Systém řízení bezpečnosti informací z pohledu fyzické bezpečnosti

Bc. Tomáš Vykydal

Diplomová práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Tomáš Vykydal**
Osobní číslo:	**L21184**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Systém řízení bezpečnosti informací z pohledu fyzické bezpečnosti**

Zásady pro vypracování

1. Zpracujte teoretický vstup do dané problematiky.
2. Proveďte analýzu současného stavu fyzické bezpečnosti daného subjektu vzhledem k řešenému problému.
3. Na základě analýzy vyhodnoťte rizika plynoucí ze současné úrovně fyzické bezpečnosti daného subjektu.
4. Na základě zjištěných rizik navrhněte opatření na zlepšení současného stavu.

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

Seznam doporučené literatury:

1. BAKER, Paul R. a Daniel J. BENNY. *The complete guide to physical security*. Boca Raton: CRC Press, 2013. ISBN 9781420099638.
2. LUKÁŠ, Luděk. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík – VeRBuM, 2015. ISBN 978--80-87500-05-7.
3. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2022**
Termín odevzdání diplomové práce: **28. dubna 2023**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou 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 Univerzita Tomáše Bati 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 – diplomovou 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 diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti, dne: 28. 9. 2025

Jméno a příjmení studenta: Bc. Tomáš Vykydal

.....
podpis studenta

ABSTRAKT

Diplomová práce se zaměřuje na problematiku systému řízení bezpečnosti informací z pohledu fyzické bezpečnosti ve vybraném subjektu. Členěna je do dvou hlavních částí, které na sebe postupně navazují. V první, teoretické části, jsou objasněny základní pojmy týkající se systému řízení bezpečnosti informací a fyzické bezpečnosti. Druhá, praktická část, se prvotně zaměřuje na základní charakteristiku vybraného subjektu. Dále je v této části prostřednictvím komparace s ČSN EN ISO/IEC 27002:2014 provedena analýza současného stavu fyzického zabezpečení informací u vybraného subjektu. V návaznosti na komparaci je pak využita jedna z metod analýzy rizik, checklist, za pomoci které, jsou zjištěna rizika související s aktuální úrovní fyzického zabezpečení subjektu a navrhnuta opatření vedoucí ke zlepšení celého systému fyzického zabezpečení.

Součástí návrhových opatření je i kalkulace nákladů na realizaci. V případě vybraného subjektu se jedná zejména o výstavbu kamenného oplocení, pořízení elektronického přístupového systému (turniketů), poplachového zabezpečovacího a tísňového systému a inovaci videodohledového systému.

Klíčová slova: bezpečnost, bezpečnost informací, fyzická bezpečnost, systém řízení bezpečnosti informací.

ABSTRACT

The diploma thesis focuses on the issue of information security management system from the perspective of physical security in the selected entity.

It is divided into two main parts, which follow each other. In the first, theoretical part, the basic concepts related to the information security management system and physical security are explained. The second, practical part, initially focuses on the basic characteristics of the selected entity. Furthermore, in this part, an analysis of the current state of physical information security of the selected entity is performed through a comparison with EN ISO/IEC 27002:2014. Following the comparison, one of the risk analysis methods, checklist, is then used to identify risks related to the current level of physical security of the entity and to propose measures leading to the improvement of the entire physical security system.

The design measures also include a cost calculation for implementation. In the case of the selected entity, these include in particular the construction of a stone fence, the acquisition of an electronic access system (turnstiles), an alarm and emergency system and an upgrade of the CCTV system.

Keywords: security, information security, physical security, information security management system.

Rád bych vyjádřil své díky všem, kteří mi při zpracování diplomové práce byli nápomocni. Zvláště bych pak chtěl poděkovat vedoucímu své diplomové práce panu Ing. Petru Svobodovi, Ph.D. za odborné vedení. Dále bych rád poděkoval panu Jiřímu Holečkovi, obchodnímu zástupci firmy ABBAS, a.s. pro jižní Moravu, za poskytnutím veškerých potřebných informací v souvislosti s funkčností a kompatibilitou vlastního návrhu systémů zabezpečení. Zároveň mé poděkování patří rodině a zejména pak manželce, za trpělivost a podporu při zpracování diplomové práce.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Pocit bezpečí je klíčový pro fungování společnosti. Ovlivňuje celkovou kvalitu života obyvatelstva a její zajištění by mělo být prioritou jednotlivců, organizací i státu. Přiznejme si však, že dnešní doba je víc než kdy dříve charakteristická rychle se rozvíjejícími informačními a komunikačními technologiemi a bezpečnost informací je pro spoustu manažerů a lídrů leckdy důležitější než bezpečnost vlastní. Data a informace dnes vládnou světu. Jejich ztráta může pro organizaci znamenat dokonce až likvidaci. Každá organizace by tak v současné době měla mít ve své organizační struktuře správně nastavený systém řízení bezpečnosti informací (Information Security Management System) - ISMS.

Bezpečnost informací se dotýká spousty oblastí, tato diplomová práce se však soustředí, jak je již z názvu patrné, na oblast fyzické bezpečnosti.

Teoretická část diplomové práce se věnuje problematice bezpečnosti z širší perspektivy, zaměřuje se na bezpečnost informací, systém řízení bezpečnosti informací a fyzickou bezpečnost. Pozornost je věnována taktéž legislativnímu vymezení, které se stalo podkladem pro tuto práci.

Praktická část se v prvotní fázi zaměřuje na základní charakteristiku vybraného subjektu. Dále je v této části prostřednictvím komparace s ČSN EN ISO/IEC 27002 provedena analýza současného stavu fyzického zabezpečení informací u vybraného subjektu. Za pomoci jedné z metod analýzy rizik, checklistu, je následně vypracován návrh na zlepšení, spolu s vyčíslením nákladů na realizaci těchto zlepšení.

CÍLE A METODY ZPRACOVÁNÍ DIPLOMOVÉ PRÁCE

Hlavním cílem diplomové práce je provést návrh opatření ke zvýšení úrovně fyzického zabezpečení v rámci vybraného subjektu (který z důvodu zachování mlčenlivosti nebude konkrétně jmenován). Pro naplnění hlavního cíle bylo nutné zaměřit se na několik dílčích cílů. Prvním z nich bylo provést rozbor problematiky systému řízení bezpečnosti informací subjektu se zaměřením na fyzickou bezpečnost. Praktická část diplomové práce se proto mimo jiné zabývá ČSN EN ISO/IEC 27002, částí fyzická bezpečnost a bezpečnost prostředí s důrazem na fyzický bezpečnostní perimetr. Dalším dílčím cílem bylo posoudit shodu stavu fyzického zabezpečení subjektu s požadavky vyplývající z ČSN EN ISO/IEC 27002. Na základě zjištěných odchylek od výše zmíněné normy jsou následně za pomoci jedné z metod analýzy rizik, checklistu, vyhodnocena rizika související se současným fyzickým zabezpečením subjektu.

Posledním dílčím cílem, který jsem si stanovil, bylo na základě komparace a checklistu navrhnout opatření směřující ke zlepšení celého systému fyzického zabezpečení ve vybraném subjektu. Součástí jednotlivých návrhových opatření je i kalkulace nákladů na jejich pořízení.

První metodou použitou k tvorbě diplomové práce, zejména pak její teoretické části, je **rešerše a sběr dat,** prostřednictvím které jsem dokázal získat podklady z literatury a právních předpisů. Tato metoda byla využita v prvotní fázi, ještě před tím, než bylo zahájeno samotné psaní diplomové práce.

K definování bezpečnosti, systému řízení bezpečnosti informací a celé fyzické bezpečnosti je využita metoda **popisu.**

Pro napsání zejména praktické části diplomové práce jsem vycházel z metod **pozorování, dotazování a rozhovoru**. Všechny tyto metody jsem uplatnil při osobním setkání s vedoucím zaměstnancem vybrané firmy, který mi mimo veškerých informací poskytl také osobní prohlídku prostor zmíněné firmy. Díky tomu jsem měl možnost získat obrazový materiál a lépe tak provést analýzu aktuálního stavu systému zabezpečení informací celé této firmy.

Z výše zmíněného tvrzení vyplývá, že dalšími metodami, které byly využity k tvorbě diplomové práce jsou **analýza a syntéza**. Za pomoci analýzy jsem dokázal zhodnotit a rozebrat celý systém současného fyzického zabezpečení zvolené firmy, za pomoci syntézy,

která je v blízkém spojení, jsem pak dokázal tento systém vyhodnotit a dojít tak k určitým závěrům.

K tvorbě zmíněných závěrů mi dopomohla metoda **komparace**, kdy jsem se pokusil srovnat aktuální stav fyzického zabezpečení firmy s doporučenými opatřeními plynoucími se zabezpečením dle ČSN EN ISO/IEC 27002. Na základě toho jsem mohl navrhnout opatření ke zlepšení systému fyzického zabezpečení, spolu s kalkulací nákladů na jejich realizaci.

I. TEORETICKÁ ČÁST

1 LEGISLATIVNÍ VYMEZENÍ

Bezpečnost je pro člověka nezbytnou součástí a zasahuje do všech možných oblastí každodenního života. Je tak zřejmé, že v České republice neexistuje pouze jedna jediná právní úprava bezpečnosti. Bezpečnost se dotýká ať už bezpečnosti člověka jako takového, tak i bezpečnosti informací, systému řízení bezpečnosti informací, kybernetické bezpečnosti, ochrany utajovaných informací a spousty dalších oblastní.

To je tedy hlavní důvod, proč pojem „bezpečnost“ nalezneme v různých zákonech a normativních dokumentech. Níže jsou uvedeny některé příklady, které mají přímou souvislost s problematikou této diplomové práce.

Ústava České republiky

Ústava je nejvyšším právním řádem České republiky. Stanovuje základní principy a pravidla, podle kterých se řídí český stát a jeho orgány. Ústava upravuje základní práva a svobody občanů, základní zásady hospodářského a politického uspořádání státu, uspořádání moci státní a samosprávné, vztahy mezi státem a církvemi a náboženskými společnostmi a další oblasti.

V Ústavě České republiky se nacházejí ustanovení, která se týkají bezpečnosti a ochrany státního území, jako například ustanovení o pravomoci armády a bezpečnostních složek státu.

Dle tohoto dokumentu tak lze říct, že základem státního zřízení je demokracie, a že státní moc musí být vykonávána v souladu se zákonem a je povinností každého jednotlivce chránit zákony. Tyto zásady jsou důležité zejména pro zachování právě zmíněné bezpečnosti a stability v zemi. (Ústavní zákon č. 1/1993 Sb.)

Občanský zákoník

Zákon č. 89/2012 Sb., občanský zákoník, je základní právní předpis, který v České republice upravuje vztahy mezi fyzickými a právnickými osobami. Mimo jiné tak definuje pojem bezpečnost jako:

„ochranu života, zdraví, osobní svobody, majetku a dalších práv a zájmů osob“. (zákon č. 89/2012 Sb.)

Trestní zákoník

Zákon č. 40/2009 Sb., trestní zákoník, je právní předpis, který stanovuje základní zásady trestního práva a trestní odpovědnosti fyzických osob.

Fyzická bezpečnost se dotýká ochrany lidí před fyzickým násilím a nebezpečím. Trestní zákoník pomáhá zajistit fyzickou bezpečnost tím, že stanovuje tresty za trestné činy, které ohrožují jejich bezpečí, a taktéž tím, že umožňuje orgánům činným v trestním řízení chránit oběti trestných činů a předcházet dalším zločinům. (Zákon č. 40/2009 Sb.)

Zákon č. 240/2000 Sb., o krizovém řízení

Bezpečnost je v zákoně č. 240/2000 Sb., o krizovém řízení, klíčovým faktorem a zajištění bezpečnosti obyvatelstva je jedním z hlavních cílů krizového řízení.

Tento zákon tak stanovuje způsob, jakým má být zajištěna ochrana obyvatelstva v případě krizových situací, včetně situací ohrožujících fyzickou bezpečnost obyvatelstva.

(Zákon č. 240/2000 Sb.)

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

Tento zákon se zaměřuje na ochranu utajovaných informací a upravuje povinnosti státních orgánů, fyzických a právnických osob, které s takovými informacemi pracují. Jedním z hlavních cílů zákona je zajistit bezpečné nakládání s utajovanými informacemi a zvýšit bezpečnost státu.

Ochrana utajovaných informací, je dle § 5 tohoto zákona zajišťována právě:

„Fyzickou bezpečností, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat“. (Zákon č. 412/2005 Sb.)

V této souvislosti zákon upravuje požadavky pro zabezpečení ochrany utajovaných informací v rámci fyzické bezpečnosti. (Zákon č. 412/2005 Sb.)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti se zaměřuje zejména na kybernetickou bezpečnost, ale zahrnuje i fyzickou bezpečnost jako jednu z důležitých součástí celkového systému zabezpečení.

Fyzická bezpečnost totiž obsahuje opatření zaměřená na ochranu informačních technologií, informačních systémů, informačních a telekomunikačních sítí a informačních zdrojů

fyzickými prostředky proti neoprávněnému vstupu, přístupu, použití, úpravě, zničení či jinému neoprávněnému zpracování nebo poškození. (Zákon č. 181/2014 Sb.)

Zákon č. 110/2019 Sb., o zpracování osobních údajů

Fyzické bezpečnosti se dotýká i zákon č. 110/2019 Sb., o zpracování osobních údajů. Tento zákon definuje fyzickou bezpečnost jako jeden z aspektů ochrany osobních údajů. Fyzickou bezpečností se z pohledu tohoto zákona rozumí zabezpečení objektů, jako jsou budovy, místnosti, skříně, archivy, kde jsou uloženy osobní údaje, a také zařízení pro jejich zpracování, jako jsou počítače, servery, mobilní telefony atd.

Konkrétně zákon stanovuje, že správce a zpracovatel osobních údajů jsou povinni zajistit fyzickou bezpečnost daných objektů a zařízení, aby se zabránilo neoprávněnému přístupu, změně, zničení nebo ztrátě těchto údajů. (Zákon č. 110/2019 Sb.)

Norma ČSN ISO/IEC 27001:2014

ČSN ISO/IEC 27001:2014 (dále jen „ČSN ISO/IEC 27001“), kterou bychom nalezli pod celým názvem: Informační technologie – Bezpečnost informací – Systémy řízení informační bezpečnosti – Požadavky, je dokument, který popisuje požadavky na systémy řízení bezpečnosti informací, poskytuje rámec pro implementaci a správu bezpečnosti informací v organizaci.

Podle této normy je bezpečnost informací definována jako:

„zabezpečení zachování důvěrnosti, integrity a dostupnosti informací prostřednictvím aplikace adekvátních bezpečnostních opatření.“ (ČSN ISO/IEC 27001)

Tato norma se vztahuje na všechny typy organizací, bez ohledu na jejich velikost nebo povahu činnosti. Obsahuje požadavky na plánování, implementaci, monitorování a zlepšování systému řízení bezpečnosti informací, aby organizace mohla účinněji řídit své informační rizika a zajistit ochranu svých informací.

Organizace, které implementují systém řízení bezpečnosti informací podle této normy, mohou být certifikovány a mít tak důkaz o tom, že jejich informace jsou řízeny a chráněny v souladu s mezinárodními standardy. (ČSN ISO/IEC 27001)

Norma ČSN EN ISO/IEC 27002:2014

ČSN EN ISO/IEC 27002:2014[1] popisuje standardy pro řízení bezpečnosti informací. Nalezneme v ní obecné zásady pro zabezpečení informací. Norma je založena na konceptu rizikového řízení a obsahuje doporučení pro identifikaci, hodnocení a řízení rizik spojených s informační bezpečností. Dále se věnuje tématům jako jsou řízení přístupu k informacím, bezpečnost sítí a komunikací, řízení bezpečnosti osobních dat, řízení bezpečnosti dodavatelů a další. (ČSN EN ISO/IEC 27002)

S oblastí fyzického zabezpečení souvisí spousty dalších norem, které se zabývají jednotlivými oblastmi tohoto zabezpečení. Jako příklad můžeme uvést ty, které budou zmíněny i v dalších částech diplomové práce.

ČSN EN 1627 - Dveře, okna, lehké obvodové pláště, mříže a okenice – Odolnost proti vloupání – Požadavky a klasifikace.

ČSN EN 50131-1 ed. 2 - Poplachové systémy – Poplachové zabezpečovací a tísňové systémy Část 1: Systémové požadavky.

ČSN CLC/TS 50131-7 - Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace**.**

ČSN EN 62676-1-1 Dohledové videosystémy 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 73 0875 - Požární bezpečnost staveb – Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení**.**

ČSN 34 2710 - Elektrická požární signalizace aj.

[1] Diplomová práce vychází z ČSN EN ISO/IEC 27002:2014, jelikož v době jejího zpracování ještě nebyla k dispozici nová verze této normy ČSN EN ISO/IEC 27002:2022 vydaná v dubnu 2023, s platností od 1.5.2023.

2 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

„Bezpečnost byla, je a bude jedním ze základních lidských potřeb. Bez bezpečnosti není nic jistého, ani zdraví, ani bohatství, ani svoboda.“ (Václav Havel)

Těmito dvěma větami dokázal Václav Havel v jednom ze svých prezidentských proslovů vystihnout důležitost bezpečnosti jako takové, bez které by jen těžko společnost dokázala fungovat. Pocit bezpečí je důležitý nejen v dobách válek a konfliktů, ale i v běžném životě. V moderní společnosti se však už nebavíme pouze o bezpečí člověka jako takového, ale nahlížíme i na bezpečnost týkající se informací. Jsou to právě informace, které se stávají klíčovým zdrojem hodnoty firem, organizací i jednotlivců či konkurenční výhodou. Ztráta, poškození nebo zneužití informací s sebou nese obrovské následky, je tak víc než nutné zajistit určitý systém zabezpečení.

2.1 Bezpečnost

Ještě dříve, než se dostaneme k samotné charakteristice bezpečnosti informací, je nutné začít úplně od začátku. Základním pojmem, ze kterého celá tato problematika vychází, je samotný pojem bezpečnost.

Původem je bezpečnost odvozena od slova „péče“. Pojem tak lze vysvětlit jako stav bez péče, tj. bez starostí. (NKP, © 2004-2014)

Terminologický slovník Ministerstva vnitra České republiky (dále jen „MVČR“) vysvětluje pojem bezpečnost jako:

„Stav, kdy je systém schopen odolávat známým a předvídatelným (i nenadálým) vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí.“ (MVČR, 2016, s. 5)

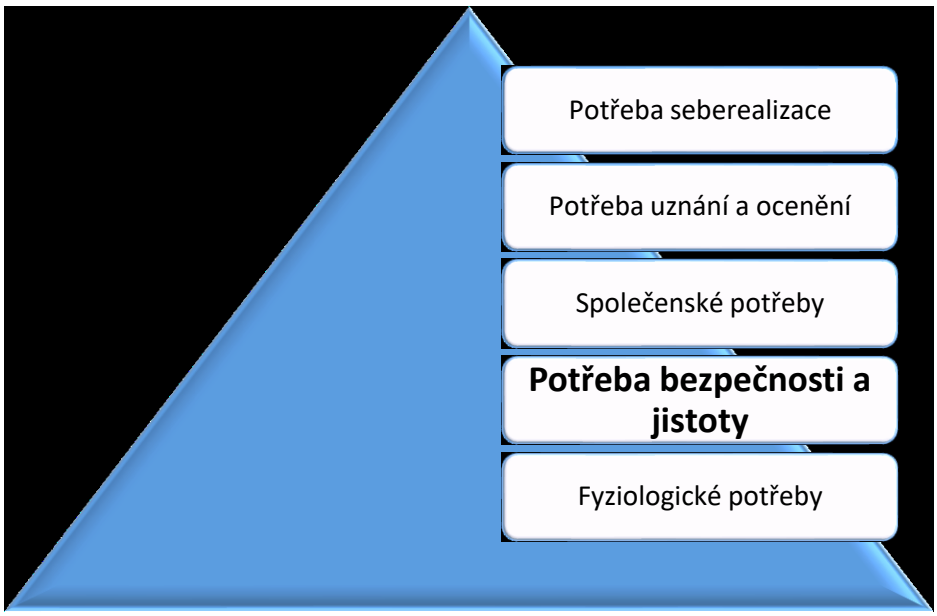
Z toho vyplývá, že bezpečnost lze definovat jako stav, kdy má člověk kontrolu nad rizikovými aspekty, které mohou způsobit případnou škodu.

V anglickém jazyce je pro překlad pojmu využíváno dvou termínů. Jedná se o „security“ a „safety“. Oba zmíněné termíny mají stejný význam slova, přece jen ale vyjadřují jiný druh bezpečnosti. (Lukáš, 2013, s. 27)

Pojem „security“ se týká ochrany jednotlivců, tj. zdraví a života osob, majetku, systému a informací, vysvětlit lze tento pojem také jako fyzické aspekty ochrany. Druhý pojem

„safety“ pak představuje bezpečnost jako ochranu před hrozbami (např. přírodními či antropogenními), které by mohly způsobit škodu. Do této skupiny lze řadit bezpečnost a ochranu zdraví při práci, požární ochranu a jiné. Na rozdíl od prvního pojmu se tak v rámci ochrany jedná spíše o aspekty emocionální. Z výše uvedeného překladu je jasné, že bezpečnosti první – „safety“ nelze dosáhnout, pokud není zaručena bezpečnost druhá – „security“. (Morgan, 2021)

Je třeba si uvědomit, že pocit bezpečí není samozřejmostí. Absence tohoto prvku přidělává lidem a organizacím starosti, skrze které je obtížné dosáhnout kvalitního fungování. Není tak překvapením, že právě pocit bezpečí je jednou ze základních lidských potřeb, které popsal i americký psycholog Abraham Harold Maslow ve své Maslowově pyramidě základních potřeb, která je znázorněna na následujícím obrázku (Obr. 1). Pocit bezpečí nalezneme ihned za fyziologickými potřebami, je tak zřejmé, že bez naplnění této potřeby by nebylo možné vést kvalitní, spokojený život, plný lásky, úcty a seberealizace. (Maslow, 2014, s. 103-115; Nakonečný, 2014, s. 161-170)



Obrázek 1 – Maslowova pyramida potřeb
(Zdroj: A. H. Maslow, zpracování vlastní)

2.2 Informace

Jedním z nejdůležitějších aktiv organizace, která je třeba v souvislosti s bezpečností chránit, jsou informace. Může se jednat o informace týkající se fungování organizace, zákazníků, zaměstnanců, know-how a spousty dalších.

V praxi se můžeme setkat s rozdělením informací do různých skupin a to např. na veřejné a neveřejné informace, důvěrné informace, osobní údaje nebo obchodní tajemství. Nejvýznamnější skupinou, se kterou se setkáváme, jsou utajované informace (dále jen „UI“). Charakterizovat je lze jako veškeré informace, které by v případě zneužití mohly způsobit újmu ČR. Dle Národního bezpečnostního úřadu (dále jen „NBÚ“) se rozdělují do čtyř základních stupňů utajení. Tyto stupně jsou obsaženy v § 4 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen zákon č. 412/2005 Sb., o ochraně UI. Jedná se o klasifikaci UI dle stupně na **vyhrazené, důvěrné, tajné** a **přísně tajné**.

Vyhrazené jsou takové informace, které by v případě zneužití byly nevýhodné pro ČR. Vyzrazení důvěrných informací by pro ČR znamenalo prostou újmu, vyzrazení tajných informací pak vážnou újmu. V případě přísně tajných informací vyzrazení znamená mimořádně vážnou újmu ČR. (Doucek, Konečný a Novák, 2019, s. 185; Zákon č. 412/2005 Sb.)

Podle toho, do jakého stupně utajení je informace zařazena, může být následně v organizaci zajištěn příslušný systém zabezpečení, stejně jako je tomu v souvislosti s informacemi, týkající se zájmů ČR.

UI tak dle druhu zajištění ochrany rozdělujeme na:

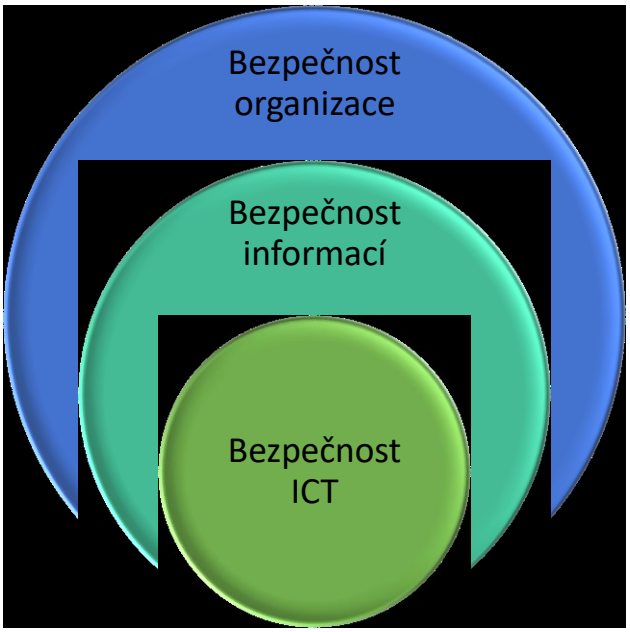
- personální bezpečnost;
- průmyslovou bezpečnost;
- administrativní bezpečnost;
- bezpečnost informačních komunikačních systémů;
- kryptografickou bezpečnost;
- fyzickou bezpečnost. (Kyncl, Konečný a Novák, 2014, s. 86; Zákon č. 412/2005 Sb.)

2.3 Bezpečnost informací

Pro pochopení problematiky této diplomové práce je nezbytné charakterizovat další velmi důležitý pojem – bezpečnost informací. Tento pojem definuje především ochranu důvěrnosti, integrity a dostupnosti informací, může se ale jednat i o zachování autenticity, odpovědnosti, nepopiratelnosti a spolehlivosti. Jedná se tak o ochranu informací všeho druhy různými způsoby.

Informační bezpečnost by v současné době měla být jakkoli zahrnuta v řízení každé organizace. Ta by měla mít ve své organizační struktuře nastavena pravidla, která pomocí opatření a postupů zajistí ochranu informací před změnou či ztrátou, stejně jako stanovení rozsahu osobám oprávněným s informacemi nakládat.

S pojmem bezpečnost informací souvisejí ještě další dva pojmy – bezpečnost organizace a bezpečnost informačních a komunikačních systémů (ICT). Zmíněné tři pojmy vystupují ve vztazích nadřízenosti a podřízenosti, jak je znázorněno na následujícím obrázku (Obr. 2).



Obrázek 2 – Vztah úrovní bezpečnosti v organizaci
(Zdroj: Doucek, 2011, s. 60; zpracování vlastní)

Z Obr. 2 je patrné, že nadřazeným pojmem skupiny pojmů je bezpečnost organizace. Jedná se o zajištění bezpečnosti objektu nebo majetku organizace např. za pomoci ostrahy. Bezpečnost informací a bezpečnost ICT tak nemůže být zajištěna, pokud není zajištěna bezpečnost organizace. Úkolem bezpečnosti informací je zajistit bezpečné nakládání

s informacemi, bezpečné způsoby zpracování dat, jejich uložení v archivu aj. Samotná bezpečnost ICT má pak chránit pouze aktiva, která se týkají informačního a komunikačního systému firmy. Ze zmíněných pojmů tak zaujímá nejmenší část. (Doucek, 2011, s. 59-60)

2.4 Model systému řízení bezpečnosti informací

Bezpečnost informací nemůže fungovat bez řízení. Je nezbytné nastavit takový systém, který dokáže bezpečnost informací účinně a účelně spravovat.

Information Security Management Systém (dále jen „ISMS“), systém řízení bezpečnosti informací, je systém, který vychází z ochrany informací a může být součástí řídících činnostní organizace. Jeho úkolem je snížit rizika související s narušením již zmíněné autenticity, důvěrnosti, integrity a dostupnosti informací organizace. Existuje řada norem, která má za úkol pomoci organizacím zavést a provozovat ISMS. Zmínit je třeba zejména normu ČSN EN ISO/IEC 27001 - Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Tato mezinárodní norma specifikuje požadavky na ustanovení, implementování a neustále zlepšování ISMS v rámci organizace a je tak základním východiskem ISMS. Dle této normy se může řídit jakákoliv organizace, bez ohledu na její velikost, typ nebo povahu činností. Pokud chce organizace dosáhnout shody s touto normou, musí se jí řídit. Jen tak může získat tuto certifikaci.

Dle této normy se ISMS charakterizuje jako:

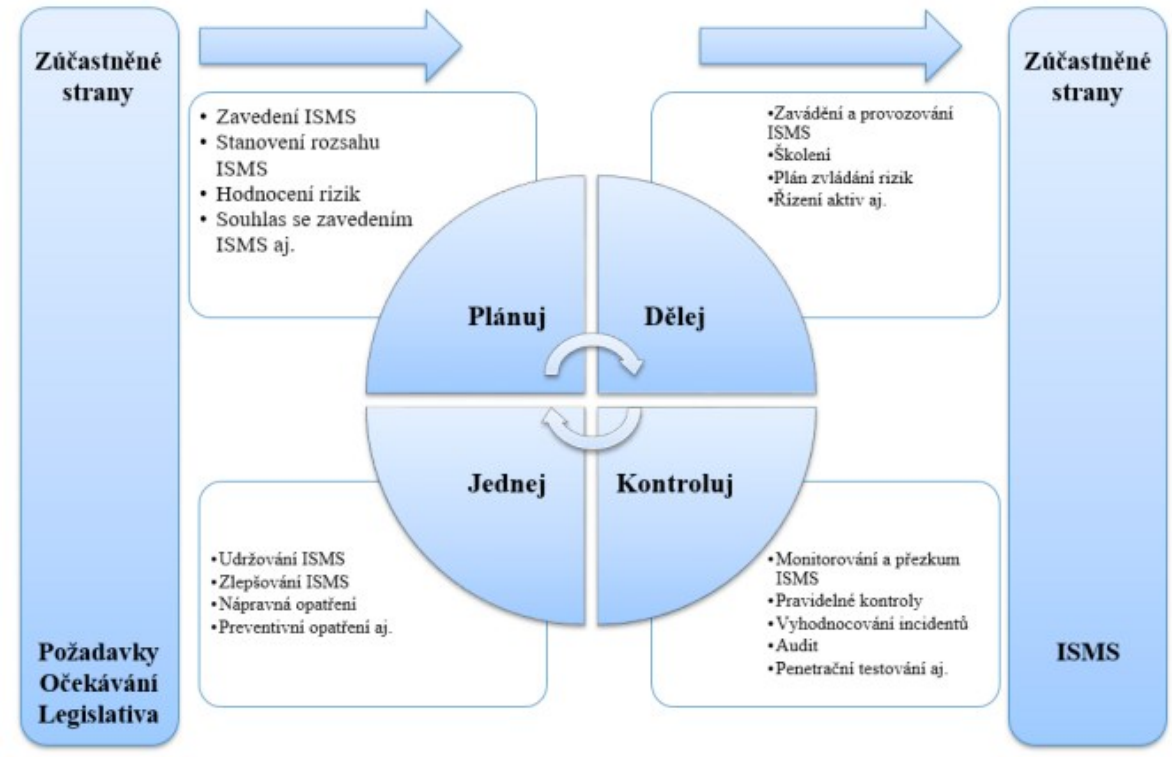
„část celkového systému řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací“. (ČSN EN ISO/IEC 27001)

Hlavním cílem ISMS je tak provádět taková opatření, které přispějí k minimalizaci, či úplnému vyloučení hrozeb. Během celého procesu dochází k řízení a správě aktiv, řízení možných rizik, zavedení opatření a kontrole celého procesu. ISMS je tak systém pod neustálým dohledem manažerů, neboť i činnost celé organizace je s tímto systémem propojena. (Doucek, 2011, s. 95-96; Jirásek, Požár, 2011, s. 2; Kolouch a Bašta, 2019, s. 255-257)

ISMS je systém založený na modelu PDCA (Plánuj – Dělej – Kontroluj – Jednej), tedy čtyřech etapách životního cyklu tohoto systému, kterými jsou:

- Ustanovení (plánuj) – cílem je nastavit objem a hranice, kterých se řízení bezpečnosti bude týkat, dále pak specifikovat manažerské role, ohodnotit rizika a na základě toho zvolit příslušná opatření;
- Zavádění a provoz (dělej) – cílem je navrhnutá opatření zavést a využívat v organizaci;
- Monitorování a přezkoumávání (kontroluj) – tato etapa má zajistit zpětnou vazbu na základě pravidelného sledování a hodnocení procesu ISMS;
- Údržba a zlepšení (jednej) – cílem poslední etapy je realizovat opatření k nápravě a přijetí preventivních opatření v souvislosti s výsledky procesu ISMS. (Kolouch a Bašta, 2019, s. 255-257)

Na následujícím obrázku (Obr. 3) jsou zobrazeny zmíněné etapy ISMS.



Obrázek 3 - PDCA model aplikovaný na procesy ISMS dle ČSN EN ISO/IEC 27001 (Kolouch a Bašta, 2019, s. 255-257)

2.5 ČSN EN ISO/IEC 27002:2014

Budování ISMS představuje trvalou činnost, jelikož se jedná o řízený proces zajištění bezpečnosti. V organizační struktuře musí mít firma zajištěnou spolupráci vedoucích osob, osob odpovědných za aplikační i provozní systémy, osoby odpovědné za jednotlivé činnosti, ale i koncové uživatele. Informační bezpečnost je zajištěna, pokud osoby spolupracují, mají znalosti či průběžně absolvují školení. Největším nebezpečím se totiž v souvislosti se zabezpečením informací stává člověk, který je odpovědný za většinu bezpečnostních incidentů. (Doucek, 2011, s. 95-96; Jirásek, Požár, 2011 s. 2-4)

Vedle základního východiska ISMS normy ČSN EN ISO/IEC 27001 stojí norma ČSN EN ISO/IEC 27002 - Soubor postupů pro řízení bezpečnosti informací. V této normě jsou obsaženy tzv. nejlepší zkušenosti řízení bezpečnosti informací. Obsahuje 133 bezpečnostních opatření, která jsou rozdělena do 11 oblastí (Obr. 4).

Obrázek 4 – Oblasti bezpečnosti informací dle ČSN EN ISO/IEC 27002
(Zdroj: Jirásek, Požár, 2011)

Jak je z Obr. 4 patrné, jednotlivými oblastmi bezpečnosti informací jsou dle této normy:

- Bezpečnostní politika = základní pravidla bezpečnosti informací, týkající se zejména aktiv;
- Organizace bezpečnosti = řízení bezpečnosti informací interních i externích subjektů;

- Řízení aktiv = přehled o existujících aktivech firmy a jejich ochrana;
- Bezpečnost z hlediska lidských zdrojů = vymezení povinností za ochranu informací u zaměstnanců;
- **Fyzická bezpečnost a bezpečnost prostředí** = ochrana zabezpečených oblastí, ať už prostor, nebo zařízení k ochraně jednotlivých prvků v organizaci;
- Řízení komunikací a řízení provozu = zajištění spolehlivého a bezpečného chodu produkčních informačních a komunikačních systémů organizace;
- Řízení přístupu = pravidla pro přidělování přístupu ke jakýmkoliv informačním prostředkům;
- Akvizice, vývoj a údržba informačních systémů = rozvoj bezpečnostních systémů za pomoci různých opatření;
- Zvládání bezpečnostních incidentů = řešení bezpečnostních incidentů dle nastavených pravidel a postupů;
- Řízení kontinuity činností organizace = zajištění prevence a minimalizace škod, která mohou nastat při haváriích, živelných pohromách a dalších mimořádných situací;
- Soulad s požadavky = naplnění požadavků, které vyplývají z právních, smluvních a jiných závazků. (ČSN EN ISO/IEC 27002; Jirásek, Požár, 2011, s. 8-9)

Tato diplomová práce, jak je již z názvu patrné, se bude zabývat oblastí v pořadí pátou, fyzickou bezpečností a bezpečností prostředí, a to zejména ve své praktické části. Je tak vhodné tuto oblast dále rozebrat.

Oblast fyzické bezpečnosti a bezpečnosti prostředí je v ČSN EN ISO/IEC 27002 sestavena tak, aby poskytla návrhy a opatření k zajištění tohoto druhu zabezpečení.

Cílem je zabránit:

- neoprávněnému přístupu do zabezpečených oblastí, poškození, nebo narušení informací;
- poškození či narušení zařízení pro práci s těmito informacemi.

Dále je tato kapitola dělena do 15 hlavních oblastí, kde je vhodné zajistit příslušný stupeň zabezpečení. Těmito oblastmi jsou

- v případě zabezpečené oblasti:
  - Fyzický bezpečnostní perimetr (jemuž bude v praktické části práce věnována největší pozornost);
  - Fyzické kontroly vstupu;
  - Zabezpečení kanceláří, místností a vybavení;
  - Ochrana před vnějšími a přírodními hrozbami;
  - Práce v zabezpečených oblastech;
  - Oblasti pro nakládku a vykládku;
- v případě zařízení potom:
  - Umístění zařízení a jeho ochrana;
  - Podpůrné služby;
  - Bezpečnost kabelových rozvodů;
  - Údržba a zařízení;
  - Přemístění aktiv;
  - Bezpečnost zařízení a aktiv mimo prostory organizace;
  - Bezpečná likvidace nebo opakované použití zařízení;
  - Neobsluhovaná uživatelská zařízení;
  - Zásada prázdného stolu a prázdné obrazovky monitoru.

(ČSN EN ISO/IEC 27002)

3 FYZICKÁ BEZPEČNOST

Jak již bylo zmíněno, bezpečnost, a to zejména fyzická, je jednou ze základních lidských potřeb. S fyzickou bezpečností se setkáváme od pradávna, hlavně tam, kde bylo třeba ochránit majetek.

3.1 Pojem fyzická bezpečnost

Pojem fyzická bezpečnost je však v českém jazyce chápána ve dvojím významu. Tím prvním je nahlížení na tento pojem jako na aktuální stav bezpečí, či nebezpečí. V případě, kdy osoba nabije cenný předmět, je pravděpodobné, že se bude snažit ochránit tento předmět před případným nebezpečím. Dosavadní slabou míru fyzické bezpečnosti tak bude třeba posílit provedením určitých opatření. (Lukáš, 2013, s. 88)

Ve druhém významu se fyzickou bezpečností, dle zákona č. 412/2005 Sb., o ochraně UI rozumí:

„systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat.“ (Zákon č. 412/2005 Sb.)

Maisner a Vlachová pak ve své knize vysvětlují, že cílem fyzické bezpečnosti je zejména:

„zamezení přístupu nepovolaných osob k jednotlivým prvkům infrastruktury, do serveroven, pracovišť správců systému apod. Snahou je vyloučit zcizení majetku přímo i nepřímo souvisejícího s informačním systémem, případně zamezit poškození hmotného i nehmotného vybavení nebo vybavení prostor. V neposlední řadě se snaží zamezit úniku informací a dat.“ (2015, s. 91)

Jedná se tak o soubor bezpečnostních prvků tvořící jeden celek, s cílem zabránit neoprávněnému vniknutí osoby na území organizace a zabránit tak odcizení nebo poškození aktiv (ať už ve smyslu majetku či informací). Těmito prvky jsou například přírodní překážky, mechanické zábranné systémy či jiné zabezpečovací prostředky. Taktéž je vhodné stanovit si fyzický bezpečnostní perimetr, který bude představovat tzv. hranici oblasti, ve které jsou zpracovávány a uchovávány důležité informace a umístěna aktiva. Prioritou zmíněných prvků ochrany však nemusí být vždy jen funkce bezpečnostní, často se jedná pouze o psychologickou funkci, která zajišťuje hlavně odstrašení pachatele. (Baker a Benny, 2013, s. 2-3; Lukáš, 2013, s. 88; Kolouch a Bašta, 2019, s. 282)

Cílem fyzické bezpečnosti je tak pachatele:

- úplně odradit či odstrašit a zabránit tak vniku (v ideálním případě);
- ztížit mu snahu, zpozdit ho a prodloužit tak dobu vniku;
- identifikovat ho, následně zadržet a předat policii. (Lukáš, 2013, s. 90)

Tato diplomová práce se bude zabývat spíše druhým pojetím fyzické bezpečnosti, zejména pak v souvislosti s řízením bezpečnosti informací.

3.2 Systém fyzické bezpečnosti

V souvislosti s MZS je velmi podstatné pokusit se zajistit co nejvyšší míru zabezpečení. Pro organizaci to tak znamená vymezit si určité principy už při samotné realizaci MZS. Jedním z nich je princip vícestupňové ochrany. Jedná se o rozdělení MZS z pohledu ochranných zón, a to na ochranu:

- perimetrickou (obvodovou);
- plášťovou (objektovou);
- prostorovou;
- předmětovou.

Perimetrická neboli obvodová ochrana, zabezpečuje ochranu po obvodu pozemku, jak je ostatně již z názvu patrné. Představuje vymezení katastrálního perimetru přírodními, nebo umělými překážkami. Jedná se o použití překážek v podobě drátěných, bezpečnostních či zděných plotů, brán, branek, řek, závor a různých druhů turniketů.

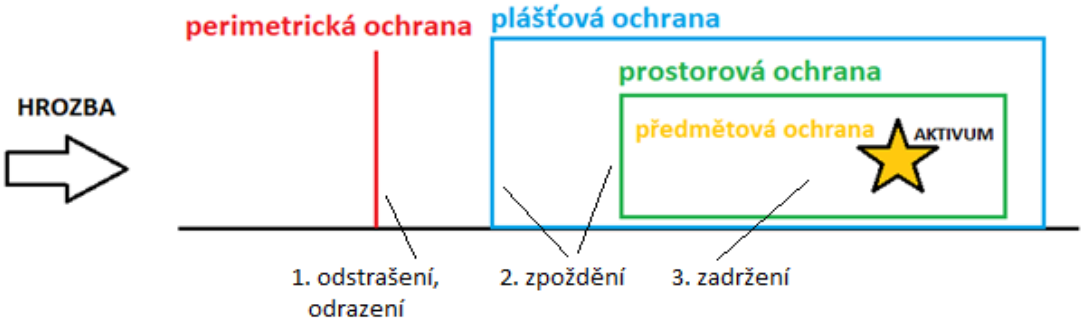
Plášťová ochrana má za úkol zabránit narušiteli vstoupit přes „plášť“ do chráněného prostoru neboli dovnitř budovy. Do této skupiny zařazujeme proniknutí přes stěny, dveře (ať už se jedná o obyčejné, bezpečnostní, pancéřované, protipožární), okna, mříže, zámkové či videodohledové systémy a další.

Prostorová ochrana zajišťuje samotnou místnost objektu střežení a zpomaluje pachateli činnost vniknutí. Tato ochrana se využívá uvnitř budovy, nejčastěji na schodištích, chodbách atd.

Předmětová ochrana chrání samotný objekt střežení, kdy při narušení dochází k vyhlášení poplachu a identifikace narušitele. Tato ochrana je nejčastěji využívána v souvislosti s cennými předměty. Jedná se o využití jak videodohledových a poplachových

zabezpečovacích systémů, tak i například skříňových či komorových trezorů. (Lukáš, 2011, s. 17-18)

Výše uvedené stupně zabezpečení, spolu s hlavními cíli fyzické bezpečnosti jsou vyobrazeny na následujícím obrázku (Obr. 5).



Obrázek 5 - Rozdělení MZS z pohledu ochranných zón
(Zdroj: Lukáš, 2011, s. 91, zpracování vlastní)

Pokud se pachatel jakýmkoli způsobem pokusí překonat vícestupňový zabezpečovací systém, v jeho prolomení sehrávají nejvýznamnější roli jeho znalosti, dovednosti a technické vybavení. Dle zmíněných schopností narušitele následně rozlišujeme čtyři stupně zabezpečení, představující rozdílné riziko. Jedná se o:

- 1. stupeň, vyjadřující nízké riziko;
- 2. stupeň, vyjadřující nízké až střední riziko;
- 3. stupeň, vyjadřující střední až vysoké riziko;
- 4. stupeň, vyjadřující vysoké riziko.

Nízké riziko představuje pro organizaci pachatel, který má malou znalost zabezpečovacích systémů a omezené nástroje. Nízké až střední riziko pak představuje pachatel, který má omezenou znalost zabezpečovacích systémů a běžné nářadí, střední až vysoké riziko pachatel, který je obeznámen se zabezpečovacími systémy a má rozsáhlý sortiment nástrojů potřebných k prolomení. Pachatel, který disponuje podrobným plánem vniknutí a má veškeré nástroje potřebné k úspěšnému vniku, dokonce i náhradní součástky obsažené v zabezpečovacích systémech poté představuje pro organizace vysoké riziko. (Lukáš, 2011, s. 18)

4 OPATŘENÍ FYZICKÉ BEZPEČNOSTI

Aby bylo docíleno zmíněných kroků, je nutné zavést takový systém fyzické bezpečnosti, který by měl prostřednictvím svých ochranných opatření zajistit komplexnost, odolnost, a vícestupňové a automatické zabezpečení.

Zákon č. 412/2005 Sb., o ochraně UI v § 27 rozděluje opatření fyzické bezpečnosti na:

- fyzickou ostrahu;
- režimová opatření;
- technické prostředky. (Zákon č. 412/2005 Sb.)

4.1 Fyzická ostraha

Fyzickou ostrahou se rozumí jedna či více osob, které svou přítomností a speciální připraveností zajišťují ochranu aktiv v organizaci. Nejčastěji se jedná o strážné, hlídací službu či policisty, kteří mají za úkol v případě nebezpečí odhalit a zadržet pachatele a zabránit tak odcizení či poškození aktiv. Toto opatření bývá ve většině případů nejnákladnějším způsobem zajišťování bezpečnosti. (Lukáš, 2011, s. 16; Lukáš, 2013, s. 91)

4.2 Režimová opatření

Režimová opatření vymezují zásady, pravidla a opatření pro vstup a vjezd do objektu, manipulaci s důležitými předměty, systém kontrol materiálu vnášeného i vynášeného atd. (Zákon č. 412/2005 Sb.)

Velký důraz se tak v souvislosti s režimovými opatřeními klade na propracovaný přístupový systém neboli systém kontrol vstupu.

Režimová opatření by měla zajistit požadovaný stupeň bezpečnosti, nikdy by však neměla být nastavena tak, aby výrazně omezovala pohyb osob v organizaci. (Lukáš, 2011, s. 15)

4.3 Technické prostředky

Technické prostředky mají zajistit efektivnější ostrahu i režimová opatření. Cílem je pachatele odradit, nebo mu alespoň jeho činnost výrazně ztížit, prodloužit tak dobu přístupu k aktivu a získat čas na jeho zadržení. Mezi obvyklé technické prostředky zařazujeme:

- **mechanické zábranné systémy** (dále řešené v normě ČSN EN 1627 - Dveře, okna, lehké obvodové pláště, mříže a okenice – Odolnost proti vloupání – Požadavky a klasifikace);
- **poplachové zabezpečovací a tísňové systémy** (dále řešené v normě ČSN EN 50131-1 ed. 2 Poplachové systémy – Poplachové zabezpečovací a tísňové systémy Část 1: Systémové požadavky a ČSN CLC/TS 50131-7 - Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace.
- **videodohledové systémy** (dále řešené v normě ČSN EN 62676-1-1 Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně);
- **systémy kontroly vstupu s elektronickou zabezpečovací signalizací** (dále řešené v normě ČSN EN 60839-11-1 Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty);
- **elektrická požární signalizace** (dále řešené v normě ČSN 73 0875 - Požární bezpečnost staveb – Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení a ČSN 34 2710 - Elektrická požární signalizace – Projektování, montáž, užívání, provoz, kontrola, servis a údržba.

Důležitou roli při fyzickém zabezpečení pak hrají dohledová a poplachová přijímací centra, kterým bude taktéž věnovaná pozornost.

(Lukáš, 2013, s. 91; Kolouch a Bašta, 2019, s. 284; Zákon č. 412/2005 Sb.)

4.3.1 Mechanické zábranné systémy

Nejstarším typem fyzické ochrany jsou mechanické zábranné systémy (dále jen „MZS“). MZS představují mechanickou bariéru před násilným vniknutím nepovolaných osob. Jednoduše řečeno se jedná o prostředky, které dokážou odradit, či alespoň znesnadnit pachateli vstup do objektu. Absence MZS vždy znamená nekvalitní ochranu, jelikož se jedná o nejdůležitější systém zabezpečení.

Každý MZS je překonatelný, nejdůležitější proměnou v souvislosti s překonáváním MZS je však čas.

Doba, kterou potřebuje pachatel na překonání MZS se označuje pojmem průlomová odolnost. Ta se dá také vyjádřit vzorcem:

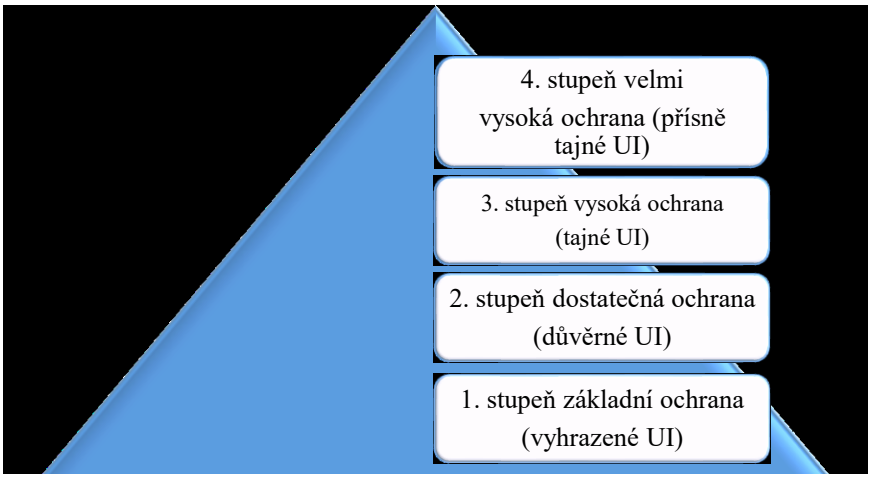
$$\Delta t = t\,2 - t\,1$$

kde Δ t vyjadřuje čas potřebný k překonání MZS, t 1 čas zahájení útoku a t 2 čas dokončení prolomení MZS. Organizace se tak vždy snaží zajistit maximální časový interval vzhledem k použitému MZS. (Uhlář, 2014, s. 10)

Ve spojení s MZS je možné narazit na tzv. pyramidu bezpečnosti. Tato pyramida představuje rozdělení jednotlivých certifikovaných MZS do čtyř stupňů bezpečnosti podle normy ČSN EN 1627 (746001) - Dveře, okna, lehké obvodové pláště, mříže a okenice – Odolnost proti vloupání – Požadavky a klasifikace. Tato norma udává míru odolnosti výrobků např. při násilném vniknutí, tj. hrubém násilí, odvrtání či vytržení apod. Certifikace je vydávána prostřednictvím certifikačních orgánů po prověření MZS akreditovanou zkušební laboratoří. Tyto zmíněné stupně bezpečnosti se následně nachází na obalech výrobků. (ČSN EN 1627)

Pyramida bezpečnosti tedy umožňuje identifikovat jednotlivé certifikované MZS a vyjádřit úroveň jakosti. (Fábera systems s.r.o., 2016)

Na následujícím obrázku (Obr. 6) jsou zobrazeny jednotlivé bezpečnostní třídy (1.-4.), jejich), stupně bezpečnosti (základní, dostatečná, vysoká, velmi vysoká) a stupně utajení dle NBÚ (vyhrazené, důvěrné, tajné, přísně tajné).



Obrázek 6 – Pyramida bezpečnosti

(Zdroj: Ivanka, 2014, s.5; zpracování vlastní)

MZS a jejich mechanické prvky, jak již bylo zmíněno, jsou řazeny mezi základní typ bezpečnosti. Těmito prvky jsou nejčastěji:

- závory, mříže;
- ploty, brány, turnikety;
- zámkové systémy;
- bezpečnostní dveře a kování;
- bezpečnostní skla;
- pokladny, trezory, bezpečnostní skříně (Ivanka, 2014, s. 4)

Paul R. Baker ve své knize označuje za jeden z důležitých mechanických prvků bezpečnosti také celkové osvětlení objektu. Jedině tak je totiž zajištěn vizuální kontakt s objektem v době, kdy je tma. Osvětlení objektu by mělo zajistit odstrašení pachatele, který se pokusí využit tmy právě k vniknutí do objektu. Osobám ostrahy to pak umožní připravit se na obrannou akci, zatímco se prozatím nacházejí v bezpečné vzdálenosti. Osvětlení je však považováno i jako psychologický odstrašující prostředek pro jednotlivce, kteří hledají příležitost ke spáchání trestné činnosti. (2013, s. 52)

4.3.2 Poplachové zabezpečovací a tísňové systémy

Poplachové zabezpečovací a tísňové systémy (dále jen „PZTS“) se označují jako elektronické systémy, jejichž úkolem je ve střeženém prostoru monitorovat veškerou činnost a v případě neoprávněného vstupu do objektu signalizovat nebezpečí – poplach. K tomu jsou využívány detektory narušení.

Detektor narušení

Dle ČSN EN 50131-1 ED. 2 můžeme detektor narušení charakterizovat jako:

„zařízení konstruované ke generování signálu nebo zprávy o vniknutí, jako reakci na nenormální stav detekující přítomnost nebezpečí“. (ČSN EN 50131-1 ED. 2)

Jedná se tak o zařízení, které určitým způsobem reaguje na změny – fyzikální jevy. Konstrukce detektoru tvoří senzorická monitorovací část, řídící část, vyhodnocovací a komunikační jednotka.

Detektory můžeme rozdělit dle různých hledisek, např. dle:

- způsobu napájení (napájené, nenapájené);

- charakteru střežené oblasti (prostorové, směrové, bariérové, polohové);
- tvaru detekční charakteristiky (se standartním rozsahem, s širokoúhlým rozsahem, s kruhovým rozsahem, se svislou bariérou, s vodorovnou bariérou, s dlouhým rozsahem);
- použitého fyzikálního signálu (elektromechanické, elektromagnetické, elektroakustické).

Elektromechanické detektory se vyznačují tím, že k detekci narušení využívají mechanickou změnu. Jedná se tak například o posuvný pohyb, který způsobí sepnutí nebo přerušení obvodu, nebo mechanická chvění způsobená pohybem narušitele. **Elektromagnetické** detektory fungují na principu elektromagnetických vln, které detektory vysílají. Jakákoliv změna je prostřednictvím jednotlivých detektorů vyhodnocována a v případě narušení přeměněna na elektrický poplachový signál. **Elektroakustické detektory** využívají ke své činnosti akustické vlny. Nejčastěji se jedná o situace, kdy detektory vyhodnocují změnu kmitočtu odražených akustických vln nebo se analyzují přijaté akustické signály. (Lukáš, 2011, s. 15-96)

Důležité je však zmínit skutečnost, že pokud nejsou informace o nebezpečí řádně a včas doručeny určeným osobám, stávají se PZTS prakticky neúčinné. Nejdůležitějším prvkem při narušení bezpečnosti je totiž právě rychlost přenesení informace o narušení a následná reakce zpracovatele. Tímto způsobem může dojít k případné eliminaci škod.

PZTS jsou nejčastěji tvořeny ústřednou, optickými či akustickými složkami a zmíněným detektorem narušení. Ústředna přijímá informace vysílané z jednotlivých detektorů narušení (využívá se i pojmů jako senzor, čidlo), vyhodnocuje je a případně vyhlašuje poplach.

PZTS jsou v dnešní době stále málo využívaným systémem, ačkoli jsou finančně celkem přívětivé. Můžeme se setkat s drátovou či bezdrátovou variantou tohoto zabezpečení. PZTS lze dělit dle přenosu, přes:

- pevnou telefonní síť;
- GSM síť v hovorovém pásmu nebo přes SMS;
- radiovou síť;
- internet.

Nejčastěji se využívají prostorové detektory a snímače, které pracují na různých principech. PZTS se instalují v rámci perimetrické, plášťové, prostorové i předmětové ochrany. V případě narušení se tato skutečnost oznamuje např. sirénou s majákem nebo zasláním poplašné zprávy na předem dohodnuté telefonní číslo. Poplach bývá spuštěn i pokud se pachatel pokusí detektor či snímač zničit.

Podrobné údaje o činnosti PZTS jsou uvedeny v normách ČSN EN 50131-1 a ČSN CLC/TS 50131-7. (Lukáš, 2011, s. 101-102; Kyncl, Konečný a Novák,2014, s. 174-175)

4.3.3 Videodohledové systémy

Videodohledové systémy (dále jen „VDS“) jsou bezesporu jedním z nejrychleji se rozvíjejících systémů. Vysoká kvalita záznamu a jednoduchá obsluha jsou hlavním důvodem oblíbenosti. Pomocí VDS je možné okamžitě získat přehled o aktuální situaci a následně ji pak správně vyhodnotit. Zakomponování VDS do zabezpečení organizace je v dnešní době již samozřejmostí. VDS lze používat jak samostatně, např. v souvislosti s monitorováním obchodu, či v integraci s dalšími systémy. Při zvažování návrhu a výběru VDS musí vzít návrhář v úvahu individuální potřeby každého zákazníka. Často se setkáváme s kombinací VDS spolu se systémem PZTS nebo s perimetrickým zabezpečením. VDS podléhají normě ČSN EN 62676-1-1 Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně.

V souvislosti s pokrokem v oblasti informačních technologií, přesněji přenosových sítí, je nejběžnějším VDS tzv. Internet Protocol, tedy přenos přes IP kamery. Tyto zařízení obsahují software, prostřednictvím kterého je možné kameru připojit k počítačové síti. Toto připojení zajistí, že uživatel může sledovat obraz v internetovém prohlížeči kdekoliv na světě se zrovna nachází. Pokud se jedná např. o dálkově polohovatelnou kameru s pohybem otáčení/naklánění a zoomem objektivu, pak se poloha kamery ovládá pomocí příkazů odeslaných z počítače uživatele nebo řídicího centra přes síť přímo do kamery.

VDS mohou fungovat na principu přenosu obrazu v aktuálním čase (maximálně s drobným zpožděním způsobeným přenosem) bez uložení, tzn. pokud se vyskytne problém, je nezbytné, aby byl zpozorován v danou chvíli a ihned řešen. Rozdílným typem VDS jsou zařízení, které zachycují obraz a rovnou ho ukládají. Tímto způsobem je tak možné vyhledávat nebo přehrávat video, které není snímáno v reálném čase.

Analýza obrazu je pak využívána zejména v souvislosti s:

- ochranou perimetru;
- detekcí pohybu;
- rozpoznávání (např. osob, SPZ atd.);
- detekcí zakrytí kamery;
- detekcí krádeže, či zanechání předmětu (v případě např. terorismu);
- různými druhy počítadel.

Na trhu existuje značné množství kamer, velmi často jsou pak využívány zejména specializované kamery na rozpoznávání SPZ, které jsou citlivé na reflexní vrstvu štítků vozidel. Takto speciálně navršené kamery tak představují vynikající příležitost provádět kontrolu vstupu do objektu pasivním způsobem.

Další ze skupiny kamer jsou termokamery, které fungují na bázi infračerveného záření. Jsou schopné pomocí odpočtu zachytit různé teplotní hodnoty. Využívají se zejména v souvislosti s měřením osob, ale i třeba teplotou místnosti.

VDS obsahují často funkci den/noc, kdy automaticky dochází k vyhodnocení světelných podmínek a následnému přepnutí barev do černého či bílého režimu. (Baker, 2013, s. 123-164; Kyncl, Konečný a Novák, s. 188-190; Securitas ČR s.r.o., 2021)

4.3.4 Systémy kontroly vstupů s elektronickou zabezpečovací signalizací

Systémem kontroly vstupů (dále jen „SKV“) se rozumí soubor postupů, které vznikají v souvislosti se snahou zajistit bezpečnost při vstupu do zabezpečeného objektu prostřednictvím jednotlivých opatření (systémová, fyzická, mechanická, elektronická). Dochází zde k řízení a evidenci veškerých přístupů na základě přidělených přístupových práv. Dle toho následně dochází k identifikaci osoby a povolení či zamítnutí vstupu. Opatření mohou být např. fyzická ostraha, mříže, zámky, turnikety a další.

SKV s elektronickou zabezpečovací signalizací je možno nalézt v ČSN EN 60839-11-1 (334593) - Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty. V této normě jsou mimo jiné obsaženy základní funkce těchto SKV, kterými jsou:

- identifikace a zpracování dat;
- programovatelnost a ovládání místa přístupu;
- styk a komunikace se vstupujícími osobami a
- poskytování hlášení o aktuálním stavu. (ČSN EN 60839-11-1)

Kontrolu přístupu tak nejčastěji zajišťujeme prostřednictvím čipových karet (karty vybavené mikročipem s pamětí) nebo pomocí elektronického klíče (uzamykací systém složený z klíče s mikroprocesorem, zámku a elektroniky). Dalšími způsoby, jak je možné zajistit identifikaci je např. heslem, které subjekt zná nebo třeba vlastním obličejem. Zmíněné identifikační prostředky následně osoba využije k projití přes zařízení, např. turniket, závory atd.

SKV je možné propojit i s dalšími systémy, jako např. s docházkovým systémem, PZTS, elektrickou požární signalizací, VDS a dalšími.

Existuje celá řada dalších SKV, to, jaký systém bude zvolen závisí na mnoha faktorech, jako např. charakter objektu, rizika, požadovaný stupeň zabezpečení atd. (ČSN EN 60839-11-1; Lukáš, 2011, s. 123-124; Kolouch a Bašta, 2019, s. 462-464; Kyncl, Konečný a Novák, s. 192-196)

4.3.5 Elektrická požární signalizace

Elektrická požární signalizace (dále jen „EPS“) je zařízení, sloužící k včasné signalizaci vzniklého požáru, nebo v lepším případě k prevenci vzniku požáru. K detekování jsou využívány hlásiče umístěné v místnostech, které v případě aktivace vysílají prostřednictvím hlásících linek informaci do ústředny. Na základě toho dojde prostřednictvím napojení dohledového a poplachového centra (bude vysvětleno v další podkapitole) k přivolání jednotky požární ochrany. Při aktivaci evakuačního systému dochází také k signalizaci, ať už optické či akustické, kdy jsou nejčastěji využívány majáky a sirény. V organizaci se tímto způsobem zajistí seznámení všech osob s hrozícím nebezpečím, jako další dochází k opatřením zabraňujícím další šíření požáru.

Nejvýznamnější funkci při vzniku požáru tak zastávají hlásiče – detektory, které mohou být:

- **tlačítkové**, využívané tam, kde se nacházejí osoby, které v případě vzniku požáru promáčknou sklo a zmáčknou tlačítko;
- **samočinné**, reagující na změny fyzikálních veličin (teplota, kouř, plamen, plyn);

- **ionizační,** měřící vodivost v ionizační komoře, při překročení dochází k poplachu;
- **opticko-kouřové,** využívající LED diodu;
- **teplotní,** reagující na rychlost nárůstu teploty v místnosti.

Existuje několik druhů EPS. Nejčastěji se setkáváme s rozdělením na jednostupňové či vícestupňové, lišící se v počtu vedlejších ústředen, a dále pak na EPS s kolektivní či individuální adresací, kdy základní rozdíl spočívá v identifikaci konkrétního hlásiče – u kolektivního nelze přesně určit.

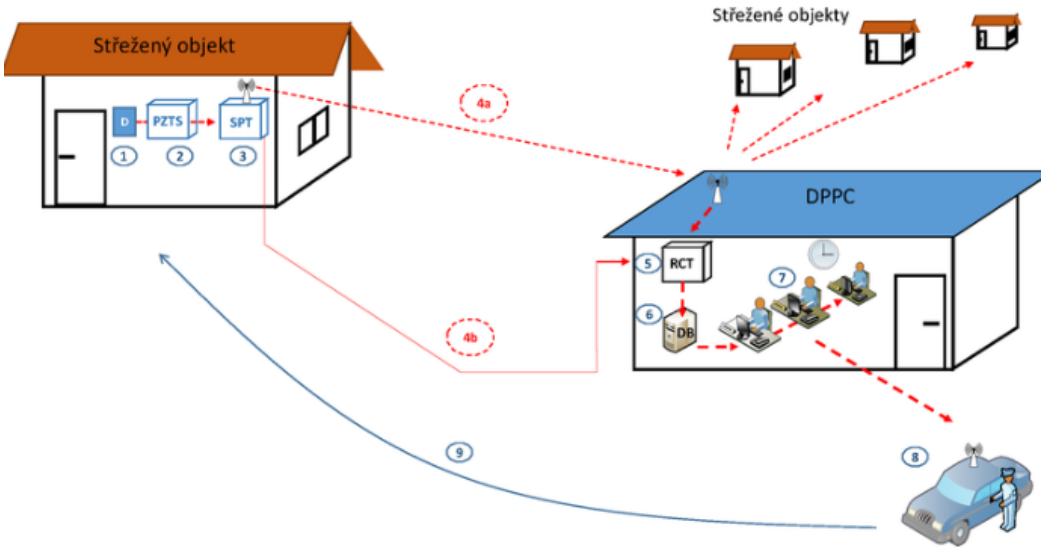
EPS tak lze definovat jako komplexní systém, který by měl rychle a spolehlivě zajistit místo určení požáru, vyhlášení poplachu, aktivaci evakuačního systému a následně přivolání jednotky požární ochrany.

EPS podléhají technickým normám ČSN 73 0875 - Požární bezpečnost staveb – Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení a ČSN 34 2710 - Elektrická požární signalizace – Projektování, montáž, užívání, provoz, kontrola, servis a údržba. (Lukáš, 2011, s. 148; Kyncl, Konečný a Novák, s. 176)

4.3.6 Dohledová a poplachová přijímací centra

V dnešní době již existuje možnost připojení vlastní organizace na dohledové a poplachové přijímací centrum (dále jen „DPPC“) a zajištění tak 24hodinové ochrany. Tento způsob je z pohledu bezpečnosti mnohem účinnější a uživatelsky přívětivější, než kdyby si musela organizace řešit potencionální výstražný signál v rámci zabezpečení sama. Profesionální dispečerské pracoviště přijímá z připojených objektů signály, vyhodnocuje situace a v případě potřeby řídí zásah. Jednotlivé organizace si mohou zvolit ze širokého rozsahu a možností těchto center. DPPC fungují v souladu s ČSN EN 50518 – Dohledová a poplachová přijímací centra. (Urban, 2019)

Na následujícím obrázku (Obr. 7) je možné vidět, jak probíhá činnost DPPC.



Obrázek 7 – Schéma DPPC

(Zdroj: Urban, 2019)

Jak je z Obr. 7 patrné, činnost DPPC probíhá již od samotného momentu, kdy detektor zjistí narušení objektu. PZTS tuto informaci vyhodnotí a předá ji přenosovému zařízení střeženého prostoru. Tato informace je následně prostřednictvím přenosové trasy předána přijímacímu centru DPPC, které ji zpracuje, vyhodnotí a předá operátorovi. Ten postupuje podle předem daných instrukcí. Pokud se v těchto instrukcích nachází i informace o nutnosti vyslání zásahové jednotky, operátor jednotku informuje a ta provede zásah na objektu. (Urban, 2019)

Dílčí závěr

Všechny výše zmíněné technické prostředky představují komplexní systém zabezpečení, jehož vývoj jde neustále dopředu. Nové materiály používané k vytvoření tohoto systému stejně jako nová konstrukční řešení vytvářejí obtížnější překážky pro pachatele. Ten musí vynaložit větší úsilí k překonání těchto překážek, potřebuje mnohem více informací a zkušeností a dochází i k prodlužování času, který potřebuje na prolomení systému zabezpečení.

Každá organizace by vždy při návrhu zabezpečovacího systému měla přemýšlet o tom, jakým způsobem je třeba aktivum ochránit. Taktéž by měla brát ohled na to, kde se aktivum nachází, proč je třeba ho chránit a před kým a tomu pak přizpůsobit případný systém zabezpečení. Stejně tak by měla úroveň jednotlivých ochran odpovídat hodnotě aktiva, aby nedocházelo k tomu, že bude systém zabezpečení nákladnější než samotné aktivum.

Neexistuje jeden nejvhodnější model zabezpečení a je tak potřeba pohlížet na aktiva individuálně. (Ivanka, 2014. s. 37)

Prvním úkolem každé organizace při navrhování fyzického zabezpečení je zaměřit se na to, jaká aktiva je potřeba ochránit. Následně je vhodné vytvořit si analýzu rizik, která umožní odhalit a pochopit rizika související s danými aktivy. Pomocí tohoto nástroje by si organizace měla rizika vyhodnotit a pokusit se zvolit taková opatření, která povedou ke snížení či vyhnutí se riziku.

II. PRAKTICKÁ ČÁST

5 CHARAKTERISTIKA SOUČASNÉHO STAVU VYBRANÉHO OBJEKTU

Další kapitola diplomové práce se bude zaměřovat na aktuální stav fyzického zabezpečení vybraného subjektu, přesněji pak na bezpečnost informací v tomto subjektu. S ohledem na charakter zvoleného tématu a s tím související zajištění mlčenlivosti o jejím zabezpečení, nebude tento subjekt jmenován.

Vybraný subjekt byl vybrán na základě vlastního uvážení, zejména z důvodu nedostatečného fyzického zabezpečení, a tudíž širokého spektra návrhů ke zlepšení tohoto zabezpečení.

Na příkladu vybraného subjektu, který bude představen, dojde k analýze aktuálního stavu systému fyzického zabezpečení informací s přihlédnutím k ČSN EN ISO/IEC 27002.

Nejvíce se bude tato kapitola diplomové práce zaměřovat na fyzický bezpečnostní perimetr, ostatní části oblasti fyzické bezpečnosti a bezpečnosti prostředí z ČSN EN ISO/IEC 27002 budou taktéž rozebrány, ne však už v takovém rozsahu.

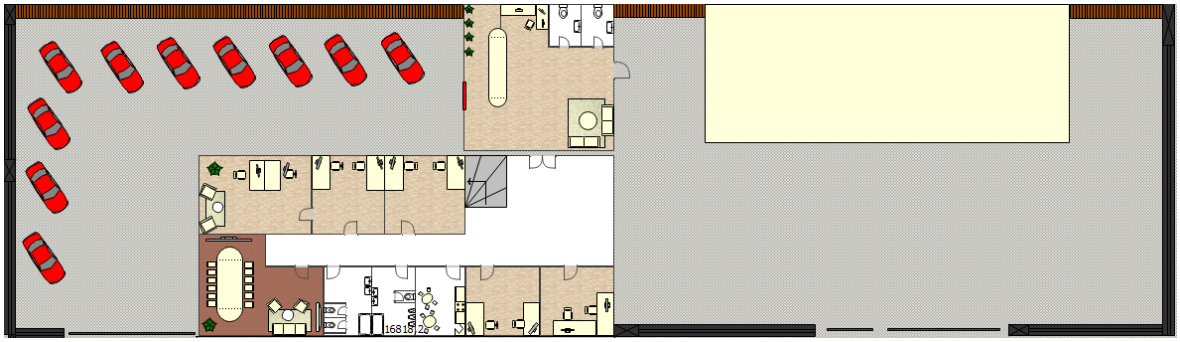
5.1 Základní údaje – popis objektu

Vybraný objekt, který bude nyní analyzován, se nachází v Brně, v městské části Brno - střed. Jedná se o volně stojící budovu ve tvaru písmene L s areálem. Objekt je situován v rušné části města, nedaleko centra. V přední části objektu se nachází čtyřproudá silnice, podél zadní části pak vede řeka. Areál po pravé straně sousedí s autobazarem. Nalevo od areálu je v současné době volné prostranství.

Obvod areálu je z největší části tvořen drátěným plotem, zbytek betonovou zdí. Ve výstavbě má subjekt novou budovu, která stojí taktéž v areálu. Po jejím dokončení se tato modernější budova stane primárním sídlem firmy. Momentálně se ale zatím veškerá činnost provádí v budově původní, starší. Součástí areálu je i parkoviště pro 10 automobilů. Do objektu firmy je možné vjet bránou podél levé strany budovy, ze směru od čtyřproudé silnice. Tento vjezd funguje jako hlavní. Vstoupit do areálu můžeme ještě brankou, nacházející se u pravé části budovy. V této části je taktéž vjezdové brána, v současné době tato brána slouží pro vjezd vozidel zabezpečující výstavbu nové budovy. Přímo do budovy vybraného subjektu je pak možné vstoupit taktéž ze dvou stran. První vchod, hlavní, disponující recepcí, najdeme z levé strany budovy po příchodu přes parkoviště. Tento vchod slouží primárně ke vstupu všech osob do objektu firmy. Do objektu je možné vstoupit i vchodem z pravé strany budovy, tento vchod je však obvykle uzavřen, klíče od něj jsou uloženy na recepci.

Je určen zejména jako jeden z únikových východů, využívá se hlavně pokud je potřeba projít skrz budovu do pravé části areálu.

Orientační plánek celého objektu je vyobrazen na následujícím obrázku (Obr. 8)



Obrázek 8 - Orientační plánek objektu

Zdroj: vlastní

Budova, ve které sídlí vybraný subjekt, má dvě podlaží. Na následujícím obrázku (Obr. 9) můžete vidět přízemí, kde se nachází zejména recepce, briefingová místnost a kanceláře.

Obrázek 9 - Orientační plánek budovy – recepce a přízemí

Zdroj: vlastní zpracování

Na Obr. 10. je vyobrazeno 1. patro budovy vybraného subjektu, tvořené kancelářemi.

Obrázek 10 - Orientační plánek budovy – 1. patro

Zdroj: vlastní zpracování

Vybraný subjekt je firmou podnikající v oblasti chemického a farmaceutického průmyslu, který byl založen v roce 1998. V současnosti má 23 zaměstnanců, pracující na plný úvazek a tři zaměstnance pracující na úvazek částečný.

Subjekt disponuje služebními vozidly, stolními počítači, notebooky, služebními mobilními telefony a dalším typickým vybavením kanceláří.

5.2 Současná zabezpečení a opatření na zabezpečení dle ČSN EN ISO/IEC 27002

V této části diplomové práce budou představeny opatření a návrhy fyzického zabezpečení vycházející z normy ČSN EN ISO/IEC 27002 spolu s popisem aktuálního stavu fyzického zabezpečení v rámci vybraného subjektu. Zjištěná data budou následně podkladem pro provedení komparace těchto dvou částí a navrhnutí opatření ke zlepšení. Budeme vycházet z jednotlivých oblastí této normy. Rozděleny budou do dvou hlavních celků, fyzické bezpečnosti a bezpečnosti zařízení.

5.2.1 Fyzická bezpečnost

Fyzická bezpečnost se týká ochrany veškerých fyzických aktiv firmy proti neoprávněnému vniknutí, poškození, či zničení. Jedná se tak především o ochranu celého objektu firmy.

Fyzický bezpečnostní perimetr

ČSN EN ISO/IEC 27002 ve svém odstavci 11.1.1 říká, že by měly být definovány bezpečnostní perimetry v rámci těch oblastí, kde se nacházejí kritické či citlivé informace. Zváženy by měly být tyto pokyny:

- měly by se určit bezpečnostní perimetry, jejich síla a umístění by se měly odvíjet od ohodnocených aktiv a rizik s tím souvisejících;
- perimetry by měly být fyzicky v pořádku, tzn. neměly by být porušeny, vnější zastřešení, stěny a podlahy by měly být z pevné konstrukce; dveře by měly být chráněny pomocí mechanismů jako např. zámky, mříže, alarm; dveře a okna by měly být v nepřítomnosti zavřeny, v úvahu by se měla vzít i další ochrana, zejména pak jedná-li se o okna v přízemí;
- fyzický přístup k místu nebo budově by měl být omezen pouze na personál oprávněný ke vstupu do objektu, dohlížet by na to měla obsluha recepce či jiné prostředky pro řízení vstupu;

- měly by být využity fyzické bariéry všude tam, kde je to účelné;
- požární dveře v celém objektu by měly být chráněny alarmem, monitorovány a testovány tak, aby byly v souladu s požárními předpisy;
- dle norem by měly být nainstalovány vhodné systémy detekce průniku tak, aby byly zajištěny dveře a okna, oblasti, které nejsou využité by pak měly být zajištěny alarmem;
- nemělo by docházet ke spojení vybavení pro zpracování informací spravované organizací a spravované externími stranami. (ČSN EN ISO/IEC 27002)

V rámci definování bezpečnostních perimetrů u vybraného subjektu, je nutné se v první řadě zaměřit na celkové fyzické zabezpečení. Struktura a rozdělení fyzického zabezpečení bude provedeno v souladu se čtvrtou kapitolou teoretické části této diplomové práce týkající se opatření fyzické bezpečnosti. Pro připomenutí se jedná o opatření fyzické bezpečnosti rozdělené na:

- Fyzickou ostrahu;
- Režimová opatření;
- Technické prostředky
  - Mechanické zábranné systémy;
  - Poplachové zabezpečovací a tísňové systémy;
  - Videodohledové systémy;
  - Systémy kontroly vstupu s elektronickou zabezpečovací signalizací;
  - Elektrická požární signalizace.

Jednotlivé oblasti fyzické bezpečnosti jsou propojené, nebo spolu úzce souvisí. Při popisu aktuální situace tak nebude možné vycházet přesně z výše uvedených bodů.

Fyzická ostraha je v rámci subjektu zabezpečována mimo pracovní dobu, od 18. do 7. hodiny. Tato osoba ve stanoveném čase dohlíží na bezpečnost uvnitř i v okolí firmy. Jejím úkolem, mimo všeobecný přehled o aktuální situaci ve firmě, je provádění obchůzek a sledování obrazu z kamerových zařízení v místnosti, která rozšiřuje prostor recepce.

Hlavním úkolem **režimových opatření** je vymezit zásady, pravidla a opatření pro vstup a vjezd do objektu. V každém případě by tak měl být zajištěn určitý systém kontrol vstupu. Ve vybraném subjektu je kontrola vstupu prováděna prostřednictvím pracovníka recepce, jehož povinností je provádět kontrolu vstupujících osob a celkově dohlížet na pohyby osob ve firmě. Bližší podrobnosti budou zmíněny v dalších částech práce.

Technické prostředky zabezpečení, jak bylo již zmíněno, můžeme rozdělit na pět skupin. Tyto skupiny si postupně rozebereme.

Co se týká mechanických zábranných systémů, z výše uvedených informací víme, že se areál subjektu nachází v zastavěné části města Brna. Tento areál je z poloviny ohraničen obvodovou zdí, zbytek tvoří drátěný plot vysoký 180 cm. Na několika místech je plot poškozen, pletivo je uvolněné, navíc se v něm nacházejí otvory.

K hlavnímu vjezdu a vstupu do areálu je určena posuvná mechanická brána, nacházející se po levé straně od budovy, která zůstává mezi 7. a 18. hodinou otevřená. Otevření a zavření této brány na začátku a konci směny zajišťuje pracovník ostrahy.

V celé firmě jsou plastová okna, osazena izolačními dvojskly. V přízemí jsou na oknech mříže. Druhé patro před případnými pachateli nijak chráněno není.

Vybraný subjekt využívá pro hlavní vstup do firmy bezpečnostní dvoukřídlé automatické dveře, vyrobené firmou Trido. Skládají se z pohonu včetně pojezdu, motoru jako řídící jednotky, řemenu a elektromechanického zámku. Využit je zde systém automatického otvíraní dveří, reagující na blížící se osoby. Jelikož tyto dveře slouží i jako dveře bezpečnostní, je u nich na spodní části, uvnitř, namontován přídavný podlahový zámek. Zůstávají odemčené v pracovní době, případně pokud je ve firmě někdo přítomen mimo tuto dobu.

Dveře do jednotlivých kanceláří jsou běžného typu, dřevěné, využívané pro kancelářské prostory, vybavené klasickým zámkovým systémem FAB. Zde prý vybraný subjekt do budoucna uvažuje o výměně za jiný, novější typ.

Areál je po setmění dostatečně osvětlen.

Poplachový zabezpečovací a tísňový systém není ve vybraném subjektu nijak řešen.

Co se týká VDS, ve vybraném subjektu se nachází dvě analogové kamery se záznamem, z nichž jedna snímá prostor parkoviště a hlavní vstup do objektu a druhá pravou stranu objektu, kde v současné době probíhá výstavba nových prostor firmy. Výstupy z VDS jsou

přenášeny na stolní počítač, nacházející se v přízemí, těsně vedle recepce v polootevřené místnosti.

Vybraný subjekt nedisponuje systémem kontroly vstupů s elektronickou zabezpečovací signalizací. Na kontroly vstupu, jak již bylo zmíněno, v pracovní době dohlíží pouze pracovník recepce. Každý zaměstnanec vlastní kartu s osobními údaji a svojí fotografií, která slouží jako průkaz ke vstupu do firmy. Tuto kartu by dle vnitřních norem firmy měl nosit na viditelném místě.

Ve všech místnostech vybraného subjektu se nacházejí autonomní hlásiče požáru (kouře), které detekují potencionální požár a vyvolají poplach. U únikových cest pak nalezneme tlačítkové hlásiče požáru, které mají v případech nouze zajistit stejnou funkci. Jsou umístěny na dosažitelném a přístupném místě.

Na chodbách, v každém patře, se pak nachází práškové hasicí přístroje.

Fyzické kontroly vstupu

Dle zmíněné normy by měl být vstup chráněn takovými opatřeními, aby se zajistilo, že přístup do organizace budou mít pouze oprávněné osoby. Zváženy by měly být tyto opatření:

- mělo by docházet k zaznamenávání data a času příchodu a odchodu jednotlivých osob, pokud by se jednalo o návštěvníky, vždy by měly být doprovázeni zaměstnanci, pokud jim již dříve nebyl udělen přístup, v souvislosti s návštěvníky by měla být prověřována jejich totožnost;
- přístup do oblastí, kde se zpracovávají důvěrné informace by měl být omezen pouze v rámci oprávněných osob, zvážen by měl být systém např. přístupových karet a tajných PINů; v případě pracovníků podpory externí strany by měl být pouze omezený přístup; přístupová práva do všech oblastí by měla být řádně přezkoumávána a pravidelně aktualizována;
- v bezpečí by měla být zachována fyzická kniha záznamů či auditní seznam všech přístupů;
- zaměstnanci a smluvní či externí strany by měly viditelně nosit určitou formu označení, pokud se např. zaměstnanci setkají v objektu s někým, kdo označení mít nebude, měly by tuto skutečnost ohlásit. (ČSN EN ISO/IEC 27002)

Fyzická kontrola vstupů je ve vybraném subjektu v pracovní době zajišťována především prostřednictvím pracovníka na recepci, který dohlíží na vstup osob do objektu hlavním vstupem. Pokud do objektu vstoupí cizí osoba, pracovník recepce by ji měl legitimovat, zapsat do knihy a oznámit její návštěvu určenému zaměstnanci. Ten by si pro osobu měl osobně přijít.

Časy příchodů a odchodů zaměstnanců firmy nijak zaznamenávány nejsou.

Subjekt má pro své zaměstnance zřízenou kartu s osobními údaji a fotografií, kterou by se měly při příchodu do firmy a odchodu z firmy legitimovat. Jedná se však o malou firmu, pohyb zaměstnanců a návštěvníků je zde nízký.

Zabezpečení kanceláří, místností a vybavení

V rámci zabezpečení kanceláří, místností a vybavení by dle normy mělo dojít k následujícím opatřením:

- klíčové vybavení organizace by mělo být umístěno tak, aby k němu neměla přístup veřejnost a zabránilo by se tak viditelnému či slyšitelnému úniku důvěrných informací;
- pokud je to možné, budovy by měly být nenápadné tak, aby neposkytovaly žádné informace o svém účelu;
- interní telefonní seznamy a adresáře by měly být lehce přístupné pro kohokoliv bez oprávnění. (ČSN EN ISO/IEC 27002)

Budova vybraného subjektu není navenek nijak nápadná, veškeré důvěrné informace jsou umístěny v kancelářích zaměstnanců, zařízení zpracovávající tyto informace nejsou umístěny tak, aby k nim měl kdokoliv přístup.

Ochrana před vnějšími a přírodními hrozbami

Každá organizace by dle této normy měla mít v rámci své organizace specialistou navržené doporučení, jak minimalizovat následky škod způsobených přírodními katastrofami (tj. požáry, záplavy, zemětřesení), zlomyslnými útoky (tj. výbuchy, občanské nepokoje) nehodami či jinými formami přírodních či člověkem způsobených pohrom. (ČSN EN ISO/IEC 27002)

Vybraný subjekt používá místní zálohu dat na NAS (Network Attached Storage) v budově firmy. Tato data jsou dále ukládána na cloudové uložiště pro firemní klientelu (OneDrive).

Přístup a integrita dat je periodicky testovaná pověřeným pracovníkem a výsledky testů jsou evidovány a sdíleny s vedením firmy.

Práce v zabezpečených oblastech

Dle zmíněné normy by neměla být práce v zabezpečených oblastech prováděna bez dohledu. Personál by si měl být vědom skutečnosti, že v těchto oblastech by měla být prováděna činnost pouze k získání potřebných informací. Dále by v souvislosti s prací v zabezpečených oblastech nemělo být povoleno používat jakékoli záznamové zařízení, pokud není stanoveno jinak. Prázdné oblasti by měly být uzamčeny a pravidelně kontrolovány. (ČSN EN ISO/IEC 27002)

Vybraný subjekt nespadá do kategorie firem, která by ve své organizaci měla zabezpečené oblasti, kterých se týká zabezpečení dle výše zmíněné normy. Informace zpracovávané v této firmě nejsou utajované, tato část tak není ve firmě nijak více řešena.

Oblasti pro nakládku a vykládku

Místa pro nakládku a vykládku, stejně jako ostatní místa jakéhokoliv přístupu do organizace by dle normy měly být kontrolovány a pokud možno izolovány od vybavení pro zpracování informací. Taktéž by měla být zvážena následující opatření:

- přístup pro nakládku a vykládku by měl být omezen pouze na oprávněné pracovníky;
- prostor pro nakládku a vykládku by měl být navržen takovým způsobem, aby se zabránilo vstupu personálu dodavatele do jiných částí organizace;
- vnější dveře pro nakládku a vykládku by měly být zabezpečeny;
- dodaný materiál by měl být zkontrolován, zda neobsahuje výbušiny, chemikálie nebo jiné nebezpečné látky; zda je v souladu s postupy týkající se řízení aktiv; zda s ním během doručování nebylo manipulováno neobvyklým způsobem. (ČSN EN ISO/IEC 27002)

Nakládka a vykládka ve vybraném subjektu probíhá z pravé boční strany budovy, kam se přijíždí druhou, vedlejší vjezdovou bránou. Tato brána slouží především pro zmíněné zásobování, v současné době taktéž pro vozy stavebních firem, které do objektu vjíždí z důvodu výstavby nové budovy. Jelikož se však jedná o malou firmu, kde neprobíhá žádné větší uskladňování zboží, nakládka a vykládka není nijak více řešena.

5.2.2 Bezpečnost zařízení

Bezpečnost zařízení je kritickým faktorem pro ochranu důležitých dat a informací. Týká se ochrany počítačů, notebooků, mobilních zařízení a celkového systému firmy proti neoprávněnému přístupu, poškození či zneužití.

Umístění zařízení a jeho ochrana

Dle výše zmíněné normy by mělo být veškeré zařízení umístěno a chráněno tak, aby se snížila rizika plynoucí z enviromentálních hrozeb a nebezpečí, či hrozeb a nebezpečí plynoucí z neoprávněného přístupu. Zařízení by měla být ochráněna těmito způsoby:

- umístění zařízení by mělo být takové, aby došlo k minimalizaci zbytečných přístupů do pracovních oblastí;
- vybavení pracující s citlivými daty by mělo být dispozičně umístěno tak, aby se při práci zabránilo sledování těchto dat neoprávněními osobami; mělo by být zabezpečeno proti neoprávněnému přístupu; mělo by být chráněno s ohledem na vliv elektromagnetického vyzařování;
- měla by být nastavena pravidla pro stravování, kouření a pití v blízkosti zařízení;
- měla by být přijata opatření, která by minimalizovala případná rizika a hrozby plynoucí např. z požáru, kouře, rušení elektrického napájení, vandalismu apod.;
- s ohledem na umístění zařízení by měla být sledována teplota a vlhkost prostředí a jiné podmínky, které by mohly ohrozit provoz zařízení;
- budovy by měly být chráněny před bleskem. (ČSN EN ISO/IEC 27002)

Zařízení zpracovávající důležité informace se ve vybraném subjektu nacházejí v jednotlivých kancelářích. Oprávnění ke vstupu do těchto kanceláří mají pouze zaměstnanci, kterým jsou jednotlivé kanceláře přiděleny, od kanceláří mají klíč. Tím je zamezen neoprávněný přístup k informacím cizím osobám.

Ve vybraném subjektu nejsou přijata žádná mimořádná opatření, která by v případě potřeby minimalizovala hrozby plynoucí z ohrožení provozu zařízení, kromě hromosvodu umístěného na budově firmy.

Podpůrné služby

Podpůrnými službami se dle normy rozumí např. elektřina, zásobování vodou, plynem, telekomunikace, kanalizace, větrání, klimatizace a další. Veškeré zařízení by tak dle této normy mělo být chráněno před výpadkem a poruchami výše zmíněných služeb. Taktéž by mělo být ve shodě se specifikací výrobce zařízení, mělo by být pravidelně kontrolováno, testováno, v případě závad by mělo dojít k upozornění varovným signálem. Vhodné je také disponovat nouzovým osvětlením a komunikací. (ČSN EN ISO/IEC 27002)

Elektřina a plyn je do vybraného subjektu dodávána z Tepláren Brno. V případě výpadku elektřiny je firma vybavena elektrocentrálou značky Rato, s elektrickým startováním se stálým výkonem do 9kVA.

Vybraný subjekt dále disponuje záložním zdrojem nepřerušovaného napájení UPS (Uninterrubtible Power Supply), který v případě potřeby zajišťuje dodávku elektrické energie pro zařízení, které nesmějí být vypnuty.

Voda a kanalizace je ve vybraném subjektu zabezpečována Brněnskými vodárnami a kanalizacemi.

Bezpečnost kabelových rozvodů

Dle zmíněné normy by měla být veškerá kabeláž určená pro přenos dat chráněna před rušením, poškozením či odposlechem. Kabeláž by měla být, tam kde je to možné, vedena v podzemí; napájecí a komunikační kabely by měly být od sebe odděleny. Pro citlivé a kritické systémy by měla být v rámci kabeláže zvážena např. instalace pancéřovaného potrubí, použití elektromagnetického stínění či řízený přístup k rozvodným místnostem. (ČSN EN ISO/IEC 27002)

Veškerou kabeláž vede vybraný subjekt ve svých budovách skrytě. Používá stíněné STP kabely tzn. elektrické kabely, které jsou obaleny vrstvou pro stínění – rušení. Datová kabeláž je oddělena od napájecí kabeláže. Rozvodná místnost je uzamčena, přístup k ní má pouze oprávněný personál. Klíč od této místnosti se vydává oproti podpisu na formulář obsahující veškeré záznamy o vstupech do rozvodné místnosti.

Údržba zařízení

Každé zařízení by dle této normy mělo být pro uchování dostupnosti a celistvosti správně udržováno. Jedná se zejména o doporučení, jako jsou např. dodržovat servisní intervaly; opravy a servis provádět prostřednictvím autorizovaných pracovníků; uchovávat veškeré

záznamy o chybách a údržbě; dohlížet na kontrolu a údržbu zařízení či dodržet požadavky na údržbu vyplývající z pojistných smluv. Pokud se jedná o zařízení, které je po údržbě opětovně uvedeno do provozu, mělo by dojít ke kontrole a zjistit, zda se zařízením nebylo manipulováno a že funguje správně. (ČSN EN ISO/IEC 27002)

Ve vybraném subjektu údržba zařízení probíhá v souladu s výše uvedenou normou. Veškeré zařízení je pravidelně kontrolováno v předepsaných intervalech prostřednictvím autorizovaných pracovníku. O zjištěných vadách při kontrole jsou vedeny záznamy. Veškeré zařízení, které je po opravě uváděno zpět do provozu je kontrolováno.

Přemístění aktiv, bezpečnost zařízení a aktiv mimo prostory organizace

Zmíněné dvě oblasti, týkající se přemístění aktiv, říkají, že žádné zařízení, informace ani software by dle výše zmíněné normy neměly být bez předchozího povolení přemísťovány mimo organizaci. Vždy by měly být určeni zaměstnanci pověření k přemísťování aktiv mimo organizaci; nastaveny by měly být taktéž časové lhůty; přemístění aktiv by mělo být určitým způsobem zaznamenáno; zaznamenávat by se měla i identita každého, kdo s aktivem zachází. V souvislosti s přemísťováním aktiv je možné provádět namátkové kontroly.

Dále by použití zařízení a aktiv mimo prostory organizace dle této normy mělo být vždy schváleno managementem organizace. Tyto aktiva a zařízení by mimo prostory organizace neměla být nikdy ponechána bez dozoru. Dodržovat by se měly pokyny výrobců, a to za všech okolností. Na základě posuzování rizik by s ohledem na lokalitu použití zařízení a aktiv měla být stanovena případná opatření. Opatřením pro snížení rizika může být i třeba odrazování zaměstnanců od práce mimo prostory organizace nebo omezené používání přenosných zařízení. (ČSN EN ISO/IEC 27002)

Aktiva, která by mohla ohrozit bezpečnost informací vybraného subjektu, jsou přemísťována pouze na základě nařízení vedoucích pracovníků, stejně tak jako jejich používání mimo prostory firmy. Jedná se například o pracovníky, kteří využívají přenosné počítače k práci z domu (Homeoffice). V těchto případech by však měla být dodržována stejná pravidla, jako při práci v objektu firmy. Zařízení by nemělo zůstávat bez dozoru, mělo by být chráněno před neoprávněným použitím cizí osobou.

Bezpečná likvidace nebo opakované použití zařízení

U všech částí zařízení, která obsahují paměťová média, by mělo být před jeho likvidací či opakovaném použití zajištěno odstranění či přepsání veškerých citlivých dat. V souvislosti s poškozenými zařízeními by se mělo vzít do úvahy i fyzické zničení. Kromě bezpečného

vymazání disku se riziko související s vyzrazením důležitých informací snižuje zašifrováním celého disku. (ČSN EN ISO/IEC 27002)

Jelikož se v souvislosti s vybraným subjektem jedná o skutečnost, že tato firma není nijak velká, nedisponuje proto ani „degausserem“ (demagnetizátorem) sloužícího k bezpečnému ničení disku. V případech, kdy lze data nějakým způsobem přepsat či vymazat, postupuje se v souladu s normou.

Vybraný subjekt navíc využívá šifrování disku (bitlocker) a to zejména proto, aby se zamezilo úniku citlivých dat například v situacích ztráty notebooku.

Neobsluhovaná uživatelská zařízení, zásada prázdného stolu a prázdné obrazovky monitoru

Všichni uživatelé obsluhující zařízení by měly být informováni o postupech k ochraně těchto zařízení. Jedná se zejména o opatření jako ukončení relace po dokončení činnosti; používání spořičů obrazovky; odhlášení z aplikací, pokud nejsou dále potřebné; používání zámku či přístupového hesla na zařízení.

Princip prázdného stolu a prázdné obrazovky monitoru dokáže zajistit snížení rizika neoprávněného přístupu, poškození či ztráty důležitých informací. V praxi znamená zásada prázdného stolu a prázdné obrazovky monitoru následující:

- důležité informace v papírové či elektronické podobě, které nejsou využívány, by měly být uzamčeny, zejména pak v případech, pokud je kancelář opuštěná;
- počítače a jiná zařízení by měla být odhlášena, chráněna heslem;
- kopírovací a jiné reprodukční technologie by měla být chráněna před neoprávněným používáním;
- média s důležitými informacemi by měla být z tiskáren odebírána okamžitě po provedení tisku.

Vhodnou formou uchování důležitých informací jsou také trezory a jiné formy zařízení, chránící tyto informace nejen před případným pachatelem, ale i před katastrofami jako např. požár, zemětřesení, záplava či výbuch. (ČSN EN ISO/IEC 27002)

Každému zaměstnanci je ve vybrané firmě přiděleno uživatelské jméno a heslo pro přístup do systému. V případě delšího nepoužívání zařízení dochází po 5 minutách k automatickému

odhlášení uživatele. Tím je přístup k informacím poskytnut pouze oprávněným pracovníkům.

Všichni zaměstnanci se řídí vnitřně nastavenými pravidly, jako např. nenechávat bez dozoru k nahlédnutí dokumenty v centrální tiskárně nebo důležité dokumenty na stolech zaměstnanců. V případech, kdy pracovník opouští kancelář, by měl uzamknout počítač.

Pracovníci jsou taktéž každoročně proškolováni v problematice potencionálního úniku důležitých informací.

5.3 Kontrolní seznam – checklist

V souvislosti s relativně obsáhlou a do jisté míry nepřehlednou předcházející podkapitolou, bude nyní navržen kontrolní seznam neboli checklist. Pomocí uvedené metody analýzy rizik, bude úkolem zhodnotit, zda fyzické zabezpečení vybraného subjektu koresponduje s opatřeními a návrhy doporučenými v rámci ČSN ISO/IEC 27002. Na základě toho budou následně vyhodnocena rizika plynoucí z absence jednotlivých položek zabezpečení a navržena opatření ke zlepšení.

Checklist je jednoduchá metoda, která je využitelná ve všech možných oblastech. Její hlavní myšlenkou je eliminovat či alespoň minimalizovat chyby a rizika, která by mohla vést k nežádoucím událostem. Checklist je založen na systému kontrolních otázek a odpovědí, který slouží jako kontrolní seznam pro ověření kroků a postupů při vykonávání určité činnosti.

Správně nastavený checklist by měl splňovat následující doporučení:

- měl by mít jasně definovaný cíl a účel;
- otázky a kroky by měly být formulovány tak, aby souvisely s danou činností a zároveň pokrývaly co nejširší spektrum potencionálních rizik;
- rizika by měla být ohodnocena a určena jejich závažnost;
- opatření by měla být nastavena tak, aby minimalizovala pravděpodobnost výskytu rizika;
- checklist by měl obsahovat také kroky pro kontrolu účinnosti opatření;
- součástí checklistu by měla být stanovena odpovědnost za kroky a opatření v procesu minimalizace rizik.

Každý checklist by měl být pravidelně aktualizován a přehodnocován, aby se zajistilo zlepšení celého procesu analýzy rizik. (ADAMEC, Vladimír, 2021; Smejkal a Rais, 2013, s. 100-115)

V rámci checklistu jsem si tak úplně na začátku stanovil cíl, kterým bylo zjistit, jaká rizika mohou v souvislosti s fyzickým zabezpečením vybraného subjektu při nedodržení návrhů a opatření vycházející s ČSN ISO/IEC 27002 nastat.

Prvním krokem tak bylo vytvořit si seznam kontrolních otázek, vycházejících z jednotlivých bodů oblasti fyzické bezpečnosti a bezpečnosti prostředí ČSN ISO/IEC 27002.

Na základě uvedených otázek byla následně zjištěna rizika plynoucí z absence jednotlivých položek fyzického zabezpečení. Posléze byla rizika ohodnocena s ohledem na pravděpodobnost a dopad těchto rizik, jak je patrné z následující tabulky (Tab. 1).

Tabulka 1 – Matice rizik

(Zdroj: ADAMEC, Vladimír, 2021; zpracování vlastní)

Dopad	Pravděpodobnost				
	1 - vzácné	2 - nepravděpodobné	3 - možné	4 - pravděpodobné	5 – téměř jisté
1 - zanedbatelný	1	2	3	4	5
2 - menší	2	4	6	8	10
3 - mírný	3	6	9	12	15
4 - výrazný	4	8	12	16	20
5 - katastrofální	5	10	15	20	25

Pomocí součinu těchto dvou veličin bylo zjištěno celkové score, na základě, kterého, bylo následně vyhodnoceno riziko jako nízké, střední, vysoké, kritické, jak je možné vidět v následující Tab. 2.

Tabulka 2 – Vyhodnocení rizika

(Zdroj: ADAMEC, Vladimír, 2021; zpracování vlastní)

Skóre	Riziko
1 - 3	nízké
4 - 6	střední
8 - 12	vysoké
15 - 25	extrémní

Ohodnocení proběhlo za pomoci konzultace s pracovníkem vybraného subjektu stejně jako zpracování celého checklistu. Posledním krokem pak bylo navrhnout, na základě zjištěných rizik, opatření na zlepšení u těch položek fyzického zabezpečení, kterými firma nedisponuje.

Tabulka 3 – Checklist

(Zdroj: vlastní)

Oblast	Otázka	Odpověď	Riziko	Ohodnocení rizika	Návrhová opatření
Fyzický bezpečnostní perimetr	Jsou definovány bezpečnostní perimetry v závislosti na bezpečnosti aktiv?	ANO	Neoprávněný vstup do objektu	8	
	Jsou veškeré bezpečnostní perimetry fyzicky v pořádku?	NE	Neoprávněný vstup do objektu	12	Zajistit ochranu oken i v 1. patře např. pomocí mříží či magnetických okenních senzorů.
	Jsou zřízeny dostatečné prostředky pro kontrolu fyzického přístupu?	NE	Neoprávněný vstup do objektu plynoucí z nepozornosti recepční	15	Kontrolu fyzického přístupu prostřednictvím pracovníka recepce vyměnit za turniket s EKV
	Jsou všude tam, kde je to účelné, postaveny fyzické bariéry zabraňující neoprávněnému přístupu?	NE	Vloupání	16	V souvislosti s nedostatečnou perimetrickou ochranou způsobenou porušeným drátěným plotem nahradit tento stávající plot plotem kamenným a zajistit tak fyzickou bariéru proti neoprávněnému přístupu.
	Jsou systémy detekce průniku nainstalovány tak, aby byly zajištěny všechna dveře a vnější okna?	NE	Vloupání, vandalismus	16	Zahrnout do zabezpečení subjektu PZTS s detektory narušení s napojením na DPPC, popřípadě zvolit efektivnější VDS
	Jsou zajištěny místnosti s počítači a komunikační místnosti?	ANO	Neoprávněný vstup	9	
Fyzické kontroly vstupu	Je vedena přesná evidence příchodů a odchodů veškerých návštěv?	ANO	Neoprávněné získání citlivých informací	9	
	Existuje v rámci firmy fyzická kniha záznamů nebo elektronický auditní záznam veškerých přístupů?	NE	Ztráta přehledu o pohybu osob v prostorách firmy	15	Zřídit systém EKV + čipové karty, navýšit tento systém o elektronickou evidenci docházek zaměstnanců
	Mají všichni zaměstnanci firmy i smluvních stran povinnost nosit viditelné označení příslušnosti k firmě?	ANO	Infiltrace neoprávněných osob do firmy	3	
	Jsou přístupová práva do zabezpečených oblastí pravidelně přezkoumávána, aktualizována a v případě potřeby rušena?	ANO	Neoprávněné získání citlivých informací	6	

Oblast	Otázka	Odpověď	Riziko	Ohodnocení rizika	Návrhová opatření
Zabezp. kanceláří, místností, vybavení	Je klíčové vybavení umístěno tak, aby se zabránilo přístupu veřejnosti?	ANO	Neoprávněné získání citlivých informací	6	
Ochrana před vnějšími hrozbami	Používá subjekt nějaký způsob ochrany dat před přírodními hrozbami, vnějšími útoky nebo nehodami?	ANO	Ztráta citlivých informací	16	
Oblasti pro nakládku a vykládku	Je proces nakládky a vykládky bezpečný?	ANO	Neoprávněný vstup	6	
Umístění zařízení a jeho ochrana	Jsou zařízení umístěna tak, aby byl minimalizován přístup neoprávněných osob a došlo k eliminaci rizika sledování?	ANO	Neoprávněné získání citlivých informací	4	
	Jsou vybavení pro ukládání dat zabezpečena proti neoprávněnému přístupu?	ANO	Neoprávněné získání citlivých informací	9	
	Jsou stanovena pravidla pro stravování, pití, kouření v blízkosti zařízení zpracovávající informace?	ANO	Poškození zařízení zpracovávající citlivé informace	8	
	Jsou budovy chráněny před bleskem?	ANO	Poškození zařízení zpracovávající citlivé informace	6	
Podpůrné služby	Disponuje subjekt veškerými nouzovými zdroji v rámci podpůrných služeb?	NE	Komplikace spojená s běžným fungováním při práci ve firmě	3	Zvážit pořízení nouzového zdroje vody
Bezpečnost kabel. rozvodů	Jsou v objektu firmy oddělené napájecí a komunikační kabely?	ANO	Poškození přijímaných informací	12	
	Je kabeláž ve vybraném subjektu, tam kde je to možné, vedena v podlaze?	ANO	Poškození přijímaných informací	12	
Údržba zařízení	Je ve vybraném subjektu prováděn pravidelný servis a údržba zařízení?	ANO	Nesprávné fungování zařízení zpracovávající citlivé informace	9	

Oblast	Otázka	Odpověď	Riziko	Ohodnocení rizika	Návrhová opatření
	Provádějí pravidelný servis a údržbu zařízení autorizovaní pracovníci?	ANO	Nesprávné fungování zařízení zpracovávající citlivé informace	9	
	Jsou uchovávány záznamy o všech chybách a veškeré preventivní a nápravné údržbě?	ANO	Nesprávné fungování zařízení zpracovávající citlivé informace	9	
	Jsou zařízení před opětovným uvedením do provozu kontrolována?	ANO	Nesprávné fungování zařízení zpracovávající citlivé informace	9	
Přemístění aktiv	Je ve vybraném subjektu zajištěn dohled nad přemísťováním aktiv?	ANO	Ztráta přehledu o aktivech firmy	6	
	Jsou při přemísťování aktiv nastavovány časové lhůty a kontrolováno jejich dodržování?	ANO	Ztráta přehledu o aktivech firmy	6	
	Jsou dodržovány pokyny související s bezpečností aktiv mimo organizaci?	ANO	Nesprávné nakládání s aktivy firmy	6	
Bezpečná likvidace nebo opakované použití zařízení	Jsou před likvidací nebo opakovaným použitím z částí zařízení obsahující paměťová média odstraněna všechna důležitá data?	ANO	Neoprávněné získání citlivých informací	12	
	Používá subjekt nějaký způsob šifrování disku?	ANO	Neoprávněné získání citlivých informací	16	
Neobsluhovaná uživatelská zařízení	Využívá subjekt v rámci zaměstnanců přístupová hesla?	ANO	Neoprávněné získání citlivých informací	16	
Zásada prázdného stolu a obrazovky	Používají zaměstnanci spořiče obrazovky?	ANO	Neoprávněné získání citlivých informací	12	
	Jsou citlivé informace o firmě v papírové nebo elektronické podobě uzamykány v době kdy nejsou využívány?	ANO	Neoprávněné získání citlivých informací	8	
	Jsou z tiskáren ihned po dokončení odebírány důležité dokumenty?	ANO	Neoprávněné získání citlivých informací	4	

V rámci checklistu jsou ohodnocena rizika vybraného subjektu související s jednotlivými oblastmi ČSN ISO/IEC 27002, dle pravděpodobnosti vzniku a dopadu rizika. Na základě toho jsou následně rizika rozřazena dle důležitosti na rizika nízká (zelená barva), střední (žlutá barva), vysoká (oranžová barva) a extrémní (červená barva).

V případě, kdy vybraný subjekt vykazuje absenci určitého druhu položky fyzického zabezpečení podle ČSN ISO/IEC 27002, jsou popsána návrhová opatření, která by bylo vhodné realizovat.

U těch položek fyzického zabezpečení, kde jsou rizika související s absencí vyhodnocena jako rizika extrémní (červená barva) a zároveň subjekt tuto absenci vykazuje, budou jednotlivá návrhová opatření podrobněji představena v následujících částech diplomové práce.

6 NÁVRHOVÁ OPATŘENÍ FYZICKÉHO ZABEZPEČENÍ

Po provedení analýzy fyzického zabezpečení firmy s ohledem na systém řízení bezpečnosti informací, bylo zjištěno několik nedostatků, které by, dle mého názoru a taktéž v souladu s ČSN EN ISO/IEC 27002, bylo vhodné odstranit. Organizaci by to přineslo vyšší stupeň zabezpečení a taktéž by došlo k výraznější ochraně důvěrných informací. Zvolená návrhová opatření budou nyní představena. Součástí bude i kalkulace nákladů na realizaci těchto opatření.

6.1 Oplocení

Na základě analýzy byly zjištěny nedostatky v perimetrické ochraně. Drátěný plot, tvořící tuto ochranu, je na několika místech poškozen, pletivo je uvolněné, navíc se v něm nacházejí otvory. Oplocení je vysoké pouze 180 cm, což je také z mého pohledu nedostatečné.

Z důvodu jednoduché překonatelnosti, tak navrhuji zvýšit náročnost překonání perimetrické ochrany. Nejúspornějším řešením by bylo vyměnit stávající pletivo za pletivo nové, vyšší, po případě přidat ještě navíc ostnatý drát. Druhým řešením, nákladnějším, ale za to z pohledu životnosti mnohem výhodnějším, se jeví vystavění kamenného skládaného plotu.

Jak je z vlastního nákresu objektu patrné, zadní strana areálu vybraného subjektu není tvořena pouze plotem, ale část obvodu se skládá ze zdí starší budovy a budovy ve výstavbě. Náklady na realizaci kamenného plotu by se tak o tuto část obvodové plochy areálu snížily. Celkově by bylo třeba pořídit 26 metrů kamenného plotu v navrhované výšce dva metry. Kamenný plot se skládá desek, abychom dosáhli požadované výšky plotu, je tak potřeba pět těchto desek. Po každých dvou metrech je třeba desky umístit do sloupků.

Následující tabulka (Tab. 4) znázorňuje náklady na pořízení 26 metrů tohoto plotu, bez nákladů na realizaci, firmou Betonové ploty Petr Harašta.

Tabulka 4 – Náklady na pořízení kamenného plotu
(Zdroj: Betonové ploty Petr Harašta ©2010–2022, zpracování vlastní)

Produkt	Bližší určení	Požadované množství (ks)	Cena (Kč)	Cena celkem bez DPH (Kč)
Kamenná deska	40 cm	5	236,-	1 180,-
Kamenné desky v požadované výšce	200 cm	14	1 180,-	16 520,-
Sloupek	1 ks	17	500,-	8 500,-
Náklady na pořízení kamenného plotu			**25 020,- Kč**	

6.2 Turnikety a elektronická kontrola vstupů

Dalším vhodným návrhem je dle mého názoru pořízení turniketů s elektronickou kontrolou vstupů (dále jen „EKV“). EKV je výhodný systém, díky kterému by se dosáhlo vysoké ochrany zabezpečení před neoprávněným vniknutím. Lidský faktor v podobě recepční nemusí být dostačující, zejména z důvodu nepozornosti či nedůslednosti. Mnohem efektivnější v souvislosti s neoprávněným vstupem cizích osob do objektu firmy přes den je dle mého názoru systém EKV spojený s turnikety.

Osobám, které by dostaly oprávnění vstupu do objektu firmy, by byly přiděleny čipové karty. Tyto čipové karty by po načtení sloužily pro vstup do objektu přes turnikety. Zaměstnanec by přiložil čipovou kartu ke čtečce, pokud by splňoval přístupové oprávnění, mohl by přes turniket projít.

Navrhoval bych pořídit dva turnikety, jejich umístění by mohlo být ve volné prostoru vedle recepce, po pravé straně, pár metrů od vstupních dveří do objektu. Pozice recepční – kontrolora, by tak mohla přes den vykonávat i jinou práci, než jen dohlížet na vstupující a odcházející osoby. Mohla by být začleněna do chodu vybraného subjektu. Výhledově by to tak pro firmu bylo hospodárnější i efektivnější.

Vhodným typem turniketu, zvoleným na základě poměru cena/výkon, se mi jeví oboustranný turniket Tristar 303, který je zobrazen na následujícím obrázku (Obr. 11). Tento turniket zajišťuje kontrolovaný vstup v obou směrech. Je vyroben z broušené nerezy, otočná ramena

pak z nerezových trubek. Disponuje automatickým sklopením ramena při zaznamenání alarmu, což je pro vybraný subjekt nepochybně jednou z důležitých vlastností. Turniket má navíc vestavěnou řídící jednotku vhodnou pro připojení jakéhokoliv přístupového nebo vstupenkového systému. Tuto možnost bych v budoucnu doporučil využít. Celý systém EKV by tak mohl být doplněn o elektronickou evidenci docházek. To by zajistilo striktnějšímu dodržování pracovní doby zaměstnanců, jelikož by byly veškeré příchody a odchody zaznamenávány. Tento systém by také přispěl ke zjištění aktuálního stavu zaměstnanců ve firmě v danou chvíli, což je např. v případě požáru, nebo kdykoliv jindy, kdy tento stav potřebujeme znát, velice přínosné.

Zavedení turniketů vybranému subjektu přineslo takový systém kontrol vstupu, který by zajistil požadovanou úroveň zabezpečení a zároveň by nedocházelo k omezení pohybu osob ve firmě.

Turniket Tristar 303 se čtečkou karet by bylo možné pořídit od firmy Detomatic s.r.o. za cenu 61 820,- Kč bez DPH.

Obrázek 11 - Turniket Tristar 303
(Zdroj: Detomatic s.r.o.)

Každý zaměstnanec by tedy vlastnil svoji čipovou kartu, která by mu sloužila pro vstup do budovy přes turnikety. V souvislosti s úpravou tohoto systému vstupů bych navrhoval umístit čtečku čipových karet i ke dveřím z pravé boční strany budovy. Tyto dveře, jak již bylo zmíněno, slouží k průchodu do zbytku areálu, nebo ho zaměstnanci mohou využívat ke vstupu do budovy. Taktéž kvůli nově vznikající budově, do které se přemístí

část zaměstnanců, bude tento průchod v budoucnu využíván častěji. Čtečku karet bych navrhoval pořídit například Rosslare AY-H12, na stránkách firmy Abbas,a.s. za 3 155,- Kč.

Pokud by se systém EKV vybranému subjektu osvědčil, mohlo by se uvažovat o instalaci čtečky karet i k jednotlivým kancelářím.

Aby mohly turnikety a dveře otvírané čipovými kartami skrze čtečku správně fungovat, je nutné zakoupit ještě dveřní modul. V případě návrhu EKV bych subjektu doporučil modul Dominus 3 ACC-2W1, na webových stránkách firmy Abbas,a.s. v ceně 8 490,- bez DPH. Jeden tento modul dokáže zajistit oboustranné ovládání turniketu nebo průchod 2x jednostrannými dveřmi. V případě turniketů a dveří je tak nutné pořídit 3 ks.

Celkové náklady na EKV, bez nákladů na realizaci, je tak možné vidět v následující tabulce (Tab. 5)

Tabulka 5 – Náklady na pořízení EKV

(Zdroj: ABBAS, a.s., ©2013-2023; Detomatic s.r.o., zpracování vlastní)

Produkt	**Bližší určení**	**Počet požadovaných kusů (ks)**	**Cena za kus (Kč)**	**Cena celkem bez DPH (Kč)**
Turniket Tristar 303	s čtečkou karet	2	61 820,-	123 640,-
Čipová karta	pro zaměstnance	50	40,-	2 000,-
Čtečka Rosslare AY-H12	boční postranní vchod	2	3 155,-	6 300,-
Dveřní modul Dominus 3 ACC-2W1	zajištění funkčnosti turniketů a dveří	3	8 490,-	25 470,-
Náklady na pořízení EKV				**157 410,- Kč**

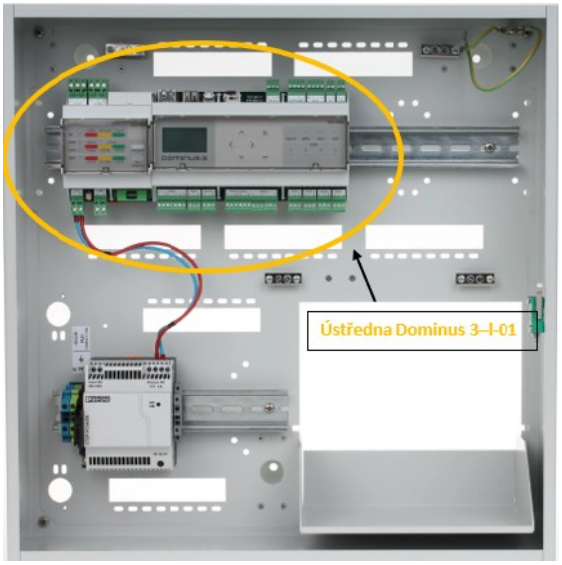
6.3 Poplachový a zabezpečovací tísňový systém

Dalším návrhovým opatřením v souvislosti se zabezpečením vybraného subjektu je zavedení PZTS – poplachového a zabezpečovacího tísňového systému v kombinaci s EKV – elektronickou kontrolou vstupů. Navrhoval bych proto systém Dominus 3, který je vhodný pro všechny typy objektů a zároveň splňuje podmínku kombinace PZTS + EKV. Tento systém je schválen akreditovanou zkušebnou, a navíc certifikován dle ČSN EN 50131 a požadavků NBÚ až do stupně 4 – vysoké riziko. Jednotlivé komponenty jsou pak vybrány na základě různých specifik, nejčastěji však s ohledem na cenu.

PZTS by v případě vybraného subjektu byla tvořena ústřednou, napájecím zdrojem, ovládacím panelem, koncentrátorem, detektory narušení a signalizačními prostředky.

Ústředna je základním modulem systému. V případě Dominusu 3 jsem zvolil ústřednu Dominus3-l-01. Tato ústředna, kterou je možné vidět na obrázku níže (Obr. 12), umožňuje připojit až 10 000 detektorů, ovládat 2 000 dveří a ve své paměti dokáže uložit 50 000 uživatelů. Přímo v ústředně je také integrován telefonní komunikátor, umožňující komunikaci s DPPC.

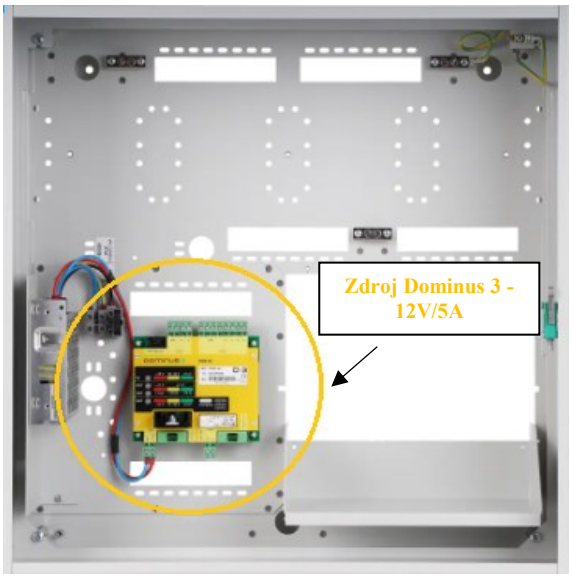
Cena této ústředny je na webových stránkách firmy Abbas,a.s. 42 560,- Kč bez DPH.



Obrázek 12 - Ústředna Dominus 3-l-01
(Zdroj: ABBAS, a.s., ©2013-2023)

Ústřednu, jak je patrné i z Obr. 12 je zapotřebí umístit do boxu se zdrojem napájení. Pořídit by vybraný subjekt mohl např. sestavu montážního boxu se systémovým zdrojem 12V/5A

D3-BOX-XL-PWR-05, která je vyobrazena na následujícím obrázku (Obr. 13). Na stránkách firmy Abbas, a.s. je cena tohoto boxu se zdrojem 14 870,- Kč bez DPH.



Obrázek 13 - Sestava montážního boxu se systémovým zdrojem
(Zdroj: ABBAS, a.s., ©2013-2023)

Součástí systému Dominus 3 musí být taktéž ovládací panel. Pomocí tohoto zařízení uvede pracovník ostrahy po odchodu posledního zaměstnance z firmy PZTS do provozu.

V souvislosti s vybraným subjektem jsem vybral dotykový ovládací panel KPD-ECO-AL-W (Obr. 14), který umožňuje odstřežení / zastřežení, kontrolu a vizualizaci přístupu. Jeho umístění bych zvolil v prostorách recepce, jelikož odstřežení a zastřežení objektu by měl na starost pracovník ostrahy. Na webových stránkách firmy Abbas, a.s. je cena tohoto ovládacího panelu 12 600,- bez DPH.

Obrázek 14 – Ovládací panel
(Zdroj: ABBAS, a.s., ©2013-2023)

V případě vybraného subjektu bych navrhoval dva druhy detektorů:

- pohybové elektromagnetické;
- magnetické (okenní).

Vybraný model **pohybového elektromagnetického detektoru** Optex FlipX FLX-A-DAM-X9 je novinkou na trhu. Disponuje inovativním senzorem pro přesné zachycení postavy člověka a duální technologií PIR (pasivní infračervený detektor) + MW (mikrovlnná detekce). Zajišťuje vysoký výkon a přesnost, jeho speciálně navržená otočná sférická čočka dokáže zaměřit ohniskovou vzdálenost každého detekčního paprsku v rozsahu 85°. Tento detektor také nabízí funkci proti zamaskování.

Ve vybraném subjektu by se nacházel v každé místnosti a na koncích chodby, v obou patrech objektu. Jeho hlavním úkolem by bylo upozornit na neoprávněný pohyb osob ve firmě po zastřežení prostorů budovy.

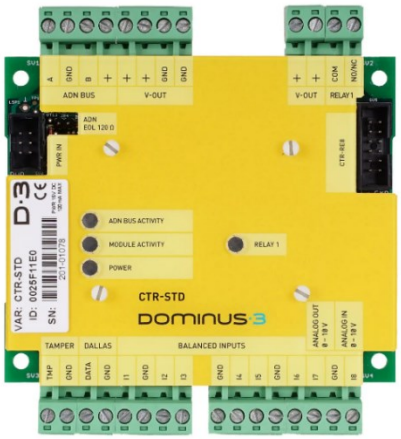
Celkem by tak bylo potřeba 17 pohybových detektorů. Cena výše zmíněného vybraného detektoru u firmy Abbas, a.s. je 2 139,- Kč bez DPH.

Dalším navrhovaným detektorem je umístění **magnetického kontaktu do okenních rámů** ve druhém podlaží objektu.

Navrhoval bych detektor MAS 303, který se skládá ze dvou částí, magnetu a senzoru. Magnet se umístí na jednu část okenního rámu a senzor na druhou. V případě, kdy se magnet vzdálí od senzoru, v systému zabezpečení se tento stav zaznamená jako „otevřeno“. Detektor tak může zabezpečovat nejen detekci neoprávněného vstupu do objektu, ale také upozornění na otevřená okna. V souvislosti s otevřenými okny totiž vznikají další rizika. Může např. dojít k poruše zařízení obsahující důležité informace, v důsledku nepříznivého počasí, tzn. dešťová voda se dostane do zařízení atd.

Celkem se v druhém podlaží firmy nachází 20 oken. Vybraný magnetický kontakt stojí na webových stránkách firmy Abbas,a.s. 428,- Kč bez DPH.

Do PZTS je nutné zahrnout také koncentrátor, což je modul určený pro připojení detektorů. V rámci vybraného subjektu jsem zvolil koncentrátor CTR-STD zahrnující 8x vstup a 1x výstup (tzn. napojení osmi detektorů a jednoho signalizačního prostředku), který je možné vidět na následujícím obrázku (Obr. 15). S ohledem na množství navrhovaných detektorů (celkem 37 ks) bude nutné k pokrytí celé budovy potřeba 5 ks těchto koncelerátorů. Cena jednoho koncentrátoru je dle firmy Abbas,a.s. 4 510,- Kč.



Obrázek 15 - Koncentrátor

(Zdroj: ABBAS, a.s., ©2013-2023)

V následující tabulce (Tab. 6) můžete vidět celkové náklady na realizaci PZTS. V nákladech nejsou započítány náklady na realizaci ani licence spojené s využíváním tohoto systému.

Tabulka 6 – Náklady na pořízení PZTS

(Zdroj: ABBAS, a.s., ©2013-2023, zpracování vlastní)

Produkt	Bližší určení	Počet pož. kusů (ks)	Cena bez DPH (Kč)	Cena celkem bez DPH (Kč)
Ústředna Dominus3-l-01	řídící jednotka	1	42 560,-	42 560,-
Sestava boxu se zdrojem D3-BOX-XL-PWR-05	systémový zdroj 12V/5A	1	14 870,-	14 870,-
Ovládací panel KPD-ECO-AL-W	x	1	12 600,-	12 600,-
Detektor Optex FlipX FLX-A-DAM-X9	pohybový elektromagnetický detektor	17	2 139,-	36 363,-
Detektor MAS 303	magnetický kontakt do okenních rámů	20	428,-	8 560,-
Koncentrátor CTR-STD	komunikace mezi ústřednou a detektory	5	4 510,-	22 550,-
Náklady na pořízení PZTS			**137 503,-**	

6.4 Videodohledové systémy

Na základě analýzy stávajícího VDS ve vybraném subjektu bych doporučil vyměnit starší modely analogových kamer za modernější IP kamery a napojit je na PZTS. S ohledem na současný stav shledávám dostatečnými pořídit tři venkovní a jednu vnitřní kameru. Dvě venkovní kamery bych navrhoval umístit v prostoru parkoviště tak, aby pokrývaly jak vjezd na parkoviště, tak vstup do budovy. Další venkovní kameru bych umístil do stejného místa, jako je již umístěná současná analogová kamera. Zabírala by převážnou část pravé strany areálu, tam, kde se budují nové prostory firmy. Jedinou z kamer, která by se nacházela uvnitř budovy, bych umístil tak, aby pokrývala prostor turniketů.

Dle požadovaných specifik a poměru cena/výkon bych navrhoval pořídit venkovní kameru značky Dahua SD42212T-HN, která je znázorněna na následujícím obrázku (Obr. 16). Jedná se o otočnou FullHD IP kameru s rozlišením 1080p, 12x optickým zoomem a certifikací IP66 (ochranou před prachem a vodou). Tato kamera je taktéž odolná proti vandalismu podle normy IK10, tělo kamery odolá nárazu objektu o váze 5 kg padající z výšky 40 cm. Kamera poskytuje vysoce kvalitní video se silným kontrastem, vysokým jasem i v protisvětle. Tuto kameru jsem zvolil taktéž pro její použití v nejnáročnějších podmínkách.

Cena venkovní kamery, kterou bych doporučil pořídit, činní na stránkách firmy ABBAS, a.s. 11 599,- bez DPH.

Obrázek 16 – Venkovní kamera Dahua
(Zdroj: ABBAS, a.s., ©2013-2023)

Jako vnitřní kameru bych navrhoval vnitřní kameru Bosch NTV-3502-F03L, která je znázorněna na následujícím obrázku (Obr. 17). Tato kamera s režimem den/noc disponuje rozlišením 1080p, vestavěným IR přísvitem 15 metrů a úhlem záběru 100°. Cena vnitřní kamery je na stránách firmy ABBAS, a.s. 8 190,- bez DPH.

Obrázek 17 – Vnitřní kamera Bosch
(Zdroj: ABBAS, a.s., ©2013-2023)

V rámci VDS doporučuji pořídit ještě digitální videorekordér, který pomáhá rozšiřovat ukládání a provoz IP kamer. Vybral bych například IP záznamové zařízení značky Dahua, NVR4108HS-P-4KS2/L, který je zobrazen na následujícím obrázku (Obr. 18). Toto zařízení umožňuje připojení až 8 IP kamer. Vybraný subjekt by dle mého návrhu měl disponovat čtyřmi kamerami, nicméně je dobré do budoucna počítat s rozšířením kamer, už jen např. z důvodu nově vznikajících prostor firmy.

Maximální rychlost záznamu zmíněného videorekordéru je 80 Mbps a data lze uložit na pevný disk o kapacitě až 10 TB.

Díky tomuto zařízení by subjekt získal další přídavné funkce VDS, kterými jsou:

- ochrana perimetru zpracovaná v kameře – tato funkce zajistí zvýšení přesnosti a omezení počtu falešných poplachů;
- detekce tváře zpracovaná v kameře – díky této funkci je z videa možné zaznamenat ten nejlepší snímek obličeje;
- detekce pohybu SMD Plus – pomocí této funkce dojde k odfiltrování nežádoucích objektů (např. zvířata, listy), které by mohly způsobit falešný poplach. Detekce pohybu je tak zaměřená na konkrétní osoby a vozidla. (ABBAS, a.s., ©2013-2023)

Cena tohoto zařízení činí na stránkách firmy ABBAS, a.s. 7 500,- Kč bez DPH.

Obrázek 18 – Digitální videorekordér Dahua
(Zdroj: ABBAS, a.s., ©2013-2023)

V souvislosti s výše zmíněným videorekordérem navrhuji taktéž pořídit pevný disk určený pro záznamová zařízení, který bude konstruován na provoz 24 hodin 7 dní v týdnu a bude mít sníženou spotřebu elektrické energie. Z široké nabídky produktů bych zvolil např. pevný disk Skyhawk HDD 6 TB, který má dostačující kapacitu pro množství až 8 kamer, záznam je pak uchováván jeden týden. Navrhovaný pevný disk je možné vidět na následujícím obrázku (Obr. 19).

Cena tohoto disku je na stránkách firmy ABBAS, a.s. 3 390,- Kč bez DPH.

Obrázek 19 – Pevný disk Skyhawk
(Zdroj: ABBAS, a.s., ©2013-2023)

Pořizovací náklady na VDS jsou znázorněny v následující tabulce (Tab. 7).

Tabulka 7 –Náklady na pořízení VDS
(Zdroj: ABBAS, a.s., ©2013-2023, zpracování vlastní)

Produkt	**Bližší určení**	**Počet požadovaných kusů (ks)**	**Cena bez DPH (Kč)**
Dahua SD42212T-HN	venkovní kamera	3	11 599,-
Bosch NTV-3502-F03L	vnitřní kamera	1	8 190,-
Dahua NVR4108HS-P-4KS2/L	záznamové zařízení	1	7 500,-
Skyhawk HDD 6 TB	pevný disk	1	3 390,-
Náklady na pořízení VDS			**53 877,-**

Vybraný subjekt by na pořízení tří kusů venkovních kamer, vnitřní kamery, záznamového zařízení a pevného disku musela vynaložit 53 877,- Kč bez DPH. Uvedená cena by v případě pořízení byla navýšena ještě o náklady za realizaci a zprovoznění, v případě diplomové práci však tyto náklady nebereme v úvahu.

6.5 Celková kalkulace navrhovaných opatření

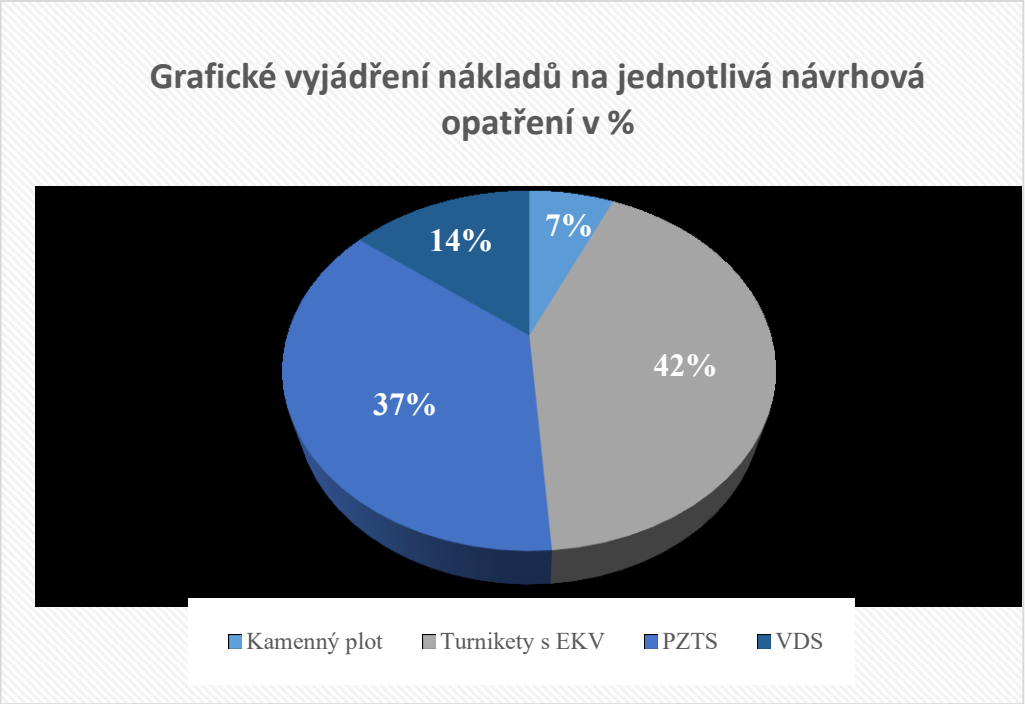
V rámci návrhových opatření bych doporučil do systému fyzického zabezpečení subjektu zahrnout kamenný plot, turnikety s EKV, PZTS a VDS. Celkové náklady je možné vidět v následující tabulce (Tab. 8). V celkových nákladech na pořízení není započtena cena práce ani další související náklady, které není možné jednoznačně vyčíslit. Jsou zde tak promítnuty pouze jednotlivé komponenty daných systémů.

Tabulka 8 – Celková kalkulace návrhových opatření

(Zdroj: ABBAS, a.s., ©2013-2023; Betonové ploty Petr Harašta ©2010–2022; Detomatic s.r.o.; zpracování vlastní)

	Cena celkem bez DPH (Kč)
Náklady na pořízení kamenného plotu	25 020,-
Náklady na pořízení turniketů s EKV	157 410,-
Náklady na pořízení PZTS	137 503,-
Náklady na pořízení VDS	53 877,-
Celková cena za návrhová opatření	**373 810,-**

Z Tab. 8 je patrné, že náklady na pořízení turniketů s EKV a náklady na pořízení PZTS jsou pro vybraný subjekt finančně nejnáročnější, jak je ostatně vidět i na grafickém znázornění jednotlivých návrhových opatření na dalším obrázku (Obr. 20).



Obrázek 20 – Grafické vyjádření nákladů na jednotlivá návrhová opatření v %
Zdroj: vlastní zpracování

Z grafického znázornění vyplývá, že nejnáročnější je pro subjekt zřídit turniket s elektronickou kontrolou vstupů, který z celkové vynaložené částky na návrhová opatření dělá 42 % této částky. Druhým náročnějším návrhem z pohledu vynaložených nákladů je poplachový zabezpečovací a tísňový systém, s 37 % částky. Ve srovnání s tím je zabezpečení videodohledových systémů (14 %) a kamenného plotu (7 %) nejméně nákladné.

ZÁVĚR

Diplomová práce se zabývá problematikou systému řízení bezpečnosti informací z pohledu fyzické bezpečnosti. V první, teoretické části práce jsou vysvětleny základní pojmy, které úzce souvisí s problematikou systému bezpečnosti informací a fyzickým zabezpečením.

Praktická část se následně věnuje charakteristice a aktuálnímu stavu fyzické bezpečnosti ve vybraném subjektu. Dále jsou představena doporučení na fyzické zabezpečení dle ČSN EN ISO/IEC 27002 a provedena komparace s aktuálním stavem fyzického zabezpečení v této firmě. Na základě zjištěných odchylek jsou za pomoci jedné z metod analýzy rizik, checklistu, vyhodnocena rizika a navržena opatření na zlepšení jednotlivých položek systému fyzického zabezpečení. Součástí jednotlivých návrhových opatření je i kalkulace nákladů na jejich pořízení.

V rámci fyzického zabezpečení vybraného subjektu navrhuji provést následující opatření ke zlepšení. Obvodovou část areálu, tvořenou pletivovým plotem, nahradit kamenným plotem vysokým dva metry. Dále by pak dle zjištění bylo vylepšit systém kontroly vstupu o elektronickou kontrolu vstupů, v souvislosti s tímto systémem využít možnost pořízení turniketů. V rámci objektu firmy pak zřídit poplachový zabezpečovací a tísňový systém, využít pohybové elektromagnetické detektory a detektory na principu magnetického kontaktu umístěné v okenních rámech. Posledním z návrhových opatření je pak nahradit stávající videodohledový systém za systém modernější.

V návaznosti na závěry této práce lze uvést, že vytyčené cíle byly naplněny.

SEZNAM POUŽITÉ LITERATURY

ABBAS, a.s., ©2013-2023. Eshop.abbas.cz. [online]. [cit. 2023-04-17]. Dostupné z: https://eshop.abbas.cz/

ADAMEC, Vladimír, 2021. *Poznámky z předmětu „Metody hodnocení rizik*".

BAKER, Paul R. a Daniel J. BENNY, 2013. The complete guide to physical security. Boca Raton: CRC Press. ISBN 9781420099638

Betonové ploty Petr Harašta ©2010–2022. Betonovyplot.cz [online]. [cit. 2023-04-22]. Dostupné z: https://www.betonovyplot.cz/xx

ČSN EN 50131-1 ED.2 - *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2007. Česká technická norma.

ČSN CLC/TS 50131-7 - *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Česká technická norma.

ČSN EN 62676-1-1 - Dohledové videosystémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Česká technická norma.

ČSN EN 1627 (74 6001) - *Dveře, okna, lehké obvodové pláště, mříže a okenice – Odolnost proti vloupání – Požadavky a klasifikace*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012. Česká technická norma.

ČSN EN 60839-11-1 - *Poplachové a elektronické bezpečnostní systémy – Část 11-1: Elektronické systémy kontroly vstupu – Požadavky na systém a komponenty.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Česká technická norma.

ČSN 73 0875 - *Požární bezpečnost staveb – Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Česká technická norma.

ČSN 34 2710 - *Elektrická požární signalizace – Projektování, montáž, užívání, provoz, kontrola, servis a údržba*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Česká technická norma.

ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Česká technická norma.

ČSN EN ISO/IEC 27002. *Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Česká technická norma.

DETOMATIC s.r.o. Detomatic.cz [online]. [cit. 2023-04-23]. Dostupné z: https://www.detomatic.cz/

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* 4., aktualiz. a rozš. vyd. Praha: Professional Publishing. Expert (Grada). ISBN 978-808-8260-394.

DOUCEK, Petr, 2011. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. Vyd. Praha: Professional Publishing. ISBN 978-80-7431-050-8.

FÁBERA SYSTEMS s.r.o., © 2016. *Co je pyramida bezpečnosti.* Faberasystems.com [online]. [cit. 2023-02-21]. Dostupné z: Co je pyramida bezpečnosti? | Fábera systems s. r. o. (faberasystems.com)

IVANKA, Ján, 2014. *Mechanické zábranné systémy.* Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 978-80-7454-427-9. [online]. [cit. 2023-03-11]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/18575/Mechanicke_zabranne_systemy-obsah.pdf?sequence=2&isAllowed=y

JIRÁSEK, Petr, Josef POŽÁR, 2011. *Trendy a řešení v oblasti analýzy a monitoringu bezpečnostních* incidentů: Systém řízení informační bezpečnosti. Cybersecurity.cz. [online]. [cit. 2023-04-17]. Dostupné z: https://www.cybersecurity.cz/data/SRIB.pdf

KOLOUCH, Jan a Pavel BAŠTA, 2019. CyberSecurity. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 978-80-88168-34-8.

KYNCL, Jaromír, Martin KONEČNÝ a Luděk NOVÁK, 2014. Bezpečnost objektu ve světle moderních technologií. 4., aktualiz. a rozš. vyd. Praha: Komora podniků komerční bezpečnosti České republiky, 2014. Expert (Grada). ISBN 978-80-260-7115-0.

LAWRENCE, Fennelly. 2016. *Effective Physical Security.* Fitfh edition. Amsterdam: Butterworth-Heinemann. ISBN 9780128044629

LUKÁŠ, Luděk, 2011. *Bezpečnostní technologie, systémy a management I.* Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-05-7

LUKÁŠ, Luděk, 2012. *Bezpečnostní technologie, systémy a management II.* Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-19-4

LUKÁŠ, Luděk, 2013. *Bezpečnostní technologie, systémy a management III*. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-35-4.

MAISNER, Martin a Barbora VLACHOVÁ. Zákon o kybernetické bezpečnosti. Komentář. Praha: Wolters Kluwer, 2015. ISBN 978-807-4788-178.

MASLOW, Abraham Harold. 2014. *Toward a Psychology of Being*. Sublime Books. ISBN 978-1627556224.

Ministerstvo vnitra České republiky, 2016. *Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu.* [online]. Ministerstvo vnitra České republiky.

MORGAN, Jecinta, 2021. Difference between safety and security. In: Differencebetween.net [online]. Feb 12, 2011. [cit. 2023-03-11]. Dostupné z: http://www.differencebetween.net/language/words-language/difference-between-safety-and-security/

NAKONEČNÝ, Milan, 2014. *Motivace chování.* 3. přeprac. vyd. Praha: Triton. ISBN 978-807-3878-306.

NÁRODNÍ KNIHOVNA ČR (NKP), © 2004-2014. Bezpečnost, etymologie slova. Ptejteseknihovny.cz [online]. [cit. 2023-02-21]. Dostupné z: https://www.ptejteseknihovny.cz/dotazy/bezpecnost-etymologie-slova

SECURITAS ČR s.r.o., 2021. *Termokamery a GDPR: Na co si dát pozor.* Securitas.cz [online]. [cit. 2023-04-03]. Dostupné z: https://www.securitas.cz/novinky--blog/blog/termokamery-a-gdpr-na-co-si-dat-pozor/

SMEJKAL, Vladimír a Karel RAIS. 2013. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada. ISBN 978-80-247-4644-9.

UHLÁŘ, Jan, 2014. *Technické prostředky ochrany objektů*. Praha: Vysoká škola regionálního rozvoje Praha. ISBN 978-80-87174-33-3.

URBAN, Miroslav, 2019. *Moderní dohledová poplachová a přijímací centra*. Portál pro technické zařízení budov. [online]. 27.11.2017 [cit. 2023-04-15]. Dostupné z: https://www.tzb-info.cz/poplachove-a-zabezpecovaci-systemy/16607-moderni-dohledova-poplachova-a-prijimaci-centra-reprezentuji-vic-nez-jen-terminologickou-zmenu.

Ústavní zákon č. 1/1993 Sb., *Ústava České republiky*

Zákon č. 412/2005 Sb., *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti*

Zákon č. 89/2012 Sb., *Občanský zákoník*

Zákon č. 40/2009 Sb., *Trestní zákoník*

Zákon č. 181/2014 Sb., *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů* (zákon o kybernetické bezpečnosti)

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČSN Česká státní norma

DPPC Dohledové a poplachové přijímací centrum

EKV Elektronická kontrola vstupů

EN Evropská norma

EPS Elektronická požární signalizace

ICT Informační a komunikační technologie

ISMS Systém řízení bezpečnosti informací

ISO International organization for standardization přeloženo do českého jazyka Mezinárodní organizace pro normalizaci

MVČR Ministerstvo vnitra České republiky

MZS Mechanické zábranné systémy

NBÚ Národní bezpečnostní úřad

PZTS Poplachové zabezpečovací a tísňové systémy

SKV Systém kontroly vstupu

UI Utajované informace

VDS Videodohledové systémy

SEZNAM OBRÁZKŮ

SEZNAM TABULEK