

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra systémového inženýrství



DIPLOMOVÁ PRÁCE

**Aplikace systémového přístupu v oblasti objektové
bezpečnosti**

Autor: Karel ZEDEK

© 2015 ČZU V PRAZE

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra systémového inženýrství

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Zedek Karel

Veřejná správa a regionální rozvoj nav.- Klatovy

Název práce

Aplikace systémového přístupu v oblasti objektové bezpečnosti

Anglický název

Application of systems approach to building security management

Cíle práce

Cílem diplomové práce je pomocí metod vícekriteriálního rozhodování, matematických metod podpořit technické řešení při výběru nové techniky pro vyšší stupeň zabezpečení objektů a oblastí.

Metodika

- nastudování odborné literatury
- výběr metod vícekriteriálního rozhodování
- zpracování dat pomocí modelů vícekriteriálního rozhodování
- interpretace výsledků a ekonomická analýza projektu
- návrh při výběru nové zabezpečovací techniky
- ekonomická analýza řešení

Harmonogram zpracování

- 03/2014 – výběr tématu
- 05/2014 - konkretizace tématu, osnova práce
- 05/2014 - účast semináři k tématu diplomové práce
- 05-06/2014 – vytvoření zadání diplomové práce
- 07-08/2014 studium literatury
- 09-11/2014 – zpracování teoretické části, konzultace s vedoucím práce
- 12/2014 – zpracování praktické části, konzultace s vedoucím práce
- 01/2015 - předložení práce vedoucímu
- 02/2015 – editace práce, zapracování připomínek, finalizace
- 03/2015 - odevzdání kompletní práce

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma „**Aplikace systémového přístupu v oblasti objektové bezpečnosti**“ vypracoval samostatně, pod vedením doc. Ing. Milana HOUŠKY, Ph.D a použil jen prameny, které uvádím v seznamu použitých zdrojů.

Praha, . listopadu 2015

.....
Bc. Karel ZEDEK

Poděkování

Rád bych touto cestou poděkoval panu doc. Ing. Milanu HOUŠKOVÍ, Ph.D., vedoucímu práce a panu Ing. Oldřichu LUŇÁČKOVÍ, Ph.D., za odbornou pomoc, cenné připomínky a odborné konzultace, které mi v průběhu zpracování této diplomové práce poskytovali. Dále bych rád poděkoval rodině, která mě po celou dobu mého studia plně a trpělivě podporovala.

Aplikace systémového přístupu v oblasti objektové bezpečnosti

Application of systems approach to building security management

Souhrn

Projekt fyzické bezpečnosti je dokument, který musí zpracovat každý subjekt, který bude ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti nakládat s utajovanými informacemi ať už jako podnikatel nebo orgán státní správy.

Cílem diplomové práce je vypracovat projekt vyššího stupně zabezpečení ochrany utajovaných informací v souladu se zákonem 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, popsat systémy ochrany v oblasti fyzické (objektové) bezpečnosti pro všechny, kteří se touto problematikou zabývají.

Výsledkem práce bylo zhodnocení stávajícího stavu zabezpečení objektu, vyhodnocení rizik, která nás v této oblasti ohrožují a navrhnutí projektu pro vyšší stupeň fyzického zabezpečení tohoto objektu a zabezpečené oblasti dle vyhlášky č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

Výstupem diplomové práce je zpracovaný projekt fyzické bezpečnosti pro společnost Product Security a.s.

Klíčová slova: fyzická bezpečnost, ochrana utajovaných informací, zabezpečená oblast, projekt fyzické bezpečnosti

Summary

Physical security project is a document that must handle each entity within the meaning of the Act no. 412/2005 Coll., on protection of classified information and security capacity to deal with classified information, whether as a business or a government body.

The aim of this thesis project is to develop a higher level of security protection of classified information in accordance with the Act 412/2005 Coll., on protection of classified information and security capacity, describe protection systems in physical (object) for the safety of all those who deal with this issue.

The result of this work was to evaluate the current state of building security, risk assessment, which we in this area compromise and propose a project for a greater degree of physical security of the building and secure the area. according to Decree no. 528/2005 Coll. on physical security and certification of technical means, as amended.

The outcome of the thesis is the design of physical security for the company as Product Security.

Keywords: physical security, protection of classified information, secured area, physical security project

Obsah

ÚVOD	9
CÍL PRÁCE A METODIKA	11
I. TEORETICKÁ ČÁST	12
1 LEGISLATIVA FYZICKÉ BEZPEČNOSTI	13
1.1 Zákony, vyhlášky a právní předpisy fyzické bezpečnosti	13
1.2 Vymezení pojmů	14
1.2.1 Zabezpečená oblast.....	15
1.2.2 Jednací oblast	15
1.2.3 Objekt	15
1.2.4 Hranice objektu	15
1.2.5 Vstup do objektu	15
1.2.6 Hrozba	15
1.2.7 Riziko	15
1.2.8 Mimořádná situace	16
1.2.9 Technický prostředek	16
1.2.10 Úschovný objekt.....	16
1.2.11 Vedoucí organizačního celku	16
1.2.12 Návrh bezpečnostního projektu	16
1.3 Stupně utajení	16
1.4 Systémový přístup	17
1.5 Fyzická bezpečnost.....	17
1.6 Ochrana objektu	18
1.6.1 Ostraha.....	18
1.6.2 Režimová opatření.....	19
1.6.3 Technické prostředky	20
2 FYZICKÁ BEZPEČNOST Z HLEDISKA TECHNICKÉ OCHRANY OBJEKTŮ	22
2.1 Mechanické zábranné systémy	22
2.1.1 Obvodová ochrana.....	24
2.1.2 Plášťová ochrana	26
2.1.2.1 Vstupní otvorové výplně	27
2.1.2.2 Okna a balkonové dveře	28
2.1.2.3 Mříže, rolety, žaluzie	28
2.1.2.4 Bezpečnostní folie a skla, vrstvený polykarbonát	29
2.1.3 Předmětová ochrana	30

2.1.3.1	Komerční úschovné objekty	31
2.1.3.2	Komorové trezory.....	32
2.1.4	Stanovení minimální doby průlomové odolnosti úschovných objektů.....	33
2.1.5	Stupně rizika ohrožených objektů	34
2.1.6	Koeficienty průlomové odolnosti úschovných objektů	35
2.1.7	Trezorové bezpečnostní třídy	35
2.1.7.1	Trezorová bezpečnostní třída 0.....	37
2.1.7.2	Trezorová bezpečnostní třída I.	37
2.1.7.3	Trezorová bezpečnostní třída II.	37
2.1.7.4	Trezorová bezpečnostní třída III.....	37
2.2	Poplachový zabezpečovací a tísňový systém a systémy pro kontrolu vstupů.....	38
2.2.1	Systémy pro kontrolu vstupu.....	38
2.2.2	Ústředna.....	39
2.2.3	Ovládací klávesnice.....	40
2.2.4	Detektory (čidla).....	40
2.2.4.1	PIR detektory.....	41
2.3	Speciální televizní systémy	44
2.4	Elektrická požární signalizace.....	45
2.5	Zařízení fyzického ničení nosičů informací	46
2.6	Certifikace NBÚ - ochrana utajovaných informací.....	47
II.	PRAKTICKÁ ČÁST	49
3	POPIS A POSOUZENÍ STÁVAJÍCÍHO ZABEZPEČENÍ ROZSÁHLÉHO OBJEKTU ..	50
3.1	Charakteristika areálu a objektu	51
3.2	Současné zabezpečení a stanovení hranice zabezpečené oblasti	51
3.2.1	Přehled použitých technických prostředků.....	52
3.2.2	Stanovení zabezpečených oblastí	52
3.2.3	Stanovení hranice zabezpečené oblasti.....	52
3.2.4	Přijátá režimová opatření fyzické bezpečnosti	53
3.2.5	Technická dokumentace FB	54
3.2.5.1	Výkresová dokumentace	54
3.2.6	Dokumentace technických prostředků.....	55
3.2.7	Ověřování funkčnosti technických prostředků	56
3.3	Návrh vyššího zabezpečení	57
3.4	Režimová opatření.....	57
3.5	Stupeň utajení utajovaných informací	58

3.6	Druh utajovaných informací.....	58
3.7	Četnost manipulace s UI.....	58
3.8	Místa výskytu utajovaných informací	58
3.9	Stanovení jednotlivých hrozeb, zranitelnosti UI a jejich vyhodnocení	59
3.9.1	Vyzrazení UI oprávněnými osobami.....	59
3.9.2	Manipulace s UI neoprávněnými osobami	59
3.9.3	Poškození (zničení) UI živelnou pohromou	60
3.9.4	Poškození (zničení) UI průmyslovou nebo technologickou havárií.....	60
3.9.5	Ztráta UI následkem teroristického útoku	61
3.9.6	Vyzrazení UI pasivním odposlechem nebo nasazením operativní techniky	61
3.9.7	Vyzrazení nebo ztráta UI z informačního systému.....	61
3.9.8	Poškození (zničení) UI v ostatních případech	62
3.9.9	Stanovení celkové míry rizika	62
3.10	Projekt fyzické bezpečnosti.....	63
3.11	Návrh projektu fyzické bezpečnosti	64
4	ZÁVĚR.....	65
	SEZNAM POUŽITÉ LITERATURY	66
	SEZNAM POUŽITÝCH ZKRATEK A POJMŮ.....	69
	SEZNAM OBRÁZKŮ.....	70
	SEZNAM TABULEK	71
	SEZNAM PŘÍLOH	72

Úvod

Fyzická, dříve nazývaná objektová bezpečnost, je od nepaměti velmi složitým systémovým procesem, kterým se zabezpečuje ostraha objektů jak technickými prostředky, tak i personálním zajištěním ostrahy před narušením, napadením, krádeží a v neposlední řadě úniku utajovaných a citlivých informací, osobních údajů či zvláštních skutečností. Historie fyzické bezpečnosti sahá hluboko do minulosti.

Již v pravěku a v pozdější době lidé mysleli na ochranu svých obydlí pomocí primitivních prvků ochrany. Vedly je k tomu různé důvody od náboženských, přes ideologické až čistě po zjištěné.

Vezmeme-li v úvahu samostatnou Československou či Českou republiku zjistíme, že první zákon na ochranu republiky byl vydán v roce 1923, který byl tvořen 8 stranami textu. V roce 1948 po komunistickém převratu a po znárodnění majetku byl vydán zákon na ochranu lidově demokratické republiky č. 231/1948. Dalším zákonem, který řešil tuto problematiku, byl zákon o státním tajemství (stupeň PTZD – přísně tajné zvláštní důležitosti) vydaný v roce 1970. Po společenských změnách na konci 80. let 20. století a zejména díky integraci České republiky do mezinárodních struktur byl vydán zákon č.148/1999 Sb., o utajovaných skutečnostech. Tento zákon vyžadoval mnoho změn, a proto byl v roce 2005 vydán zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Tento základní právní předpis stanovuje povinnosti a pravidla pro práci s utajovanými informacemi. Porušením těchto povinností a pravidel může dojít ke spáchání přestupku nebo jiného správního deliktu a v neposlední řadě ke spáchání trestného činu. Z tohoto zákona bude v této práci ještě mnohokrát citováno.

Práce s utajovanými informacemi je velmi citlivá záležitost, ke které je třeba přistupovat velmi zodpovědně.

V dnešní složité době při vzrůstající kriminalitě a vysokého technického vybavení pachatelů, kteří jsou svou vynalézavostí stále drzejší, je třeba nepodceňovat ostrahu objektů a velmi důkladně ji naplánovat a všemi možnými a dostupnými prostředky nám svěřený majetek a poté zvlášť utajované a citlivé informace chránit.

Vybudování ochrany utajovaných informací zahrnuje soustavu několika do sebe zapadajících systémů, které jsou na sobě závislé a splňují požadavky předepsané již zmíněným právním předpisem. Dokument, který řeší provedení zabezpečení objektu a další

přijatá opatření k ochraně utajovaných informací se nazývá – projekt fyzické bezpečnosti. Bez tohoto dokumentu se nelze v zabezpečeném objektu (oblasti) seznamovat a ani pracovat s utajovanými informacemi.

Diplomová práce může být využita bezpečnostním managementem v soukromém sektoru, jak tomu je i v této práci, tak hlavně ve složkách, které jsou zahrnuty v integrovaném záchranném systému (policie, armáda atd...). V institucích veřejného sektoru se jedná hlavně o personální bezpečnost ve vztahu k významnému rozsahu dat, se kterými operuje.

CÍL PRÁCE A METODIKA

Cíl práce

Cílem diplomové práce je vypracovat projekt vyššího stupně zabezpečení ochrany utajovaných informací a popsat systémy ochrany v oblasti fyzické (objektové) bezpečnosti pro všechny, kteří se touto problematikou zabývají. Dalším cílem je vyhodnotit rizika, která nás v této oblasti ohrožují. U vybraného objektu zhodnotit stávající stav zabezpečení a navrhnout projekt pro vyšší stupeň fyzického zabezpečení objektu a zabezpečené oblasti.

Metodika práce

Diplomová práce bude rozdělena do dvou částí. V teoretické části práce bude popsáno zajištění objektu z obecného hlediska, budou vysvětleny základní pojmy, které budou předmětem této práce. Bude vysvětleno vše, co bude potřeba na ochranu a bezpečnost objektů proti neoprávněné manipulaci a úniku utajovaných informací.

V praktické části bude popsán rozsáhlý objekt firmy Product Security a.s. (po dohodě s vedoucím práce změněn název a parametry objektu z důvodu utajení skutečného subjektu) a v něm vybraná budova, kde bude provedena analýza stávajícího stavu fyzického zabezpečení a bude navržen nový bezpečnostní projekt na vyšší stupeň zabezpečení. V zabezpečené oblasti se budou ukládat utajované informace podléhající stupni utajení Důvěrné a Tajné.

I. TEORETICKÁ ČÁST

1 Legislativa fyzické bezpečnosti

V našem právním řádu dnes nenajdeme žádnou právní legislativu, která by samostatně právně upravovala činnost v oblasti fyzické bezpečnosti, ochrany osob a majetku. Proto musíme vycházet z mnoha jiných právních předpisů.

1.1 Zákony, vyhlášky a právní předpisy fyzické bezpečnosti

Jedna z prvních právních úprav fyzické bezpečnosti byla řešena ve Vyhlášce Národního bezpečnostního úřadu č. 258/1998 Sb. o objektové bezpečnosti ze dne 30. října 1998, která byla dnem 28. prosince 1999 zrušena a nahrazena předpisem 339/1999 Sb., s účinností od 28. prosince 1999.

Fyzická bezpečnost se postupem času rychle vyvíjela, a proto bylo žádoucí reflektovat tyto změny a připravit a schválit nový zákon řešící adekvátně tuto problematiku.

V roce 2005 ze dne 21. září byl schválen zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, který nabyl účinností 1. ledna 2006. Tímto dnem se upustilo od názvu objektová bezpečnost a nahradil ho název „fyzická bezpečnost“.

Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.¹

V souvislosti se zákonem 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti byly vydány právní prováděcí předpisy (vyhlášky) Národního bezpečnostního úřadu, které doplňují zákon a upravují jednotlivé druhy zajištění ochrany utajovaných informací do větších detailů:

- Vyhláška č. 523/2006 Sb. *„O bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládající s utajovanými informacemi a o certifikaci stínících komor“*,
- Vyhláška č. 525/2006 Sb. *„O provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací“*,

¹ § 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

- Vyhláška č. 526/2005 Sb. „ *O stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti)*“,
- Vyhláška č. 527/2005 Sb. „*O stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti)*“,
- Vyhláška č. 528/2006Sb. „*O fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů*“,
- Vyhláška č. 529/2006 Sb. „ *O administrativní bezpečnosti a o registrech utajovaných informací*“,
- Vyhláška č. 363/2011 Sb. „*O personální bezpečnosti a o bezpečnostní způsobilosti*“,
- Vyhláška č. 405/2011 Sb. „*O průmyslové bezpečnosti*“,
- Vyhláška č. 432/2011 Sb. „ *O zajištění kryptografické ochrany utajovaných informací*“, ve znění vyhlášky č. 417/2013 Sb.,
- *Prováděcí právní předpisy k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti),²*
- Vyhláška č. 522/2005 Sb. „*Nářízení vlády, kterým se stanoví seznam utajovaných informací (SUI)*“,
- *Normativní výnos Ministerstva obrany č.77/2013 “ Fyzická bezpečnost v rezortu Ministerstva obrany”.*

1.2 Vymezení pojmů

Zákon č. 412/2005 Sb. a další právní prováděcí předpisy definují základní pojmy z oblasti fyzické bezpečnosti. Jako stěžejní byly vybrány následující pojmy:

² <https://www.govcert.cz/cs/legislativa/legislativa/>

1.2.1 Zabezpečená oblast

- Prostor, který je ohraničený a ve kterém se ukládají utajované informace. Zabezpečenou oblast tvoří např. místnost, několik místností, trakt budovy nebo i celá budova s uzamykatelnými vstupy zabezpečenými průleznými otvory). V polních podmínkách ji tvoří např. ohraničený uzavřený prostor pro osádku (přepravované osoby nebo náklad) dopravního prostředku nebo vojenské techniky, kontejner, stan apod.³

1.2.2 Jednací oblast

- Jednací oblastí je ohraničený prostor v objektu. Utajovanou informaci stupně utajení Přísně tajné nebo Tajné lze pravidelně projednávat pouze v jednací oblasti.

1.2.3 Objekt

- Prostor, který je ohraničený a ve kterém se zpracovávají utajované informace. Objekt tvoří např. část areálu nebo celý areál dislokace organizačního celku nebo pracoviště, budova anebo její část, skupina místností nebo pouze jedna místnost. V polních podmínkách je to ohraničený prostor vymezený pro vytvoření zabezpečené oblasti.⁴

1.2.4 Hranice objektu

- Plášť budovy, fyzická bariera (oplocení) nebo jinak viditelně vymezená hranice.

1.2.5 Vstup do objektu

- Místo určené pro vstup a výstup osob a místo pro vjezd a výjezd dopravních prostředků.

1.2.6 Hrozba

- Možnost vyražení nebo zneužití utajované informace při narušení objektové (fyzické) bezpečnosti.

1.2.7 Riziko

- Pravděpodobnost, že se určitá hrozba uskuteční.

³ Čl. 10 a 11 RMO č. 14/2013 Věstníku *Ochrana utajovaných informací v rezortu Ministerstva obrany*

⁴ § 24 odst. 2,4 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

1.2.8 Mimořádná situace

- Stav, kdy bezprostředně hrozí, že dojde k vyrazení nebo zneužití utajované informace.

1.2.9 Technický prostředek

- Bezpečnostní prvek, jehož použitím se zabraňuje, ztěžuje, oznamuje nebo zaznamenává narušení zabezpečení objektu, zabezpečené oblasti a dále ničí utajované informace.

1.2.10 Úschovný objekt

- Trezor nebo jinak uzamykatelná schránka stanovená v příloze č. 1 vyhlášky.⁵

1.2.11 Vedoucí organizačního celku

- Osoba pověřená plněním povinností ve vztahu k fyzické (objektové) bezpečnosti.⁶

1.2.12 Návrh bezpečnostního projektu

- Analýza stávajícího stavu fyzické bezpečnosti a návrh opatření fyzické bezpečnosti k ochraně utajovaných informací stanoveného stupně utajení, jehož obsahem je návrh instalace technických prostředků do budov a objektů rezortu.⁷

1.3 Stupně utajení

Utajovaná informace, která je chráněna souborem opatření fyzické bezpečnosti se ukládá v zabezpečené oblasti a klasifikuje se stupněm utajení:

- *Přísně tajné* – jestliže její vyrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmů České republiky,
- *Tajné* - jestliže její vyrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,
- *Důvěrné* - jestliže její vyrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,
- *Vyhrazené* - jestliže její vyrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.⁸

⁵ § 2 odst. b,d,f,g,i,j Vyhlášky č. 528/2005 o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů

⁶ Čl. 4 odst. a) a čl. 57 RMO č. 14/2013 Věstníku

⁷ Čl. 2 odst. i) NVMO č. 77/2013 Fyzická bezpečnost v resortu Ministerstva obrany

⁸ § 4 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

1.4 Systémový přístup

Na zajištění fyzické bezpečnosti se můžeme dívat jako na systém, který je v teorii systémů definován jako množina prvků a množina vazeb mezi nimi, které společně určují vlastní fyzickou bezpečnost.

Zásada systémového přístupu vyžaduje zabývat se všemi prvky systému v jejich vzájemném působení a vazbou na okolí. Opomine-li se některý s prvků systému ochrany utajovaných informací nebo jeho vliv, v neposlední řadě to může mít nedozírné a nevratné následky.

Komplexnost systémového přístupu a jeho aplikace je potřeba při jeho projektování respektovat a na její tvorbu prosazovat obsazováním potřebných specialistů na jednotlivé obory bezpečnosti.⁹

1.5 Fyzická bezpečnost

Cílem provádění fyzické bezpečnosti je navrhnout takový systém zabezpečení, který by měl zabránit proniknutí nepovolané osoby do objektu, zjišťovat proniknutí nepovolané osoby do objektu, činit opatření k minimalizaci následků proniknutí nepovolané osoby do objektu a předcházet úniku, ztrátě, znehodnocení nebo zničení utajované skutečnosti v důsledku vzniku mimořádné události.¹⁰

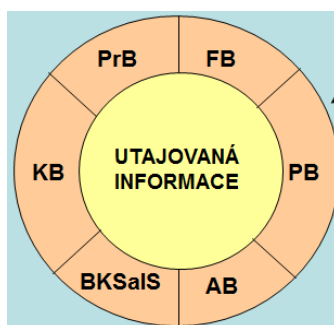
Aby byla fyzická bezpečnost k ochraně utajovaných informací funkční, musíme aplikovat systémový přístup v několika druzích zajištění ochrany:

- personální bezpečnost - kterou tvoří výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím, jejich výchova a ochrana,
- průmyslová bezpečnost - kterou tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu s tímto zákonem,

⁹ NĚMEC, V., *Projektový management*, s. 26

¹⁰ LAUCKÝ, V., *Technologie komerční bezpečnosti I*, s. 81

- administrativní bezpečnost - kterou tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi,
- fyzická bezpečnost - kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat,
- bezpečnost informačních nebo komunikačních systémů - kterou tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému,
- kryptografickou ochranou - kterou tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací.¹¹



Obrázek č. 1 Schéma systému ochrany utajovaných informací

1.6 Ochrana objektu

Ochrana objektu se zabezpečuje kombinací těchto bezpečnostních opatření:

- ostraha,
- režimová opatření,
- technické prostředky.

1.6.1 Ostraha

Ostraha se nepřetržitě zajišťuje u objektu, ve kterém se nachází zabezpečená oblast kategorie:

- přísně tajné, nejméně 2 osobami u objektu,

¹¹ § 5 odst. a,b,c,d,e,f zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

- tajné, nejméně 1 osobou u objektu a 1 další osobou, které kombinace opatření podle §30 odst. 1 písm. b), c) a f) umožní rychlý zásah, je-li provádění ochrany utajovaných informací narušeno,
- důvěrné, nejméně 1 osobou, které kombinace opatření podle § 30 odst. 1 písm. b) a c) umožní rychlý zásah, je-li provádění ochrany utajovaných informací narušeno.¹²

Ostraha objektů je vykonávána:

- proškolenými zaměstnanci provozovatele objektu,
- příslušníky ozbrojených sil nebo ozbrojených sborů nebo zaměstnanci pověřené bezpečnostní služby.

V případě objektu, ve kterém se nachází zabezpečená oblast kategorie Důvěrné, Tajné anebo Přísně tajné nebo jednacích oblastí, je nutné stanovit pravidla pro výkon ostrahy v písemné formě. V zabezpečených oblastech, ve kterých se ukládají utajované informace Evropské unie stupně utajení Důvěrné a vyšší, se zabezpečuje ostrahou typu 2 a vyšší s tím, že frekvence obchůzek musí být stanovena v intervalech ne větších než 2 hodiny. První obchůzka ostrahy se provede ihned po skončení pracovní doby.

V případě vyhlášení poplachu v zabezpečené oblasti nebo jednacích oblastech kategorie Přísně tajné a Tajné musí být ostraha schopna do 5 minut od přijetí poplašného nebo nouzového signálu z objektu, provést zásah na příslušném stanovišti.

Ostrahu typu 1 lze použít jen pro zabezpečené oblasti kategorie Důvěrné nebo Vyhrazené. Ostraha musí být vybavena při obchůzce prostředky umožňující spojení se stanovištěm pro stálý výkon ostrahy. Doba reakce ostrahy na poplašný nebo nouzový signál musí být ověřována provozovatelem objektu.¹³

1.6.2 Režimová opatření

Předmětem těchto opatření jsou vypracované směrnice dané organizací, dle kterých se řídí jak vlastní zaměstnanci tak i cizí osoby přicházející do objektu. Nedodržení těchto bezpečnostních směrnic může být narušen systém fyzické bezpečnosti a ohrožena ochrana utajovaných skutečností.

¹² § 28 odst 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

¹³ Příloha 1 k vyhlášce č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 425/2011 Sb.

Režimová opatření stanoví vedoucí organizačního celku v projektu fyzické bezpečnosti s využitím článku 9.¹⁴

Režimová opatření nám stanoví:

- oprávnění osob a dopravních prostředků pro vstup a vjezd do objektu, oprávnění osob pro vstup do ZO a JO a podmínky a způsob kontroly vynášení a vyvážení věcí nebo utajovaných skutečností z objektu,
- režim pohybu osob, věcí, dopravních prostředků a utajovaných skutečností v objektu a jeho jednotlivých částech v pracovní a mimopracovní době,
- způsob manipulace s klíči a identifikačními prostředky a medii, které se používají pro systémy zabezpečení vstupů (elektrická zámková zařízení a systémy pro kontrolu vstupů), kterými se zejména určuje systém a způsob označování, přidělování a odevzdávání klíčů, jejich úschovy a evidence, uložení duplikátů a způsob jejich používání,¹⁵
- způsob manipulace s technickými prostředky a jejich používání.

Veškerá oprávnění k režimovým opatřením vydává odpovědná osoba nebo jí pověřená osoba. Oprávnění ke vstupu do zabezpečené oblasti stanovené kategorie lze vydat pouze osobě, která je držitelem „Oznámení o splnění podmínek“ pro přístup k utajovaným informacím stupně utajení Vyhrazené nebo „Osvědčení fyzické osoby“ příslušného stupně utajení Důvěrné a vyšší a je řádně poučena.

1.6.3 Technické prostředky

Po ostraze je to jeden z nedůležitějších systémů zabezpečení objektů. Technickým prostředkem je bezpečnostní prvek, jehož použitím se zabráňuje nebo omezuje narušení ochrany objektu nebo zabezpečené oblasti. Cílem technického zabezpečení je vyplnit slabá místa fyzické ostrahy, nepřetržité střežení a monitorování chráněného objektu.

Technickými prostředky zejména jsou:

- mechanické zábranné prostředky – mezi ně řadíme úschovné objekty, zámky, dveře, mříže, fólie, bezpečnostní rámy a skla,
- systémy EZS – zařízení elektronické zabezpečovací signalizace, sloužící k zajišťování a vyhodnocování neoprávněného vstupu,

¹⁴ Čl.8 NVMO č.77/2013 Fyzická bezpečnost v resortu Ministerstva obrany

¹⁵ <http://www.magazin.specialista.info/view.php?cisloclanku=2005100201>

- systémy SKV – systémy pro zabezpečení a kontrolu vstupu do objektů, zabezpečených oblastí, zařízení sloužící k elektronickému prokazování oprávněnosti a totožnosti osob, případně kontroly auditu kontrolu,
- tísňové systémy - zejména tísňové hlásiče fungující jako součást elektronického zabezpečení,
- systémy EPS – zařízení elektronické požární signalizace,
- systémy CCTV – speciální televizní systémy pro snímání a zobrazování pohybu osob a dopravních prostředků v objektech,
- systémy na detekci látek a vyhledávání kovů,
- zařízení fyzického ničení nosičů informací,
- zařízení proti aktivnímu a pasivnímu odposlechu utajovaných informací z vnějšího prostředí.¹⁶

¹⁶ § 30 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

2 FYZICKÁ BEZPEČNOST Z HLEDISKA TECHNICKÉ OCHRANY OBJEKTŮ

V této kapitole se budeme věnovat již zmíněným technickým prostředkům podrobněji. Popíšeme si řadu systémů, prostředků a příslušenství, které se používají k nepřetržitému střežení objektu.

V předchozí kapitole byly zmíněny technické prostředky, které se používají pro ochranu objektů. Nyní si v této kapitole popíšeme systémy, které řadíme mezi nejvíce používané technické prostředky:

- mechanické zábranné systémy,
- poplachový zabezpečovací a tísňový systém a systémy pro kontrolu vstupů,
- zařízení elektronické požární signalizace,
- zařízení fyzického ničení informací.

2.1 Mechanické zábranné systémy

Mechanická ochrana objektů a majetků je stará jako samo lidstvo. Jednoduché stavby kolem osad, pevností a hradeb nepředstavovaly nic jiného než zřizování mechanických zábranných systémů k ochraně a bezpečnosti proti útokům a napadení nepřítelem, zabezpečení jak života a zdraví obyvatel, tak i jejich majetku. Jejich posláním z hlediska bezpečnosti je odradit, ztížit nebo i zcela znemožnit pachateli jeho vniknutí do chráněného objektu. Charakteristickým znakem těchto překážek (zábran) je jejich bezpečnostní úroveň určující pasivní bezpečnost resp. průlomovou odolnost. Základní úlohou je vytvořit pevnou hranici, která stěžuje násilné vniknutí nepovolané osoby do chráněné zóny nebo objektu (především přes oplocení, dveřními nebo okenními otvory) a vytvořit tak co nejdelší dobu, kterou musí pachatel vynaložit na její překonání, aby byla pro pachatele neúnosná.

Mechanické zábranné systémy (SM) jsou jedním z technických prvků ve struktuře Integrovaného bezpečnostního systému, kde můžeme uvést ještě systémy signalizační a monitorovací (SE), systémy organizačních opatření a ostrahy (SO). Integrovaný bezpečnostní systém lze definovat jako neprázdnou množinu **S**, tvořenou množinou prvků **M**, univerzem

systemu a množinou G , charakteristickou systemu, danou závislostmi mezi veličinami prvků množiny M i mezi prvky množiny M a okolím systemu:¹⁷

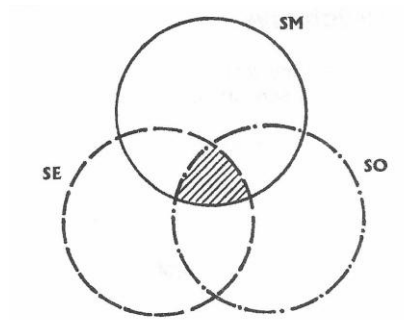
$$IBS = \{M, G\}$$

kde:

- universum Integrovaného bezpečnostního systemu M je tvořeno prvky množiny SM , SE a SO ,
- charakteristiky G je tvořena vazbami mezi prvky M a okolím systemu.



Obrázek č. 2 System bezpečnosti a ochrany majetku¹⁸



Obrázek č. 3 System bezpečnosti a ochrany majetku¹⁹

Integrovaný bezpečnostní system má smysl jako celek a jeho účinnost lze hodnotit pozitivně pouze v případě, že jeho reakce pokryje časový interval potřebný k překonání překážky pachatelem.

Doba, kterou musí pachatel vynaložit na překonání mechanické pevnosti MZS, se nazývá **průlomová odolnost**.

Překonatelnost každého mechanického zábranného systemu se liší množstvím vydané energie a druhu náradí použitých k překonání dané překážky. Tím je určena úroveň bezpečnostního objektu.

Postavením mechanických zábranných systemů v systemu komplexního zabezpečení je dáno jejich schopností vytvořit kvalifikovanou zábranu proti průniku pachateli do

¹⁷UHLÍŘ, J., *Technická ochrana objektů. I. díl Mechanické zábranné systémy II*, s. 11,13

¹⁸IVANKA, J., *Mechanické zábranné systémy*, s. 3

¹⁹UHLÍŘ, J., *Technická ochrana objektů. I. díl Mechanické zábranné systémy II*, s. 14

chráněného objektu, což je vyjádřeno maximálním prodloužením časového intervalu Δt , který pachatel potřebuje k překonání překážky a tím k dosažení svého cíle. Tento vztah můžeme vyjádřit:

$$\Delta t = t_2 - t_1 \text{ (min)}$$

kde:

Δt časový interval potřebný k překonání překážky

t_1 čas zahájení útoku na překážku

t_2 čas konečného překonání překážky²⁰

Mechanické zábranné systémy nasazené na ochranu objektů lze rozdělit do tří okruhů ochranných zón:

- **Obvodová ochrana** – zajišťuje bezpečnost po obvodu chráněného objektu nebo prostoru. Obvodem objektu většinou rozumíme jeho katastrální hranice ohraničené obvykle přírodními nebo umělými bariérami (ploty, zdi atd.) na přilehlých pozemcích.
- **Plášťová ochrana** - je základem ochrany při střežení hranice objektu. Zahrnuje technická opatření, která znemožňuje únik informací z pláště objektu. Je nasazována na nejcitlivější místa průlomu, jako jsou dveře, okna. Nasazením plášťové ochrany představuje jeden z nejlepších způsobů zabezpečení a její výhodou je rychlá detekce při pokusu o vniknutí přes plášť střeženého objektu a je umístována právě u dveří a oken.²¹
- **Předmětová ochrana** – zabezpečuje prostory nebo úschovná místa, kde jsou uloženy utajované informace, cenné předměty před neoprávněnou manipulací s nimi popř. pokusu o jejich zcizení.

2.1.1 Obvodová ochrana

Základním prvkem obvodové (perimetrické) ochrany je zajistit vnější ochranu objektu na jeho hranici, a v prostoru mezi objektem a touto stanovenou hranicí. Tato hranice musí být jednoznačně stanovena přírodními nebo umělými překážkami (plot, zeď). Jedná se o oplocení

²⁰IVANKA, J. *Mechanické zábranné systémy*, s. 44

²¹ <http://www.ictsecurity.cz/odborne-clanky/fyzicka-ochrana-dat.html>

o ohrazení hlídané oblasti (pozemku) včetně vstupních branek, bran, závor, propustí apod., které omezují přístup nežádoucích osob do chráněného prostoru. Na hranici perimetru je možné detekovat možné změny na oplocení či jeho narušení nepovolanou osobou ještě dříve, než se prostorem areálu přiblíží ke střeženým objektům. Vhodným doplněním ochrany perimetru je použití infračervených nebo mikrovlnných bariér a detektorů. Pro perimetrickou ochranu lze také zvážit nasazení kamerového systému, jehož monitorovací a vyhodnocovací zařízení je vybaveno poplachovým systémem, který vyhodnocuje změny ve snímané scéně a následně vyhlásí poplach.²²

Obecně lze mechanické zábranné systémy obvodové ochrany, které se skládají nejen z drátěného oplocení a pevných bariér, ale i doplňkových prvků, rozdělit do šesti základních skupin:

- klasické drátěné, dřevěné, zděné oplocení,
- bezpečnostní oplocení,
- vysoce bezpečnostní oplocení,
- vrcholové zábrany,
- podhrabové překážky,
- vstupy, vjezdy a jiné vstupní jednotky.²³

Dle typu stupně ochrany musí být hranice perimetru tvořena po celém obvodu fyzickou bariérou (plotem). Fyzické bariéry jsou vyžadovány po celém obvodu hranice objektu tam, kde to umožňuje její charakter. Konstrukce přístupových bodů (vstupních bran) musí být na stejné bezpečnostní úrovni jako konstrukce fyzické bariéry (oplocení). Na všech přístupových bodech musí být zajištěn stejný standard kontroly vstupu.



Obrázek č.4 Fyzická bariera typu 4



Obrázek č. 5 Samonosná bezpečnostní brána²⁴

²²<https://moodle.unob.cz/pluginfile.pdf>

²³ UHLÍŘ, J., *Technická ochrana objektů. I.díl Mechanické zábranné systémy II*, s. 23

²⁴ www.dirickx.cz

2.1.2 Plášťová ochrana

Základními zabezpečovacími prvky plášťové ochrany jsou mechanické zábranné systémy, které mají poslání zabránit, ztížit, popřípadě odvrátit úmysl vniknutí pachatele do zabezpečeného objektu. Plášť objektu je zpravidla tvořen:

- stavebními prvky budov,
- otvorovými výplněmi.

Velmi důležitými stavebními prvky plášťové ochrany objektů jsou stěny, podlahy, stropy, střechy. Jejich odolnost proti průlomu je závislá především na druhu použitého materiálu, jeho pevnosti, tloušťce a vlastnímu provedení výstavby.

Zvlášť důležité je kontrolovat objekty, které mají společné obvodové zdivo v řadové zástavbě, kde by mohlo dojít k průlomu uvnitř objektu probouráním společné zdi anebo nedovolenému vniknutí střechou.²⁵ Zde bychom mohli nasadit kombinaci detektorů magnetických kontaktů detekující otevření otevíratelných otvorů, detektorů tříštění skla, popřípadě využít IR závor pro střežení stěn s více vstupy nebo otvory.

Z hlediska použitého materiálu můžeme rozlišit dva typy staveb:

- *lehké stavby* – jejich pasivní bezpečnost vůči okolí je velmi nízká a použitý materiál odpovídá nižšímu stupni zabezpečení. Zde může uvést např. sádkartonové příčky a výplně, vlnité a profilové plechy, zděné příčky, betonové výplně bez výztuže do tloušťky 150 mm.
- *pevné stavební konstrukce* - nabízejí velkou škálu odporové odolnosti vzhledem k použití stavebního materiálu a dosahované tloušťky. Používají se při stavbách objektů a zabezpečených oblastí pro vyšší stupeň zabezpečení. Základním požadavkem odolnosti lze požadovat obvodové zdivo o tloušťce minimálně 300 mm provedené z plných cihel, které zděno na vápenocementovou maltu. Pro bariéry betonové se doporučuje tloušťka minimálně 150mm a musí být armovány statickou výztuží.

²⁵ UHLÍŘ, J., *Technická ochrana objektů. I. díl Mechanické zábranné systémy II*, s. 47

Otvorové výplně (např. dveře, okna vikýře apod.) vyplňují otvory v plášti budovy, bez kterých by se plášťová ochrana neobešla. Jsou jednou z nejvíce průlomových oblastí při vniknutí do zabezpečeného objektu. Otvorové výplně objektů můžeme rozdělit do čtyř základních skupin.

2.1.2.1 Vstupní otvorové výplně

Statistiky jednoznačně hovoří až o 90%, kdy pachatelé vloupání využili lehce překonatelné vstupní dveře. Proto musíme vnímat, že jako nedělitelný celek ke vstupním dveřím patří:

- dveřní křídlo (hlavně jeho výplň),
- uchycení dveří (dveřní závěs),
- zárubeň,
- dveřní zadlabávací zámek, cylindrická vložka,
- vrchní dveřní kování (bezpečnostní štít vlastního zámku).



Obrázek č. 6 Bezpečnostní dveře²⁶

²⁶ <http://www.bezpecnostnidvere.info>

2.1.2.2 *Okna a balkonové dveře*

Z hlediska překonání překážky do objektu jsou na druhém místě policejních statistik a to hlavně u přízemních nebo jednoposchodových budov. Proto z bezpečnostního hlediska je velmi důležité, aby okna a balkonové dveře byly zabezpečeny vždy tak, aby bylo zabráněno vniknutí bez použití násilí. Do této kategorie můžeme také i další otvory do objektu jako jsou vikýře, garážová vrata, větrací šachty atd.²⁷

2.1.2.3 *Mříže, rolety, žaluzie*

Mříže se používají hlavně k zabezpečení prosklených otvorových výplní (především dveří a oken) k zabránění násilnému vniknutí do zabezpečeného objektu. Představují jednu z nejstarších mechanických zábran, která se používá. Podobně můžeme použít i bezpečnostní rolety, které nám ale neposkytují takovou ochranu jako kvalitní mříže. Do této skupiny můžeme ještě zařadit žaluzie, které naopak pouze chrání prostor zájmu hlavně proti slunci či nežádoucímu nahlížení.

Na základě rozmanitosti jejich umístění a s tím souvisejících požadavků na bezpečnostní třídu můžeme mříže rozdělit podle:

- Konstrukce
 - ✓ pevně kotvené,
 - ✓ odnímatelné,
 - ✓ otevírací (otočné, sklopné, posuvné, mřížkové),
 - ✓ navíjecí (s průhledným – neprůhledným výpletem).
- Umístění
 - ✓ vnější (ploché, předsazené),
 - ✓ vnitřní,
 - ✓ meziokenní.
- Materiálu
 - ✓ ocelové,
 - ✓ duralové.²⁸

²⁷ UHLÍŘ, J., *Technická ochrana objektů. I. díl Mechanické zábranné systémy II*, s. 48

²⁸ Tamtéž, s. 58



Obrázek č. 7 Bezpečnostní mříž- dveře



Obrázek č. 8 Nůžková bezpečnostní mříž²⁹

2.1.2.4 **Bezpečnostní fólie a skla, vrstvený polykarbonát**

Především prosklené otvory pláště budovy potřebují odpovídající ochranu, která by měla souhlasit se stupněm předpokládaného nebezpečí. Velmi účinnou zbraní proti rozbití těchto výplní a vniknutí do zabezpečeného objektu, jsou **bezpečnostní a ochranné fólie**. Nalepení těchto fólií na prosklenou plochu je ekonomicky velmi levnější a estetičtější než mříže. Bezpečnostní fólie je většinou průhledná, tloušťky několika milimetrů. Při kvalitní instalaci je téměř neviditelná. Propustnost světla se pohybuje až kolem 90%.

Technologie výroby těchto prostředků byla vyvinuta v USA pro NASA v programu kosmického výzkumu. Sklo o tloušťce 5-7 mm polepené vhodnou fólií slouží velmi dobře jako mechanická zábrana.

V praxi se ukazuje, že pachatel po pokusu o rozbití skleněné výplně od dalšího jednání zpravidla pouští a do zabezpečeného objektu se nedostane neboť útok je viditelný a hlučný.

Na podobné bázi fungují **bezpečnostní skla**, která nám chrání otvorové výplně proti násilnému vniknutí. Bezpečnostní skla se vyrábí ve dvou modifikacích:

- bezpečnostní skla tvrzená,
- bezpečnostní skla vrstvená.

²⁹ <http://www.next.cz/cs/produkty/pc-3-bezpecnostni-mrize/pr-22-nuzkove-mrize/>



Obrázek č. 9 Bezpečnostní sklo ³⁰

Vrstvený polykarbonát (obchodní označení Lexgard – GEP) se skládá z několika tabulí Lexanu slepených k sobě, tedy bez folií. Lexard má vysokou odolnost při relativně nízké tloušťce. Tento materiál je používán většinou proti střelným zbraním a ohni. ³¹

2.1.3 Předmětová ochrana

Předmětová ochrana je doplňující zabezpečení prostorové a plášťové ochrany, která samostatně zabezpečuje vybrané předměty v objektu (většinou velmi vysoké hodnoty), které chrání je před odcizením či zničením. Detektory předmětové ochrany jsou zpravidla přiřazeny do samostatně ovládané skupiny, což umožňuje střežení těchto předmětů i v době většího pohybu osob v dané oblasti. Mezi prvky předmětové ochrany můžeme zařadit:

- komerční úschovné objekty (skříňové trezory, ohnivzdorné trezory, trezory na zbraně atd.),
- komorové trezory (monolitické, panelové, kombinované).

Dle stupně zabezpečení, ve kterém se objekt nachází, důležitosti a stupně utajované informace a cennosti musíme zvážit a navrhnout příslušnou instalaci mechanických zábranných prostředků. Musíme brát ohled na přírodní vlivy, možnosti vloupání a také kdo by mohl mít o střežené věci zájem.

³⁰ <http://www.wdokna.cz/varianty-sklenenych-vyplni-oken-a-dveri/>

³¹ UHLÍŘ, J., *Technická ochrana objektů. I. díl Mechanické zábranné systémy II*, s. 66

V současné době jsou dobrým vodítkem pro výběr výše bezpečnostní úrovně mechanických zábranných systému tzv. bezpečnostní třídy a usnadňují orientaci ve výběru mechanických bezpečnostních prvků.



Obrázek č. 10 Bezpečnostní třídy dle EN1627 ³²

2.1.3.1 Komerční úschovné objekty

Komerční úschovné objekty jsou objekty speciálně určené pro zabezpečení a ukládání utajovaných informací, důležitých dokumentů, cenných předmětů nebo zbraní. Ohnivzdorné úschovné objekty mohou zabránit zničení nosičů dat v případě vzniku požáru budovy. Tyto trezory jsou instalovány do zabezpečených oblastí dle požadavku zadavatele.



Obrázek č. 11 Trezor řady TLA - bezpečnostní třída I dle ČSN EN 1143.1 ³³

³² IVANKA, J., *Mechanické zábranné systémy*, s. 50

³³ <http://www.aparch.cz/trezory-tla-bezpecnostni-trida-i-dle-csn-en-1143-1/>

2.1.3.2 Komorové trezory

Komorové trezory jsou takové úschovné objekty, které jsou součástí pevných staveb budov. Tyto trezory mají velmi velkou mechanickou odolnost. Jejich průlomová odolnost se shoduje s parametry stěn, podlah a stropů. Mají certifikovanou odolnost proti vniknutí a jejich vnitřní rozměry v uzavřeném stavu vždy přesahují hodnotu 1 metru ve všech směrech. Tloušťka se může lišit v závislosti na použitém místě, respektive stupni bezpečnosti a účelu, kterému bude trezor sloužit. Jejich bezpečnost je dána odolností všech jednotlivých komponentů (součástí) bezpečnostní konstrukce pláště a dveří, včetně zámku.

Komorové trezory musí být vždy doplněny speciálními konstrukčně řešenými komorovými dveřmi. Tyto dveře tvoří jeden z nejdůležitějších prvků trezoru, protože jsou vstupní branou do celého trezoru. Při návrhu bezpečnostních trezorových dveří bychom měli vždy používat nejlepší materiály certifikované na nejvyšší možnou bezpečnostní třídu. Vysoký stupeň ochrany tvoří kompaktní vrstva, která se skládá z různých odolných materiálů. Dveře od komorových trezorů mívají tloušťku (0,3 - 2) metry a jejich hmotnost přesahuje mnohdy i 2 tuny. Aby nedocházelo k neoprávněným vstupům do trezorových místností (komorových trezorů), používáme vždy ke vstupu kombinaci dvou a více osob, z nichž každá má svůj speciální klíč. Trezor má zpravidla nastaven vstup tak, aby jednoho člověka dovnitř nepustil. Kromě klasických bezpečnostních, zámků bývají přístupové mechanismy doplněny o biometrickou identifikaci oprávněných osob.

Komorové trezory tedy můžeme rozdělit do tří hlavních skupin, a to:

- *monolitické komorové trezory* - vznikají přímo při výstavbě celého objektu uložením betonové směsi do speciální bezpečnostní výztuže, čímž vznikne požadovaný tvar, jaký má mít zřizovaný úschovný objekt,
- *panelové komorové trezory* - vznikají poskládáním předem vyrobených panelových betonových prefabrikátů, skládají se na místě do požadovaného tvaru,
- *kombinované (smíšené) komorové trezory* - vznikají kombinací předchozích dvou technologií, tzn. trezorovou podlahu vyrobíme např. monolitickou konstrukcí, strop a stěny postavíme z betonových panelů.³⁴

³⁴ IVANKA, J., *Mechanické zábranné systémy*, s. 57



Obrázek č. 12 Komerový trezor ČNB³⁵

2.1.4 Stanovení minimální doby průlomové odolnosti úschovných objektů

U úschovných objektů je potřeba stanovit minimální průlomovou odolnost ($T_{\text{vloupání}}$), kterou zjistíme výpočtem, dle níže uvedeného vzorce, v němž se vychází z typu úschovného objektu (komorový nebo skříňový trezor), kvalifikované bezpečnostní třídy daného výrobku a z odpovídajícího počtu odporových jednotek [RU], které konkrétní typově odzkoušený výrobek vykázal při fyzických zkouškách.³⁶

Doba minimální průlomové odolnosti u úschovných objektů je dána vztahem:

$$T_{\text{vloupání}} = [(V_R - BV) \div C_1] (2 \div 3) [s]$$

$T_{\text{vloupání}}$ doba minimální průlomové odolnosti úschovného objektu

V_R hodnota průlomové odolnosti úschovného objektu

³⁵http://ekonomika.idnes.cz/moody-s-zhorsila-vyhled-pro-ceske-banky-ohrozuje-je-krize-eurozony-1pj-/ekonomika.aspx?c=A111202_011049_ekonomika_jan

³⁶ IVANKA, J., *Mechanické zábranné systémy*, s. 44

- U skříňového trezoru je rovna průměrné hodnotě částečného a úplného průlomu
- U trezorových dveří a komorového trezoru jde o hodnotu pro úplný průlom

BV..... základní ocenění – číselná hodnota přidělená určitému nářadí

C1..... koeficient průlomové odolnosti úschovného objektu

(2÷3)..... koeficient navýšení

2.1.5 Stupně rizika ohrožených objektů

Bezpečnostní úroveň nám charakterizuje každou zábranu, která je reprezentovaná pasivní bezpečností, resp. *průlomovou odolností*. Za obecně kvantitativní ohodnocení překážky považujeme časový interval, který pachatel potřebuje k jejímu přelomení.

Tento vztah je možno vyjádřit:

$$R = T_{\text{vloupání}} / t_i$$

při podmínce: $t_i > 1$

kde:

R stupeň rizika ohrožení objektu (koeficient rizikovosti)

$T_{\text{vloupání}}$ doba minimální průlomové odolnosti úschovného objektu

t_i čas potřebný k zásahu orgánů PČR, resp. Služby

Skutečné riziko ohrožení chráněného zájmu bude tím menší, čím bude koeficient „R“ větší. Má-li-být aplikovaná ochrana účelná, musí být jeho hodnota větší než „1“. Bude-li rovna „1“ nebo menší, nemůžeme hovořit o jakékoliv efektivitě ochrany. Naopak čím bude

tento koeficient větší, tím se bude riziko ohrožení snižovat a systém zabezpečení chráněného zájmu bude kvalitnější.

Při návrhu MZS pro daný objekt se doporučuje následující postup:

- podle akceschopnosti SBS (event. Policie ČR) určíme čas zásahu,
- podle důležitosti chráněného zájmu stanovíme koeficient rizikovosti „R“,
- podle těchto údajů a hodnot stanovíme minimální průlomový čas pro MZS, resp. jejich průlomovou odolnost,
- následně můžeme navrhnout konkrétní systém mechanického zajištění objektu.³⁷

2.1.6 Koeficienty průlomové odolnosti úschovných objektů

Bezpečnostní třída	Koeficient C ₁ [RU/min]
0 - I	5
II - III	7,5
III - VII	10
VIII - XI	15
XII - XIII	35

Tabulka č. 1 Koeficienty průlomové odolnosti³⁸

2.1.7 Trezorové bezpečnostní třídy

Certifikované trezory jsou řazeny do bezpečnostních tříd. Bezpečnostní třída vyjadřuje, jaká je odolnost trezoru proti vloupání. Čím vyšší bezpečnostní třída trezoru, tím je trezor odolnější a bezpečnější. Trezory se certifikují podle výsledku zkoušek dle ČSN EN 1143-1 - Skříňové trezory, trezorové dveře a komorové trezory.

³⁷ IVANKA, J., *Mechanické zábranné systémy*, s. 45

³⁸ KŘEČEK, S., *Příručka zabezpečovací techniky*, s. 185

V následující tabulce jsou uvedeny minimální požadavky pro klasifikaci trezorových dveří a komorových trezorů do bezpečnostních tříd ³⁹:

Bezpečnostní třída	Zkouška napadením s využitím nářadí (kapitola 7)	Zámky ^a		Doplňkový požadavek pro označení EX (volitelné) (kapitola 9)	Doplňkový požadavek pro označení CD (volitelné) (kapitola 10)
		Počet	Třída podle EN 1300		
	Hodnota průlomové odolnosti pro úplný průlom RU			Hodnota průlomové odolnosti po výbuchu RU	Hodnota průlomové odolnosti c RU
0	30	1	A	<i>b</i>	<i>d</i>
I	50	1	A	<i>b</i>	<i>d</i>
II	80	1	A	4	<i>d</i>
III	120	1	B	6	<i>d</i>
IV	180	2	B	9	<i>d</i>
v	270	2	B	14	1 800
VI	400	2	C	20	2 000
VII	600	2	C	30	2 300
VIII	825	2	C	41	2 500
IX	1 050	2	c	53	3 500
X	1 350	2	c	68	4 500
XI	2 000	3	C nebo	100	6 000
		2	D		
XII	3 000	3	C nebo	150	7 500
		2	D		
XIII	4 500	2	D	225	9000

a Nepoužívá se pro klasifikaci komorových trezorů bez dveří.
b EX označení není přípustné pro bezpečnostní třídy 0 a 1.
c Hodnota průlomové odolnosti pro úplný průlom při vrtání diamantovým korunovým vrtákem.
d CD označení není přípustné pro bezpečnostní třídy 0 až IV.

Tabulka č. 2 Minimální požadavky bezpečnostních tříd trezorů ⁴⁰

³⁹ <http://www.metalsafe.cz/cs/vse-o-trezorech/bezpecnostni-tridy-trezoru>

⁴⁰ IVANKA, J., *Mechanické zábranné systémy*, s. 58

2.1.7.1 Trezorová bezpečnostní třída 0.

- nejnižší kategorie,
- dle NBÚ (Zák. č.528/2005Sb.) se jedná o úschovný objekt typ 2 (SS1 = 2 body) (dle dříve platných zákonů splňuje podmínky pro uschování dokumentů - Důvěrné),
- vhodné pro uschování - dokumentů, dokladů, léků, cenností a ostatních finančních hotovostí cca do 150 tis. Kč (nutno konzultovat s vaší pojišťovnou - částky se liší), zbraní do 10 ks a nábojů do střelných zbraní v počtu do 10 tis. ks.

2.1.7.2 Trezorová bezpečnostní třída I.

- standard, dobrá volba pro domácnost,
- dle NBÚ (zák.č.528/2005 Sb.) se jedná o úschovný objekt typ 3 (SS1 = 3 body) (dle dříve platných zákonů splňuje podmínky pro uschování dokumentů - Tajné),
- vhodné pro uschování - dokumentů, dokladů, léků, cenností a ostatních finančních hotovostí cca do 300 tis.Kč (nutno konzultovat s vaší pojišťovnou - částky se liší), zbraní do 20 ks, nábojů do střelných zbraní v počtu do 20 tis. ks.

2.1.7.3 Trezorová bezpečnostní třída II.

- vyšší standard,
- dle NBÚ (zák.č.528/2005 Sb.) se jedná o úschovný objekt typ 4 (SS1 = 4body) (dle dříve platných zákonů splňuje podmínky pro uschování dokumentů – Přísně tajné)
- vhodné pro uschování - dokumentů, dokladů, léků, cenností a ostatních finančních hotovostí cca do 500 tis.Kč (nutno konzultovat s pojišťovnou - částky se liší).

2.1.7.4 Trezorová bezpečnostní třída III.

- vysoký stupeň ochrany,
- vhodné pro uschování - dokumentů, dokladů, léků, cenností a ostatních finančních hotovostí nad 500 tis.Kč (nutno konzultovat s pojišťovnou - částky se liší).

Vyšší bezpečnostní třídy /IV. - XIII/ jsou převážně určeny pro bankovní a finanční instituce.⁴¹

Pro splnění bezpečnosti trezoru musí být trezor vždy pevně přikotven k podlaze nebo ke zdi. K tomu jsou určeny otvory v plášti trezoru. Pro správný výběr kotvícího prvku musí být respektována stavební hmota, ke které bude trezor přikotven. Nejbezpečnější ukotvení

⁴¹ <http://www.trezor.cz/podpora-a-servis/bezpecnostni-tridy-a-deleni-trezoru.htm>

vám zaručí tzv. plné stavební hmoty (např. beton, přírodní kámen, plná cihla), jejich vlastnostmi jsou vysoká pevnost v tahu a hustá struktura bez dutin. Zde je možné dosáhnout vysoké rozpínací síly a nízké upevňovací hloubky kotevního prvku, což zajišťují ocelové šroubové rozpínací kotvy, které vynikají nadprůměrnou pevností, rychlou a bezpečnou montáží. Jiným, méně vhodným způsobem ukotvení je použití univerzálních hmoždinek s vruty.

Dalším technickým prostředkem, který je nasazován k ochraně majetku a utajovaných informací a které doplňují mechanické zábranné systémy, jsou poplachové zabezpečovací a tísňové systémy a systémy pro kontrolu vstupů (SKV).

2.2 Poplachový zabezpečovací a tísňový systém a systémy pro kontrolu vstupů

Poplachový zabezpečovací a tísňový systém (dříve nazývaný Elektrická Zabezpečovací Signalizace EZS) je určen především k včasné detekci přítomnosti nebo pokusu o neoprávněné vniknutí narušitele do střeženého prostoru, ochraně předmětů a přivolání pomoci v případě tísně. Je zároveň určen k signalizaci poplachových stavů do místa s trvalou ostrahou na tzv. pultu centrální ostrahy (PCO).

2.2.1 Systémy pro kontrolu vstupu

ACS neboli systém kontroly vstupů (Access Control System). Tyto systémy sledují, evidují a řídí průchod či přístup osob do vymezených prostor na základě definovaných oprávnění. Osoby využívající vstup do zabezpečených prostor používají bezkontaktní identifikační prvek, kterým může být karta, přívěšek na klíče, případně některý z biometrických údajů, kterým se u přístupového terminálu identifikují a po kladném ověření jejich přístupových práv jim systém povolí otevřít dveře, nebo projít turniketem, otevře se jim závora apod. Systém pracuje ON-LINE a komunikuje s centrální databází, kde jsou definována práva jednotlivých osob pro přístup do konkrétních oblastí. Prostřednictvím tohoto systému je hmotný i nehmotný majetek organizace chráněn tak, že nedovolí vstup

neoprávněné osobě a zároveň se získává přehled o pohybu pracovníků po areálu a kontrolujete přístup ke chráněným utajovaným informacím.⁴²



Obrázek č. 13 Systém pro kontrolu vstupu



Obrázek č. 14 Biometrický systém kontroly vstupu⁴³

Základními dokumenty pro techniku a navrhování PZTS jsou normy skupiny ČSN EN 50 131. Tyto normy řeší problematiku techniky a doporučují i zásady pro instalaci. Jsou v nich kategorizovány i komponenty PZTS podle rizik. V průmyslových a komerčních objektech se většinou nasazují komponenty pro stupeň zabezpečení 2.

Na trhu můžeme objevit mnoho druhů elektronických zámkových systémů, které různé firmy nabízejí od jednoduchých čteček karet až po velmi složité s biometrickou identifikací, které jsou ovšem velmi ekonomicky náročné.

Systém PZTS tvoří:

2.2.2 Ústředna

Zařízení pro zpracování a příjem informací z nainstalovaných detektorů. Ovládá, indikuje a inicializuje přenos informací z koncových zařízení. Zabezpečovací ústředna se skládá z plošného spoje s mikroprocesorem, výstupy pro zapojení jednotlivých zón s detektory a záložní zdrojovou částí, která je velmi důležitá při výpadku elektrického proudu.

⁴² <http://www.meritgroup.cz/elektronicka-kontrola-vstupu.asp>

⁴³ <http://www.eatonelektrotechnika.cz/cz/poplachove-zabezpecovaci-a-tisnove-systemy-ezs.html>



Obrázek č. 15 Ústředna v plastovém krytu GFlex 20 - V3 7Ah s komunikátorem a LCD kláv-MK ⁴⁴

2.2.3 Ovládací klávesnice

Důležitý prvek určený k ovládání a programování vlastní ústředny. Zadáním uživatelského hesla může být ovládáno kódování a dekodování jednotlivých střežených zón, rušení poplachů, atd.

2.2.4 Detektory (čidla)

Koncová konverzní zařízení sloužící ke snímání specifických fyzikálních signálů spojených s proniknutím narušitele do střeženého objektu a pohybu v něm. V případě zjištění takovýchto projevů je vyvolán poplach a následná bezpečnostní opatření.

Detektory můžeme rozdělit na:

- podle zdroje akustického signálu:
 - pasívní – vyhodnocující akustický signál vznikající při překonání bariér a při pohybu nepovolaného objektu v chráněné oblasti; detektory obsahují pouze přijímač akustického signálu,
 - aktivní – detekují překonání bariér a nebo pohyb nežádoucího objektu v zabezpečeném prostoru na základě změny charakteristiky akustické tlakové vlny vysílané detektorem; detektory obsahují jak vysílač, tak i přijímač akustického signálu.
- podle použitého frekvenčního pásma:
 - detektory pracující v akustickém pásmu 16 Hz – 20 kHz,
 - detektory pracující v ultrazvukovém pásmu – více jak 20 kHz,

⁴⁴ <http://www.t-bau.cz/elektroinstalace/elektricke-zabezpecovaci-systemy/>

- podle určení z hlediska prostorového působení:
 - detektory na perimetrickou ochranu – IR závory a bariéry, zemní tlakové hadice, pasivní infračervená čidla,
 - detektory na prostorovou ochranu objektů – pasivní a aktivní IR čidla, ultrazvuková čidla, mikrovlnná čidla, kombinovaná duální čidla,
 - detektory na plášťovou ochranu objektů – magnetické kontakty, tříštivý čidla, otřesová čidla, poplachové fólie a tapety atd.,
 - detektory na předmětovou ochranu objektů – čidla na ochranu závěsných předmětů, kapacitní čidla. ⁴⁵

2.2.4.1 PIR detektory

Pasivní infračervená čidla (Passive infra red sensor), označována jako PIR detektory, jsou nejčastěji využívanými detektory ve standardních zapojeních systémů PZTS. Jednoduše můžeme konstatovat, že PIR detektory jsou schopny zachytit pohyb těles, která mají jinou teplotu, než je teplota přirozeného pozadí. Jejich funkce je založena na zachycení změn vyzařování v infračerveném pásmu kmitočtového spektra elektromagnetického vlnění. Nejlépe reagují na teploty blízké povrchu lidského těla (od 25°C do 40°C).

IR záření vyzařované snímaným prostředím je optikou rozděleno na detekční zóny.

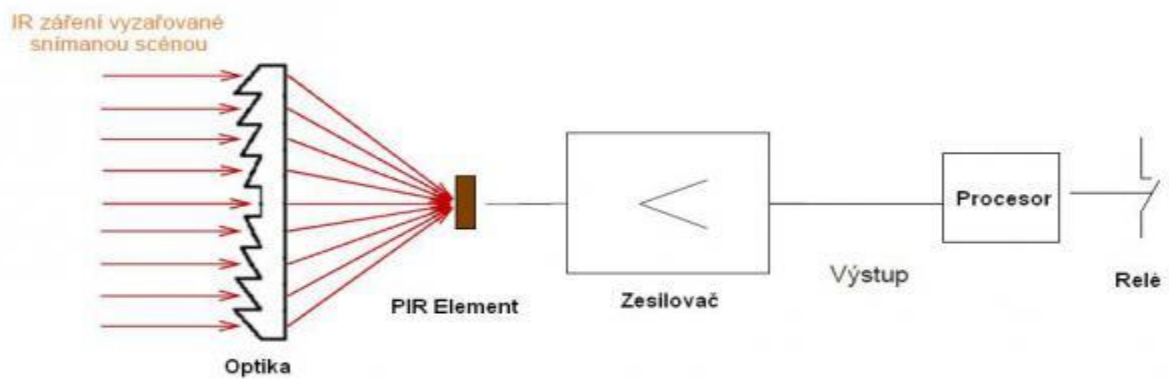
Toto záření poté dopadá na pyroelement. Při změně hodnoty záření pyroelement vyše signál, který je zesílen zesilovačem.

Pyroelement je základní funkční prvek PIR detektoru. Je to polovodičová součástka (ze sloučenin na bázi lithia a tantalu). Pyroelektrické detektory jsou citlivé na ozáření infračerveným světlem tak, že začnou generovat elektrický povrchový náboj Q. Pokud se změní hodnota dopadajícího infračerveného záření na povrch pyroelektrického materiálu, změní se tím i hodnota elektrického povrchového náboje. Tato změna náboje je měřena citlivým FET tranzistorem, který je přímo vestavěný ve snímači. Pyroelektrický snímač je citlivý ve velkém vlnovém rozsahu a proto je před pyroelektrický snímač aplikován filtr záření, který propouští infračervené záření o vlnových délkách v rozsahu 8 až 14 μm. Lidské tělo emituje do prostoru záření o vlnové délce 9,4 μm. ⁴⁶

⁴⁵ LUKÁŠ, L. a kol., *Bezpečnostní technologie, systémy a management*, s. 74

⁴⁶ UHLÁŘ, J., *Technická ochrana objektů II. díl - Elektrické zabezpečovací systémy II*, s. 60

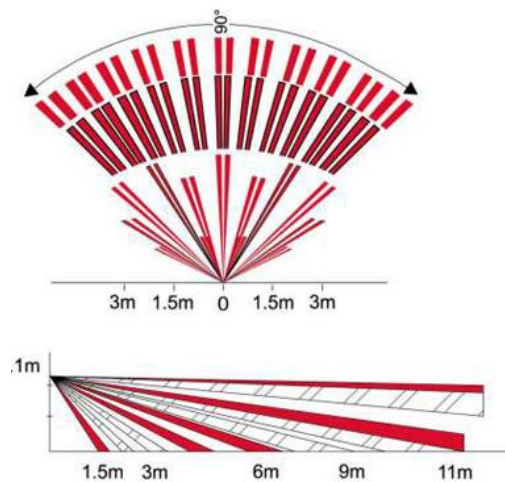
Blokové schéma PIR detektoru



Obrázek č. 16 Blokové schéma PIR detektoru ⁴⁷

PIR čidla nejčastěji dělíme dle charakteristiky snímaného prostoru na základě tvaru čočky:

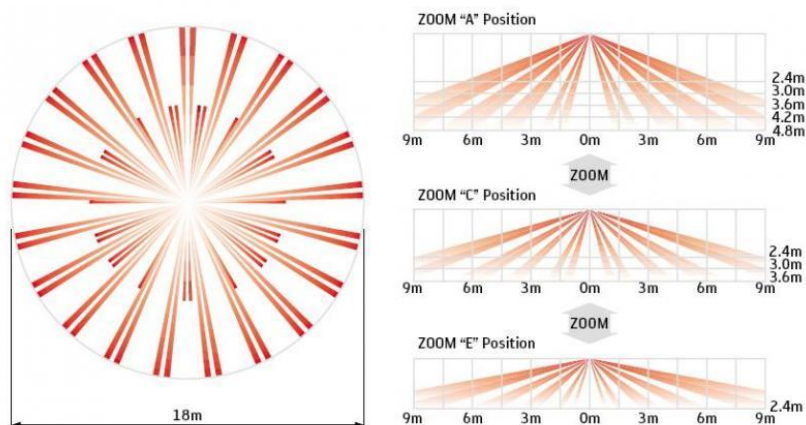
- Vějíř (dosah 12 – 15 metrů, šířkový úhel 90°),
- Záclona (dosah 12 – 15 metrů, šířkový úhel 15°),
- Dlouhý dosah (dosah 20 – 35 metrů, šířkový úhel 15°),
- Stropní (dosah 8 – 12 metrů, šířkový úhel 360°).



Obrázek č. 17 Vyzářovací charakteristika PIR detektoru pohybu⁴⁸

⁴⁷ <http://www.hw.cz/automatizace/pir-cidlo-skvely-sluha-ale-zly-pan.html>

⁴⁸ <http://www.stasanet.cz/Paradox-a-ostatni-EZS/Vnitni-detekce/Detektory>



Obrázek č. 18 Vyzařovací charakteristika stropního PIR detektoru pohybu ⁴⁹

Samotná instalace detektorů může být metalickým vedením, což je z technického hlediska jednodušší a jednotlivé prvky jsou zpravidla levnější. Výhodou jsou již připravené rozvody v průběhu výstavby nebo rekonstrukce objektů.

V případě instalace PZTS do již hotového objektu je alternativou bezdrátové zařízení, ale výhoda snadné instalace je vykoupena jinými nedostatky (pravidelné náklady na výměnu baterií, elektromagnetický smog).



Obrázek č. 19 Sada PIR detektorů ⁵⁰

⁴⁹ <http://www.eurosat.cz/2662-optex-sx-360z.html>

⁵⁰ <http://www.bfb-falco.cz/klient.html>

2.3 Speciální televizní systémy

Kamerové systémy (Closed Circuit Television – CCTV) nebo také průmyslové kamery jsou nejčastějším doplňkem zabezpečení objektů. Uzavřené kamerové systémy patří v současnosti mezi nejúčinnější a nejvíce používané prostředky ochrany majetku jak v průmyslové, tak i v komerční činnosti. Prostřednictvím těchto kamerových systémů lze střežit rozsáhlé komplexy budov, monitorovat a zaznamenávat pohyb osob ve střeženém prostoru a dodatečně identifikovat pachatele trestné činnosti.

Kamerové systémy můžeme rozdělit na:

- *Analogové kamerové systémy* - analogové kamery se vyznačují velice dobrým poměrem výkon (kvalita obrazu)/cena. Výhodou analogových kamer je veliký výběr různých typů kamer.
- *IP kamerové systémy* - tyto systémy jsou založeny na digitalizaci videosignálu. Pro snímání se používají síťové (IP) kamery. Tyto kamery vycházejí z analogových kamer, oproti nim jsou však vybaveny mechanismy pro přenos a zpracování videosignálu v digitální podobě. Každá síťová kamera má určitou IP adresu, s jejíž pomocí lze zařízení jednoznačně identifikovat na síti.
- *Hybridní kamerové systémy* – tyto systémy jsou pomyslným prostředníkem mezi analogovými a digitálními systémy a kombinují mechanismy z obou skupin. Významný prvek hybridních systémů je tzv. videosever, což je zařízení, které zpracovává analogový videosignál z kamery a převádí jej na digitální informaci.⁵¹



Obrázek č. 20 Typy bezpečnostních kamer⁵²

⁵¹ <http://www.t-bau.cz/elektroinstalace/kamerove-systemy>

⁵² <http://di.com.pl/informacje/galeria,46366,12333.html>

2.4 Elektrická požární signalizace

Elektrická požární signalizace (dále pouze EPS) je systém, který má za úkol včasnou detekci případně prevenci vzniku požáru. Použití těchto systémů je značně rozsáhlé, a používáné všude, kde by mohlo hrozit vznik požáru. Jedná se o plně automatické systémy, které mohou dále varovat osoby, nacházející se v ohrožené lokalitě, spouštět hasební prvky určené k likvidaci požárů (např. sprinklery), zajistit únikové cesty z místa požáru a nakonec to nejdůležitější – zavolat hasičský záchranný sbor (HZS).

Prvky EPS mají za úkol přesně detekovat místo požáru, a tuto informaci předat dalším prvkům řetězce zpracování v co nejkratším možném čase.

Komplexně řešený systém EPS umožňuje:

- rychlé a spolehlivé určení místa požáru,
- vyhlášení požárního poplachu akustickým signálem,
- aktivaci a řízení evakuačního systému v dané oblasti,
- ovládání a signalizaci stavu dalších požárně bezpečnostních zařízení,
- automatickou komunikaci s HZS.

Ústředna EPS má za úkol zpracovat informaci z hlásičů a vybavit výstup, tj. signalizovat vznik požáru v hlídané oblasti, aktivaci výstupních obvodů pro signalizaci místa požáru v objektu a jeho předání hasičskému záchrannému sboru v případě potřeby. Současně musí provést sérii opatření, např. odblokování únikových cest, otevření kouřových klapek, odpojení výrobních či jiných technologií nebo aktivaci požárního rozhlasu za účelem záchrany lidí a technologie a přípravy budovy pro příjezd hasičů. K akustické a optické signalizaci poplachu slouží sirény a majáky.⁵³



Obrázek č. 21 Prvky EPS⁵⁴

⁵³ LUKÁŠ, L. a kol. *Bezpečnostní technologie, systémy a management I*, s. 148

⁵⁴ <http://www.tzb-info.cz/pozarni-ochrana/8586-siemens-na-veletrhu-pragoalarm-pragosec-2012>

Prvky Poplachového zabezpečovacího a tísňového systému mohou být instalovány buď jako samostatná aplikace nebo jako součást dalších systémů v rámci integrace – např. systému řízení přístupu, perimetrického či monitorovacího kamerového systému. PZTS je obvykle vyveden na pult centralizované ochrany (PCO) do z místa s trvalou ostrahou a to buď radiovou cestou, případně po telefonních nebo datových linkách. V případě alarmu, nebo jiné mimořádné události zajišťuje řešení situace operátor PCO.⁵⁵

2.5 Zařízení fyzického ničení nosičů informací

Skartace je jednou z nejspolehlivějších způsobů, jak zlikvidovat utajované nebo citlivé dokumenty. Zařízení fyzického ničení nosičů informací se od sebe liší typem řezu, velikostí odpadní nádoby, výkonem a stupněm utajení. Skartují se papíry, diskety, CD, DVD, filmy, osobní karty. Další způsob ničení je ohněm, kterým se likvidují, flash, paměťové karty HDD.

Skartovací stroje dělíme dle typu na 0 – 4 bez bodového hodnocení a stupně ničení utajované informace. Při vyšším stupni se kombinuje řez proužek a příčný řez. Velikost odpadních částic je řešena ve Vyhlášce č. 528/2008 Sb., o fyzické bezpečnosti a certifikaci prostředků, ve znění pozdějších předpisů a musí odpovídat výši stupně utajované informace.

Proužek – listy papírů jsou rozřezány na proužky po celé jeho délce. Podélný řez přináší výhodu skartace většího množství dokumentů najednou než u příčného řezu.

Příčný řez – listy papírů jsou rozřezány na podélné proužky a příčně na krátké částice. Výhodou je vyšší stupeň utajení a výrazně větší kapacita odpadové nádoby než u řezu v proužku.



Obrázek č. 22 Skartovací stroj JAWS C9, řez 2x8mm, NBÚ certifikát stupeň 3 ⁵⁶

⁵⁵ <http://www.t-bau.cz/elektroinstalace/elektricke-zabezpecovaci-systemy/>

⁵⁶ <http://www.texpo-cz.cz/skartovaci-stroj-jaws-c9-kapacita-11listu-rez-2x8mm-nbu-certifikat-stupen-3->

2.6 Certifikace NBÚ - ochrana utajovaných informací

Na závěr této kapitoly je potřeba se zmínit o certifikaci technických prostředků pro ochranu utajovaných informací. Každý konkrétní prostředek, který je nasazen na zabezpečení objektu vyšší třídy, musím projít tzv. certifikací. Touto certifikací se rozumí posouzení technických parametrů výrobků a zařízení používaných k ochraně utajovaných informací a vystavení certifikátu na základě odborného posudku odborného pracoviště, který zahrnuje certifikát shody od certifikačního orgánu.

Novelou vyhlášky č. 528/2005 Sb. došlo ke zrušení certifikace technických prostředků, které nejsou hodnoceny a zařazovány do tříd nebo stupňů. Jedná se o technické prostředky uvedené v odst. 1) § 30 zákona č. 412/2005 Sb. pod písmeny d), f), g) a i) tj.:

- speciální televizní systémy,
- zařízení elektrické požární signalizace,
- zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů,
- zařízení proti pasivnímu a aktivnímu odposlechu utajované informace.

Národní bezpečnostní úřad bude dále vydávat certifikáty na následující technické prostředky:

- mechanické zábranné prostředky,
- elektrická zámková zařízení a systémy pro kontrolu vstupů,
- zařízení elektrické zabezpečovací signalizace,
- tísňové systémy,
- zařízení fyzického ničení nosičů informací nebo dat.

Certifikace uvedených druhů technických prostředků pro ochranu utajovaných informací se řídí pravidly dokumentu „Certifikační postup NBÚ – verze 2012“, který je uveden na stránkách NBÚ.⁵⁷

⁵⁷ <http://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost/certifikace/certifikačni-postup-nbu/informace-k-certifikacnimu-postupu-nbu/>

Závěr

V teoretické části této práce byly uvedeny základní důležité pojmy a informace k zabezpečení objektu, právní normy řešící fyzickou bezpečnost a podrobněji je popsána technická ochrana, kam zařadíme mechanické zábranné systémy, poplachové zabezpečovací a tísňové systémy, systémy pro kontrolu vstupů, zařízení elektronické požární signalizace a zařízení fyzického ničení informací. V další části této práce bude popsán konkrétní postup při zabezpečení rozsáhlého objektu a zabezpečených oblastí.

II. PRAKTICKÁ ČÁST

3 POPIS A POSOUZENÍ STÁVAJÍCÍHO ZABEZPEČENÍ ROZSÁHLÉHO OBJEKTU

V praktické části byl vybrán modelový rozsáhlý objekt firmy, kterou pojmenujeme Product Security a.s., protože analýza a nový návrh zabezpečení nesmí být veřejným dokumentem a musí se postupovat dle platných předpisů proti vyzrazení. Dokumentace zabezpečení objektu na vyšší stupeň obsahuje utajované informace stupně Vyhrazené a tedy veřejnosti nedostupné. Zveřejnění režimových opatření, způsobu ostrahy a dokumentace k zabezpečovacímu systému takového objektu by mohlo mít velmi nedozírné důsledky a mohlo by dojít k porušení zákona.

V tomto areálu, kde se nachází daný objekt, bude provedena analýza stávajícího stavu fyzického zabezpečení a bude navržen nový bezpečnostní projekt na vyšší stupeň zabezpečení. V zabezpečené oblasti se budou ukládat utajované informace podléhající stupni utajení Důvěrné a Tajné.

Společnost Product Security a.s., pro naše účely bude umístěna do lokality Olomouc, splňuje stanovené podmínky pro práci s utajovanými informacemi. Doposud přicházela do styku pouze s dokumenty stupně utajení Vyhrazené a v budoucnu plánuje zabezpečovat objekty s vyšším stupněm utajení, a proto potřebuje zvýšit zabezpečení objektu u dvou zabezpečených oblastí. V budoucnu počítá se zpracováním a ukládáním utajovaných informací až do stupně utajení Tajné.



Obrázek č. 23 Posuzovaný objekt v dané lokalitě⁵⁸

⁵⁸ <http://mapy.cz/letecka>

3.1 Charakteristika areálu a objektu

Areál se nachází v lokalitě města Olomouc v jedné městské části. V okolí areálu je rodinná zástavba a malé podnikatelské subjekty. Dále se zde nachází škola, školní hřiště a sportovní hala. Areál je po celém obvodu ohraničen betonovou zdí o výšce v rozmezí 2,5m – 3,5m a v kritických místech osnatým žiletkovým drátem. Do areálu se vjíždí a vstupuje hlavní branou z ulice Okružní. Ostatní vjezdové brány jsou zabezpečeny a uzamčeny proti vniknutí. V areálu se nachází několik dalších budov, které jsou využívány pro potřebu společnosti. V odpoledních a nočních hodinách je areál uzavřen a střežen bezpečnostní agenturou.

Objekt, který je posuzován, je zrekonstruovaná jednopodlažní budova A (administrativní budova společnosti) v areálu firmy Product Security a.s., od ostatních budov není oddělena oplocením. Terén kolem budovy je rovinný a travnatý. V objektu jsou umístěny ZO č. 1, 2. Objekt má jeden vstup. Vstup do objektu je dveřmi s uzamykacím systémem.

3.2 Současné zabezpečení a stanovení hranice zabezpečené oblasti

V současné době jsou objekty a zabezpečené oblasti v areálu společnosti Product Security a.s. zabezpečeny pro kategorii Vyhrazené. Z hlediska množství utajovaných informací se jedná o ukládání hardwarových a softwarových komponentů z pracovních stanic kategorie Vyhrazené.

Objekt má viditelně vymezenou hranici, která není v celé vlastní délce shodná s hranicí zabezpečených oblastí. Hranici objektu tvoří plášť vnitřního a vnějšího obvodového zdiva budovy A. Minimální síla obvodových zdí je 300 mm, vnitřních zdí je 150 mm. Minimální síla podlahové a stropní konstrukce je 200 mm. Objekt je dle statě č. 3 a 6 přílohy č. 1 k vyhlášce 528/2005 Sb. typu 1 vylehčená prefabrikovaná konstrukce, která chrání osoby, materiál a zařízení před povětrnostními vlivy.

Ostrahu zabezpečují zaměstnanci bezpečnostní agentury. Fyzická ostraha vykonává ostrahu objektů A, B, C, D a je zabezpečena 2 člennou směnou. Stanoviště ostrahy je na budově č. B u vstupu do areálu. Ostraha provádí pravidelné obchůzky v intervalu do 6 hodin. První obchůzka se provádí ihned po ukončení pracovní doby. Ostraha je vybavena při obchůzkách prostředky umožňující spojení se stanovištěm pro stálý výkon služby. V průběhu

výkonu ostrahy, včetně doby obchůzek, je stanovišti stálé služby neustále přítomna jedna osoba určená pro její výkon.

Režim návštěv v objektu je dle vyhlášky č. 528/2005 Sb. v platném znění stanoven s doprovodem.

3.2.1 Přehled použitých technických prostředků

V současné době není objekt vybaven žádným poplachovým zabezpečovacím a tísňovým systémem. Objekt a zabezpečovací místnosti kategorie Vyhrazené jsou zabezpečeny pouze certifikovanými a necertifikovanými mechanickými zábrannými systémy. Úschovné objekty jsou necertifikované pouze se zápisem o shodě. Zařízení fyzického ničení nosičů informací typu 2 je umístěno v ZO č. 1 a zařízení fyzického ničení nosičů informací typu 3 je umístěno v ZO č. 2.

3.2.2 Stanovení zabezpečených oblastí

V objektu se nachází ZO č. 1 v místnosti č. 3 a ZO č. 2 v místnosti č. 4. Kategorie ZO je stanovená na stupeň Vyhrazené.

3.2.3 Stanovení hranice zabezpečené oblasti

Zabezpečená oblast č. 1 kategorie Vyhrazené, stanovená třída II se nachází v objektu kategorie Vyhrazené v místnosti č. 3 v 1. NP budovy A – administrativní budova společnosti, pracoviště zabezpečení materiálem, úložna pracoviště zabezpečení materiálem. Minimální síla obvodových zdí je 300 mm, minimální síla vnitřních zdí je 150 mm. Minimální síla podlahové a stropní konstrukce je 200 mm. Oblast má pouze jeden vstup a jedno okno, jehož výška nad terénem je menší než 5,5 m.

Zabezpečená oblast je typu 2 a průlezné otvory jsou zabezpečeny certifikovanými mechanickými zábrannými prostředky. Mechanické zábranné prostředky jsou pevné konstrukce a nevykazují znaky poškození nebo opotřebení, které by znemožnili identifikovat pokusy o neoprávněný vstup.

Zabezpečená oblast č. 2 kategorie Vyhrazené, stanovená třída II se nachází v objektu kategorie Vyhrazené v místnosti č. 4 v 1. NP budovy A – administrativní budova společnosti, pracoviště technologií. Minimální síla obvodových zdí je 300 mm, minimální síla vnitřních

zdí je 150 mm. Minimální síla podlahové a stropní konstrukce je 200 mm. Oblast má pouze jeden vstup a jednou okno, jehož výška nad terénem je menší než 5,5 m.

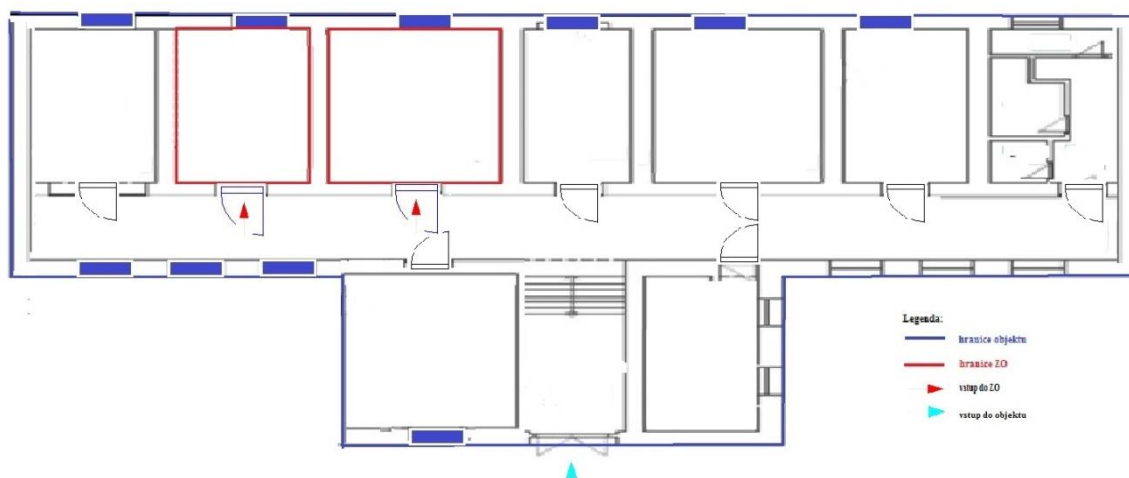
Zabezpečená oblast je typu 2 a průlezné otvory jsou zabezpečeny certifikovanými mechanickými zábrannými prostředky. Mechanické zábranné prostředky jsou pevné konstrukce a nevykazují znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup.

3.2.4 Přijatá režimová opatření fyzické bezpečnosti

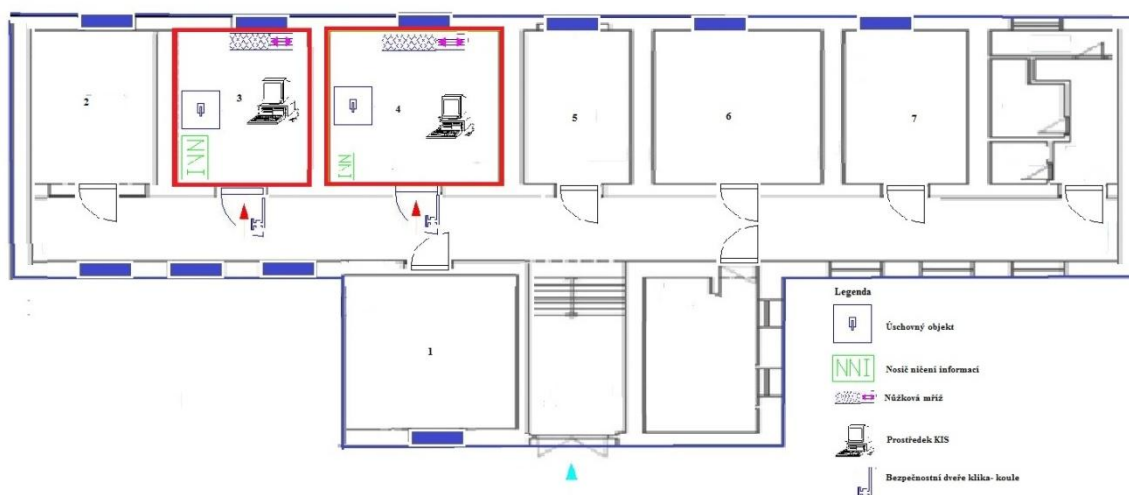
- **režim pohybu osob v objektu** - v objektu je stanoven režim návštěv s doprovodem. Všechny osoby se mohou pohybovat v doprovodu (povinnost nosit viditelně IP) pouze s oprávněnou osobou. V mimopracovní době smí do objektu vstupovat pouze oprávněné osoby. O návštěvách je vedena evidence v „Knize návštěv“ u vstupu do areálu, která obsahuje osobní identifikační údaje návštěvy a časové údaje o tom, kdy byla vykonána.
- **režim pohybu osob v ZO** - oprávněné osoby samostatně (na základě předaných vstupních prostředků), všichni ostatní pouze v doprovodu těchto osob.
- **režim pohybu utajovaných informací v objektu a ZO** - oprávněná osoba je povinna zajistit utajované informace tak, aby se k nim nedostaly, nebo se s nimi neseznámily neoprávněné osoby. V objektu i v ZO lze zpracovávat pouze utajované informace do stupně utajení Vyhrazené.
- **pravidla pro manipulaci s klíči** - klíči od objektu a ZO disponují pouze osoby, kterým byly klíče protokolárně předány oproti podpisu na základě jejich oprávnění ke vstupu do objektu a ZO nebo osoby, které jsou uvedeny na schránce s klíči a mohou se v objektu a ZO pohybovat samostatně. Klíče od objektů jsou uloženy v zapečetěné schránce č. 1 na stanovišti ostražky. Klíče od ZO č. 1, 2 se ukládají pod stálým dohledem ostražky v zapečetěné schránce a jsou předávány proti podpisu v knize „Kniha výdeje schránek s klíči R“. Duplikáty klíčů od objektu a ZO jsou uloženy v UO v kanceláři bezpečnostního manažera společnosti v obálce č. 1, 2.

3.2.5 Technická dokumentace FB

3.2.5.1 Výkresová dokumentace



Obrázek č. 24 Stanovení hranice objektu a ZO



Obrázek č. 25 Rozmístění technických prostředků V

3.2.6 Dokumentace technických prostředků

TECHNICKÝ PROSTŘEDEK (výčet)	UMÍSTĚNÍ (ZO)	BODOVÉ OHODNOCENÍ/TYP/ IČ CERTIFIKÁTU/PROHLÁŠENÍ O SHODĚ
Úschovný objekt KOVONA A 807 výr.č. 11111	1	S1=1/typ 1/ zápis o shodě
Úschovný objekt KOVONA A 807 výr.č. 22222	2	S1=1/typ 1/ zápis o shodě
Úschovný objekt Informační systém	1	S1=1/typ 1/certifikát S000115
Mříže Typ Nůžková mříž dvoukřídlová 99	1	SS3=2,SS4=2/typ 2/ certifikát T0025/2010
Mříže Typ Nůžková mříž dvoukřídlová NMK3-T	2	SS3=3,SS4=2/typ 3/ certifikát T0024/2010
Dveře Typ: BEDEX VARIO V 3 s požární odolností se zárubní MRB	1	SS3=3,SS4=2/typ 3 /certifikát T0093/2010
Dveře Typ: SOLODOOR protipožárně odolné	1,2	S1=1/typ 1/ zápis o shodě
Uzamykací systém Typ: bezpečnostní kování R1 cylindrická vložka MULT-T-LOCK	1,2	SS4=2/typ 2/ certifikát T0081/2010 certifikát T0022/2010
Zařízení fyzického ničení nosičů informací Typ JAWS S4 (řez 2x12mm)	1,2	bez bodového hodnocení/typ 3/certifikát T 5012 /2008
Dveře (výstupní,vnitřní)	1,4	typ 0
Okna	1,2	typ 0

Tabulka č. 3 Dokumentace technických prostředků V

3.2.7 Ověřování funkčnosti technických prostředků

Funkční zkoušky technických prostředků se provádí nejméně 1x za 12 měsíců v rámci ověřování opatření fyzické bezpečnosti v souladu s § 10, odst. 1 vyhlášky č. 528/2005 Sb. Zápis o provedení funkčních zkoušek je uveden v části 6.

(Pozn.: v rámci zápisu ověřování opatření FB bude písemně uvedeno, že byly dále provedeny funkční zkoušky u konkrétních technických prostředků (všechny vypsány) a bude uvedeno s jakým závěrem)

3.3 Návrh vyššího zabezpečení

Uživatel v souladu s požadavky vyplývajících s platných právních předpisů požaduje zabezpečit objekt (oblast) budovy A 1. nadzemní podlaží proti úmyslné a organizované trestné činnosti, krádežím, neoprávněné manipulaci s utajovanými informacemi, zabezpečení proti vstupu nepovolaných osob, jak v pracovní době, tak v mimo pracovní dobu a proti neoprávněným osobám.

Zabezpečení zabezpečené oblasti kategorie Důvěrné a Tajné budou v souladu s vyhláškou 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků zabezpečeny certifikovanými mechanickými zábrannými prostředky pro danou kategorii (bezpečnostní dveře, okenní vnitřní nůžkové mříže, uzamykací systém), elektrickou zabezpečovací signalizací (EZS), systémem kontroly vstupu SKV, elektrickou požární signalizací (EPS), úschovnými objekty typu 1 pro uložení utajované dokumentace.

U společnosti Product Security a.s. se budou vyskytovat UI vlastní nebo poskytnuté zpravidla spolupracujícími subjekty v rámci České republiky (také "ČR"). Dále se budou vyskytovat neutajované a UI poskytnuté stranami NATO, EU a ostatními smluvními stranami. Charakter poskytovaných a u společnosti vznikajících UI vyplývá z nařízení vlády č. 240/2008, kterým se mění nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam UI ve znění pozdějších předpisů. U společnosti Product Security a.s. se jedná především o UI při státních zakázkách především v působnosti resortu MO ČR.

3.4 Režimová opatření

V rámci režimových opatření je potřeba zamezit vstupu osob, které nemají oprávnění pro vstup do prostorů společnosti Product Security a.s a ochranu UI.

Objekt budova A – hlavní vstup zabezpečit elektronickým vstupem pro zamezení pohybu neoprávněných osob, vedlejší vchody do budov chránit proti neoprávněnému vniknutí do budovy zařízením elektrické zabezpečovací signalizace. Pro manipulaci s klíči, jejich odevzdávání a úschovu a evidence na stanovišti ostražky, zavěsit skříně na ukládání krabiček s klíči (neutajované místnosti) a elektronickou úložnu krabiček s klíči (režimové místnosti).

Zabezpečení ochrany přístupových bodů (vstupních bran) po obvodu fyzické bariéry (hranice, oplocení) ponechat na stávající úrovni, která je dostačující. Při vstupu do zabezpečené oblasti a objektu neoprávněnou osobou, zamezit seznámit se s utajovanou informací.

3.5 Stupeň utajení utajovaných informací

U společnosti se budou vyskytovat, vznikat a zpracovávat utajované informace následujících stupňů utajení:

- Vyhrazené - ANO
- Důvěrné - ANO
- Tajné – ANO
- Přísně tajné - NE

3.6 Druh utajovaných informací

U společnosti se budou vyskytovat utajované informace vlastní nebo poskytnuté zpravidla spolupracujícími subjekty v rámci ministerstev ČR.

Charakter poskytovaných a u společnosti vznikajících UI vyplývá z nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. U společnosti se jedná především o UI v oblasti působnosti Ministerstva obrany, tj. přílohy č. 6 k uvedenému nařízení vlády. V současné době se zpracovává okolo 120 Vyhrazených dokumentů ročně. Předpokládaný rozsah výskytu a zpracování UI v následujícím roce bude okolo 100 dokumentů V a okolo 20 dokumentů D, T.

3.7 Četnost manipulace s UI

Manipulace s utajovanými informacemi v podmínkách společnosti: **pravidelná**

3.8 Místa výskytu utajovaných informací

Ukládání a manipulace s utajovanými informacemi bude pouze v zabezpečených oblastech (dále také „ZO“).

S utajovanými informacemi lze manipulovat:

- v zabezpečené oblasti - ANO
- v objektu mimo zabezpečenou oblast – ANO
- v odůvodněných případech s písemným souhlasem vedoucího organizace mimo „objekt“.

Manipulovat s UI lze pouze za podmínek, stanovených v § 24 odst. 5 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále také „zákon“). Utajované informace mohou zpracovávat nebo s nimi jinak manipulovat pouze ty osoby, které splňují podmínky přístupu k UI příslušného stupně utajení stanovené zákonem (dále také „oprávněné osoby“).

3.9 Stanovení jednotlivých hrozeb, zranitelnosti UI a jejich vyhodnocení

Vyhodnotit rizika a stanovit jejich míru je povinen, v souladu s vyhláškou č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků odpovědná osoba nebo jím pověřená osoba.

3.9.1 Vyzrazení UI oprávněnými osobami

Úmyslné nebo neúmyslné vyzrazení UI je porušení povinností oprávněných osob vyplývajících ze zákona a jeho prováděcích vyhlášek, zejména vyhlášky č. 529/2005 Sb. o administrativní bezpečnosti a o registrech utajovaných informací, a dále z interních normativních aktů souvisejících s ochranou UI.

O způsobech nakládání s UI jsou příslušníci společnosti pravidelně proškolení. V minulosti nedošlo v prostoru objektu k neoprávněnému nakládání s UI poučenými osobami.

Neoprávněné nakládání s UI listinného charakteru - v minulosti k neoprávněnému nakládání s UI v listinné podobě nedošlo, ale do budoucna nelze vyloučit selhání lidského faktoru.

Bezpečnostním ředitelem byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na

střední riziko.

3.9.2 Manipulace s UI neoprávněnými osobami

Zpravidla se jedná o náhodné seznámení se s UI nebo trestnou činnost (vloupání do objektu a ZO, přepadení oprávněné osoby, která s UI manipuluje, přenáší a přepravuje ji mimo „objekt“, nálezem utajovaného dokumentu apod.).

Hrozba je zpravidla představována formou násilné trestné činnosti. V minulosti nedošlo v prostoru objektu k neoprávněnému nakládání s UI poučenými osobami ani k násilné trestné činnosti. Uvedenou skutečnost nelze do budoucna vyloučit. Ke krádeži materiálu u společnosti nedocházelo. Vzhledem k poměrně velkému počtu zaměstnanců a velké cirkulaci návštěv nelze do budoucna toto vyloučit.

Bezpečnostním ředitelem byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na

střední riziko.

3.9.3 Poškození (zničení) UI živelnou pohromou

Zahrnuje možnosti poškození nebo zničení UI živelnou pohromou, zemětřesením, povodní, bleskem, požárem, vichřicí nebo omezení možnosti chránit UI v případě jejího vzniku.

V minulosti nedošlo ke vzniku uvedené hrozby, přesto nelze vyloučit vliv nenadálých přírodních jevů.

Bezpečnostním ředitelem byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na

malé riziko.

3.9.4 Poškození (zničení) UI průmyslovou nebo technologickou havárií

Zahrnuje možnost poškození nebo zničení UI průmyslovou a technologickou havárií (např. únikem nebezpečných chemických látek a přípravků ze stacionárních zdrojů, při jejich přepravě; únikem vody následkem poruchy na potrubí apod.) nebo omezení možnosti chránit UI za této situace.

Vzhledem k umístění objektů se nepředpokládá možnost hrozby poškozením nebo zničením UI v důsledku průmyslové nebo technologické havárie a následně k možnosti neoprávněného nakládání s UI za této situace. Nejbližší objekty, které by mohly způsobit technologickou havárii vlastního objektu je ve vzdálenosti cca 500 m benzínová pumpa do vzdálenosti cca 200 m mlékárny a pekárny, do vzdálenosti 500 m zimní stadion. K technologické havárii dosud nedošlo, ale vzhledem k možnosti selhání lidského faktoru nebo technických prostředků do budoucna toto nelze vyloučit.

Bezpečnostním ředitelem byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na

střední riziko.

3.9.5 Ztráta UI následkem teroristického útoku

Možnost ztráty UI při teroristickém útoku jednotlivce nebo skupiny je na velice nízké úrovni.

K sabotáži na zařízení objektů v areálu společnosti dosud nedošlo a nedochází. Do budoucna toto nelze vyloučit z důvodu selhání lidského faktoru. K ohrožení osob při teroristickém útoku dosud nedošlo, ale do budoucna to nelze vyloučit vzhledem k možnostem výskytu teroristických hrozeb.

Výhružky o umístění výbušniny nebyly dosud zaznamenány a do budoucna není předpoklad, že tato situace nastane.

Bezpečnostním ředitelem byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na

malé riziko.

3.9.6 Vyzrazení UI pasivním odposlechem nebo nasazením operativní techniky

Získání UI odposlechem, nasazením operativní techniky nelze vyloučit. Pro zhodnocení hrozby je rozhodující skutečnost, zda UI mají charakter informací, které lze odposlechem získat a zda jsou z pohledu nasazení operativní techniky zajímavé.

Prostory objektů areálu se jeví jako nezajímavé k nasazení operativní techniky a to z důvodu jejího nepravidelného projednávání. Při projednávání UI jsou provedena maximální možná opatření k zamezení odposlechu. Únik UI prostřednictvím slovních vyjádření zaměstnanců mimo organizaci dosud nebyl zaznamenán, ale do budoucna nelze vyloučit selhání lidského faktoru a morálního selhání zaměstnanců.

Bezpečnostním ředitelem byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na

střední riziko.

3.9.7 Vyzrazení nebo ztráta UI z informačního systému

Možnosti úniku UI zpracovávaných v elektronické podobě, zničení nebo poškození dat charakteru UI nebyly doposud zaznamenány, tak jako kopírování nebo neoprávněný vstup do IS nebo počítačové sítě.

UI jsou zpracovávány na vyčleněných počítačích IS, nacházejících se v zabezpečených oblastech. O způsobech práce na počítači IS byly všichni uživatelé IS proškoleni.

Opomenutí nebo zanedbání povinnosti pracovníků uživatele v plnění předepsaných úkolů a kontrol dosud nedošlo, ale do budoucna nelze vyloučit selhání lidského faktoru

Bezpečnostním ředitelem byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na

střední riziko.

3.9.8 Poškození (zničení) UI v ostatních případech

Možnosti ztráty, zcizení, poškození nebo zničení UI např. při ohrožení státu (válečné nebezpečí, útok cizí moci, snaha o destrukci demokratického zřízení vnitřními silami), při změně politické situace apod. není zcela vyloučeno.

Bezpečnostním ředitelem byla na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací stanovena míra rizika na

střední riziko.

3.9.9 Stanovení celkové míry rizika

Při vyhodnocení rizik je zohledněn zejména druh, stupeň a rozsah UI, specifika manipulace s UI a jejich zranitelnost vůči specifikovaným hrozbám.

Na základě zhodnocení jednotlivých rizik stanovil bezpečnostní ředitel pro tento objekt celkovou míru rizika na

střední riziko.

3.10 Projekt fyzické bezpečnosti

Dokument musí zpracovat každý subjekt, který bude ve smyslu zákona č. 412/2005 Sb., nakládat s utajovanými informacemi ať už jako podnikatel nebo orgán státní správy. Před prvním zpracováním či seznámením s utajovanou informací je potřeba zabezpečit a učinit opatření, která jsou nezbytná k ochraně utajovaných informací. Dle kategorie utajení zabezpečit objekt mechanickými zábrannými systémy, instalací poplachového zabezpečovacího a tísňového systému, instalací elektronické kontroly vstupu nebo speciálních televizních systémů. Musí být vydána pravidla jak s utajovanými informacemi nakládat, určit pohyb zaměstnanců a návštěv po objektu, popřípadě i vozidel. Vypracovaný projekt pro určitou kategorii musí být podstoupen ke schválení Národnímu bezpečnostnímu úřadu.

Schválený projekt se ukládá u pověřené osoby nebo u bezpečnostního ředitele.

Právně je projekt fyzické bezpečnosti řešen v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti ve druhé části, hlava V, § 32 a 33. Samotný obsah projektu záleží na kategorii daného objektu, zabezpečené oblasti či jednacím místnosti.

Projekt pro objekt a zabezpečenou oblast kategorie Vyhrazené musí obsahovat:

- určení objektu a zabezpečených oblastí, včetně jejich hranic a určení kategorie a tříd zabezpečených oblastí,
- způsob použití opatření fyzické bezpečnosti.

Zvýšená pozornost se věnuje projektu fyzické bezpečnosti, kde se nachází objekty a zabezpečené oblasti kategorie Důvěrné, Tajné a Přísně tajné. V těchto případech musí projekt obsahovat tyto náležitosti:

- určení objektu a zabezpečených oblastí, včetně jejich hranic a určení kategorií a tříd zabezpečených oblastí,
- vyhodnocení rizik,
- způsob použití opatření fyzické bezpečnosti,
- provozní řád objektu,
- plán zabezpečení objektu a zabezpečených oblastí v krizových situacích.

Právním prováděcím předpisem, který stanoví bodové ohodnocení jednotlivých opatření fyzické bezpečnosti, nejnižší míru zabezpečení zabezpečené oblasti a jednacích oblastí, základní metodu hodnocení rizik, další požadavky na opatření fyzické bezpečnosti a náležitosti certifikace technického prostředku, je vyhláška č. 528/2005Sb., o fyzické bezpečnosti a certifikaci technických prostředků ve znění pozdějších předpisů.

3.11 Návrh projektu fyzické bezpečnosti

V rámci řešení této práce byl jejím autorem zpracován návrh projektu fyzické bezpečnosti pro soukromou společnost Product Security a.s. Z důvodu vlastního formátování byla vložena do diplomové práce jako příloha č. 1.

4 Závěr

Cílem diplomové práce bylo vypracovat projekt vyššího stupně zabezpečení ochrany utajovaných informací a popsat systémy ochrany v oblasti fyzické (objektové) bezpečnosti pro všechny, kteří se touto problematikou zabývají.

Práce byla rozdělena do dvou částí – teoretickou a praktickou.

V teoretické části práce byla popsána legislativní úprava, která se zabývá ochranou utajovaných informací s důrazem na nejdůležitější části zákona 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti a prováděcích předpisech k tomuto zákonu. Dalším zdrojem informací, který řeší fyzickou bezpečnost a hlavně přesnou strukturu projektu fyzické bezpečnosti a jednotlivé bodového ohodnocení byla Vyhláška 528/2005 Sb., ve znění vyhlášky č. 19/2008 Sb. Ve druhé části bylo popsáno zajištění objektu z obecného hlediska, byly vysvětleny základní pojmy, které byly předmětem této práce.

V praktické části byl popsán fiktivní rozsáhlý objekt firmy Product Security a.s. a v něm vybraná budova, kde byla provedena analýza stávajícího stavu fyzického zabezpečení a navržen nový bezpečnostní projekt na vyšší stupeň zabezpečení zabezpečených oblastí, kde se budou ukládat utajované informace podléhající stupni utajení Důvěrné a Tajné.

Popsání fyzické bezpečnosti a hlavně v nějakém konkrétním případě je velmi složité a veřejně nedostupné. Tyto informace podléhají danému stupni utajení, a proto byl vybrán, posuzován a vypracován fiktivní objekt a projekt fyzické bezpečnosti.

Z důvodu velikého množství druhů jak mechanických zábranných systémů tak i poplachových zabezpečovacích a tísňových systému, bylo vybráno do této práce pouze to podstatné, co bylo potřeba pro dané zabezpečení.

Obsah této diplomové práce může být návodem pro bezpečnostní management v soukromém sektoru, jak tomu je i v této práci, tak hlavně ve složkách, které jsou zahrnuty v integrovaném záchranném systému (policie, armáda atd...). V institucích veřejného sektoru se jedná hlavně o personální bezpečnost ve vztahu k významnému rozsahu dat se kterými operuje.

SEZNAM POUŽITÉ LITERATURY

IVANKA, Ján. *Mechanické zábranné systémy*, Vyd. 2. Zlín 2014, Universita Tomáše Bati ve Zlíně, 146 s. ISBN 978-80-7454-427-9

KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*, Vyd. 3. Cricetus 2006, 313 s. ISBN 80-902938-2-4

LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*, Vyd. 3. Zlín 2010, 81 s. ISBN 978-80-7318-889-4

LUKÁŠ, Luděk a kol. *Bezpečnostní technologie, systémy a management I*, Vyd. 1 Zlín 2011, VeRBuM, 316 s. ISBN 978-80-87500-05-7

NĚMEC, Vladimír. *Projektový management*, vydala GRADA Publishing, a.s. 2002, 183 s. ISBN 80-247-0392-0

UHLÁŘ, Jan. *Technická ochrana objektů. I.díl Mechanické zábranné systémy II*, Praha 2004, 177 s. ISBN 80-7251-172-6

UHLÁŘ, Jan. *Technická ochrana objektů II. díl - Elektrické zabezpečovací systémy II*, Praha: PA ČR 2005, 228 s. ISBN 80-7251-189-0

LEGISLATIVA A NORMY

Česko. Vláda. Zákon č. 412/2005 Sb., o *ochraně utajovaných informací a o bezpečnostní způsobilosti*, ve znění pozdějších předpisů [online]. 118 s. (PDF) [cit. 2015-08-21]
Dostupný z WWW:

<http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/>

Česko. Ministerstvo obrany. RMO č. 14/2013 Věstníku *Ochrana utajovaných informací v resortu Ministerstva obrany*. 24 s.

Česko. Vláda. Vyhláška č. 528/2005 o *fyzické bezpečnosti a certifikaci technických prostředků*, ve znění pozdějších předpisů[online]. 7 s. (PDF) [cit. 2015-08-20]
Dostupný z WWW:

<http://www.nbu.cz/cs/pravni-predpisy/provadecci-pravni-predpisy/vyhlaska-c-5282005/>

Česko. Ministerstvo obrany. NVMO č. 77/2013 *Fyzická bezpečnost v resortu Ministerstva obrany*. 32 s.

INTERNETOVÉ ZDROJE

- Technické prostředky.* [online] © 2015. [cit. 2015-09-08]. Dostupné z <http://www.magazin.specialista.info/view.php?cislocclanku=2005100201>
- Fyzická bariera typu.* [online] © 2015. [cit. 2015-09-21]. Dostupné z <http://www.dirickx.cz>
- Samonosná bezpečnostní brána typu 4.* [online] © 2015. [cit. 2015-09-21]. Dostupné z <http://www.dirickx.cz>
- Plášťová ochrana.* [online] © 2015. [cit. 2015-09-9]. Dostupné z <http://www.ictsecurity.cz/odborne-clanky/fyzicka-ochrana-dat.html>
- Bezpečnostní dveře.* [online] © 2015. [cit. 2015-09-22]. Dostupné z <http://www.bezpecnostnidvere.info>
- Bezpečnostní mříže – nůžkové.* [online] © 2015. [cit. 2015-09-22]. Dostupné z <http://www.next.cz/cs/produkty/pc-3-bezpecnostni-mrize/pr-22-nuzkove-mrize/>
- Perimetrická ochrana.* [online] © 2015. [cit. 2015-09-9]. Dostupné z <https://moodle.unob.cz/pluginfile.pdf>
- Legislativa kybernetické bezpečnosti.* [online] © 2015. [cit. 2015-09-9]. Dostupné z <https://www.govcert.cz/cs/legislativa/legislativa/>
- Bezpečnostní sklo.* [online] © 2015. [cit. 2015-09-10]. Dostupné z <http://www.wdokna.cz/varianty-sklenenych-vyplni-okna-a-dveri/>
- Bezpečnostní třída trezorů.* [online] © 2015. [cit. 2015-09-10]. Dostupné z <http://www.aparch.cz/trezory-tla-bezpecnostni-trida-i-dle-csn-en-1143-1/>
- Komorový trezor ČNB.* [online] © 2015. [cit. 2015-09-11]. Dostupné z <http://ekonomika.idnes.cz/>
- Bezpečnostní třídy komorových trezorů.* [online] © 2015. [cit. 2015-09-12] Dostupné z <http://www.metalsafe.cz/cs/vse-o-trezorech/bezpecnostni-tridy-trezoru>
- Trezorové bezpečnostní třídy.* [online] © 2015. [cit. 2015-09-12] Dostupné z <http://www.trezor.cz/podpora-a-servis/bezpecnostni-tridy-a-deleni-trezoru.htm>
- Systém kontroly vstupu.* [online] © 2015. [cit. 2015-09-12] Dostupné z <http://www.meritgroup.cz/elektronicka-kontrola-vstupu.asp>
- Poplachové zabezpečovací a tísňové systémy.* [online] © 2015. [cit. 2015-09-13] Dostupné z <http://www.eatonelektrotechnika.cz/cz/poplachove-zabezpecovaci-a-tisnove-systemy-ezs.html>
- Blokové schéma PIR detektoru.* [online] © 2015. [cit. 2015-09-15] Dostupné z <http://www.hw.cz/automatizace/pir-cidlo-skvely-sluha-ale-zly-pan.html>
- Vyzařovací charakteristika PIR detektoru.* [online] © 2015. [cit. 2015-09-16] Dostupné z <http://www.stasanet.cz/Paradox-a-ostatni-EZS/Vnitni-detekce/Detektory>

Vyzařovací charakteristika stropního PIR detektoru. [online] © 2015. [cit. 2015-09-20] Dostupné z <http://www.eurosat.cz/2662-optex-sx-360z.html>

Sada PIR detektorů. [online] © 2015. [cit. 2015-09-16] Dostupné z <http://www.bfb-falco.cz/klient.html>

Kamerové systémy. [online] © 2015. [cit. 2015-09-20] Dostupné z <http://www.t-bau.cz/elektroinstalace/kamerove-systemy/>

Typy bezpečnostních kamer. [online] © 2015. [cit. 2015-10-04] Dostupné z <http://di.com.pl/informacje/galeria,46366,12333.html>

Prvky EPS. [online] © 2015. [cit. 2015-10-04] Dostupné z <http://www.tzb-info.cz/pozarni-ochrana/8586-siemens-na-veletrhu-pragoalarm-pragosec-2012>

Elektrické zabezpečovací systémy. [online] © 2015. [cit. 2015-10-06] Dostupné z <http://www.t-bau.cz/elektroinstalace/elektricke-zabezpecovaci-systemy/>

Skartovací stroj JAWS. [online] © 2015. [cit. 2015-10-9] Dostupné z <http://www.texpo-cz.cz/skartovaci-stroj-jaws-c9-kapacita-11listu-rez-2x8mm-nbu-certifikat-stupen-3>

Certifikační postup NBÚ. [online] © 2015. [cit. 2015-10-9] Dostupné z <http://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost/certifikace/certifikacni-postup-nbu/informace-k-certifikacnimu-postupu-nbu/>

Areál společnosti. [online] © 2015. [cit. 2015-10-9] Dostupné z <http://mapy.cz/letecka>

Certifikát technického prostředku. [online] © 2015. [cit. 2015-10-20] Dostupné z <http://www.dverebedex.cz/certifikaty/certifikaty-vydane-nbu>

SEZNAM POUŽITÝCH ZKRATEK A POJMŮ

ACS – Přístupový kontrolní systém - Acces Control System
CCTV - Uzavřený přenos televizního signálu - Closed circuit TV
ČSN EN - Česká technická norma přejímající evropskou normu
EZS - Elektronické zabezpečovací systémy - Electronic Security System
EPS - Elektronické požární signalizace - Fire Alarm System
MW detektor – Mikrovlnný detektor - Micro Wave Detector
LAN - Lokální síť (počítačová) - Local Area Network
LCD - Displej z tekutých krystalů - Liquid Crystal Display
NBÚ - Národní Bezpečnostní Úřad
PCO - Pult centrální ochrany
PIR detektor - Pasivní infračervený detektor - Passive Infrared Detector
ZO - Zabezpečená oblast
JO - Jednací oblast
PFB - Projekt fyzické bezpečnosti
PZTS - Poplachové zabezpečovací a tísňové systémy
ČR - Česká republika
NATO - Severoatlantická aliance - North Atlantic Treaty Organization
EU - Evropská unie - European Union
UI - Utajovaná informace
IS - Informační systém

SEZNAM OBRÁZKŮ

Obr. č. 1 Schéma systému ochrany utajovaných informací	19
Obr. č. 2 Systém bezpečnosti a ochrany majetku	24
Obr. č. 3 Systém bezpečnosti a ochrany majetku	24
Obr. č. 4 Fyzická bariera typu 4	26
Obr. č. 5 Samonosná bezpečnostní brána	26
Obr. č. 6 Bezpečnostní dveře	28
Obr. č. 7 Bezpečnostní mříž- dveře	30
Obr. č. 8 Nůžková bezpečnostní mříž	30
Obr. č. 9 Bezpečnostní sklo	31
Obr. č. 10 Bezpečnostní třídy dle EN1627	32
Obr. č. 11 Trezor řady TLA - bezpečnostní třída I dle ČSN EN 1143.1.....	32
Obr. č. 12 Komerový trezor ČNB	34
Obr. č. 13 Systém pro kontrolu vstupu	40
Obr. č. 14 Biometrický systém kontroly vstupu	40
Obr. č. 15 Ústředna v plastovém krytu GFlex 20 - V3 7Ah s komunikátorem a LCD kláv-MK	41
Obr. č. 16 Blokované schéma PIR detektoru	43
Obr. č. 17 Vyzařovací charakteristika PIR detektoru pohybu	43
Obr. č. 18 Vyzařovací charakteristika stropního PIR detektoru pohybu	44
Obr. č. 19 Sada PIR detektorů	44
Obr. č. 20 Typy bezpečnostních kamer	45
Obr. č. 21 Prvky EPS	46
Obr. č. 22 Skartovací stroj JAWS C9, řez 2x8mm, NBÚ certifikát stupeň 3	47
Obr. č. 23 Posuzovaný objekt v dané lokalitě	51
Obr. č. 24 Stanovení hranice objektu a ZO	56
Obr. č. 25 Rozmístění technických prostředků	56
Obr. č. 26 Vyznačení hranice objektu, hranice ZO a rozmístění technických prostředků D, T	82
Obr. č. 27 Certifikát technického prostředku	86
Obr. č. 28 Příloha certifikátu technického prostředku	87

SEZNAM TABULEK

Tabulka č. 1 Koeficienty průlomové odolnosti	36
Tabulka č. 2 Minimální požadavky bezpečnostních tříd trezorů	37
Tabulka č. 3 Dokumentace technických prostředků V	56
Tabulka č. 4 Bodové ohodnocení opatření fyzické bezpečnosti T	74
Tabulka č. 4 Bodové ohodnocení opatření fyzické bezpečnosti D	76
Tabulka č. 5 Přehled použitých technických prostředků D, T	84

SEZNAM PŘÍLOH

Příloha č. 1 Projekt fyzické bezpečnosti	67
--	----

Projekt fyzické bezpečnosti

objekt společnosti Product Security a.s.

administrativní budova (budova A) – I. nadzemní podlaží

zabezpečené oblasti

Důvěrné a Tajné

Vypracoval: Bc. Karel ZEDEK

I. Určení objektu a zabezpečených oblastí

Obecný úvod

Objekt, který je posuzován, je zrekonstruovaná jednopodlažní budova A (administrativní budova společnosti) v areálu firmy Product Security a.s. Od ostatních budov není oddělena oplocením. Terén kolem budovy je rovinný a travnatý. V objektu jsou umístěny ZO č. 1, 2 kategorie Důvěrné a Tajné. Objekt má jeden vstup. Vstup do objektu je realizován dveřmi s uzamykacím systémem. Projekt fyzické bezpečnosti je v souladu se zákonem 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a vyhláškou č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků a za ochranu utajovaných informací zodpovídá ředitel společnosti.

Stanovení objektu a zabezpečených oblastí

Objekt typu 2 společnosti Product Security a.s, je nepodsklepená jednopodlažní budova o půdorysné velikosti 14,20 x 52,40 m. Hranici objektu tvoří plášť vnitřního a vnějšího obvodového zdiva budovy A. Minimální síla obvodových zdí je 300 mm, vnitřních zdí je 150 mm. Minimální síla podlahové a stropní konstrukce je 200 mm. Objekt je dle statě č. 3 a 6 přílohy č. 1 k vyhlášce 528/2005 Sb. typu 2 lehká stavební konstrukce, průlezné otvory jsou zabezpečeny mechanickými zábrannými systémy a poplachovými zabezpečovacími a tísňovými systémy. Na vnějším plášti jsou instalované hromosvody. Typ střechy budovy tvoří dřevěný sedlový krov v krajních částech valbový.

Do budovy je jeden vchod, který je zabezpečen vchodovými dvoukřídlovými dveřmi ze 2/3 zaskleným bezpečnostním izolačním sklem, uzamykatelným bezpečnostním zámkem a elektronickou kontrolou vstupu na čipovou kartu společnosti. Vstup je povolen pouze osobám, které splňují bezpečnostní předpisy dle zákona 412/2005 Sb. a určuje ho bezpečnostní ředitel společnosti. Stávající samostatný objekt není od ostatních budov oddělen oplocením.

V objektu se kromě neutajovaných materiálů nachází dokumenty, které nejsou určeny ke zveřejnění (dokumentace obsahující obchodní tajemství atd.) a dále utajované materiály do stupně utajení Tajné.

Z hlediska množství utajovaných informací se může jednat řádově o 120 dokumentů do stupně utajení Tajné.

V objektu se nachází dvě zabezpečené oblasti:

- zabezpečená oblast č. 1 kategorie Důvěrné, stanovená třída II má hranici shodnou s hranicí objektu. Nachází se v místnosti č. 3 v 1. NP budovy A – administrativní budova společnosti, pracoviště zabezpečení materiálem, úložna pracoviště zabezpečení materiálem. Minimální síla obvodových zdí je 300 mm, minimální síla vnitřních zdí je 150 mm. Minimální síla podlahové a stropní konstrukce je 200 mm. Zabezpečená oblast má pouze jeden vstup a jednu okno, jehož výška nad terénem je menší než 5,5 m.

Zabezpečená oblast je typu 2, průlezné otvory jsou zabezpečeny certifikovanými mechanickými zábrannými prostředky – certifikovaná nůžková mříž dvoukřídlá typ 2, vstupní certifikované dveře BEDEX VARIO V3 s požární odolností typu 3 a bezpečnostním kováním R1 a cylindrickou vložkou MULT-T-LOCK typu 2. V zabezpečené oblasti se nachází úschovný objekt TLA 6 typ 3 a certifikované zařízení fyzického ničení nosičů informací JAWS S 4 typ 3.

Poplachový zabezpečovací a tísňový systém tvoří detektor otevření MAS 303 umístěn na okně a vstupních dveřích, detektor pohybu Duální PIR + MX RK815DT-G3, detektor tříštění skla FG 1625TAS-G3 a na vstupu bezkontaktní čtečka karet Cotag Asset 301. Instalace PZTS je typu 3. Narušení prostoru je signalizováno u ostrahy v budově B.

- zabezpečená oblast č. 2 kategorie Tajné, stanovená třída II má hranici shodnou s hranicí objektu. Nachází se v místnosti č. 4 v 1. NP budovy A – administrativní budova společnosti, pracoviště technologií. Minimální síla obvodových zdí je 300 mm, minimální síla vnitřních zdí je 150 mm. Minimální síla podlahové a stropní konstrukce je 200 mm. Zabezpečená oblast má pouze jeden vstup a jednu okno, jehož výška nad terénem je menší než 5,5 m.

Zabezpečená oblast je typu 2, průlezné otvory jsou zabezpečeny certifikovanými mechanickými zábrannými prostředky – certifikovaná nůžková mříž dvoukřídlá NMK3-T typ 3, vstupní certifikované dveře BEDEX VARIO V3 s požární odolností typu 3 a zadlabávacím elektromechanickým zámkem ABLOY BEF 022421 typu 3. V zabezpečené oblasti se nachází úschovný objekt TLA 4 typ 3 a certifikované zařízení fyzického ničení nosičů informací JAWS S 4 typ 3.

Poplachový zabezpečovací a tísňový systém tvoří detektor otevření MAS 303 umístěn na okně a vstupních dveřích, detektor pohybu Duální PIR + MX RK815DT-G3, detektor tříštění skla FG 1625TAS-G3, na stropě místnosti je nainstalován automatický požární hlásič SS2351KNL. Pro vstup do zabezpečené oblasti je nainstalována bezkontaktní čtečka karet COTAG s PIN klávesnicí Asset 311 a pro odchod z místnosti bezkontaktní čtečka karet COTAG Asset 301. V místnosti je také instalován tísňový hlásič S3040/SROV typu 3. Pro nouzové opuštění prostoru bez použití bezkontaktní karty je vedle dveří umístěno bezpečnostní odchodové tlačítko s výstupem do PZTS, které rozbitím skla nouzově otevře bezpečnostní dveře. Instalace PZTS je typu 3. V zabezpečené oblasti je umístěno certifikované zařízení fyzického ničení nosičů informací JAWS S 4 typ 3. Narušení prostoru je signalizováno u ostražky v budově B.

Ústředna PZTS je instalována v místnosti č. 4 - systém Asset 804.

Popis areálu a okolí z hlediska bezpečnosti:

Terén kolem areálu je rovinný a nachází se v zastavěné městské části města Olomouc a vizuální pozorování z okolí je možné v rozsahu 20% ze strany Okružní ulice. Uvnitř areálu jsou komunikace s asfaltovým a betonovým povrchem, které umožňují zásah hasičského požárního sboru, Policie České republiky, zásahové jednotky, vozidel likvidační skupiny. Celý areál společnosti je zabezpečen zděným oplocením po celém obvodu objektu (zdivo plné cihly, betonové prefabrikáty, ocelový plech) vyšší jak 2,5 m. Oplocení areálu je od budovy A vzdáleno asi 35 metrů. Přístup do areálu je možný pouze hlavní branou (vstupem pro pěší, vjezd pro motorová vozidla), vstup do areálu je kontrolován bezpečnostní agenturou a kontrola je prováděna 24 hodin.

II. Vyhodnocení rizik

Hrozby rizik můžeme rozdělit na vnější prostředí a vnitřní prostředí.

Z vnějších rizik se můžeme zaměřit na tyto rizika

- krádež informací a materiálu,
- technologické havárie ve vlastním objektu nebo v dalších objektech,
- přírodní vlivy,
- ohrožení osob při živelné pohromě,
- výhružky o umístění výbušniny v budově,
- sabotáže a ozbrojené útoky na zařízení objektu.

Ke krádežím informací a materiálu může dojít v následujících případech:

- při služebním jednání cizích příslušníků s pracovníky,
- při služebním jednání vlastními příslušníky,
- při zabezpečení chodu – opravy a údržba, přítomnost pracovníků zabezpečujících firem. Vstup do prostor pracoviště je kontrolován a obsluhován stálou dozorčí službou. Pohyb návštěv v prostorech pracoviště je pouze s doprovodem. Tyto skutečnosti snižují vznik možných rizikových situací.

V minulosti se tato skutečnost nestala, do budoucna ji však nelze vyloučit.

Míra rizika – střední.

Při technologických haváriích ve vlastním objektu nebo v dalších objektech nebo při působení přírodních vlivů na budovu může dojít k ohrožení utajovaných informací tím, že se na odstraňování následků budou podílet nepovolané osoby a dojde k seznámení s těmito skutečnostmi.

Mezi nejrozšířenější nebezpečné látky na přilehlém území patří amoniak. Tato chemická látka je provozována ve vodárnách, zimních stadiónech, v zařízeních pro zpracování masa, mlékárnách, nemocnicích. Zimní stadion Olomouc, nebezpečná látka amoniak, množství 6 tun, předpokládaná vzdálenost ohrožení okolí 230 m. Masokombinát Olomouc, nebezpečná látka amoniak, množství 9 tun, předpokládaná vzdálenost ohrožení

okolí 300 m. Mlékárna Olomouc, nebezpečná látka amoniak, množství 10 tun, předpokládaná vzdálenost ohrožení okolí 330 m.

V minulosti se tato skutečnost nestala, do budoucna ji nelze vyloučit.

Míra rizika – střední.

Ohrožení osob při živelné pohromě může nastat při živelných pohromách a při odstraňování jejich následků.

V minulosti se tato skutečnost nestala, do budoucna ji však nelze vyloučit.

Míra rizika – střední.

V případě **výhrůžky o umístění výbušniny** při opuštění budovy příslušníky útvaru z důvodu oznámení o uložení výbušniny. Budova se nachází ve vojenském areálu – omezený vstup nepovolaných osob.

V minulosti se tato skutečnost nestala, do budoucna ji však nelze vyloučit.

Míra rizika – střední.

Sabotáže a ozbrojené útoky na zařízení objektu – vzhledem k současné mezinárodní situaci a zvýšené aktivitě teroristických skupin je nutné toto riziko zohlednit.

Míra rizika – střední.

Z vnitřních rizik se můžeme zaměřit na tyto rizika:

- opomenutí nebo zanedbání povinností pracovníků při plnění předepsaných úkolů,
- neoprávněné nakládání s utajovanou informací v listinné podobě,
- neoprávněné zpracování utajované informace na osobních počítačích,
- únik utajovaných informací prostřednictvím slovních vyjádření zaměstnanců mimo organizaci.

Opomenutím nebo zanedbáním povinností pracovníků při plnění předepsaných úkolů může dojít k situaci, že se nepovolaná osoba při vstupu na toto pracoviště může seznámit s utajovanými informacemi. Příslušníci útvaru jsou pravidelně školeni v oblasti OUI a seznámeni s podmínkami vstupu cizích osob na pracoviště a zákazu vnášení komunikačních a záznamových prostředků. Pohyb cizích osob po pracovišti je povolen pouze s doprovodem.

V minulosti se tato skutečnost nestala, lidský faktor však nelze zcela vyloučit.

Míra rizika – střední.

K neoprávněnému nakládání s utajovanou informací v listinné podobě může dojít v případě, že utajovaná informace listinného charakteru bude vynesena z prostorů pracoviště v rozporu s platnými zásadami a dojde k seznámení nepovolanými osobami. Pracovníci jsou pravidelně školeni a kontrolováni v oblasti OUI.

V minulosti se tato skutečnost nestala, do budoucna ji však nelze vyloučit.

Míra rizika – střední.

K neoprávněnému zpracování utajované informace na osobních počítačích může dojít v pracovní době jednotlivými příslušníky pracoviště.

V minulosti tato skutečnost nenastala, lidský faktor však nelze zcela vyloučit.

Míra rizika – střední.

K úniku utajovaných informací prostřednictvím slovních vyjádření zaměstnanců mimo organizaci může dojít nepatřičným slovním vyjádřením příslušníků pracoviště během rodinného nebo společenského života. Příslušníci pracoviště jsou pravidelně školeni v oblasti OUI.

V minulosti se tato skutečnost nenastala, lidský faktor však nelze vyloučit.

Míra rizika – střední.

Vyhodnocení rizik:

Uživatel po vyjádření komise v souladu s § 10 odst. 2 vyhl. NBÚ č. 528/2005 Sb., stanovil míru rizika:

„STŘEDNÍ“

Uživatel v souladu s požadavky vyplývajícími z platných právních předpisů požaduje zabezpečit objekt (oblast) budovu A 1. nadzemní podlaží proti úmyslné a organizované trestné činnosti, krádežím, neoprávněné manipulaci s utajovanými informacemi, zneužití hmotného majetku uživatele, zabezpečení proti vstupu nepovolaných osob, jak v pracovní době, tak v mimopracovní době a proti neoprávněným osobám vlastním i cizím.

III. ZPŮSOB POUŽITÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI

Tabulka bodového ohodnocení opatření fyzické bezpečnosti a zabezpečené oblasti D a T.

Zabezpečená oblast č. 1

Zabezpečená oblast je označena:	místnost č.1 - pracoviště zabezpečení materiálem a úložna pracoviště zabezpečení materiálem		
Účel místnosti	Trvalé pracoviště poučené osoby – pracoviště zabezpečení materiálem a úložna pracoviště zabezpečení materiálem stupně TAJNÉ		
Kategorie	TAJNÉ	Třída	II.
Míra rizika	střední		
Bezpečnostní opatření	Typ	Bod. hodnocení	
Úschovný objekt	typ 3	SS1 = 3bod	
Zámek úschovného objektu	typ 2	SS2 = 2 bod	
Celkové hodnocení úschovného objektu a jeho zámku	S1 = 6 bod		
Zabezpečená oblast	typ 3	SS3 = 3 body	
Uzamykací systém	typ 2	SS4 = 2 body	
Celkové hodnocení místnosti a jejího uzamykacího systému	S2 = 6 bodů		
Objekt	S3 = 0 bod		
Kontrola vstupu	typ 2	SS6 = 2 bod	
Režim návštěv	s doprovodem	SS7 = 3 body	
Celkové hodnocení kontroly vstupu	S4 = 5 bod		
Ostraha	typ 3	SS8 = 3 body	
Zařízení EZS	typ 3	SS91 = 3 body	
Instalace zařízení EZS	typ 3	SS92 = 3 body	
Mezivýsledek (SS91+SS92)/2 *SS92/OBL	SS9 = 3 bodů		
Celkové hodnocení ostrahy objektu a EZS	S5 = 6 body		
Fyzické bariery	Typ 2	SS10 = 2 bodů	
Kontrola vstupu v přístupových bodech perimetru	realizována	SS11 = 1 bodů	
Namátkové vstupní a výstupní prohlídky	realizovány	SS12 = 1 bodů	
Perimetrický detekční systém (PDS)	není realizován	SS13 = 0 bodů	
Bezpečnostní osvětlení perimetru	není realizováno	SS14 = 0 bodů	
Kamerový systém CCTV – doplněk perimetru	není realizován	SS15 = 0 bodů	
Celkové hodnocení ochrany perimetru	S6 = 4 bodů		
Celkové bodové ohodnocení zabezpečené oblasti č. 3	13 bodů		

Dosažené body		Míra rizika
Povinné:(S1) + (S2) + (S3)	9	12 splněno
Povinné:(S4) + (S5)	5	11 splněno
Nepovinné:(S6)	5	4 nesplněno
Celkový výsledek	19	23 splněno

Tabulka č. 4 Bodové ohodnocení opatření fyzické bezpečnosti T

Hodnoty proměnných S1 až S6, získané vyplněním této tabulky, je nutno porovnat s tabulkou minimálních požadovaných hodnot ohodnocení úrovně fyzické bezpečnosti pro ZO a JO (viz. Příloha č. 1 vyhl. NBÚ č. 528/2005 Sb.) a na základě tohoto porovnání učinit závěr, zda jsou přijatá bezpečnostní opatření dostatečná.

Závěr z vyhodnocení navrhovaného stavu: vyhovující

Zabezpečená oblast č. 2

Zabezpečená oblast je označena:	místnost č.2 - pracoviště zabezpečení materiálem a úložna pracoviště zabezpečení materiálem		
Účel místnosti	Trvalé pracoviště poučené osoby – pracoviště zabezpečení materiálem a úložna pracoviště zabezpečení materiálem stupně DŮVĚRNÉ		
Kategorie	DŮVĚRNÉ	Třída	II.
Míra rizika	střední		
Bezpečnostní opatření	Typ	Bod. hodnocení	
Úschovný objekt	typ 2	SS1 = 2bod	
Zámek úschovného objektu	typ 2	SS2 = 2 bod	
Celkové hodnocení úschovného objektu a jeho zámku	S1 = 6 bod		
Zabezpečená oblast	typ 2	SS3 = 2 body	
Uzamykací systém	typ 2	SS4 = 2 body	
Celkové hodnocení místnosti a jejího uzamykacího systému	S2 = 4 bodů		
Objekt	S3 = 0 bod		
Kontrola vstupu	typ 2	SS6 = 2 bod	
Režim návštěv	s doprovodem	SS7 = 3 body	
Celkové hodnocení kontroly vstupu	S4 = 5 bod		
Ostraha	typ 3	SS8 = 3 body	
Zařízení EZS	typ 3	SS91 = 3 bodů	
Instalace zařízení EZS	typ 3	SS92 = 3bodů	
Mezivýsledek (SS91+SS92)/2*SS92/OBL	SS9 = 3 bodů		
Celkové hodnocení ostrahy objektu a EZS	S5 = 6 body		
Fyzické bariery	Typ 2	SS10 = 2 bodů	
Kontrola vstupu v přístupových bodech perimetru	realizována	SS11 = 1 bodů	
Namátkové vstupní a výstupní prohlídky	realizovány	SS12 = 1 bodů	
Perimetrický detekční systém (PDS)	není realizován	SS13 = 0 bodů	
Bezpečnostní osvětlení perimetru	není realizováno	SS14 = 0 bodů	
Kamerový systém CCTV – doplněk perimetru	není realizován	SS15 = 0 bodů	
Celkové hodnocení ochrany perimetru	S6 = 3 bodů		
Celkové bodové ohodnocení zabezpečené oblasti č. 2	13 bodů		

Dosažené body		Míra rizika
Povinné:(S1) + (S2) + (S3)	8	10 splněno
Povinné:(S4) + (S5)	3	11 splněno
Nepovinné:(S6)	3	3 nesplněno
Celkový výsledek	14	21 splněno

Tabulka č. 5 Bodové ohodnocení opatření fyzické bezpečnosti D

Hodnoty proměnných S1 až S6, získané vyplněním této tabulky, je nutno porovnat s tabulkou minimálních požadovaných hodnot ohodnocení úrovně fyzické bezpečnosti pro ZO a JO (viz. Příloha č. 1 vyhl. NBÚ č. 528/2005 Sb.) a na základě tohoto porovnání učinit závěr, zda jsou přijatá bezpečnostní opatření dostatečná.

Závěr z vyhodnocení navrhovaného stavu: vyhovující

Technická dokumentace fyzické bezpečnosti.

Výkresová dokumentace s vyznačením hranice objektu zabezpečené oblasti a rozmístění technických prostředků určených k ochraně utajovaných informací je v příloze č. 1.

Dokumentace technických prostředků, která obsahuje seznam použitých technických prostředků a údaje o certifikaci a zápisy o posouzení shody je uvedena v příloze č. 2 tohoto projektu. Zároveň jsou zde kopie certifikátů Národního bezpečnostního úřadu a zprávy o posouzení shody.

Certifikace

Certifikát technického prostředku vydaný NBÚ nesmí být v době instalace technického prostředku starší dvou let.

IV. PROVOZNÍ ŘÁD

Pravidla pro režim pohybu osob a dopravních prostředků v objektu

Vstupním místem do areálu firmy Product Security a.s. je hlavní vstupní a vjezdová brána z hlavní ulice. Oprávnění ke vstupu vydává ředitel společnosti nebo jím pověřená osoba. Kontrola osob a vjezdu motorových vozidel je zabezpečována dvoučlennou směnou pracovníky ochrany objektu složenou z určených příslušníků bezpečností agentury 24 hodin.

Všichni oprávnění zaměstnanci jsou povinni prokazovat se při příchodu do areálu identifikační kartou společnosti. Identifikační karta se nosí viditelně na vnější straně oděvu po celou dobu pobytu v areálu společnosti. Při zjištění užívání identifikační karty neoprávněnou osobou, tuto událost okamžitě hlásit bezpečnostnímu řediteli společnosti.

Těmto zaměstnancům je v pracovní době vstup povolen a jejich vstup se neeviduje. Nerespektování zásad používání identifikačního průkazu ke vstupu (vjezd) se považuje za porušení pracovních povinností. Držitel průkazu je povinen chovat se tak, aby nedošlo ke ztrátě, zneužití nebo poškození průkazu. Pokud taková událost nastane, je povinen tuto skutečnost neprodleně hlásit bezpečnostnímu řediteli společnosti.

Ostatní příchozí osoby do areálu společnosti se evidují (zapisují) do knihy vstupu (vjezdu) osob (vozidel) do objektu a jsou označeni visačkou „Návštěva - Visitor“. Evidence je vedena v písemné podobě. Záležitost, pro kterou se osoby dostavili, se řeší před stanovištěm ostrahy. Pokud záležitost vyžaduje vstup do rozsáhlého objektu, požádá pracovník ostrahy cestou navštívené osoby vyzvednutí návštěvy.

Po vydání jednorázového povolení oprávnění ke vstupu do objektu s nápisem „Návštěva – Visitor“ (po provedení zápisu osobních údajů osoby vstupující do rozsáhlého objektu a jejich ověření na základě průkazu totožnosti), jej doprovází.

Navštívený zaměstnanec návštěvu po skončení účelu návštěvy doprovodí ke vstupu do areálu. Ostraha odebere jednorázové oprávnění ke vstupu do objektu s nápisem „Návštěva – Visitor“ a zaznamená čas odchodu. Předá povolení k vydání jednorázového oprávnění ke vstupu a vjezdu do objektu osobě, která návštěvu doprovázela. Tato jej následně předá členovi ostrahy.

U vjezdu vozidel se stálým povolením k vjezdu s nápisem Vjezd vozidla povolen, kontroluje jeho platnost. Údaje nutné k vjezdu do areálu se nezaznamenávají. Člen ostrahy následně zkontroluje pohledem vnitřek vozidla a ložnou plochu (zavazadlový prostor), zda nejsou přepravovány neoprávněné osoby nebo materiál, který zjevně nemá být přepravován. U všech přepravovaných osob zkontroluje průkaz ke vstupu vydaný společností.

Prozatímní oprávnění ke vstupu do objektu nebo na základě povolení k vydání jednorázového oprávnění ke vstupu a vjezdu do objektu vydá jednorázové oprávnění ke vstupu s nápisem „Návštěva – Visitor“. Veškerá povolení pro vstup osob a vjezd vozidel uděluje bezpečnostní ředitel nebo pověřená osoba.

Pravidla pro režim pohybu osob v zabezpečených oblastech

Vstupovat do objektu mohou samostatně pouze oprávněné osoby, kterým byly protokolárně předány prostředky potřebné ke vstupu do „objektu“ (klíče od vstupních dveří, kódy EZS, identifikační prvky SKV apod.).

Do zabezpečené oblasti mohou samostatně vstupovat pouze ty oprávněné osoby, kterým byly protokolárně přiděleny prostředky potřebné ke vstupu do zabezpečené oblasti (klíč od vstupních dveří, kód EZS, identifikační prvek SKV s nadefinovaným právem vstupu apod.). Další oprávněné osoby, případně návštěvy, mohou do zabezpečené oblasti vstupovat pouze v doprovodu oprávněné osoby, která může do zabezpečené oblasti vstupovat samostatně.

Osoba (návštěva), která nedisponuje s identifikační kartou společnosti nebo prozatímním oprávněním ke vstupu do objektu, je oprávněná vstupovat do budovy s doprovodem. Návštěvy jsou viditelně označeny jednorázovým oprávněním ke vstupu do objektu s nápisem „Návštěva – Visitor“. O návštěvách je vedena evidence v „Knize vstupu (vjezdu) osob (vozidel) do objektu“ u bezpečnostní ostrahy areálu, která obsahuje osobní identifikační údaje návštěv a časové údaje o tom, kdy byla návštěva vykonána.

Uživatel zabezpečené oblasti zodpovídá za to, že se nepovolaná osoba neseznámí s utajovanou informací.

Pravidla pro režim pohybu utajovaných informací v objektu

S utajovanými informacemi (dále jen „UI“) lze manipulovat v objektu (mimo zabezpečenou oblast), pokud jsou splněny požadavky § 24 odst. 5 písm. b) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále také „zákon“). S UI mohou v objektu manipulovat pouze oprávněné osoby, které splňují požadavky přístupu k UI příslušného stupně utajení stanovené zákonem, za předpokladu, že je zajištěno, že k UI nebude mít přístup neoprávněná osoba. Při manipulaci s UI mezi

oprávněnými osobami se používají administrativní pomůcky v souladu s § 3 vyhlášky č. 529/2005 Sb., které se ukládají v souladu s § 3 odst. 8 citované vyhlášky.

Utajované informace se mohou, v souladu s § 24 odst. 5 písm. c) a d) zákona v odůvodněných případech zpracovávat mimo objekt, pokud je zajištěno, že k UI nemá přístup neoprávněná osoba. Písemný souhlas k manipulaci mimo objekt je oprávněn vydat pouze ředitel společnosti. Přenášení a přepravu UI lze provádět pouze v souladu s vyhláškou č. 529/2005 Sb.

Pravidla pro užívání technických prostředků

Do budovy je jeden vchod, který je zabezpečen vchodovými dvoukřídlými dveřmi ze 2/3 zaskleným bezpečnostním izolačním sklem, uzamykatelným bezpečnostním zámkem a elektronickou kontrolou vstupu na čipovou kartu společnosti. Vstup je povolen pouze osobám, které splňují bezpečnostní předpisy dle zákona 412/2005 Sb. a určuje ho bezpečnostní ředitel společnosti. V mimo pracovní dobu od 16:00 do 5:30 je vchod uzamčen ostrahou objektu.

V zabezpečené oblasti č. 1 typu 2, jsou průlezné otvory zabezpečeny certifikovanými mechanickými zábrannými prostředky – certifikovaná nůžková mříž dvoukřídlá typ 2, vstupní certifikované dveře BEDEX VARIO V3 s požární odolností typu 3 a bezpečnostním kováním R1 a cylindrickou vložkou MULT-T-LOCK typu 2. V zabezpečené oblasti se nachází úschovný objekt TLA 6 typ 3 a certifikované zařízení fyzického ničení nosičů informací JAWS S 4 typ 3. Poplachový zabezpečovací a tísňovým systémem tvoří detektor otevření MAS 303 umístěn na okně a vstupních dveřích, detektor pohybu Duální PIR + MX RK815DT-G3, detektor tříštění skla FG 1625TAS-G3 a na vstupu bezkontaktní čtečka karet Cotag Asset 301. Instalace PZTS je typu 3.

V zabezpečené oblasti č. 2 typu 2, jsou průlezné otvory zabezpečeny certifikovanými mechanickými zábrannými prostředky – certifikovaná nůžková mříž dvoukřídlá NMK3-T typ 3, vstupní certifikované dveře BEDEX VARIO V3 s požární odolností typu 3 a zadlabávacím elektromechanickým zámkem ABLOY BEF 022421 typu 3. V zabezpečené oblasti se nachází úschovný objekt TLA 4 typ 3 a certifikované zařízení fyzického ničení nosičů informací JAWS S 4 typ 3. Poplachový zabezpečovací a tísňovým systémem tvoří detektor otevření MAS 303 umístěn na okně a vstupních dveřích, detektor pohybu Duální PIR + MX RK815DT-G3, detektor tříštění skla FG 1625TAS-G3, na stropě místnosti je nainstalován automatický požární hlásič SS2351KNL. Pro vstup do zabezpečené oblasti je

nainstalována bezkontaktní čtečka karet COTAG s PIN klávesnicí Asset 311 a pro odchod z místnosti bezkontaktní čtečka karet COTAG Asset 301. V místnosti je také instalován tísňový hlásič S3040/SROV typu 3. Pro nouzové opuštění prostoru bez použití bezkontaktní karty je vedle dveří umístěno bezpečnostní odchodové tlačítko s výstupem do PZTS, které rozbitím skla nouzově otevře bezpečnostní dveře. Instalace PZTS je typu 3. V zabezpečené oblasti je umístěno certifikované zařízení fyzického ničení nosičů informací JAWS S 4 typ 3. Narušení prostoru je signalizováno u ostrahy v budově B.

Elektrický zabezpečovací systém, který chrání objekt a zabezpečenou oblast, mohou obsluhovat pouze osoby, kterým byl protokolárně předán prostředek k jeho ovládnutí (kód, identifikační karta atd.). Vstupní prostředky mohou být přiděleny pouze osobám, které splňují požadavky přístupu k UI příslušného stupně utajení stanovené zákonem.

Povinností uživatele je zajišťovat pravidelné revizní kontroly, a to v periodách stanovených výrobcem, dodavatelem nebo servisní firmou, případně vždy, když dojde k poškození EZS, rozšíření EZS, výměně EZS apod. Údaje o provozu EZS se evidují v provozní knize EZS.

Pokyny pro používání prostředků elektrické požární signalizace (dále také „EPS“) jsou specifikovány v projektové dokumentaci, případně v instrukcích dodaných výrobcem, dodavatelem nebo servisní organizací. Veškerá manipulace s EPS musí být v souladu s podmínkami stanovenými příslušným HZS.

Povinností uživatele je zajišťovat pravidelné revizní kontroly, a to v periodách stanovených výrobcem, dodavatelem nebo servisní firmou, případně vždy, když dojde k poškození EPS.

Utajované informace příslušného stupně utajení lze skartovat pouze na skartovacím stroji, který je NBÚ certifikován pro stejný stupeň utajení jako příslušná UI nebo pro stupeň utajení vyšší. Při skartaci musí být dodržovány pokyny pro obsluhu skartovacího stroje, dle dokumentace výrobce.

Na skartovacím stroji se provádějí periodické revize ve stejných lhůtách jako revize přenosných elektrických spotřebičů.

Pravidelné funkční zkoušky jsou prováděny minimálně 1x za 12 měsíců v rámci ověřování, zda použítá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a platným právním předpisům.

Pravidla po manipulaci s klíči a identifikačními prostředky

Klíče od objektu, ZO a úschovných objektů jsou uloženy v zapečetěných schránkách (tubách) na klíče na stanovišti ostrahy. Schránky na klíče jsou označeny číslem, které se shoduje s číslem přiděleného ukládacího oddílu v rámci ukládacího místa, jménem a příjmením odpovědné osoby oprávněné výběrem, číslem pečeti. Klíče od ZO č. 1 kategorie Důvěrné (místnost č. 3), a ZO č. 2 kategorie Tajné (místnost č. 4), klíče od mříží a úschovných objektů jsou uloženy v režimových tubách (budova B, 1. NP, ZO kategorie Vyhrazené č. 1, místnost č. 2 – stanoviště stálé ostrahy) v schránce na klíče č. 1 a 2. a jsou opatřeny štítkem s údaji čísla místnosti a stupně utajení ZO. Tuby s klíči jsou vydávány oproti podpisu oprávněné osobě a zapsány do „Knihy výdeje tub od režimových pracovišť“.

Je zakázáno bez povolení bezpečnostního ředitele klíče od ZO vynášet z areálu společnosti a vytvářet jejich kopie.

V případě ztráty, vyrazení vstupních prostředků, či zjištění jiného porušení klíčového režimu jsou oprávněné osoby povinny zajistit odstranění závady a stanovení náhradního způsobu ochrany UI do doby přijetí nápravných opatření. Tuto skutečnost okamžitě hlásit bezpečnostnímu řediteli.

Duplikáty klíčů jsou uloženy u bezpečnostního ředitele v místnosti č. 5, budovy A.

Pravidla pro výkon ostrahy

Ostrahu objektu typu 3 zabezpečují zaměstnanci bezpečnostní agentury. Fyzická ostraha vykonává ostrahu objektů A, B, C, D a je zabezpečena 2 členou ostrahou 24 hodin. Stanoviště ostrahy je na budově č. B u vstupu do areálu a je umístěné od zabezpečené oblasti kategorie Důvěrné a Tajné nejméně do 500 m, aby zásah ostrahy byl proveden do 5 minut od přijetí poplašného nebo nouzového signálu z objektu, zabezpečené oblasti. Ostraha je vybavena při obchůzce prostředky umožňující spojení se stanovištěm pro stálý výkon ostrahy. Ostraha provádí pravidelné obchůzky v intervalu do 6 hodin. První obchůzka ostrahy se provádí ihned po ukončení pracovní doby. Ostraha je vybavena při obchůzkách prostředky umožňující spojení se stanovištěm pro stálý výkon ostrahy. V průběhu výkonu ostrahy, včetně doby obchůzek, je stanovišti stálé ostrahy neustále přítomna jedna osoba určená pro výkon ostrahy. Režim návštěv v objektu je dle vyhlášky č. 528/2005 Sb. v platném znění stanoven s doprovodem.

V. PLÁN ZABEZPEČENÍ OBJEKTU A ZABEZPEČENÝCH OBLASTÍ **V KRIZOVÝCH SITUACÍCH**

Popis opatření k minimalizaci hrozeb a zranitelnosti popsaných v kapitole IV.

V kapitole IV. byly popsány hrozby vnitřního a vnější prostředí, se kterými je možno se setkat při práci s utajovanými informacemi.

Pravidelné proškolení podřízených pracovníků v ochraně utajovaných informací vede k minimalizaci hrozeb a je organizováno ředitelem společnosti. Jednou za 12 měsíců je povinnost provést kontrolu dodržování všech povinností dodržování zákona 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Hrozba, že dojde k vyzrazení nebo zneužití UI je minimalizována souborem opatření fyzické, personální a administrativní bezpečnosti a to tak, aby každá osoba, která má přístup k utajované informaci, s ní mohla v objektu bez obav pracovat.

Každý pracovník, který zjistil porušení povinností při ochraně utajovaných informací, je podle zákona č. 412/2005 Sb. povinen neprodleně toto oznámit vedoucímu objektu, který zajistí ohlášení zjištěného skutku na NBÚ a přijme opatření k odstranění příčin a nepříznivých následků.

Pokyny pro ochranu utajovaných informací v případě vzniku mimořádné situace.

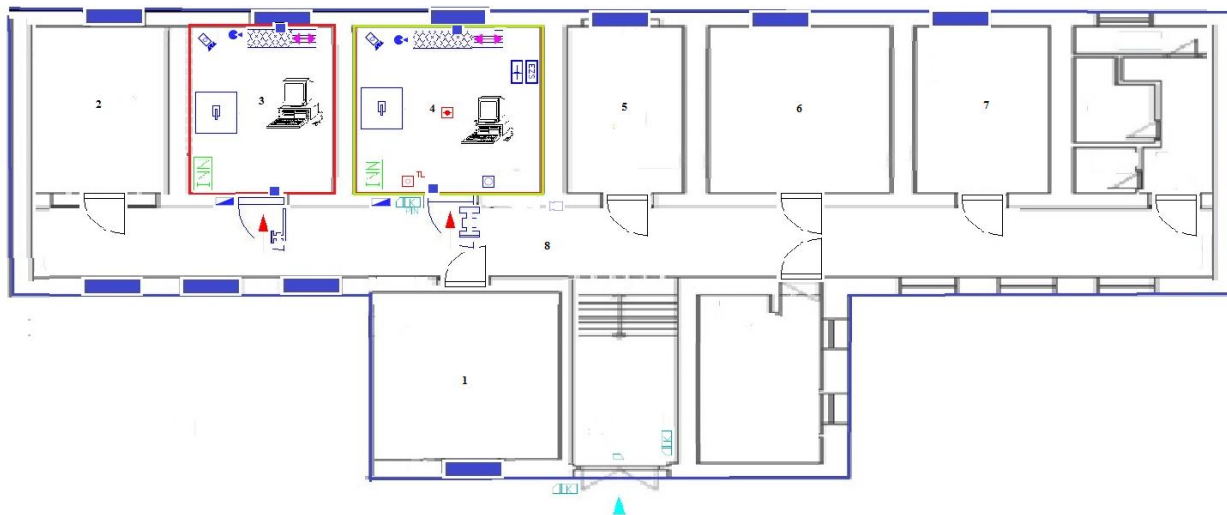
Mimořádnou situací, dle § 2 písm. i) vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, je stav, kdy bezprostředně hrozí, že dojde k vyzrazení nebo zneužití UI.

V případě vypuknutí požáru, v objektu nebo ZO je vyslán signál ústředně EZS, která začne signalizovat vznik nebezpečí a deaktivuje střežení ZO pro potřeby likvidace požáru. K této likvidaci musí být povolána pověřená osoba k zabezpečení a přemístění utajovaných informací do bezpečí. K přesunu těchto dokumentů určení pracovníci přistaví služební vozidlo před budovu A, naloží do něho evakuované utajované informace, které okamžitě přepraví do zabezpečené oblasti buď některého z útvarů Policie ČR nebo na NBÚ. K minimalizaci této hrozby jsou pracovníci jednou ročně proškoleni z protipožárních zásad a pověřený pracovník společnosti zpracovává Poplachové požární směrnice.

Tato opatření je potřeba udělat i v případě havárie vodovodních rozvodů nebo střešní konstrukce. Při vzniku jakékoli krizové situace anebo při vzniku mimořádné události neprodleně informovat ředitele společnosti, který rozhodne o dalších opatření.

Příloha č. 1 Projektů fyzické bezpečnosti

Výkresová dokumentace zabezpečených oblastí a schéma rozmístění technických prostředků



Obrázek č. 26 Vyznačení hranice objektu, hranice ZO a rozmístění technických prostředků D, T

LEGENDA

	- hranice objektu
	- hranice zabezpečené oblasti D
	- hranice zabezpečené oblasti T
	- ústředna ESZ
	- zdroj 230/12 V
	- záložní zdroj
	- linkový modul
	- klávesnice
	- magnetický kontakt
	- prostorový PIR/MW detektor
	- detektor tříštění skla
	- tísňový hlásič
	- opticko – kouřový detektor
	- požární tlačítko
	- siréna vnitřní
	- čtečka bezkontaktních karet COTAG
	- čtečka bezkontaktních karet s PIN klávesnicí
	- el. zámek

Příloha č. 2 Projektu fyzické bezpečnosti

Přehled použitých technických prostředků

TECHNICKÝ PROSTŘEDEK (výčet)	Počet	UMÍSTĚNÍ (ZO)	BODOVÉ OHODNOCENÍ/TYP/ IČ CERTIFIKÁTU
Úschovný objekt TLA 4	1	4	S1=6/typ 3/ certifikát T 0004/2013
Úschovný objekt TLA 6	1	3	S1=6/typ 3/ certifikát T 0004/2013
Mříže Typ Nůžková mříž dvoukřídlová 99	1	3	S2=4/typ 2/ certifikát T0025/2010
Mříže Typ Nůžková mříž dvoukřídlová NMK3-T	1	4	S2=6/typ 3/ certifikát T0024/2010
Dveře Typ: BEDEX VARIO V 3 s požární odolností se zárubní MRB	1	4	S2=6/typ 3/ certifikát T0093/2010
Typ: BEDEX VARIO V 3 s požární odolností se zárubní MRB	1	3	S2=6/typ 3/ certifikát T0093/2010
Uzamykací systém Zadlabávací elektromechanický zámek ABLOY BEF 022421	1	4	SS4= 3/typ 3/ certifikát T 0075/2013
Uzamykací systém Typ: bezpečnostní kování R1 cylindrická vložka MULT-T-LOCK	1	3	SS4=2/typ2/ certifikát T0081/2010 certifikát T0022/2010
Zařízení fyzického ničení nosičů informací Typ JAWS S4 (řez 2x12mm)	1	3	bez bodového hodnocení/typ 3/ certifikát T 5012 /2008
Zařízení fyzického ničení nosičů informací Typ INTIMUS 45CC4 (řez 1,9x15mm)	1	3	bez bodového hodnocení/typ 3/ certifikát T 5012 /2008
Dveře (výstupní, vnitřní)		Budova A	typ 0
Okna		3,4	typ 0

TECHNICKÝ PROSTŘEDEK (výčet)	Počet	UMÍSTĚNÍ (ZO)	BODOVÉ OHODNOCENÍ/TYP/ IČ CERTIFIKÁTU
Systém kontroly vstupu Asset 804	1	budova B stanoviště ostahy	SS6=2/typ 2/ certifikát T 3001/2013
Systém kontroly vstupu Bezkontaktní čtečka Asset 301	1	Budova A vstup	SS6=2/typ 2/ certifikát T 3001/2013
Systém kontroly vstupu Bezkontaktní čtečka Asset 311	2	3,4	SS6=2/typ 2/ certifikát T 3001/2013
Detektor otevření MAS 303	4	3,4	SS91=3/typ 3/ certifikát T 1017/2014
Detektor pohybu Duální PIR+MW RK815DT-G3	2	3,4	SS91=3/typ 3/ certifikát T1008/2013
Detektor tříštění skla FG 1625TAS-G3	2	3,4	SS91=3/typ 3/ certifikát T1050/2013
Tlačítkový tísňový hlásič S3040/SR	1	4	SS91=3/typ 3/ certifikát T1114/2012
Automatický požární hlásič SS2351KNL	1	4	Bez certifikátu
Vnitřní nezálohovaná siréna SA 913F	1	chodba č. 8	Bez certifikátu

Tabulka č. 6 Přehled použitých technických prostředků D,T

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Pošt. příhr. 49
150 06 Praha 56

Národní bezpečnostní úřad vydává podle § 46 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

CERTIFIKÁT

technického prostředku

Evidenční číslo: T0030/2015

Bezpečnostní dveře BEDEX VARIO EL VD3

Bezpečnostní dveře BEDEX VARIO EL VD3 s protipožární odolností EI 30D1

(Název a typové označení technického prostředku)

Výrobce: MRB Sazovice, spol. s r.o.

Sídlo: Sazovice 191
763 01 Mysločovice

IČ:
63488051

Držitel: MRB Sazovice, spol. s r.o.

Sídlo: Sazovice 191
763 01 Mysločovice

IČ:
63488051

Tento certifikát potvrzuje ověření způsobilosti technického prostředku typu:

3

Bodové hodnocení technického prostředku podle přílohy č. 1 vyhlášky č. 528/2005 Sb.,
o fyzické bezpečnosti a certifikaci technických prostředků:

SS3=3, SS4=2

Platnost certifikátu do 20.4.2018

Datum vydání certifikátu: 27.4.2015

Náměstek ředitele
Národního bezpečnostního úřadu



Mgr. Marek Šimandl, MPA
014361

Přílohy 1/1

(Příloha je nedílnou součástí certifikátu a lze je reprodukovat pouze společně)

Obrázek č. 27 Certifikát technického prostředku⁵⁹

⁵⁹ <http://www.dverebdex.cz/certifikaty/certifikaty-vydane-nbu>

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Pošt. příhr. 49
150 06 Praha 56

Národní bezpečnostní úřad vydává podle § 46 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

PŘÍLOHU K CERTIFIKÁTU

Identifikační číslo: **T0030/2015**

Příloha číslo: **1**

Bezpečnostní dveře BEDEX VARIO EL VD3, Bezpečnostní dveře BEDEX VARIO EL VD3 s protipožární odolností EI 30D1 se záruční MRB, otevírané směrem do chráněného prostoru nebo ven z chráněného prostoru, provedení pravé a levé, šířky 700 mm až 1000 mm, výšky 1970 mm až 2200 mm. Přehled komponent, kterými je možno certifikovaný výrobek osazovat je uveden v příloze certifikačního protokolu C 87/2015, vydaného certifikačním orgánem č. 3025 společností TREZOR TEST s.r.o. Tento přehled je k dispozici u držitele certifikátu. Výrobek je vyráběn v režimu akreditované certifikace od 20. 4. 2015.

Platnost certifikátu do: 20.4.2018

Datum vydání certifikátu: 27.4.2015

Otisk úředního razítka



Náměstek ředitele
Národního bezpečnostního úřadu

(Handwritten signature)
Mgr. Marek Šimandl MPA

Certifikát a přílohu lze reprodukovat pouze společně.

Obrázek č. 28 Příloha certifikátu technického prostředku⁶⁰

⁶⁰ <http://www.dverebedex.cz/certifikaty/certifikaty-vydane-nbu>