Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Technické zabezpečení firmy

Bakalářská práce

2021 Ondřej Linsbauer

Univerzita Pardubice

Fakulta ekonomicko-správní

Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Ondřej Linsbauer**
Osobní číslo:	**E18786**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Téma práce:	**Technické zabezpečení firmy.**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je zhodnotit stávající zabezpečení malé firmy. Na základě analýzy rizik a používaných technických prostředků odhalit případné nedostatky v technickém zabezpečení firmy a udělat nový návrh na zabezpečení movitých věcí a dat.

Osnova:
- Základní pojmy a související legislativa.
- Možnosti zabezpečení dat ve firmě.
- Prostředky technického zabezpečení objektu firmy.
- Analýza stávajícího stavu zabezpečení objektu firmy a firemních dat.
- Identifikace nedostatků
- Návrh možného zlepšení technického zabezpečení firmy.

Rozsah pracovní zprávy: **cca 35 stran**

Rozsah grafických prací:

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

Seznam doporučené literatury:

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

DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

KIZZA, Joseph Migga. *Guide to computer network security*. Fourth edition. Cham, Switzerland: Springer- Verlag, 2017. Computer communications and networks. ISBN 978-3-319-55605-5.

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

Zdroje na internetu.

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

Datum zadání bakalářské práce: **1. září 2020**

Termín odevzdání bakalářské práce: **30. dubna 2021**

L.S.

prof. Ing. Jan Stejskal, Ph.D.	**RNDr. Ing. Oldřich Horák, Ph.D**
děkan	vedoucí ústavu

V Pardubicích dne 1. září 2020

PROHLÁŠENÍ AUTORA

Prohlašuji:

Práci s názvem Technické zabezpečení firmy jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury. Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 29.4.2021

Ondřej Linsbauer v. r.

Poděkování

Tímto bych rád poděkoval vedoucí mé bakalářské práce Ing. Haně Jonášové, Ph.D. za její odbornou pomoc, cenné rady a doporučení, které mi pomohly při zpracování této bakalářské práce. Dále bych chtěl poděkovat své rodině a všem, kteří mě podporovali při tvorbě této práce.

ANOTACE

Bakalářská práce se zabývá technickým zabezpečením malé firmy. Obsahem práce je seznámení s možnostmi zabezpečení firmy, odhalení nedostatků v zabezpečení a na základě analýzy rizik navrhnout možné zlepšení.

KLÍČOVÁ SLOVA

Analýza rizik, hrozba, riziko, nový návrh zabezpečení

TITLE

A technical security of a company

ANNOTATION

This bachelor thesis focuses on the technical security of a small company and includes familiarization with a company's security options and detection of security deficiencies. It proposes possible improvements based on a risk analysis.

KEYWORDS

Risk analysis, threat, risk, a new security proposal

OBSAH

ÚVOD **11**
1 ZÁKLADNÍ POJMY A LEGISLATIVA **12**
1.1 Základní pojmy 12
1.2 Legislativa 12
1.3 Technické normy 13
2 OBVODOVÁ OCHRANA **14**
2.1 Mechanické systémy obvodové ochrany 14
2.2 Poplachové zabezpečovací systémy obvodové ochrany 14
3 PLÁŠŤOVÁ OCHRANA **16**
3.1 Mechanické systémy plášťové ochrany 16
3.2 Poplachové zabezpečovací systémy plášťové ochrany 17
4 PROSTOROVÁ OCHRANA **18**
5 PŘEDMĚTOVÁ OCHRANA **19**
5.1 Mechanické systémy předmětové ochrany 19
5.2 Poplachové zabezpečovací systémy předmětové ochrany 19
6 OCHRANA LIDÍ **20**
7 ZABEZPEČENÍ DAT **21**
7.1 Ochrana fyzického přístupu k nosičům dat 21
7.2 Ochrana logického přístupu k datům 21
7.3 Autentizace 21
7.4 Ochrana uložených dat 22
7.5 Ochrana dat před zničením 22
7.6 Antivirová ochrana 23
7.7 Elektronický podpis 23
8 ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE **24**
8.1 Manuální (tlačítkové hlásiče) 24
8.2 Požární hlásiče automatické (samočinné) 24
9 KAMEROVÉ SYSTÉMY **26**
9.1 IP kamerové systémy 26
9.2 AHD kamerové systémy 26
10 ELEKTRONICKÁ KONTROLA VSTUPŮ **28**
10.1 Přístupové systémy 28
10.2 Biometrické systémy 28

11 ANALÝZA RIZIK 29
11.1 Druhy analýzy rizik 29
11.2 Naložení s rizikem 30
12 POPIS VYBRANÉHO OBJEKTU FIRMY 31
12.1 Základní údaje o firmě 31
12.2 Objekt firmy 31
13 SOUČASNÉ ZABEZPEČENÍ FIRMY 34
13.1 Obvodová ochrana 34
13.2 Plášťová ochrana 34
13.3 Prostorová ochrana 35
13.4 Předmětová ochrana 36
13.5 Ochrana lidí 36
13.6 Zabezpečení dat 36
14 NEDOSTATKY V ZABEZPEČENÍ FIRMY 37
15 NÁVRHY NA ZLEPŠENÍ 38
15.1 Obvodová ochrana 38
15.2 Plášťová ochrana 41
15.3 Prostorová ochrana 42
15.4 Elektrická požární signalizace 42
16 ANALÝZA RIZIK 44
16.1 Neoprávněné vniknutí 45
16.2 Vloupání 46
16.3 Požár 48
ZÁVĚR 50
POUŽITÁ LITERATURA 52

SEZNAM ILUSTRACÍ A TABULEK

Obrázek 1: Analýza rizik 29
Obrázek 2: Objekt firmy XY 32

Tabulka 1: České technické normy.....13
Tabulka 2: Bezpečnostní třídy dveří.....16
Tabulka 3: Náklady na IP kamerový systém 39
Tabulka 4: Náklady na nové oplocení 40
Tabulka 5: Náklady na bezpečnostní fólii 41
Tabulka 6: Náklady na bezdrátový zabezpečovací systém.....42
Tabulka 7: Náklady na elektrickou požární signalizaci.....43

SEZNAM ZKRATEK A ZNAČEK

GDPR	General Data Protection Regulation
EU	Evropská unie
ČSN	Česká technická norma
PIR	Pasivní infračervené čidlo
EPS	Elektrická požární signalizace
HZS	Hasičský záchranný sbor
ZDP	Zařízení dálkového přenosu
LED	Light-Emitting Diode
CO	Oxid uhelnatý
CCTV	Closed-circuit television
PZTS	Poplachový zabezpečovací a tísňový systém
IP	Internet protocol
AHD	Analog High Definition
OZ	Očekávaná ztráta
HA	Hodnota aktiva
PZ	Podíl ztráty
ROV	Roční očekávané výskyty
ROZ	Roční očekávané ztráty
HBO	Hodnota bezpečnostního opatření
RNBO	Roční náklady bezpečnostního opatření
KOPIS	Krajské operační a informační středisko

Úvod

Potřeba ochrany majetku před nebezpečím a s tím spojená signalizace nebezpečí v případě ohrožení bezpečnosti provází lidstvo od nepaměti. Hrozby mohly přicházet jak od nepřátel, tak v podobě přírodních sil (požár, povodeň). S vývojem civilizace se také vyvíjely prostředky sloužící k ochraně majetku, prostředky signalizující možné ohrožení bezpečnosti a systémy monitorující určitý prostor.

V současné době, kdy policejní statistiky vykazují nárust kybernetické kriminality a kriminality v oblasti majetkové trestné činnosti, jsou kladeny neustále vetší požadavky na zabezpečení veškerého majetku a dat. Tato práce se zabývá možnostmi, jak tyto hrozby eliminovat a zároveň představuje prostředky sloužící k zabezpečení objektu. Práce konkrétně představuje prvky obvodové, prostorové, plášťové a předmětové ochrany. Dále se tato práce zabývá možnostmi zabezpečení firemních dat, prostředky tísňové ochrany fyzických osob, elektrickou požární signalizací, kamerovými systémy a elektronickou kontrolou vstupů do zabezpečeného objektu.

Cílem práce je zhodnotit stávající zabezpečení malé firmy. Na základě analýzy rizik a používaných technických prostředků odhalit případné nedostatky v technickém zabezpečení firmy a udělat nový návrh na zabezpečení movitých věcí a dat.

1 ZÁKLADNÍ POJMY A LEGISLATIVA

Právní řád státu tvoří soubor právních předpisu, který obsahuje jednotlivé právní normy. Legislativa je součástí vnějších norem, které musí organizace nebo podnik při svém fungování dodržovat a tvoří tak pro podnik vnější omezení. [18]

1.1 Základní pojmy

Bezpečnost - schopnost odolávat předvídatelným a známým vnitřním nebo vnějším hrozbám. [2]

Riziko - možnost, že nastane událost, kterou z bezpečnostního hlediska považujeme za nežádoucí. [21]

Aktivum - majetek v daném prostředí, který by měl být chráněn. [12]

Hrozba - zdroj nějaké negativní události, osoby, aktivity nebo síly. Hrozba má negativní vliv na bezpečnost, může způsobit ztrátu nebo škodu na majetku. [11]

Hrozby se dělí na [12]:

Objektivní:

- Přírodní, fyzické (např. požár, povodeň)
- Fyzikální (např. elektromagnetické záření)
- Technické nebo logické (např. porucha paměti)

Subjektivní:

- Neúmyslné (např. působení neškoleného uživatele)
- Úmyslné (vnější nebo vnitřní útočníci)

1.2 Legislativa

V právním řádu České republiky není objektová bezpečnost upravena samostatně. Je tedy potřeba vycházet z jiných právních předpisů (zákonných norem). Předpisy související se zabezpečením objektu upravuje Zákon č. 412/2005 o ochraně utajovaných informací a bezpečnostní způsobilosti. Narušení počítačové bezpečnosti je upravováno Zákonem č. 40/2009 Sb. Všechny firmy a instituce, které zpracovávají osobní údaje a data se musí řídit nařízením (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údaj (GDPR). GDPR představuje nový právní rámec ochrany osobních údajů, který je platný na území EU. Jeho cílem je hájit práva občanů EU proti neoprávněnému zacházení s osobními údaji a daty. [10][12][27]

1.3 Technické normy

V České republice a ve většině zemí EU je používání technických norem dobrovolné. Tomu odpovídá právní úprava v ČR stanovující, že česká technická norma není obecně závazná. Existují případy, kdy vyplývá povinnost dodržovat požadavky uvedené v českých technických normách a to nařízením právního předpisu, smluvní dohodou nebo rozhodnutí správního orgánu. Plnění požadavků stanovených technickými předpisy českými technickými normami je jednoznačný způsob, jak prokázat kvalitu zabezpečovacích systémů a celkového zabezpečení objektu. [23]

Českých technických norem je velké množství. Tabulka 1 uvádí příklad některých norem.

Tabulka 1: České technické normy

ČSN EN 54-1	Elektrická požární signalizace - Část 1: Úvod
ČSN EN 50131-1 ed.2	Poplachové systémy – Elektrické zabezpečovací systémy – Část 1: Všeobecné požadavky
ČSN EN 62676-1-1	Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-1: Systémové požadavky - Obecně
ČSN EN 1143-1+A1	Bezpečnostní úschovné objekty - Požadavky, klasifikace a metody zkoušení odolnosti proti vloupání - Část 1: Skříňové trezory, ATM trezory, trezorové dveře a komorové trezory
ČSN ISO/IEC 27033-2	Informační technologie - Bezpečnostní techniky - Bezpečnost sítě - Část 2: Směrnice pro návrh a implementaci bezpečnosti sítě
ČSN EN 1627	Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Požadavky a klasifikace
ČSN 916010	Úschovné objekty. Zkušební metody a klasifikace odolnosti proti vloupání. Skříňové a komorové trezory
ČSN EN 50132-7	Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích – Část 7: Pokyny pro aplikaci

Zdroj: upraveno podle [6][17][26]

2 OBVODOVÁ OCHRANA

Obvodová ochrana představuje prostředky, které zajišťují bezpečnost vymezeného území a prostor okolo chráněného objektu. [16]

2.1 Mechanické systémy obvodové ochrany

Základním znakem mechanických systémů obvodové ochrany je jejich prostorová vzdálenost od chráněného objektu (budova, místnost apod.). Vizuálně označují hranici pozemku a vytvářejí fyzickou i tzv. právní hranici pozemku. Tyto mechanické zábrany mohou být dle potřeby doplněny i monitorovacími a detekčními systémy. [16][24]

Prvky obvodové ochrany tvoří [16]:

- zdi - mají za úkol znesnadnit přelezení nebo podlezení. Zdi musí být pevné, stát na podezdívce a být vysoké minimálně 2,5 m,
- ploty - jsou tvořeny pevnou konstrukcí se sloupky zajištěnými proti vyvrácení a výplní z drátěného pletiva.,
- průchozí prvky zdí a plotů - např. dveře, brány, turnikety a závory. Tyto prvky musí být bezpečně a pevně ukotveny do plotů, zdí a musí mít bezpečný uzamykací systém,
- vrcholová ochrana - tvoří ochranu na vrcholu zdí a plotů. Patří mezi ně konstrukce z ostnatého drátu, žiletkového drátu a pevné hroty na vrcholu,
- visací zámky - jedná se o samostatné zabezpečovací prostředky z hlediska otevíracího elementu se rozlišují visací zámky obyčejné, dozické, motýlkové cylindrické a heslové.

2.2 Poplachové zabezpečovací systémy obvodové ochrany

Tvoří ji prostředky signalizující narušení obvodu střeženého území a prostoru kolem střeženého objektu. Obvod objektu je tvořen katastrální hranicí, která je vymezena umělými bariérami (např. zdi, ploty). [17]

Prvky perimetrické ochrany [16]:

- mikrofonické kabely - využívají se k ochraně drátěných plotů. Mechanická námaha nebo záchvěvy mikrofonického kabelu jsou převáděny na elektrický signál,
- infračervené závory a bariéry - patří mezi nejrozšířenější druh venkovních obvodových čidel. Vysílající a přijímací strany jsou mezi sebou propojeny jedním nebo více infračervenými paprsky,

- zemní tlakové hadice - jsou to hydraulické, tlakové, podzemní čidla tvořená dvěma pružnými hadicemi položenými po celém obvodu pozemku v rozteči 1 metr. Hadice jsou napuštěny nemrznoucí kapalinou reagující na změnu tlaku,
- perimetrická pasivní infračervená čidla - používají se jako doplněk kamerových systémů. Pracují na principu infračerveného čidla (PIR), detekují pohyb zvířat, lidí a dalších objektů.

3 PLÁŠŤOVÁ OCHRANA

Představuje prostředky zabezpečující a zabraňující narušení všech stavebních otvorů objektu. [17]

3.1 Mechanické systémy plášťové ochrany

Tvoří mechanické systémy, které mají za úkol ztížit a prakticky znemožnit vniknutí do chráněného prostoru v objektu prostřednictvím stavebních otvorů. [16][24]

Prvky plášťové ochrany tvoří [16][24]:

- vstupní otvorové výplně (dveře) - skládají se z dveřního křídla, uchycení dveří, zárubně, vrchního dveřního kování, zadlabacího zámku a cylindrické vložky. Evropské normy definují tzv. bezpečnostní třídy dveří, které uvádí Tabulka 2: Bezpečnostní třídy dveří,

Tabulka 2: Bezpečnostní třídy dveří

Bezpečnostní třída	Předpokládaný způsob napadení
RC1	Dveře neodolají ani fyzické síle nebo jednoduchému nářadí. Náhodný zloděj si s nimi bez větších problémů či hluku snadno poradí.
RC2	Dveře odolají příležitostnému zloději, který se pokouší o vloupání s použitím jednoduchého nářadí a fyzického násilí. Zloděj s malými znalosti o odolnosti, který má málo času a snaží se nezpůsobit hluk, dveře nepřekoná.
RC3	Dveře bez problémů odolají zloději, který používá fyzickou sílu i běžné mechanické nástroje. Pokud zloděj nezná složitý systém zamykání dveří, nedostane se skrz.
RC4	Na dveře nestačí ani fyzická síla ani mechanické nástroje. Bez vrtačky a zámečnických nástrojů se přes dveře nedostane ani zkušený zloděj.
RC5	Dveře překoná jen opravdový profík s elektrickou bruskou. Rozhodně se neznepokojuje se způsobeným hlukem.
RC6	Bez dvouručního elektrického nářadí a znalostí se zabezpečovacím systémem dveří si zloděj neškrtne.

Zdroj: upraveno podle [6]

- okna - rámová konstrukce s průsvitnou nebo průhlednou výplní usazené do obvodové stěny objektu. Konstrukčním materiálem (kromě výplňového skla) je kov, plastická hmota, dřevo nebo jejich kombinace,
- mříže - mechanické zábrany zasklených ploch. Dle konstrukce se mříže dělí na pevně kotvené, odejímatelné, otevírací, navíjecí,

- bezpečnostní fólie - snižují riziko násilného vniknutí do objektu a nabízí srovnatelně kvalitní zabezpečení s mřížemi,
- bezpečnostní skla - chrání zasklené plochy otvorových výplní. Bezpečnostní skla se dělí na bezpečnostní skla tvrzená a bezpečnostní skla vrstvená.

3.2 Poplachové zabezpečovací systémy plášťové ochrany

Tvoří ji prostředky signalizující narušení plášťové ochrany budov. Plášťová ochrana zabezpečuje a zabraňuje narušení všech stavebních otvorů objektu (např. dveře, okna šachty). [17]

Prvky plášťové ochrany [16]:

- magnetické kontakty (čidla otevření) - jsou tvořeny jazýčkovým kontaktem a permanentním magnetem. Různé druhy magnetických kontaktů umožňují skrytou nebo povrchovou montáž do oken či dveří,
- čidla na ochranu skleněných ploch - dělí se na kontaktní čidla, která zachycují vlnění vyvolaná rozbíjení skla. Aktivní čidla, která vyhodnocují změny přenosu oproti normálnímu stavu uloženého v paměti čidla a akustická čidla, která vyhodnocují následující akustický efekt při rozbití,
- mechanické kontakty - jsou mikrospínače zabudované do rámu proti západce zámku,
- vibrační čidla - slouží k hlídání průrazu stavebních konstrukcí a stěn. Umisťují se na luxfery, místa možného průchodu zdí, rámy dveří a oken,
- poplachové fólie, skla - pracují na principu přerušení vodivého média uvnitř nosiče (fólie, sklo) nebo pásku vodivé fólie na povrchu hlídané plochy,
- drátová čidla - jemná ocelová lanka propojená s mikrospínačem. Slouží ke střežení prostupů ventilace do objektu.

4 PROSTOROVÁ OCHRANA

Tvoří ji prostředky zabezpečující prostor uvnitř chráněného objektu. Prostorová ochrana je spuštěna po překonání obvodové nebo plášťové ochrany vniknutím neoprávněné osoby do vnitřních prostor objektu. [17]

Prvky prostorové ochrany [16]:

- pasivní infračervená čidla - jsou označována jako PIR čidla (passive infra red senzor). Zachycují změny vyzařování v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění. Zorné pole senzoru je závislé na provedení optiky a dosah senzoru na kvalitě optiky čidla. Volba optiky umožňuje střežit rozsáhlé prostory do cca 60 m nebo méně rozsáhlé prostory do vzdálenosti cca 15 m. Kruhovým uspořádáním optiky lze u čidel pro stropní montáž zachytit velkou plochu v rozsahu 360°,
- ultrazvuková čidla - jsou o označována jako US čidla (ultrasonic sensor). Využívají části spektra mechanického vlnění. Vysílač vysílá vlnění o stálém kmitočtu a přijímač přijímá odražené vlnění od překážek. Dosah ultrazvukových čidel je cca 10 m a umisťují se do uzavřených prostor. Měly by být instalovaná tak, aby pohyb pachatele směřoval k čidlu (radiálně),
- mikrovlnná čidla - označují se jako MW čidla (microwave sensors). Pracují na stejném fyzikálním principu jako čidla ultrazvuková. Podobně jako ultrazvuková čidla by se i mikrovlnná čidla měla instalovat tak, aby pohyb pachatele směřoval k čidlu (radiálně),
- kombinovaná (duální) čidla - využívají se v prostorách s obtížnými podmínkami a nabízí se kombinace pasivních infračervených a ultrazvukových čidel nebo pasivních infračervených a mikrovlnných čidel. Aplikace dvou druhů čidel pracujících na odlišných fyzikálních principech snižuje riziko spuštění falešného poplachu.

5 PŘEDMĚTOVÁ OCHRANA

Jedná se o prostředky, které slouží jako bezpečnostní úschovné objekty. Využívají se pro úschovu finanční hotovosti, cenností, cenných papírů, dokumentů apod. [16]

5.1 Mechanické systémy předmětové ochrany

Prvky předmětové ochrany tvoří [24]:

- skříňové trezory (mobilní a vestavěné) - chrání svůj obsah proti vloupání. Nejčastěji jsou vyrobeny ze speciálních slitin nebo z oceli,
- ohnivzdorné skříně - jsou vyrobeny z ocelových a nehořlavých materiálů, které zajišťují bezpečnost uložených věcí a odolnost proti ohni,
- příruční pokladny - jsou uzamykatelné kovové (plechové) pokladny. Využívají se na drobné platby,
- manipulační schránky - mají nižší bezpečnostní úroveň. Jsou určeny ke krátkodobé úschově cenností a hotovosti.

5.2 Poplachové zabezpečovací systémy předmětové ochrany

Tvoří ji prostředky signalizující neoprávněnou manipulaci s chráněným předmětem (např. úschovná místa - trezory). [17]

Prvky předmětové ochrany [4][16]:

- kapacitní čidla - slouží k indikaci doteku nebo přiblížení ke chráněnému předmětu,
- tíhové detektory - reagují na změnu tíhy, kterou působí předmět na detektor,
- akcelerační detektory - případnou manipulaci s chráněným předmětem detekují pomocí nenulového zrychlení detektoru.

6 OCHRANA LIDÍ

Tvoří ji prostředky tísňové ochrany signalizující zdravotní problémy či ohrožení života fyzických osob. Signalizace může být vyvolána definovaným způsobem manipulace (nášlapná tísňová lišta), manuálně (stisknutí tlačítka). [17]

Prvky tísňové ochrany [16]:

- veřejné tísňové hlásiče - jsou to mikrospínače nebo magnetické kontakty zapouzdřené do formy tlačítka,
- speciální tísňové hlásiče - jsou podobně jako veřejné tísňové hlásiče mikrospínače nebo magnetické kontakty zapouzdřené do formy nožní spínací lišty či tlačítka,
- osobní tísňové hlásiče - jsou bezdrátové hlásiče provedením podobné dálkovému ovládání, malým pagerům, náramkům nebo přívěskům. Nejsou tedy vázané na jedno stálé pracovní místo.

7 ZABEZPEČENÍ DAT

Informační systémy využívají jisté báze dat. Data jsou uložena v souborech na disku, v tabulkách databází, převáděna na papír a rozesílána poštou nebo rozesílána elektronickou poštou. Důvěrná data by neměla být přístupná všem lidem a je nutné je chránit proti třem druhům nebezpečí [8]:

- zničení - ochrana dat proti neúmyslnému a úmyslnému zničení,
- modifikace - ochrana dat proti neoprávněné změně,
- kompromitace - ochrana důvěrnosti dat před prozrazením.

7.1 Ochrana fyzického přístupu k nosičům dat

Data jsou vždy uložena na nějakém nosiči a přístup k těmto nosičům by měl být omezený. Ochranu přístupu k datům má na starost operační systém, který zajišťuje, aby se k datům nedostal nikdo, kdo nemá oprávnění se k nim dostat. Problém nastává v okamžiku, kdy je nosič odcizen z přirozeného prostředí do prostředí cizího s jinými přístupovými právy. Dalším důvodem k zajištění fyzické bezpečnosti je možnost zničení dat útočníkem, požárem a podobně. [8]

Nosiče je tedy nutné ochránit proti dvěma druhům nebezpečí [8]:

- ochrana proti neoprávněným osobám - k nosičům dat by měli mít přístup pouze ty osoby, které přístup potřebují ke své činnosti. Místnost je potřeba zajistit vhodnými prostředky, aby se k nosičů nedostal nikdo neoprávněný,
- ochrana proti přírodním živlům - nosiče dat by měli být uloženy v prostředí, které přírodní katastrofy co nejméně poškodí. K ochraně se využívají požární čidla a umístění systémů do vyšších pater mimo dosah velké vody.

7.2 Ochrana logického přístupu k datům

Operační systém svými prostředky chrání přístup k uloženým datům na discích. Hlídá, aby k nim neměl přístup uživatel bez potřebných přístupových práv. Systém musí vyžadovat dostačující důkaz o identitě uživatele. [8]

7.3 Autentizace

Autentizace slouží k identifikaci uživatele. Tato služba poskytuje systém se schopností ověřit, že uživatel je ten, za koho se vydává. Před autentizací musí proběhnout identifikace, kdy

uživatel prohlásí, kdo vlastně je. Dále provede autentizaci, kdy své tvrzení prokáže. Důkaz začíná získáním autentizační informace od uživatele. [8][15]
Na výběr máme tři metody nebo jejich kombinaci [8]:

- důkaz znalostí - uživatel zadá své heslo,
- důkaz vlastnictvím - uživatel vkládá do čtečky bezpečnostní předmět,
- důkaz vlastností - uživatel se prokazuje jedinečnou tělesnou vlastností, například otiskem prstů.

Autentizační protokol použije získanou informaci k přesvědčení serveru o pravé identitě uživatele. Poté je uživateli přidělena v systému virtuální identita a začíná pracovat systém pro řízení přístupů. [8]

7.4 Ochrana uložených dat

K ochraně uložených dat se využívá kryptografie zabývající se návrhem šifrovacích algoritmů. Úkolem kryptografie je zajistit důvěrnost chráněných dat. Nepovolaná osoba nesmí mít možnost přečíst data chráněná kryptografickými prostředky. [8]
Možnosti použití kryptografie v oblasti ochrany uložených dat [8]:

- off-line šifrování vybraných souborů - do systému je nainstalován program, který je určený k zašifrování požadovaných souborů. V krajním případě mohou být použity například kompresní programy typu PKZIP nebo ZIP, které jsou vybaveny jednoduchým šifrováním,
- online šifrování všech souborů - šifrovací program je nainstalovaný do operačního systému. Šifruje všechny soubory podle nastavených kritérii. Například soubory uložené v chráněné složce nebo soubory, které jsou odesílány elektronickou poštou,
- šifrovací disk - do operačního systému je naistalován ovladač, který šifruje všechen tok dat směřující na disk.

7.5 Ochrana dat před zničením

Data mohou být zničena dvěma způsoby, buď jsou smazána či poškozena na nosiči, nebo je nosič fyzicky zlikvidován. Základní ochranou proti zničení dat je jejich systematická záloha. Zálohování je mechanismus, při kterém jsou vybraná data uložena na jiné médium. V případě, že je zničeno první médium jsou data obnovena ze zálohy. Zálohování by se mělo provádět pravidelně a co nejčastěji. Existují systémy, které zálohování provádějí automaticky, dokážou stáhnout potřebná data, zašifrovat je a uložit na záložní médium. Umějí data také zálohovat inteligentně, to znamená, že jsou ukládána pouze data, která se změnila od poslední zálohy. [8]

7.6 Antivirová ochrana

Ochrana počítačů proti virům. Antivirový systém je potřeba správně nakonfigurovat (testování příchozích souborů, pravidelné testování, odesílání hlášení správci) a pravidelně aktualizovat. Antivirus by měl být nainstalován na pracovních stanicích, proxy i na poštovním serveru. S antivirovou ochranou souvisí pravidlo záplatování systému. Většina virů používá bezpečnostní díry, které jsou už známé a existují na ně výrobci oficiálně vydané záplaty. Záplatování není jen ochrana proti virům, chrání také počítač proti hackerským útokům. [8]

7.7 Elektronický podpis

Jsou specifická data, která nahrazují v počítači vlastnoruční podpis. Elektronický podpis je vytvořen pro konkrétní data (např. text). Pomocí počítače je možné ověřit, jestli je platný. Pro vytvoření elektronického podpisu se využívají asymetrické šifrovací algoritmy. Odesílatel si zvolí soukromý klíč a příslušný veřejný klíč. Veřejný klíč zveřejní, aby ho měli příjemci k dispozici, a soukromý klíč si bezpečně uschová. Odesílatel vytvoří otevřený text, který zkopíruje a jeho kopii zašifruje pomocí svého soukromého klíče. Poté odesílatel zašle příjemci původní otevřený text i zašifrovanou kopii otevřeného textu. Příjemce obdrží zašifrovanou kopii i původní otevřený text, zašifrovanou kopii otevřeného textu dešifruje pomocí veřejného klíče odesílatele. Tím získá otevřený text, který porovná s původním otevřeným textem. Pokud jsou oba texty stejné, pak nemohlo dojít k modifikaci otevřeného textu. [12]
Elektronický podpis zajišťuje bezpečnostní funkce [12]:

- autenticita - ověření identity jedince, který elektronický podpis vytvořil,
- integrita - ověření, že nedošlo ke změně v podepsaném dokumentu od vytvoření elektronického podpisu. To znamená, že dokument (podepsaný soubor) není úmyslně či neúmyslně poškozen,
- nepopiratelnost - autor nemůže tvrdit, že nevytvořil elektronický podpis příslušný k dokumentu,
- časové ukotvení - elektronický podpis může obsahovat časové razítko, které prokazuje čas a datum podepsání dokumentu.

8 ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE

Elektrická požární signalizace (EPS) je soubor technických zařízení, které slouží k detekci požáru a následné signalizaci prostřednictvím hlásičů požáru. Signály z těchto hlásičů jsou přijímány ústřednou EPS. U ústředny EPS musí být zajištěna stála obsluha, která v případě požáru upozorní jednotku hasičského záchranného sboru (HZS). V případě, že není zajištěna 24 hodinová obsluha, je systém EPS připojený zařízením dálkového přenosu (ZDP) k centrálnímu dohledovému pultu příslušného (HZS). [5][17]

8.1 Manuální (tlačítkové hlásiče)

Jsou určené k vyhlášení poplachu osobou, která zjistí požár. Manuální hlásiče jsou vždy červené barvy. U manuálních hlásičů musí být zajištěno, aby nedošlo k náhodné nebo samovolné aktivaci, což bývá docíleno tím, že k aktivaci hlásiče je potřeba rozbít sklíčko. Tlačítkové hlásiče bývají nejčastěji umístěny na únikových cestách, u výstupů z těchto cest, do míst se stálou obsluhou nebo do míst pohybu osob. [16]

8.2 Požární hlásiče automatické (samočinné)

Slouží k monitorování určitého fyzikálního nebo chemického jevu, reagují na něj a informaci předávají do požární ústředny. Automatické hlásiče reagují na původní jevy požáru, kterými jsou nárust teploty, kouř, plameny. Nejvíce používány jsou bodové hlásiče, které se nejčastěji instalují na strop. Plocha pokrytí hlásičem je omezena, proto se ve větších místnostech využívá větší počet hlásičů, aby pokrytí prostoru odpovídalo stanoveným požadavkům. [16]
Druhy automatických hlásičů [16]:

- teplotní hlásiče - v případě překročení určité teploty předají teplotní hlásiče elektrický signál ústředně EPS, která vyhlásí poplach. Nevýhodou teplotních hlásičů je nastavení nízké nebo vysoké prahové teploty. V případě, kdy je prahová teplota nízká, může dojít k falešným poplachům při nárustu teploty z jiných důvodů než je požár. V případě, kdy je naopak prahová teplota nastavena vysoko, dochází k ohlášení požáru pozdě,
- optické hlásiče kouře - využívají optickou vazbu mezi fotodiodou a pulzující infračervenou LED diodou. Diody jsou umístěny v komoře, do které nemůže vniknout světlo z cizího zdroje, ale může do ní vniknout kouř,
- ionizační hlásiče kouře - identifikují požár na základě uvolnění plynů a kouře na bázi uhlíku do ovzduší. Ionizační hlásiče reagují i na malou koncentraci ionizovaných částic ve vzduchu. Jsou tedy velmi citlivé i na kouř, který není viditelný lidským okem. Hlavní výhoda tohoto typu hlásiče je nízká cena a jednoduchá výroba,

- hlásiče multisenzorové s využitím plynové detekce (CO) - využívají kombinaci teplotního, chemického a optického senzoru. Jedná se o nejnovější generaci hlásičů požárů s inteligentní vyhodnocovací elektronikou, která vytváří novou úroveň technologií detekce požáru. Multisenzorové hlásiče jsou mimořádně odolné proti falešným poplachům,
- optické hlásiče plamene - identifikují infračervené a ultrafialové záření vydávané plamenem. Tyto hlásiče se montují na strop nebo na stěnu. Slouží spíše jako doplněk k teplotním, optickým nebo ionizačním detektorům,
- lineární optický hlásič - samočinný hlásič indikující vznikající požár zeslabením intenzity infračerveného paprsku částicemi kouře. Tento typ hlásičů se nejčastěji využívá v halách a v rozsáhlých prostorách,
- aspirační (nasávací) požární hlásiče - využívají se v místnostech nebo objektech, ve kterých jsou vyžadovány vysoce citlivé požární hlásiče. Tento typ hlásiče signalizuje požár v ranném stádiu, čímž minimalizuje následky vzniklého požáru,
- tlakové hlásiče - jsou tvořeny snímací trubicí a vyhodnocovací jednotkou. Poplach je vyvolán změnou tlaku způsobenou zvýšením okolní teploty ve snímací trubici. Výhodou tlakových hlásičů je, že detekční trubice je umístitelná skoro všude. Detekční části hlásiče nevadí hmyz, prach a další faktory, které u jiných hlásičů spouštějí plané poplachy.

9 KAMEROVÉ SYSTÉMY

Kamerové systémy CCTV slouží k monitorování střeženého objektu i okolí kolem něj. Jsou schopny kontrolovat rozsáhlé prostory v reálném čase**.** Trendem současných CCTV systémů je efektivnost, vysoká kvalita zvukového záznamu, snímaného obrazu a také jednoduchá obsluha. Proto patří k nejrychleji se rozvíjejícím a nejčastěji žádaným systémům. Kamerové systémy lze pro monitorování používat samostatně nebo je sloučit s dalšími systémy do komplexnějších celků. Podle požadavků zákazníka se CCTV systémy instalují společně s identifikačními systémy, docházkovými systémy, systémy PZTS, s perimetrickým zabezpečením a dalšími bezpečnostními systémy. Přenosové možnosti komunikačních sítí umožňuje sjednocení všech bezpečnostních systémů do jednoho řídícího monitorovacího (dohledového) pracoviště. [17][25]

9.1 IP kamerové systémy

S technickým pokrokem v oblasti přenosových sítí a v oblasti digitalizace videosignálu se začínají stále více používat IP kamery (IP Internet Protocol). V pouzdře IP kamery je mimo videokamery nainstalován také integrovaný webový server, který zajišťuje připojení videokamery k počítačové síti, digitalizaci a komprimaci videosignálu. IP kamery mají implementované webové stránky (http), umožňující v rámci lokální počítačové sítě sledovat obraz v libovolném internetovém prohlížeči prakticky z libovolného místa na světě. [17]

IP kamery využívají větší šířky pásma, což dovoluje přenášet obraz ve Full HD nebo i vyšším rozlišení. Kvalita výsledného obrazu je lepší ve srovnání s obrazem analogovým. IP kamery mají možnost detekce pohybu (nezávislé na záznamovém zařízení), lepší snímkovací frekvenci a možnost pokročilejší analýzy obrazu. [13]

9.2 AHD kamerové systémy

Vznikly jako náhrada za analogové kamerové systémy. Obraz se přenáší v analogové podobě od kamery do záznamového zařízení, které musí být dostatečně výkonné pro zpracování obrazu. Záznamové zařízení AHD kamer je hybridní. Do jednoho systému můžeme připojit IP kamery i staré analogové kamery. [14]

Dělení kamer podle jejich konstrukčního provedení [22]:

- standardní kamery - ve standardním provedení mají tělo ve tvaru krabice. Objektiv kamery se volí na základě prostředí, do kterého bude kamera instalována. Tento typ kamer je určen do vnitřního prostředí. Při použití ve venkovním prostředí je potřeba použít venkovní vyhřívaný kryt,
- kompaktní kamery - při jejich výběru je nutné zohlednit způsob použití a prostředí i možnost IR přísvitu pro používání v noci,
- dome kamery - jsou stropní kamery v kopulovitém krytu určené pro montáž na stěnu či strop. Díky svému vzhledu jsou tyto kamery nenápadné a při použití krytu s kouřovým sklem není možné poznat, kam jsou namířeny. Kamery v provedení se zesílenou konstrukcí odolnou proti vandalům jsou schopny odolat i útokům kovovou tyčí nebo kamenem,
- otočné kamery - jsou nejvíce univerzálními kamerami. Tyto Kamery se mohou otáčet až o 360 stupňů a dle typu kamery může být použit až 36x zoom. Tyto vlastnosti umožňují sledování střežených míst pomocí minimálního počtu kamer. Otočné kamery jsou určeny do vnitřních i venkovních prostředí,
- bezdrátové kamery - tento typ kamer je používán v místech, kde je komplikovaná instalace kabeláže nebo pro mobilní systémy. Nevýhodou je omezený dosah. Pro přenos signálu na větší vzdálenosti je potřeba použít samostatné přenosové zařízení s externí anténou,
- speciální skryté kamery - jedná se o miniaturní kamery zabudované do jiných zařízení (např. pohybové detektory).

10 ELEKTRONICKÁ KONTROLA VSTUPŮ

Jednou z hlavních částí bezpečnostních systémů jsou prvky sloužící k ověřování identity osob. Elektronickou kontrolu vstupů můžeme definovat jako systém určený k automatizovanému řízení vstupů v hlídané oblasti. K ověřování se využívá autentizace, což je ověření, zda je daná osoba tou osobou, za kterou se vydává. Tento typ systémů je vhodný, jak pro plášťovou ochranu, tak pro obvodovou ochranu. [4][5]

10.1 Přístupové systémy

Slouží k otevírání dveří, registraci a kontrolu vstupu osob do objektu a jeho částí. [5]
Druhy přístupových systémů [17][25]:

- elektronický klíč - je inteligentní uzamykací systém, který se skládá ze zámku, elektroniky a klíče s mikroprocesorem,
- čipové identifikační prvky - uchovávají informace v paměťovém čipu, který je zalisován do štítku, přívěsku nebo čipové karty,
- bezkontaktní přístupové systémy - označujeme je jako vstupníky. Jsou to nosiče identity pro bezkontaktní čtení. Mohou být v podobě přívěsků, skleněných trubiček a čipových karet.

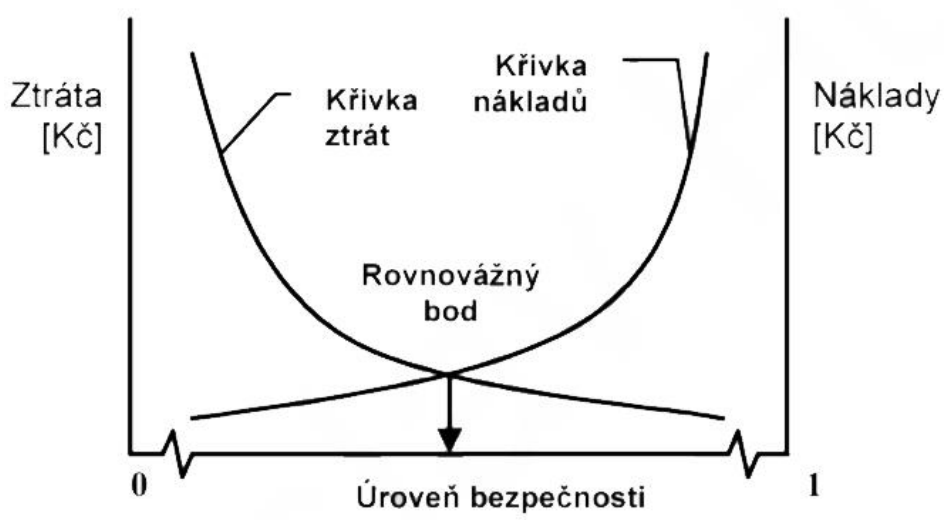
10.2 Biometrické systémy

Biometrika je jednoznačně určující identifikace osob na základě jedinečných fyziologických znaků člověka. Biometrický systém se skládá ze snímacího modulu, který získává biometrická data osoby. Rozpoznávacího modulu, který extrahuje tzv. příznaky. Porovnávacího modulu, který porovnává získané příznaky s daty uloženými v databázi uživatelů a rozhodovacího modulu, který rozhoduje, zda se snímané údaje shodují s daty uloženými v databázi. [5]
Výhody biometrických identifikací jsou [5]:

- univerzálnost - každá osoba je jejím nositelem,
- jedinečnost - každá osoba je jedinečná. Neexistují dvě osoby se stejnými biometrickými charakteristikami,
- permanence - biometrické charakteristiky osoby se nemění s časem,
- jednoduchost - biometrické charakteristiky jsou měřitelné kvantitativně a získané charakteristiky jsou přesné a jednoduché,
- přijatelnost - snímání biometrických charakteristik není náročné.

11 ANALÝZA RIZIK

Riziko popisuje pravděpodobnost, že nastane událost, kterou z bezpečnostního hlediska považujeme za nežádoucí. Způsobené škody mohou být více, či méně tolerované. Aby byla organizace schopna posoudit, co je pro ni přijatelné a co ne, přijímala správné rozhodnutí a aplikovala účinná bezpečnostní opatření, musí co nejlépe poznat potencionální hrozby vzdálené i blízké okolí a vlastní zranitelnost. Pravidelná analýza rizik viz Obrázek 1: Analýza rizik je systematický přístup k posouzení hrozeb a odhalení zranitelnosti. Rozhodnutí, zda bude dané riziko akceptováno, eliminováno nebo odstraněno, závisí na stupni závažnosti a nákladů potřebných na jeho řešení. Cílem analýzy rizik je zjištění toho, co je pro organizaci cenné a důležité, co je tolerovatelné a co už ne. [12]



Obrázek 1: Analýza rizik

Zdroj: [12]

11.1 Druhy analýzy rizik

Orientační analýza rizik - používá se jako součást budování bezpečnostní politiky. Bere v úvahu nejvýznamnější hrozby a aktiva. [12]

Elementární analýza rizik - je založena na převzetí opatření na základě podobného systému a ze všeobecných norem. K provedení nevyužívá žádné výpočty. Tento druh analýzy je časové i finančně nenáročný, ale na jejím základě se mohou volit zbytečně silná a drahá opatření, nebo naopak nedostatečně silná opatření. [12]

Neformální analýza rizik - provedení analýzy rizik na základě interních nebo externích odborníků na bezpečnost. Nepoužívají se standardní strukturované metody, vyskytuje se vyšší pravděpodobnost opomenutí některých rizik a dochází ke snadnému ovlivnění volby

subjektivními neprokázanými názory řešitelů. Typické pro tuto analýzu je časová a finanční nenáročnost, rychlé provedení a je vhodná pro malé organizace. [12]

Detailní analýza rizik – používá standardní strukturované metody ve všech fázích. Vysoká časová a finanční náročnost. Výhodu je malá pravděpodobnost přehlédnutí některých rizik, oprávněnost zvolených bezpečnostních opatření a nesnadné ovlivnění volby subjektivními názory řešitelů. [12]

Ke každé z těchto analýz můžeme přistupovat z kvantitativního nebo kvalitativního hlediska. [12]

- kvantitativní přístup – využívá číselní hodnoty, kvalita analýzy závisí na úplnosti a přesnosti číselných hodnot a platnosti použitých modelů,
- kvalitativní přístup – využívá slova k popisu rozsahu možných pravděpodobností a následků, že se přihodí.

11.2 Naložení s rizikem

Management firmy má za úkol zvolit co nejvhodnější opatření vůči hrozbám, které mohou nastat. Na základě analýzy rizik se management firmy může vypořádat s každým rizikem čtyřmi způsoby [12]:

- snížení rizika - implementování bezpečnostních opatření za účelem blokování hrozeb a eliminace slabin,
- akceptování rizika - smíření se s rizikem v případě, že je cena opatření vyšší něž očekáváná ztráta,
- postoupení rizika - přesunutí rizika a ceny ztráty jinému subjektu např. pojištění,
- ignorace rizika - spoléhání se na to, že riziko nikdy nenastane. Jde o nesprávné neracionální rozhodnutí.

12 POPIS VYBRANÉHO OBJEKTU FIRMY

Pro účely mé bakalářské práce jsem vybral skutečnou firmu. Firma si nepřeje zveřejňovat svůj název, proto bude označována jako firma XY.

Cílem této práce je zhodnotit stávající stav zabezpečení firmy, odhalit případné nedostatky v zabezpečení a navrhnout vhodná opatření. Na základě analýzy rizik doporučit, zda je vhodné daná rizika úplně odstranit, eliminovat nebo akceptovat. To závisí na závažnosti rizika a nákladů potřebných na jeho řešení.

Při návrhu nových bezpečnostních opatření by se mělo dodržovat jednoduché pravidlo, které říká, že bezpečnostní opatření mají smysl v případě, kdy náklady na jejich zavedení nepřesáhnou cenu chráněných aktiv. [8]

12.1 Základní údaje o firmě

Firma XY se zabývá výrobou vyfukovaných plastů, výseků z fólie, izolačních a hydroizolačních folií, které se využívají v automobilovém, kožedělném, textilním a stavebním průmyslu. Mimo vlastní výrobu distribuuje PVC fólie, geotextílie, drenážní rohože a další izolační materiály.

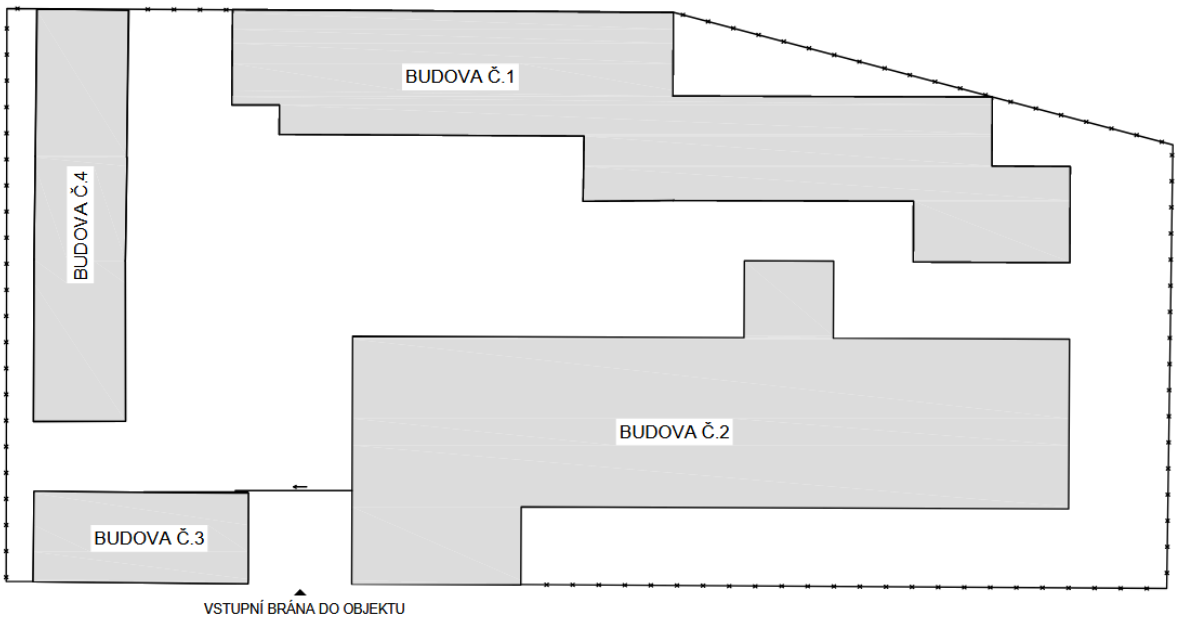
Firma zaměstnává 11 zaměstnanců a řadí se tak mezi malé podniky. Jako malé podniky jsou označovány podniky, které zaměstnávají méně než 50 osob a jejich aktiva, nebo obrat nepřesahuje 10 milionů EUR. [7]

Sídlo firmy leží u lesa na kraji města. Firma sousedí se dvěma dalšími firmami, zahrádkářskou kolonií a komplexem garáží. Lokalita u lesa na kraji města může být pro potencionální pachatele lákavá. V případě odhalení se mohou snadno schovat, popřípadě utéct lesem.

12.2 Objekt firmy

Objekt firmy XY viz Obrázek 2 se rozléhá na rozloze 3800 m^2. Je tvořen čtyřmi budovami, které slouží jako výrobní, kancelářské, skladovací prostory a prostory pronajímané za účelem komerčního nájmu. Celý objekt je po obvodu obehnán plotem složeným ze 3D panelů, které jsou doplněny o žiletkový drát. Vjezd do areálu je zabezpečen posuvnou bránou s elektrickým pohonem, kterou je možné otevřít čipem, dálkovým ovladačem nebo klíčem. Čipy a klíče od brány mají majitelé firmy a všichni zaměstnanci kromě účetní. Všechny budovy v areálu firmy jsou vybudovány z pevných stavebních materiálů. Budova č.3 je pronajímána soukromé osobě

a část budovy č.2 je pronajímaná jiné společnosti za účelem zisku komerčního nájmu. Firma XY je odpovědná za bezpečnost celého objektu, do kterého je zahrnuta i pronajímaná budova č.3 a pronajímané prostory budov č.2. Osoby v pronájmu mají přístup pouze do svých pronajatých prostor. Bez vědomí zástupců firmy XY se nemohou pohybovat po areálu firmy ani v prostorách, které nemají pronajaté.



Obrázek 2: Objekt firmy XY

Zdroj: vlastní zpracování

Budova č.1

Budova č.1 o rozloze 616 m^2 je hlavní dvoupatrová budova firmy XY. V prvním patře jsou umístěny tři výrobní dílny, kancelář skladníka, šatna, WC se sprchou, kuchyňka a rozvodna elektrické energie. Součástí prvního patra je garáž na vysokozdvižný vozík. Ve druhém patře jsou umístěny dvě kanceláře a mála místnost se serverem. Tyto prostory jsou propojeny s prvním patrem pomocí schodiště. Zbylé prostory druhého patra slouží jako sklad. Přistup do těchto prostor je možný pomocí výtahu.

Budova č.2

Budova č.2 o rozloze 833 m^2 je třípatrovou budovou firmy XY. První a druhé patro budovy slouží k pronájmu jiné společnosti, která využívá tyto prostory ke skladování. Tato společnost má přístup do budovy dvěma vstupy, které se nachází mimo areál firmy a v budově se dostane pouze do svých pronajatých prostor. Třetí patro slouží firmě XY jako sklad materiálu a zařízení. V případě velkého množství zakázek nebo zavedení nové výroby by byla tato budova využita

k rozšíření výrobních prostor. Zaměstnanci firmy XY využívají k přístupu do této budovy výtah nebo ocelové protipožární dveře.

Budova č.3

Budova č.3 o rozloze 123 m^2 je jednopatrová budova pronajímána soukromé osobě za účelem zisku komerčního nájmu. Majitel pronajaté budovy má přístup do budovy dvěma vstupy, které se nachází mimo areál firmy.

Budova č.4

Budova č.4 o rozloze 220 m^2 je jednopatrová budova sloužící jako sklad firmy XY. V této budově je skladován materiál potřebný k výrobě a také vyrobený materiál připravený k expedici.

13 SOUČASNÉ ZABEZPEČENÍ FIRMY

V této kapitole je popsán současný stav zabezpečení objektu a firemních dat.

13.1 Obvodová ochrana

Představuje prostředky, které zajišťují bezpečnost vymezeného území. Úkolem obvodové ochrany je zabránit nebo co nejvíce ztížit vniknutí do areálu firmy. Areál firmy XY je obehnaný plotem ze silně zinkovaných svařovaných 3D panelů, mimo plot podél příjezdové cesty naproti budově č.2. Výška tohoto plotu je 1,2 metru a není doplněný vrcholovou ochranou, což snižuje kvalitu zabezpečení a umožňuje snadnější vniknutí do objektu. Zbylé oplocení bylo nově postaveno v roce 2010, je vysoké 2,5 metrů, na vrcholu je doplněno o žiletkový drát a kvůli zvýšení odolnosti a stability je usazeno do betonových podhrabových desek. Žiletkový drát je účinnější bezpečnostní prvek než ostnatý drát, má mnohem silnější odrazující efekt a je obtížnější na překonání. Vjezd do areálu je zabezpečen posuvnou bránou s elektrickým pohonem, která je doplněna o ostré hroty na vrcholu. Bránu je možno otevřít dálkovým ovládáním. Lze jí také otevřít přímo u brány pomocí bezpečnostního klíče po zadání kódu nebo po přiložení čipu na ovládací panel u brány. Brána bývá standartně zavřená, výjimkou je 6. až 14. hodina, v tomto časovém rozmezí je obrána otevřena z důvodu příjezdu a odjezdu odběratelů dodavatelů materiálu, kteří se po příjezdu do areálu nahlásí u skladníka v kanceláři a po areálu firmy se pohybují pouze v jeho přítomnosti. Po druhé hodině, kdy skladník odchází domů je brána uzavřena. Dalšími vstupy do objektů firmy jsou klasické plastové dveře do budovy č.2, které využívá majitel pronajatých prostor v této budově. Dále hliníkové dveře a hliníková vrata do budovy č.3, které využívá pronajímatel této budovy.

V rámci obvodové ochrany využívá Firma XY pouze mechanických systémů, mezi které patří plot, posuvná brána s bezpečnostní uzamykacím systémem a vrcholová ochrana v podobě žiletkového drátu nebo ostrých hrotů.

13.2 Plášťová ochrana

Je tvořena prvky, které mají za úkol ztížit a prakticky znemožnit vniknutí do chráněného prostoru v objektu prostřednictvím stavebních otvorů. Všechny budovy v areálu firmy jsou vybudovány z pevných stavebních materiálů, které spolehlivé zabraňují pachateli v probourání do budovy. Každá budova v areálu firmy má jinou úroveň plášťové ochrany.

Budova č.1 má čtyři vchody. První vchod vede do chodby, kde se nachází vstup do výrobních prostor a schodiště do vrchních kanceláří. Tento vchod je uzavřen staršími dřevěnými dveřmi,

které chrání bezpečnostní mříž pevně ukotvená ke zdi budovy a uzamčená bezpečnostním visacím zámkem s tvrzeným okem. Zbylé tři vstupy vedou do prostor výroby firmy a jsou uzavřeny dvoukřídlými plechovými vraty, které jsou také chráněny mřížemi. Stejným způsobem je uzavřena i garáž pro vysoko zdvižný vozík. Okna v budově jsou plastová vyplněna dvojsklem. V prvním patře jsou okna podobně jako vchody chráněna bezpečnostními mřížemi pevně ukotvené ke zdi budovy.

Budova č.2 má dva vstupy mimo areál firmy uzavřený plastovými dveřmi. Tento vstup využívají vlastníci pronajímaných prostor. Další vstupy do budovy jsou přímo v areálu firmy. Prvním vstupem jsou plechová vrata od výtahu a druhým ocelové protipožární dveře. Okna v celé budově jsou plastová vyplněná dvojsklem.

Budova č.3 má dva vstupy mimo areál firmy. Prvním jsou hliníkové dveře a druhým hliníková vrata. Vstup z této budovy do areálu firmy nebyl využíván, proto bylo provedeno jeho zazdění. Okna této budovy jsou stejně jako dveře hliníková bez jakékoli ochrany.

Budova č.4 má tři vstupy, které jsou stejně jako vstupy do hlavní budovy uzavřeny dvoukřídlými plechovými vraty uzamčenými bezpečnostním visacím zámkem.

V rámci plášťové ochrany využívá Firma XY pouze mechanických systémů, mezi které patří různé typy dveří, oken a mříže, které zabezpečují vchody a okna budovy č. 1.

13.3 Prostorová ochrana

Je tvořena prostředky zabezpečující prostor uvnitř chráněného objektu po překonání obvodové ochrany a vniknutí neoprávněné osoby do vnitřních prostor objektu. Firma XY je vybavena výstražnou sirénou a dvaceti pasivními infračervenými čidly umístěnými ve venkovních prostorách areálu i ve vnitřních prostorách budov. Tyto systémy jsou připojeny na centrální pult ochrany, jehož dohledové a poplachové příjímací centrum se nachází v Praze. Při odchodu zaměstnanců z firmy jsou tyto systémy spuštěny zakódováním objektu na panelu u hlavní brány a dají se vypnout čipem nebo zadáním přístupového pinu na stejném panelu u vstupní brány.

V rámci prostorové ochrany využívá tedy Firma XY pasivní infračervená čidla a sirénu signalizují narušení prostor firmy.

13.4 Předmětová ochrana

V kanceláři skladníka je umístěna příruční pokladna, do které se ukládají menší peněžní obnosy z drobného prodeje. Každý den před odchodem skladníka z práce jsou peníze spočítány a pokladna je uložena do skříňového trezoru v kanceláři ve druhém patře hlavní budovy.
V rámci předmětové ochrany využívá Firma XY pouze mechanické systémy, mezi které patří příruční pokladna a skříňový trezor.

13.5 Ochrana lidí

Firma XY nemá žádné prostředky signalizující zdravotní problémy či ohrožení života fyzických osob. Ve firmě chybí také elektrická požární signalizace, která slouží k detekci požáru a chrání tak majetek firmy i zaměstnance firmy.

13.6 Zabezpečení dat

Firma XY má snahu co nejlépe zabezpečit svá data. Místnost, ve které je uložen server se nachází ve druhém patře hlavní budovy. Místnost je uzamčena, aby se do ní nedostala nepovolaná osoba a předešlo se tak úmyslnému či neúmyslnému poškození uložených dat nebo jejich odcizení. Do této místnosti nemá přístup nikdo ze zaměstnanců firmy kromě vedoucího pracovníka. Umístění serveru ve vyšším patře zamezí mimo jiné poškození dat následkem přírodního živlu, kterým je velká voda.

Firma XY používá na všech svých počítačích pouze licencovaný software. Antivirovou ochranu firmě XY poskytuje společnost Avast. Antivirová ochrana je nainstalovaná na všech zařízeních připojených k firemní síti a chrání je tak před pokročilými kybernetickými útoky. Každý pracovník firmy se přihlašuje do počítače na základě přiděleného uživatelského jména a hesla. Heslo si zaměstnanci volí sami. Každé heslo, které si zaměstnanci zvolí musí obsahovat minimálně šest znaků a skládá se z písmen, číslic a symbolů. Jelikož si zaměstnanci volí silná hesla není důvod k časté změně hesel, která vede k tomu, že si je nebudou pamatovat. Při práci na počítači mají zaměstnanci přístup pouze k datům, které potřebují ke své práci. To souvisí i s přístupem na internet prostřednictvím počítače, který je poskytnut pouze těm, kteří využívají internet ke své práci. Firma provádí také pravidelnou zálohu svých dat. Záloha dat je prováděna každý den na server umístěný ve firmě. Jednou týdně je prováděna záloha dat i na server do Brna, kde mají sídlo majitelé Firmy XY.

14 NEDOSTATKY V ZABEZPEČENÍ FIRMY

Cílem této kapitoly je odhalení nedostatků v zabezpečení dat a objektu firmy XY. Na základě zjištění současného stavu zabezpečení je nedostatkem v obvodovém zabezpečení objektu starý plot podél příjezdové cesty. Výška plotu je 1,2 metru, bez vrcholové ochrany je pro potencionálního pachatele snadno překonatelný. Nedostatkem obvodové i prostorové ochrany je absence kamerového systému, který slouží k monitorování střeženého objektu a okolí kolem něj.

Co se týče plášťové ochrany je největším nedostatkem chybějící zabezpečení oken v prvních patrech budov č.2 a 3, které chrání zasklené plochy a omezují tak možnosti násilného vniknutí do objektu prostřednictvím těchto otvorových výplní. Nedostatkem plášťové ochrany budov jsou i chybějící bezpečnostní systémy signalizující neoprávněné vniknutí do prostor budov č. 2 a 3 prostřednictvím vchodových dveří, která jsou mimo areál firmy.

Posledním výrazným nedostatkem v zabezpečení je absence elektrické požární signalizace, jelikož firma pracuje s vysoce hořlavým materiálem, považuji chybějící EPS za velký nedostatek v zabezpečení firmy.

Ve firmě ještě nikdy nedošlo k závažnějším zdravotním problémům nebo ohrožení života. Zaměstnanci pracují v minimálním počtu dvou osob na směně, případnou zdravotnickou pomoc může zavolat někdo ze zaměstnanců. Z toho důvodu nenavrhuji žádné prostředky signalizující zdravotní problémy.

V rámci zabezpečení firemních dat nejsou žádné výraznější nedostatky. Firmě bych jenom doporučil zálohovat data i na nějaké cloudové uložiště.

15 NÁVRHY NA ZLEPŠENÍ

Cílem je návrh opatření odstraňující nedostatky v zabezpečení budov a areálu firmy. Návrhy na zlepšení se týkají prostředků obvodové ochrany, plášťové ochrany, prostorové ochrany a elektrické požární signalizace.

Pří návrhu nového oplocení části areálu a výběru bezpečnostních fólií pro zabezpečení skleněných ploch jsem využíval internetové stránky. V případě návrhu kamerového systému a bezdrátového zabezpečovacího systému jsem oslovil firmu IT Outsourcing se kterou firma XY spolupracuje. Pro návrh elektrické požární signalizace jsem oslovil firmu PATROL group s.r.o., kterou jsem vybral na základě doporučení a spokojenosti firem, které s PATROL group s.r.o spolupracují.

15.1 Obvodová ochrana

Na základě nedostatků současné obvodové ochrany objektu bych doporučil zavedení IP kamerového systému. IP kamery využívají větší šířky pásma, což dovoluje přenášet obraz ve Full HD nebo i vyšším rozlišení. Kvalita výsledného obrazu je lepší ve srovnání s obrazem analogovým. IP kamery mají možnost detekce pohybu, lepší snímkovací frekvenci a možnost pokročilejší analýzy obrazu. Životnost kamer je zhruba 15 let.

Pro objekt firmy byl navrhnut firmou IT Outsourcing kamerový systém DAHUA, který se skládá ze sedmi bezpečnostních IP 5 Mpx kamer, NVR nahrávacího komponentu a dvou HDD disků. Náklady na kamerový systém jsou uvedeny v Tabulka 3. Firmu IT Outsourcing jsem vybral z toho důvodu, že s ní firma XY spolupracuje a je s jejich službami spokojena.

Tabulka 3: Náklady na IP kamerový systém

Kamerový systém DAHUA	
Počet IP 5 Mpx kamer	7 ks
Cena kamery	4 461,16 Kč bez DPH
Celková cena kamer	31 228,1 Kč bez DPH
NVR nahrávací komplet s napájením	
Cena NVR nahrávacího kompletu	10 661,16 Kč bez DPH
HDD disk	
Počet HDD disků	2 ks
Cena HDD disku	3 214,88 Kč bez DPH
Celková cena HDD disků	6 429,76 Kč bez DPH
Kabeláž CAT 5E	
Kabeláž 1 m	8,26 Kč bez DPH
Kabeláž 300 m	2 478 Kč bez DPH
Práce	
Montáž systému	4 214.9 Kč bez DPH
Nastavení systému do PC/tel.	1 652.9 Kč bez DPH
Celková cena kamerového systému	56 665 Kč bez DPH

Zdroj: vlastní zpracování

Cena kamerového systému včetně kabeláže, montáže kamer i nastavení systému do PC a telefonu je 56 665 Kč bez DPH.

Dalším prvkem pro zlepšení obvodové ochrany objektu je výstavba nového oplocení podél příjezdové cesty naproti budově č.2. Oplocení je zde nízké, bez jakékoliv vrcholové ochrany, což výrazně snižuje úroveň zabezpečení a velmi usnadňuje proniknutí potencionálního pachatele do objektu firmy. Zbylé oplocení areálu firmy je nově vystavěné v roce 2010. Tvoří ho silně zinkované svařované 3D panely s vrcholovou ochranou usazené do betonových podhrabových desek. Z důvodu snadné překonatelnosti starého oplocení navrhuji výstavbu oplocení nového, stejné konstrukce, jaké je oplocení vystavěné v roce 2010. Pro návrh nového oplocení jsem využil internetové stránky, na kterých jsem vyhledal stejné komponenty, ze kterých je vystavěno zbylé oplocení areálu. Životnost pletiva se pohybuje kolem 20 až 40 let. Náklady na výstavbu uvádí Tabulka 4.

Do celkových nákladů není započítaná cena za odstranění starého oplocení, výkopové práce a výstavba nového oplocení. Tuto cenu musí stanovit firma, která bude najatá na výstavbu nového oplocení na základě náročnosti terénu.

Tabulka 4: Náklady na nové oplocení

Plotový panel 3D PVC 203 cm	
Počet m plotového panelu	50 m
Cena za 2,5 m	685,12 Kč bez DPH
Celková cena za panely	13 703 Kč bez DPH
Betonová podhrabová deska 2450 x 200 x 50 mm	
Počet desek	20 ks
Cena za 2,45 m desky	387,60 Kč bez DPH
Celková cena za desky	7 752 Kč bez DPH
Plotový sloupek STRONG zelený 260 cm x 48 mm x 2 mm	
Počet sloupků	21 ks
Cena sloupku	461,98 Kč bez DPH
Celková cena sloupků	9 702 Kč bez DPH
Žiletkový ostnatý drát, spirála – průměr 300 mm	
Počet metrů drátu	150 m
Cena za 8-12 m	288,43 Kč bez DPH
Celková cena za drát	4 327 Kč bez DPH
Průběžný držák podhrabové desky 20 cm	
Počet držáků	21 ks
Cena držáků	114,88 Kč bez DPH
Celková cena za držáky	2 413 Kč bez DPH
Bavolet PVC 48 mm	
Počet bavoletů	21 ks
Cena bavoletu	296,69 Kč bez DPH
Celková cena za bavolety	6 231 Kč bez DPH
Celková cena za oplocení	44 128 Kč bez DPH

Zdroj: upraveno podle: [20]

Cena nového oplocení bez nákladů na odstranění starého oplocení, výkopových prací a výstavby nového oplocení je 44 128 Kč bez DPH.

15.2 Plášťová ochrana

Na základě nedostatků současné plášťové ochrany bych doporučil instalovat do oken v prvních patrech budov č.2 a 3 bezpečnostní fólii. Toto opatření zvýší úroveň plášťové ochrany a podstatně ztíží potencionálnímu pachateli vniknutí do budovy. Pachatelé se snaží vniknout do objektu co nejrychleji, aby nebyli odhaleni. Proniknout do objektu přes okno chráněné touto ochranou by znamenalo pro pachatele značné časové zdržení a vyvinutí velké fyzické námahy, což je pro pachatele riskantní a mohli by být odhaleni.

Bezpečnostní fólie snižují riziko násilného vniknutí do objektu a nabízí srovnatelně kvalitní zabezpečení jako mříže. Výhodami fólií jsou např. estetičtější vzhled oproti mřížím, běžný způsob údržby, průměrná životnost 15 let, omezení tepelných ztrát, schopnost zadržet až 99% škodlivého UV záření. [3]

Pro zabezpečení skleněných ploch jsem na internetových stránkách vybral bezpečnostní fólii SMC AX 300 μm 12 Mil. Je to certifikovaná fólie v kategorii odolnosti EN 356 P2A o tloušťce 300 μm. Fólie splňuje nejpřísnější kritéria pro ochranu a bezpečnost osob a majetku, je také uznávaná pojišťovnami k zabezpečení objektu. [19]

Náklady na bezpečnostní fólii jsou uvedeny v Tabulka 5.

Tabulka 5: Náklady na bezpečnostní fólii

Bezpečnostní fólie SMC AX 300 um 12 Mil	
Počet m^2 fólie	129 m^2
Cena za m^2 fólie	690 Kč bez DPH
Cena za montáž m^2 fólie	190 Kč bez DPH
Celková cena za fólii	113 520 Kč bez DPH

Zdroj: upraveno podle [9]

Cena bezpečnostní fólie včetně montáže je 113 520 Kč bez DPH.

Dalšími prvky, které bych doporučil zavést na zlepšení plášťové ochrany budov č.2 a 3, jsou chybějící bezpečnostní systémy signalizující neoprávněné vniknutí do těchto budov prostřednictvím vchodových dveří, které se nacházejí mimo areál firmy. Pro tento účel byl navrhnut opět firmou IT Outsourcing bezdrátový zabezpečovací systém AJAX BEDO, který se skládá z dveřních čidel, pasivního infračerveného čidla, venkovní sirény a zaváděcího setu obsahující dveřní čidlo a pasivní infračervené čidlo. Životnost toho systému je zhruba 20 let. Náklady na tento bezdrátový bezpečnostní systém jsou uvedeny v Tabulka 6.

Tabulka 6: Náklady na bezdrátový zabezpečovací systém

Bezdrátový zabezpečovací systém AJAX BEDO	
Cena zaváděcího setu	7 843 Kč bez DPH
Pasivní infračervené čidlo (PIR)	
Cena PIR čidla	1 396,7 Kč bez DPH
Dveřní čidlo	
Počet dveřních čidel	3 ks
Cena dveřního čidla	1 396,7 Kč bez DPH
Celková cena dveřních čidel	4 190 Kč bez DPH
Venkovní siréna	
Cena venkovní sirény	2 719 Kč bez DPH
Práce	
Montáž systému	1 983,5 Kč bez DPH
Nastavení systému do PC/tel.	661 Kč bez DPH
Celková cena systému AJAX BEDO	18 793 Kč bez DPH

Zdroj: vlastní zpracování

Cena bezdrátového zabezpečovacího systému včetně montáže i nastavení systému do PC a telefonu je 18 793 Kč bez DPH.

15.3 Prostorová ochrana

Na základě nedostatků současné prostorové ochrany objektu bych doporučil zavedení IP kamerového systému. Náklady na zavedení IP kamerového systém jsou uvedeny v Tabulka 3.

15.4 Elektrická požární signalizace

Posledním návrhem na zlepšení zabezpečení objektu firmy je instalace elektrické požární signalizace (EPS) sloužící k detekci požáru a jeho následné signalizaci. Návrh EPS pro všechny budovy v objektu provedla firma PATROL group s.r.o. PATROL group s.r.o jsem vybral na základě doporučení a spokojenosti firem, které s PATROL group s.r.o spolupracují.

Elektrická požární signalizace se skládá z mnoha komponent, mezi ty hlavní patří sirény, ústředna EPS, zařízení dálkového přenosu, tlačítkové hlásiče určené k vyhlášení poplachu osobou, která zjistí požár. Dále pak multisenzorové hlásiče, které je možné použít jako teplotní hlásič, opticko-kouřový hlásič nebo jako kombinovaný opticko-kouřový/teplotní hlásič podle specifických požadavků firmy. Životnost EPS je zhruba 20 let.

U ústředny EPS by ve firmě XY nebyla zajištěna stálá obsluha, která v případě požáru upozorní jednotku hasičského záchranného sboru (HZS). Proto by byl systém EPS připojen

prostřednictvím zařízení dálkového přenosu (ZDP) k pultu centralizované ochrany (PCO) umístěného na krajském operačním a informačním středisku (KOPIS) Hasičského záchranného sboru. Jednalo by se tedy o bezobslužný režim obsluhy EPS.

Firma XY by v případě zavedení EPS platila firmě PATROL měsíčně částku 7.049 Kč bez DPH za služby, které zahrnují: trvalé střežení systému EPS napojeného objektu. Střežení je prováděno v režimu 24/7/365 operačním důstojníkem KOPIS. Dále pak poplatek za provoz objektového vysílače v privátní tříoperátorové síti GPRS, včetně poplatku za speciální SIM této služby, poplatek za provoz objektového vysílače v privátní rádiové síti PATROL, včetně poplatku Českému telekomunikačnímu úřadu, za napojení střeženého systému EPS objektu do PCO provozovaných společností PATROL na KOPIS HZS a pracovišti dohledu PATROL, za pololetní a roční kontrolu provozuschopnosti ZDP dle vyhlášky č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci) a za periodickou revizi elektrického zařízení ZDP dle ČSN 342710 a zajištění nepřetržité servisní pohotovosti k zajištění trvalé provozuschopnosti propojeného systému.

V platbě nejsou zahrnuty náklady na náhradní díly, materiál a opravy. Cena za služby není započítána do nákladů na zavedení EPS uvedené v Tabulka 7.

Tabulka 7: Náklady na elektrickou požární signalizaci

EPS ústředna včetně příslušenství	
Cena EPS ústředny a příslušenství	136 901,4 Kč bez DPH
Hlásiče a příslušenství EPS	
Cena hlásičů a příslušenství EPS	213 138,7 Kč bez DPH
Vstupně/výstupní moduly	
Cena vstupně/výstupních modulů	21 173 Kč bez DPH
Optické a akustické signalizační zařízení	
Cena optického a akustického zařízení	35 000 Kč bez DPH
EPS - Provozní dokumentace a zkoušky	
Cena provozní dokumentace a zkoušek	110 550 Kč bez DPH
EPS - Kabely, lišty, pomocný materiál	
Cena pomocného matriálu, kabelů a lišt	129 550 Kč bez DPH
Instalační a stavební práce	
Cena instalačních a stavebních prací	211 350 kč bez DPH
Celková cena EPS	857 664 Kč bez DPH

Zdroj: vlastní zpracování

Cena zavedení elektrické požární signalizace včetně veškerého příslušenství, instalace a stavebních prací je 857 664 Kč bez DPH.

16 ANALÝZA RIZIK

V rámci bakalářské práce použiji orientační kvantitativní analýzu rizik, která využívá na rozdíl od popisné škály uplatňované v kvalitativních analýzách číselných hodnot. Na základě výsledků analýzy rizik by se měla firma XY rozhodnout, zda investovat do zdokonalení zabezpečení objektu za účelem snížení rizika nebo riziko podstoupit, akceptovat či ignorovat.
V rámci analýzy rizik musíme určit [12]:

Seznam aktiv a stanovení hodnot aktiv (HA)

Jako aktiva označujeme majetek podniku nebo hospodářské prostředky. Pojem majetek zahrnuje všechny věci, pohledávky, peníze a jiné majetkové hodnoty, které slouží k podnikání a patří podnikateli. [1]
Aktivem je tedy cokoli, co by mělo být v dané firmě chráněno. Hodnota aktiv je uváděna v Kč. Mezi aktiva firmy XY patří např. výrobní stroje, vyrobený materiál na skladě, materiál k výrobě, ale i dopravní prostředky, software, počítačové vybavení, peněžní prostředky apod. Hodnota aktiv firmy XY se pohybuje kolem 6 miliónů Kč.

Možné hrozby

Hrozbou označujeme možnost odhalení zranitelného místa. Zranitelným místem je absence bezpečnostního opatření, která může být využita ke způsobení škody nebo k potencionálnímu trestnému činu.

Podíl ztráty (PZ)

Poměrná ztráta, kterou by měla firma očekávat, v případě, že budou aktiva ovlivněna nějakým rizikem.

Očekávanou ztrátu (OZ)

Náklady související s jedním uskutečněným rizikem vůči aktivům.

Roční očekávané výskyty (ROV_1)

Představují očekávanou roční frekvenci výskytu možného rizika nebo hrozby za rok.

Roční očekávané ztráty (ROZ_1)

Představují očekávané roční náklady výskytu hrozby na aktiva.

Přehled bezpečnostních opatření

Bezpečnostní opatření chrání aktiva proti jedné nebo více hrozbám a odstraňují tak zranitelná místa. Implementace bezpečnostních opatření slouží ke snížení nebo eliminaci ročních očekávaných výskytů hrozeb, čím se sníží i roční očekávané ztráty.

Analýzu ročních nákladů na bezpečnostní opatření aktiv vůči každé hrozbě (RNBO)

Pří výpočtu ročních nákladů na bezpečnostní opatření je třeba vzít v potaz životnost bezpečnostního opatření.

Nové roční očekávané výskyty (ROV_2)

Nové roční očekávané výskyty po implementací bezpečnostních mechanismů.

Nové roční očekávané ztráty (ROZ_2)

Nové roční očekávané ztráty po implementací bezpečnostních mechanismů.

Analýzu hodnoty bezpečnostních opatření aktiv vůči hrozbám (HBO)

Hodnota bezpečnostního opatření může nabývat záporných i kladných hodnot.

16.1 Neoprávněné vniknutí

Tato hrozba se týká obvodové ochrany. Jedná se o to, aby se do areálu firmy nedostala neoprávněna osoba za účelem získání informací o firmě a zaměstnancích, páchání škod na aktivech firmy nebo krádeže.

Stanovení podílu ztráty (PZ)

Firma XY je v současné době vybavena některými prvky obvodové, plášťové, prostorové a předmětové ochrany. Podíl ztráty stanovuji orientačně na hodnotu 0,3.

Výpočet očekávané ztráty (OZ)

OZ = HA x PZ

OZ = 6 000 000 x 0,3

OZ = 1 800 000 Kč

Stanovení ročních očekávaných výskytů (ROV_1)

Dle statistiky firmy XY o počtu neoprávněných vniknutí do objektu firmy od vzniku do současné doby stanovuji roční očekávané výskyty na hodnotu 0,17 (čtyři neoprávněné vniknutí za 24 let)

Výpočet roční očekávané ztráty (ROZ_1)

$ROZ_1 = OZ \times ROV_1$

$ROZ_1 = 1\,800\,000 \times 0{,}17$

$ROZ_1 = 306\,000$ Kč

Firma by si měla každý rok spořit 306 000 Kč pro případ, že by nastala hrozba neoprávněného vniknutí.

Přehled bezpečnostních opatření

- Kamerový systém
- Nové oplocení

Analýza ročních nákladů na bezpečnostní opatření (RNBO)

RNBO = cena bezpečnostního opatření (Kč) / délka životnosti bezpečnostního opatření (rok)

$RNBO_{Kamerového\ systému}$ = 56 665 / 15

$RNBO_{Kamerového\ systému}$ = 3 778 Kč

$RNBO_{Oplocení}$ = 44 128 / 30

$RNBO_{Oplocení}$ = 1 471 Kč

Nové roční očekávané výskyty (ROV_2)

Nové roční očekávané výskyty po implementací bezpečnostních mechanismů stanovuji orientačně na hodnotu 0,05 (jednou za 20 let)

Nové roční očekávané ztráty (ROZ_2)

$ROZ_2 = OZ \times ROV_2$

ROZ_2 = 1 800 000 x 0,05

ROZ_2 = 90 000 Kč

Analýza hodnoty bezpečnostních opatření aktiv vůči hrozbám (HBO)

$HBO = (ROZ_1 – ROZ_2) – RNBO$

HBO = (306 000 – 90 000) – (3 778 + 1 471)

HBO = 210 751 Kč

Implementací těchto bezpečnostních opatření sníží firma XY výskyt hrozby neoprávněného vniknutí a sníží tak i očekávané ztráty ročně o 210 751 Kč ročně.

16.2 Vloupání

Tato hrozba se týká plášťové ochrany. Vloupání je způsob spáchání trestného činu. Pachatel vnikne do uzavřeného prostoru překonáním překážky pomocí hrubé síly, lsti nebo překonáním uzamčení. Tato hrozba souvisí s hrozbou neoprávněného vniknutí. Areál firmy se nachází

u lesa na kraji města, což potencionálnímu pachateli umožňuje snadný útěk. Je tedy velmi pravděpodobné, že by mohlo dojít k vloupání do některé z budov firmy.

Stanovení podílu ztráty (PZ)

Firma XY je v současné době vybavena některými prvky obvodové, plášťové, prostorové a předmětové ochrany. Jelikož se tato hrozba vztahuje nejvíce na budovy č.2 a 3 kvůli úrovni jejich plášťové ochrany, stanovuji podíl ztráty orientačně na hodnotu 0,1.

Výpočet očekávané ztráty (OZ)

OZ = HA x PZ
OZ = 6 000 000 x 0,1
OZ = 600 000 Kč

Stanovení ročních očekávaných výskytů (ROV_1)

Dle statistiky firmy XY o počtu vloupání do objektů firmy od vzniku do současné doby stanovuji roční očekávané výskyty na hodnotu 0,17 (čtyři neoprávněné vniknutí za 24 let)

Výpočet roční očekávané ztráty (ROZ_1)

$ROZ_1 = OZ \times ROV_1$
$ROZ_1 = 600\,000 \times 0{,}17$
$ROZ_1 = 102\,000$ Kč
Firma by si měla každý rok spořit 102 000 Kč pro případ, že by nastala hrozba vloupání.

Přehled bezpečnostních opatření

- Bezdrátový zabezpečovací systém
- Bezpečnostní fólie

Analýza ročních nákladů na bezpečnostní opatření (RNBO)

RNBO = cena bezpečnostního opatření (Kč) / délka životnosti bezpečnostního opatření (rok)
$RNBO_{\text{Zabezpečovacího systému}} = 18\,793 / 20$
$RNBO_{\text{Zabezpečovacího systému}} = 940$ Kč
$RNBO_{\text{Bezpečnostní fólie}} = 113\,520 / 15$
$RNBO_{\text{Bezpečnostní fólie}} = 7\,568$ Kč

Nové roční očekávané výskyty (ROV_2)

Nové roční očekávané výskyty po implementací bezpečnostních mechanismů stanovuji orientačně na hodnotu 0,05 (jednou za 20 let)

Nové roční očekávané ztráty (ROZ_2)

$ROZ_2 = OZ \times ROV_2$

$ROZ_2 = 600\,000 \times 0{,}05$

$ROZ_2 = 30\,000$ Kč

Analýza hodnoty bezpečnostních opatření aktiv vůči hrozbám (HBO)

$HBO = (ROZ_1 - ROZ_2) - RNBO$

$HBO = (102\,000 - 30\,000) - (940 + 7\,568)$

$HBO = 63\,492$ Kč

Implementací těchto bezpečnostních opatření sníží firma XY výskyt hrozby vloupání a sníží tak i očekávané ztráty ročně o 63 492 Kč.

16.3 Požár

Firma XY pracuje s hořlavými látkami, což zvyšuje pravděpodobnost vypuknutí požáru. Požár může vzniknout nějakou závadou (např. porucha stroje), nedbalostí pracovníka (např. špatné zacházení se zařízeními). Jelikož jsou všechny budovy starší výstavby, je další možností vypuknutí požáru ve všech budovách areálu závada elektroinstalace.

Stanovení podílu ztráty (PZ)

V areálu firmy se nacházejí čtyři budovy, které nejsou vzájemně propojeny. Případný požár, který vypukne v jedné z budov se velkou pravděpodobností nerozšíří na další budovy. Největší pravděpodobnost vypuknutí požáru je budova č. 1, ve které se nachází výrobní dílny a rozvodna elektrické energie. Podíl ztráty stanovuji orientačně na hodnotu 0,4.

Výpočet očekávané ztráty (OZ)

$OZ = HA \times PZ$

$OZ = 6\,000\,000 \times 0{,}4$

$OZ = 2\,400\,000$ Kč

Stanovení ročních očekávaných výskytů (ROV_1)

Dle statistiky firmy XY o počtu vypuknutí požáru v areálu firmy od vzniku do současné doby stanovuji roční očekávané výskyty na hodnotu 0,21 (5 vypuknutí požáru za 24 let)

Výpočet roční očekávané ztráty (ROZ_1)

$ROZ_1 = OZ \times ROV_1$

$ROZ_1 = 2\ 400\ 000 \times 0{,}21$

$ROZ_1 = 504\ 000$ Kč

Firma by si měla každý rok spořit 504 000 Kč pro případ, že by nastala hrozba vypuknutí požáru.

Přehled bezpečnostních opatření

- Elektrická požární signalizace

Analýza ročních nákladů na bezpečnostní opatření (RNBO)

RNBO = cena bezpečnostního opatření (Kč) / délka životnosti bezpečnostního opatření (rok)

$RNBO_{EPS} = 857\ 664 / 20$

$RNBO_{EPS} = 42\ 883{,}2$ Kč

Nové roční očekávané výskyty (ROV_2)

Nové roční očekávané výskyty po implementací bezpečnostního mechanismu stanovuji orientačně na hodnotu 0,05 (jednou za 20 let)

Nové roční očekávané ztráty (ROZ_2)

$ROZ_2 = OZ \times ROV_2$

$ROZ_2 = 2\ 400\ 000 \times 0{,}05$

$ROZ_2 = 120\ 000$ Kč

Analýza hodnoty bezpečnostních opatření aktiv vůči hrozbám (HBO)

$HBO = (ROZ_1 - ROZ_2) - RNBO$

$HBO = (504\ 000 - 120\ 000) - 42\ 883{,}2$

$HBO = 341\ 117$ Kč

Implementací tohoto bezpečnostního opatření sníží firma XY výskyt hrozby neoprávněného vniknutí a sníží tak i očekávané ztráty ročně o 341 117 Kč.

ZÁVĚR

V současné době jsou kladeny neustále vetší požadavky na zabezpečení veškerého majetku a dat. V této bakalářské práci se zabývám mechanickými a poplachovými zabezpečovacími systémy obvodové, plášťové, prostorové a předmětové ochrany. Dále se zabývám možnosti ochrany zaměstnanců a firemních dat, elektrickou požární signalizací, kamerovými systémy, elektronickou kontrolou vstupů a analýzu rizik, která popisuje pravděpodobnost a následky negativní události.

Cílem práce je vytvoření návrhu na zlepšení zabezpečení vybrané firmy. Prvním krokem k vytvoření návrhu bylo zjištění a popis současného stavu zabezpečení areálu firmy, budov a dat, na jehož základě jsem odhalil nedostatky v zabezpečení.

Za hlavní nedostatek v obvodové ochraně považuji staré oplocení podél příjezdové cesty. Pro návrh nového oplocení jsem využil internetové stránky, podle kterých jsem navrhnul oplocení stejné konstrukce, které tvoří zbylé oplocení areálu. Cena nového oplocení činí 44 128 Kč bez DPH. Mezi hlavní nedostatky v plášťové ochraně budov považuji chybějící zabezpečení oken v prvních patrech budov č.2 a 3 a chybějící bezpečnostní systémy signalizující neoprávněné vniknutí do prostor budov č. 2 a 3 prostřednictvím vchodových dveří, která jsou mimo areál firmy. Pro zabezpečení skleněných ploch jsem na internetových stránkách vybral bezpečnostní fólii SMC AX 300 µm 12 Mil. Cena bezpečnostní fólie činí 113 520 Kč bez DPH. Pro zabezpečení vchodových dveří, která jsou mimo areál firmy byl navržen firmou IT Outsourcing bezdrátový zabezpečovací systém. Cena bezdrátového zabezpečovacího systému činí 18 793 Kč bez DPH. Dalším nedostatkem v obvodové a zároveň prostorové ochraně je absence kamerového systému, který slouží k monitorování objektu a jeho okolí. Pro objekt firmy byl navržen kamerový systém firmou IT Outsourcing. Cena kamerového systému činí 56 665 Kč bez DPH. Posledním výrazným nedostatkem v zabezpečení firmy je absence elektrické požární signalizace detekující vzniklý požár. Návrh na zavedení EPS pro všechny budovy v objektu provedla firma PATROL group s.r.o. Cena zavedení elektrické požární signalizace činí 857 664 Kč bez DPH. Celkové náklady na nové zabezpečení firmy tedy činí 1 090 770 Kč bez DPH.

V závěru práce jsem provedl orientační analýzu rizik. Na základě výsledků této analýzy by se měla firma XY rozhodnout, zda investovat do zdokonalení zabezpečení objektu za účelem snížení rizika nebo riziko podstoupit, akceptovat či ignorovat.

V rámci hrozby neoprávněného vniknutí, která se týká obvodové ochrany by měla firma očekávat roční ztrátu 306 000 Kč v případě, že by toto riziko nastalo. Implementací

bezpečnostních opatření, kterými jsou nové oplocení a kamerový systém by firma snížila roční očekávané výskyty hrozby a snížila by tak i očekávané ztráty o 210 751 Kč ročně. V rámci hrozby vloupání, která se týká plášťové ochrany by měla firma očekávat roční ztrátu 102 000 Kč v případě, že by toto riziko nastalo. Implementací bezpečnostních opatření, kterými jsou bezdrátový zabezpečovací systém a bezpečnostní fólie by firma snížila roční očekávané výskyty hrozby a snížila by tak i očekávané ztráty o 63 492 Kč ročně. V rámci hrozby vypuknutí požáru by měla firma očekávat roční ztrátu 504 000 Kč v případě, že by toto riziko nastalo. Implementací bezpečnostního opatření, kterým je elektrická požární signalizace by firma snížila roční očekávané výskyty hrozby a snížila by tak i očekávané ztráty o 341 117 Kč ročně.

Dle mého názoru by firma XY neměla spoléhat na skutečnost, že se riziko neuskuteční, jako je to v případě elektrické požární signalizace. Z analýzy rizik je patrné, že by firma implementací nových bezpečnostních opatření snížila ztráty, které by mohli nastat a zvýšila by tak i míru zabezpečení celého areálu firmy.

POUŽITÁ LITERATURA

[1] Aktiva, majetek (Assets) - *ManagementMania.com.* [online]. ©2011, 12.08.2017 [cit. 2021-04-28]. Dostupné z: https://managementmania.com/cs/aktiva

[2] Bezpečnost, ochrana – *Wikisofia.* [online]. ©2013 ISSN [cit. 2021-04-28]. Dostupné z: https://wikisofia.cz/wiki/Bezpe%C4%8Dnost,_ochrana

[3] Bezpečnostní fólie. *Okenní fólie (folie) - Petr Benda* [online]. ©2002 - 2018 [cit. 2021-04-28]. Dostupné z: https://www.benda-folie.cz/bezpecnostni-folie

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

[5] ČANDÍK, Marek. *Objektová bezpečnost II*. Zlín: Univerzita Tomáše Bati, 2004. Učební texty vysokých škol. ISBN 80-7318-217-3.

[6] Čím se odlišují bezpečnostní třídy dveří? – HT dveře. *htdvere.cz* [online]. [cit. 2021-04-28]. Dostupné z: https://www.htdvere.cz/poradna/cim-se-odlisuji-bezpecnostni-tridy-dveri/

[7] Definice malého a středního podniku aneb tichý zabiják dotací. *pravniprostor.cz* [online]. ©1999, 16.10.2019 [cit. 2021-04-28]. Dostupné z: https://www.pravniprostor.cz/clanky/obchodni-pravo/problematika-spojovani-malych-a-strednich-podniku-z-pohledu-dotacnich-pravidel

[8] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[9] Fólie na okna - Ceník - Petr Benda. *Okenní fólie (folie) - Petr Benda* [online]. ©2002 [cit. 2021-04-28]. Dostupné z: https://www.benda-folie.cz/ceniky

[10] GDPR (obecné nařízení): Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů:* [online]. ©2013 [cit. 2021-04-28]. Dostupné z: https://www.uoou.cz/gdpr/ds-3938/p1=3938

[11] Hrozba (Threat) - *ManagementMania.com.* [online]. ©2011, 17.02.2016 [cit. 2021-04-28]. Dostupné z: https://managementmania.com/cs/hrozba-threat

[12] HUB, Miloslav. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.

[13] IP kamery. *Jabloshop* [online]. [cit. 2021-04-28]. Dostupné z: https://www.jabloshop.cz/ip-kamery

[14] Kamerové systémy - IP kamery. *Kamerové systémy | Kamerové systémy Brno, Praha, Ostrava | Kamerový systém* [online]. [cit. 2021-04-28]. Dostupné z: https://www.kamerovysystem.cz/kamerove-systemy/ahd-kamery/ahd_kamerove_systemy.php

[15] KIZZA, Joseph Migga. *Guide to computer network security*. Fourth edition. Cham, Switzerland: Springer-Verlag, 2017. Computer communications and networks. ISBN 978-3-319-55605-5.

[16] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 3. [Blatná: Cricetus], 2006. ISBN 80-902938-2-4.

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

[18] Legislativa (Legislation) - *ManagementMania.com.* [online]. ©2011, 30.07.2017 [cit. 2021-04-28]. Dostupné z: https://managementmania.com/cs/legislativa

[19] *Okenní fólie (folie) - Petr Benda* [online]. [cit. 2021-04-28]. Dostupné z: https://www.benda-folie.cz/images/parametry/folie/fusion_smc_ax_12.jpg

[20] Pletiva Dobrý - pletiva, ploty prodáváme i montujeme. *levne-pletivo.cz* [online]. [cit. 2021-02-13]. Dostupné z: https://www.levne-pletivo.cz/

[21] Riziko - Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. ©2020 Ministerstvo vnitra České republiky, všechna práva vyhrazena, 2003 [cit. 2021-04-28]. Dostupné z: https://www.mvcr.cz/clanek/riziko.aspx

[22] Rozdělení a druhy bezpečnostních kamer CCTV. *Využití bezpečnostních kamerových systémů* [online]. ©2011 [cit. 2021-04-28]. Dostupné z: http://www.hlidacikamery.cz/druhy-kamer/

[23] Stanovení úrovně zabezpečení objektů a provozoven proti vloupání podle evropských technických norem. *Ministerstvo vnitra České republiky* [online]. ©2020 [cit. 2021-04-28]. Dostupné z: https://www.mvcr.cz/clanek/stanoveni-urovne-zabezpeceni-objektu-a-provozoven-proti-vloupani-podle-evropskych-technickych-norem.aspx

[24] UHLÁŘ, Jan. *Technická ochrana objektů*. 1. díl, Mechanické zábranné systémy II. Praha: Vydavatelství Policejní akademie ČR, 2004. ISBN 80-7251-172-6.

[25] UHLÁŘ, Jan. *Technická ochrana objektů*. 3. díl, Ostatní zabezpečovací systémy. Praha: Vydavatelství Policejní akademie ČR, 2006. ISBN 80-7251-235-8.

[26] URBAN, Miroslav a Tomáš KONÍČEK. Předpisy související s poskytováním technických služeb k ochraně majetku a osob *Ministerstvo vnitra České republiky* [online]. ©2021, 17.9.2010 [cit. 2021-04-28]. Dostupné z: https://www.mvcr.cz/clanek/dokumenty-prevence-aktuality-predpisy-souvisejici-s-poskytovanim-technickych-sluzeb-k-ochrane-majetku-a-osob.aspx

[27] Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti - Zákony.cz. *Zákony.cz - Právní poradna, smlouvy* [online]. Heagl, s.r.o., ©2020 [cit. 2021-04-28]. Dostupné z: https://www.zakony.cz/zakony/2005/401/zakon-412-2005-Sb-SB2005412