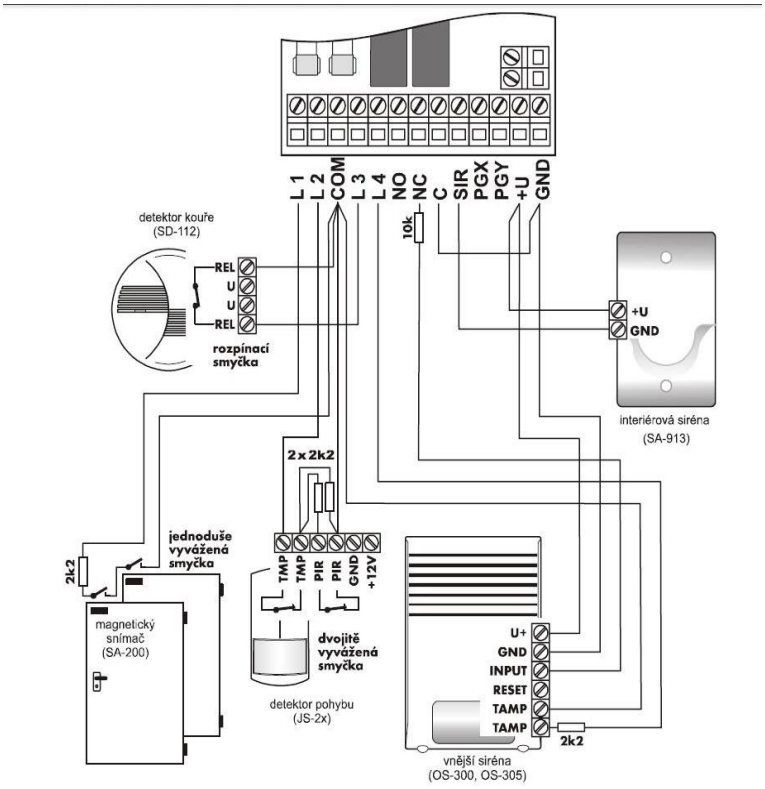
SIR výstup pro sirénu (jištěno pojistkou FU1 1A). V klidu je tato svorka spojena se svorkou +U, při poplachu přepne na GND. Klasickou sirénu zapojte mezi svorky +U a SIR (max. odběr 0,7 A). Dvouvodičovou zálohovanou sirénu zapojte mezi svorky SIR a GND (při poplachu se přeruší dobíjení). Na svorky SIR je též možno nastavit hlasité akustické potvrzování ovládání a testování systému (viz. část 9.19)

PGX je výstupní svorka (spíná na GND, max. 12V/100mA). Funkce tohoto výstupu je nastavitelná (viz. 9.6). Z výroby má funkci předpoplachu (sepnuto během příchodového zpoždění). Stav výstupu PgX ústředna vybavená radiovým modulem předává též bezdrátově pro řízení modulů řady UC.

PGY je výstupní svorka (spíná na GND, max. 12V/100mA). Funkce tohoto výstupu je volitelná (viz.9.6). Z výroby má funkci zajištěno. Stav výstupu PgY ústředna vybavená rádiovým modulem předává též bezdrátově pro řízení modulů řady UC.

+U výstup zálohovaného napájecího napětí pro periferie (jištěno pojistkou FU1 1A). Maximální možný trvalý odběr této svorky je 0,4 A (krátkodobě lze odebírat až 1,2 A – po dobu max. 15 minut – 1x za 1 hodinu). Napětí tohoto výstupu ústředna hlídá a pokud dojde k jeho výpadku, signalizuje poruchu ústředny (porucha C).

GND společný mínus pól napájecího zdroje.[3]



Obr.22 Schéma zapojení ústředny [3]

8.2 PLÁŠŤOVÁ OCHRANA

V objektu se nachází 8 dvoukřídlých plastových oken, kdy navrhuji u oken detektory, které zabezpečí prostor oken po celé délce. Jako řešení se mi jeví zde umístit detektory rozbití skla v kombinaci s PIR detektorem. V současné době existují na trhu duální detektory, kdy firma Jablotron nabízí detektor JS-25 Combo, který nabízí ochranu v podobě prostorové ochrany snímačem PIR a detektorem rozbití skla. Má 3 samostatné výstupy, kdy je zde výstup rozbití skla, pohyb osoby a sabotáže snímače.

PIR snímač zpracovává signál metodou násobné analýzy signálu. Snímač tak dosahuje vysoké citlivosti a odolnosti proti planým poplachům,

Detektor rozbití skla užívá duální metodu, při které se vyhodnocují změny tlaku vzduchu v místnosti, kdy tuto změnu způsobí náraz do okna a následný zvuk vyvolaný samotným rozbitím skleněné tabule. Detektor lze snadno nastavit a zvolit si potřebnou citlivost. Snímač lze namontovat do rohu, ale i na rovnou zeď. Společně s detektorem lze použít nastavovací propojku, která zvýší prostor detekční analýzy. V detektoru lze také nastavit zónu pro pohyb domácích zvířat.

Jeho cena je také velice příznivá, kdy se zde cena pohybuje okolo 800,-Kč.

Specifikace detektoru JS-25 Combo

Napájení: 12 V ss ± 25%

Klidový odběr (bez LED): max.10 mA

Maximální odběr (včetně LED): max. 35 mA

Max. průřez přívodních vodičů: 1 mm2

Zatížitelnost sabotážního výstupu: spínač max. 60 V / 50 mA

vnitřní odpor max. 16 Ohm

Zatížitelnost poplachového výstupu: spínač max. 60 V / 50 mA

vnitřní odpor max. 30 Ohm

Detekční vzdálenost do 9 m

Minimální plocha okenní výplně 0,6 x 0,6 m

Doba stabilizace po zapnutí: max. 60 s

Klasifikace dle ČSN EN 50131-1, ČSN CLC/TS 50 131-2-7-1

stupeň 2 (střední až vysoké riziko)

Prostředí dle ČSN EN 50131-1 II. vnitřní všeobecné

Rozsah pracovních teplot -10 až +40 °C

EMC ČSN EN 50130-4,ČSN EN 55022

Obr.24 Detektor JS-25 Combo [3]

V našem systému bude zapotřebí 7 ks těchto detektorů a to na zabezpečení všech místností s okny a dveřmi.

8.2.1 Siréna

Siréna bude v objektu nainstalovaná z důvodu zvukové signalizace, kdy jak již bylo uvedeno budova se nachází v obytné zóně a siréna tak může případného narušitele odradit od dalšího napadení objektu a může upozorni obyvatele sousedních domů na narušení objektu. Tím může dojít k tomu, že se můžou najít případní svědci, kteří zahlédnou případného pachatele a přispět k jeho odhalení a nebo může být na místo přivolána policie. Jako vhodnou sirénu jsem vybral tyto dva druhy:

OS-350 pro použití na venkovní stěně budovy a poté pro zvýšení akustického efektu pro použití uvnitř budovy bych vybral SA-913 interiérovou sirénu s červeným blikačem.

Siréna OS-350 je venkovní nezálohová siréna vybavena dvojicí sabotážních kontaktů, které detekuji otevření krytu a stržení sirény ze zdi. Siréna je vybavena, také blikajícím světlem, která zaručí optickou signalizaci alarmu. Celá siréna je uzpůsobena použitím ve venkovních prostorách a její tělo tvoří mechanicky odolný plastový obal, který je odolný vůči UV záření, kdy elektronické části jsou lakovány což zvyšuje jejich odolnost vůči vlhkosti.

Technické parametry:

Napájení	10 až 17 V stejnosměrných
Odběr	250mA / 12V
Siréna	piezoelektrická, 112dB
stupeň krytí	IP 34D
stupeň zabezpečení	dle ČSN 50131-1
třída prostředí IV	venkovní všeobecné -25 až 60 °C
rozměry	230x158x75

Obr.24 Siréna OS-350. [3]

Siréna SA-913 je určena pro použití v interiérech a při použití vytváří nesnesitelný hluk, který má také za úkol rozladit útočníka a tím mu podstatným způsobem ztížit orientaci. Je zde také červené světlo, které také může způsobit dezorientaci narušitele a to především v noci, kdy blikající světlo ztěžuje orientaci v prostoru.

Technické parametry

Napájení	11 až 14 V Dc
Odběr	250 mA
Akustický výkon	110 dB/m

Obr.25 Siréna SA-913 [3]

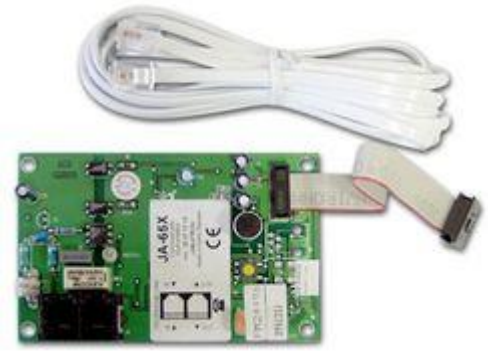
Klávesnice JA-60F umožňuje ovládat systém JA-60 a plně jej programovat. Připojuje se bezdrátově a není za potřebí propojovací kabel. Klávesnici nainstalujeme vedle hlavního vchodu, kde první a poslední zaměstnanec provede odkódování nebo zakódování celého systému. Umožňuje naprogramovaní v master kódu, například telefonní čísla na které bude odesláno hlášení. Manipulace s klávesnicí vede k vyhlášení sabotážního poplachu. Sledován je též počet pokusů o zadání správného kódu.

Klávesnice provádí pravidelně autotest a hlásí svůj stav kontrolním přenosem do systému (ztrátu spojení systém sleduje).

Klávesnici lze též užít ke změnám nastavení ústředny, nebo jako diagnostický prostředek k testování systému.

Obr. 26 Klávesnice JA-60F [3]

Bezdrátový komunikátor JA-63X je určen pro předávání poplachového signálu pomocí hlasové zprávy, zprávy SMS a komunikovat s pultem centrální ochrany. Je schopen odeslat až 5 zpráv SMS na přednastavená tel. čísla. Nejjednoduší je tyto čísla navolit při propojení s PC vybaveným programem ComLink.



Obr.27: Bezdrátový komunikátor JA-63X [3]

Bezdrátový magnetický snímač JA-60N

Bezdrátový magnetický detektor JA-60N je určen k indikaci narušení objektu otevřením dveří a oken. Kromě toho má detektor vstupy pro připojení externích snímačů.

Nežádoucí manipulace s výrobkem nebo snaha o jeho odstranění vede k vyslání sabotážního signálu. Detektor provádí pravidelně autotest a hlásí svůj stav kontrolním přenosem do systému.

Tento detektor využiji především pro zabezpečení hlavních vstupních dveří a dveří od garážových vrat.

Obr. 28 Bezdrátový magnetický snímač JA-60N [3]

Bezdrátový detektor kouře JA-65ST slouží k detekci požáru a nebezpečí požáru. Skládá se ze dvou detektorů a to optického a teplotního. Optický detektor pracuje na principu rozptýleného světla a je velice citlivý na částice, které obsahuj kouř v hustém dýmu. Je však méně citlivý na kouř vznikající z hoření látek jako je alkohol, který má v kouři daleko menší částice. Z toho důvodu je detektor obsazen ještě detektorem teplot, který však nen tak citlivý. Detektor komunikuje bezdrátově a je napájen třemi bateriemi AA. životnost detektoru je asi 3 roky. Pokrytí plochy jedním detektorem je cca.150 m^2

Technické parametry:

Komunikační pásmo	433,92 MHz
Dosah	100m
Citlivost detektoru	m = 0,11 - 0,13 dB/m dle ČSN EN 54-7
Detekce teplot	třída A2 dle ČSN EN 54-5
Poplachová teplota	60 až 70°C

Detektor splňuje všechny potřebné normy dle ČSN EN 54.

Obr.29 Bezdrátový detektor kouře JA-65ST [17]

8.3 ZABEZPEČENÍ DOKUMENTŮ V TIŠTĚNÉ PODOBĚ

Dokumenty, které jsou vytištěné v papírové podobě je nutno také archivovat a to nejlépe v prostoru samotné firmy. Jelikož množství dokumentů za dobu existence firmy přesahuje množství 10.000 složek což je asi 20.000 stran textů, tak je nutné tyto dokumenty uskladnit v kovové skříni. Jako ideální volba se mi jeví spisová policová skříň SPS 02E. A to především cenou, kdy cena nepřevyšuje částku 5.000,-Kč. Skříň bude plně postačovat našemu účelu, kdy se nepředpokládá, že pojistné smlouvy budou předmětem samotného útoku. Skříň je kovová a zabrání základnímu napadení a tak uchrání data před zneužitím. Ukládací prostor této kovové skříně lze přizpůsobit našim požadavkům, kdy takto zde můžeme pohodlně uložit veškeré potřebné dokumenty.

Obr. 30 Spisová policová skříň SPS 02E [18]

Falešná kamera CCD

Dále bych navrhnul na objekt z venkovní strany z ulice Mrštíkova nainstalovat falešné bezpečnostní kamery. Kamery sice nepořizují žádný záznam, ale skvěle poslouží k odrazení případného útočníka, kdy tyto kamery jsou k nerozeznání od kamer plně funkčních.

Pořízení plnohodnotného kamerového systému by bylo finančně natolik náročné, kdy by se takováto investice nevyplatila v vzhledem k rozpočtu celého zabezpečovacího systému a případný obrazový záznam by byl využitelný až v případě narušení objektu a v dalším šetření policie. Pro majitele by funkční kamerový systém neměl prakticky žádný význam. Dále také identifikace pachatele za pomocí venkovních kamer je pro polici obtížná.

V případě, že se útoční rozhodne i přes to, že je v objektu, který je předmětem jeho zájmu je nainstalovaná kamera tento objekt napadnout, tak se ve většině případů bude maskovat, tak aby byla znesnadněna jeho následná identifikace. Před instalací jakéhokoliv kamerového systému se záznamem bychom nejprve měli zabezpečit chráněný prostor jinými stupni ochrany. Kamerový systém se záznamem by měl být poslední stupeň ochrany.

Po instalaci kamerového systému v prostoru objektu musí být toto označeno cedulí a nálepkou a to na viditelném místě.. Nainstalování kamerového systému je vyloučeno v prostorách určených k ryze soukromým úkonům (toalety, sprchy, kabinky na převlékání, atd.).

Zaměstnanci firmy musí být o nasazení kamerového systému na pracovišti průkazně informováni.

Další podmínkou, pokud chci pořizovat kamerový záznam, je registrace tohoto kamerového systému na Úřadu na ochranu osobních údajů, kdy nám toto ukládá § 16 zák.č.101/2000 Sb. Registrační formulář jde vyplnit on-line na www.uoou.czv v registru najdeme formulář *Oznámení o zpracování osobních údajů podle § 16 zákona č. 101/2000 Sb.*

Tyto podmínky a nutné úkony, které musíme provést v případě instalování záznamového kamerového zařízení jsou složité a v našem případě se tak stává instalace kamerového nahrávacího systému zbytečné.

Obr.31 Falešná kamera CCD [9]

Rozmístění bezpečnostních prvků v objektu

Při vstupu do objektu umístíme ovládací klávesnici JA-60F, která bude sloužit k uvedení objektu do stavu střežení a od střežení a to při příchodu a odchodu zaměstnanců do firmy. Z toho vyplívá, že při příchodů zaměstnanců bude nutno nejprve odstřežit celý objekt a poté začít otevírat dveře garáže. Toto, ale nebude žádný problém, neboť zaměstnanci přicházejí do práce v 07:45 hod. a nejprve se převlečou do pracovního oblečení v šatně, která je situovaná v hlavním objektu za hlavními dveřmi. Stejně tak i při odchodu prochází v 17:00 hod. poslední pracovník hlavním vchodem z budovy, kdy při tomto zastřeží celý objekt.

Do kanceláře ředitele, která má okna vedoucí do ul. Mrštíkova, které jsou opatřena mříží umístíme bezdrátový detektor JS-25 COMBO signalizující rozbití okna v kombinaci s PIR detektorem. Tento detektor je bezdrátový a zabezpečí celý prostor kanceláře proti pohybu a rozbití okna. Dále do kanceláře nainstalujeme bezdrátový detektor kouře JA-65ST, který v případě požáru vyvolá poplach. V kanceláři ředitele bude nainstalována i ústředna JA-63KR.

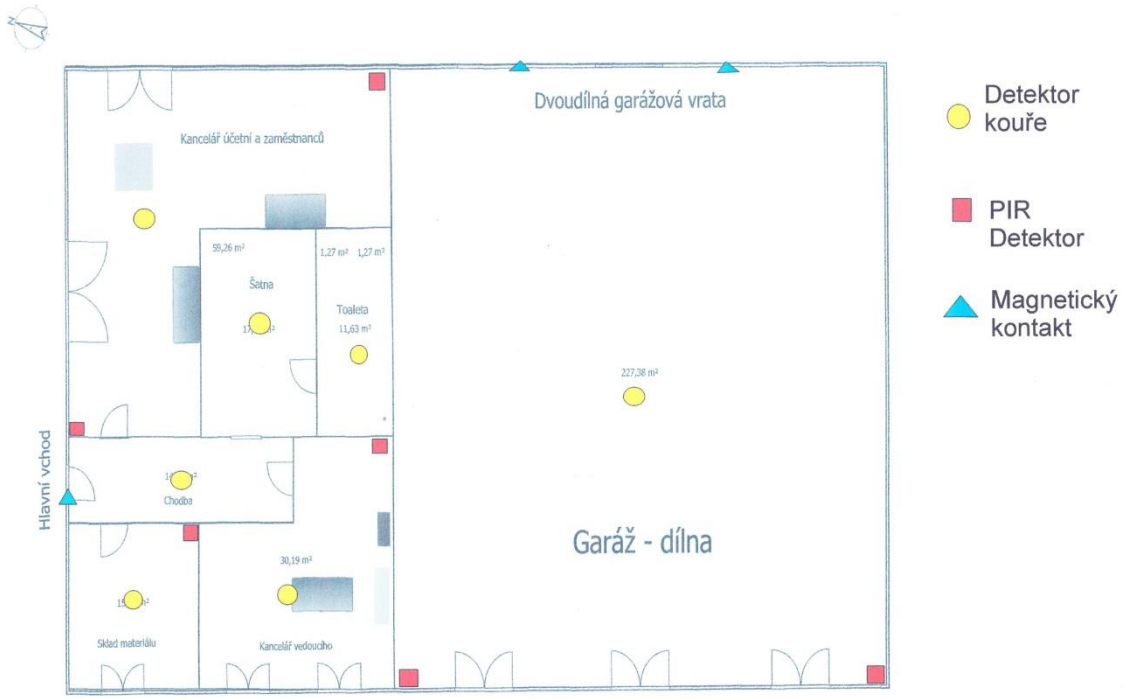
V hlavní přístupové chodbě bude nainstalován bezdrátový snímač kontaktů JA-60N, na chodbě nejsou žádná okna a tak je zde zbytečný detektor JS-25 Combo. Snímač kontaktů bude nainstalován na hlavních vstupních dveří. V případě neoprávněného otevření dveří bude okamžitě vyhlášen poplach. Dále v chodbě bude nainstalován detektor kouře JA-65ST.

V kanceláři účetní budou nainstalovány dva detektory JS-25 COMBO a to z toho důvodu, aby byl pokryt celý prostor kanceláře, která je ve tvaru L a detektor kouře JA-65ST. Místnost je opatřena dvěma dvoukřídlými okny, která vedou do dvora firmy, který je oplocen.

V šatně a na toaletě bude nainstalován pouze detektor kouře JA-65ST a to z toho důvodu, že místnosti nemají žádná okna a jsou dostupné pouze z již zabezpečeného prostoru.

V prostoru skladiště, kdy je zde instalováno okno do ul. Mrštíkové vybavené mříží nainstalujeme bezdrátový detektor JS-25 COMBO signalizující rozbití okna v kombinaci s PIR detektorem a bezdrátový detektor kouře JA-65ST.

Prostor garáže, která zabírá plochu až 230 m^2 bude zabezpečen dvěma detektory JS-25 COMBO, dvěma bezdrátovými snímači kontaktů JA-60N, které budou nainstalována na dveřích garáže a jedním detektorem kouře JA-65ST.



Obr.32 Rozmístění detektorů v objektu. Zdroj. Vlastní

9 CENOVÝ ROZPOČET NA ZABEZPEČENÍ

Celkové náklady na zabezpečení firmy dosáhnou částku 39.395,-Kč s DPH, kdy zde není započítána montáž. Prvky jsem se snažil zvolit bezdrátově, aby se tak snížily náklady na montáž. Cena montáže by neměla přesáhnou částku 4.000,-Kč.

Na zabezpečení dat v el podobě:

1 x Wi-Fi router TP Link TL-WR1042 ND	cena 1.200,-Kč DPH
1 x NAS server	cena 7.200,-Kč s DPH
2 x pevný disk WD Red 1 TB	cena 3.600,-Kč s DPH
Celkem	**cena 12.000,-Kč s DPH**

Cena zabezpečení budovy:

1 x Ústředna JA-63KR	cena 2.930,-Kč s DPH
1 x Klávesnice JA-60F	cena 1.600,-Kč s DPH
1x Komunikátor JA-65X	cena 1.175,-Kč s DPH
6 x Bezdrátový komb. detektor JA-25 Combo	cena 4.620,-Kč s DPH
3 x Bezdrátový magnetický spínač JA-60N	cena 2.500,-Kč s DPH
7 x Bezdrátový komb. detektor kouře a teploty JA65ST	cena 5.900,-Kč s DPH
1 x Venkovní siréna OS-350	cena 870,-Kč s DPH
1 x Vnitřní siréna SA-913FM	cena 280,-Kč s DPH
3 x Falešná kamera CCD	cena 1.000Kč s DPH
Montáž + kabeláž	cena 4.000,-Kč s DPH
Celkem	**cena 27.395,-Kč s DPH**

10 ZÁVĚR

V diplomové práci jsem zhodnotil na základě zadání současný stav a úroveň zabezpečení sídla firmy řešící pojistné události, kdy jsem si vybral firmu Autoglass, která se zabývá výměnou čelních oken v rámci pojistných událostí na vozidlech.

Jako hlavní nedostatek zabezpečení firmy se mi jevila absolutní absence zabezpečení zpracovávaných dat, které se následně ukládaly a to s veškerými osobními údaji o klientech. Data jako rodná čísla, adresy trvalého bydliště, které podléhají zákonu o ochraně osobních údajů č.101/2000 Sb. a s tím možnosti dostat se do rozporu s tímto zákonem při nedostatečné ochraně těchto údajů. Firma také nebyla nijak zabezpečená pomocí EZS. a prostor firmy nebyl nijak střežen.

Jako první jsem navrhnul zabezpečit elektronická data ukládáním na NAS server pomocí malé firemní sítě tvořenou Wi-Fi routrem TP Link. V případě odcizení NAS jsem navrhl data na discích chránit pomocí šifrování za pomoci programu TrueCryp. Takto by uložené osobní údaje v případě odcizení celého NAS nebyly zneužity a došlo by pouze k materiální škodě nikoliv škodě způsobené ztrátou důvěry zákazníka a popřípadě vystavení postihu od Úřadu pro ochranu osobních údajů. Ochranu osobních údajů a jejich uložiště jsem si dal jako hlavní cíl diplomové práce. Samotným napadením firmy by došlo pouze k malým finančním ztrátám a to z toho důvodu, že ve firmě je pouze základní vybavení, kdy se jedná o 2 PC a rádio. Dá se předpokládat, že nábytek nebude cílem útoku. Vzhledem k tomu, že v garáži se provádí základní opravy a výměna autoskel, tak garáž není vybavena žádným drahým zařízením. Finanční hotovost se po pracovní době uchovává mimo firmu.

Vzhledem k absenci EZS jsem navrhnul firmu zabezpečit bezdrátovou ústřednou od firmy Jablotron JA-63KR, kdy k této ústředně jsem navrhnul připojit kombinovaný detektor rozbití skla a PIR detektoru. Tento detektor jsem umístil do všech místností, kde se nacházejí okna a je tak možnost vniknutí do firmy právě okny. Dále jsem zde použil bezdrátový magnetický kontakt dveří, také od firmy Jablotron - JA 60N. Tímto jsem zabezpečil hlavní vstupní dveře a dveře od garáže. Na ústřednu JA-63KR jsem také připojil bezdrátová kombinovaný hlásič požáru JA-65ST, který bude umístěn do všech místností firmy.

K ústředně JA-63KR jsme ještě připojili bezdrátový komunikátor JA-63, který umožňuje při napadení objektu a vyhlášení poplachu odeslat na požadované tel. čísla SMS s vybraným textem a to dle druhu poplachu. V prostoru firmy jsem nainstaloval dvě sirény,

které mají za úkol upozornit o napadení objektu sousedy a to vzhledem k tomu že se jedná o hustě obydlenou oblast a také má ztížit případnému útočníkovi orientaci a to z důvodu světelného blikače a silného hluku.

Ústřednu JA-63KR jsem nepřipojoval na žádný PCO a to z toho důvodu, že jsem využil ustanovení § 10 zák.č.273/2008 Sb o Polici ČR, kdy je zde dána polici ČR povinnost konat v případě, že se dozví o možném protiprávním jednání.

V případě, že majitel firmy poté co obdrží SMSku informujícího jej o napadení objektu, a ten se nemůže na místo dostat v požadovaném časovém horizontu, postačí o této skutečnosti informovat linku 158, která z výše uvedeného ustanovení § 10 musí konat a musí tak na místo vyslat hlídku PČR, která celou situaci prověří, kdy ze zákona má hlídka povinnost se na místo dostavit do 15 minut.

Tím, že jsem ústřednu nezapojil na pult centralizované ochrany, který ve většině případů provozuje soukromá bezpečnostní firma za měsíční paušál jsme takto snížili nutné náklady na vytvoření a provozování takovéhoto zabezpečovacího systému.

Další prioritou mé diplomové práce bylo minimalizovat náklady na pořízení a provozování takovéhoto systému. Myslím si, že celkový rozpočet, který nepřesáhl částku 40.000,-Kč toto splnil. Abychom případného útočníka odradili od napadení objektu, tak je objekt opatřen atrapou kamer CCD. Vzhledem k rozpočtu by funkční kamerový systém byl drahý a v tomto případě neefektivní.

Vzhledem ke způsobu páchání trestné činnosti a to především krádeže vloupáním dle § 205 odst.1 písm.b) tr. zákoníku, kdy tato činnost je v oblasti Hodonína páchána nekvalifikovaným způsobem, kdy se jedná především o drogově závislé pachatele a útoky jsou v naprosté většině provedeny hrubou silou, tak jsem přesvědčen, že takovéto zabezpečení je dostatečné a tím jsem i splnil zadání mé diplomové práce.

Conclusion

In the master thesis I have assessed a current state and level of security in the company dealing with insured events. For this purpose I have chosen company „Autoglass“, which focuses on windscreens changing within car insured events.

An absence of the company security within data processing, which was subsequently saved with all personal information of clients, seemed to me as a greatest weakness. Data as a birth certificate numbers and permanent addresses which are subject of Personal Data Protection Law no. 101/200 and the possibility to be contrary to this law in case of lack of data protection. The company was not secured with EZS as well as not secured company site.

As first I proposed to secure electronic data by saving it on NAS server with a small company network created by Wi-Fi router TP Link. I proposed to have data on discs protected by encryption program TrueCryp in case of NAS stealing. Saved personal data would not be misused in case of NAS stealing and the damage emerging from the theft would have just material character but it would not cause loss of client's confidence as well as any actions made by Office for Personal Data Protection.

I determined the protection of personal data and its storage as a main object of my master thesis. If the company was attacked there would be only small financial losses because the company office is equipped very simply – two PC and one radio. We can presume that the furniture will not be subject of the attack. Considering the fact, that there are made just basic repairs and windscreen changes in the garage, the place is not secured by any expensive devices. The cash is stored only out of the company office after the working hours.

Considering the EZS absence I suggested to secure the company with wireless switchboard from the company Jablotron "JA-63KR" together with connection to combined detector of glass breakage and PIR detector. I placed this detector to all rooms with windows (and where is the possibility to get inside of the company office). Then I used wireless magnetic doors contact, also from the company Jablotron – "JA 60N". In this way I secured the main entrance and garage door. I connected the switchboard JA-63KR to combined fire alarm JA-65ST which will be placed to all rooms of the company.

I connected the wireless communicator JA-63 which enables to send on determined phone number a message with text in case of alarm, to the switchboard JA-63KR. In the company

site I installed there two sirens which can warn about the attack the neighbors because the surrounding area is densely populated and this provision is also supposed to make the orientation of attacker more difficult by the light and sound noise.

I did not connect the switch board JA-63KR to any PCO because I used the regulation § 10 of the law no. 273/2008 on Police of the Czech Republic where is imposed the duty of police to act in case of possible illegal behavior.

In case, that the company owner receives SMS informing him about attack of the company and the owner cannot come to that place in demanded time interval, it is sufficient to inform about this situation the police which is obligated according the regulation § 10 to act and dispatch a patrol which has to check the situation and according the law is obligated to reach the place by 15 minutes.

Since I did not connect the switchboard to the centralized protection panel which is usually run by private security company for monthly-fee I lowered costs necessary to create and run such security system.

Following priority of my master thesis was to minimize expenses for buying and running such system. I suppose, that total budget which did not exceeded amount of 40.000.- Czech crown fulfilled this task. The company area is equipped with camera imitation CCD to discourage a potential attacker from attacking. Functional camera system would be too expensive and ineffective in consideration of the budget.

Considering the way of crime committing and especially burgling as stated in § 205 paragraph 1, letter b) of criminal code, when these crimes are committed in the region of Hodonin in very unqualified way – by drug addicted persons and attacks are mostly made by brute force – I am convinced that this security is sufficient and in this way I fulfilled the assignment of my master thesis.

SEZNAM POUŽITÉ LITERATURY

[1] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011, 316 s. ISBN 978-808-7500-057

[2] LG Group. [online]. [cit. 2013-05-26]. Dostupné z: http://www.lcgroup.cz/divize-elektro/ezs/venkovni-detektory

[3] Jablotron. [online]. [cit. 2013-05-26]. Dostupné z: www.jablotron.cz

[4] Zákon č.273/2008 Sb., O Polici České republiky

[5] HBS Hodonín. [online]. [cit. 2013-05-24]. Dostupné z: www.hbs-hodonin.cz

[6] BRABEC, František. Bezpečnost pro firmu, úřad, občana. 1.vyd. Praha: PublicHistory, 2001, 400 s. ISBN 80-864-4504-6.

[7] VYMĚTAL, Dominik. Informační systémy v podnicích: teorie a praxe projektování. 1. vyd. Praha: Grada, 2009, 142 s. ISBN 978-802-4730-462

[8] FRIEDMAN, George. The intelligence edge: how to profit in the information age. 1 st ed. New York: Crown, c1997, 276 s. ISBN 06-096-0075-3.

[9] Sirius Zlin. [online]. [cit. 2013-05-26]. Dostupné z: www.sirius-zlin.cz

[10] AlarmTec. [online]. [cit. 2013-05-26]. Dostupné z: http://zabezpeceni.obchodnici.eu

[11] AlarSvet. [online]. [cit. 2013-05-26]. Dostupné z: http://www.alarmsvet.cz/

[12] Google. [online]. [cit. 2013-05-26]. Dostupné z: http://maps.google.cz/

[13] Policie České republiky. [online]. [cit. 2013-05-26]. Dostupné z: http://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2013.aspx

[14] Alza.cz. [online]. [cit. 2013-05-26]. Dostupné z: www.alza.cz/

[15] CZC.cz. [online]. [cit. 2013-05-26]. Dostupné z: www.czc.cz/

[16] Zákon č.101/2000 Sb., O Ochraně osobních údajů

[17] Jablotron. [online]. [cit. 2013-05-26]. Dostupné z: http://www.axlelectronics.cz/

[18] Jastcz. [online]. [cit. 2013-05-26]. Dostupné z: http://www.jastcz.cz/kovovy-nabytek/sps-02e-spisova-policova-skrin

[19] VŠB – TU OSTRAVA. *Ochrana objektu - transport peněz, cenin a eskorta osob*. 2008. Dostupné z: www.fbi.vsb.cz/miranda2/export/sites-root/fbi/.../ochrana_objektu.pdf

[20] Zabezpecovacky.cz [online]. [cit. 2013-05-26]. Dostupné z: http://www.zabezpecovacky.cz/

[21] Kryptologie - Univerzita Hradec Králové. [online]. [cit. 2013-05-27]. Dostupné z: http://kryptologie.uhk.cz/54.htm

[22] Elektronický podpis. [online]. [cit. 2013-05-27]. Dostupné z: http://sandbox.cz

SEZNAM ZKRATEK

CCD	Charge coupled device - součástka používaná pro snímání obrazové informace
CMOS	Complementary Metal–Oxide–Semiconductor - používá se na výrobu čipů
ČSN	Česká státní norma
PIR	Passive Infrared Receiver – pasivní infračervený detektor
PPC	Poplachové přijímací centrum
PGM	Programmable ouput – programovatelný výstup ústředny
LAN	Local Area Network – místí počítačová síť
CCTV	Closed circuit television – Uzavřený televizní okruh
DES	Data Encryption Standard – symetrická šifra
3DES	Triple Data Encryption Standard - 3 symetrická šifra
IDEA	International Data Encryption Algorithm - algoritmus o délce 128 bitů

SEZNAM OBRÁZKŮ

SEZNAM TABULEK