Zabezpečení a ochrana objektu obchodně výrobního podniku

Michal Košut

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2018/2019

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

Jméno a příjmení:	**Michal Košut**
Osobní číslo:	**L16035**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**

Téma práce: **Zabezpečení a ochrana objektu obchodně výrobního podniku**

Zásady pro vypracování:

1. **Vypracujte z dostupné odborné literatury teoretickou část na téma zabezpečení a ochrana objektů.**
2. **Zmapujte a popište současné zabezpečení podniku.**
3. **Posuďte rizika zabezpečení podniku metodami analýzy rizik.**
4. **Zhodnoťte současný stav a navrhněte nápravné opatření, která povedou ke zvýšení úrovně zabezpečení podniku.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management IV. Zlín: Radim Bačuvčík – VeRBuM, 2014. ISBN 978-80-87500-57-6.

[2] IVANKA, Ján. Mechanické zábranné systémy. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-910-5.

[3] UHLÁŘ, Jan. Technická ochrana objektů. Praha: Vydavatelství PA ČR, 2006. ISBN 80-7251-235-8.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **doc. Ing. Miroslav Tomek, PhD.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **30. listopadu 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

V Uherském Hradišti dne 30. listopadu 2018

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji 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;
- 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;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15. 5. 2019

Jméno a příjmení studenta: Michal Košut

.....
podpis studenta

ABSTRAKT

V bakalářské práci se zabývám problematikou zabezpečení a ochranou objektu obchodně-výrobního podniku. Bakalářská práce se skládá ze dvou částí.

V teoretické části budou popsány základní prvky zabezpečení a jejich užívané pojmy, jejich funkce a technický popis. Obvodová ochrana, plášťová ochrana, režimová ochrana, poplachové zabezpečovací a tísňové systémy, elektrická požární signalizace, kamerového systému a formy soukromé bezpečnostní agentury.

Praktická část práce bude zaměřena na vybraný objekt. Následně bude zmapováno a popsáno současné zabezpečení objektu. Součástí práce bude SWOT analýza, Ishikawa diagram a metoda PNH zabezpečení vybraného podniku.

Na základě zjištěných výsledků bude vypracováno vyhodnocení a navržení vhodných opatření k doplnění zabezpečení a ochrany objektu, které by vedlo ke snížení možnosti zranitelnosti podniku a vnějších hrozeb.

Klíčová slova: bezpečnost, hrozba, obchod, ochrana, podnik, výroba, zabezpečení.

ABSTRACT

In my bachelor thesis I deal with problematics of security of a commercial manufacturing company premises. The thesis is consists of two main parts.

The first part is teoretical. There are described the basic elements of security, most used terms of this topic, functions and technical description. Some of the terms are: circuit protection, cover protection, mode protection, alarm security and emergency systems, fire alarm system, CCTV (closed circuit television) and forms of private security agency.

In the practical part I do focus on specific object. Then I describe current level of security by the active and passive elements. Part of the thesis is SWOT analysis, Ishikawa diagram and PHN security method of the company.

On the basis of the results are created evaluations and suggestions of recommended and suitable precautions to increase security and protection level of the building. These precautions should decrease possibility of vulnerability of the company and external threats.

Keywords: safety, threat, commerce, protection, company, production, security

Rád bych poděkoval doc. Ing. Miroslavovi Tomkovi, Ph.D. za odborné vedení, poskytnutí cenných rad, informací, pomoci a času v průběhu zpracování bakalářské práce. Dále bych rád poděkoval i rodině za podporu během mého studia.

OBSAH

ÚVOD

Zabezpečení a ochrana objektů má v dnešní době významnou roli, která vede k poklesu a eliminaci rizika poškození zájmů jedince, souboru či celého podniku. Ke korektnímu zajištění funkční ochrany je nutné zkombinovat jednotlivé prvky tak, aby tvořily kompatibilní, rovnovážný a rezistentní systém. Aktuální možnosti zabezpečení jsou na vysoké technické úrovni.

Cílem bakalářské práce je zmapovat a popsat aktuální zabezpečení podniku, na základě shromážděných podkladů vypracovat analýzu rizik a následně navrhnout opatření, která povedou ke zvýšení úrovně zabezpečení podniku.

Bakalářská práce je rozdělena do dvou kapitol, na teoretickou a praktickou část. V teoretické části je zmíněno několik zásadních událostí, které proběhly v podnicích na území České republiky. Navazují právní předpisy pro zabezpečení budov a popis možných způsobů zabezpečení podniků jako jsou např. fyzická ochrana, mechanické zábranné systémy, režimová ochrana a prostředky technické ochrany. Teoretická část je ukončena popisem jednotlivých cílů práce a použitými metodami k odhalení možných hrozeb a rizik pro obchodně výrobní podnik.

Praktická část se zabývá posouzením současného stavu zabezpečení obchodně výrobního podniku, zmapováním objektu a popisem jednotlivých typů ochran uvedených v teoretické části. Následuje aplikace SWOT analýzy, Ishikawa diagramu a metody PNH. Praktickou část uzavírá návrh na zvýšení zabezpečení objektu obchodně výrobní společnosti s vyhodnocením ekonomických nákladů.

Práce má odpovědět na otázky, zdali je zabezpečení podniku vyhovující a dostatečné, jakých ochran využívá a je-li možné zvýšení míry zabezpečení a ochrany objektu obchodně výrobního podniku.

I. TEORETICKÁ ČÁST

1 VÝZNAM ZABEZPEČENÍ OBJEKTU OBCHODNĚ VÝROBNÍ SPOLEČNOSTI

V dnešní uspěchané, moderní a pokročilé době spjaté s technologickým rozvojem je nutné věnovat problematice ochrany a zabezpečení podniků zvýšenou pozornost. A to z důvodu ochrany majetku společnosti, ale i zdraví zaměstnanců a pracovníků.

1.1 Negativní události vzniklé v historii obchodně výrobních podniků

Za zmínku stojí několik tragických událostí, při kterých došlo ke škodám na majetku, ale především ke ztrátám lidských životů. Jedná se o požáry výrobních hal nebo napadení řídících pracovníků v podniku. K nevýznamnějším událostem lze zařadit následující události:

- 2009 – Česká republika, Zlínsko, v tamní tiskárně Graspo postřelil propuštěný zaměstnanec dva manažery,
- 2011 - Česká republika, Kunovice, ve společnosti Aircraft útočník zastřelil dva vrcholové manažery a postřelil ředitelku společnosti,
- 2015 – Česká republika, Litvínov, požár v chemičce Unipetrol způsobil škodu dvanáct a půl miliardy korun českých.

Z uvedených důvodů je potřebné věnovat pozornost komplexnímu zabezpečení podniků.

1.2 Právní předpisy zabezpečení objektů

Právní předpisy platí ve všech oborech a jinak tomu není ani v oblasti zabezpečení podniků. Mezi primární právní předpisy patří Listina základních práv a svobod, Občanský zákoník, Trestní řád a Trestní zákon, které je nutné dodržovat a respektovat. Na jedné straně je na ochranu podniku nahlíženo z pohledu vlastníků, kteří se snaží o maximální zabezpečení podniku, vlastního i svěřeného majetku. Na straně druhé je pohled občana. Avšak nikdy nesmí být překročeny právní hranice ochrany tak, aby bylo způsobeno zasažení do práv a svobod. [1]

Instalované zabezpečovací systémy musí splňovat vlastnosti vyžadované normami a právními předpisy. Pro zabezpečení budov platí především české technické normy (dále jen „ČSN“) nebo normy evropské či mezinárodní, které bývají označeny zkratkami EN, ISO, IEC a ETSI, které jsou veřejně dostupné. Tyto předpisy jsou přejaty do struktury českých norem. Česká technická norma je formulací nároků na výrobky, procesy či služby, aby byly

vhodné pro své použití. Stanovují základní požadavky na kvalitu, bezpečnost, ochranu zdraví a životního prostředí. [2]

Mezi základní normy patří:

- Vyhláška č. 23/200/Sb. – O technických podmínkách požární ochrany staveb.
- ČSN EN 50131-1 až 6 – Poplachové systémy. Elektrické zabezpečovací systémy.
- ČSN EN 50136-1-1 – Poplachové systémy – Poplachové přenosové systémy a zařízení.
- ČSN EN 54-1 až 7 – Elektrická požární signalizace.
- ČSN EN 54-10 až 25 – Elektrická požární signalizace.
- ČSN EN 50398-1 – Poplachové systémy – Kombinované a integrované poplachové systémy – Část 1: Obecné požadavky.
- ČSN EN 62676-1-1 – Dohledové video systémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně.
- ČSN EN 60839-11-1 – Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty.
- ČSN EN 50133-1; 2; 7 – Systémy kontroly vstupu pro použití v bezpečnostních aplikacích
- ČSN EN 1627 – Dveře, okna, lehké obvodové pláště, mříže a okenice – Odolnost proti vloupání – Požadavky a klasifikace.

2 ZPŮSOBY ZABEZPEČENÍ OBCHODNĚ VÝROBNÍCH PODNIKŮ

Již v dávné historii se naši předkové zabývali ochranou a zabezpečením svých obydlí před napadením zvířaty nebo protivníky. Mezi první způsoby zabezpečení byly našimi předky budovány ohrady a vznikala první hradiště. V době nedávno minulé si většina podniků vystačila s visacím zámkem na bráně, standardní zámkovou dveřní vložkou, případně s mřížemi na oknech a vstupních dveřích.

Dnešní technologie dovolují použít nespočet systémů, které umožňují zvýšit úroveň zabezpečení objektu. Na trhu bezpečnostních technologií je možno vybrat z mnoha profesionálních firem, které nabízí poradenství a realizaci zabezpečení objektů různými typy a úrovněmi systémů. Nabídka těchto systémů je stále širší i finančně dostupnější než před několika lety.

Ve stručnosti stojí za zmínku vyjmenovat několik způsobů zabezpečení objektů:

- mechanické zábranné systémy (dále jen „MZS“),
- poplachové zabezpečovací a tísňové systémy (dále jen „PZTS“),
- elektrické požární systémy (dále jen „EPS“),
- uzavřený televizní okruh (dále jen „CCTV“),
- systém kontroly vstupu (dále jen „ACS“),
- pult centrální ochrany („dále jen PCO“).

Bezpečnostní systém představuje nástroj pro zajištění bezpečnosti daného prostředí v požadovaném čase a pro stanovený účel. [3]
Bezpečnostní systém má především plnit následující role:

- preventivní – který se zaměřuje na předcházení vzniku nebezpečných událostí,
- pohotovostní – zajištění stálé připravenosti k řešení krizového systému (dále jen „KS“),
- informační – zajištění včasných informací o vzniku KS,
- reakce na vzniklé KS – schopnost řešit vzniklé situace včas a efektivně. [3]

Spousta společností spoléhá na technologické zabezpečení budov a mnohdy pomíjí fyzickou ostrahu, která celému zabezpečení dává přidanou hodnotu. Nejlepším zabezpečením je prevence, což znamená pravidelné školení zaměstnanců, správců systémů, ale i pravidelné prohlídky, revize a testování všech systémů.

Úroveň zabezpečení je odvislá od:

- technické vyspělosti objednatele,
- zvoleného systému,
- profesionality zhotovitele,
- zkušeností zhotovitele,
- úrovně nastavení,
- dodržování pravidel zaměstnanci,
- pravidelné údržbě,
- rychlosti zásahu v případě narušení. [3]

2.1 Fyzické zabezpečení objektu obchodně výrobní společnosti

Fyzické zabezpečení objektu obchodně výrobní společnosti je možno chápat jako zabezpečení nestátní organizace fungující na komerčním principu. Provozovat fyzické zabezpečení objektu může pouze osoba vlastnící licenci pro provozování Soukromé bezpečnostní služby (dále jen „SBS“), kterou vydává Ministerstvo vnitra. Všichni provozovatelé SBS jsou povinni každoročně Ministerstvu vnitra předkládat zprávu o provozu za uplynulý kalendářní rok, nebo aktuálního období, pokud své působení v toto roce započal nebo ukončil. [4] Výkon činnosti SBS spočívá:

- v projektování,
- organizování,
- řízení,
- kontrole,
- výkonu ochrany,
- strážní služby,
- převozu finančních hotovostí,
- realizaci výjezdových skupin. [4]

Soukromé bezpečnostní služby sehrávají důležitou roli při ochraně majetku a osob, protože na rozdíl od technických způsobů ochrany zabezpečení mohou případné nebezpečí odvrátit. Technická ochrana takové jevy pouze detekuje nebo o jejich vzniku informuje. Pracovníci SBS nikdy nesmí zneužít své pozice. Nesmí zkoumat, hledat nebo se zajímat o náboženské přesvědčení, o rasový původ, politické přesvědčení, zdravotní stav či sexuální orientaci osob. Jejich provoz musí být v souladu s právními předpisy a zákony České republiky. [4]

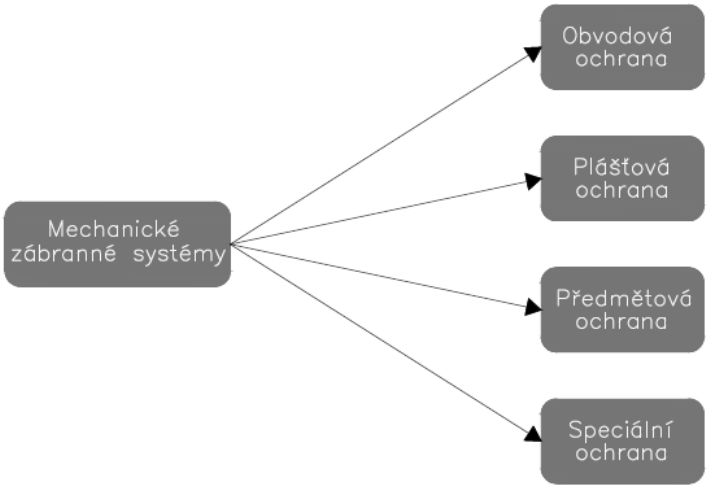
Fyzická ochrana je činnost vedoucí k zabránění trestné a protiprávní činnosti zajišťované soukromou bezpečnostní službou pomocí osoby pověřené ochranou a ostrahou osob a majetku. Při jejím provádění musí být dodrženy všechny právní normy.

Fyzická ochrana zahrnuje:

- kontrolu vjezdu a výjezdu vozidel, kontrola nákladu a příslušných dokladů,
- udržování pořádku,
- kontrolu prostorů,
- kontrolu osob při vstupu nebo odchodu, kontrolu jejich dokladů a zavazadel,
- odebrání věci, která byla ukradena nebo je na toto podezření,
- hlášení nehod. [3]

2.2 Mechanické zábranné systémy

Mechanické zábranné systémy jsou pokládány za primární složku ochrany osob a objektů [5]. Do této kategorie spadají všechny mechanické prvky, které komplikují nebo znesnadňují neoprávněné proniknutí do chráněného prostoru přes oplocení, dveře, okna nebo manipulaci se střeženými předměty v chráněném prostoru. Mechanické zábranné systémy dodávají ochranu svou mechanickou pevností, která je dána průlomovou odolností, již musí pachatel při pokusu o vniknutí do střeženého prostoru překonat a mnohdy je tato doba pro agresora neúnosná. Rozdělení MZS je zobrazeno na obr. 1. [6]



Obrázek 1 - Rozdělení mechanických zábranných systémů [6]

2.2.1 Obvodová ochrana

Obvodovou ochranu tvoří prostředky, které vytvářejí hranici a oddělují chráněný objekt od ostatních pozemků. Fyzickou hranici mohou tvořit umělé bariéry, jako například různé druhy oplocení, zdiva, kombinací zdiva a oplocení, nebo přírodní bariéry.

Rozdělení obvodové ochrany:

- drátěné oplocení,
- bezpečnostní oplocení,
- vysoko bezpečnostní oplocení,
- vrcholové zábrany,
- podhrabové překážky,
- vstupy a vjezdy. [6]

Vstupy a vjezdy patří do skupiny obvodové ochrany, které zvyšují bezpečnost objektu a zabraňují volnému proniknutí do prostoru chráněného objektu. Jsou hranicí mezi kontrolovaným a volným prostorem. Za nejvhodnější je považováno mít co nejmenší počet vstupů a vjezdů, čímž je sníženo riziko pokusů o neoprávněný vstup.

Rozdělení dle použití:

- pro osoby,
- pro dopravní prostředky.

Způsob zabezpečení vstupů:

- brankou,
- turniketem,
- bezpečnostní propustí.

Způsob zabezpečení vjezdů:

- brány,
  - posuvné,
  - otočné.
- závory. [6]

Závory slouží jako vhodný doplněk vjezdu nebo výjezdu z podniku, když jsou otevřeny brány. V tomto případě závory plní kontrolní funkci.

Turniket je zařízení, které by mělo zabránit vstupu neoprávněné osoby, nebo umožnit průchod pouze jedné osoby do chráněného objektu. Turnikety je možné napojit na PZTS, kdy při vyhlášení poplachu se turnikety zablokují, nebo na EPS, kdy se turnikety odblokují a jsou volně průchozí. Napájení lze zálohovat pomocí záložních akumulátorů nebo dieselagregátu. Turnikety umožňují škálu nastavení, např. úroveň zabezpečení, rychlost otvírání a zavírání křídel, emergenci atd. Turnikety nabízí široké pole uplatnění a jejich využití je možné např. v oplocení objektu, na vstupu do budovy, vstupy sportovních areálů atd.

Základní rozdělení turniketů:

- trnové,
  - tripodové,
  - jednoramenné.
- křídlové,
  - otočné,
  - posuvné.
- branky,
- plno profilové (obr. 2),
- rotační. [7]

Obrázek 2 - Turniket plno profilový – Rexon Dea 3 [8]

2.2.2 Plášťová ochrana

Do plášťové ochrany jsou zařazeny všechny konstrukce, které oddělují interiér budovy od exteriéru. Plášť objektu tvoří stěny, stropy, střechy, okna, dveře a vrata. Konstrukce, která tvoří plášťovou ochranu musí splňovat řadu požadavků, tak, aby odolávala vnitřním i vnějším vlivům prostředí a současně byla zachována správná funkce objektu. [6]

Základní otvorovou výplní je okno, které plní funkci přirozeného osvětlení a větrání. Okna se liší dle použitého materiálu při výrobě. Zabezpečení okenních otvorů ovlivňují faktory jako rám, křídlo, kování, sklo, případně fólie na skla, rolety a mříže. V současné době se používají bezpečnostní fólie na skleněné výplně oken. Tento typ zabezpečení oken je ekonomicky méně nákladný a designově přijatelnější než mříže. [9]

2.2.3 Předmětová ochrana

Předmětovou ochranu je možno chápat jako zabezpečení a ochranu míst a předmětů, kde jsou uschovány různé cennosti, jako například finanční hotovost, know-how podniku, utajované informace atd., před neoprávněným nakládáním. [10]

2.3 Režimová ochrana

V praxi se lze setkat taktéž s označením organizační nebo administrativní ochrana. Je to administrativně organizační uspořádání vztahů mezi pracovníky, jejich činnostmi a procesy se dosahuje optimálního stavu v daném podniku. Současně řeší, jakým způsobem budou pracovníci postupovat při ochraně podniku, a to v souladu se zákony a jeho potřebami.

Režimová ochrana se týká:

- činnosti pracovníků uvnitř podniku (zaměstnanci),
- pohybu a chování návštěv,
- výstupu dat a informací vně podniku. [3]

Rozdělení režimové ochrany:

- vstupní a výstupní režim osob – kontrola vstupu zaměstnanců a návštěv do podniku,
- vstupní a výstupní režim dopravních prostředků – kontrola vozidel při vjezdu i odjezdu z objektu, kontrola vyvážených předmětů a materiálů,
- pohyb zaměstnanců uvnitř podniku – určení části podniku s omezeným přístupem;

- provozní režim – zajištění plynulosti a bezpečnosti provozu,
- materiálový a expediční režim – postup při příjmu, výdeji a skladování materiálu,
- klíčový režim – stanoví postup při půjčování, označování, přidělování klíčků nebo výměně zámků. [11]

2.4 Technická ochrana

Technická ochrana se skládá z detekčních systémů, které vyhodnocují a předávají data o chráněném zájmu (objektu). Technická ochrana je účinným doplňkem klasické ochrany. [9]

2.4.1 Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací a tísňové systémy sestávají z poplachových zabezpečovacích systémů (dále jen „PZS“) pro detekci a signalizaci narušení chráněného objektu a poplachových tísňových systémů (dále jen „PTS“) pro případ nouze jako např. napadení, únik plynu atd. Dříve byly tyto systémy známé jako EZS nebo elektrické zabezpečovací a tísňové systémy. Poplachové zabezpečovací a tísňové systémy (dále jen „PZTS“) jsou v současné době považovány za nejspolehlivější ochranu, a to z hlediska možného překonání narušitelem. [10]

Primárním účelem PZTS je ochrana proti fyzickému narušení střeženého prostoru. Bývá rovněž často využívána k detekci kouře, úniku plynů či sledování hladiny vody proti zaplavení kotelen průmyslových nebo soukromých prostorů. [10]

Poplachové zabezpečovací a tísňové systémy je možné rozdělit na klasické prvky PZTS propojené kabeláží pro napájení jednotlivých prvků a přenos informací, bezdrátové a kombinované. [10]

Charakteristika systému klasického systému PZTS:

- jsou cenově dostupnější,
- nejsou závislé na bateriích.

Charakteristika bezdrátového systému PZTS:

- snadná a rychlá montáž i demontáž,
- snadná rozšiřitelnost systému,
- nevýhodou je omezení vzdálenosti dosahu ústředna – snímač,

- napájení bateriemi – systém automaticky upozorní uživatele na pokles napětí pod danou úroveň prostřednictvím GSM nebo emailu.

Každý systém PZTS je složen z následujících prvků:

- detektory:
  - pohybu – čidla PIR,
  - rozbití skla – tříštivé detektory,
  - magnetické kontakty,
  - otřesu,
  - antimasking,
  - plynu,
  - zaplavení,
  - kouře,
- ústředny:
  - smyčkové,
  - adresné,
  - smíšené,
  - bezdrátové,
- signalizační zařízení:
  - akustická,
  - optická,
  - smíšená,
- ovládací zařízení:
  - kódová klávesnice,
  - dálkový ovladač,
  - RFID,
- napájecí zařízení,
- kabelové rozvody. [9]

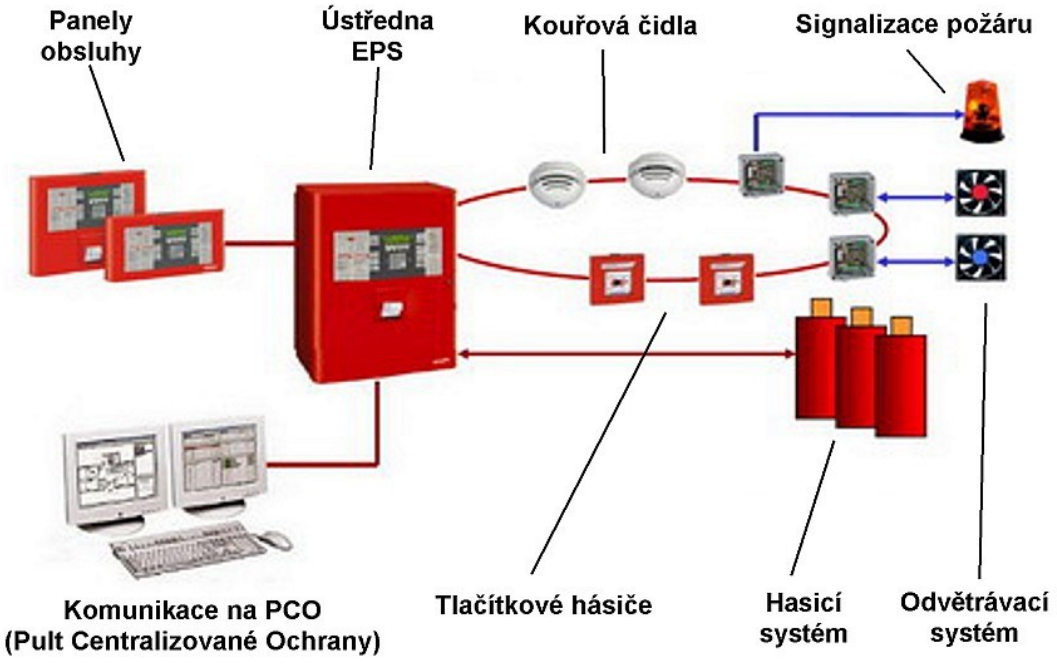
2.4.2 Elektrická požární signalizace

Elektrická požární signalizace je systém pro včasnou detekci zárodku požáru, jeho lokalizaci a spuštění odpovídajících zařízení, která jsou součástí systému protipožárních bezpečnostních opatření (obr. 3). Nasazením systému EPS je tak možné zabránit prvořadě újmě

lidských životů, finančních a materiálových ztrát. Škody vzniklé požárem jsou vždy výrazně vyšší, než náklady související s pořízením EPS a jeho provozem. [9]

Jednotlivé prvky systému EPS:

- ústředna,
- obslužný panel,
- požární hlásiče:
  - tlačítkové hlásiče,
  - autonomní,
  - samočinné hlásiče,
- signalizační poplachové zařízení:
  - akustické (sirény),
  - optické (majáky),
- napájecí zdroje. [10]



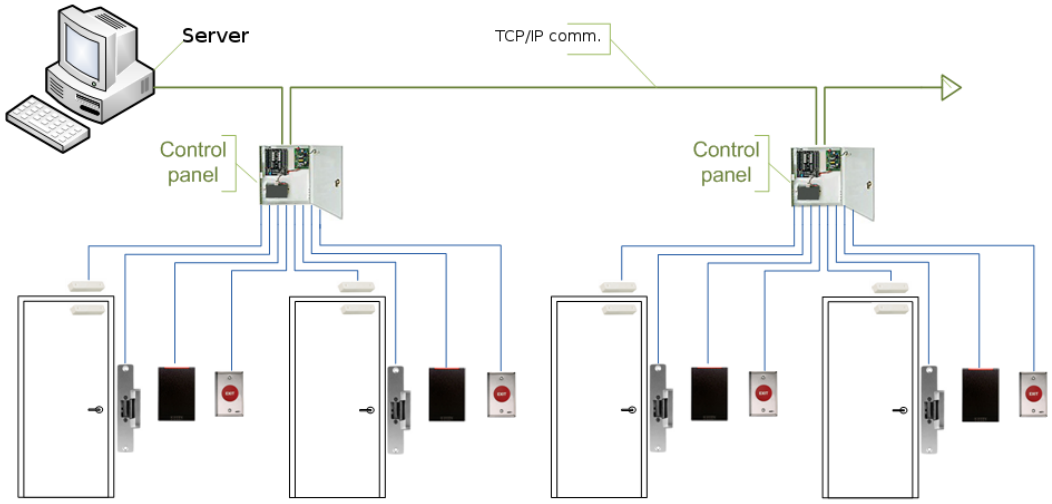
Obrázek 3 - Systém elektrické požární signalizace [12]

2.4.3 Systém kontroly vstupu – Access control systém

Systém kontroly vstupu je systém opatření, který vede k zajištění řízení kontroly a evidence vstupu osob do prostor objektu na základě vyhodnocení a následné identifikace. Jedná se

především o povolení nebo zabránění vstupu osob do zabezpečených prostor, které mohou být definovány do různých zón a systém současně umožňuje sledování pohybu v jednotlivých zónách. [5] Zároveň lze definovat funkci antipassback, což je zabránění opakovaného průchodu. [12] Blokové schéma systému kontroly vstupu je zobrazeno na obrázku 4.

Systém kontroly vstupu může být nastaven různými parametry tak, že umožňuje omezit vstup do chráněných prostor pouze v určitém časovém úseku, dané skupině osob nebo jiným subjektům s vlastní identifikační kartou nebo vědomostí vstupního kódu. Systém kontroly vstupu se nevztahuje jenom na přicházející osoby, ale také na projíždějící automobily.



Obrázek 4 - Schéma systému kontroly vstupu [13]

ACC systém se skládá z:

- RFID snímačů (obr. 5),
- Identifikačních prvků – karty, čipy,
- převodníků,
- programového vybavení,
- napájecích zdrojů,
- ovládacích prvků:
  - turnikety,
  - elektrické zámky,
  - závory,
- řídících jednotek. [14]

Přístupový systém je vždy vhodné doplnit o turnikety, které zvýší úroveň zabezpečení.

Obrázek 5 - Čtečka ID karet [15]

2.4.4 Uzavřený televizní okruh

Nejčastěji se v praxi lze setkat se zkratkou CCTV (Closed Circuit Television), neboli uzavřený televizní okruh, zjednodušeně řečeno kamerový systém. [16]

Využívá libovolný počet monitorovacích zařízení v uzavřeném televizním okruhu. Mezi výhody CCTV patří především pokrytí i velmi rozsáhlých střežených prostorů v on-line režimu. Sytém umožňuje pořizovat záznamy v závislosti na kapacitě úložiště. Záznamy pořízené prostřednictvím CCTV lze zpětně zobrazit a využít k provedení případné analýzy. [17]

Skladba kamerového systému:

- záznamové zařízení,
- kamery:
  - PZT,
  - statické,
  - statické DOME,
  - digitální IP,
  - analogové,
- objektivy,
- zobrazovací zařízení. [16]

V současné době jsou nejpoužívanější IP kamery, které využívají strukturované kabeláže počítačových sítí, což umožňuje přenášet obraz kvalitněji a rychleji. Jednotlivé kamery lze

jednoduše nastavovat a ovládat přes internet. Napájení kamer lze realizovat zdrojem nebo pomocí PoE. V případech, kdy není možné realizovat kabelové rozvody, lze použít bezdrátových kamer. Podmínkou pro použití bezdrátových kamer je viditelnost mezi přijímačem a vysílačem signálu.

Zařazení systému CCTV bývá stanoveno dle úrovně rizika a na základě toho jsou na systém kladeny funkční požadavky. Jako jsou např.:

- ukládání dat,
- archivace a zálohování dat,
- záznam událostí (poplach, výpadek napájení, změna konfigurace atd.),
- monitorování přepojení (ověřování spojení atd.),
- detekce sabotáže (ztráta signálu, změna pozice kamery atd.),
- přístupové úrovně (aktualizace systému, přiřazení oprávnění atd.),
- přístup k datům (on-line, uložená data, mazání atd.),
- identifikace dat (lokalita, zdroj obrazu, datum, čas atd.). [12]

Součástí kamerového systému mohou být kamery pro rozpoznávání registračních značek automobilů, kdy ideální stav je propojení s přístupovým systémem.

3 CÍLE A METODY POUŽITÉ PRÁCE

Hlavním cílem a myšlenkou této práce bude posouzení současného zabezpečení a ochrany objektu obchodně výrobního podniku. Použitím vhodných metod bude kladen zřetel a důraz na nalezení slabých míst a možných hrozeb z hlediska zabezpečení areálu a majetku soukromé společnosti.

3.1 Jednotlivé cíle práce

Jednotlivé cíle zabezpečení a ochrany obchodně výrobního podniku:

- vypracování teoretické části na téma zabezpečení a ochrana objektů z dostupné literatury,
- zmapování a popis současného zabezpečení a ochrany podniku,
- posouzení rizik zabezpečení a ochrany podniku metodami analýzy rizik,
- zhodnocení současného stavu a navržení nápravných opatření, která povedou ke zvýšení úrovně zabezpečení podniku.

V teoretické části budou popsány teoretické možnosti a souvislosti spjaté se zabezpečením osob, objektů a majetku, které jsou vystaveny možným hrozbám a rizikům, jež mohou být způsobeny vědomou či nevědomou činností zaměstnanců podniku, případně cizí osobou. Přestože v historii podniku nedošlo k žádným nežádoucím incidentům, lze považovat současný stav zabezpečení za nedostatečný.

3.2 Metody použité v práci

Současná technologicky vyspělá doba nabízí nepřeberné množství bezpečnostních mechanických a elektronických prvků, které slouží k zabezpečení objektů. K odhalení možných hrozeb a rizik jsem použil následující metody:

- Analýza rizik:
  - Ishikawa diagram,
  - PNH metoda.
- SWOT analýza strategického plánování,
- Pozorováním – aplikace metody pozorováním byla provedena napříč všemi systémy zabezpečení např. při vjezdu automobilů do areálu, při vstupu zaměstnanců, při obhlídce PZTS, atd.

- Syntéza – metodu syntézy jsem aplikoval při sdružení mnoha informací do jednoho bloku, např. při vyhledání informací v odborné literatuře a následném zpracování do souvislosti.

II. PRAKTICKÁ ČÁST

4 POSOUZENÍ SOUČASNÉHO ZABEZPEČENÍ OBJEKTU OBCHODNĚ VÝROBNÍHO PODNIKU XY

V práci je posuzován reálný objekt. Z bezpečnostních důvodů nelze uvést přesnou lokalizaci a specifikaci řešeného podniku.

4.1 Zmapování objektu a jeho popis

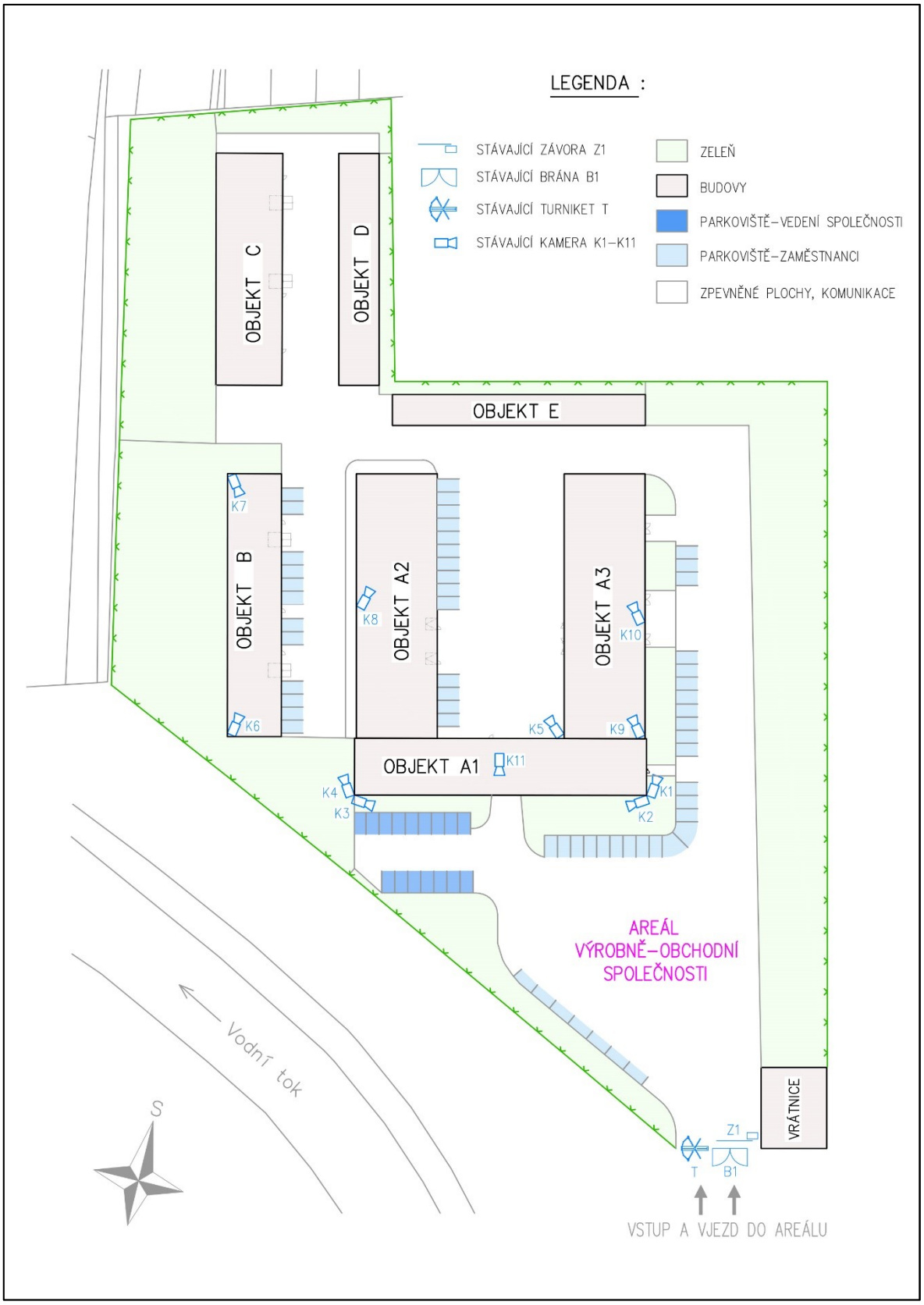
Posuzovaný objekt je situován v zastavěné oblasti, a tak jsou jeho hranice ze severní a východní strany obklopeny soukromými stavebními parcelami. Z jižní strany objekt lemuje místní vodní tok. Ze západní strany objekt sousedí s cyklostezkou a zemědělskou půdou. Celková rozloha objektu dosahuje 18 300 m². Objekty jsou pro orientaci popsány písmeny římské abecedy. Budova označena písmenem A1 je jako jediná dvoupodlažní. V druhém patře budovy sídlí vedení společnosti, oddělení obchodu a vývoje SW. V přízemí budovy se nachází středisko podpory zákazníka, ekonomické oddělení, jídelna a sociální zařízení.

Sklad strojní výroby je v současné době situován v budově A3. Písmenem A2 jsou označeny prostory náležící elektro výrobě a jejím skladovým prostorům. V halách B a C se nachází strojní výroba, kde se kompletují jednotlivé produkty portfolia společnosti. Nově postavené budovy D a E jsou určeny ke skladování finálních výrobků. Jedná se o studený sklad.

Všechny budovy jsou vybaveny PZTS, této problematice bude podrobněji věnována samostatná kapitola 4.6.1.

Hranici areálu podniku tvoří oplocení, které je součástí obvodové ochrany a tomuto tématu se bude více věnováno v samostatné kapitole 4.2.

Pro lepší orientaci jednotlivých objektů byla vytvořena mapka (obr. 6) se zakreslením hranice pozemku, vstupu a vjezdu do areálu a jednotlivých objektů. Výsledný obrázek zobrazuje podobu celého areálu s hranicí pozemku, označenými budovami, umístěním jednotlivých kamer CCTV a oplocení. Pro jednodušší orientaci je vytvořena legenda s vysvětlivkami.



Obrázek 6 - Situační mapa podniku s legendou [vlastní]

4.2 Obvodová ochrana

Oplocení areálu je realizováno po celém obvodu areálu společnosti. V západní části areálu je oplocení tvořeno z klasického pletiva výšky 2 m s ocelovými sloupky, které jsou osazeny v betonových soškách (obr. 7). Toto oplocení nese stopy opotřebení a jeho výměna z důvodu zvýšení zabezpečení areálu společnosti je nezbytná.

Obrázek 7 - Stávající drátěné oplocení [vlastní]

Zbývající oplocení (obr. 8) je realizováno z trapézového plechu výšky 2 m. Je osazeno na ocelové konstrukci z čtvercového profilu 60 x 60 mm. Na tuto ocelovou konstrukci je osazena kulatina 10 mm, která tvoří konstrukci pro dvě řady ostnatého drátu. Pod ocelovou konstrukcí plotu je betonový základ šíře 30 cm, který lze považovat za podhrabovou zábranu. Na oplocení není instalováno žádné elektrické zabezpečovací zařízení.

Vjezd do areálu je zabezpečen ocelovou bránou a závorami, které jsou ovládány pomocí systému ACS, podrobněji se tomuto tématu věnuji v kapitole 4.6.3.

Areál není v současné době hlídán SBS.

Obrázek 8 - Stávající oplocení [vlastní]

4.3 Plášťová ochrana

Objekty A1, A2, A3 jsou stavebně propojeny a jejich konstrukce je tradičního zděného charakteru. Objekty B, C, D, E jsou samostatně stojící budovy ocelové konstrukce. Plášťová ochrana objektu je tvořena:

- Stavebními prvky – jak již bylo uvedeno, obvodové a nosné konstrukce u objektů A1, A2, A3 jsou stavebně propojeny a jejich konstrukce je betonovo-cihlového charakteru. Vnitřní příčky jsou zhotoveny suchou výstavbou ze sádrokartonových desek. Střecha objektů je rovná, opatřenou atikou, izolace střechy je realizována produktem Fatrafol. Objekty B, C, D, E jsou samostatně stojící budovy ocelové konstrukce se sendvičovým opláštěním. Střecha je zhotovena z ocelové konstrukce a vlnitého plechu.
- Otvorovými výplněmi – administrativní budova je osazena hliníkovými okny, ostatní budovy jsou osazeny standardními plastovými okny. Dveře jsou v kancelářských prostorech vždy jednokřídlé. Zárubně jsou obložkové a křídlo dveří je standardní v prostřední části prosklené. Zámkové vložky jsou FAB. Vchod do administrativní budovy je možný přes Automatické lineární dveře s prosklenou výplní. Boční vstupy do hlavní budovy a vstupy do ostatních budov jsou opatřeny plastovými dveřmi. Do sociálních místností jako např. WC nebo šatna jsou osazené jednokřídlé plno profilové dveře osazené do ocelové zárubně. Pro nakládání a vykládání materiálů jsou osazena rolovací vrata. Haly sloužící pro skladování finálních produktů mají vždy pouze jeden vstup.

4.4 Předmětová ochrana

Předmětovou ochranu je možno chápat jako zabezpečení a ochranu míst a předmětů, kde jsou uschovány různé cennosti, jako například finanční hotovost, know-how podniku, utajované informace atd., před neoprávněným nakládáním. [10]

4.5 Režimová ochrana

Režimová ochrana je soubor opatření, která vedou k optimalizaci procesů daného podniku. Jedním z mnoha odvětví režimové ochrany je klíčový režim, kterému se věnuji v následující kapitole. [18]

Ve společnosti je zaveden postup pro nakládání s klíči, který je zdokumentován v interní směrnici. Tato směrnice přímo určuje:

- odpovědnost za jednotlivé klíče,
- kde jsou klíče uloženy,
- kdo může klíče kopírovat,
- jak se mohou klíče půjčovat,
- postup výměny zámků.

U správce budov je instalována prosklená skříň, ve které jsou uloženy všechny klíče a sešit, kde se zapisují zápůjčky jednotlivých klíčů, jež jsou označeny visačkou s číslem dveří. Součástí zápisu je datum vypůjčení, jméno a příjmení pracovníka, podpis a datum vrácení klíče.

4.6 Technická ochrana

Technická ochrana je monitorování objektů či areálů za pomoci automatických technických prostředků. Technická ochrana zajišťuje vyšší efektivitu jiných druhů ochrany. [10]

4.6.1 Poplachový zabezpečovací a tísňový systém

Podnik má sjednanou smlouvu s SBS, která v případě narušení objektu a vyhlášení poplachu:

- kontaktuje pověřeného pracovníka podniku,
- vyjíždí k zásahu,
- provádí kontrolu objektu.

Všechny budovy areálu jsou zabezpečeny systémem PZTS, kde jsou v jednotlivých místnostech, halách a skladech umístěna čidla PIR. Proti vniknutí rozbitím okenní výplně jsou instalovány detektory rozbití skla. Součástí PZTS jsou kouřové detektory. Na opláštění budov jsou umístěny opticko-akustické sirény. Rolovací vrata jsou opatřena magnetickými kontakty. Na obrázku 9 je zobrazeno kouřové čidlo, čidlo rozbití skla a PIR detektor.

Obrázek 9 - Kouřové čidlo, rozbití skla a PIR detektor [vlastní]

Při obhlídce areálu a jednotlivých budov bylo zjištěno, že v místnostech 005, 032, 017, 303, byla čidla demontována, ale již nebyla vrácena či nahrazena. V těchto místech v současné době vyčnívají pouze kabely ze zdi (obr. 10).

Obrázek 10 - Demontované čidlo PZTS [vlastní]

4.6.2 Elektrická požární signalizace

Systém EPS není v Areálu podniku realizován. V době kolaudace hlavního areálu a následně dalších skladovacích budov nebyl systém EPS orgány statní správy vyžadován. Případný vznik požáru detekují snímače kouře, napojené na systém PZTS. V celém areálu jsou rozmístěny prvky požární ochrany, jako např. hasící přístroje, které prochází pravidelnou revizní kontrolou, o které je vyhotoven protokol.

4.6.3 Systém kontroly vstupu

Vstup do objektu je zabezpečen plno-profilovým turniketem, který je doplněn čtečkou přístupového systému. Osobám bez přístupové RFID karty není vstup do objektu umožněn. Návštěvy se musí hlásit pomocí zvonku interkomu, který danou osobu přesměruje na sekretariát, odkud může být tlačítkem umožněn vstup.

Vjezd do objektu je opatřen bránou ocelové konstrukce a závorou ve směru vjezdu i výjezdu.

Systém vjezdu je řízen přístupovým systémem ve dvou časových zónách. V pracovní době jsou v provozu závory a brána je deaktivována. Mimo pracovní dobu jsou deaktivovány závory, ráhna jsou zdvižena a aktivní je brána.

Vjezd do objektu je možný pomocí:

- snímače přístupového systému,
- dálkovým ovladačem, kterým disponuje pouze management podniku,
- GSM bránou.

V oplocení areálu společnosti je umístěn turniket pro přicházející osoby, které přiloží čipovou kartu na čtečku umístěnou na těle turniketu. Číslo karty je obratem vyhodnoceno serverem a v rozmezí necelé vteřiny je osobě povolen vstup do objektu. Tímto způsobem je provedena elektronická kontrola oprávněného vstupu. V případě neoprávněného vstupu (např. mimo povolený čas) se na čtečce rozsvítí červená kontrolka a systém odmítne vpustit pracovníka do objektu.

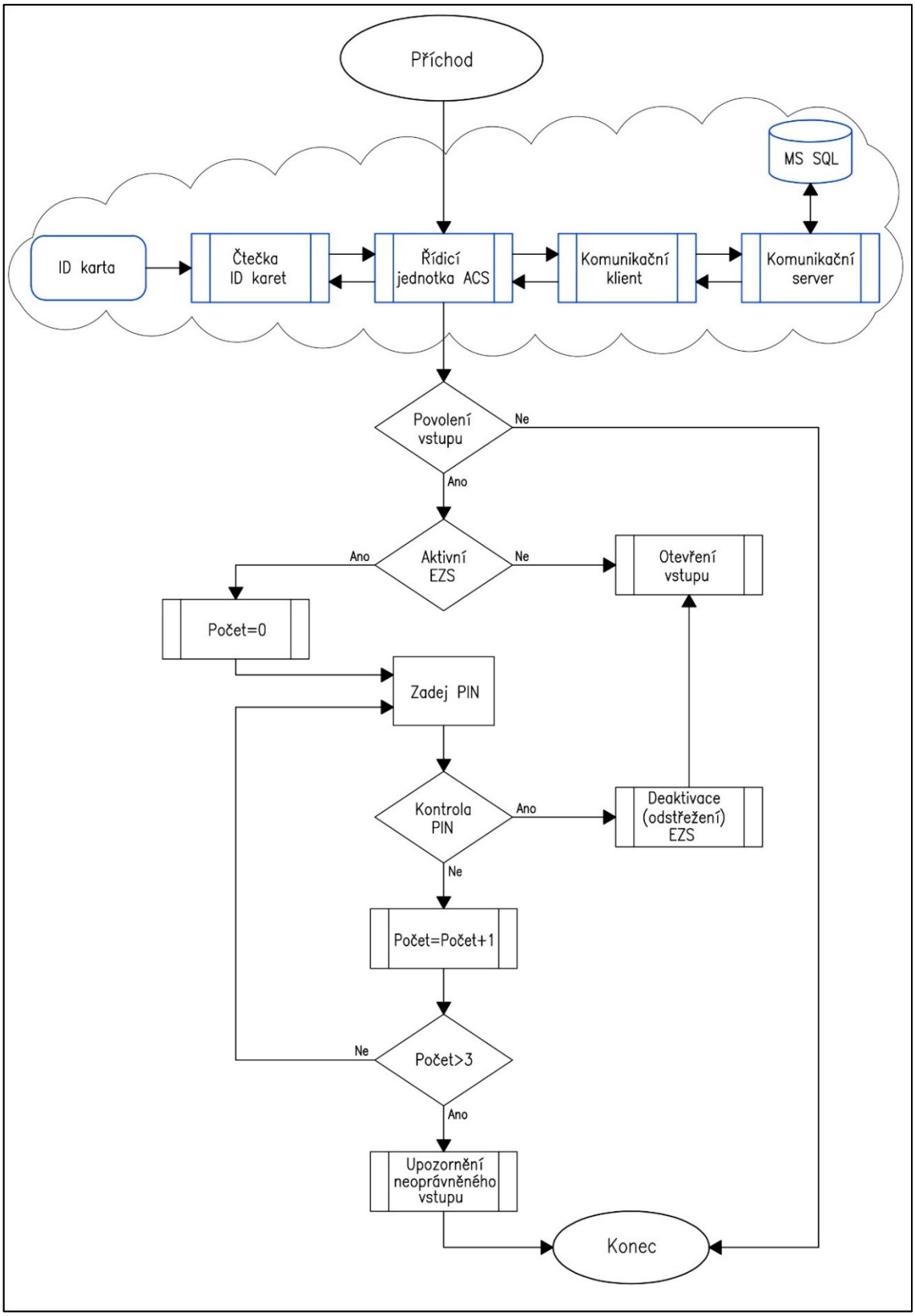
Do podniku lze vjet i automobilem, v tomto případě musí dotyčná osoba zastavit automobil před závorou nebo bránou. Po přiloží karty ke RFID snímači umístěného ve sloupku u vozovky je vjezd povolen nebo odmítnut.

Dalším krokem, který musí osoba provést, je přístup do konkrétní budovy v areálu. Pracovník opět přiloží čipovou kartu k RFID čtečce, která je umístěna u vstupních dveřích objektu, následně probíhá vyhodnocení oprávnění vstupu. Pracovník vchází do objektu, je-li objekt zastřežen, systém po zadání kódu automaticky odstřeží jednotlivé úseky budovy, dle přiděleného oprávnění. Na obrázku 11 je znázorněn rozhodovací diagram vstupu zaměstnance do podniku. Při přiložení karty k RFID snímači je nutné zadání PIN kódu. Oprávnění vstupu kanceláří budov je nastaveno v pracovní dobu pro všechny karty definované v systému. V mimopracovní dobu je oprávnění nastaveno pouze pro pracovníky dané kanceláře nebo místnosti.

Stěžejní vlastnosti systému ACS:

- definování oprávnění jednotlivých ID karet,
- kontrola vícenásobných vstupů (tzv. antipassback),
- zpřístupnění aktuálních stavů systému:
  - kde se karta nachází,
  - stav zařízení,
  - signalizace alarmových stavů,
- kontrola otevření dveří, v případě překročení nastaveného timeoutu je zaslána alarmová hláška,
- integrovaná definice výtahových snímačů s definicí pater,
- definice pater výtahových snímačů,
- vzdálená správa snímačů,
- režim dvou karet,
- definice typů karet,
- uživatelsky přívětivé přidělování přístupových práv,
- předdefinované šablony přístupových práv,
- ovládání PZTS snímači identifikačních karet,
- návaznost na systém EPS. [17]

Další možností vjezdu do podniku dopravním prostředkem je použití mobilního telefonu, kdy prostřednictvím GSM brány je závora nebo brána ovládána. Podmínkou použití otevření závory či brány pomocí GSM je znalost telefonního čísla.



Obrázek 11 - Diagram ACS při vstupu zaměstnance do společnosti [vlastní]

4.6.4 Uzavřený televizní okruh objektu

Je soubor technických prostředků umožňující pořizování a uchovávání obrazového záznamu sledovaných míst. Společnost má kamerový systém nahlášený u Úřadu pro ochranu osobních údajů (dále jen „ÚOOÚ“), který přesně stanovuje podmínky pro provoz CCTV, včetně lhůty uchovávání záznamu, která byla stanovena na dobu na tří dnů.

Kamerový systém je v současné době tvořen 11 kamerami, 6 kamer je umístěno v interiéru budov a 5 kamer je umístěno na vnějším opláštění budov. Všechny monitorované prostory jsou označeny nálepkou. Ve všech případech je využito analogové či IP rozhraní. Rozmístění kamer je znázorněno na přiloženém situační výkrese (obr. 6). Soupis jednotlivých kamer je následující:

- Kamera 1–5 - kamery jsou umístěny na vnějším plášti budovy a snímají hlavní vstup do budovy, boční vstup do budovy (obr. 14), zadní nádvoří budovy A3 a A2, nádvoří mezi budovami A2 a B. Jedná se o typ kamer IP Zavio. Výřez snímaného obrazu je zobrazen na obr. 12 a 13.

Obrázek 12 - Kamera 5 výřez pohledu [vlastní]

Obrázek 13 - Kamera 4 výřez pohledu [vlastní]

- Kamera 6–7 - kamery jsou umístěny v hale B, kde snímají prostor montáže sériové výroby produktů společnosti a expedice. Typ kamer IP Vivotek.
- Kamera 8 - kamera je instalována v hale A2, kde jsou snímány prostory zakázkové výroby montáže. Typ kamery IP Vivotek.
- Kamera 9–10 - kamery jsou umístěny v prostoru dílny a skladu na hale A3, kdy snímají prostor výroby obalů a prostor skladových zásob. Typ kamery IP Vivotek.
- Kamera 11 - umístění kamery je v hlavním vstupu budovy A1, kdy je snímán prostor centrálního vstupu. Typ kamery: analogová kamera KTN&C + převodník.

Výřez umístění kamer na plášti budovy je znázorněn na obrázku 14.

Obrázek 14 - Umístění kamer 1 a 2 [vlastní]

Přenos dat probíhá prostřednictvím IP sítě strukturované kabeláže. Síť pro provoz CCTV je fyzicky oddělena, je tedy pro tuto potřebu vybudována samostatná síť. Na CCTV síť je napojeno DVR, kde jsou uchovávány záznamy. Přístup do úložiště nebo online přenosu kamer je prostřednictvím webové aplikace, která je chráněná uživatelským jménem a heslem. Úložiště dat je umístěno v serverovně podniku, kde je omezený a řízený přístup. Záznamy jsou ukládány po dobu tří dnů. Konfiguraci a zásahy do systému CCTV mohou provádět pouze pověření odpovědní technici střediska správy informačních technologií. Veškeré zásahy do systému jsou vedeny v provozním deníku. Všechny monitorované prostory jsou označeny informační tabulkou. [Interní zdroj podniku]

5 APLIKACE METODY SWOT ANYLÝZY, ISHIKAWA DIAGRAMU A METODY PNH

Jednou z metod, jak posoudit zabezpečení objektu, může být analýza rizik a některé z jejích metod. Analýza rizik je proces pochopení povahy rizika a určení jeho úrovně. Analýza rizika dává podstatu pro hodnocení rizika a následné zacházení sním. Riziko může být přijatelné, kterému není nutné věnovat pozornost a nepřijatelné, které musí být následně ošetřeno. [19]

Vnímání nebezpečí – má vliv na rozhodování a chování lidí, které může být ovlivněno:

- věkem,
- pohlavím,
- zkušenostmi,
- poznáním situace,
- informacemi,
- osobní situací,
- důvěrou.

Tato kapitola se zabývá analýzou stávajícího zabezpečení areálu obchodně výrobního podniku. Aplikace metody pozorováním, byla provedena napříč všemi systémy zabezpečení a zabývám se jí v kapitole 4. Metoda SWOT včetně tabulek, digramu a popisu je zpracována v kapitole 5.1. Vypracování Ishikawa digramu je provedeno v kapitole 5.2. a vyhodnocení metody PNH je v uvedeno v kapitole 5.3.

5.1 Metoda SWOT

Metoda SWOT analýzy je metodou strategie řízení managementu, analyzuje interní prostředí (silné a slabé stránky) a externí prostředí (příležitosti a hrozby). Zkratka SWOT je sestává z prvních písmen slov Strengths, Weaknesses, Opportunities a Threats. [20]

Cílem této analýzy je nalezení silných a slabých stránek, příležitostí a hrozeb podniku. Zhodnocení těchto stránek je uvedeno v tabulkách 1, 2 a grafu 1.

Tabulka 1 – SWOT analýza [vlastní]

Parametr	*Hodnocení*	*Váha*	*Celkem*
Silné stránky			
Kvalifikace zaměstnanců	3	0,1	0,3
Kvalita výrobků HW	2	0,2	0,4
Kamerový systém	4	0,3	1,2
PZTS	5	0,3	1,5
Kvalitní servis	2	0,1	0,2
Celkem		**1**	**3,6**
Slabé stránky			
Slepé místo kamerového systému	-4	0,3	-1,2
Výstupní kontrola produktů	-1	0,1	-0,1
Absence EPS	-2	0,3	-0,6
Absence SBS	-2	0,1	-0,2
Oplocení areálu	-2	0,2	-0,4
Celkem		**1**	**-2,5**
Příležitosti			
Trh v zahraničí USA, Rusko	2	0,1	0,2
Zavedení ostrahy areálu	4	0,3	1,2
Státní zakázky	3	0,3	0,9
Vývoj nových produktů	2	0,1	0,2
QDP – Quick delivery program	3	0,2	0,6
Celkem		**1**	**3,1**
Hrozby			
Konkurence	-1	0,1	-0,1
Vstup cizích osob do objektu podniku	-4	0,2	-0,8
Výpadek napájení el. energií	-2	0,2	-0,4
Krádež	-3	0,3	-0,9
Nedostatek pracovních sil na trhu	-2	0,2	-0,4
Celkem		**1**	**-2,6**

Silné stránky (zjištěné silné stránky společnosti):

- kvalifikace zaměstnanců: zaměstnanci podniku jsou pravidelně školeni jak interními školiteli, tak i externími spolupracovníky, nebo absolvují školení u certifikovaných společností,
- kvalita výrobků HW: kvalita výrobků je díky pravidelným školením pracovníků na vysoké úrovni,
- kamerový systém: v podniku je instalovaný kamerový systém, díky kterému mají odpovědní pracovníci obrazový záznam o aktuálním dění,

- PZTS: v celém podniku jsou rozmístěny prvky PZTS, čidla PIR, tříštivé detektory a senzory detekce kouře,
- kvalitní servis: společnost disponuje servisním střediskem pro rychlou podporu zákazníků.

Slabé stránky (významem určení slabých stránek je upozornit na zjištěné nedokonalosti v zabezpečení podniku):

- slepé místo kamerového systému: v současné době není pokrytí kamerami po celém areálu podniku, nutné doplnění,
- výstupní kontrola produktů: v případě nekvalitní výstupní kontroly budou z podniku expedovány poruchové produkty,
- absence EPS: přestože jsou v areálu podniku instalována kouřová čidla, považuji absenci EPS za slabou stránku podniku, problém shledávám v rychlosti zásahu složek integrovaného záchranného systému,
- absence SBS: do areálu podniku se nelze dostat přes vstupní turniket, avšak v pracovní dobu lze podlézt závoru a další pohyb navštěvujících osob je bez dohledu. Z tohoto důvodu hrozí volný pohyb osob po areálu podniku, případný nekontrolovaný vstup do části podniku, v horším případě hrozí úraz procházející soby,
- oplocení areálu: na západní straně areálu je oplocené nedostatečné a vyžaduje rekonstrukci.

Příležitosti (záměrem příležitostí bylo zjistit možný rozvoj firmy):

- trh v zahraničí: záměr rozšířit prodej produktů do nových oblastí,
- zavedení ostrahy areálu: schopnost zvýšit zabezpečení celého areálu, povědomí o pohybujících se neznámých osobách,
- státní zakázky: společnost má potenciál realizovat více veřejných zakázek,
- vývoj nových produktů: zajistí společnosti náskok na trhu před konkurencí,
- quick delivery program: výroba turniketů na sklad a jejich následná expedice do tří pracovních dnů.

Hrozby (úmyslem je vybrané hrozby identifikovat, rozpoznat a eliminovat):

- konkurence: výstrahou je v současné době konkurence především oblasti cenové politiky, která přichází z východu, a to především z Turecka a Číny,
- vstup cizích osob do podniku: neznámé osoby pohybující se v prostorách podniku, které mohou odcizit různé předměty v majetku společnosti nebo způsobit úraz sobě nebo jiné osobě,

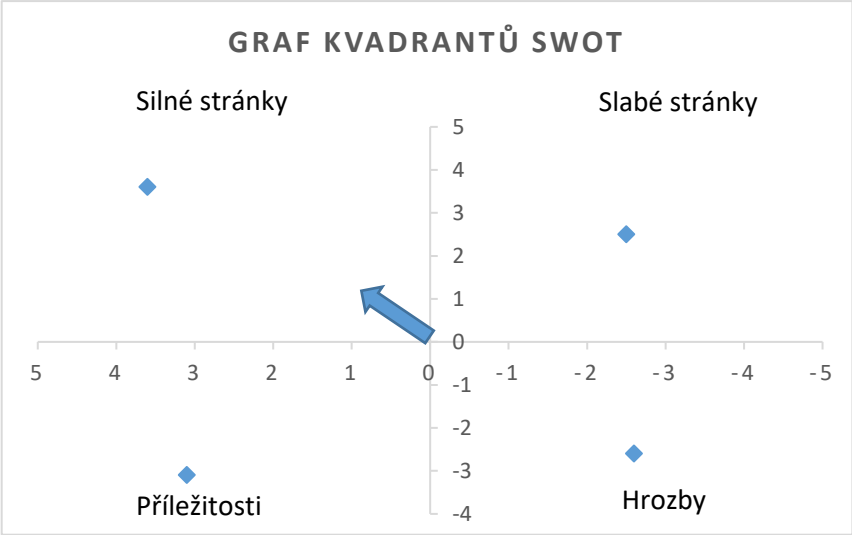
- výpadek napájení el. energie: v podniku jsou zálohované systémy PZTS, ACS, SK samostatnými záložními zdroji nebo lokálnímu UPS, avšak výpadek elektrické energie může ochromit výrobní činnost a tím i dohodnuté termíny dodávek,
- krádež: odcizení majetku společnosti zaměstnanci nebo neznámým pachatelem,
- nedostatek lidských zdrojů na trhu: momentálně probíhá období nedostatku odborných pracovních sil na trhu, proto jsou mnohdy zaměstnáni pracovníci bez praxe nebo odbornosti.

Tabulka 2 – Vyhodnocení SWOT analýzy [vlastní]

Vyhodnocení SWOT analýzy			
Silné stránky – Slabé stránky	3,6	-2,5	**1,1**
Příležitosti – Hrozby	3,1	-2,6	**0,5**

Vyhodnocení kvadrantů je zobrazeno v tab. 2, ze které je patrné, že silné stránky převažují na slabými a příležitosti převažují nad hrozbami, jedná se tedy o strategii spojenectví.

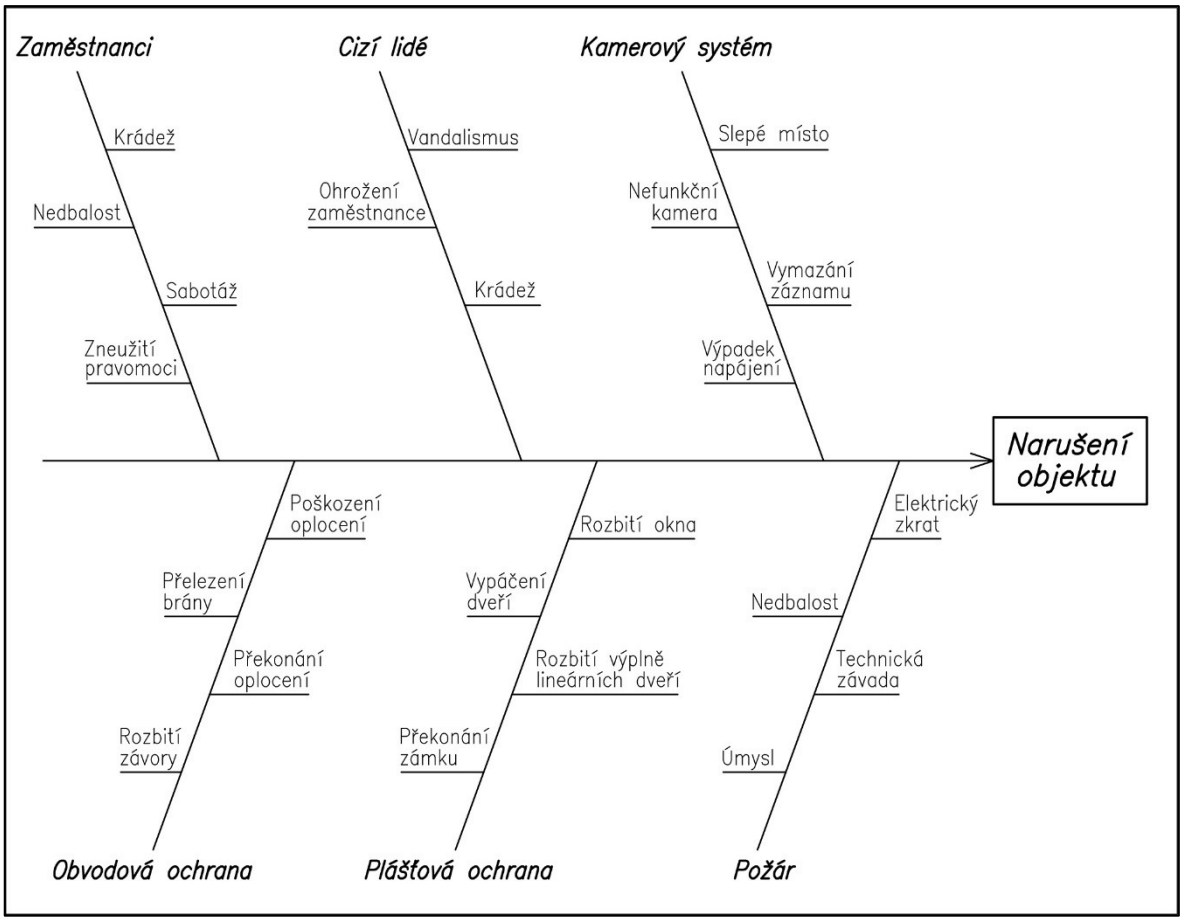
Graf 1 – Graf kvadrantů SWOT analýzy [vlastní]



Strategie vychází z dat uvedených v tabulce 2. Rozdíl mezi vnitřními faktory dosáhl hodnoty 1,1 a hodnota vnějších faktorů dosáhla hodnoty 0,5. Z uvedených hodnot vyplývá, že případnou strategií bude spojenectví, kdy podnik musí využít co nejvíce silných stránek, aby využil možné příležitosti. [18]

5.2 Ishikawa diagram

Ishikawa diagram neboli diagram rybí kosti je známý taktéž pod názvem diagram příčin a následků. Tento diagram je použit pro nalezení příčin, které vedou k narušení zabezpečení a ochrany podniku. Do hlavních příčin je zadáno: zaměstnanci, cizí lidé, kamerový systém, obvodová ochrana, plášťová ochrana a požár (obr. 15).



Obrázek 15 - Ishikawa diagram [vlastní]

Obvodová ochrana patří do první linie, kterou musí pachatel překonat. Proto patří k nejrizikovějším. Pokud se narušitel rozhodne překonat obvodovou ochranu, pravděpodobně by se pokusil překonat vjezdovou bránu nebo drátěné oplocení, následně by se pohyboval uvnitř areálu podniku. Při pokusu o narušení plášťové ochrany by útočník zvolil rozbití otvorových výplní, pravděpodobně skleněné výplně vstupních lineárních dveří. Dalším rizikem jsou lidé cizí nebo zaměstnanci, kteří mohou způsobit škody nedbalostí nebo úmyslným jednáním. Tito lidé mohou způsobit škody na materiálech, odcizením majetku nebo dokumentace. U kamerového systému může dojít k závadě na systému, tedy samotné kamery, záznamového zařízení nebo výpadku napájení celého systému. Posledním rizikem je vznik požáru

a materiálního poškození, ovšem i poškození serverovny, což by ochromilo chod celého podniku.

5.3 Metoda PNH

Metoda PNH je jednoduchá polokvantitativní bodová metoda k vyhodnocení rizik. Tato metoda je použita k řešení a vyhodnocení daných rizik zabezpečení obchodně výrobního podniku. Vyhodnocení rizik je provedeno v tabulce 3.

Tabulka 3 – Vyhodnocení metody PNH [vlastní]

Druh činnosti	Zdroje rizika	Identifikace nebezpečí	Vyhodnocení závažnosti rizika				Opatření k omezení rizika
			P	N	H	R	
Člověk	Nedbalost	Poškození stroje	4	2	1	8	Organizační opatření, zavedení SBS
	Sabotáž	Úmyslné znehodnocení	1	3	4	12	Organizační opatření, zavedení SBS
	Vandalismus	Sprejerství	3	4	4	48	Organizační opatření, zavedení SBS
	Elektrické zařízení	Úraz el. proudem při vytažení přívodního kabelu	3	3	4	36	Pravidelné revize el. zařízení, poučení pracovníků, udržování technického stavu
	Napadení zaměstnance	Úraz	1	2	3	6	Organizační opatření, zavedení SBS, evidence návštěv a dodavatelů
Majetek podniku	Krádež	Produktů portfolia podniku	4	3	4	48	Organizační opatření, zavedení SBS
	Poškození vybavení	Poničení strojů a zařízení	2	3	2	12	Organizační opatření, pravidelná školení zaměstnanců
	Sabotáž	CCTV	2	5	4	40	Pokrytí slepých míst CCTV
	Sabotáž	PZTS	3	4	3	36	Pravidelné kontroly a revize PZTS
Plášťová ochrana	Rozbití okna	Úraz	2	3	2	12	Pokrytí slepých míst CCTV
	Vypáčení dveří, vrat	Poškození zařízení podniku	2	1	3	6	Pravidelné kontroly PZTS
Obvodová ochrana	Rozbití závory	Nehoda	4	4	4	64	Snížení rychlosti v areálu podniku
	přelezení brány	Úraz	3	4	3	36	Doplnění výstražného značení
	Poškození oplocení	Úraz, zničení majetku	3	3	3	27	Pokrytí slepých míst CCTV, zavedení SBS

Jednotlivým rizikům bylo přiřazeno bodové hodnocení v rozmezí 1-5 a byla navržena a popsána opatření k omezení rizika.

Z dat uvedených v tabulce 3 vyplývá, že největší hrozbou pro podnik je rozbití závory, která se řadí do druhého rizikového stupně. Rozbití závory by mohlo vést k dopravní nehodně s fatálními následky. V rizikovém stupni tři, tedy v mírném riziku, je zřejmé nebezpečí úrazu eklektickým proudem, krádeže, sabotáže či poškození oplocení. Rizika spadající do čtvrtého stupně jsou akceptovatelná.

Riziko bylo vyhodnoceno ve třech složkách:

- P – pravděpodobnost vzniku,
- N – pravděpodobnost následků – závažnost nebezpečí,
- H – názor hodnotitele,
- R – celkové hodnocení rizika. [21]

Celkové vyhodnocení rizika je získáno součinem jednotlivých složek, výsledkem je hodnota míry rizika R (tabulka 4):

$$\mathbf{R = P \times N \times H}$$

Tabulka 4 – Stupnice rizik [21]

Rizikový stupeň	Celkové hodnocení rizika-R	Míra rizika
I.	> 100	Nepřijatelné riziko
II.	od 51 do 100	Nežádoucí riziko
III.	od 11 do 50	Mírné riziko
IV.	od 3 do 10	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

6 NÁVRH NA ZVÝŠENÍ ZABEZPEČENÍ OBJEKTU OBCHODNĚ VÝROBNÍHO PODNIKU

Návrh na zvýšení zabezpečení objektu obchodně výrobního podniku vyplývá z kapitoly 4, kde byl pomocí popsaných metod proveden popis a zhodnocení jednotlivých druhů zabezpečení areálu podniku. Z uvedeného popisu jednotlivých kapitol plynou nedostatky v popsaných systémech, a to více či méně závažné. V této kapitole bylo provedeno zhodnocení zabezpečení objektu společnosti a následně uveden seznam nápravných opatření vedoucích ke zvýšení zabezpečení areálu před případným narušitelem vedoucí k fyzické újmě nebo finanční ztrátě.

6.1 Návrh na zřízení fyzické ostrahy formou bezpečnostní služby

Zřízení fyzické ochrany je vhodné, nikoliv prioritní. Mezi hlavní úkoly fyzické ostrahy by patřila kontrola areálu v mimopracovní dobu, ve kterou by pracovníci ostrahy prováděli pravidelné obchůzky areálu, kontrolu uzamčení jednotlivých budov. V pracovní době by byla hlavní náplní ostrahy kontrola vstupujících a odcházejících osob, evidence návštěv a kontrola automobilů při vjezdu i výjezdu. V tabulce 5 jsou uvedeny ekonomické náklady na zřízení fyzické ostrahy podniku formou bezpečnostní služby.

Tabulka 5 – Rozpočet provozu SBS [vlastní]

Provoz soukromé bezpečnostní agentury				
Provoz SBS				
Popis položky	**Počet**	**MJ**	**Cena**	**Celkem**
Fyzická ochrana	720	hod	150	108 000
Počet měsíců	12	ks	108 000	1 296 000
CELKEM bez DPH:				**1 296 000,00 Kč**

6.2 Zkvalitnění obvodové ochrany

V kapitole obvodové ochrany byly shledány nedostatky v oplocení západní strany (obr. 7), kde podél pozemku společnosti vede cyklostezka. Zde se nachází jednoduché oplocení, které nese známky mnohaletého použití a dle mého názoru se jedná o bezpečnostní mezeru, kudy může případný narušitel jednoduše vniknout do areálu společnosti, a to bez použití

speciálního nářadí. Oplocení areálu v této části je nutné vybudovat nové. Jsou navrženy dvě varianty vybudování nového oplocení:

- **Varianta 1:** Vybudovaní klasického drátěného oplocení, kdy se vyhloubí jámy pro betonové sošky, ve kterých budou ukotveny sloupky průměru 50 mm s povrchovou úpravou poplastováním. Výška sloupků bude 2 400 mm, samotné drátěné oplocení bude dosahovat výšky 2 000 mm a nad pletivem bude ještě ve dvou řadách instalovaný ostnatý drát. Cenový rozpočet je uveden v tabulce 6.

Tabulka 6 – Rozpočet na vybudování klasického drátěného oplocení [vlastní]

Oplocení areálu obchodně-výrobní společnosti						
Oplocení klasickým drátěným pletivem			**Dodávka**		**Montáž**	
Popis položky	**Počet**	**MJ**	**Cena**	**Celkem**	**Cena**	**Celkem**
Svařované pletivo Pilonet Middle, oko 50 x 100 mm, barva zelená, 2 000 mm	100	m	104,8	10 480	127	12650
Plotový sloupek DAMIPLAST® zelený Zn + PVC, průměr 48 mm, síla stěny 1,5mm, 2 600 mm	50	ks	238	11 900		-
Výkop a betonáž sloupku	50	ks		-	379	18 950
Beton pro betonáž sloupku	50	ks	141	7 044		
Vzpěra DAMIPLAST® zelená Zn + PVC, průměr 42 mm, síla stěny 1,5mm, 2 400 mm	8	ks	1 674	13 392	288	2 300
Beton pro betonáž vzpěry	8	ks	141	1 127		-
Vázací drát PVC 1,4/2,00 mm,50 m, zelený	1	kpl	130	130		-
Ostnatý drát	200	m	6	1 200	58	11 600
Demontáž stávajícího oplocení	200	m	-	-	75	15 000
Likvidace oplocení	1	kpl	12 850	12 850		
Doprava	1	kpl	5 000	5 000		-
Celkem				**63 123**		**60 500**
CELKEM bez DPH:				**123 622,00 Kč**		

- **Varianta 2:** Vede ke sjednocení typu oplocení celého areálu. Jedná se o ekonomicky nákladnější variantu, ale na druhou stranu jde o mnohem pevnější, stabilnější a hůře překonatelnou zábranu. Pro realizaci je nutné vyhloubit výkop po celé délce ve hloubce cca 600 mm. Na dno výkopu nasypat 10 mm štěrkopísku a následně betonu, který bude převyšovat okolní terén o 200 mm, čímž je dosaženo podhrabové překážky. Do betonového základu se instalují sloupy čtvercového profilu o rozměru 60 x 60 mm. Následně se na tyto sloupy připevní vodorovná konstrukce stejných

parametrů jako jsou sloupy. Na tuto vodorovnou konstrukci bude již osazeno samotné oplocení z trapézových plechů výšky 2 000 mm. Konstrukce bude opatřena povrchovou úpravou žárovým zinkováním. Nad trapézový plech bude doplněn ostnatý drát ve dvou řadách s rozestupem 200 mm. Rozpočet na oplocení s plnou výplní je uveden v tabulce 7.

Tabulka 7 – Rozpočet na vybudování oplocení z vlnitého plechu [vlastní]

Dodávka a montáž oplocení z plného plechu				
Oplocení plným plechem				
Popis položky	**Počet**	**MJ**	**Cena**	**Celkem**
Demontáž stávajícího oplocení a likvidace	1	kpl	15 000	15 000
Hloubení rýh š do 600 mm v hornině tř. 3 objemu do 100 m3	20	m³	117	2 340
Příplatek za lepivost k hloubení rýh š do 600 mm v hornině tř. 3	20	m³	7	140
Uložení sypaniny na skládky	20	m³	11	220
Základové konstrukce z betonu prostého	20	m³	2 798	55 960
Jekl čtvercový 60 x 60 x 4 mm	325	m	116	37 700
Zátka čtvercová 60 x 60 mm stěna 2,6 - 4 mm černá	52	ks	23	1 196
Tabulový plech T-12 šedý 0,60 2 m	90	ks	285	25 650
Ostnatý drát	200	m	5	1 000
Montáž oplocení	100	m	127	12 700
Dokumentace skutečného provedení stavby	1	kpl	3 000	3 000
Náklady na zřízení, provoz a zrušení staveniště	1	kpl	12 000	12 000
CELKEM bez DPH:				**166 906,00 Kč**

Z pohledu autora se jeví výhodněji varianta číslo 2, protože se jedná o kvalitnější a trvanlivější oplocení, které je hůře překonatelné a současně povede k typovému sjednocení oplocení. Mezi objekty A3 a E je navrženo doplnění elektromechanické závory, která zamezí náhodnému vjezdu návštěvníků přijíždějících automobilem do prostoru výroby. Pořizovací náklady na tuto závoru činí 32 500 Kč.

6.3 Zkvalitnění režimové ochrany

Zkvalitnění režimové ochrany je možné pomocí elektronických systémů, které dokáží evidovat každé půjčení nebo vypůjčení klíčů, a naopak neumožní zapůjčení klíčů osobám, které nemají k tomu kroku oprávnění. Jedním z možných řešení jsou inteligentní klíčové trezory (obr. 16). Trezory mohou pracovat v autonomním režimu, kdy není nutné propojení do IT sítě společnosti a všechny informace jsou uchovány ve vnitřní paměti řídící jednotky, nebo mohou pracovat v on-line režimu, kdy jsou všechna data o provozu trezoru zapisována do SQL databáze. Data lze taktéž exportovat na SIM kartu, pro kterou je v trezoru slot.

Hlavním prvkem takového zařízení je stříbrný váleček připomínající náboj, ve kterém je ukrytý čip s elektronickým kódem. Tento náboj se připevní k danému klíči nebo svazku bezpečnostní pečetí, a tím jsou klíče označeny. Pro každý náboj systém vygeneruje pozici uvnitř trezoru, kde je pevně uzamčen a mohou ji odemknout pouze uživatelé s definovaným oprávněním. Po nastavení systému a jednotlivých oprávnění systém zaznamenává každý pohyb klíčů v trezoru. Informace, kdo a kdy si klíče půjčil, lze zjistit jednoduše na displeji ovládacího panelu. Mezi výhody systému patří modulárnost trezorů a možnost určit čas uživatelům, kdy bude klíč k dispozici. [22]

Obrázek 16 - Elektronický klíčový trezor [23]

6.4 Návrh na doplnění technické ochrany

V kapitole doplnění technické ochrany jsou rozebrány nedostatky jednotlivých druhů zabezpečení objektů.

6.4.1 Poplachové zabezpečovací a tísňové systémy

Pozorovací metodou bylo při obhlídce jednotlivých místností zjištěno, že některá pohybová čidla byla demontována a již nebyla nahrazena. Důvod demontáže nebylo možno zjistit, ale

lze se domnívat, že demontáž čidel byla provedena z důvodu stavebních úprav nebo z důvodu poruchy.

Systém je nutné doplnit o chybějící PIR čidla v jednotlivých místnostech. Jedná se celkem o čtyři čidla PIR a v poměru cena / úroveň zabezpečení se jedná o minimální náklady. Rozpočet na doplnění čidel uvádím v tabulce 8.

V kapitole PZTS jsou popsaná chybějící pohybová čidla v jednotlivých místnostech. Po tomto doplnění bude systém kompaktní.

Tabulka 8 – Rozpočet doplnění PZTS [vlastní]

Oprava PZTS						
PZTS			**Dodávka**		**Montáž**	
Popis položky	**Počet**	**MJ**	**Cena**	**Celkem**	**Cena**	**Celkem**
Digitální PIR detektor s dlouhým dosahem 15 m	4	ks	680	2 720	250	1 000
Sběrnicový posilující zesilovač a napájecí zdroj 1,7A, kontrola stavu	1	ks	4 580	4 580	450	450
Sběrnicový rozšiřující modul 8 zón (16 ATZ), PCB	1	ks	1 560	1 560	550	550
Kabel SYKFY 3x2x0,5	160	m	6	1 024	16	2 560
Lišta 18x18	100	m	16	1 560	20	2 000
Kabel CYSY 2x1,5	100	m	10	980	12	1 200
Dokumentace skutečného stavu	1	kpl	-	-	2 000	2 000
Drobný instalační materiál	1	kpl	500	500	500	500
Programování, nastavení dle požadavků uživatele, zaškolení obsluhy	1	kpl		-	3 500	3 500
Celkem				**12 924**		**13 760**
CELKEM bez DPH:				**26 684,00 Kč**		

6.4.2 Elektrická požární signalizace

Přestože jsou v areálu rozmístěna kouřová čidla napojená v systému PZTS, je důležité, aby byl v podniku místo těchto kouřových čidel instalován regulérní systém elektrické požární signalizace. Je navržena instalace systému Lites. Součástí návrhu je cenová kalkulace, která je uvedena v tabulce 9, doplnění systému EPS. Tato kalkulace je pouze orientační, přesné náklady bude možno určit až po zpracování projektové dokumentace.

Na ústřednu Lites MHU111 je navrženo napojení čidel ze všech budov podniku. K ústředně budou připojeny 4 linky, které budou rozděleny do 7 skupin. Ústředna bude instalována

v samostatném požárním úseku objektu A2. Ústředna bude pomocí výstupů napojena na pult centrální ochrany. Zařízení EPS bude plně adresovatelné, což zaručí komfort obsluhy, přehlednost a snadnější budoucí servisní úkony. Případné vznikající požáry budou signalizovány samočinnými čidly.

Tabulka 9 – Rozpočet doplnění EPS [vlastní]

Elektrická požární signalizace						
Elektrická požární signalizace			**Dodávka**		**Montáž**	
Popis položky	**Počet**	**MJ**	**Cena**	**Celkem**	**Cena**	**Celkem**
MHU 111 anal. adr. ústředna EPS - 256 adres	1	ks	31 999	31 999	450	450
MHS 811 tablo obsluhy	1	ks	19 875	19 875	450	450
MHY 918/R jedn.výst.8xreleový výstup	3	ks	4 918	14 754	450	1 350
MHY 912 OPPO	1	ks	5 775	5 775	450	450
Klíčový trezor požární ochrany KTPO vč. zámku pro ZL. kraj	1	ks	17 600	17 600	4 500	4 500
Akumulátor 28Ah	1	ks	3 892	3 892	85	85
Zábleskový maják	2	ks	1 840	3 680	190	380
Kabel J-Y(ST)-Y 1x2x0,8	4400	m	9	39 160	18	79 200
Kabel JE-H(ST)-H 1x2x0,8	600	m	25	14 880	18	10 800
Kabel JE-H(ST)-H 10x2x0,8	100	m	45	4 520	18	1 800
Trubka PVC tuhá 25 mm, vč. příchytek	2600	m	29	75 400	25	65 000
Trubka PVC ohebná 25 mm	300	m	8	2 400	25	7 500
Kabelová příchytka	5000	ks	15	75 000	24	120 000
MHG 262i hlásič kouře optický	417	ks	890	371 130	250	104 250
MHG 362 hlásič tepelný	12	ks	910	10 920	250	3 000
MHY 734 zás.pro adr. a interakt. Hlásiče	429	ks	161	68 897	250	107 250
MHA 141 hlásič tlačítkový	24	ks	1 301	31 231	340	8 160
ROLPSB/RL/R/D elektrická siréna s majákem	36	ks	680	24 480	190	6 840
Popisný štítek hlásiče	453	ks	10	4 530	5	2 265
Provozní kniha EPS	1	ks	250	250	40	40
Zařízení dálkového přenosu	1	ks		-	25 000	25 000
Programování a oživení systému	1	kpl		-	15 000	15 000
Komplexní zkoušky zařízení, výchozí revize	1	kpl		-	10 000	35 000
Zaškolení obsluhy	1	kpl		-	4 500	4 500
Protipožární utěsnění prostupů	1	kpl		-	25 000	25 000
Dokumentace skutečného provedení	1	kpl		-	1 500	1 500
Doprava, přesun materiálu	1	kpl		-	20 000	20 000
Celkem				**820 374**		**649 770**
CELKEM bez DPH:				**1 470 144 Kč**		

Hlásiče požáru budou připojeny na vedení hlásících linek dvoudrátově vodičem JySt Y 1x2x0,8. Automatické hlásiče jsou umístěny tak, aby v maximální míře postihly střežený prostor. Budou instalovány na strop, přibližně doprostřed místnosti. Hlásiče musí být umístěny tak, aby k nim byl zajištěn přístup pro zkoušky a opravy. Manuální hlásiče jsou umístěny na přístupových cestách do prostor ve výšce 1,5 m nad podlahou. Nastavení citlivosti hlásičů bude na střední stupeň 3. Hlásiče dodavatel opatří štítky s jednoznačnou identifikací. Sirény budou instalovány na stěně ve výšce 3-4 m a směrovány do místnosti.

Vedení kabelových rozvodů je navrženo v pevných nebo ohebných trubkách dle obecně platných zásad pro pokládání slaboproudých vedení s odstupy od vyšší napěťové soustavy min. 30 cm. Všechny kabelové prostupy protipožárními přepážkami musí být protipožárně utěsněny. Po dokončení kabeláže bude provedeno měření kabelů a vystaven protokol.

Ve výrobních halách bude kabelová instalace vedena po povrchu nebo v kabelových žlabech MARS, ze kterých budou vyvedeny odbočky k jednotlivým čidlům. V tabulce 7 jsou uvedeny náklady na instalaci a implementaci systému EPS. V této kalkulaci není zahrnuto propojení na pult centrální ochrany Hasičského záchranného systému, která musí být nedílnou součástí zprovoznění a provozu EPS.

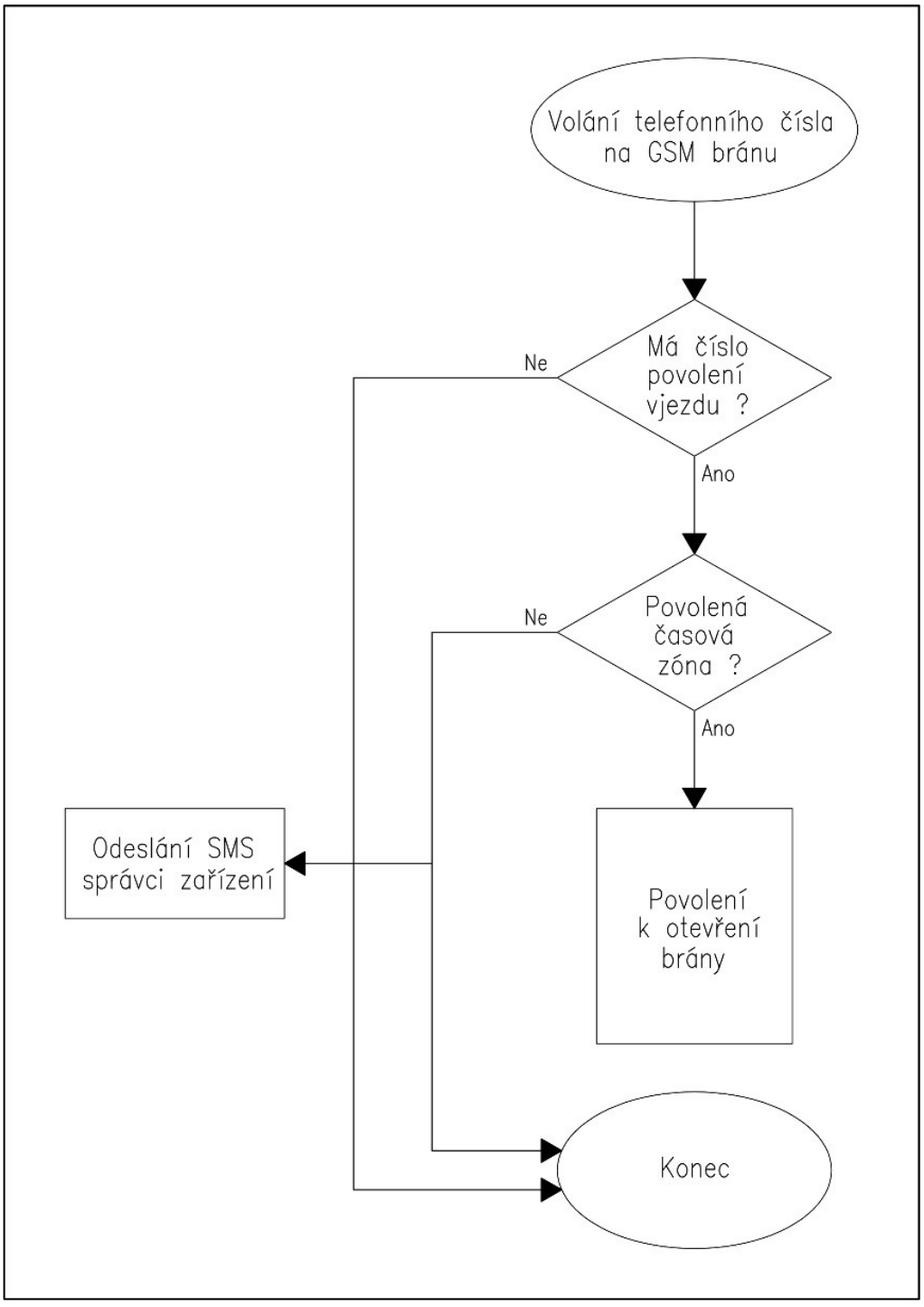
Součástí instalace musí být dle ČSN 342740 revizní zpráva a zaškolení obsluhy. Revizní zprávy musí být vykonávané v pravidelných intervalech.

6.4.3 Systém kontroly vstupu

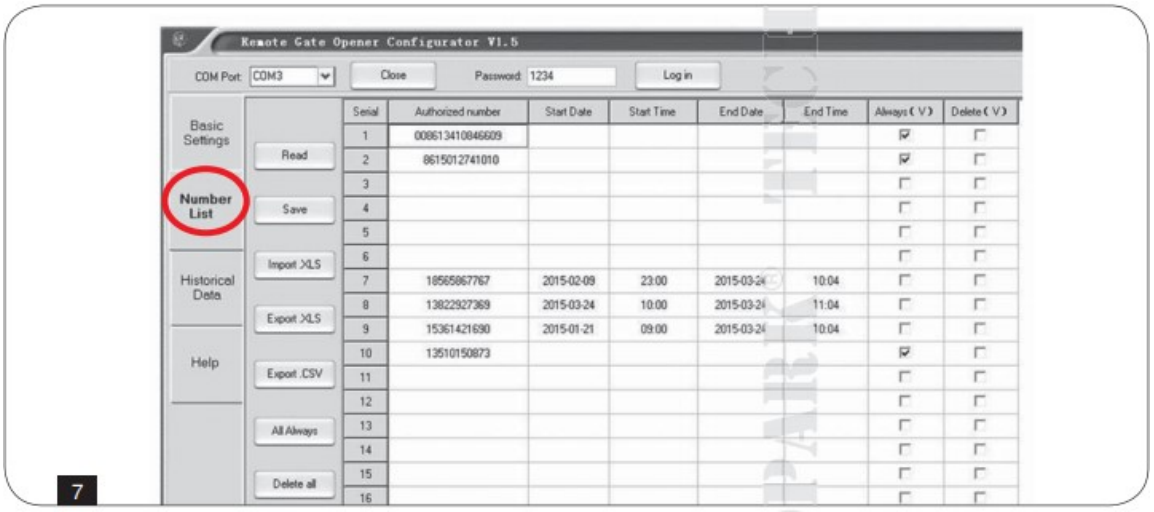
Jedním z nedostatků v zabezpečení objektu byl shledán přístupový systém, kde pro vjezd dopravních prostředků je použitá zastaralá GSM brána. Každá osoba znající telefonní číslo GSM brány může kdykoliv do objektu proniknout. Riziko představují především bývalí zaměstnanci, dodavatelé společnosti, externí pracovníci a další osoby, kterým bylo toto číslo zprostředkováno.

Je navrženo doplnění moderního zařízení, kde je možná administrace uživatelů v seznamu telefonních čísel, např. SBM 1000. V tomto seznamu je možné přiřazovat oprávnění, tedy zdali má telefonní číslo oprávnění otevřít závoru / bránu nebo nemá toto oprávnění. Další možností je nastavení konkrétních dnů, především pracovních nebo mimopracovních. Nastavení umožňuje přiřadit časovou zónu, zde doporučuji rozdělení na pracovní dobu od 5:30 hodin do 17:00 hodin, kdy bude povolen vjezd všem vozidlům uvedeným na seznamu a mimopracovní dobu od 17:01hodin do 5:29 hodin, kdy bude do objektu povolen vjezd

pouze managementu a vedoucím pracovníkům společnosti. Výhodou této GSM brány je možnost přidělení oprávnění po jednotlivých telefonních číslech, které je znázorněno v rozhodovacím diagramu (obr.17), což dosavadní instalované zařízení neumožňuje. Nastavení brány je velmi jednoduché a uživatelsky přívětivé (obr. 18). Při prozvonění brány není tento hovor zpoplatněn, takže se jedná o ekonomicky výhodný provoz. Na obrázku 17 je zobrazen rozhodovací digram vjezdu do objektu podniku za použití SBM 1000.



Obrázek 17 - Rozhodovací diagram při použití GSM brány SBM 100 [vlastní]



Obrázek 18 - Editace seznamu autorizovaných čísel [24]

Rozpočet na doplnění nové GSM brány je velmi jednoduchý. Modul se dá pořídit za cca 3 600 Kč a k tomu je nutné objednat odbornou firmu, která provede instalaci a nastavení, lze odhadnout na částku 5 000 Kč. Celkové náklady na pořízení nové GSM brány činí 8 600 Kč.

6.4.4 Uzavřený televizní okruh

Uzavřený televizní okruh je v současné době realizován pouze na budovách A1, A2, A3, B. Na těchto lokalitách je rozmístění kamer správné a záznam CCTV zabírá všechny prostory.

Pro úplné zabezpečení objektu je nutné CCTV doplnit o chybějící kamery, je navrženo doplnění statických IP kamer Vivotek, které jsou již instalovány. Pro přehlednost je doplnění kamer znázorněno na situační mapě (obr. 18), kde jsou nově navržené kamery zakresleny červeně. Finanční náklady na doplnění kamer jsou uvedeny v tabulce 10.

Současně je vhodné doplnění kamerového systému o kameru na rozpoznávání registračních značek, čímž by bylo zaznamenáno každé vozidlo, které vjelo do areálu podniku. V případě že k tomu nedojde, bude muset značku zadat ručně do systému obsluha, ale to pouze v případě, kdy bude na vstupu do objektu fyzická ochrana. V tabulce 8 jsou uvedeny náklady na pořízení kamery s rozpoznáváním registračních značek. Umístění kamery je navrženo na budově vrátnice pro ovládání vjezdové závory. Tento typ kamery by nahradil případnou GSM bránu. Přestože se jedná o ekonomicky náročnější řešení, rozpočet je uveden v tabulce 11, přidanou hodnotou kamery se čtením registračních značek je komfort, kdy není nutné používat ovladače, mobilní telefony či jiná ovládací zařízení.

Tabulka 10 – Rozpočet doplnění kamerového systému [vlastní]

Rozšíření kamerového systému						
IP kamerový systém			**Dodávka**		**Montáž**	
Popis položky	**Počet**	**MJ**	**Cena**	**Celkem**	**Cena**	**Celkem**
VIVOTEK IB8367A	7	ks	9 725	68 075	1 998	13 986
Venkovní techno polymerový kryt pro kamery PUNTO	7	ks	1 488	10 413	325	2 275
Synology DS115j Disk Station	1	ks	3 050	3 050	1 170	1 170
Synology Camera License Pack x 1	7	ks	1 488	10 413	130	910
WD RED NAS EDITON WD10EFRX 1TB SATA / 600 - NAS certified	1	ks	2 225	2 225	195	195
Cisco SF100D-08P, 8-Port 10 / 100 Switch, POE 33,12W / 4 ports	1	ks	2 900	2 900	520	520
Kabel UTP Solarix CAT5E UTP vnitřní	500	m	7	3 250	16	7 800
Dokumentace skutečného stavu	1	kpl	-	-	2 500	2 500
Drobný instalační materiál	1	kpl	1 200	1 200	650	650
Nastavení systému, instalace, zaškolení	1	kpl	-	-	6 500	6 500
Celkem				**101 525**		**36 506**
CELKEM bez DPH:				**138 031 Kč**		

Po tomto doplnění bude celý areál monitorován. Případný narušitel bude vždy zaznamenán kamerovým systémem.

Popis budoucích jednotlivých kamer a jejich umístění:

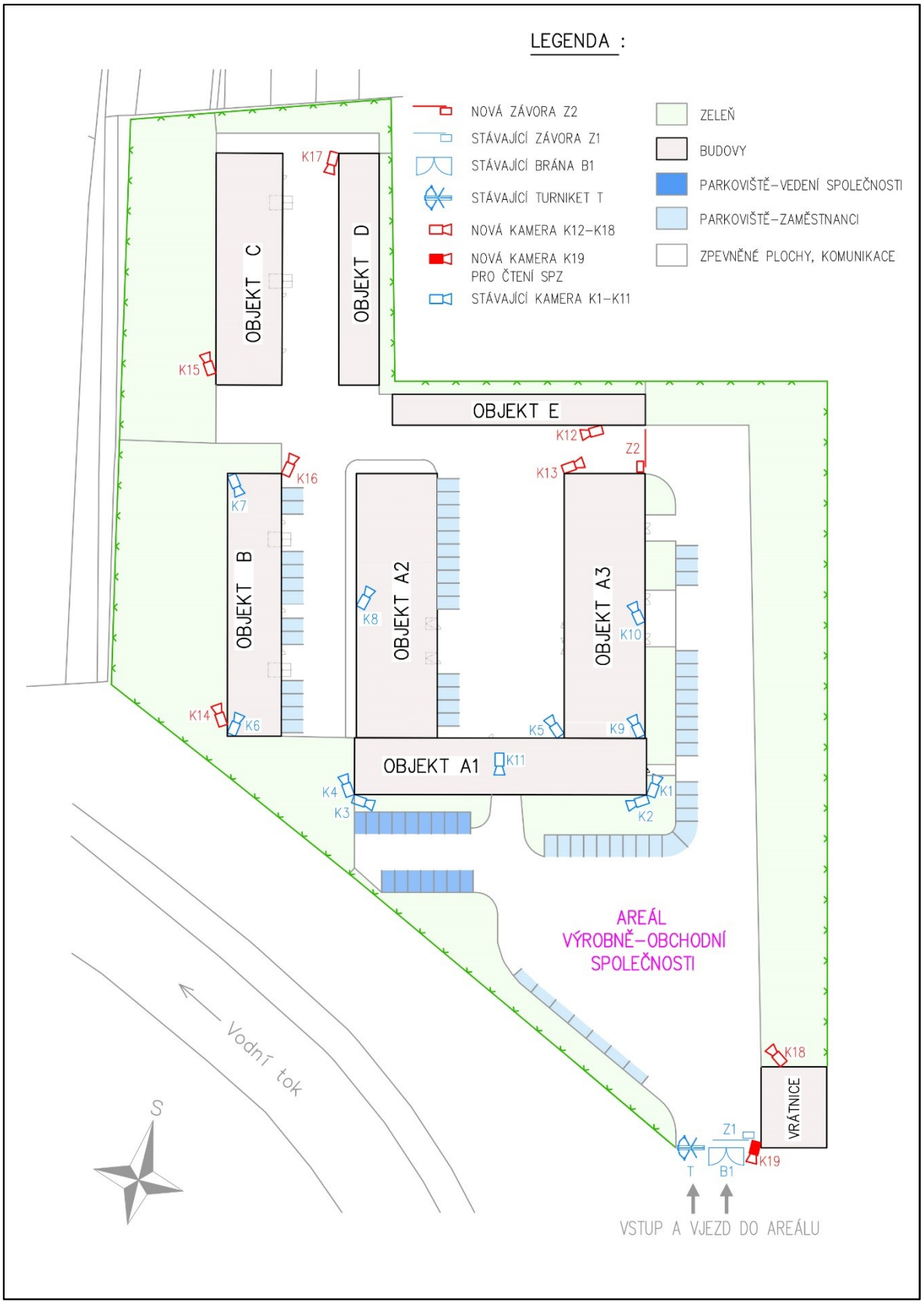
- Kamera 12–13 budoucí umístění na výrobní hale A3 a E. Kamery budou snímat prostory před skladovací halou E a vjezd do výrobní části.
- Kamera 14–15 budoucí umístění na výrobní hale B a 1x výrobní hala C. Kamery budou zabírat prostory za výrobní halou, monitoring západní části perimetru podniku.
- Kamera 16–17 budoucí umístění 1x výrobní hala B a 1x výrobní hala D. Kamery budou snímat záběr prostorů před výrobními halami B, C, D.
- Kamera 18 bude umístěna na vrátnici a bude monitorovat prostor před administrativní budovou.
- Kamera 19 na rozpoznávání RZ. Kamera bude umístěna na budově vrátnice, tak aby snímala přijíždějící automobily. Osazena bude IP kamery DAUHA s napájením PoE.

Rozmístění nově navržených kamer je zobrazeno na obr. 19. Nově navržené kamery jsou zvýrazněny červeně, stávající již instalované kamery jsou zobrazeny modrou barvou.

Do White listu budou zaneseny všechny registrační značky automobilů firemních, soukromých (zaměstnanců), známé registrační značky dodavatelů a externích pracovníků. V rámci pracovní doby by systém umožnil vjezd do areálu. V mimopracovní době by byl vstup umožněn pouze s platnou ID kartou. Pro případné návštěvy je možné v aplikaci pro správu registračních značek nastavit jednorázový vjezd. V případě propojení databáze registračních značek s přístupovým systémem, tedy provázání registrační značky a identifikačním číslem karty, by byly v historii systému dohledatelné všechny uskutečněné vjezdy. V případě, že registrační značka nebude na white listu, bude o tomto pokusu vjezdu neznámé značky zaslána alarmová hláška, která bude evidována v samostatné tabulce. Vzhledem k platnosti GDPR nebude systém ukládat fotografie RZ, ale bude je zasílat ve formě alfanumrického řetězce do systému ACS, kde bude probíhat vyhodnocení a uchování historie.

Tabulka 11 – Rozpočet kamerového systému rozpoznávání RZ [vlastní]

Rozšíření kamerového systému						
Kamerový systém rozpoznávání registračních značek automobilů			**Dodávka**		**Montáž**	
Popis položky	**Počet**	**MJ**	**Cena**	**Celkem**	**Cena**	**Celkem**
ITC237-PW1B-IRZ – Inteligentní 2 Mpx (Full HD) kompaktní kamera IP pro vjezdové brány, rozlišení 1920 x 1080 px @ 50 fps, Smart IR LED dosvit 3–8 m, IP 67,	1	Ks	18 590	18 590	1 998	1 998
Propojovací box, hliníkový, pro kamery Dahua,	1	Ks	850	850	500	500
Dahua průmyslový switch 5x 1000 Mbps + 1x SFP Gbit, podpora PoE pro 4 porty, 4x PoE+ (IEEE802.3at),	1	Ks	6 545	6 545	520	520
Napájecí zdroj 48 V DC / 2,5 A, vstupní napětí 176–264 V AC	1	Ks	1 860	1 860	550	550
Kabel UTP Solarix CAT5E UTP vnitřní	20	M	7	130	16	312
Kabel CYKY 3 C x 1,5	15	M	15	228	18	270
Dokumentace skutečného stavu	1	Kpl	-	-	500	500
Oživení systému RZ a zaškolení obsluhy	1	Kpl	-	-	8 500	8 500
Celkem				**28 203**		**13 150**
CELKEM bez DPH:				**41 353,00 Kč**		



Obrázek 19 - Situační mapa podniku – doplnění kamer a závory [vlastní]

ZÁVĚR

V práci je řešeno zabezpečení a ochrana objektu obchodně výrobní společnosti. Práce je rozdělena do teoretické a praktické části. V teoretické části jsou popsány jednotlivé odborné termíny a jejich význam a popsány možnosti zabezpečení. V praktické části je popsáno současné zabezpečení, a to po jednotlivých kapitolách. Závěrem mé práce je zhodnocení jednotlivých systémů a popis zjištěných nedostatků včetně detailního popisu. Následně jsou navržena nápravná opatření, která povedou ke zvýšení zabezpečení objektu společnosti proti narušitelům. Součástí práce jsou rozpočty navržených opatření nebo doplnění systému PZTS, ACC, CCTV a plášťové ochrany.

Cílem práce bylo popsat současný stav zabezpečení objektu obchodně výrobní společnosti, jeho analýza a vypracování návrhu na zvýšení zabezpečení a ochrany objektu podniku. V práci je popsáno, jakým způsobem je nyní zajištěna obvodová, plášťová, režimová a technická ochrana. Následně byla vypracována SWOT analýza, kde bylo zjištěno, že nejsilnější stránkou jsou poplachové zabezpečovací a tísňové systémy. Naopak nejslabší stránkou je absence EPS. Příležitostí pro podnik je zavedení fyzické ochrany a největší hrozbou je krádež. Následně byl vypracován Ishikawa diagram příčin a následků, na který částečně navazuje metoda PNH.

V kapitole návrhové části byla popsána opatření vedoucí ke zvýšení úrovně zabezpečení podniku. Je navrženo zřízení fyzické ostrahy formou SBS. Pro zlepšení obvodové ochrany byla navržena rekonstrukce stávajícího oplocení západní strany. V rámci režimové ochrany je navržen elektronický klíčový trezor. Na zlepšení technické ochrany je nutné doplnění čidel PZTS, zřízení nové EPS s napojením na PCO HZS a v systému CCTV je nutné k eliminaci slepých míst doplnění kamer. V částí přístupového systému bude nutná výměna GSM modulu ovládání závory. V práci jsou nastíněny finanční náklady nutných opatření. Rozhodneli se vedení podniku realizovat všechna navržená opatření, celkové náklady dosáhnou částky 1 875 618 Kč. K tomu je nutné započíst roční náklady na provoz SBS, které činí 1 296 000 Kč. Z pohledu autora považuji za nejdůležitější realizaci doplnění PZTS, rekonstrukci obvodové ochrany v západní části podniku, výměnu GSM modulu ACS a doplnění kamer CCTV. Zřízení SBS a EPS považuji za důležité, nikoliv však za prioritní. Zabezpečení objektu podniku je nutné neustále zdokonalovat v souladu s rostoucími nároky na zabezpečení majetku a zdraví osob, souměrně s technologickým vývojem zabezpečovacích systémů.

SEZNAM POUŽITÉ LITERATURY

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

[2] Co je to technická norma? *ÚNMZ: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví* [online]. 2018 [cit. 2018-10-13]. Dostupné z: http://www.unmz.cz/urad/co-je-to-technicka-norma-

[3] TOMEK, Miroslav. *Ochrana a bezpečnost objektů a osob: Přednášky a materiály pro výuku kombinovaného studia*. Uherské Hradiště.

[4] BRABEC, František. *Hlídací služby*. Praha: Eurounion, 1995. ISBN isbn80-85858-12-6.

[5] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management IV*. Zlín: Radim Bačuvčík - VeRBuM, 2014. ISBN 978-80-87500-57-6

[6] IVANKA, Ján. *Mechanické zábranné systémy*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. ISBN 978-80-7318-910-5.

[7] Turnikety a branky. *Cominfo security first* [online]. 2010 [cit. 2018-10-13]. Dostupné z: http://www.cominfo-trade.com/cz/produkty/turnikety-a-branky/

[8] REXON DEA 3. In: *Cominfo security first* [online]. Zlín, 2010 [cit. 2018-11-28]. Dostupné z: https://www.cominfo-trade.com/cz/produkty/turnstiles-rexon/rexon-dea-3

[9] UHLÁŘ, Jan. *Technická ochrana objektů*. Praha: Vydavatelství PA ČR, 2006. ISBN 80-7251-235-8.

[10] UHLÁŘ, Jan. *Technická ochrana objektů*, *II. díl* Praha: Vydavatelství PA ČR, 2005. ISBN 80-7251-189-0.

[11] Čo je to režimová ochrana? *DAST HOLDING, a.s* [online]. Bratislava, 2005 [cit. 2018-11-22]. Dostupné z: http://www.dastholding.sk/security/faq/rezimova-ochrana

[12] LOVEČEK, Tomáš, Andrej VEĽAS a Martin ĎUROVEC. *Bezpečnostné systémy: poplachové systémy*. Žilina: Žilinská univerzita v Žiline, 2015. Vysokoškolské učebnice. ISBN 978-80-554-1144-6.

[13] *MOJEservery.cz* [online]. [cit. 2019-04-17]. Dostupné z: https://havel.mojeservery.cz/produkty-sluzby/bezkontaktni-rfid-pristupovy-system/

[14] Přístupový systém - ACCESS: Systém Infos. In: *Cominfo Security First: Váš partner pro bezkontaktní identifikaci a vstupní zařízení* [online]. [cit. cit. 2018-10-13]. Dostupné z: http://www.cominfo-trade.com/cz/reseni/pristupovy-system

[15] Čtečka bezkontaktních karet. In: *Cominfo Security First: Váš partner pro bezkontaktní identifikaci a vstupní zařízení* [online]. Zlín, 2017 [cit. 2018-10-13]. Dostupné z: http://www.cominfo-trade.com/cz/produkty/komponenty-a-hardware/rfid-reader

[16] LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management II*. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 978-80-87500-19-4.

[17] LOVEČEK, Tomáš a Peter NAGY. Bezpečnostné systémy: Kamerové bezpečnostné systémy. Žilina: Žilinská univerzita J. M. Urbana, 2008. ISBN 978-80-8070-893-1.

[18] Čo je to režimová ochrana. *DAST HOLDING, a.s* [online]. Bratislava, 2005 [cit. 2018-11-22]. Dostupné z: http://www.dastholding.sk/security/faq/rezimova-ochrana

[19] VARGOVÁ, Slavomíra. *Analýza rizik: Přednášky, konzultace, materiály pro výuku kombinovaného studia*. Uherské Hradiště, 2017.

[20] PALEČEK, Miloš. *Prevence rizik*. Praha: Oeconomica, 2006. ISBN 80-245-1117-7.

[21] KOUDELKA, Ctirad a Václav VRÁNA. *Rizika a jejich analýza: VŠB - TU Ostrava [online]*. Ostrava, 2006 [cit. 2018-12-04]. Dostupné z: http://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf

[22] Inteligentní klíčové trezory. *Traka* [online]. Praha, 2012 [cit. 2018-11-22]. Dostupné z: http://www.traka.cz/inteligentni-klicove-trezory

[23] Elektronický klíčový trezor. In: *Traka* [online]. Praha, 2012 [cit. 2018-11-22]. Dostupné z: https://www.traka.cz/inteligentni-klicovy-trezor-serie-m-0

[24] SBM 1000. *Technopark* [online]. Brno, 2017 [cit. 2018-11-22]. Dostupné z: https://eshop.technopark.cz/static/_dokumenty/2/2/9/3/7/SBM1000_verze2.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Přístupový systém
CCTV	Kamerový systém
DVR	Digital video recorder
EPS	Elektrická požární signalizace
FSTP	Shielded Twisted Pair
FTP	Foiled Twisted Pair
GDPR	General Data Protection Regulation
GSM	Global System for Mobile (Groupe Spécial Mobile, Globální systém pro mobilní komunikaci)
H	Názor hodnotitele
KS	Krizový stav
MK	Magnetický kontakt
MZS	Mechanické zábranné systémy
N	Pravděpodobnost následků – závažnost nebezpečí
P	Pravděpodobnost vzniku
PCO	Pult centrální ochrany
PIN	Personal identification number
PoE	Power over Ethernet
PTS	Poplachové tísňové systémy
PZS	Poplachové zabezpečovací systémy
PZTS	Elektrické zebezpečovací a tísňové systémy
R	Celkové hodnocení rizika
RFID	Radio Frequency Identification
RZ	Registrační značka automobilů
SBS	Soukromá bezpečnostní služba

SK	Strukturovaná kabeláž
ÚOOÚ	Úřad pro ochranu osobních údajů

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH