Návrh na zabezpečení velké tiskárny včetně osob a vozidel

Bc. Andrea Talašová

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

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

Jméno a příjmení:	**Bc. Andrea Talašová**
Osobní číslo:	**A14386**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Návrh opatření k zabezpečení velké tiskárny včetně kontroly osob a vozidel**
Téma anglicky:	**Draft Measures to Secure Large Printers – Including Checks on Persons and Vehicles**

Zásady pro vypracování:

1. **Zpracujte systémy vhodné pro zabezpečení velké tiskárny.**
2. **Popište organizační strukturu, pohyb osob a materiálů v tiskárně.**
3. **Analyzujte rizikové faktory v tiskárně s ohledem na minulé události.**
4. **Navrhněte režimová opatření pro pohyb osob ve firmě.**
5. **Doporučte technická opatření pro zabezpečení firmy včetně zajištění přístupových bodů proti průniku zbraní, výbušnin a jiných nebezpečných látek.**
6. **Proveďte ekonomické zhodnocení navrhovaných řešení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BRABEC, František. Ochrana bezpečnosti podniku. Vyd. 1. Praha: Eurounion, 1996, 203 s. ISBN 80-85858-29-0.**
2. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 978-80-7318-889-4.**
3. **UHLÁŘ, Jan. Technická ochrana objektů. Vyd. 1. Praha: Vydavatelství PA ČR, 2005, 229 s. ISBN 80-7251-189-0.**
4. **IVANKA, Ján. Systemizace bezpečnostního průmyslu I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 123 s. ISBN 978-80-7318-850-4.**
5. **UHLÁŘ, Jan. Technická ochrana objektů. Vyd. 1. Praha: Vydavatelství PA ČR, 2006, 246 s. ISBN 80-7251-235-8.**
6. **BRABEC, František. Hlídací služby. Praha: Eurounion, 1995, 259 s. ISBN 80-85858-12-6.**
7. **ČERNÝ, Josef. Evropský výcvikový modul pro základní ostrahu. Vyd. 1. Zlín: Univerzita Tomáše Bati, Technologická fakulta, 2003, 152 s. ISBN 80-7318-107-x.**
8. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 122 s. ISBN 80-7318-231-9.**

Vedoucí diplomové práce: **Ing. Rudolf Drga, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **5. února 2016**

Termín odevzdání diplomové práce: **16. května 2016**

Ve Zlíně dne 5. února 2016

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

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 připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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/bakalářské 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, dne …….

podpis diplomanta

ABSTRAKT

Diplomová práce pojednává o problematice bezpečnosti a možnostech jejího zajištění v provozu velké tiskárny. V teoretické části jsou specifikovány pojmy bezpečnost, riziko a elektronické zabezpečovací systémy a detektory kovů. Dále je zde popsána bezpečnostní služba a jednotlivé druhy ochrany. Praktická část je poté zaměřena na analýzu bezpečnostní situace v tiskárně, s cílem navrhnout řešení v podobě režimových a technických opatření, která zvýší úroveň zabezpečení v tiskárně. Jsou zde také specifikovány rizikové faktory, které se mohou podílet na vzniku nežádoucích událostí. Závěr práce poté obsahuje ekonomické zhodnocení navrhovaného řešení zabezpečení tiskárny.

Klíčová slova: bezpečnost, riziko, režimové opatření, analýza, kamerový systém, detektory

ABSTRACT

The thesis discusses the security issues and the possibilities of ensuring the operation of a printer. The theoretical part specifies the terms security, risk and electronic security systems and metal detectors. There is also described security service and the different types of protection. The practical part is then focused on the analysis of the security situation in the printer, in order to propose solutions in the form of procedural and technical measures that increase the level of security in the printer. There are also specified risk factors that may be involved in the occurrence of adverse events. Conclusion of work then includes the economically evaluate proposed solutions to security printers.

Keywords: security, risk and regular measure, analyze, CCTV, detectors

Ráda bych poděkovala Ing. Rudolfovi Drgovi, Ph.D. za vedení, podporu a pomoc pří psaní diplomové práce.
Dále bych chtěla poděkovat svým rodičům za jejich trpělivost podporu během celého studia.

OBSAH

ÚVOD

Bezpečnost je v dnešní společnosti vnímána, jako jeden z významných fenoménů, kterému je potřeba věnovat zvýšenou pozornost. Bezpečnost by měla být součástí každodenních situací, ale vždy tomu tak bohužel není. Ať už nás o tom přesvědčují stále častější a sofistikovanější systematické snahy o narušení bezpečnosti v podobě teroristických útoků nebo migrační krize, která je středem zájmu největších světových odborníků na bezpečnost.

Bezpečnost se dá rozdělit na přibližně padesát oblastí a jednou z nich, je oblast zabezpečení budov proti nepovolenému vstupu, v podobě technických a režimových opatření. Tato problematika je řešena jak v soukromé, tak i veřejné sféře, a je tedy významnou oblastí, kterou je třeba se zabývat. Ať už se jedná o provoz malého obchodu nebo budovu parlamentu, každý objekt by měl splňovat určitá bezpečnostní kritéria, v podobě implementovaných bezpečnostních opatření. Tato problematika je předmětem této diplomové práce, která je zaměřena na soukromou sféru.

Teoretická část je zaměřena na vysvětlení pojmů riziko a bezpečnost. Je zde charakterizována problematika elektronických zabezpečovacích systémů. Z této oblasti jsou zde detailněji popsány jednotlivé části poplachových systémů, včetně systému pro kontrolu vstupu a sledovacích systémů pro použití v bezpečnostních aplikacích (CCTV). V této části diplomové práce, je také rozpracována oblast bezpečnostní služby a základní druhy ochrany, které úzce souvisí s tématem.

Praktická část diplomové práce je zaměřena na analýzu a popis velké tiskárny, která je předmětem mého výzkumu. Důraz je kladen především na rizikové faktory, vyskytující se v dané oblasti. Na základě analýzy stávající situace ve firmě, je navrženo konkrétní řešení, v podobě efektivních režimových a technických opatření, která by měla zlepšit bezpečnostní situaci v tiskárně, vzhledem k událostem, které se zde odehrály v minulosti.

V závěru práce je pak zpracována ekonomická analýza, která je zaměřena na finanční zhodnocení navrhovaných řešení. Cílem této analýzy je poskytnout přehled nákladů, které by měly být vynaloženy na zlepšení bezpečnostní situace ve firmě, s cílem předcházet rizikovým událostem, které by mohly představovat budoucí hrozby.

I. TEORETICKÁ ČÁST

1 TERMINOLOGIE A LEGISLATIVA

Kapitola terminologie a legislativa popisuje pojmy jako je bezpečnost, riziko základní druhy ochrany a bezpečnostní riziko. Dále popisuje normy týkající se zabezpečení tiskárny.

1.1 Terminologie

V oblasti terminologie si více přiblížíme pojmy riziko, bezpečnost a základní druhy ochrany.

1.1.1 Riziko

Riziko je výraz spojený s pravděpodobností nebo s možností škody. Je to nějaká očekávaná hodnota škody, výsledek aktivace určitého nebezpečí, které vyústí v určitý negativní následek, škodu. Riziko vyjadřuje míru a stupeň ohrožení. Tímto pojmem se vyjadřuje pravděpodobnost, že vznikne negativní jev a zároveň i důsledky tohoto jevu. Vyjadřuje, kolikrát se negativní jev vyskytne a co způsobí.

Riziko má vždy dva rozměry:

- pravděpodobnost vzniku nebezpečné situace ohrožení
- závažnost možného vzniku

Analýza rizik – Prvním krokem procesu snižování rizika je jejich analýza. Analýza rizik je obvykle chápána jako proces definování hrozeb, pravděpodobnosti jejich uskutečnění a dopadu na aktiva, tedy stanovení rizik a jejich závažnosti.

Analýza rizik zahrnuje:

1. Identifikaci rizik – vymezení posuzovaného subjektu a popis aktiv, které vlastní,
2. stanovení hodnoty aktiv – určení hodnoty aktiv a jejich význam pro subjekt,
3. identifikaci hrozeb a slabin – určení druhů událostí a akcí, které mohou ovlivnit negativně hodnotu aktiv, určení slabých míst subjektu,
4. stanovení závažnosti hrozeb a míry zranitelnosti – určení pravděpodobnosti výskytu hrozby a míry zranitelnosti subjektu vůči dané hrozbě. [16]

Bezpečnostní riziko

Při vyhledávání a stanovování bezpečnostních rizik je potřeba si ujasnit pojem hrozba.

- *„Co osobě nebo objektu hrozí?*
- *Od koho jí to hrozí?*

Sedm základních otázek: Kdo, Co, Kdy, Kde, Jak, Čím, Proč?“ [1]

1.1.2 Bezpečnost

Bezpečnost je pojem bezpečnostní terminologie. Bývá definována negativně, ve vztahu k (neexistujícím) nebezpečím, hrozbám apod. V angličtině a francouzštině rozlišují security a safety; tato odlišnost se v ostatních jazycích neobjevuje. Taktéž v češtině nemá náhradu. *„Safety of radiation sources se obzvláště týká opatření snižujících pravděpodobnost, že v jaderném zařízení nebo u rentgenového přístroje se přihodí nehoda, jež přivodí nepřípustné ozáření lidí. Security of radioactive materials naproti tomu znamená zabránění např. neautorizovaného zneužití ionizujících a štěpných materiálů. Protiopatření k posílení safety a security se přirozeně zřetelně odlišuji. V tomto smyslu je bezpečnost pojímána jako ideální typus, protože většinou je možné dosáhnout pouze určitého rozsahu eliminace hrozeb či ochrany před hrozbami.“* [15]

„Podle Petra Robejška slovo „securitas“ pochází ze „sine-cura“ nebo-li „bez starosti“ a může byt chápána jako stav všeobecné jistoty, „nebezpečnosti“. V realitě nedosahuje bezpečnost ani přibližně tu úroveň, kterou sugeruje slovo bezpečnost sám, nýbrž opatří spíše obecnou ideu o žádoucím stavu a nasměrování pokusů ke snížení rizik.“ [15]

Slovo bezpečnost bývá doplňováno i jinými adjektivy, která se vztahují především k charakteru (původu):

1. hrozeb, které bezpečnost ohrožuji,
2. opatřeni, prostředků nebo instituci, které mají bezpečnost zajišťovat a chránit,
3. objektů, jejichž bezpečnost má být chráněna. [15]

1.1.3 Událost v minulosti

Před několika lety, kdy firma propustila jednoho ze zaměstnanců došlo později ve firmě ke střelbě. Bývalý zaměstnanec postřelil dva představitele firmy a zbraň poté obrátil proti sobě. Ve dvou případech se jednalo o střelná poranění hlavy, další osoba byla zraněna v oblasti třísel, horní končetiny a krku. Bývalý zaměstnanec, střelec, při převozu do nemocnice zraněním podlehl. Propuštěný zaměstnanec se mstil za propuštění z důvodu opakovaného hrubého porušování pracovní kázně. V té době se snižovaly počty zaměstnanců. Tehdy se jednalo o snižování počtu zaměstnanců, nešlo ale o hromadné propouštění.

1.1.4 Základní druhy ochrany

Řešení skutečných problémů ochrany musí být pokaždé prováděno komplexně, přestože jednotlivé druhy ochrany jsou natolik specifické, že se jimi nyní budeme zabývat samostatně. Zabezpečovací systémy dělíme na čtyři základní druhy ochrany:

- Klasická ochrana
- Režimová ochrana
- Fyzická ochrana
- Technická ochrana

Klasická ochrana

Představuje nejstarší typ ochrany a spočívá v tom, že k zajištění příslušného objektu použijeme taková mechanická zařízení, která jej dovolí spolehlivě ochránit. Jedná se zejména o vytváření různých zábran, znemožňujících zpravidla odcizení či zničení cenných předmětů, výrobku, zboží, zařízení anebo takových překážek, které by pachateli značně ztížily dosažení jeho cíle.

Tyto různé zábrany odpovídaly technické úrovni své doby, ať už šlo o ploty, mříže, budovy na nepřístupných místech, různé typy zámku apod. Každým dnem se s technickým pokrokem zábrany stále zdokonalovaly a doposud se zdokonalují, avšak zároveň se objevovaly a i nyní se objevují prostředky, jak tyto zábrany překonávat. Klasická ochrana je základem každého zabezpečovacího systému. Setkáváme se s ní prakticky na každém objektu. Často bývá chápána jako zcela postačující ochrana proti vloupání, když

mechanické zábrany mohou být hodnoceny jedině z hlediska času, po který vydrží odolávat napadení.

Prostředky klasické ochrany musí být vždy kombinovány s ostatními druhy ochrany a vzájemně se s nimi doplňovat a podporovat.

Režimová ochrana

Je souborem organizačně administrativních opatření a postupů směřujících k zajištění požadovaných okolností pro funkci zabezpečovacího systému a jeho sladění s provozem chráněného objektu. Ve své podstatě režimová ochrana zajišťuje možnost funkce ostatních druhů ochrany a rovněž snižuje zranitelnost chráněných zájmů množstvím dalších forem kriminální trestné činnosti, jako je vandalismus, výtržnosti, loupeže, přepadení, drobné krádeže, sabotáže, žhářství, průmyslová špionáž. V praxi jde o směrnice pro vstup, odchod a pohyb osob po objektu, pro manipulaci s hodnotami a informacemi, provoz a využívání zabezpečovacích systémů, výkon služby ostrahy objektu.

Základním problémem není vytvoření účinných bezpečnostních směrnic jako režimových opatření, ale jejich prosazování a zavádění do každodenního života objektu. To se může zdařit jenom v úzké součinnosti se všemi pracovníky objektu a s plnou podporou vedení. V každé pokročilé společnosti se potřeba systematického řešení ochrany stala organickou součástí struktury podniků a organizací.

Režimová opatření se dělí na:

- Vnější,
- vnitřní.

Vnější režimová opatření

Tato opatření se týkají zvláště vstupních a výstupních podmínek u chráněného objektu, prostorů, kterými se vozidla i osoby dostávají do objektu a kudy jej opouštějí. Jsou to hlavně osobní a nákladové brány. Opatření režimového charakteru většinou stanoví kde, kdy, jak a čím se smí nebo nesmí do objektu vstupovat a objekt opouštět. Také je důležité, že se stanoví konkrétní kontrolní opatření, která se obvykle pří projektování řeší předpokládanou ostrahou – fyzickou silou.

Vnitřní režimová opatření

Vnitřní režimová opatření chráněného objektu se týkají dodržování následujících bezpečnostních směrnic:

- Omezení pohybu osob a vozidel v objektu jen na určité oblasti nebo okruhy. Většinou se s tím spojuje i omezení vstupu do určitých prostorů pouze pro konkrétní pracovníky. Tam, kde se jedná o prostory zvláštní důležitosti, bývá takový prostor i uvnitř objektu ohrazen a vstup bývá kontrolován ostrahou objektu,
- zvláštního režimu, dodržovaného na vnitřní straně vnějšího ohrazení. To spočívá jak v udržování dobrého stavu ohrazení, tak ve vytvoření přehledových nebo i kontrolních pásem u tohoto ohrazení. Dále v zajištění osvětlení, ve vytvoření druhého vnitřního oplocení, které umožňuje do chráněného prostoru vpouštět psy. Na druhé straně je to vytvoření technických ochranných bariér, které upozorňují na přiblížení živého subjektu nebo mechanického prostředku, režimu pohybu materiálu, vytvářejícímu podmínky, které zamezují úniku zbytných nebo neevidovaných materiálů nebo výrobků, skladových režimů, určujících způsob příjmu a výdeje materiálů od překročení hranice objektu až po jeho opuštění a řady dalších dílčích opatření.[5]

Ochrana vnitřních a vnějších vztahů

1. Ochrana vnitřních vztahů:

- *„Detektivní ochrana proti zakázanému podnikání zaměstnanců uvnitř chráněného objektu a na jeho úkor*
- *Detektivní ochrana proti rozkrádání uvnitř podniku*
- *Informační funkce pro potřeby personální práce.*

2. Ochrana vnějších vztahů:

- *Ochrana proti úniku utajovaných nebo důvěrných informací*
- *Informační činnost o konkurenci*
- *Informační činnost marketingového charakteru*
- *Ochrana proti formám firemní špionáže.“* [10]

Fyzická ochrana

Ochrana prováděná strážnými, vrátnými, hlídací službou či policisty. Na její úrovni závisí výsledná činnost všech ostatních druhů ochrany. *„I když postupy a prostředky klasické, režimové, technické ochrany jsou spolehlivé, jsou vyhovující jen do určité míry účinnosti reakce lidí.“* Fyzická ochrana patří mezi nejdražší ochranu, co se týká zabezpečení. Na rozdíl do jiných druhů ochrany, které vyžadují poměrně vysoké počáteční investice (kromě režimové) a potom jen nízkou režii, fyzická ochrana má pořizovací náklady poměrně nízké (výstroj, výzbroj, základní výcvik), ale vysokou režii. Je potřebné ji kombinovat s dalšími dostupnými prostředky ochrany, abychom docílili co nejvyšší efektivnosti. [5]

Ochrana podle časového rozvrhu:

- *„Fyzická ochrana v době pracovní doby*
- *Fyzická ochrana nepřetržitá*
- *Fyzická ochrana nárazová*

Podle druhu výkonu:

- *Fyzická ochrana dohledová*
- *Fyzická ochrana doprovodná*
- *Fyzická ochrana víceúčelová, atd.*

Podle způsobu zajištění:

- *Fyzická ochrana z řad vlastních pracovníků*
- *Fyzická ochrana na smluvním základě*
- *Fyzická ochrana smíšená*

Podle způsobu výstroje a výzbroje:

- *Fyzická ochrana ozbrojená*
- *Fyzická ochrana neozbrojená*
- *Fyzická ochrana civilní*
- *Fyzická ochrana uniformovaná, atd.“* [9]

Technická ochrana

Je to relativně nový druh zabezpečení objektů, protože tyto prostředky jsou z hlediska dnešních požadavků i technických možností spolu s rychlostí zákroku zásahové jednotky nejspolehlivější a špatně překonatelné. Velmi dobře doplňují dosavadní systém klasické ochrany. Hlavní funkce spočívá v tom, že velmi rychle reagují na změny vyvolané pachatelem, díky těmto změnám indikovaným i na větší vzdálenosti, uvádějí v činnost síly schopné v dalším průběhu narušení pachateli zabránit a dostihnout jej prakticky ještě před dokonáním činu.

Tato ochrana není sama o sobě ochranou, ale má směrem k pachateli odstrašující účinek. Obecně jde o detekční systém a ten zajišťuje a předává informace o situaci v chráněném prostoru. *„Situací v daném prostoru rozumíme souhrn fyzikálních i jiných veličin, které jsou technickými prostředky vyhodnocovány jako „možnost nebezpečí.“* [5]

Úkoly technické ochrany v rámci zabezpečení objektů velmi účinně doplňuje dosavadní bezpečnostní systém a má dva úkoly:

1) *„Podpořit klasickou ochranu, zajišťovat a předávat informace při jejím napadení, umožnit tak fyzické ochraně včasný zásah,*

2) zvýšit efektivnost fyzické ochrany, např.: aby hlídka jako fyzická ostraha prošla kolem každého prostředku klasické ochrany alespoň jednou za dobu odpovídající jeho zpožďovacího reflexu.“ [5]

Při vhodném výcviku a odpovídajících prostředků technické ochrany dostačuje malá zásahová jednotka, která reaguje na poplachový signál. V komplexu centralizované ochrany tak několik mužů střeží mnoho objektů mnohokrát účinněji, než by to dokázali jednotliví ochránci přímo v objektech. *„Prostředky technické ochrany jsou označovány jako elektrické zabezpečovací systémy.“* [5]

Technickou ochranu objektů můžeme pro začlenění do zabezpečovacího systému dělit do čtyř skupin:

- *„Prostorového zaměření,*
- *Způsobu předání poplachového signálu,*
- *Kategorie rizikovosti chráněného objektu,*
- *Stupně zabezpečení chráněného objektu.“* [5]

1.1.5 Bezpečnostní služba

Bezpečnostní službou se rozumí ochrana a ostraha osob a majetku, jakož i ochrana dalších práv a svobod prováděná jako podnikání, tak činnost obdobného charakteru prováděná pro vlastní potřebu ochrany a ostrahy osob a majetku v rámci vlastní organizace.

Soukromá bezpečnostní služba (dále jen SBS) je činnost agentury, založené a fungující na komerčním základě, která spočívá v projektování, organizování, řízení a kontrole, jakož i ve vlastním výkonu ochrany a ostrahy majetku a osob, strážní služby a ostatních specifických činností, které jsou SBS zajišťovány.

Pod pojmem SBS jsou zahrnuty tyto činnosti:

- Hlídací služby
- Detektivní služby
- Technické služby k ochraně majetku a osob
- Zajišťování vlastní ochrany

Za žádoucí stav je třeba považovat nedotknutelnost majetku, nedotknutelnost osob, nedotknutelnost práv a oprávněných zájmů občanů, firem, organizací, respektování zásad občanského soužití apod. Subjektem poskytování soukromých bezpečnostních služeb a realizátorem soukromé bezpečnostní činnosti je soukromá bezpečnostní agentura. [2]

Soukromé bezpečnostní služby plní úkoly při:

a) Ochraně majetku (objektů, věcí, zboží, atd.), a to jak vlastní SBS, tak obstaravatelsky ve prospěch právnických či fyzických osob, pro něž soukromá bezpečnostní služba vykonává činnost na smluvním základě
b) Ochraně života a zdraví, bezpečnosti osob, lidské důstojnosti
c) Zajišťování práv a oprávněných zájmů jak fyzických tak právnických osob
d) Zajištění bezpečné přepravy peněžních hotovostí, zboží
e) Zabezpečení veřejného pořádku a bezpečnosti v objektech nebo prostorách, jež jsou majetkem společnosti pro niž je služba poskytována na smluvním základě
f) Ochraně obchodních a jiných oprávněných zájmů firem a občanů, pro něž je soukromá bezpečnostní služba vykonává činnost hlídacích nebo detektivních služeb na smluvním základě (včetně ochrany před únikem obchodních a jiných důvěrných informací)
g) Realizaci technických, režimových nebo režimově technických opatření. [3]

Bezpečnostní pracovník

Bezpečnostní pracovník pátrá po příznacích požáru, vyhlašuje poplach při jeho zjištění, určuje příčinu požáru, rozhoduje o způsobu likvidace požáru. Udržuje přihlížející osoby nebo skupiny osob v bezpečné vzdálenosti rizikových míst, zaznamenává osobní data svědků a zjišťuje totožnost obětí mimořádné události. Zůstává v kontaktu se zadavatelem, informuje osoby a vedoucí pracovníky. *„Aktivuje a deaktivuje elektronický zabezpečovací systém dle předepsaného postupu. Kontroluje nouzové východy a udržuje únikové cesty průchodné, bez překážek.“* Také poskytuje první pomoc pracovníkům nebo návštěvám v chráněném objektu a zajišťuje přivolání pomoci. Kontroluje vydávání vstupních karet, zjišťuje chyby ve výdeji a vrácení klíčů, poznamenává a hlásí nepravidelnosti, které mohou ovlivňovat zvýšení bezpečnostního rizika. *„Udržuje v čistotě a pořádku služební místnost, podává svému nadřízenému návrhy na zlepšení vnitřních směrnic pro objekt, pracovních náplní jednotlivých funkcí, spolupracuje s firemními odborníky na zlepšení legislativy. Bezpečnostní pracovník dále odhaluje nebezpečí, které mohou ohrozit zaměstnance, nebezpečí pro zdraví a bezpečnost jejich práce.“* Nahlašuje pracovníky, kteří nedodržují pravidla bezpečnosti a zdraví při práci a hlásí objevená nebezpečí pro zdraví a bezpečnost práce. *„Je povinen ochraňovat důkazy, které se vztahují k důvodu nehody nebo úrazu.“* [4]

Stupeň zabezpečení objektu

V tabulce jsou popsány rizika, stupně zabezpečení a znalosti a vybaveni narušitelů. V Praktické části budu navrhovat nové zabezpečení a k nim přiřadím stupeň zabezpečení dle této tabulky.

Tabulka 1. Zobrazení stupňů zabezpečení objektu [8]

Riziko	**Znalosti a vybavení narušitelů**	**Stupeň zabezpečení**
nízké	Předpokládá se, že narušitelé mají malou znalost PZS a že mají k dispozici omezený sortiment snadno dostupných nástrojů.	1
nízké až střední	Předpokládá se, že narušitelé mají určité znalosti o PZS a že použijí základní sortiment nástrojů a přenosných přístrojů.	2
střední až vysoké	Předpokládá se, že narušitelé jsou obeznámeni s poplachovým zabezpečovacím systémem a mají úplný sortiment nástrojů a přenosných elektrických zařízení.	3
vysoké	Používá se tehdy, když zabezpečení má prioritu před všemi ostatními hledisky. Předpokládá se, že narušitelé mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení a nástrojů včetně prostředků pro náhradu rozhodujících prvků v PZS. Pokud je PZS rozdělen do jasně definovaných subsystémů, PZS může zahrnovat komponenty různých stupňů v každém subsystému. Stupeň subsystému je dán nejnižším stupněm vnitřního komponentu. Komponenty, které jsou společné pro více subsystémů, mají stupeň stejný jako subsystém s nejvyšším stupněm.	4

1.2 Legislativa

V podkapitole legislativa se seznámíme s normami a systémy, které souvisejí se zabezpečením tiskárny.

1.2.1 Poplachové systémy

Základní členění norem v oblasti poplachových systémů.

Normy

- ČSN EN 50 130 Poplachové systémy (všeobecné požadavky)
- ČSN EN 50 131 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy
- ČSN EN 50 132 Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích
- ČSN EN 50 133 Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích
- ČSN EN 50 134 Poplachové systémy – Systémy přivolání pomoci [24]

Další normy

ČSN EN 54 Elektrická požární signalizace

Poplachové systémy – Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací systémy slouží k signalizaci nebezpečí v chráněném prostoru a informují o nežádoucím vniknutí do chráněného objektu. Tyto systémy mohou být kombinovány i s indikací jiných nebezpečí, např. tísňové hlášení při přepadení objektu, požární nebezpečí, únik plynu atd.

Systémy PZS fungují většinou ve dvou režimech:

- **V nočním režimu**, kdy chrání zpravidla všemi detektory celý objekt,
- **v denním režimu**, kdy je budova v normálním provozu a hlídá se jen instalace systému a vybrané předměty předem určené (trezory, vystavované předměty, apod.). [7]

Poplachové zabezpečovací systémy dělíme na:

Poplachový zabezpečovací systém - PZS

Poplachový tísňový systém - PTS

PZTS zaznamenávají rozvoj z mnoha hledisek.

Rozdělujeme je na:

- *„PZTS komunikátory,*
- *PZTS ovládací periferie,*
- *PZTS a inteligentní elektroinstalace,*
- *PZTS aktivní Ochrana“*. [11]

PZTS komunikátory

„Kvalitní přenos informací z PZTS jsou nejdůležitější funkcí celého systému. Přenosová trasa od komunikátoru na straně PZTS až po komunikátor na straně DPPC (dohledové poplachové přijímací centrum) je zabezpečena poplachovým přenosovým systémem (PPS). V dnešní době se pro komunikaci PZTS s PPC používají tyto možnosti spojení:

a) PSTN - zprávy z chráněného objektu jsou přenášeny pevnou telefonní sítí
b) GSM/GPRS – přenos dat z objektu na PPC je proveden pomocí GSM sítě v hovorovém pásmu.
c) Rádiové spojení – rádiový přenos je nejrychlejším způsobem přenosu. Poplach z objektu je přenesen na PPC za cca 3 sec., přenos je zdarma.
d) TCP/IP – zprávy se z PZTS přenášejí prostřednictvím LAN modulu. Jde o moderní zařízení pro přenos dat z objektu na PPC v reálném čase přes internet.“ [11]

PZTS ovládací periferie

V dřívější době se využíval systém, který se nastavoval pomocí hexadecimální a binární soustavy. Dnes se tyto systémy nahrazují designovou klávesnicí s LCD displejem, který umožňuje uživateli přístup do systému včetně všech jeho funkcí. Aby se uživatelům ovládání ulehčilo, začínají se používat bezkontaktní karty, čipy, klíčenky apod. V současnosti je populární biometrická čtečka otisků prstů. Tyto čtečky jsou velmi efektivní, neboť identifikují uživatele podle otisku prstů nebo podle zadaného PIN kódu.

PZTS a inteligentní elektroinstalace

„Inteligentní elektroinstalace se dělí na funkci domovního spínače do dvou funkčních bloků, senzoru a aktoru.

Senzor – neliší se nijak od klasického spínače, stiskem tlačítka se rozsvítí nebo zhasne světlo. Při stisku vysílá zprávu, že se má zařízení zapnout nebo vypnout.

Aktor – je spínač, který přijímá zprávu od různých senzorů a při požadavku připojí spotřebič ke zdroji energie.Takto lze definovat, jakým vypínačem bude spotřebič ovládán.“ [11]

PZTS aktivní ochrana

Podmínkou kvalitního zabezpečení je chránit objekt od začátku pokusu o narušení až do příjezdu pomoci. Jedním ze systémů, který majetek ochrání a zároveň neohrožují lidský život a zdraví jsou zamlžovací systémy. Ty znemožní pachateli pohyb po objektu, neboť vytvoří neprůhlednou clonu. Ta dezorientuje narušitele a eliminuje škody, které by mohl způsobit.

Výhody zamlžovacích systému:

- Zamezení škod na majetku,
- Možné snížení nákladů na pojištění,
- Výhodná alternativa proti odcizení předmětů,
- Nenarušení obchodních aktivit apod. [11]

Hlavním cílem poplachových zabezpečovacích systémů je odhalit nežádoucí pohyb v hlídaném prostoru, detekovat otevření dveří, rozbití oken, požár apod.
Koncová zařízení umožňují rozpoznat narušení střeženého objektu, například akustická siréna, optická signalizace. „*Pro dálkový přenos signalizace na pult centralizované ochrany je potřeba radiových modemů nebo telefonních komunikátorů.“* [7]
Zvláštním druhem systému PZS je zařízení pro střežení obvodu rozsáhlých areálů tzv. perimetrická ochrana. Tato ochrana umožňuje zachytit případného narušitele ještě před vniknutím do střeženého objektu a dává bezpečnostním složkám více času pro zásah. „*Analogickým elektronickým zabezpečením je tzv. elektronická požární signalizace (EPS), ta plní funkci ochrany objektu před přírodními živly (požáry, krupobití). Instalace*

elektronické zabezpečovací signalizace se považuje za důvěrnou informaci firmy, kde je tato signalizace instalována.“ [7]

Poplachové zabezpečovací systémy se člení na:

- *„Detektor,*
- *ústředna,*
- *přenosové prostředky,*
- *signalizační zařízení,*
- *doplňková zařízení.“* [5]

Detektor

Je zařízení okamžitě reagující na fyzikální změny, které souvisejí s narušením střeženého objektu či prostoru nebo na nežádoucí manipulaci se střeženým předmětem. *„Při indikování stavu narušení reaguje čidlo vysláním poplachového signálu nebo zprávy.“* [5]

Ústředna

„Přijímá a zpracovává informace z čidel podle stanoveného programu a požadovaným způsobem je realizuje. Dále umožňuje ovládání a indikaci zabezpečovacího systému, zajišťuje jeho napájení a inicializaci následného přenosu informací.“ [5]

Přenosové prostředky

Zajišťují přenos výstupních informací z ústředny do místa signalizace, případně pokynů opačným směrem.

Signalizační zařízení

Zajišťují převedení informací na vhodný signál (poplach nebo výstrahu).

Doplňková zařízení
usnadňují řízení systému nebo umožňují realizovat některé speciální funkce.

Výhodou poplachového zabezpečovacího systému je, že chráněné prostory nemusí být fyzicky střeženy, systém poskytuje ochranu před násilným otevřením dveří nebo oken, poskytuje ochranu před užitím interních a externích detekčních zařízení, aj. [5]

Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích

CCTV jsou přenosy realizované pomocí analogových nebo IP kamerových systémů. Součástmi systému CCTV jsou kamera, přenos videa do dohledového centra, dohledové centrum pro zobrazení situace, záznam. Užití kamer, videí a monitorů slouží ke sledování chráněného objektu. Výhodou může být podpora bezpečnostního personálu, který může sledovat oblast, jako je např. několikapatrová administrativní budova nebo omezený počet pracovníků, dále může být užívaná jako samostatné a nezávislé pozorovací médium tam, kde jsou kamery umístěny v oblastech zvýšeného rizika, např. vstupní místa. Systémy CCTV jsou zařízení se stálými náklady, aktivita v pokrytém místě může být poznamenávána pro budoucí vyhodnocení nebo pro kontrolu strážných. [12]

Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích

Pohybem osob, vozidel, případně dalších nositelů ID karet chápeme vstupy a vjezdy do chráněného objektu a výstupy z nich, průchody dveřmi, turnikety nebo závorami.

Systém kontroly vstupu je určený pro kontrolu, řízení a zpracování pohybů a přístupů osob, vozidel nebo výrobků, uskutečněných pomocí identifikačních karet s využitím podpůrného hardwaru (zejména různých typů snímačů) a souboru programových modulů na příslušných počítačích.

Tento systém umožňuje omezit vstup do určitých prostor jen v určitou dobu nebo určité skupině osob s vlastní identifikační kartou nebo znalostí vstupního kódu.

Základní funkční vlastnosti systému ACCESS:

- *„Zavedení pojmu snímač (kontrolované místo vstupu) a zóna (množina snímačů definující vstupy do určité oblasti)*
- *definování práv jednotlivých ID karet pro vstup do zóny*
- *kontrola násobných vstupů (tzv. antipassback) – časový (určitou dobu se nesmí opakovat pokus o průchod) nebo globální antipassback (kdy doba není definována)*
- *zpřístupnění aktuálních stavů systému (kde se která identifikační karta nachází, stav zařízení, signalizace alarmových stavů) pomocí monitorovacích úloh*
- *činnost sledování překročení doby nezbytné k zavření dveří, kontrola otevření dveří jiným způsobem než identifikační kartou*

- *definice různých úrovní alarmových stavů systému*
- *vzdálená správa snímačů*
- *zavedení definice typů karet (skupiny osob) a k nim odpovídající*
- *jednoduché přiřazování přístupových práv, možnost definovat šablony přístupových práv*
- *ovládání bezpečnostních ústředen PZS snímači identifikačních karet*
- *vyhodnocení dat ze systémů EPS.“* [17]

Povolený pohyb osob se děje definováním přístupových oprávnění jednotlivých osob, které se vždy skládá z:

- Určitého snímače nebo množiny snímačů,
- definované doby průchodu (časové zóny),
- volitelné speciální chování karty podle jejího typu. [17]

Poplachové systémy – Systémy přivolání pomoci

Tísňový prostředek je prvek tísňové ochrany, který slouží k ochraně osob a majetku v případě jejich přímého ohrožení. Hlavním účelem tísňového prostředku je včasné podání informace, hlavním cílem je zamezení vzniku nestandardní situace, eliminace hrozeb a rizik s nimi spojených. Účelem je dosáhnout přerušení průběhu nestandardních procesů a snížení rozsahu následků přepadení, nehod aj. Poplachový tísňový systém (dále jen PTS) slouží především k ochraně života a zdraví osob.Tyto prostředky se využívají u poplachového tísňového systému. Systému umožňující uživateli možnost vyvolání úmyslného poplachového stavu do míst, odkud je možné poskytnout pomoc. Vyvolat poplach lze manuálním aktem, zprostředkovaně definovaným způsobem, nebo automaticky. V minulosti se používaly u nekomerčních objektů, mimo soukromou sféru, časem se rozšířil i pro komerční oblast, k soukromým osobám.

Na trhu se nabízí několik druhů tísňových prostředků, které se liší účelem svého použití. Můžeme je rozdělit na veřejné, speciální a osobní.

Veřejné tísňové hlásiče

Jejich hlavním účelem je vyvolání tísňového hlášení veřejností nebo pracovníkem v daném chráněném objektu. Jsou umístěny na veřejně přístupných místech, tak, aby kdokoli, kdo se ocitne v nebezpečí, mohl rychle přivolat pomoc.

Speciální tísňové hlásiče

Jsou určené k nepozorovanému vyvolání tísňového hlášení v případě přímého ohrožení. Bývají umístěny skrytě. Nejčastěji se instalují v chráněných objektech, jako například v bankách, obchodních centrech apod.

Osobní tísňové hlásiče

Příslušná osoba je nosí u sebe k použití v případě tísně, pracují bezdrátově. Jsou napájeny z baterie nebo akumulátoru. Mohou být určeny pro osoby pracující na odlehlých pracovištích, kde dochází např. k napadení osob nebo vloupání se do objektu. Bývají ve tvaru hodinek, přívěšků, náramků atd. [13]

Elektrická požární signalizace (EPS)

EPS je komplexní soubor technických zařízení, sloužících pro včasnou detekci požáru, lokalizaci jeho vzniku a následného předání poplachové informace k zajištění hasičského zásahu. Systém EPS tak účinně zabraňuje nejen vzniku rozsáhlých materiálových ztrát, ale i možným ztrátám na lidských životech.

Elektrická požární signalizace informuje o vzniku požáru akustickou a optickou signalizací přímo v daném objektu, popřípadě pomocí dálkového přenosu na pult centrální ochrany (PCO), který je u hasičského záchranného sboru (HZS).

Dalšími možnými výstupy technologie EPS mohou být např. automatická aktivace hasících systémů, ovládání a kontrola východů a dveří, evakuační rozhlas, aj. [13]

Systémy EPS jsou obsluhovány klávesnicí nebo přímo z počítače přes běžné komunikační rozhraní. Informace o poplachu je obdobně jako u poplachového zabezpečovacího systému možno předat na hasičský záchranný sbor, na telefon nebo na tablo obsluhy. Současně lze využít optické nebo zvukové signalizace. Součástí obslužných software obvykle bývají grafická zobrazení střeženého objektu se zákresem jednotlivých hlásičů. Při vyhlášení alarmu se obsluha lehce orientuje, ve které části objektu hrozí nebezpečí požáru a může včas provést varování a další nezbytná opatření. Nedílnou součástí stavební projektové dokumentace objektů zpravidla bývají i projekty EPS. Povinné jsou v budovách, kde se předpokládá větší koncentrace osob. Projekt EPS je nutno nechat schválit reviznímu technikovi hasičského záchranného sboru příslušného obvodu. Instalované systémy

podléhají ze zákona každoroční revizi. Funkční a zrevidovaný systém EPS je další podmínkou pojišťovacích společností pro pojištění daného objektu.

Rozdělení EPS

Adresovatelné systémy

Tento systém dokáže na jedné průběžné smyčce ovládat stovky koncových zařízení s konkrétními adresami. Přitom lze jednotlivé skupiny hlásičů nebo jednotlivé hlásiče samostatně ovládat, nastavovat práh jejich citlivosti a v případě potřeby je vypínat nebo zapínat.

Bezdrátové systémy

Jejich využití je zejména v aplikacích, kde není možné z jakéhokoli důvodu instalovat kabely, případně existuje požadavek na snadnou přenositelnost systému. Vzhledem k tomu, že u těchto systémů odpadá nutnost náročného budování kabelových tras a rozvodů, vyniká instalace svojí rychlostí.

Nejčastěji používané požární hlásiče

- Požární hlásiče kouře reagující na kouř vznikajícího požáru,
- Požární hlásiče tepla reagující na zvýšení teploty nad prahovou hodnotu,
- Tlačítka sloužící k manuálnímu nahlášení požáru,
- Lineární hlásiče reagující na přerušení infračerveného paprsku kouřem,
- Plamenné hlásiče reagující na charakteristiku plamene,
- Hlásiče do prostředí s nebezpečím výbuchu.[18]

1.2.2 Nepoplachové systémy

Mezi nepoplachové systémy patří např. mechanické zábranné systémy, bezpečnostní folie atd.

Mechanické zábranné systémy

Mechanické zábranné prostředky jsou určené k ochraně proti násilnému vniknutí neoprávněných osob. Jejich úkolem je narušitele při jejich překonávání co nejvíce zdržet. Všechny mechanické systémy jsou nakonec překonatelné. Doba překonání závisí na kvalitě a umístění. Vliv na překonání mechanických zábranných systému má i znalost

konstrukce ze strany pachatele nebo druh použitých nástrojů při překonávání. Můžeme sem zařadit například bezpečnostní dveře, mříže, ploty atd. [11]

Rozdělení technických ochran MZS

Mechanické zábranné systémy tvoří páteř technického zabezpečení objektu.

Dělit je lze do čtyř skupin:

Obvodová ochrana

Ochrana tykající se prostředků, které zajišťují bezpečnost vyhrazenému prostoru kolem chráněného objektu. Obvodem objektu rozumíme katastrální hranice vymezené např. přírodními bariérami (keřové porosty, vodní toky aj.), nebo umělými bariérami (ploty).

Plášťová ochrana

Jedná se o zabezpečení vstupu všech otvorů do objektu, např. dveří, oken, tím případnému pachateli zabraňuje narušení.

Předmětová ochrana

Slouží k zabezpečení místa, kam se ukládají peníze, cennosti, utajované skutečnosti před odcizením nebo neoprávněnou manipulací.

Speciální ochrana

Chemická ochrana předmětů, cenin apod.

Prostředky individuální ochrany

Těmito prostředky se rozumí nepřenosové i přenosové technické předměty, už zmíněné v předchozích oblastech. [14]

Bezpečnostní folie

Bezpečnostní fólie můžeme instalovat tam, kde potřebujeme chránit skleněné plochy oken či dveří před vloupáním do objektu. Bezpečnostní fólie na sklo se využívá k zabezpečení oken. Zároveň, bezpečnostní a ochranné folie, ochraňují neoprávněné osoby před zraněním rozbitým sklem. Ochranné fólie jsou nejjednodušším způsobem zajištění skel před vysypáním a poraněním osob. Hlavní užití najdou například u průchozích dveří a skleněných ploch na schodištích. Snižují riziko vykradení, slouží i proti slunečnímu záření, zabraňuje vandalismu, zabraňuje průniku cizích osob, prostupu cizích předmětů aj. [19]

2 KONTROLNÍ SYSTÉM

Kontrola vstupu je nejdůležitější hledisko bezpečnosti. Poplachové systémy vyžadují formu identifikace, jako je karta nebo číslo ověřené čtecím zařízením, ještě před povolením vstupu do chráněného objektu.

- *„Vstupní karta, tím se rozumí různé druhy magnetických a čipových karet, spony, přívěsky a jiné identifikátory,*
- *čtečka na terminál je zařízení na načítání karet, klávesnice, kódovaný zámek,*
- *prvek činící rozhodnutí je procesor, počítač nebo jednotka kontroly dveří,*
- *výstupy, tzn. napájecí zdroj pro zámek, signál pro poplachový systém, signál pro kamery, bariery a jiná zařízení.“* [4]

Po mechanické stránce je požadován elektricky ovládací zámek a automatický zavírač dveří. Pokud je použita vstupní karta u vstupu, tak předem naprogramovaný prvek rozhoduje, zda bude nebo nebude dovolen vstup. Pokud bude přístup povolený, tak je signál po otevření zámku vysílán přes výstup a událost je zaznamenána pro budoucí kontrolu. Výhodou je, že systémy kontroly vstupu mohou být napojeny na elektronické zámky dveří a mohou odepřít vstup neoprávněným osobám, mohou zaznamenat všechny podrobnosti o tom, kdo oprávněně vstoupil, i všechny, kteří vstoupili do chráněného objektu nebo jej opustili, systémy mohou být napojeny na poplachový systém, který spustí poplach v případě neoprávněného vstupu, vstup může být omezen na určité oblasti podle předem určených časových rozvrhů, vstupní místa mohou být monitorována z centrálního místa místo fyzického sledování pracovníkem u brány. [4]

2.1 Rozdělení identifikačním prvků

- Magnetické identifikační karty
- Optické identifikační karty s čárovým kódem
- Indukční identifikační karty
- Čipové identifikační prvky

Magnetické identifikační karty

„Magnetická identifikační karta je identifikační prvek ve formě plastové destičky, která má velikost předepsanou danou mezinárodní normou, na které je nanesen proužek

magnetického nosiče.“ Informace se zapisují pomocí nahrávací hlavy na magnetický proužek, který obsahuje všechny údaje včetně oprávnění, kam a kdy může zaměstnanec nebo případně návštěva vstupovat. *„Z hlediska ochrany objektu je funkce registrace pracovní doby a tím eventuálně výpočtu mzdy. Ke čtení dochází protažením karty štěrbinou, ve které je čtecí hlava. Zápis informace na magnetický proužek má různé kódování, dle použitého systému. Bezpečnost není velká, neboť lze bez problémů magnetickou kartu přečíst a vyrobit duplikát.“* [6]

Optické identifikační karty s čárovým kódem

„Čárový kód je řada vertikálních čar různé tloušťky s mezerami.“ Když se identifikační kartou s čárovým kódem přejede nad snímacím zařízením, je vysílán IR paprsek černými pruhy absorbován, zatímco od světlých mezer se odrazí. Fotosenzor snímače přijímá odražené světlo a převádí je na elektrický signál. Skener vytváří slabý signál pro mezery a silnější signál pro pruhy. *„Čárový kód obsahuje start znak, zadanou informaci, kontrolní součet s stop znak. Řazení čar a ploch musí mít logický řád*.“ Tento symbol čárového kódu graficky vyjadřuje číslo prvku, který identifikuje oprávněnou osobu. Musí být udělaný tak, aby byl schopen přečtení, dekódování a následného zpracování výpočetní technikou. Čárové kódy jsou buď nekryté nebo tzv. maskované čárové kódy, kde je identifikační karta s čárovým kódem buď zapouzdřená v PVC fólii s ochranou maskovací vrstvou, nebo je na čárovém kódu nanesen maskovací lak, který je propustný jen pro infračervené světlo speciálních snímačů, a proto není možné vyrobit kopii prostým okopírováním. „*U tohoto typu karet je možnost čtení kódu i bezkontaktními snímači na vzdálenost několika desítek centimetrů při použití speciálních zařízení.“* [6]

Indukční identifikační karty

„Pracují na principu elektromagnetické indukce. V nosiči je zakódována informace. Dostane-li se identifikační prvek de elektromagnetického pole snímače, dochází ke změně homogenity pole přesně stanoveným způsobem. Tato změna je snímačem vyhodnocena a převedena do datové podoby k dalšímu zpracování.“ [6]

Tyto karty vynikají zvýšenou mechanickou pevností a odolností proti opotřebení, stabilitou záznamu a ztíženou kopírovatelností. Jsou určeny především pro průmyslové použití.

Čipové identifikační prvky

Čipové identifikační prvky mají záznam informace v paměťovém čipu, který bývá zalisován do karty, štítku, přívěšku nebo speciálního kovového pouzdra. Při kontaktu nebo přiblížení identifikačního prvku se snímačem dochází k přečtení, popřípadě i k zápisu informace a následuje její další zpracování. Čipové karty postupně nahrazují karty magnetické a dostávají se tak téměř do všech oblastí našeho života. *„Tyto moderní prvky se vyznačují vysokou odolností a spolehlivostí. V dnešní době představují jeden ze základních pilířů komplexních elektrických vstupních systémů.“* Jednodušší provedení čipových prvků lze pouze číst a jejich obsah je stanoven výrobcem, dokonalejší typy dovolují zápis a tím pádem i modifikaci a transport dat. Čipové identifikační prvky lze dále dělit na dotykové a bezdotykové. [6]

2.2 Kontrola přístupových bodů

Přístupovým bodem myslíme uspořádání všech prvků, které umožňují kontrolovaný přístup do prostoru nebo k informacím v přístupově daném místě. Přístupový bod je tvořen z:

- Místa přístupu – zařízení, které může být ovládáno k poskytnutí přístupu, brány turnikety, dveře apod.,
- Rozhraní místa přístupu – zařízení, které ovládá otevření a zabezpečení místa přístupu,

  - řídící jednotka - obsahuje řídící logiku, vstupy/výstupy, potřebné k ovládání APAS, zabezpečuje převod dat z identifikačního zařízení, komunikaci apod.,

    - Snímače místa přístupu – čtečka, biometrie, klávesnice,
    - APAS – ovládací prvky a senzory přístupového místa,

  - vstupní prvky – spínače, magnetické kontakty, optické závory,

  - výstupní prvky – zámek, motor turniketu, otvírač apod.

  Struktura celého přístupového systému se skládá z :

    - Jednoho nebo více přístupových bodů,
    - Hlavní řídící jednotky,
    - Napájení,
    - Komunikační sítě,
    - Řídícího a obslužného pracoviště. [11]

3 DETEKTORY KOVŮ

Jedná se o velmi účinné, univerzální technické prostředky bezpečnostních prohlídek. Jsou rozšířenou skupinou bezpečnostních prohlídek.V dnešní době se tyto detektory vyrábí z pevných a tuhých materiálů na bázi karbonových vláken, polymerů, na bázi křemíku se univerzálnost detektorů kovů snižuje. Detektory kovů mají mezi bezpečnostními prostředky své nenahraditelné místo.

Dělení detektorů

Detektory můžeme rozdělit podle způsobu konstrukce, podle technického vývoje a podle způsobu použití.

Podle způsobu konstrukce se detektory kovů dělí na:

- Ruční detektory kovů,
- Průchozí detektory kovů (detekční rámy).

Podle technického vývoje se rozdělují na:

- I. generaci (systémy s útlumem cívky rezonantního obvodu),
- II. generaci (frekvenční systémy),
- III. generaci (pulsně-indukční systémy).

Podle způsobu použití k bezpečnostní prohlídce na:

- Ruční detektory kovů pro prohlídku osob (detekce zbraní, výbušnin),
- Rámové detektory kovů pro prohlídku osob (detekce zbraní, výbušnin),
- Detektory kovů v obuvi (detekce zbraní, výbušnin),
- Stolní detektory kovů pro kontrolu došlých zásilek (detekce nástražných výbušných systémů).

Dále dělíme detektory podle zaměření na rámové detektory kovů a ruční detektory kovů.

3.1 Detekční rámy

Rámové detektory kovů obecně slouží k vyhledávání střelných zbraní, výbušnin u osob, které vstupují do chráněného objektu. Detekční rámy můžou sloužit také pro vyhledávání kovových předmětů v tom případě, kdy osoba opouští chráněný objekt a chceme si prověřit, zda kovové součásti nevynáší z objektu. Předností těchto detektorů je zejména to, že velikost signálu závisí pouze na tvaru, velikosti, poloze a vlastnostech tělesa, nikoli jako

u ručního detektoru kovů na momentální vzdálenosti cívky od tělesa. To umožňuje efektivní využívání nastavení minimální úrovně signálu pro vyhlášení zvukového a světelného alarmu. Signál od drobných kovových součástek oděvu spolu se signály lidského těla nevytváří falešné poplachy. Avšak komplikací detekce je vlastní tělo, které působí jako velký objem slané vody a tím zkresluje signál od hledaného kovu. Dále se stává, že cívky detektorů přijímají i nežádoucí signály z okolí. Jedná se například o motory, televize, světelné zdroje aj. Tyto nežádoucí pohyby jiných předmětů blízko detekčního rámu mohou být přístroji identifikovány a často i eliminovány. Nicméně v oblasti pracoviště by tyto rušivé zdroje měly být odstraněny, jinak nelze dosáhnout detekční přesnosti. Nejznámějším využitím průchozích detektorů kovů je detekce zbraní. Citlivost přístroje se nastaví tak, aby reagoval i na ty nejmenší typy zbraní, které chceme přes rámový detektor kontrolovat. Nastavení velké citlivosti není problém, ale detektor může ztratit na efektivnosti a může spustit falešný poplach. To se týká například kovových součástek oděvů prohlížených osob s kovovými předměty v kapsách.

3.2 Ruční detektory kovů

Ruční detektory kovů se používají pro bezpečnostní prohlídku k vyhledávání kovových zbraní. Síla vyhledávacích signálů je omezena velikostí detektoru a kapacitou zdroje elektrické energie v podobě akumulátoru. Ruční detektor funguje na stejné bázi jako rámový detektor. Kontrola osob se musí provádět v těsné blízkosti nad povrchem těla, intenzita budoucího pole je omezena. Týká se to osob, které používají kardiostimulátor. Elektromagnetické pole by ho mohlo poškodit, což by mělo pro tuto osobu vážné následky. Nedostatkem, který ruční detektor představuje, je jeho malá snímací plocha. Aby byla provedena dostatečně velká bezpečnostní kontrola, je nutné provádět detekci tak, aby bylo snímáno místo vedle místa, což je v konečném výsledku velmi namáhavé a zdlouhavé. Ruční detektory jsou doplňkovým předmětem rámových detektorů. Souhra a propojenost mezi rámovým detektorem a ručním detektorem kovu zvyšuje efektivnost bezpečnostní kontroly a zkracuje délku trvání prohlídky. [20]

II. PRAKTICKÁ ČÁST

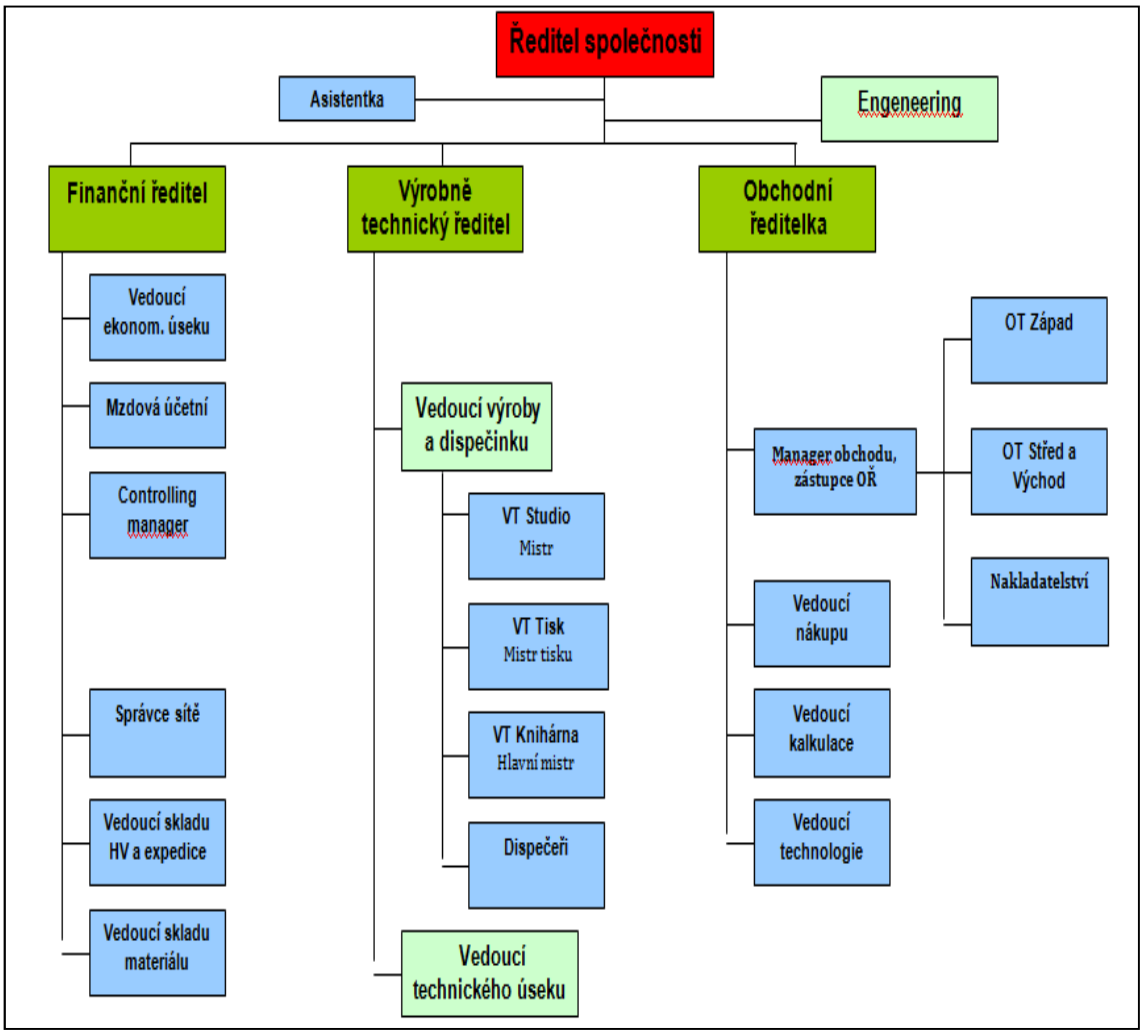
4 VÝROBNÍ ORGANIZACE - TISKÁRNA

Podnik patří mezi významné evropské ofsetové tiskárny. Zkušený tým odborníků na grafiku, tisk a knihařské zpracování se průběhu celého výrobního procesu se podílí na prvotřídní kvalitě nabízených služeb i vytištěné produkce. Řemeslo a zkušenosti zaměstnanců i nové technologie jsou základem každodenní práce. Kontrola kvality probíhá v průběhu celého výrobního procesu, což představuje příjem a kontrolu dat, tisk, knihařské zpracování, dokončovací práce, balení a expedice. Plní i nestandardní polygrafické požadavky.

4.1 Základní parametry organizace

Na výrobě zakázek se podílí až 250 zaměstnanců, ročně je zde vytisknuto více než 20 000 000 publikací. 60% produkce směřuje do zahraničí. Výrobní organizace využívá 1280 m^2 výrobní plochy. Podnik pracuje nepřetržitě 7 dní v týdnu, 24 hodin denně. Je partnerem nejvýznamnějšího českého knižního veletrhu Svět knihy. Každoročně se účastní významných akcí a veletrhů, jako např. Frankfurter Buchemesse, Lepziger Buchmesse. Vlastní certifikáty o kvalitě řízení i ochraně životního prostředí. Výrobní organizace dodržuje systém environmentálního managementu zavedený podle normy ISO 14001:2004, dále dodržuje platnou legislativu České republiky a Evropské unie v oblasti ochrany životního prostředí. Vstupní materiály jsou používaná na všech úrovních výroby, splňují evropské normy o nezávadnosti. Vše, co je vytisknuto je vyráběno s certifikátem FSC® nebo PEFC. Tiskárna důsledně třídí odpady a předává je oprávněným firmám k ekologickému zpracování, dbá na snižování emisí. [21]

4.2 Organizační struktura podniku



Obrázek 1. Schéma organizační struktury

Vlastníci organizace vlastní celou společnost. Řídící management se stará o chod podniku. Ředitel společnosti řídí celou společnost. Asistentka ředitele vede sekretariát společnosti a je k dispozici jednotlivým ředitelům. Engeneering má na starosti řízení výrobních procesů a standardů. Finanční ředitel je zodpovědný za veškeré finanční záležitosti. Vedoucí ekonomického úseku dbá na správné zařazení účetních položek. Mzdová účetní má na starosti evidenci zaměstnanců a jejich mzdy. Controling manager a správce sítě je jedna osoba, která vyhodnocuje informace z informačního systému a řeší nákup SW a HW. Vedoucí skladu hotových výrobků a expedice zajišťuje uskladnění hotových výrobků a jejich následnou expedici. Vedoucí skladu materiálu zajišťuje uskladnění materiálu pro

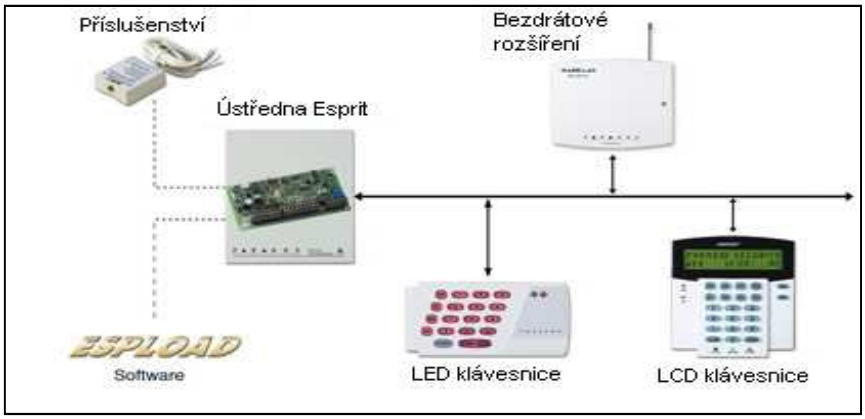
výrobu a jeho výdej na jednotlivé zakázky. Výrobně technický ředitel je zodpovědný za optimální výrobní proces a řídí vedoucího výroby a dispečinku a mistry výroby. Vedoucí technického úseku má na starosti technické vybavení, stroje a zařízení, jejich následnou údržbu a bezpečnost práce. Obchodní ředitel je zodpovědný za zajištění zakázek pro výrobu tak, aby byly stroje maximálně využity a řídí obchodní týmy a nakladatelství. Vedoucí nákupu zajišťuje veškerý nákup materiálu potřebný pro výrobu a chod společnosti. Vedoucí kalkulace zodpovídá za správné nastavení kalkulačních vzorců pro jednotlivé zakázky. Vedoucí technologie má na starosti optimalizaci výrobního procesu jednotlivých zakázek. Pro další potřeby budu používat výraz zaměstnavatelé, kteří přijímají pracovníky a starají se o celou organizaci.

4.3 Současný stav zabezpečení organizace

V současné době je podnik zabezpečen poplachovým zabezpečovacím systémem značky Paradox. Tento systém je ovládán číselným kódem s napojením na pult centrální ochrany. Systém je v tiskárně umístěn na třech místech. Majitelé mají zájem o inovování tohoto systému s umístěním na více místech. Dále je v organizaci systém CCTV, který funguje a netřeba ho měnit. Kamery jsou umístěny jak uvnitř tiskárny, většinou ve výrobě, na skladech, tak i venku před vchodem do budovy a v zadní části budovy, kde je vjezd k rampě do skladu tiskárny. U vstupu na vrátnici sedí bezpečnostní pracovník, který sleduje veškerý pohyb v objektu. Požární zabezpečovací systém má organizace instalovaný má a hlásiče jsou umístěny v prvním i ve druhém podlaží - ve výrobě, ve skladech, u vstupu do budovy, v kancelářích. Objekt spadá do režimu fyzické ostrahy budovy a okolí. Je nepřetržitě střežen strážní službou u vstupu do tiskárny i zezadu podniku, ka, vstupují zaměstnanci a kudy vozidla vjíždí přes vrátnici do chráněného objektu. Co se týká mechanických zabraných systémů ke kontrole vozidel, společnost má k dispozici jen vrátnici bez závory. V další kapitole o závorách, oplocení a jiných mechanických zábranných systémech budu pojednávat a navrhuji řešení na základě události vzniklých situací v minulosti.

Současný poplachový zabezpečovací systém (PZS)

Jak už jsem zmínila výše, organizace využívá PZS, který by chtěla inovovat. Zde popisuji o jaký současný systém se jedná.



Obrázek 2. Schéma zabezpečovacího systému Esprit [25]

Tento systém firma pořizovala na základě zkušeností jiné společnosti. Výhodou systému je tedy zkušenost s dlouhodobým provozem a jeho nízká cena. Za přednost považuji programování a základní vlastnosti, které jsou společné i pro jinou řadu ústředen. Systém využívá technologii Zdvojených zón ATZ. Díky této technologii umožňuje zapojit dva detektory včetně ochranných kontaktů na jeden kabelový pár. K ústředně lze doplnit další moduly, různé typy klávesnic, moduly výstupů rozšiřujícími komunikátory aj. [25]

Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích

Tiskárna je zabezpečena kamerovým systémem vnitřním i venkovním. Pohyb po budově i v okolí chráněného objektu je monitorován a ukládán po dobu jednoho měsíce. Pracovník ostrahy, sleduje pohyb a v případě potíží, se přepojuje na pult centralizované ochrany (PCO). Podnik nemá v úmyslu kamerový systém měnit, se stávajícím je spokojena.

Obrázek 3. Vnitřní kamera organizace [26]

Obrázek 4. Venkovní kamera organizace [27]

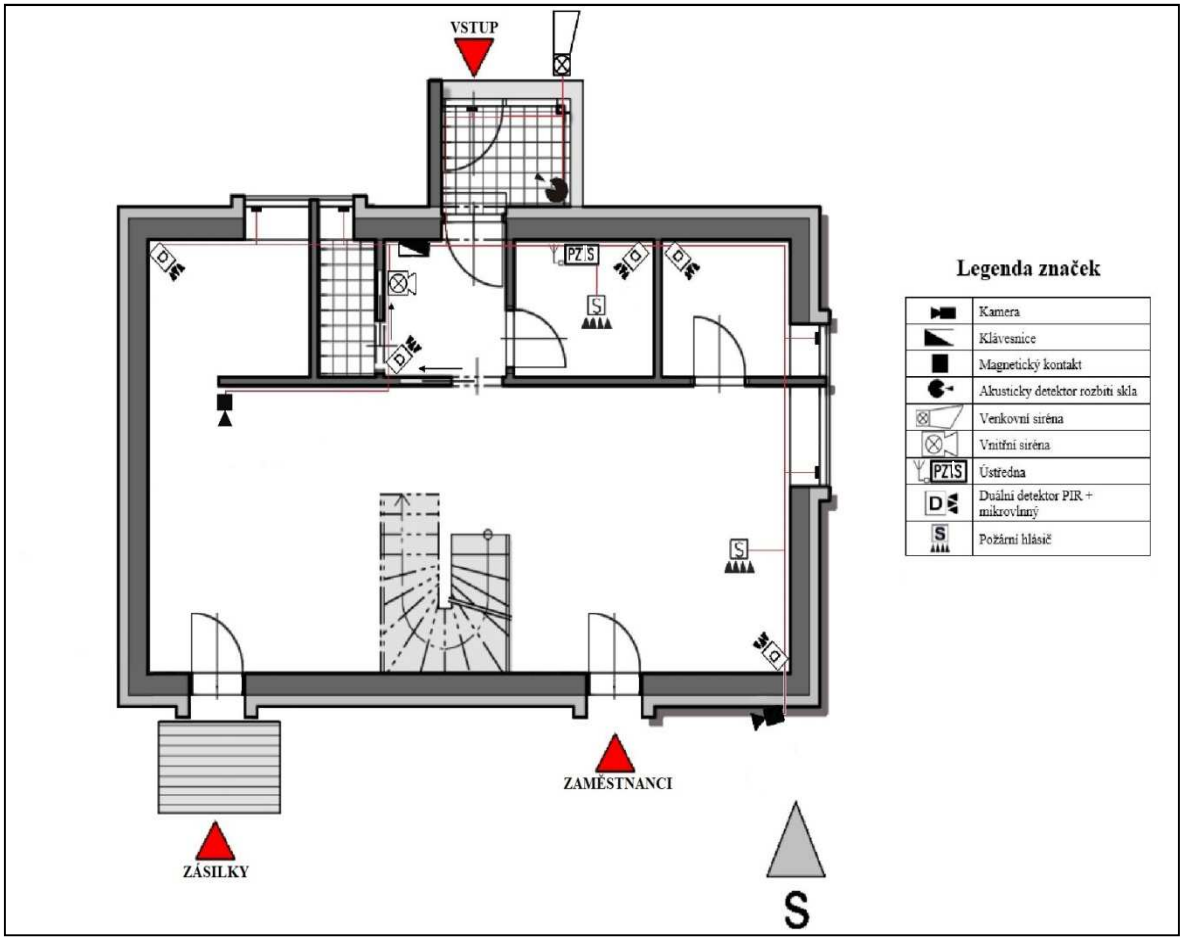
Obrázek 5. Dohledové stanoviště organizace [27]

Elektrická požární signalizace (EPS)

Jelikož PZS tvoří velmi důležitou a nezbytnou součást protipožární ochrany, podnik od svého počátku má tento systém nainstalován. Hlásič je umístěn po celém objektu, v každé místnosti. Níže na obrázku specifikuji, kde přesně se hlásiče požáru nachází. Systém je propojen s poplachovým zabezpečovacím systém a se systémem uzavřeného televizního okruhu.

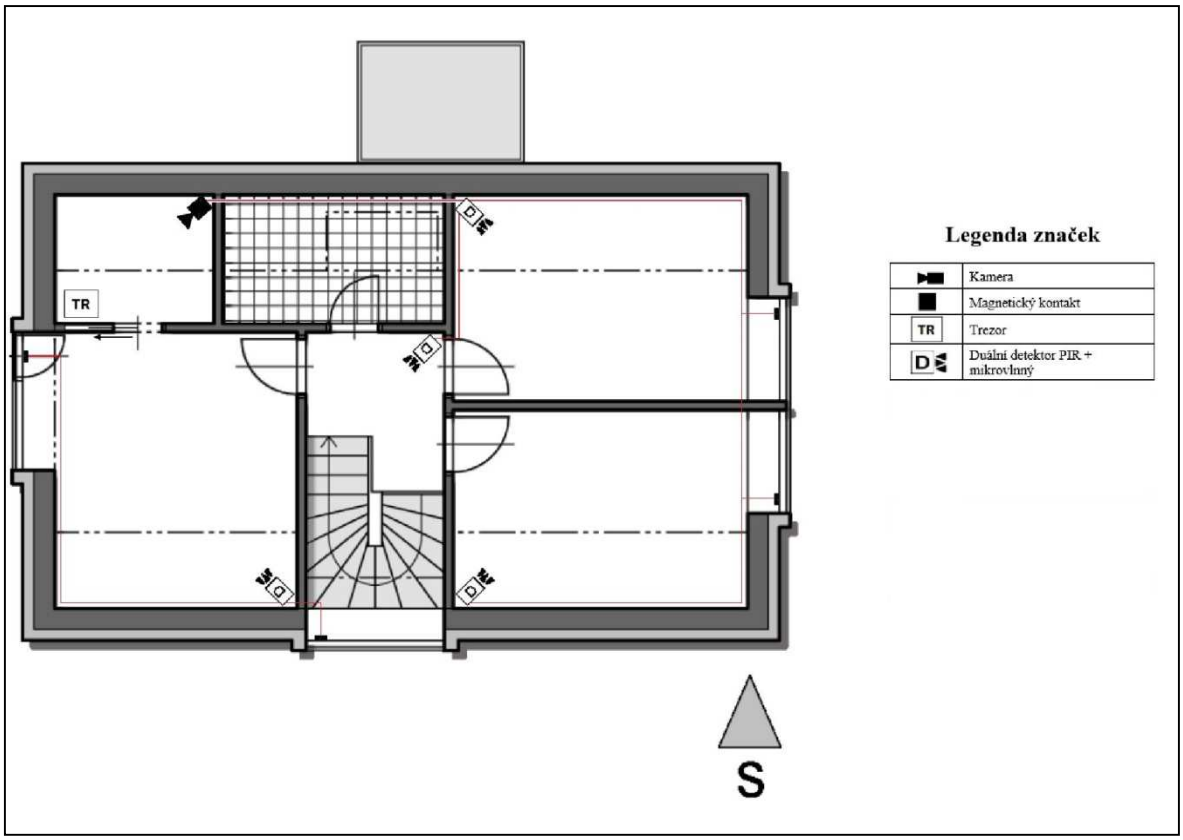
4.4 Současné zobrazení stavu bezpečnostních systémů

I.NP – Zde je vyznačen současný stav systémů, které má podnik k dispozici. Hlavní vstup do budovy je nahoře a tímto vstupem vstupují pouze majitelé, zaměstnavatelé a návštěvy firmy. Vstup je opatřen vrátnicí ve které je ostraha objektu a poplachovým a tísňovým zabezpečovacím systémem (PZTS), kdy tísňový systém podnik doposud nevyužívá a nemá instalován. Jsou zde vyznačeny detektory, kamery, požární hlásiče, (více legenda značek).



Obrázek 6. Současné zabezpečení organizace (I.NP)

II.NP – V tomto patře se nachází kanceláře vedení podniku. Na obrázku 7 jsou vyznačeny detektory pohybu, nachází se tady trezor a ten je opatřen kamerovým systémem. Vše je sledováno v ostrahou objektu, která se nachází na vrátnici u hlavního vchodu pro zaměstnavatele v přízemním podlaží.



Obrázek 7. Současné zabezpečení organizace (II.NP)

5 RIZIKOVÉ FAKTORY PODNIKU S OHLEDEM NA MINULÉ UDÁLOSTI

Na základě události v minulých letech, kdy došlo k vážnému postřelení dvou zaměstnavatelů a ke smrti bývalého zaměstnance, jsou následující podkapitoly zaměřeny na rizikové faktory, kde popisuji například vztahy mezi vlastníky, vztahy mezi zaměstnanci, pokus o vykradení firmy, průnik cizích osob a vandalismus.

Níže bych navrhovala kontrolní přístupový systém, aby nedošlo k průniku osoby, které není povolen přístup do podniku, s čímž také souvisí použití tísňového tlačítka.

5.1 Vztah majitel x řídící management

Situace mezi vlastníky a řídícím managementem ve firmě je na dobré úrovni. Obvykle se zde objevují jen slovní potyčky, které neústí ve vážnější konflikty. Vztahy mezi zaměstnavateli se tedy zatím řešit nemusí. Ve druhém podlaží, ve kterém jsou kanceláře, jsou nainstalovány kamery a v každé místnosti jsou také detektory pohybu. Nejsou zde zatím nutná žádná důkladnější bezpečnostní opatření.

5.2 Vztah zaměstnanec x zaměstnanec

Pravomoci zaměstnance vychází ze schopnosti pracovat a možnostech tuto práci v podniku odmítnout. Tito lidé, se také podílejí na fungování podniku a poskytují tudíž informace, které jsou důležité pro řízení podniku. Spokojený zaměstnanec zůstává v podniku a posiluje se jeho loajalita, kdežto nespokojený zaměstnanec má tendenci z podniku odejít.

Vztahy mezi zaměstnanci ve firmě mohou být na různé úrovni. V některých by mohlo docházet k šikaně slabšího člověka, který je spíše uzavřený a moc se ve společnosti vůči ostatním zaměstnancům neprojevuje. Další obětí může být nově příchozí zaměstnanec. V mnoha případech pak tento zaměstnanec podnik raději opustí, než by se účastnil konfliktů mezi spolupracovníky.

Mohou se vyskytovat i konflikty.Tyto konflikty mohou způsobit zaměstnanci psychické problémy. Zaměstnanec se může zhroutit nebo může neadekvátně reagovat. Samozřejmě, že tyto problémy se poté projevují na práci zaměstnance.

V těchto situacích by měl nadřízený eventuální konflikt co nejdříve vyřešit. Také by si měl vytvořit lepší prostředí, provést brainstorming, být asertivní, získat fakta, shodnout se na

problému společně, hledat možná řešení a přijmout je. Toto je úkolem personálního ředitele, vzdělávání, které by vedlo ke zlepšení firemní kultury.

5.3 Vztah zaměstnanec x zaměstnavatel

Vzhledem k problémům na pracovišti se může stát, že zaměstnanec situaci nezvládne a bude reagovat nepřiměřeně.

Bohužel může dojít i k případu šikany v organizaci. Aby zaměstnanec nedospěl k závěru, že se chce pomstít, jak by se mohlo stát, lze se samozřejmě šikaně ze strany nadřízeného bránit a to několika způsoby.

Je dobré si uchovávat důkazy, jako je například písemná dokumentace nebo emaily. Zaměstnanec by měl být také asertivní a měl by si zajistit svědectví osob, které byly u chování nadřízeného anebo se obrátit na vyššího nadřízeného, popřípadě na personální oddělení.

5.4 Pokus o vykradení firmy

Vykrást firmu se může pokusit jak zaměstnanec, tak i majitel nebo osoba, která v podniku vůbec nepracuje. Většinou se jedná o odcizení peněz ze stran zaměstnanců. Důvodem krádeže ve firmě byl, a doposud je, nespokojený zaměstnanec. Z těchto důvodů by měla být firma lépe zabezpečena. Pachatel se může pokusit do firmy dostat okny, vstupem pro zaměstnance i veřejnost nebo vchodem pro příjem zásilek.

V dalších kapitolách lze vidět návrh změn v bezpečnosti. Z pohledu vykradení firmy se bude jednat o přidání prvků PZTS.

5.5 Průnik cizích osob

Proti průniku cizích osob, je velmi důležitý bezpečnostní přístupový systém, aby se předešlo situacím, jako je vniknutí bývalého zaměstnance, který se chtěl pomstít kvůli výpovědi apod. Přístupový systém, který by předešel takovým situacím, je navržen v dalších kapitolách. Patří sem turnikety, určeny ke kontrole vcházejících osob, kamery, ochranná opatření ke vchodu pro zaměstnance, ochrana vchodu pro příjem zásilek atd.

5.6 Vandalismus

Vandalismus v objektu tiskárny může být realizován v mnoha podobách. Ze strany nespokojeného zaměstnance může dojít k úmyslnému poškození velmi cenných strojů nebo velké zakázky, což by mělo velký dopad nejen na finanční stránku firmy, ale také na její pověst. Vandalismus se ve firmě objevuje v současnosti velmi zřídka.

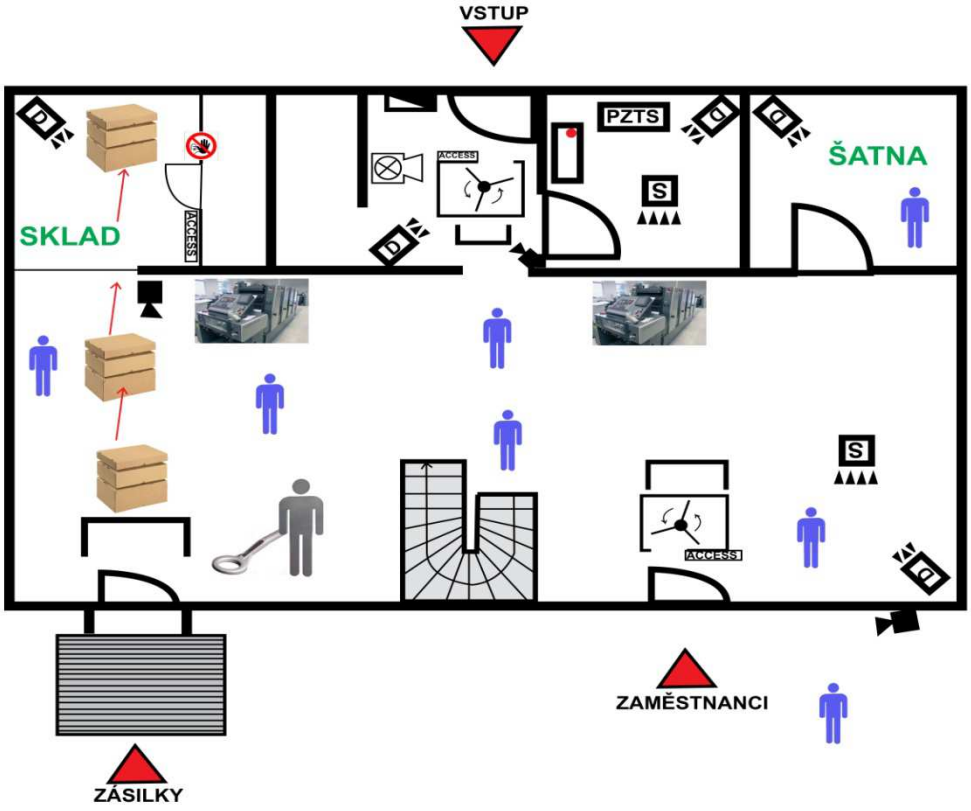
V případě vandalismu také dochází k poškození budov firmy, respektive jejich vnějšího pláště. Vandalové tyto plochy (omítky budov apod.) využijí pro malování různých kreseb, ve kterých např. projevují svůj vztek nebo prostřednictvím nevhodného nápisu, napadají osoby ve firmě. Tento projev vandalismu se ve firmě projeví především na finanční stránce a to z důvodu úprav budovy do původního stavu. Navrhovala bych proto firmě častější kontrolní obchůzky, které by měly být zaměřeny na ostrahu objektů, aby se zamezilo poškozování pláště objektu.

6 NÁVRH NOVÉHO ZABEZPEČENÍ ORGANIZACE

V této kapitole bych společnosti navrhla inovaci poplachového zabezpečovacího systému (PZS). Dále z důvodu jen obyčejné vrátnice u vstupu do budovy i zezadu budovy, kde vjíždí vozidla, bych doporučila docházkový systém, kdy zaměstnavatelé, zaměstnanci, návštěvy apod. budou vstupovat a pohybovat se po objektu jen s čipovou kartou a na základě minulé události, při které došlo k zastřelení a postřelení osob v objektu bych navrhovala poplachový tísňový systém (PTS).

6.1 Pohyb osob a materiálu v tiskárně

Zaměstnanci se mohou v prvním patře tiskárny pohybovat kdekoli, až na místnost vedle skladu, kde se nachází sklad nebezpečných látek a přístup tam má pouze pověřený zaměstnanec, který disponuje identifikační kartou od skladu. Cizí osoby a návštěvy vstupují do objektu hlavním vchodem na vrátnici čekají na příchod někoho z vedoucích osob na směně a na pokyny od zaměstnavatelů. Často se například jedná o exkurze z různých škol, nebo zákazníků. Velký prostor na obrázku pod skladem, vrátnicí, šatnou je výrobní hala. Přes výrobní halu se materiál se přiváží a odváží z rampy a většinou tento proces vykonává zaměstnanec podniku, který je přepravou pověřen a jezdí pro materiál. Zaměstnanci do objektu vstupují z druhé strany budovy a prochází do šatny přes výrobní halu. Nevstupují do objektu přes hlavní vstup.

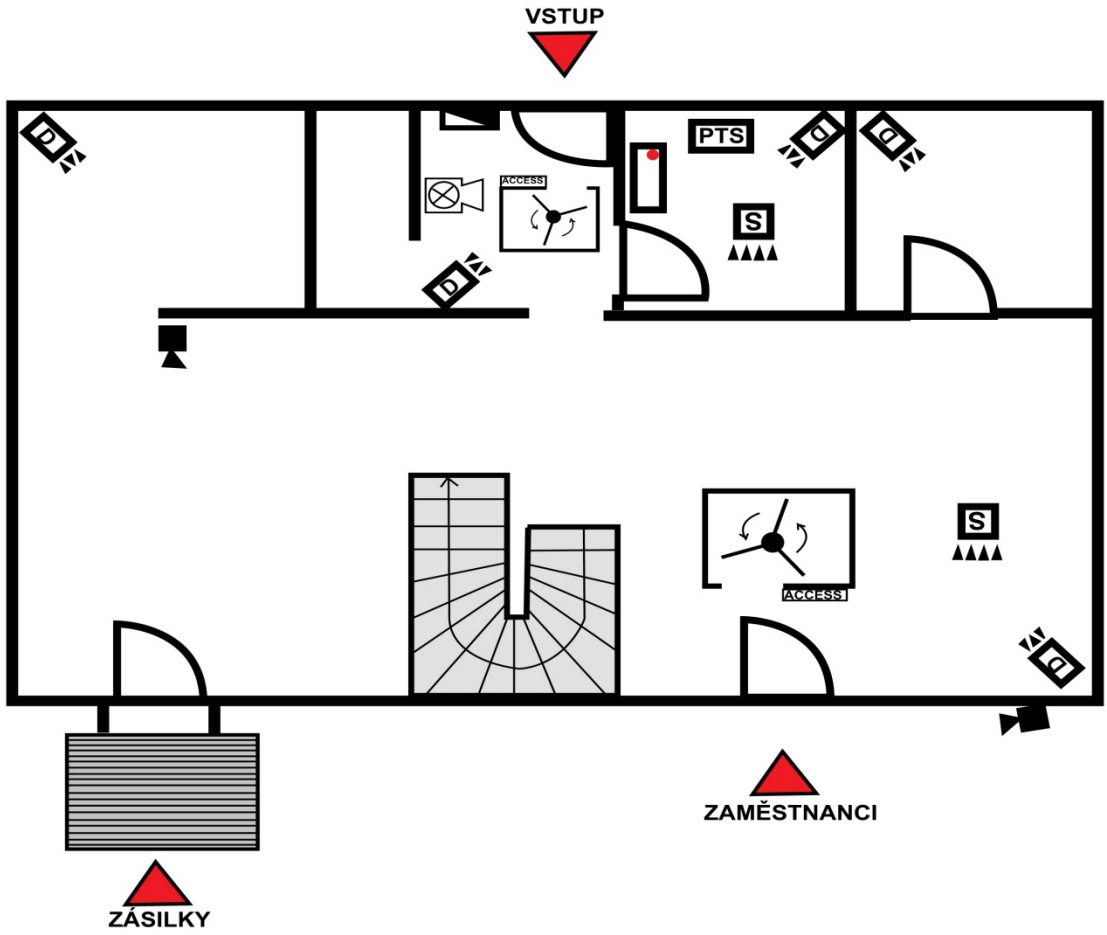


Obrázek 8. Znázornění pohybu osob a materiálu v podniku

6.2 Návrh režimového opatření – přístupový systém

Podnik zatím nedisponuje žádným systémem, který by kontroloval příchody a odchody zaměstnanců, ostrahy a osob, které podnik navštěvují. Zaměstnanec se vždy prokazuje jen obyčejnou průkazkou na vrátnici. Zavedením nového přístupového systému a dodržováním pravidel systému zvýšíme ochranu osob, objektu, celého majetku.

Na obrázku jsou znázorněny turnikety a instalovaný kontrolní přístupový systém ACCESS, který se nachází u hlavního vstupu do budovy a také u vstupu do budovy pro zaměstnance. Dále je nově zobrazeno tísňové tlačítko, které se nachází pod stolem pracovníka ostrahy na vrátnici (obrázek samotné vrátnice zobrazen níže v podkapitole 6.4).



Obrázek 9. Návrh kontrolního propustkového systému ACCESS

Vnější režimová opatření

Vnější režimová opatření se týkají osob, které se dostávají do chráněného objektu nebo objekt opouští. Navrhuji zde přejít na automatický časový režim - docházkovým systémem. Bude zde nastaven režim DEN, režim NOC. Zaměstnavatelé, neboli řídící pracovníci, se v režimu DEN do objektu dostanou bez jakékoli potíže. Jakmile vstoupí, dveře se ihned zavřou, tudíž se zamezí průchod neoprávněné osobě. Tím se zvýší bezpečnost a nedojde k vniknutí žádné cizí osoby. Návštěvy se do budovy dostanou jen v režimu DEN a to jen v pevné pracovní době řídících pracovníků od pondělí do pátku, v čase od 8:00 do 18:00 hodin, vchodem pro zaměstnavatele, kdy bude nastaven obousměrný provoz dveří. Po skončení pevné pracovní doby se aplikace nastaví na jednosměrný provoz dveří, kdy bude návštěvám vstup zakázán.

Vnitřní režimová opatření

Tato opatření se týkají osob pohybujících se uvnitř budovy, konkrétně v dané v určitém prostoru. Budou zde vyhrazené prostory, které budou přístupné pouze pro určité zaměstnance. Ti budou mít své čipové karty, které jim umožní vstup do chráněného prostoru.

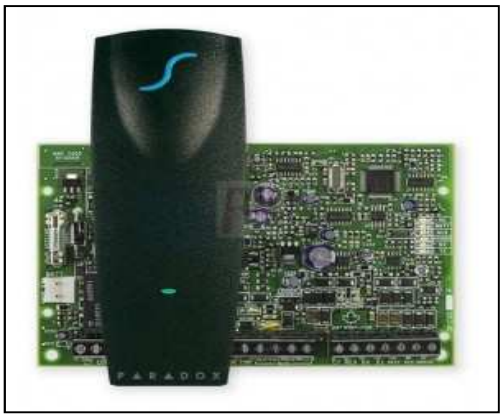
Níže navrhuji přístupový systém, který zabrání průchodu cizích osob a zajistí větší a důkladnější kontrolu osob, které budou vstupovat a pohybovat se po chráněném objektu.

Přístupový systém (ACCESS)

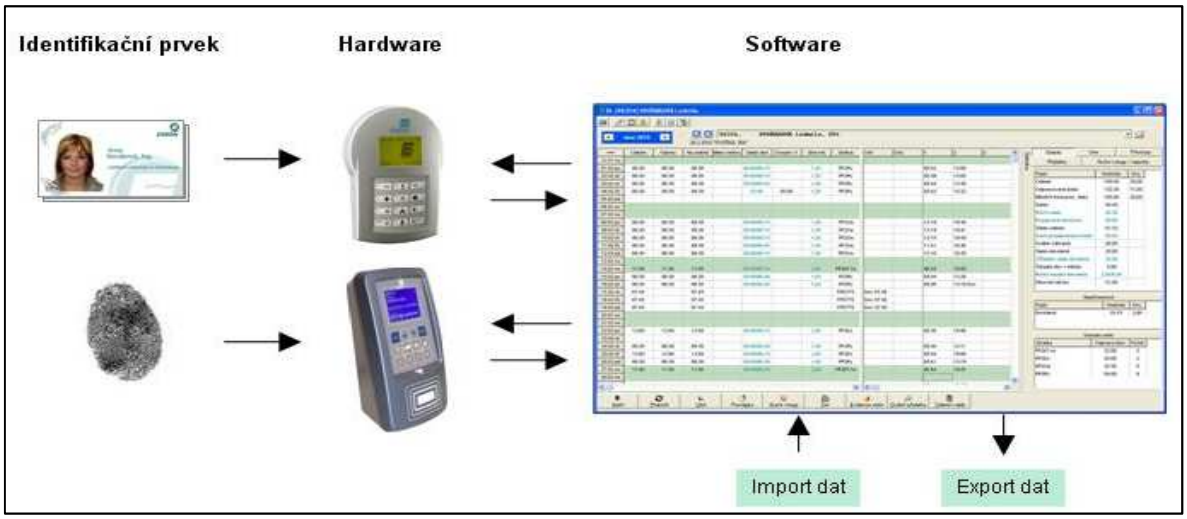
U ústředny, kterou jsem navrhla se dá využít i možnost použití Access. Do systému lze zařadit čtečky, které se mohou využívat k zastřežení a odstřežení zóny a tím řídit pohyb po chráněném objektu. Navrhuji turniket, který bude osazen čtečkou karet a to jak u předního vstupu do budovy tak i u zadního vstupu pro zaměstnance a u skladu nebezpečných látek. Zadním vstupem budou vstupovat zaměstnanci a osoby které přivezou zásilky do objektu, přes čtečky karet. Rampu, přes kterou se dováží a vyváží zásilky z tiskárny a do tiskárny, navrhuji ve vstupu ohraničit detekčním rámem, rovněž tak vstup pro zaměstnance.

ACCESSPACK 910-ACM12+R910

Tento nadstavbový balík je určen pro ústřednu EVO 192. Zde se dá připojit i modul po sběrnici k ústředně R 910, ty jsou jak pro vnitřní, tak pro venkovní použití. Modul je nutné uložit do boxu, který obsahuje napájení. Čtečkou se osadí turniket na obou stranách.



Obrázek 10. Čtečka R910 s modulem ACM 12 [31]



Obrázek 11. Bezkontaktní přístupový systém [32]

6.3 Inovace poplachového zabezpečovacího systému

Jak už jsem zmínila, tiskárna využívá systém firmy Paradox. Paradox je kanadská společnost se sídlem v Montrealu, založená v roce 1989. V současné době patří k předním organizacím ve vývoji technologií v oblasti zabezpečovacích systémů. Paradox klade velký důraz na vývoj a inovaci. Každoročně jsou do oddělení výzkumu a vývoje investovány nemalé prostředky. První série detektorů pohybu zaznamenala velký ohlas. Patenty těchto detektorů jsou stále používány. O pár let později Paradox světu představil sérii zabezpečovacích systémů Digiplex se systémem zabezpečené rozšiřitelné sběrnice. V roce 2001 byla pro změnu představena série bezdrátových systémů. V dnešní době společnost nabízí kompletní sortiment produktů pro zabezpečení malých objektů, ale i velkých sídel nadnárodních společností. [22]

Informace o střežených prostorech

Jedná se o zabezpečení vnitřních i vnějších prostor tiskárny. Jde o zabezpečení dvoupodlažního objektu, kde jsou tři vstupy do objektu. Tiskárna má 275 zaměstnanců, kteří pracují v nepřetržitém provozu. Obchodní oddělení a střední management v jednosměnném provozu. Příjem materiálu prochází přes nákladní rampu přímo do skladovacího prostoru, expeduje se opět přes nákladní rampu ze skladu hotových výrobků.

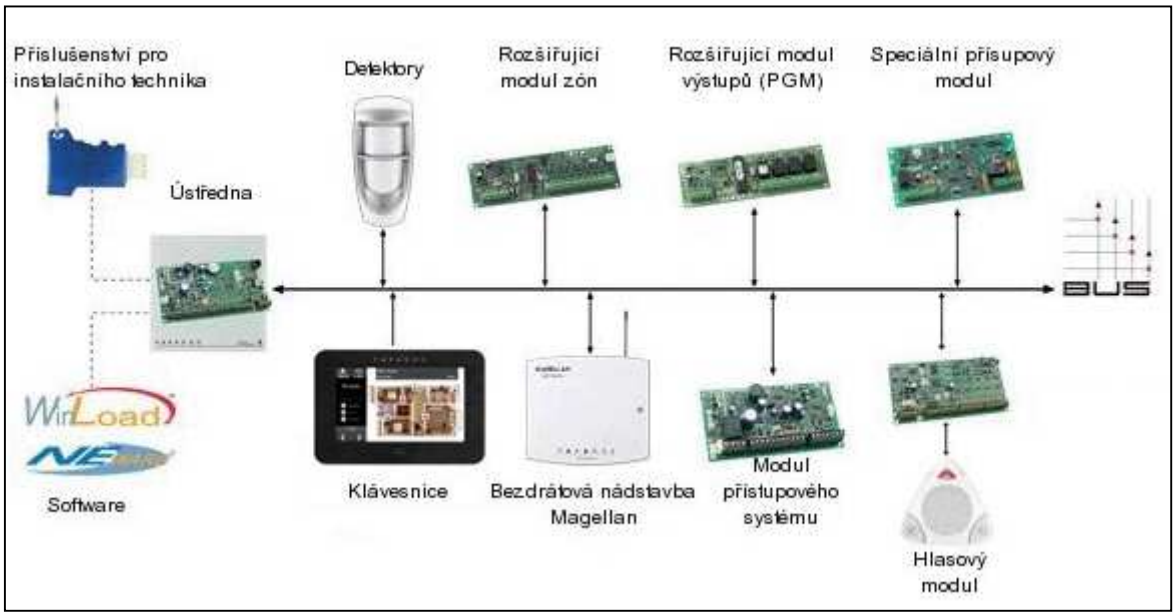
Ústředna Digiplex EVO192

Umožňuje do systému připojit 192 jednotlivých zón. Ústředna nabízí 5 PGM výstupů. Ústředna Digiplex EVO192 je plně adresovatelný sběrnicový systém, do kterého lze zařadit až 254 sběrnicových modulů (klávesnice, bezdrátová nadstavba, expandery, doplňkové zdroje, posilovač sběrnice, hlasová nadstavba, atd.). dále i samostatné sběrnicové detektory. Vedle klasických NC24 zón s výstupem relé a zón tvořených sběrnicovými detektory, lze tvořit i bezdrátové zóny připojením bezdrátové nadstavby RTX3. Deska ústředny obsahuje osm samostatných vstupů pro jednotlivé zóny, což díky technologii ATZ25 představuje až šestnáct zón. Další vlastností je tzv. Multibus, který umožňuje upgrade firmware modulů na sběrnici a to pomocí modulu 307USB, IP100/150. Ústřednu můžeme použít jako přístupový systém připojením klávesnice K641R nebo přístupového modulu ACM12.

Obrázek 12. Panel - Ústředna Digiplex EVO192 [28]

K641+ klávesnice

LCD klávesnice Digiplex K641 umožňuje snadný přístup ke všem bezpečnostním funkcím systému. Pomocí klávesnice lze systém rychle ovládat, přehledně zobrazuje informace o stavu systému, dále upravuje parametry a funkce systému. Displej se 32 znaky znázorňuje všechny stavy a naznačuje postupy ovládání systému.



Obrázek 13. Schéma zabezpečovacího systému Paradox Digiplex [25]

Obrázek 14. Sestava Digiplex EVO192 [29]

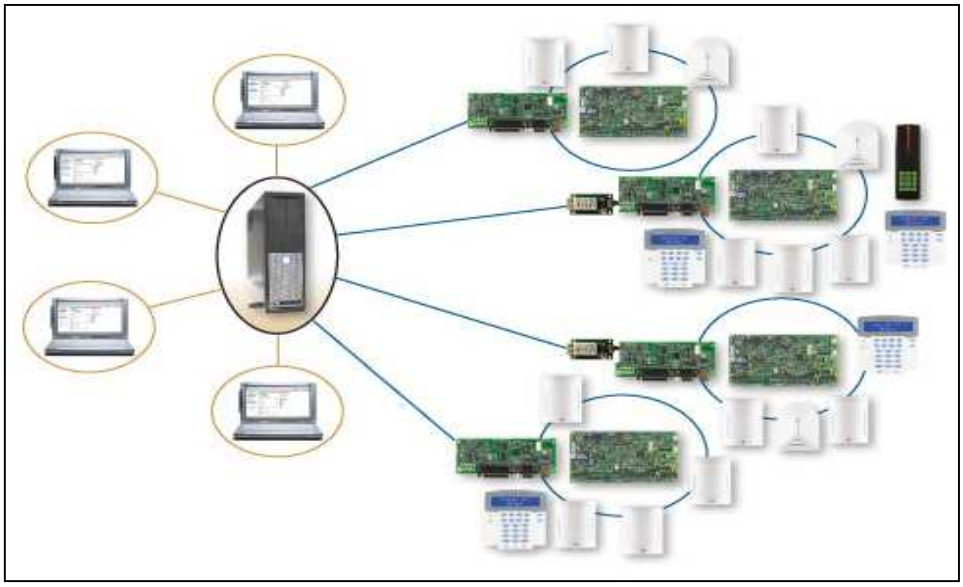
Komunikační modul PCS200

Komunikační modul PCS200 předává PZS ústřednám Paradox možnost bezdrátové komunikace, zasílání SMS zpráv, zprávu o vypnutí a zapnutí systému, vzdáleně komunikovat se softwarem Winload před GPRS. Tohle je dosaženo pomocí 4-vodičové sériové spojení mezi ústřednou a modulem PCS200. Modul PCS200 lze instalovat až 2m od EZS ústředny. Anténu na modulu lze nainstalovat až do vzdálenosti 18m od zařízení, pomocí volitelného anténní prodloužení v závislosti na síle signálu.

Obrázek 15. GSM komunikátor [30]

Security view

Z důvodu rozlehlosti objektu bych doporučila doplnit navrhovaný systém PZS vizualizačním softwarem „Security view", který je určen ke sledování, ovládání, vyhodnocování a archivaci událostí z připojené ústředny Digiplex EVO192. Vizualizační software se nainstaluje na osobní počítač, který by byl k dispozici fyzické ostraze objektu. Spojení s ústřednou se navazuje pomocí integračního modulu. Software umožňuje vložit půdorys monitorovaných objektů. Lze také umísťovat značky jednotlivých prvků (detektory, klávesnice, čtečky) a tvořit popisy podsystémů, dveří a detektorů ve vizualizaci software.



Obrázek 16. Schéma Security View [28]

Hlášení poplachu

Prostřednictvím GSM komunikátoru budou předávány informace nejen o stavu systému, ale hlavně o narušení objektu. Tyto informace budou zasílány na služební mobilní telefon ostrahy objektu. Ostraha objektu je v případě vyhlášení poplachu povinna ověřit vzniklou situaci a poté ihned informovat ředitele společnosti.

Stupeň zabezpečení objektu

Stupeň zabezpečení závisí na požadované úrovni zabezpečení. Záleží na typu objektu, předpokládaných znalostech narušitelů a jejich použitého vybavení. S ohledem na bezpečnostní posouzení a zjištěných skutečností, a na provozní režim objektu a požadavek na střežení i kancelářských a technických prostor, bych navrhovala rozdělení systému PZS do čtyř podsystémů s různým stupněm zabezpečení, viz. tabulka v teoretické části práce. Kancelářské prostory bych zařadila do druhého stupně zabezpečení. Výrobní prostory, ve kterých je pohyb zaměstnanců nepřetržitý zařadím do třetího stupně zabezpečení. Skladovací prostory s veškerým materiálem, kde může dojít k odcizení jakéhokoli nářadí, pomůcek apod., krádežím, bych doporučila čtvrtý stupeň zabezpečení.

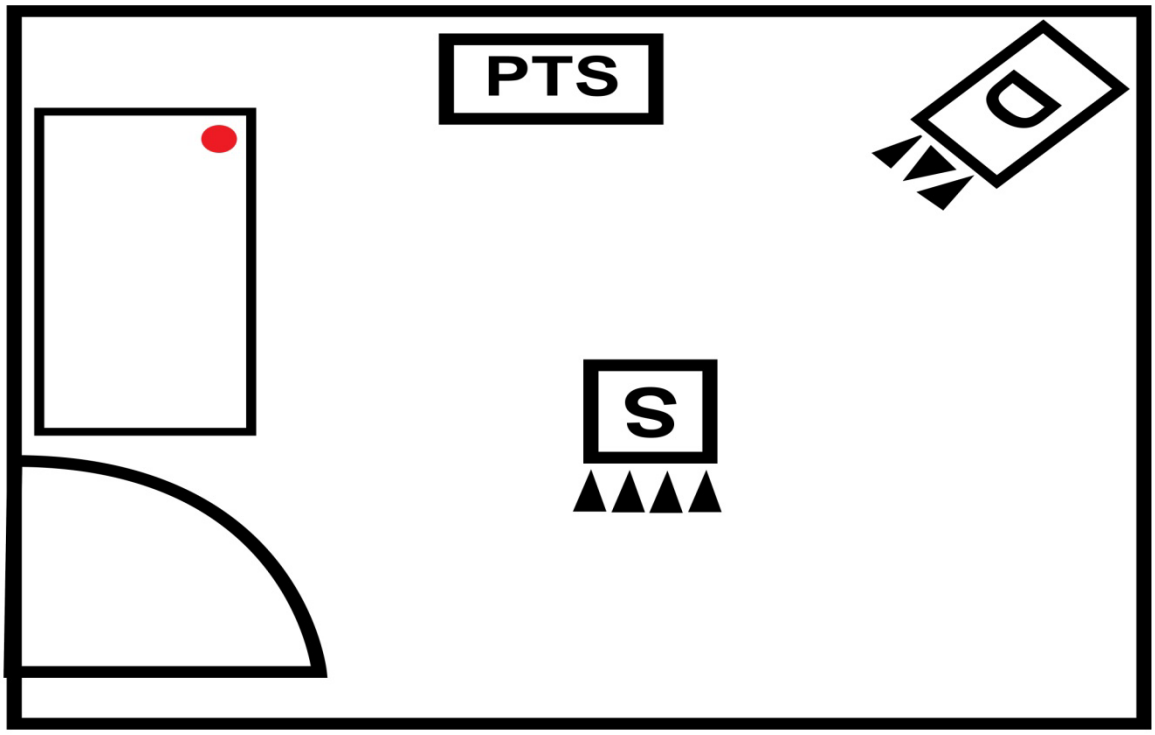
Údržba bezpečnostního systému

Z důvodu spolehlivého provozu celého systému PZS se doporučuje pravidelné přezkoušení systému. Nejlépe minimálně jednou za tři měsíce. Dále je nutno dvakrát ročně provést kompletní revizi systému prostřednictvím montážní organizace.

6.4 Poplachový tísňový systém (PTS)

V této podkapitole, jelikož organizace nemá instalované, tím pádem nemůže využívat tlačítko tísně, bych navrhovala, jak už bylo řečeno z důvodu události z předešlých let, bezdrátové tlačítko tísně instalovat na hlavní vrátnici u vchodu do budovy, i na vrátnici v zadní části budovy, kudy vjíždí vozidla do areálu.

Na obrázku je vyobrazena místnost vrátnice s poplachovým zabezpečovacím systémem (PTS), dále v pravém horním rohu se nachází duální detektor PIR – mikrovlný a uprostřed místnosti je požární hlásič. Vedle dveří je stůl a pod stolem, pro případ nebezpečí, se nachází tísňové tlačítko (červená tečka).



Obrázek 17. Znázornění tísňového tlačítka na vrátnici

VERIA 10200

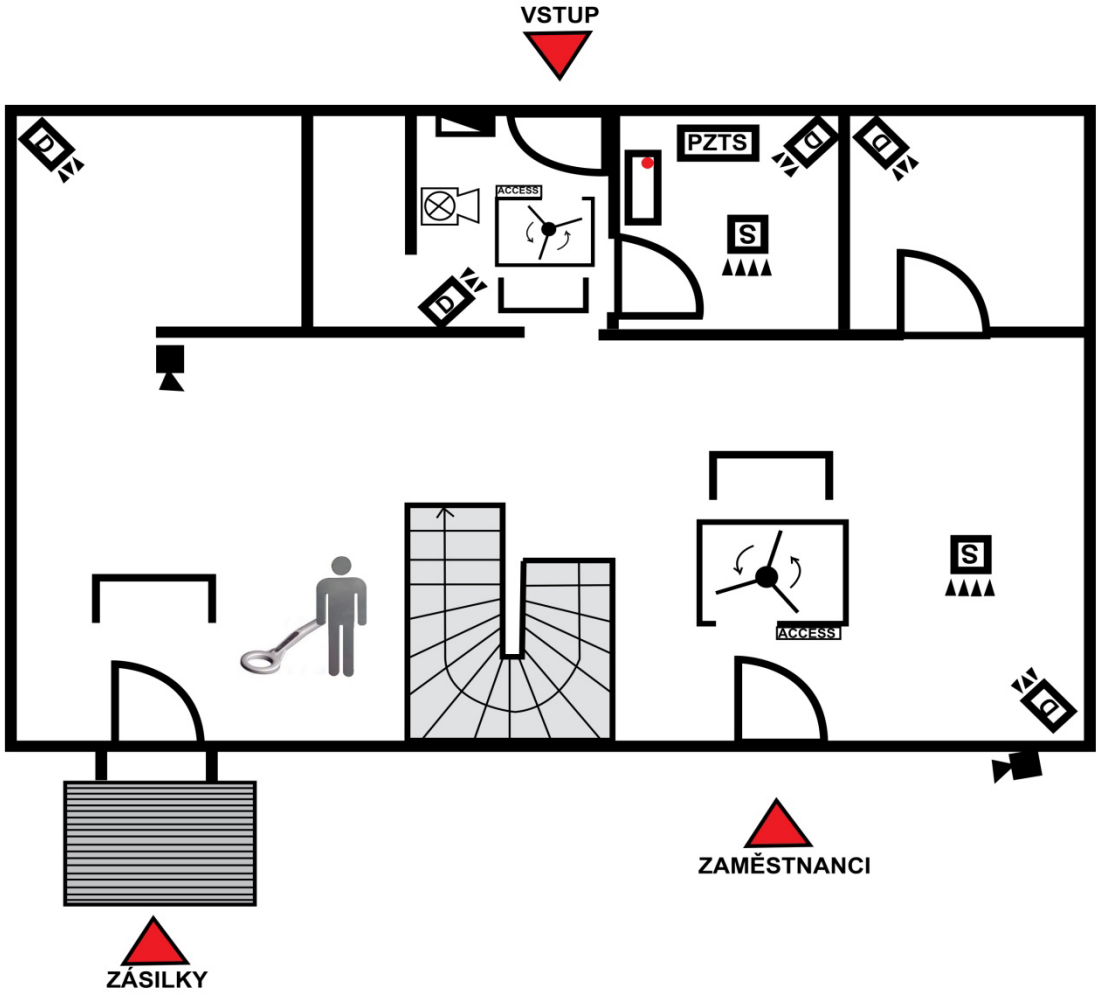
Bezdrátové tísňové tlačítko slouží k okamžitému vyvolání alarmu a přivolání pomoci. Připevněno bude na obou vrátnicích pod stolem tak, aby stisk v případě ohrožení byl co nejrychlejší. Na tlačítku se bude muset nakonfigurovat kód ústředny. Přenosová frekvence tohoto tlačítka je 433.92MHz – dosah 100m. Tlačítko bude napájeno vnitřní baterií 12V. Jakmile je tlačítko stisknuto, ústředna vyšle signál poplachu a uskuteční hovor na přednastavená telefonní čísla.

Obrázek 18. Bezdrátové tísňové tlačítko [33]

6.5 Zobrazení návrhu nového zabezpečení podniku

I.NP – Na obrázku je vyznačen PZTS místo pouze poplachového systému (PZS). Na vrátnici se ostraze objektu nabízí už i tlačítko tísně, v případě napadení bezpečnostního pracovníka nebo v případě jiného nebezpečí. Jsou zde už nově turnikety se systémem ACCESS. Dále je zde, na rozdíl od původního stavu, vyobrazen bezpečnostní detektor kovů pro důkladnější kontrolu jak osob, tak zásilek a také ruční detektor kovů.

II.NP – Po návrhu nového zabezpečení podniku zůstává beze změn.



Obrázek 19. Zobrazení nového návrhu zabezpečení v podniku

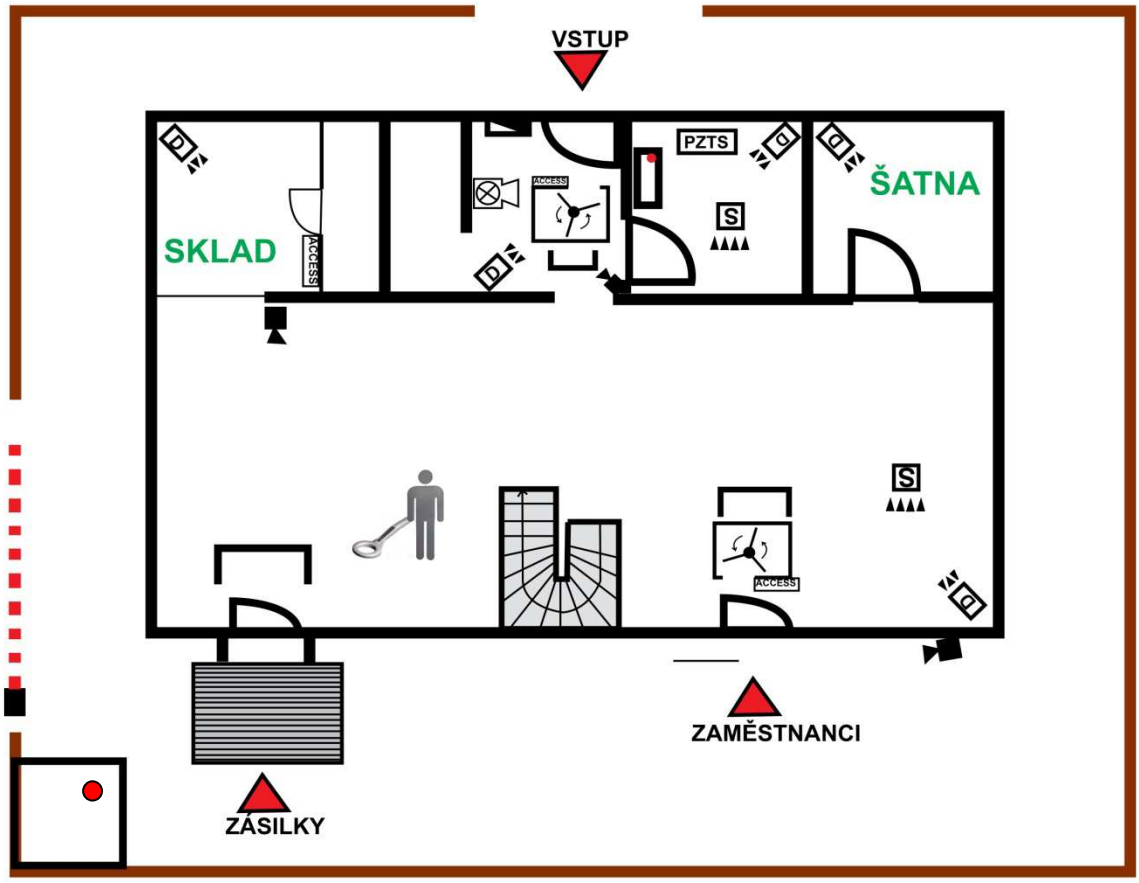
6.6 Navržená technická opatření – mechanické zábranné systémy

Podnik zatím nemá vytvořenou technickou ochranu budovy a areálu. Technickou ochranou rozumíme takový soubor přijatých bezpečnostních opatření, jehož použití v praxi zabraňuje, ztěžuje nebo oznamuje narušení ochrany objektu a celé zabezpečené oblasti. Nedílnou součástí ochrany budov je tzv. klasická ochrana, tedy využívání mechanických prostředků, zařízení a komponentů, které svou konstrukcí znemožňují jejich jednoduché překonání.

Co se týká mechanických zábranných systémů, navrhovala bych firmě závoru k vrátnici u zadního vjezdu do areálu, neboť doposud byl průjezd kolem vrátnice volný. Dále ke vstupu (jak už jsem zmiňovala výše, kdy se bude procházet do budovy na čipovou kartu)

turnikety. Z důvodu minulé události ke vstupům pro zaměstnance i k rampě, kde se předávají zásilky dovnitř budovy i ven z budovy, rámový detektor kovu, popřípadě i ruční detektor kovu.

Co se týká technického zabezpečení, na obrázku je znázorněn návrh turniketů, k oběma vstupům, kudy vcházejí osoby i se systémem ACCESS. Dále je zde, jak už bylo řečeno, u vchodu pro zaměstnance hned za turniketem umístěn rámový detektor,stejně jako u vchodu, kde se přijímají a odesílají zásilky. Tam zásilky navíc ručním detektorem kovu kontroluje pověřený pracovník. Okolo podniku se navrhuji oplocení, které podnik v doposud nemá, zezadu budovy u vrátnice, bych navrhovala závoru a na vrátnici pod stolem tísňové tlačítko.



Obrázek 20. Navržená technická opatření

Ploty

Ploty jsou prvním důležitým mechanickým prvkem obvodové ochrany tiskárny. Nejenže vizuálně charakterizují hranici pozemku, který patří k areálu a tak vytvářejí právní hranici, ale také ztěžuje nežádoucím osobám vstup do areálu podniku. K ohraničení samotného objektu a pozemku bych doporučila panelové ploty SECURIFOR 2D.

Panelové ploty SECURIFOR 2D

Panelové ploty Securifor 2D jsou navrženy k ochraně průmyslových areálů a tam, kde je důležité zvýšení bezpečnosti. Aby útočník plot překonal, bude potřebovat čtyřikrát více času než u tradičního plotu z pleteného pletiva. Malá oka plotu a silné dráty zajišťují lepší ochranu – je mnohem obtížnější plot přešplhat a silné dráty je obtížné přestřihnout pomocí nářadí, které malými oky plotu nelze prostrčit. U systému Securifor 2D je velmi vysoký faktor zpomalení – vstupu nevítaných hostů je zabráněno po delší dobu, než v případě tradičních plotů. [34]

Obrázek 21. Panelový plot [34]

Vjezdové závory

Vjezdové závory slouží pro zamezení vjezdu nepovolaných vozidel do areálu firmy. Závory se dělí dle konstrukce a šířky komunikace. Ovládání závory a zabezpečení je řešeno vždy dle individuálních potřeb zákazníka. Je to technický prvek, který vyžaduje dohled a to z důvodu nekontrolovatelného přechodu osob. Zde bych tedy doporučila u vrátnice s fyzickou ostrahou závoru. Může tak probíhat kontrola osob a automobilu na přítomnost výbušnin a nebezpečných látek pomocí ručního detektoru. Z hlediska použití a častému dennímu používání bych zvolila automatickou závoru AGF3.

Automatická závora AGF3

Automatická závora AGF3 je určena pro instalace s nejvyšší intenzitou provozu. Je navržena s rámovou konstrukcí a kompozitovými kryty karosérie. Kompozitové kryty jsou vyrobeny z pevnostního materiálu s výztuhami z nerezového plechu v kombinaci se skleněnými vlákny. Povrch karoserie je tvořen vrstvou probarvené pryskyřice v odstínu RAL. Designové řešení přináší vysokou estetickou hodnotu. Jedinečná mechanická odolnost a korozivzdornost zaručuje dlouhou životnost celého zařízení. Obsahuje vstupy pro bezpečnostní prvky a umožňuje automatické zavírání po nastaveném čase. [35]

Obrázek 22. Automatická závora [35]

Turnikety

V areálech, kde je velká frekvence osob, jsou nejvhodnějším řešením interiérové tříbodové turnikety, vstupní branky a vysokokapacitní turnikety řešení, které umožňují oprávněným osobám projít rychle a bez překážek. Pro vyšší úroveň zabezpečení jsou vhodnější plno vysoké turnikety a bezpečnostní otočné dveře. Do areálu tiskárny, bych doporučila plnorozměrový turniket, který by byl umístěn do prostoru u vstupu do objektu z přední i zadní strany a směřován před detektor kovu. Díky turniketu budou jak zaměstnanci a také návštěvy pouštěny k detektoru kovu postupně.

Plnorozměrový turniket

Plnorozměrový turniket, lakovaný nebo nerez provedení, elektromechanický obousměrný 3-ramenný rotor. Robustní konstrukce zajišťuje jednoduchý a bezproblémový provoz. Jejich využití je jak v interiéru – bezpečností otočné dveře, tak i v exteriéru. Během jedné minuty dokáže bezpečně turniket propustit až 30 osob. [36]

Obrázek 23. Plnorozměrový turniket [36]

Rámové a ruční detektory kovu

Pro zajištění bezpečnosti objektů a osob v areálu, či pro potlačení vnášení zbraní do objektu tiskárny, můžeme použít rámové a ruční detektory kovu. Fyzikální princip detekce je naprosto bezpečný a zdravotně nezávadný. Rámové detektory oproti ručním detektorům mají velkou výhodu především ve vysoké kvalitě, životnosti, jednoduché obsluze a jednoznačné signalizací alarmu, včetně určení pozice předmětu na těle prohlížené osoby. Ruční detektory mají největší výhodu v pořizovací ceně, ale oproti rámovým detektorům při průchodu většího počtu osob, může dojít k časovému zdržení. [23]

Rámové detektory kovu

Rámový detektor je určen pro detekci zbraní (a dalších kovových předmětů) u osob a u zásilek procházejících rámem. Detektor je základní součástí komplexního zabezpečovacího systému určeného ke zvýšení ochrany budovy tiskárny.

Do všech vstupů areálu firmy bych doporučila rámový detektor GATE2101-II a to především z hlediska výkonu a ceny.

Rámový detektor kovů GATE2101-II

Multizónový průchozí detekční rám s šesti vzájemně překrývajícími se detekčními oblastmi a LCD zobrazovacím displejem. Detekční rám má velmi vysokou citlivost, která je však nastavitelná. Výhodou je možnost automatické kalibrace na detekovaný předmět. Brána má světelnou a akustickou signalizaci, potlačuje interferenci a má ochranu proti neoprávněné manipulaci. Doplňkové funkce jsou statistiky průchodů osob a vyhodnocení poplachů.

Vlastnosti:

- Signalizace LED,
- 6 vzájemně překrytých detekčních oblastí,
- Nastavitelná citlivost detekce - 100 úrovní,
- Nastavitelné druhy poplachů,
- Ochrana heslem proti neoprávněné manipulaci,
- Kontrola místně nebo vzdáleně operátorem,
- Statistiky průchodů a alarmů. [37]

Obrázek 24. Průchozí detekční rám [37]

Ruční detektor kovu

Doporučila bych doplnění rámového detektoru o ruční detektor kovů MD – 200, který bude mít obsluha u sebe.

Ruční detektor kovu MD – 200

Tento ruční detektor kovu detekuje všechny kovové zbraně až po nejmenší kapesní nože a zbraně. Jeho použití je velice snadné. Stačí stisknout tlačítko a automatické obvody detekují všechny kovové předměty. Při detekci detektor pípne nebo začne vibrovat – lze nastavit. Navíc má opravdu nízkou spotřebu energie. Další výhodou je jeho nízká váha a dobrá ergonomie.

Vlastnosti:

- vysoká citlivost pro feromagnetické i neferomagnetické kovy
- současná světelná i zvuková indikace
- výdrž baterií až 40 hodin
- automatické upozornění před vybitím baterií [37]

Obrázek 25. Ruční detektor kovů [37]

6.6.1 Doporučení do budoucna

Níže popisuji doporučení, týkající se mechanických zábranných systémů.

Detektory výbušnin a nebezpečných látek

V dnešní době, kdy nastal velký nárůst teroristických útoků a jiných hrozeb, by měly firmy přemýšlet o doplnění takových technických prostředků, které dokáží detekovat přítomnost hledaných látek. Za detekci nebezpečných látek je obvykle považována detekce výbušnin, radioaktivních materiálů a jiných nebezpečných látek ohrožujících lidský život. Tyto detektory výbušnin a nebezpečných látek jsou schopny detekovat látky i z míst, které byly pouze v kontaktu s osobou s těmito látkami nakládající, například z klik v místnosti či u automobilu.

Vzhledem k ceně detektoru nebezpečných látek, který se pohybuje okolo 1 500 000,- Kč, jsem ho zde uvedla jako ukázku a možnost jeho doplnění v budoucnu. V dnešní době bych určitě doporučila jako prioritu nákup detektoru výbušnin, který může využívat fyzická ostraha přímo u závory a kontrolovat tak automobily i osoby při v jezdu do areálu.

FidoX3

FidoX3 je detektor ultra stopových koncentrací výbušnin (tzv. ETD detektory - Explosive Trace Detectors), který nabízí nejvyšší momentálně dostupnou citlivost. Detektor je vybaven velkým transreflexním barevným displejem a jeho obsluha je velmi jednoduchá. Celé zaškolení obsluhy trvá cca. 30 minut. FidoX3 reaguje na vojenské, průmyslové, kapalné i domácí výbušniny, včetně TATP, HMTD, dusičnanu amonného, peroxidu vodíku nebo

nitromethanu. V případě kritického zahlcení je výměna senzorového elementu snadná a rychlá a tudíž je možné okamžitě pokračovat v detekci. Přístroj naběhne do provozuschopného stavu během několika minut od zapnutí, baterie umožňuje až 8 hodin nepřetržitého provozu. Vlastní design detektoru vycházel z mnohaletých zkušeností z nasazení v kritických misích, je tedy dotažen do nejmenších detailů. Detektor se velmi dobře drží a snadno se ovládá, je lehký a velmi odolný. Pro obsluhu tedy není problém s detektorem nepřetržitě pracovat i po dobu mnoha hodin a to i v obtížných podmínkách. [38]

Obrázek 26. Detektor výbušnin [38]

Mobilní FT-IR spektrometr TruDefender FT

Přístroj slouží k identifikaci pevných a kapalných látek na základě infračervené spektrometrie s fourierovou transformací. Přístroj je schopen identifikovat cca 11 000 potenciálně nebezpečných látek během několika sekund. Tento přístroj k měření využívá diamantový jedno-odrazový ATR nástavec. Díky diamantovému ATR a speciálnímu přípravku pro reprodukovatelné přitlačení vzorku k ATR spektrometr umožňuje snadné měření kapalin, past, prášku a pevných vzorků. [38]

Obrázek 27. Přístroj k identifikaci pevných a kapalných látek [38]

7 EKONOMICKÉ ZHODNOCENÍ NAVRHOVANÝCH ŘEŠENÍ

V následujících tabulkách jsem spočítala, kolik by firma musela investovat, pokud by chtěla pořídit vše, co navrhuji v novém návrhu na zabezpečení organizace.

Vzhledem k minulé události firma chtěla inovovat starý zabezpečovací systém a souhlasila s projektem systému novějšího s dalšími doplňkovými funkcemi, přístupového systému pro kontrolu vstupu, tísňového tlačítka.

Ceny uvedené ve všech tabulkách jsou ceny orientační dohledány z internetu anebo po poptávce u distributora.

Tabulka 2. Ekonomické zhodnocení PZTS

Název	Cena/Ks	Počet ks	Cena celkem
Ústředna Digiplex EVO 192	3 500 Kč	1	3 500 Kč
Klávesnice Digiplex K641	3 900 Kč	1	3 900 Kč
Komunikační modul PCS200	6 360 Kč	1	6 360 Kč
Security view	19 500 Kč	1	19 500 Kč
Přístupový systém	15 000 Kč	1	15 000 Kč
ACCESSPACK 910-ACM12+ R910	7 300 Kč	3	21 900 Kč
Tísňové tlačítko VERIA 10200	500 Kč	2	1 000 Kč

Cena celkem za instalaci bez DPH	**71 160 Kč**
Cena celkem za instalaci včetně 21% DPH	**86 103 Kč**

Vzhledem k velikosti objektu a areálu je cena základních technických opatření adekvátní. Nejdražší položku zde tvoří plnorozměrový turniket, poté celkové oplocení areálu a rámový detektor, jelikož by bylo vhodné tyto detektory pořídit tři, dva ke vstupům osob a jeden ke kontrole zásilek. Všechny technické prvky jsou blíže popsány a specifikovány v podkapitole 6.5.

Tabulka 3. Ekonomické zhodnocení technických opatření

Název	Cena/Ks	Počet ks	Cena celkem
Panel Nylofor* 2 D	1 200 Kč	95	114 000 Kč
Automatická Závora	36 800 Kč	1	36 800 Kč
Plnorozměrový turniket SESAME-P	154 700 Kč	2	309 400 Kč
Rámový detektor GATE2101 - II	28 000 Kč	3	84 000 Kč
Ruční detektor MD - 220	850 Kč	3	2 550 Kč

Cena celkem bez DPH	**546 750 Kč**
Cena celkem včetně DPH	**661 567 Kč**

V poslední tabulce bych organizaci do budoucna, z důvodů ať už teroristických útoků nebo jiných hrozeb, doporučila pořídit dva technické prostředky, detektor výbušnin a dále přístroj sloužící k identifikaci pevných a kapalných látek. Jedná se už o cenově velmi nákladné položky. Opět bych zmínila, že cena je pouze orientační (není přesně stanovená) z internetu nebo po poptávce u distributora.

Tabulka 4. Ekonomické zhodnocení doporučených technických opatření

Název	Cena/Ks	Počet ks	Cena celkem
Detektor výbušnin FIDO X3	450 000 Kč	1	450 000 Kč
Mobilní FT-IR spektrometr TruDefender FT	500 000 Kč	1	500 000 Kč

Cena celkem bez DPH	**950 000 Kč**
Cena celkem včetně DPH	**1 149 500 Kč**

Jelikož ceny jsou poměrně vysoké, doporučovala bych investorovi rozdělení investic do dvou realizací.

První část realizace

Do první části realizace bych doporučila co nejdříve pořídit celý nový poplachový zabezpečovací a tísňový systém, který navrhuji v kapitole 6. Jedná se o ústřednu Digiplex EVO 192, hlavně kontrolní přístupový systém a také tísňové tlačítko. Celková částka je zde poměrně přijatelná a vzhledem minulé události bych doporučila pořídit tento systém ihned.

Druhá část realizace

Do druhé části realizace bych zařadila oplocení areálu panely 2D, plnorozměrový turniket, závoru, zde je důležité ponechat u vjezdu fyzickou osobu, která nadále bude kontrolovat osoby a automobily, které budou směřovat do areálu tiskárny Dále bych doporučila pořídit, minimálně na zkoušku, alespoň jeden detekční rám a pokud se osvědčí, navrhovala bych pořídil i další dva ke všem vchodům do budovy. Ruční detektory kovu jsou cenově nižší položkou, také doporučuji pořídit.

Doporučení do budoucna

Nákup přístroje sloužícího k identifikaci pevných a kapalných látek vzhledem k ceně 500 000,- Kč je největší investicí. U detektoru výbušnin je, dle mého názoru, cena naprosto adekvátní a to vzhledem ke snadnému používání a možnosti kontroly jak osob, tak i automobilů u vjezdu do areálu.

ZÁVĚR

Cílem mé diplomové práce bylo zpracovat zabezpečení velké tiskárny z pohledu rizikovosti objektu a procesů, které v něm probíhají. Tyto dvě oblasti spolu velmi úzce souvisí, proto provedená analýza s návrhem bezpečnostních opatření vytváří holistický pohled na bezpečnostní situaci v celé organizaci.

Vzhledem k častějším a rozsáhlejším bezpečnostním incidentům, probíhajícím ve veřejném i soukromém sektoru, je oblast zabezpečení objektů velmi aktuálním tématem v dnešní společnosti. Jelikož se jedná o oblast, která se týká organizace jako celku, tedy všech úrovní řízení, je nutné provádět pravidelnou analýzu tohoto prostředí s důrazem na kritické hodnocení současného stavu. V celosvětovém kontextu je pak oblast zabezpečení objektů a procesů, které v nich probíhají, předmětem neustálého vědeckého vývoje, který přináší stále nové poznatky v tomto oboru. Tyto nové informace přispívají ke zlepšení bezpečnostní situace v organizacích, což vede k předcházení budoucích rizikových situací, které mohou mít destruktivní následky.

Bezpečnostní incidenty a rizika jsou již dnes nedílnou součástí tohoto světa a je třeba tuto skutečnost respektovat. Je ale samozřejmě potřeba se naučit na tyto situace adekvátně reagovat, s cílem minimalizovat nežádoucí dopady. Tohoto stavu lze dosáhnout v podobě sofistikovanějších režimových a bezpečnostních opatření, která budou implementována v daných organizacích, s ohledem na charakter jejich činnosti.

Vzhledem k bezpečnostní situaci, která byla předmětem analýzy této diplomové práce, jsem zvolila přístup, který je zaměřen na návrh režimových opatření s ohledem na procesy a činnosti, probíhající ve velké tiskárně. Dílčí částí této práce je také návrh zabezpečení tohoto objektu proti průniku zbraní a nebezpečných výbušných látek, s cílem zamezit opakování situace, která zde nastala před několika lety a která také přispěla k tomu, aby se bezpečností tohoto objektu začal podnik seriózněji zabývat. Na závěr této práce je předloženo ekonomické zhodnocení, které by mělo přinést přehled reálných nákladů, které je třeba investovat na zlepšení dané situace.

Doufám, že tato práce pomohla případnému čtenáři k vytvoření odborného pohledu na danou problematiku, s cílem rozšířit jeho znalostí v této oblasti. Každý z nás pracuje v nějakém podobném objektu, myslím si, že toto téma se týká nás všech, celé společnosti. Mým přáním je, aby tato práce byla využita nejen pro tuto organizaci, ale také pro jiné objekty podobného charakteru, pro které může být velmi přínosná.

SEZNAM POUŽITÉ LITERATURY

[1] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 978-80-7318-889-4.

[2] IVANKA, Ján. *Systemizace bezpečnostního průmyslu I*. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 123 s. ISBN 978-80-7318-850-4.

[3] BRABEC, František. *Hlídací služby*. Praha: Eurounion, 1995, 259 s. ISBN 80-85858-12-6.

[4] ČERNÝ, Josef. *Evropský výcvikový modul pro základní ostrahu*. Vyd. 1. Zlín: Univerzita Tomáše Bati, Technologická fakulta, 2003, 152 s. ISBN 80-7318-107-x.

[5] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II*. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-80-7318-631-9.

[6] UHLÁŘ, Jan. *Technická ochrana objektů*. Vyd. 1. Praha: Vydavatelství PA ČR, 2006, 246 s. ISBN 80-7251-235-8.

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

[8] UHLÁŘ, Jan. *Technická ochrana objektů*. Vyd. 1. Praha: Vydavatelství PA ČR, 2005, 229 s. ISBN 80-7251-189-0.

[9] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 122 s. ISBN 80-7318-231-9.

[10] BRABEC, František. *Ochrana bezpečnosti podniku*. Vyd. 1. Praha: Eurounion, 1996, 203 s. ISBN 80-85858-29-0.

[11] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management I*. 1. vyd. Zlín: VeRBuM, 2011. ISBN 978-80-87500-05-7.

[12] KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 2. [S.l.: s.n.], 2003. ISBN 80-902938-2-4.

[13] *ELEKTRICKÁ POŽÁRNÍ SIGANLIZACE: elektronické zabezpečení objektů* [online]. [cit. 2016-04-21]. Dostupné z: www.maxprogres.cz

[14] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management IV.: teorie a praxe ochrany majetku a fyzické bezpečnosti*. 1. vyd. Zlín: VeRBuM, 2014. ISBN 978-80-87500-57-6.

[15] *Bezpečnost: Bezpečnost* [online]. [cit. 2016-04-20]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/

[16] TALAŠOVÁ, Andrea. *Spolehlivost lidského činitele a možná rizika na pracovišti* [online]. Zlín, 2013 [cit. 2016-04-20]. Dostupné z: https://stag.utb.cz/portal/. Bakalářká práce. UTB.

[17] *ACCESS: Elektronické zabezpečení objektů* [online]. [cit. 2016-04-21]. Dostupné z: http://www.cominfo-trade.com/cz/reseni/pristupovy-system

[18] *EPS: elektronická požární signalizace* [online]. [cit. 2016-04-21]. Dostupné z: http://www.systemy-stech.cz/elektronicka-pozarni-signalizace-eps/

[19] *BEZPEČNOSTNÍ FOLIE: zabezpečení objektů* [online]. [cit. 2016-04-21]. Dostupné z: http://www.next.cz/bezpecnostni-folie

[20] VAŇÁSKOVÁ, Lenka. *Bezpečnostní detektory kovů na letištích* [online]. Zlín, 2011 [cit. 2016-04-21]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/. Bakalářská práce. UTB.

[21] *Fakta organizace* [online]. [cit. 2016-04-21]. Dostupné z: http://www.graspo.com

[22] *Paradox: O společnosti* [online]. [cit. 2016-04-21]. Dostupné z: http://www.paradox.cz/paradox.php

[23] *Tuebor: elektronické zabezpečení* [online]. [cit. 2016-04-21]. Dostupné z: http://www.tuebor.cz/

[24] VALOUCH, Jan. *Projektování integrovaných systémů* [online]. Zlín, 2013 [cit. 2016-04-22]. Dostupné z: https://digilib.k.utb.cz

[25] *Zabezpečovací systém* [online]. [cit. 2016-04-21]. Dostupné z: http://www.eurosat.cz/

[26] *CCTV: systém uzavřených televizních okruhů* [online]. [cit. 2016-04-21]. Dostupné z: http://www.fogart.cz/cctv/

[27] *CCTV: systém uzavřených televizních okruhů* [online]. [cit. 2016-04-21]. Dostupné z: http://www.falcocomputer.cz/elektroinstalace/cctv-kamerove-systemy/

[28] *Ústředny a sestavy* [online]. [cit. 2016-04-25]. Dostupné z: www.abalarm.cz

[29] *Zabezpečovací systémy Paradox Digiplex* [online]. [cit. 2016-04-25]. Dostupné z: www.ssam.com

[30] *Zabezpečení budov: GSM komunikátor* [online]. [cit. 2016-04-25]. Dostupné z: www.zabezpeceni-budov.cz

[31] *ACCESSPACK* [online]. [cit. 2016-04-25]. Dostupné z: http://www.variant.cz/zbozi/0702-233-accesspack-acm12-r910

[32] *Bezkontaktní identifikační systém* [online]. [cit. 2016-04-25]. Dostupné z: www.eskon.cz

[33] *Domovní alarmy* [online]. [cit. 2016-04-25]. Dostupné z: http://domovni-alarmy.heureka.cz/bezdratove-tisnove-tlacitko-veria-10201/

[34] *Panelové ploty* [online]. [cit. 2016-04-25]. Dostupné z: http://www.betafence.cz/inspirace/inspirace-1/panelove-ploty-securifor-pro-vysokou-bezpenost¨

[35] *Automatická závora* [online]. [cit. 2016-04-25]. Dostupné z: http://www.autogard.cz/produkty/zavory/automaticka-zavora-agf3/

[36] *Plnorozměrový turniket* [online]. [cit. 2016-04-25]. Dostupné z: http://www.acsline.cz/cs/plnorozmerovy-turniket

[37] *Detektory kovů* [online]. [cit. 2016-04-25]. Dostupné z: https://eshop.eurosat.cz/

[38] *Laboratorní technika* [online]. [cit. 2016-04-25]. Dostupné z: http://www.rmi.cz/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PZTS	Poplachový zabezpečovací a tísňový systém
PZS	Poplachový zabezpečovací systém
PTS	Poplachový tísňový systém
ACCESS	Access Control System – systém kontroly vstupu
CCTV	Closed Circuit Television - uzavřený televizní okruh
EPS	Elektronická zabezpečovací signalizace
HZS	Hasičský záchranný sbor
PCO	Pult centralizované ochrany
DPPC	Dohledové poplachové a přijímací centrum
SBS	Soukromá bezpečnostní služba
SW	Software
HW	Hardware
Apod.	A podobně
Atd.	A tak dále
Např.	Například
Tzv.	Takzvaně
Aj.	A jiné
Tzn.	To znamená

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: PROTIPOŽÁRNÍ OPATŘENÍ

Příčina požárů je souhrn dějů předcházejících vlastnímu zapálení. Příkladem je technická závada na elektrickém zařízení. Nemusí vždy způsobit požár, neboť ten vznikne tehdy, pokud technická závada způsobí jiskru nebo dostatečné teplo k zapálení hořlavé látky.

Mezi nejčastější příčiny požáru patří:

Nedbalost pro používání tepelných spotřebičů či jejich nesprávná instalace: např. spotřebiče ponechané v provozu bez dozoru umístěné blízko hořlavých materiálů, nedostatečná kontrola teploty atd.

- Hořlavé a výbušné prachy

Např. špatné odsávání, pracovní postupy se zdrojem tepla nebo jisker v prašném prostředí, nedostatek monitorování, měření atd.

- Nedbalost

Např. kouření v zakázaných prostorách, narušování bezpečnostního zařízení, odstranění kontrolních čidel atd.

- Špatná údržba

Např. nedostatek údržby v pracovní oblasti a zařízení, přeplněné odpadkové koše a nádoby apod.

- Samovznícení

Např. nedostatečné dodržování předepsaných postupů pro manipulaci a skladování s materiály schopnými samovznícení, nánosy různých druhů nátěrových hmot apod.

Třídy požárů

Požáry lze dělit do čtyř tříd:

Třída A: požáry pevných hořlavých hmot – papír, dřevo

Třída B: požáry hořlavých kapalin – benzin

Třída C: požáry plynů – propan, butan

Třída D: požáry hořlavých kovů – aluminium

Hasící přístroje

Hasící přístroje jsou prostředky požární ochrany, na něž se vztahují základní ustanovení právních a technických předpisů. Hasící přístroje jsou přenosné, pojízdné, přívěsné.

Vnější povrch hasícího přístroje je červený. Přístroje plněné CO2 jsou značeny černým pruhem na horní zaoblené části láhve. Hasící přístroje podléhají pravidelným kontrolám, které musejí být prováděny jen oprávněnými osobami a musejí být označeny druhem a datem poslední kontroly.

Tabulka 5. Typy hasících přístrojů pro třídy [4]

Typ	**Třída**
Voda	A
Pěna	A, B

Prášek A, B, C a požáry, kde je riziko elektronického zřízení pod proudem. CO_2, B, C a požáry, kde je riziko elektronického zařízení pod proudem.

Princip hašení a užití hasících přístrojů

Oheň bude hořet do té doby, dokud bude pohromadě palivo, kyslík a teplo. Principem je odstranění nejméně jednoho z prvku požárního trojúhelníku.

K dosažení tohoto slouží tři prostředky:

- Izolace – odstraněním paliva nebo odklizením, pokud možno největší části paliva. Např. požár prasklého plynového potrubí – při uzavření přívodu se zastaví přívod paliva.
- Ředění nebo snížení dusivého efektu – Snížení nebo zamezení kyslíku k ohni. Kyslík je důležitý pro udržení ohně a příkladem toho může být instrukce uzavřít za sebou všechny dveře při evakuaci, což omezí množství kyslíku a zpomalí šíření ohně.
- Chlazení – nejobecnější způsob hašení požáru. Zahrnuje lití co největšího množství vody, která je nejefektivnějším hasícím mediem, pokud budeme mluvit o nákladech. Chlazení odvádí nebo snižuje množství tepla, a tím snižuje možnost rozšíření ohně. Aby oheň mohl pokračovat, musí být zachována dostatečná teplota.

Požární prevence

- Udržovat volné únikové cesty (chodby, schodiště…)
- Dodržovat bezpečné vzdálenosti pro hořlavé materiály od zdrojů tepla
- Uniklé hořlavé kapaliny musí být hned zachyceny vhodným sorbentem a ten zlikvidován uložením v předepsaných nádobách
- Zdroje tepla a elektrické spotřebiče nesmí zůstat ponechány v provozu bez dozoru
- Pravidelně kontrolovat všechny hasící přístroje, aby byly vždy na svém místě, v provozuschopném stavu a byl k nim volný přístup
- Být seznámen s evakuačními plány, kdyby nastala mimořádná událost
- Zachovávat správný systém záznamů a hlášení [4]