

Komplexní návrh zabezpečení objektu, ve kterém dochází ke styku s utajovanými informacemi

Comprehensive Design of the Object Coming into Contact with Confidential Information

Bc. Josef Novák



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Josef NOVÁK**
Osobní číslo: **A09384**
Studijní program: **N 3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Komplexní návrh zabezpečení objektu, ve kterém dochází ke styku s utajovanými informacemi.**

Zásady pro vypracování:

1. Seznamte se s platnou legislativou s důrazem na vyhlášku č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.
2. Vypracujte literární rešerši zaměřenou na zabezpečení objektů mechanickými a elektrickými zábrannými systémy.
3. Navrhněte způsob zabezpečení daného objektu.
4. Navrhněte certifikované prvky pro zabezpečovací systém.
5. Vypracujte ucelený návrh systému včetně popisu projektu, výkresové dokumentace, blokových schémat zapojení, rozpočtu a rozpisu prvků.
6. Posuďte ekonomickou náročnost navrženého zabezpečovacího systému.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: tištěná/elektronická

Seznam odborné literatury:

1. KINDL, J.: Projektování bezpečnostních systémů I. Zlín : Univerzita Tomáše Bati, 2007. ISBN:978-80-7318-554-1.
2. Národní bezpečnostní úřad [online]. 2008 [cit. 2011-02-04]. Ochrana utajovaných informací. Dostupné z WWW: www.nbu.cz.
3. KŘEČEK, S.: Příručka zabezpečovací techniky, Cricetus, 2006. ISBN:80-902938-2-4.
4. Skupina norem ČSN EN 50 130, 50 131, 50 132, 50 133, ČSN EN 54.
5. BASTIAN, P.: Praktická elektrotechnika. Europa Sobotáles, Brno, 2004. ISBN 808670615X.

Vedoucí diplomové práce:

doc. Mgr. Milan Adámek, Ph.D.
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

25. února 2011

Termín odevzdání diplomové práce:

27. května 2011

Ve Zlíně dne 25. února 2011

prof. Ing. Vladimír Vašek, CSc.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce má čtenářům poskytnout ucelený obraz o ochraně utajovaných informací, především se však zabývá jejich fyzickou ochranou. Úkolem je navrhnout komplexní systém technického zabezpečení podle požadavků NBÚ.

Klíčová slova: Národní bezpečnostní úřad, utajovaná informace, stupeň utajení, fyzická bezpečnost, technické prostředky, zabezpečená a jednací oblast, návrh zabezpečení, poplachový zabezpečovací a tísňový systém

ABSTRACT

This thesis has provided readers with a comprehensive picture of the protection of classified information, but primarily concerned with their physical protection. The challenge is to design a comprehensive system of technical support as required by the NSA.

Keywords: National security agency, classified information, classification, physical security, technical resources, secure and meeting area, security design, security and emergency alarm system

Touto cestou chci vyjádřit poděkování vedoucímu diplomové práce doc. Mgr. Milanu Adámkovi, Ph.D. za jeho odborné vedení, dále bych rád poděkoval Ing. Petru Kováčovi za informace a čas, který mi věnoval při vypracování mé diplomové práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD.....	10
I TEORETICKÁ ČÁST.....	11
1 POJEM UTAJOVANÁ INFORMACE.....	12
1.1 UTAJOVANÉ INFORMACE V PRÁVNÍM ŘÁDU ČR	12
1.2 CHARAKTERISTIKA UTAJOVANÉ INFORMACE.....	12
1.3 KLASIFIKACE UTAJOVANÝCH INFORMACÍ.....	13
1.4 PROSTŘEDKY OCHRANY UTAJOVANÝCH INFORMACÍ	14
1.4.1 Personální bezpečnost	14
1.4.2 Průmyslová bezpečnost	15
1.4.3 Administrativní bezpečnost.....	15
1.4.4 Fyzická bezpečnost	16
1.4.5 Bezpečnost informačních a komunikačních systémů	16
1.4.6 Kryptografická ochrana.....	16
2 FYZICKÁ BEZPEČNOST.....	17
2.1 OPATŘENÍ FYZICKÉ BEZPEČNOSTI.....	17
2.1.1 Ostraha	18
2.1.2 Režimová opatření	18
2.1.3 Technické prostředky	18
2.2 PROJEKT FYZICKÉ BEZPEČNOSTI.....	19
3 STRUKTURA PROJEKTU FYZICKÉ BEZPEČNOSTI	20
3.1 VYHODNOCENÍ RIZIK.....	20
3.1.1 Specifikace aktiv	20
3.1.2 Stanovení hrozeb	20
3.1.3 Stanovení zranitelností a jejich vyhodnocení.....	21
3.1.3.1 Výběr identifikovaných a ohodnocených hrozeb	22
3.1.3.2 Výběr zranitelných míst objektu a chráněného prostoru	23
3.1.3.3 Sestavení matice hodnocení zranitelnosti	23
3.1.4 Stanovení míry rizika	24
3.2 URČENÍ OBJEKTU, ZABEZPEČENÝCH OBLASTÍ A JEDNACÍCH OBLASTÍ	25
3.3 ZABEZPEČENÍ ZABEZPEČENÉ OBLASTI	26
3.4 ZABEZPEČENÍ JEDNACÍCH OBLASTÍ.....	27
3.5 ZABEZPEČENÍ TECHNICKÉHO ZAŘÍZENÍ	28
3.6 ZABEZPEČENÍ FYZICKOU OSTRAHOU A REŽIMOVÝMI OPATŘENÍMI	29
3.6.1 Fyzická ostraha zabezpečené oblasti a jednacích oblastí.....	29
3.6.2 Fyzická ostraha technického zařízení.....	29
3.6.3 Zabezpečení režimovým opatřením	30
3.7 BODOVÉ HODNOCENÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI	30
3.7.1 Minimální požadované hodnoty míry zabezpečení.....	30
3.8 TECHNICKÁ DOKUMENTACE FYZICKÉ BEZPEČNOSTI.....	31
4 ZÁKLADNÍ POKYNY PŘI NÁVRHU BEZPEČNOSTNÍHO SYSTÉMU.....	32

4.1	ZADÁNÍ PROJEKTU.....	32
4.2	IDENTIFIKACE NEBEZPEČÍ.....	32
4.3	STUPEŇ ZABEZPEČENÍ	33
4.4	TŘÍDA PROSTŘEDÍ.....	34
4.5	VOLBA KOMPONENTŮ A JEJICH UMÍSTĚNÍ.....	34
II	PRAKTICKÁ ČÁST	36
5	PROJEKT ZABEZPEČENÍ OBJEKTU	37
5.1	STRUČNÝ POPIS OBJEKTU	37
6	BEZPEČNOSTNÍ POSOUZENÍ OBJEKTU	38
6.1	STANOVENÍ METODY ANALÝZY RIZIK.....	38
6.2	IDENTIFIKACE AKTIV A STUPNĚ UTAJOVANÝCH INFORMACÍ	38
6.3	URČENÍ VELIKOSTI ÚJMY	39
6.4	ANALÝZA BEZPEČNOSTNÍHO PROSTŘEDÍ	39
6.5	VYHODNOCENÍ ZRANITELNOSTI OBJEKTU	40
6.6	BODOVÉ HODNOCENÍ BEZPEČNOSTI.....	41
7	URČENÍ ZABEZPEČENÝCH A JEDNACÍCH OBLASTÍ.....	42
7.1	STANOVENÍ OBJEKTU, JEHO TYPU A HRANIC.....	42
7.2	STANOVENÍ ZABEZPEČENÝCH OBLASTÍ, JEJICH HRANIC, TYP, KATEGORIE, TŘÍDY	42
7.3	STANOVENÍ JEDNACÍCH OBLASTÍ	43
7.4	PŮVODNÍ ZABEZPEČENÍ	43
8	NÁVRH ZABEZPEČENÍ.....	44
8.1	POPLACHOVÝ ZABEZPEČOVACÍ A TÍŠŇOVÝ SYSTÉM	44
8.1.1	Stupeň zabezpečení a rozsah střežení.....	44
8.1.2	Třída okolního prostředí.....	44
8.1.3	Použité prostředky	44
8.1.4	Ústředna PZTS	45
8.1.5	Detektory	46
8.1.5.1	Prostorová ochrana	46
8.1.5.2	Plášťová ochrana.....	48
8.1.5.3	Sabotážní ochrana	49
8.1.6	Tísňový systém.....	49
8.1.7	Ovládání systému	49
8.1.8	Ohlašování poplachu a komunikace.....	50
8.1.9	Způsob vedení tras kabeláže	51
8.1.10	Napájení a zálohování napájení	51
8.1.11	Nastavení systému.....	54
8.2	INTEGROVANÝ PŘÍSTUPOVÝ SYSTÉM	56
8.2.1	Přístupový modul	56
8.2.2	Čtecí zařízení a přístupová karta	57
8.2.3	Dveřní kontakt a elektromechanický zámek	58
8.2.4	Nastavení přístupu.....	59
8.3	ELEKTRICKÁ POŽÁRNÍ SIGNALIZACE	60
8.3.1	Ústředna EPS	60
8.3.2	Způsob detekce požáru.....	61

8.3.3	Signalizace poplachu	62
8.3.4	Vedení kabeláže	62
8.3.5	Napájení a zálohování napájení	62
8.4	MECHANICKÉ ZÁBRANNÉ SYSTÉMY	63
8.4.1	Zabezpečená oblast kategorie Důvěrné.....	63
8.4.2	Zabezpečená oblast Tajné	64
8.4.3	Zabezpečení jednací oblasti Tajné	65
8.5	TECHNICKÁ OCHRANA PROTI AKTIVNÍMU A PASIVNÍMU ODPOSLECHU	65
8.6	ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ	66
8.7	BODOVÉ POROVNÁNÍ REALIZOVANÉHO A POŽADOVANÉHO ZABEZPEČENÍ.....	67
8.8	SOUPISKA POUŽITÝCH PRVKŮ.....	67
ZÁVĚR		68
ZÁVĚR V ANGLIČTINĚ.....		69
SEZNAM POUŽITÉ LITERATURY.....		70
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....		72
SEZNAM OBRÁZKŮ		74
SEZNAM TABULEK.....		75
SEZNAM ROVNIC		77
SEZNAM PŘÍLOH.....		78

ÚVOD

Problematika ochrany utajovaných informací je ve své podstatě a širším slova smyslu problematikou ochrany informací vůbec. Informace dnes představují pro řadu firem a státních institucí hodnoty, jejichž ohrožení nebo ztráta mohou být pro tyto subjekty fatální.

V rámci diplomové práce se v první kapitole teoretické části zabývám samotným pojmem utajované informace a její začlenění do legislativy České republiky. V dalších částech této kapitoly popisují prostředky ochrany utajovaných informací. Samostatnou kapitolou je ovšem fyzická bezpečnost ochrany utajovaných informací, která je prakticky páteří celé této diplomové práce. Tato kapitola se zabývá ochranou objektů, ve kterých dochází ke styku s utajovanými informacemi. Protože je fyzická bezpečnost sama o sobě velmi rozsáhlá, je největší pozornost věnována technickým prostředkům ochrany utajovaných informací a jejich projektování.

Cílem práce je vytvořit komplexní zabezpečení objektu, které bude respektovat požadavky Národního bezpečnostního úřadu podle vyhlášky č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků.

I. TEORETICKÁ ČÁST

1 POJEM UTAJOVANÁ INFORMACE

Informaci považujeme za utajovanou, pokud přístup k ní je jakýmkoli způsobem omezený. Přesněji řečeno, vůle a zájem držitele určité informace rozhoduje o tom, zda informace má být utajena a komu a za jakých podmínek bude zpřístupněna. Smysl utajování je jednoduchý: znalost utajované informace, představuje pro oprávněnou osobu výhodu, která ji umožňuje získat náskok vůči jiným osobám, skupinám nebo institucím. Jsou to informace běžně nepřístupné širokému okolí. [1]

1.1 Utajované informace v právním řádu ČR

V současné době je platná právní úprava utajovaných informací obsažena v zákonech, nařízeních vlády a prováděcích vyhláškách NBÚ. Samotný pojem utajované informace (dále UI) je specifický a je definován zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. § 1 tohoto zákona upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a požadavky na jejich ochranu.

1.2 Charakteristika utajované informace

Podle právního řádu České republiky se UI specifikuje třemi základními znaky:

- a) **Utajení** – tzn. omezenou možností přístupu k UI, dosahované pomocí zvláštního režimu, jehož záměr je omezit znalost o obsahu této informace na určený okruh fyzických osob. Režim utajení, je soubor pravidel, činností a opatření s cílem maximálně zajistit, aby s UI nepřišla do styku nepovolaná osoba a aby s informací nebylo nakládáno způsobem, který je nepřijatelný. Rudolf Musil ve své knize Ochrana utajovaných skutečností¹ říká:

„Utajování je specifický systém ochrany utajované skutečnosti, který zajišťuje současně:

¹ Rudolf Musil používá ve své knize výraz ochrana utajovaných skutečností, podle zákona č. 412/2005 Sb., je slovo skutečnost nahrazeno slovem informace.

- *důvěrnost utajované skutečnosti, tzn., že neoprávněná (neautorizovaná) osoba se s utajovanými skutečnostmi nejen neseznámí, ale ani k ní nepronikne, aby mohla s utajovanou skutečností neoprávněně nakládat jiným způsobem,*
- *integritu utajované skutečnosti, která znamená, že utajovaná skutečnost nemůže být neoprávněnou osobou jakkoliv modifikována (změněna, poškozena či zničena) a*
- *dostupnost utajované skutečnosti, tzn., že zajišťuje i rychlý a úplný přístup k utajované skutečnosti pro oprávněné osoby. “ [1]*

b) **Újma** – v případě neoprávněného nakládání s UI vzniká možnost újmy. Podle hrozby vzniku újmy se jednotlivé utajované informace hodnotí na příslušné stupně. Podle §3 zákona o ochraně utajovaných informací se újmou zájmu České republiky rozumí poškození nebo ohrožení zájmu ČR. Podle závažnosti poškození nebo ohrožení se újma člení na mimořádně vážnou újmu, vážnou újmu, prostou újmu a nevýhodné pro zájmy ČR. Jako újmu zájmu ČR lze považovat oblasti politické (zachování ústavnosti, svrchovanosti a územní celistvosti), obrany státu, veřejné bezpečnosti, ekonomických zájmů, práv a svobod fyzických a právnických osob, ochrana zdraví a života fyzických osob.

c) **Sankce** – vzniká jako negativní následek při porušení zákona a souvisejících předpisů v souvislosti s utajovanými informacemi. Hrozba sankcí představuje prostředek, jakým stát prosazuje svůj zájem na ochraně UI a na dodržování stanovených pravidel. Sankce mají několik podob, od majetkových až po omezení osobní svobody fyzické osoby. [1]

1.3 Klasifikace utajovaných informací

Vyjadřuje význam chráněného zájmu prostřednictvím klasifikace UI do jednotlivých stupňů utajení. Každá utajovaná informace musí být označena příslušným stupněm utajení a tento stupeň musí být stanoven správně. Stupeň utajení utajované informace se stanoví podle významu chráněného zájmu, závažnosti obsahu utajované informace a s využitím seznamu utajovaných informací. Seznam oblastí utajovaných informací a jejich stupeň utajení je definován v nařízení vlády č. 522/2005 Sb.

§ 4 zákona č. 412/2005 Sb. určuje 4 stupně utajení:

- a) stupeň utajení „**Přísně tajné**“ – vyzrazení UI neoprávněné osobě nebo její zneužití může způsobit mimořádně vážnou újmu zájmům České republiky. Je nejvyšším stupněm utajení.
- b) stupeň utajení „**Tajné**“ – je o stupeň nižší utajení, její vyzrazení neoprávněné osobě by mohlo způsobit vážnou újmu zájmům ČR.
- c) stupeň utajení „**Důvěrné**“ – je druhý nejnižší stupeň utajení UI. Vyzrazení nebo zneužití informace neoprávněnou osobou by mohl mít za následek prostou újmu na zájmu ČR.
- d) stupeň utajení „**Vyhrazené**“ – je nejnižším stupněm utajení a její vyzrazení by mohlo být nevýhodné pro zájmy České republiky. [2]

1.4 Prostředky ochrany utajovaných informací

Prostředky ochrany utajovaných informací jsou ze zákona definovány jako systém opatření, jejichž účelem je zajistit ochranu UI buď určitým způsobem (technické prostředky), nebo před určitou nežádoucí situací (seznámení nepovolané osoby s UI) a při jejich zpracování a evidenci a nakládání s UI v určitém prostředí.

Základním a primárním cílem prostředků ochrany utajovaných informací je ochránit je před neoprávněným nakládáním. Jednotlivé oblasti prostředků ochrany UI jsou zaměřeny na specifické systémy opatření.

1.4.1 Personální bezpečnost

Personální bezpečnost je základním druhem prostředků ochrany utajovaných informací. Hlavním cílem personální bezpečnosti je, aby se s UI seznamovala pouze fyzická osoba, která je bezpodmínečně potřebuje pro výkon své činnosti. Kromě ověřování podmínek, které musí fyzická osoba splnit, aby jí byl umožněn přístup k utajované informaci, zahrnuje personální bezpečnost i výchovu těchto osob. Za pro školení fyzických osob, které mají přístup k UI, je určena odpovědná osoba. Ta je povinna jednou ročně zajistit u osob, které mají přístup k utajované informaci, proškolení z právních předpisů v oblasti ochrany UI.

Podmínky přístupu k utajované informaci se liší podle stupně utajení, k níž má mít fyzická osoba přístup. Pro stupeň utajení „Vyhrazené“ ověřuje podmínky přístupu odpovědná osoba nebo Národní bezpečnostní úřad. Pro vyšší stupeň utajení se splnění podmínek ověřuje v bezpečnostním řízení. [1]

1.4.2 Průmyslová bezpečnost

Stanovuje podmínky přístupu podnikatele k utajované informaci a formy přístupu podnikatele k utajované informaci.

„Na základě ustanovení § 15 zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti ve znění pozdějších předpisů lze podnikateli umožnit přístup k utajované informaci, jestliže jej nezbytně potřebuje k výkonu své činnosti a je držitelem platného osvědčení podnikatele podle § 54 zákona příslušného stupně utajení, pokud zákon nestanoví jinak.“ [3]

Podle způsobu, jakým bude podnikatel přistupovat k UI, mohou nastat dvě varianty přístupu k utajované informaci. Tyto formy přístupu jsou definovány v § 20 odst. 1, zákona o ochraně UI. Podnikatel má podle tohoto ustanovení přístup k utajované informaci:

- a) která u něho vzniká nebo je mu poskytnuta,
- b) která u něho nevzniká, ani mu není poskytována, ale ke které mají přístup zaměstnanci podnikatele nebo osoby jednající jménem podnikatele nebo za podnikatele, a to v souvislosti s výkonem pracovní nebo jiné činnosti pro podnikatele na základě smlouvy. [2]

1.4.3 Administrativní bezpečnost

Pravidla administrativní bezpečnosti jsou uvedena v § 21 až 23 zákona č. 412/2005 Sb. a ve vyhlášce č. 529/2005 Sb.

Primárním cílem administrativní bezpečnosti je ochrana UI při jejich tvorbě, příjmu, evidenci, zpracování, přepravě, ukládání, vyřazování, skartaci, archivaci a jiné manipulaci. Vyhláška řeší způsob stanovení příslušného stupně utajení, jeho změny, zrušení a vyznačení na utajovaných písemnostech. Současně se zabývá zavedením administrativních pomůcek a manipulací s utajovanou písemností.

1.4.4 Fyzická bezpečnost

Je tvořena souborem opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat. Fyzickou bezpečností se budu podrobněji zabývat v samostatné kapitole.

1.4.5 Bezpečnost informačních a komunikačních systémů

Bezpečnost IS v oblasti ochrany utajovaných informací má stále větší význam a je přímo úměrná nárůstu významu informačních a komunikačních technologií. Bezpečnost informačních a komunikačních systémů je rozpracována ve vyhlášce č. 523/2005 Sb. Tato vyhláška se zabývá požadavky na IS a podmínkami jeho bezpečného provozování v závislosti na stupni utajení utajovaných informací, s nimiž nakládá, a na bezpečnostním provozním módu. Součástí vyhlášky je obsah bezpečnostní dokumentace informačního systému.

1.4.6 Kryptografická ochrana

Kryptografická ochrana je rozpracována ve vyhlášce č. 524/2005 Sb., o zajištění kryptografické ochrany UI a vyhláškou č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany UI.

Za kryptografickou ochranu se považuje systém opatření k ochraně utajovaných informací pomocí kryptografických metod při zpracování, přenosu, ukládání a archivaci UI ve výpočetních a informačních systémech. Zákon v rámci kryptografické ochrany jednoznačně požaduje odborně způsobilé pracovníky pro specializovanou činnost a kryptografické prostředky certifikované NBÚ.

2 FYZICKÁ BEZPEČNOST

Fyzická bezpečnost ochrany utajovaných informací se zabývá otázkou ochrany objektů, ve kterých dochází ke styku s utajovanými informacemi, jejich vznikem a uchováváním. V rámci fyzické bezpečnosti se řeší, jaké prostředky budou k ochraně UI použity, jejich přibližný rozsah, způsob a podmínky použití. Instituce se musí rozhodnout, zda budou utajované informace zpracovávány a uchovávány v jednom nebo několika objektech, musí zvolit vhodný rozsah zabezpečení a určit jestli bude k ochraně objektu využito fyzické ostrahy a jestli tuto ostrahu provede soukromá bezpečnostní služba nebo bude zajištěna z vlastních zdrojů. Podrobnosti pak instituce rozpracuje v projektu fyzické bezpečnosti.

Cílem fyzické bezpečnosti ochrany utajovaných informací je stanovit opatření a pravidla, aby nedošlo k neoprávněnému nakládání s UI. V rámci fyzické bezpečnosti je nutné si položit několik základních otázek, především jakým způsobem bude provedeno nasazení konkrétních technických prostředků a na kterých místech v organizaci se budou UI vyskytovat. Výsledkem je pak určení hranic objektu a jeho zařazení do příslušné kategorie, určení zabezpečené oblasti a její zařazení do příslušné kategorie a třídy.

§24 zákona č. 412/2005 Sb., definuje základní pojmy objekt, zabezpečenou oblast a jednací oblast. Za objekt je považována budova nebo jiný ohraničený prostor, ve kterém se nachází zabezpečená oblast nebo jednací oblast. Zabezpečenou oblastí je ohraničený prostor v objektu, kterému je přiřazena kategorie podle stupně utajení UI, která se v ní nachází. Jedací oblastí je ohraničený prostor v objektu, kde dochází k projednávání UI stupně utajení Přísně tajné nebo Tajné.

Realizace stanovených opatření je popsána v projektu fyzické bezpečnosti, který je zpracovaný podle specifikace uvedené v příloze č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.

2.1 Opatření fyzické bezpečnosti

Jsou účinná opatření k ochraně objektů, ve kterých se vyskytují utajované informace. V §27 zákona č. 412/2005 Sb., je stanoveno, že ochrana objektu se provádí kombinovaným využitím bezpečnostních opatření, kterými jsou fyzická ostraha objektu, režimová opatření a technické prostředky.

2.1.1 Ostraha

Představuje v souvislosti s ochranou utajovaných informací přímé nasazení lidské síly v určitém režimu před neoprávněným nakládáním nepovolané osoby s UI. Činnost fyzické ostrahy při ochraně utajovaných informací je zaměřena na kontrolu osob a dopravních prostředků, které do objektu vstupují nebo jej opouštějí. Ostraha by měla věnovat i pozornost provozu uvnitř objektu a kontrolovat, zda pohyb osob a dopravních prostředků odpovídá režimovým opatřením. Organizace, ve které dochází ke styku s UI, musí rozhodnout, zda bude ostraha zajištěna zaměstnanci organizace nebo externí bezpečnostní službou. [1]

2.1.2 Režimová opatření

§29 zákona č. 412/2005 Sb.: „*Režimová opatření stanoví oprávnění osob a dopravních prostředků pro vstup a vjezd do objektu, oprávnění osob pro vstup do zabezpečené oblasti a jednacích oblastí a způsob kontroly těchto oprávnění a dále způsob manipulace s klíči a identifikačními prostředky, které se používají pro systém zabezpečení vstupů podle §30 odst. 1 písm. b), a způsob manipulace s technickými prostředky a jejich používání. Režimová opatření stanoví též oprávnění při výstupu osob a výjezdu dopravních prostředků z objektu a pro jejich kontrolu, podmínky a způsob kontroly pohybu osob v objektu, zabezpečené oblasti a jednacích oblastí a způsob kontroly a vynášení utajovaných informací z objektu, zabezpečené oblasti a jednacích oblastí.*“ [2]

2.1.3 Technické prostředky

Technickými prostředky se rozumí praktické využití elektronických a mechanických systémů určených k ochraně utajovaných informací nebo nakládání s nimi pomocí výpočetní techniky a informačních systémů. Při návrhu technických prostředků bezpečnosti UI platí pravidlo, že úroveň a účinnost celého systému zabezpečení je totožná s úrovní a účinností nejslabšího článku systému.

Podle použití se technické prostředky zabezpečení dělí podle různých hledisek, např. podle technického principu, na kterém jsou založeny, podle předmětu, který mají chránit a podle nebezpečí nebo rizika, kterému jsou vystaveny.

2.2 Projekt fyzické bezpečnosti

Projekt fyzické bezpečnosti je vypracováván v rámci bezpečnostního projektu organizace. Zabývá se touto stránkou bezpečnostního projektu organizace, která je zaměřena na ochranu objektů, v nichž se v organizaci nakládá s utajovanými informacemi.

Projektem fyzické bezpečnosti se podrobně zabývá §32 zákona č. 412/2005 Sb., který chápe projekt fyzické bezpečnosti jako dokument, který obsahuje:

- a) umístění zabezpečených oblastí v objektu včetně jejich hranic,
- b) určení kategorií a tříd zabezpečených oblastí,
- c) hodnocení rizik,
- d) způsob použití opatření fyzické bezpečnosti,
- e) provozní řád objektu,
- f) plán zabezpečení objektu a zabezpečených oblastí v krizových situacích. [2]

Struktura projektu fyzické bezpečnosti se liší podle stupně zabezpečení zabezpečené oblasti a jednacích oblastí.

3 STRUKTURA PROJEKTU FYZICKÉ BEZPEČNOSTI

Představuje vlastní zpracování projektu fyzické bezpečnosti dle §32 zákona č. 412/2005 Sb. Při zpracování projektu je závazným předpisem vyhláška č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb., včetně přílohy č. 1 a č. 2 ve znění pozdějších předpisů. [4]

3.1 Vyhodnocení rizik

Úvodní činností před zpracováním bezpečnostního projektu fyzické bezpečnosti je vyhodnocení rizik. Tento dokument neobsahuje režimová opatření, pouze je hodnotí a je-li to třeba, navrhuje další režimová opatření a ostatní prostředky ochrany. Vyhodnocení rizik nemá všeobecně platnou strukturu. Zpracovává se písemně, protože je vyžadováno jako součást dokumentace fyzické bezpečnosti. Dokument vyhodnocení rizik je rozdělen do čtyř kroků.

3.1.1 Specifikace aktiv

V tomto kroku se definují pro organizaci všechna kritická aktiva společně s množstvím utajovaných informací podle stupně utajení, které se v objektu vyskytují nebo budou vyskytovat. [6]

3.1.2 Stanovení hrozeb

Pod pojmem hrozba rozumíme označení konkrétního, fyzicky existujícího subjektu, jevu, okolnosti nebo události s potenciálem způsobit ujmu (škodu, ztrátu), jako důsledek neoprávněného nakládání s utajovanou informací.

Proces stanovení hrozby spočívá v odhalení možných negativních událostí a jevů existujících v různých podobách v bezpečnostním prostředí, které mohou přivodit ohrožení UI. Cílem identifikace hrozeb je:

- a) identifikace zdrojů ohrožení ve vztahu k ochraně utajovaných informací,
- b) zjištění příčin ohrožení,
- c) analýza výskytů hrozeb v minulosti,
- d) stanovení velikosti každé identifikované hrozby.

Základním obsahem identifikace a hodnocení hrozeb je:

- a) **zpracování informací o vnějším a vnitřním bezpečnostním prostředí**, jejichž cílem je zajistit věrohodné, aktuální a relevantní informace o situaci a stavu ve vnějším a vnitřním bezpečnostním prostředí, potřebné pro identifikování relevantních ohrožení.
- b) **vypracování soupisu hrozeb**, které mohou mít vztah k fyzické bezpečnosti chráněného prostoru. Jak by mohl vypadat příklad možného soupisu hrozeb je uvedeno v příloze č. 1 této práce.
- c) **ohodnocení velikosti ohrožení**. Cílem hodnocení jednotlivých hrozeb utajovaných informací je přiřazení číselné hodnoty nebo slovního ohodnocení ke každé identifikované hrozbě, kterou je možné přiřadit k danému objektu nebo chráněnému prostoru. K hodnocení hrozeb je použita kvalitativní metoda, stanovující velikost ohrožení ze vzájemných vztahů **zdroj, motivace, záměr útočníka** nebo **příčina** (v souvislosti s živelnými pohromami) a **výskyt případů** v minulosti.

Existuje zdroj ohrožení?	Je známa motivace, záměr útočníka nebo příčina?	Existuje případ výskytu z minulosti?	Hodnocení ohrožení
Ano	Ano	Ano	Velké (V)
Ano	Ano	Ne	Velké (V)
Ano	Nedá se s určitostí stanovit	Ne	Střední (S)
Ano	Ne	Ne	Malé (M)
Nedá se s určitostí definovat	Ne	Ne	Malé (M)
Nedá se s určitostí definovat	Nedá se s určitostí stanovit	Ne	Malé (M)
Nedá se s určitostí definovat	Ne	Ne	Ohrožení není (0)

Tabulka 1. Postup hodnocení ohrožení

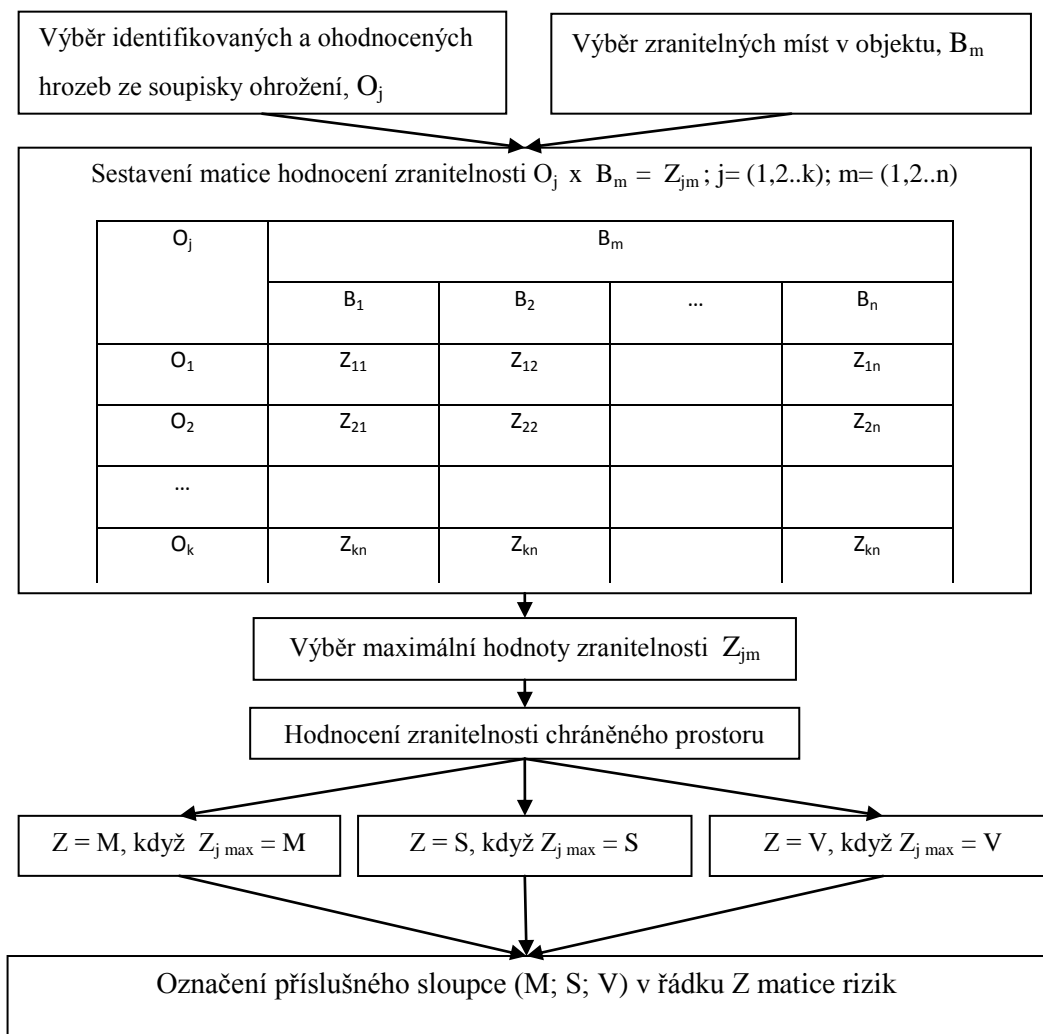
Po ohodnocení jednotlivých hrozeb se stanoví velikost celkového ohrožení UI. Při stanovení celkového ohrožení UI se uplatní princip, že celková velikost ohrožení se určí podle velikosti toho ohrožení, která má nejvyšší hodnotu. [7]

3.1.3 Stanovení zranitelností a jejich vyhodnocení

Hodnocení zranitelnosti objektu (chráněného prostoru) je vyjádření možnosti:

- a) s jakou mohou být části objektu a chráněného prostoru nebo prvky systému ochrany objektu a chráněného prostoru překonané identifikovanými hrozbami,

- b) jak mohou být zaměstnanci organizace nebo příslušníci fyzické ostrahy nápomocni nepovolané osobě k neoprávněnému přístupu k UI,
- c) jak může dané ohrožení narušit bezpečnost objektu.



Obrázek 1. Algoritmus hodnocení zranitelnosti chráněného prostoru [7]

3.1.3.1 Výběr identifikovaných a ohodnocených hrozeb

Pro potřeby hodnocení zranitelnosti chráněného prostoru se vyberou pouze ty hrozby ze soupisky ohrožení, které byly ohodnoceny minimálně jako malé (M). Hrozby, které byly ohodnoceny 0, neexistují, proto se k hodnocení nepoužívají.

3.1.3.2 Výběr zranitelných míst objektu a chráněného prostoru

Zranitelná místa v objektu a chráněného prostoru B_m mohou být:

- B_1 - perimetr objektu, okolí objektu, přístupy k objektu,
- B_2 - stavební prvky objektu (stěny, podlahy, stropy, střechy),
- B_3 - otvorové výplně (vstupy, dveře, okna, větrací a technologické otvory),
- B_4 - zaměstnanci, cizí osoby,
- B_5 - způsob manipulace s utajovanými informacemi (např. ukládání, vytváření),
- B_6 - fyzická ochrana objektu a chráněného prostoru,
- B_7 - ochrana vnitřních prostorů technickými prostředky, režimová opatření.

3.1.3.3 Sestavení matice hodnocení zranitelnosti

Matice hodnocení zranitelnosti je ve tvaru $j \times m$, kde j znázorňuje počet ohrožení s minimální hodnotou Malá (M) a m představuje počet skupin zranitelných míst. Příklad matice hodnocení zranitelnosti je uveden v Tabulka 2.

Ohrožení O_j	Zranitelná místa B_m	
	B_1	B_2
O_6	Z_{61}	Z_{62}
O_7	Z_{71}	Z_{72}
O_8	Z_{81}	Z_{82}
O_9	Z_{91}	Z_{92}

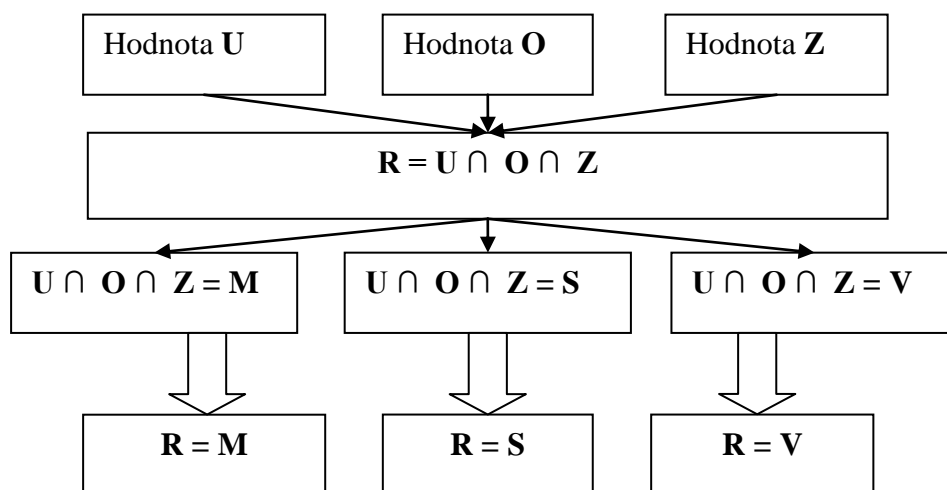
Tabulka 2. Příklad matice hodnocení zranitelnosti

Hodnocení zranitelnosti spočívá ve vyjádření možnosti, že daný typ ohrožení využije zranitelné místo v objektu na ohrožení bezpečnosti objektu a utajovaných informací. Stupnice hodnocení zranitelnosti začíná na **malé zranitelnosti (M)**, kdy dané ohrožení může jen těžko využít zranitelného místa na ohrožení UI. Pokud existuje možnost, že zranitelné místo bude daným ohrožením překonané, jedná se o **střední zranitelnost (S)**. **Velká zranitelnost (V)** představuje vysokou pravděpodobnost zneužití zranitelného místa k získání přístupu k UI. Tímto způsobem se hodnotí každý typ ohrožení O_j s každou skupinou zranitelných míst B_m a výsledek se zapíše do příslušného pole matice Z_{jm} .

Výsledná zranitelnost objektu je daná hodnotou zranitelnosti toho zranitelného místa, které bylo ohodnoceno jako nejzranitelnější. [7]

3.1.4 Stanovení míry rizika

Míra rizika ohrožení utajovaných informací se stanoví jako funkce tří faktorů. Jsou to **velikost újmy U**, která může vzniknout jako následek neoprávněné manipulace s UI, **velikost ohrožení O**, která byla identifikována v bezpečnostním prostředí chráněného prostoru a **velikost zranitelnosti Z** objektu. Výsledná **míra rizika R** se stanoví jako průnik těchto funkcí.



Obrázek 2. Postup při stanovení míry rizika

Velikost újmy U	Velikost ohrožení O								
	Malá			Střední			Velká		
	Zranitelnost Z								
	Malá	Střední	Velká	Malá	Střední	Velká	Malá	Střední	Velká
Nevýhodné pro zájmy ČR	M	M	M	M	S	S	S	S	V
Prostá újma	M	M	M	S	S	S	S	V	V
Vážná újma	M	S	S	S	S	V	V	V	V
Mimořádně vážná újma	S	S	S	S	V	V	V	V	V

Obrázek 3. Příklad určení míry rizika ohrožení utajovaných informací [7]

Získaná hodnota míry rizika ohrožení UI slouží dále k posouzení dostatečnosti bezpečnostních opatření podle tabulky minimálních požadovaných bodových ohodnocení opatření fyzické bezpečnosti chráněných prostorů.

3.2 Určení objektu, zabezpečených oblastí a jednacích oblastí

Určení objektu, zabezpečených oblastí a jednacích oblastí se v úvodu zabývá:

- a) **obecným popisem** areálu organizace a obsahuje
 - obecný úvod – adresa,
 - popis areálu / budovy – popis hranice, počet budov, počet podlaží, vstupy, případně zabezpečení,
 - okolí – charakter objektů, které by mohly mít vliv na bezpečnost,
 - cizí subjekty v areálu / budově – počet, název, zaměření činnosti,
 - schéma
- b) **stanovením objektu** - Jak už jsem uvedl v kapitole 2, objektem se rozumí budova nebo jiný ohraničený prostor, ve kterém se nacházejí zabezpečené nebo jednací oblasti.
- c) **stanovením hranice objektu** - hranicí objektu se myslí plášť budovy, fyzická bariera (plot) nebo jinak viditelně vymezená hranice. Hranici objektu stanoví provozovatel objektu.
- d) **stanovením typu objektu** - vychází se ze stavebně – technického pojetí objektu, kdy se hodnotí, jaké stavební konstrukce jsou stěny, podlahy a stropy. Zároveň se hodnotí, jakým způsobem jsou zabezpečeny průlezné otvory, jak vysoko jsou nad terénem a jestli lze k nim jednoduše proniknout ze střechy, hromosvodů, parapetů, stromů nebo jiných budov. V příloze č. 1 k vyhlášce č. 528/2005 Sb. je uvedeno 5 typů objektů.
- e) **určením zabezpečených oblastí** – Zabezpečenou oblastí je ohraničený prostor uvnitř objektu, kde se zpracovávají nebo ukládají UI. Hranici zabezpečené oblasti a její zařazení do příslušné kategorie a třídy stanovuje provozovatel objektu.
- f) **určením jednacích oblastí** – Stejně jako zabezpečená oblast je jednací oblastí ohraničený prostor v objektu, ale na rozdíl od ní zde dochází k projednávání

utajovaných informací. Hranice jednacích oblastí je opět stanovena provozovatelem² objektu.

3.3 Zabezpečení zabezpečené oblasti

Zabezpečení zabezpečené oblasti a hranice objektu je zajišťováno kombinací opatření fyzické bezpečnosti - ostraha, režimová opatření, technické prostředky. Rozsah použití technických prostředků k zabezpečení zabezpečené oblasti (dále ZO) se stanoví v závislosti na kategorii a třídě dané zabezpečené oblasti a vyhodnocení rizik.

Zabezpečené oblasti se podle nejvyššího stupně utajení UI, která se v nich ukládá, zařazují do kategorií Vyhrazené, Důvěrné, Tajné, Přísně tajné. Současně se podle možnosti přístupu k utajované informaci dělí ZO do **třídy I.**, kdy vstupem do této oblasti dochází k seznámení s utajovanou informací a **třídy II.**, kdy vstupem do této oblasti nedochází k seznámení s UI. Vstup do zabezpečené oblasti a výstup z ní musí být kontrolovány opatřeními fyzické bezpečnosti. Neoprávněná osoba může vstoupit pouze do ZO **třídy II.**, a to s osobou, která má do této oblasti vstup povolen.

Rozsah zabezpečení ZO technickými prostředky pro jednotlivé kategorie:

- a) **Vyhrazené** – mechanické zábranné prostředky,
- b) **Důvěrné** – mechanické zábranné prostředky a poplachové zabezpečovací systémy,
- c) **Tajné, Přísně tajné** – mechanické zábranné prostředky, systémy pro kontrolu vstupů, poplachové zabezpečovací systémy, speciální televizní systémy, zařízení elektrické požární signalizace. Speciální televizní systémy lze nahradit tísňovými systémy.

Zabezpečené oblasti kategorie **Důvěrné** a **vyšší**, v kterých je trvale zajištěna přítomnost zde pracujících osob, se zabezpečují hlavně mechanickými zábrannými prostředky a poplachovými zabezpečovacími systémy, anebo tísňovým systémem. Plní – li tyto ZO zároveň úlohu stanovišť určených pro stálý výkon ostrahy, nemusí být vybaveny zařízeními PZS. Při použití speciálních televizních systémů nesmí být narušena ochrana

² Provozovatel objektu - je to odpovědná osoba nebo osoba jí k tomu pověřená podle § 2 písmene e) zákona č. 412/2005 Sb.

utajovaných informací. K zajištění ochrany ZO kategorie **Důvěrné** a **vyšší** se používají pouze certifikované technické prostředky, necertifikované technické prostředky je možné použít pouze v případě, že nesníží úroveň ochrany požadovaný pro daný stupeň zabezpečení. Pro kategorii **Vyhrazené** je možné použít certifikované i necertifikované technické prostředky.

Zabezpečení zabezpečené oblasti se provádí také na hranici objektu, ve kterém se tato oblast nachází. Použití technických prostředků se stanoví v závislosti na nejvyšší kategorii ZO, která se nachází v objektu, na základě vyhodnocení rizik a podle charakteru hranice objektu.

Rozsah zabezpečení ZO na hranici objektu technickými prostředky pro jednotlivé kategorie:

- a) **Vyhrazené** - mechanické zábranné prostředky,
- b) **Důvěrné** a **Tajné** - mechanické zábranné prostředky a poplachové zabezpečovací systémy,
- c) **Přísně tajné** – mechanické zábranné prostředky, poplachové zabezpečovací systémy, speciální televizní systémy.

Utajovaná informace se ukládá v zabezpečené oblasti, popřípadě v úschovném objektu, je – li jeho bodová hodnota uplatněna v projektu fyzické bezpečnosti pro příslušnou zabezpečenou oblast. Zákon dále ukládá povinnost mít v objektu zařízení fyzického ničení nosičů informací.

V případech kdy hranice objektu je totožná s hranicí zabezpečené oblasti, je rozsah opatření fyzické bezpečnosti určen požadavky na kategorii dané ZO. [4]

3.4 Zabezpečení jednacích oblastí

Podobně jako v kapitole 3.3 je zabezpečení jednacích oblastí (dále JO) a hranice objektu prováděno kombinací opatření fyzické bezpečnosti. Jednací oblast a hranici objektu stanovuje provozovatel objektu.

K určení rozsahu použití fyzické bezpečnosti k zabezpečení JO se využívá stejných postupů jako v případě stanovení rozsahu použití fyzické bezpečnosti zabezpečených oblastí a to v závislosti na stupni UI, které jsou v jednacích oblastech pravidelně projednávány a na výsledku hodnocení rizik.

Jednací oblasti pro pravidelné projednávání UI stupňů utajení **Tajné** a **Přísně tajné** se zabezpečují mechanickými zábrannými prostředky, systémy pro kontrolu vstupů, zařízeními PZS, speciálními televizními systémy, zařízeními EPS a zařízeními proti pasivnímu a aktivnímu odposlechu utajované informace.

K zajištění ochrany jednacích oblastí se používají certifikované technické prostředky, které lze nahradit necertifikovanými technickými prostředky pouze za předpokladu, že nesníží úroveň ochrany požadované pro daný stupeň utajení.

Stejně jako u ZO, se zabezpečení JO dále provádí na hranici objektu, ve kterém se tato oblast nachází. Rozsah použití technických prostředků závisí na stupni UI, které jsou v jednací oblasti projednávány, dále na vyhodnocení rizik a charakteru hranice objektu. Hranice objektu je zabezpečena mechanickými zábrannými prostředky, zařízeními PZS a speciálním televizním systémem. V objektu musí být umístěno zařízení fyzického ničení nosičů informací. V případě že hranice objektu je totožná s hranicí JO, je rozsah použití opatření fyzické bezpečnosti určen požadavky na zabezpečení jednací oblasti.

Odpovědná osoba je povinna zajistit ochranu projednávaných UI proti jejich úniku. Ke splnění této povinnosti je odpovědná osoba povinna požádat NBÚ o provedení kontroly zda v jednací oblasti nedochází k nedovolenému použití technických prostředků určených k získávání informací. Tuto kontrolu zajišťuje Národní bezpečnostní úřad v součinnosti se zpravodajskými službami a PČR. [4]

3.5 Zabezpečení technického zařízení

Technické zařízení obsahující utajovanou informaci stupně utajení **Důvěrné** a **vyšší** se ukládá v zabezpečené oblasti. Provozovatel objektu stanovuje hranici zabezpečené oblasti, ve které je technické zařízení umístěno. Zabezpečení ZO, ve které je umístěno technické zařízení, je zajišťováno podle §5 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.

Rozsah použitých technických prostředků a další překážek k zabezpečení ochrany utajovaných informací v technických zařízeních stanovuje provozovatel objektu takovým způsobem, aby byla zajištěna informovanost ostrahy o právě probíhajícím pokusu o narušení bezpečnosti UI a zpomalila se cesta útočníka na cestě k utajované informaci v technickém zařízení. Nejblíže k technickému zařízení se zpravidla umísťuje nejodolnější technický prostředek. [4]

3.6 Zabezpečení fyzickou ostrahou a režimovými opatřeními

3.6.1 Fyzická ostraha zabezpečené oblasti a jednacích oblastí

Ostraha se nepřetržitě zajišťuje u objektu, ve kterém se nachází **zabezpečené oblasti** kategorie Přísně tajné, Tajné a Důvěrné. Rozsah zabezpečení pro jednotlivé kategorie ZO:

- a) **Vyhrazené** – zabezpečená oblast této kategorie je chráněna ostrahou v rozsahu stanoveném odpovědnou osobou,
- b) **Důvěrné** – nejméně jednou osobou, které kombinace opatření (elektrická zámková zařízení, systémy pro kontrolu vstupů, zařízení PZS) umožní efektivně ochránit UI,
- c) **Tajné** – nejméně jednou osobou u objektu a 1 další osobou, které kombinace opatření (elektrická zámková zařízení, systémy pro kontrolu vstupů, zařízení PZS a zařízení EPS) umožní rychlý zásah, je – li provádění ochrany UI narušeno,
- d) **Přísně tajné** – nejméně dvěma osobami u objektu.

Fyzická ostraha se uskutečňuje u **jednacích oblastí** kategorie **Přísně tajné** a **Tajné**. Rozsah jejich zabezpečení její totožný s rozsahem zabezpečení fyzické ostrahy u zabezpečených oblastí. Ostraha se zajišťuje zaměstnanci orgánu státu, právnické osoby nebo podnikající fyzické osoby, o jejíž objekt jde, příslušníky ozbrojených sil nebo ozbrojených sborů anebo zaměstnanci bezpečností ochranné služby. [4]

3.6.2 Fyzická ostraha technického zařízení

Pro ostrahu technického zařízení se liší typ ostrahy podle stupně utajení, kterou zařízení obsahuje:

- a) **Důvěrné** – stanovena ostraha typu 4 nebo vyšší podle přílohy č. 1 k vyhlášce č. 528/2005 Sb.,
- b) **Tajné** – stanovena ostraha typu 4 s pravidelnými obchůzkami v intervalu ne větším než 4 hodiny nebo ostraha vyšší podle stejné přílohy,
- c) **Přísně tajné** – stanovena ostraha typu 5 podle přílohy č. 1

Provozovatel objektu stanovuje časové limity pro ostrahu, které musí dodržet při zásahu proti útočníkovi. Tyto limity uvádí provozovatel v projektu fyzické bezpečnosti. Čas se určuje podle počtu a druhu technických zařízení a jiných překážek, které musí útočník

překonat k cestě za UI v technickém zařízení. Časové limity se musí pravidelně ověřovat a upravovat podle nových skutečností.

Zásah proti útočníkovi je prováděn minimálně dvěma fyzickými osobami v jakémkoliv místě objektu nebo zabezpečené oblasti, kde došlo k narušení ochrany UI v technickém zařízení nebo k vyhlášení poplachového nebo nouzového signálu, aniž by byla oslabena ochrana UI na jiném místě. [4]

3.6.3 Zabezpečení režimovým opatřením

Stanovují:

- a) oprávnění pro osoby a dopravní prostředky pro vstup nebo vjezd do objektu a dále stanovují oprávnění pro vstup osob do zabezpečených oblastí,
- b) kontrolní opatření pro vstup do zabezpečených oblastí,
- c) podmínky a způsob kontroly pohybu osob v objektu, ZO, JO a dále určují způsob kontroly vynášení informací z objektu, ZO, JO
- d) režim manipulace s klíči, identifikačními daty a technickými prostředky.

3.7 Bodové hodnocení opatření fyzické bezpečnosti

Míra zabezpečení jednacích oblastí a zabezpečené oblasti opatřeními fyzické bezpečnosti se určuje pomocí bodových hodnot těchto opatření v závislosti na vyhodnocení rizik. Bodové hodnoty pro jednotlivé opatření jsou stanoveny prováděcím právním předpisem v příloze č. 1. k vyhlášce č. 528/2005 Sb.

Opatření fyzické bezpečnosti nebo kombinace více těchto opatření musí odpovídat alespoň nejnižší míře zabezpečení jednacích oblastí nebo zabezpečené oblasti a stanoví se v závislosti na vyhodnocení rizik a na stupni utajení utajovaných informací, které jsou v jednacích oblastech pravidelně projednávány, nebo na kategorii zabezpečené oblasti.

3.7.1 Minimální požadované hodnoty míry zabezpečení

K vyhodnocení minimální požadované hodnoty míry zabezpečení zabezpečených oblastí a jednacích oblastí se vychází z tabulky bodové hodnoty nejnižší míry zabezpečení a z nabídky bezpečnostních opatření uvedených v příloze č. 1. k vyhlášce č. 528/2005 Sb. Tabulka a nabídka bezpečnostních opatření slouží jako pomocné prostředky a musí být použity při vyhodnocování požadavků na fyzickou bezpečnost. Pokud je jasné, že přijatá opatření nejsou adekvátní, pak i v případě, že je dosaženo požadovaných bodových hodnot,

které vyhovují těmto standardům, může se na základě správného posouzení rizik ukázat, že je nutno zvážit zavedení doplňujících opatření nebo alternativních kombinací. Tabulka slouží pouze jako předloha, na jejímž základě jsou určovány úrovně bezpečnostních opatření. Základem pro zavedení příslušných opatření a postupů je vyhodnocení rizika vycházející z prostředí, ve kterém se UI nacházejí.

Bodová hodnota bezpečnostních opatření, která jsou požadována pro zajištění příslušného stupně ochrany, je odvozována z popisu bezpečnostních opatření. Dvě bodové hodnoty vycházejí z povinných opatření a zbývajících z opatření ostatních. Tento systém závazných a doplňujících opatření má zajistit vyváženost jednotlivých kroků a umožňuje postupovat pružně při výběru opatření, jejichž cílem je dosáhnout společného stupně ochrany s přihlédnutím k bezpečnostnímu zařízení, vybavení a lidskému potenciálu.

3.8 Technická dokumentace fyzické bezpečnosti

Jsou to dokumenty vztahující se k technickým prostředkům v rámci fyzické bezpečnosti. Podle vyhlášky č. 528/2005 Sb. technická dokumentace obsahuje technické údaje, pokyny a pravidla pro používání technických prostředků v zabezpečené a jednacích oblastech a obsahuje i příslušné certifikáty k technickým prostředkům. Bezpečnostní standardy NBÚ člení strukturu technické dokumentace:

- **Výkresová dokumentace** - obsahuje zejména vyznačení hranice objektu, hranic jednotlivých zabezpečených a jednacích oblastí a rozmístění technických prostředků určených k ochraně utajovaných informací v objektu a zabezpečených a jednacích oblastech,
- **Dokumentace technických prostředků** – obsahuje především údaje o názvu, počtu a typu technického prostředku, jeho umístění v objektu a základní informace
 - a) **Certifikované technické prostředky** – kopie certifikátu a přílohy z doby instalace
 - b) **Necertifikované technické prostředky** – zápis o posouzení shody z doby instalace (uvezení specifikace a způsob použití). [5]

4 ZÁKLADNÍ POKYNY PŘI NÁVRHU BEZPEČNOSTNÍHO SYSTÉMU

Jaký postup zvolit při návrhu a realizaci bezpečnostního systému jsem se snažil nastínit do následujících podkapitol.

4.1 Zadání projektu

Zadání projektu vychází nejčastěji z bezpečnostní politiky, kterou implementuje zákazník ve vlastní organizaci. U větších organizací na bezpečnostní politiku obvykle navazují bezpečnostní standardy – interní předpisy, které definují rozsah a úroveň bezpečnostních opatření pro jednotlivé typy objektů. Podkladem pro zpracování bezpečnostní politiky jsou bezpečnostní analýzy. Na základě bezpečnostní analýzy je zákazníkovi vytvořen systémový návrh, který představuje prvotní koncepci zabezpečení objektu a cenovou nabídku. [8]

4.2 Identifikace nebezpečí

Základní otázkou při identifikaci nebezpečí je, jaký majetek se vlastně střeží. To znamená, že se provede posouzení střežených objektů, s cílem stanovit nezbytnou úroveň systému zabezpečení. Před zpracováním systémového návrhu je důležité stanovit rozsah a charakter majetku, který se ve střežených objektech nachází. Hlavní aspekty posouzení představují:

- **druh majetku** – snadnost zpeněžení, atraktivnost pro pachatele,
- **hodnota majetku** – maximální pravděpodobná hodnota přímé ztráty, následné výdaje související se ztrátou, osobní vztahy,
- **objem nebo velikost majetku** – snadnost krádeže a transportu, snadnost zpeněžení
- **historie krádeží** – počet předcházejících krádeží ve střežených objektech, způsoby vloupání při předcházejících krádežích,
- **nebezpečí pro okolní prostředí** – zneužití střeženého majetku,
- **poškození** – vandalismus na střeženém objektu, riziko zhářství.

Nezbytnou součástí identifikace nebezpečí je obhlídka objektu, jejímž cílem je identifikace slabých míst v objektu. Faktory, které je přitom nutno posoudit jsou stavební provedení objektu, kde se hodnotí:

- **konstrukce** – stěn, střech, podlah, pokud jsou tak i sklepení,

- **stavební otvory** – konstrukce oken, dveří, střešních světlíků, ventilačních kanálů a ostatní otevírané části budovy,
- **personál** – počet osob normálně přítomných ve střežených objektech, charakter pobývajících osob, přítomnost pracovníků ochrany, hodnocení možného přístupu veřejnosti,
- **držitelé klíčů** – dosažitelnost držitelů klíčů schopných reagovat na činnost PZTS
- **umístění objektu** – umístění v oblasti s vysokým rizikem kriminality, sousední budovy, rychlost předpokládaného zásahu,
- **stávající zabezpečení** – kvalita a rozsah stávajících zabezpečovacích zařízení MZS a EZS,
- **historie krádeží** – počet a způsob předcházejících vloupání,
- **místní legislativa a předpisy** – bezpečnostní požadavky na technická zařízení, požární předpisy,
- **poloha objektu** – rozlišení jestli se jedná o městskou zástavbu nebo o venkov. [10]

4.3 Stupeň zabezpečení

Stupeň zabezpečení systému PZTS závisí na požadované úrovni zabezpečení stanovené při analýze rizik. Norma ČSN CLC/TS 50 131 – 7 definuje čtyři stupně zabezpečení, kterými se řídíme při volbě zařízení.

1) Stupeň 1 – Nízké riziko

Předpokládá se, že narušitelé nebo lupiči mají malou znalost PZTS a k dispozici mají omezený sortiment snadno dostupných nástrojů.

2) Stupeň 2 – Nízké až střední riziko

U tohoto stupně zabezpečení se předpokládá, že narušitelé mají určité znalosti o PZTS a mají k dispozici základní sortiment nástrojů a přenosných přístrojů.

3) Stupeň 3 – Střední až vysoké riziko

Narušitelé nebo lupiči jsou seznámeni s PZTS a mají úplný sortiment nástrojů a přenosných elektronických zařízení.

4) Stupeň 4 – Vysoké riziko

Vychází se z předpokladu, že narušitelé nebo lupiči jsou schopni nebo mají možnost zpracovat podrobný plán narušení nebo loupeže a mají kompletní sortiment zařízení včetně prostředků pro náhradu komponentů v PZTS. [12]

4.4 Třída prostředí

Třída prostředí jednotlivých komponentů systému je závislá na podmínkách prostředí, jakým bude vystavena během svého provozu. Podle normy ČSN CLC/TS 50 131 – 7 se dělí prostředí do čtyř tříd.

1) Třída prostředí 1 – vnitřní

Toto prostředí se obvykle vyskytuje ve vnitřních prostorách při stále teplotě v rozmezí od + 5 °C do + 40 °C.

2) Třída prostředí 2 – vnitřní všeobecné

Jedná se o prostředí vnitřní, ve kterém není stálá teplota (chodby, haly) a může zde docházet ke kondenzaci na oknech a v prostorech kde vytápění není trvalé. Teplota se bude pohybovat v rozmezí od – 10 °C do + 40 °C.

3) Třída prostředí 3 – venkovní chráněné nebo extrémní vnitřní podmínky

Vlivy prostředí vyskytující se obvykle vně budov, přičemž komponenty PZTS nejsou plně vystaveny povětrnostním vlivům. Komponenty poplachového systému se musí vypořádat s teplotou v rozmezí od – 25 °C do + 50 °C.

4) Třída prostředí 4 – venkovní všeobecné

Komponenty poplachového systému jsou vystaveny vlivům prostředí a povětrnostním podmínkám vně budov. Předpokládají se změny teplot v rozmezí od – 25 °C do + 60 °C. [12]

4.5 Volba komponentů a jejich umístění

Volba komponentů zabezpečovacího systému je zřejmě nejdůležitější částí samotného návrhu zabezpečení a logicky navazuje na předchozí kroky v průběhu návrhu zabezpečení konkrétního objektu.

Je důležité stanovit, jaký druh ochrany bude pro objekt nejvhodnější. Můžeme vybírat z několika systémů, ale vždy je lepší jejich kombinace.

- a) mechanické zábranné systémy
- b) poplachové zabezpečovací systémy
- c) sledovací systémy
- d) systémy kontroly vstupů

U každého z těchto systémů je dobré volit certifikované prvky, abychom měli jistotu o jejich správné funkčnosti a předešli tak možným komplikacím například

s elektromagnetickou kompatibilitou. U mechanických systémů je potřeba zvolit vhodnou bezpečnostní třídu, která určuje odolnost proti násilnému vniknutí.

Umístění komponent PZTS určuje, jak bude daný prostor zabezpečen proti případnému pokusu o neoprávněný pohyb v místě střežení. Je důležité se zajímat, na jakém principu pracují jednotlivé detektory a jestli je jejich detekční charakter vhodný do chráněného prostoru. Detektory mají být umístěny v souladu s doporučeními výrobce.

Pokud systém PZTS využívá komunikaci s PCO (dnes je tato zkratka nahrazena podle normy ČSN CLC/TS 50136 – 7 výrazem poplachové přijímací centrum) nebo s majitelem objektu musí být komunikátor umístěn uvnitř střeženého prostoru. Jestliže je PZTS dělen do podsystemů o různém stupni zabezpečení, má být komunikátor umístěn v prostoru s nejvyšším stupněm zabezpečení.

Tísňová zařízení mají být umístěna v souladu s doporučením výrobce, aby umožňovala vysokou naději na jejich aktivaci v případě přepadení nebo hrozby.

Výstražná zařízení mají být umisťována na místech, která nejsou snadno dosažitelná a zároveň umožňují účinnou signalizaci poplachu a musí být upevněna tak, aby se snížila možnost jejich demontáže bez vyhlášení poplachu.

II. PRAKTICKÁ ČÁST

5 PROJEKT ZABEZPEČENÍ OBJEKTU

5.1 Stručný popis objektu

Obecný úvod

- objektem je blíže nejmenovaná firma, pracující v oblasti návrhu a vývoje IS,
- předmětem činnosti je kompletní správa a hosting některých IS státní správy a samosprávy.

Popis budovy

- objekt se nachází v 60 tisícovém městě,
- je lokalizovaný v řadové zástavbě, objekt disponuje třemi nadzemními podlažími,
- samotná softwarová firma sídlí v jedné budově v 1. nadzemním podlaží a 2. nadzemním podlaží, 3. nadzemní podlaží je ve vlastnictví firmy, ale je nevyužito,
- jelikož se jedná o řadovou zástavbu, tvoří hranici objektu z východu a západu zdivo ostatních budov. Hranici ze severu a jihu tvoří zdivo a okna. V 1. nadzemním podlaží se ze severní strany nachází balkon s dvěma vstupy do kanceláří,
- rozměry budovy 12 x 25m.

Okolí objektu

- objekt je situován v části města, kde není mnoho obytných prostor, v noci méně frekventované,
- v okolí se nenachází žádné výrobní objekty, které by mohly mít bezprostřední vliv na bezpečnost objektu.

Cizí subjekty v budově

- v přízemí se nachází několik obchodů, včetně jednoho e-shopu s výpočetní technikou a s vlastním skladem,
- dvě místnosti využívá bezpečnostní firma.

6 BEZPEČNOSTNÍ POSOUZENÍ OBJEKTU

6.1 Stanovení metody analýzy rizik

Při řešení úlohy analýzy rizik v oblasti fyzické bezpečnosti budu využívat kvalitativně induktivní expertní metody, protože:

- podmínky a předpoklady vzniku rizik jsou velmi proměnlivé,
- kvantitativní vyjádření parametrů rizik je s ohledem na různorodost podmínek a výrazný vliv lidského faktoru poměrně obtížné,
- kvalitativní metody nevyužívají množství statistických údajů, ale využívají logické vazby mezi faktory ovlivňující vznik rizika,

Při stanovení míry rizika ohrožení utajovaných informací, vycházím z předpokladu vzájemné závislosti **velikosti újmy** způsobené jako důsledek neoprávněné manipulace s utajovanou informací, dále z pravděpodobností neoprávněné manipulace s utajovanou informací představující **výběr identifikovaných a ohodnocených hrozeb** a ze **zranitelnosti chráněného prostoru**. Míra rizika se tedy vyjádří jako průnik všech faktorů.

6.2 Identifikace aktiv a stupně utajovaných informací

Jelikož se jedná o firmu produkující software a informační systémy a která zároveň provozuje ve svých prostorách servery pracující jako hostingová centra, bude identifikace aktiv a stanovení stupně utajení následující podle Tabulka 3.

	Aktiva	Množství	Stupeň utajení
1.	PC	29	Tajné, Důvěrné
2.	hosting server	9	Tajné
3.	server home	3	Důvěrné
4.	software	1	Důvěrné
5.	dokumentace	1	Důvěrné

Tabulka 3. Identifikace aktiv a stupně utajení

6.3 Určení velikosti újmy

Protože byla v organizaci identifikována aktiva se stupněm utajení **TAJNÉ** a **DŮVĚRNÉ**, bude určení velikosti újmy odpovídat uvedeným stupňům utajení. V prvním případě bude velikost újmy **Vážná újma**, která by vznikla při neoprávněné manipulaci s UI a mohla by způsobit vážné škody v oblasti bezpečnosti, konkurenceschopnosti a ekonomických zájmů společnosti. V druhém případě se jedná o možný vznik **Prosté újmy**.

6.4 Analýza bezpečnostního prostředí

Cílem analýzy bylo získat věrohodné, aktuální a relevantní informace o současném stavu a situaci ve vnějším a vnitřním bezpečnostním prostředí organizace. Na základě této analýzy jsem vytvořil soupisku možných ohrožení a jejich slovní hodnocení podle velikosti ohrožení. Vzhledem k umístění a charakteru objektu se analýza vztahovala především k poloze objektu, zabezpečení ochrany objektu, možnosti vzniku technických poruch, zaměstnancům a ostatnímu personálu a možnosti vzniku mimořádné události. Celkové hodnocení ohrožení odpovídá nejvyššímu identifikovanému ohrožení, tedy **VELKÉ**.

Tabulka 4. Soupiska ohrožení objektu

Ohrožení		Existuje zdroj ohrožení?	Motivace, záměr, příčina	Výskyt případu v minulosti (ANO/NE)	Hodnocení hrozby (0; M; S; V)
Z hlediska polohy a umístění objektu	O ₁	Ne	Ne	Ne	0
	O ₇	Ano - Náhodný lupič	Nedá se s určitostí definovat	Ne	Střední
Zabezpečení ochrany objektu	O ₈	Ano - Lupič s přípravou	Ano - Zisk	Ne	Velké
	O ₉	Ano - Vandalismus	Nedá se s určitostí definovat	Ne	Střední
	O ₁₀	Ano - Návštěvy	Nedá se s určitostí definovat	Ne	Střední
	O ₁₈	Ano - Rozvod el. energie	Ne - Havárie, požár, záplavy, plyn, sabotáž	Ne	Malé
Technické poruchy	O ₁₉	Ne - Rozvod vody			0
	O ₂₀	Ne - Rozvod a zásobníky plynu			0
Zaměstnanci	O ₂₂	Ano - Vlastní zaměstnanci - oprávněné osoby	Ne - Zisk, nedbalost, neznalost, vydírání	Ne	Malé
	O ₂₄	Ano - Servisní služby, obslužný personál	Nedá se s určitostí definovat	Ne	Střední
Výjimečný a nouzový stav	O ₂₈	Ano – Požár v objektu	Nedá se s určitostí definovat	Ne	Střední

6.5 Vyhodnocení zranitelnosti objektu

Jakým způsobem se stanovuje zranitelnost objektu jsem se snažil vysvětlit v kapitole 3.1.3 Stanovení zranitelností a jejich vyhodnocení. Vytvořil jsem matici hodnocení zranitelnosti pro daný objekt. Indexy ohrožení O_j odpovídají soupisce ohrožení podle přílohy jedna a indexy zranitelných míst B_m jsem uvedl na straně 23.

Ohrožení O_j	Zranitelná místa B_m					
	B_1	B_2	B_3	B_4	B_5	B_7
O_7	S	M	M	M	M	S
O_8	S	S	S	S	S	S
O_9	M	M	M	M	M	M
O_{10}	M	M	M	M	M	M
O_{18}	M	M	M	M	S	S
O_{22}	M	M	M	M	S	S
O_{24}	M	M	M	S	S	S
O_{28}	M	M	S	S	S	S

Tabulka 5. Matice zranitelnosti objektu

Výsledná zranitelnost objektu byla vyhodnocena jako **STŘEDNÍ**, protože se zde nevyskytuje žádná hodnota zranitelnosti VELKÁ. Nyní můžu ze zjištěných informací stanovit předpokládanou míru rizika, která bude dále sloužit k určení bodové hodnoty zabezpečení ZO a JO. Ze zjištěných údajů jsem pro oba stupně utajení určil pravděpodobnost míry rizika jako **VELKÁ**.

Velikost újmy U	Velikost ohrožení O								
	Malá			Střední			Velká		
	Zranitelnost Z								
	Malá	Střední	Velká	Malá	Střední	Velká	Malá	Střední	Velká
Nevýhodné pro zájmy ČR	M	M	M	M	S	S	S	S	V
Prostá újma	M	M	M	S	S	S	S	V	V
Vážná újma	M	S	S	S	S	V	V	V	V
Mimořádně vážná újma	S	S	S	S	V	V	V	V	V

Tabulka 6. Výsledná míra rizika v objektu

6.6 Bodové hodnocení bezpečnosti

Na základě vyhodnocení míry rizika a stupně utajovaných informací se stanoví minimální bodová hodnota zabezpečení zabezpečené oblasti a jednacích oblastí. K tomuto účelu využijí tabulku bodových hodnot nejnižší míry zabezpečení.

V rámci společnosti se v zabezpečených oblastech a jednacích oblastech ukládají a projednávají informace stupně utajení **TAJNÉ** a **DŮVĚRNÉ**. Míra rizika ohrožení utajovaných informací byla vyhodnocena jako **VELKÁ**. V prvním případě by měla bodová hodnota zabezpečení zabezpečené oblasti činit minimálně 20 bodů a jednacích oblastí minimálně 16 bodů, v druhém případě je minimální hodnota zabezpečené oblasti 16 bodů.

ZABEZPEČENÁ OBLAST KATEGORIE Tajné	Míra rizika		
	malá	střední	velká
Povinné : (S1) + (S2) + (S3)	8	9	10
Povinné : (S4) + (S5) **	4	5	5
Nepovinné : (S6)	4	5	5
Celkový výsledek	16	19	20

Tabulka 7. Bodové hodnoty zabezpečené oblasti [5]

JEDNACÍ OBLAST pro pravidelné projednávání utajovaných informací stupňů utajení Tajné	Míra rizika		
	malá	střední	velká
Povinné : (S2) + (S3)	5	5	6
Povinné : (S4) + (S5) **	4	5	5
Nepovinné : (S6)	4	5	5
Celkový výsledek	13	15	16

Tabulka 8. Bodové hodnoty jednacích oblastí [5]

ZABEZPEČENÁ OBLAST KATEGORIE Důvěrné	Míra rizika		
	malá	střední	velká
Povinné : (S1) + (S2) + (S3)	6	8	9
Povinné : (S4) + (S5)	2	3	3
Nepovinné : (S6)	3	3	4
Celkový výsledek	11	14	16

Tabulka 9. Bodové hodnoty zabezpečené oblasti kategorie Důvěrné [5]

7 URČENÍ ZABEZPEČENÝCH A JEDNACÍCH OBLASTÍ

7.1 Stanovení objektu, jeho typu a hranic

Budova, ve které dochází ke styku s utajovanými informacemi, je tří podlažní řadový městský dům bez oplocení, využívaný ke komerčním účelům. Objektem je 1. a 2. nadzemní podlaží. Hranici objektu tvoří venkovní plášť budovy sestavený z cihlových a tvárnicových zdí a z 10 plastových oken v každém z podlaží. Objekt jsem určil jako **Objekt typ 3** podle přílohy č. 1. k vyhlášce č. 528/2005 Sb. Jedná se o objekt, jehož stěny, podlahy a stropy mají pevnou stavební konstrukci z cihel nebo tvárnic.

Bodové hodnocení objektu **S3 = 0**, protože hranice objektu je v celé své délce shodná s hranicí zabezpečené oblasti.

7.2 Stanovení zabezpečených oblastí, jejich hranic, typ, kategorie, třídy

a) 1. nadzemní podlaží

- **Typ:** Zabezpečená oblast typ 2, kde stěny, podlahy a stropy jsou zděné cihlové konstrukce tloušťky do 150 mm. Bodové hodnocení tohoto typu ZO je **SS3 = 2**.
- **Kategorie:** V zabezpečených oblastech 1. NP se ukládají a zpracovávají utajované informace stupně utajení **DŮVĚRNÉ**. Jedná se o pracoviště bez stálé přítomnosti zde pracujících osob. V tomto patře se nachází kancelář vedoucího a 3 další kanceláře, servrovna a toaleta. Přístup do patra je možný pouze ze schodiště.
- **Třída:** Možnost přístupu k utajované informaci je II.

b) 2. nadzemní podlaží

- **Typ:** Stejně jako první patro je zabezpečená oblast typ 2. Bodové hodnocení ZO je **SS3 = 2**.
- **Kategorie:** V zabezpečených oblastech 2. NP se ukládají, zpracovávají utajované informace stupně utajení **TAJNÉ**. V 2. NP se ve všední dny v noci nacházejí dva pracovníci v kanceláři vedle servrovny hostingového centra.
- **Třída:** Možnost přístupu k utajované informaci je II.

7.3 Stanovení jednacích oblastí

- **Typ:** Jednací oblast je umístěna ve 2. NP a je součástí hranice zabezpečené oblasti. Bodové hodnocení proto odpovídá ZO, **SS3 = 3**.
- **Kategorie:** V jednací oblasti 2. NP se projednávají utajované informace stupně utajení **TAJNÉ**.
- **Třída:** Možnost přístupu k utajované informaci je II.

Hranice zabezpečených a jednacích oblastí je totožná s hranicí objektu, která je tvořena pláštěm budovy.

Hranice objektu, zabezpečených a jednacích oblastí je znázorněna v příloze této práce.

7.4 Původní zabezpečení

Stávající zabezpečení objektu představuje poplachový zabezpečovací systém s ústřednou PZS od firmy PARADOX a prostorová ochrana s pohybovými detektory PIR v každé místnosti. Přístup do budovy není zabezpečen žádným certifikovaným mechanickým zabraným systémem. Přístup do chráněného prostoru je řešen mříží s obyčejnou cylindrickou vložkou, která je umístěna na schodišti v 1. NP, plášťová ochrana a tísňový systém nejsou realizovány.

Současný stav zabezpečení byl shledán jako nedostatečný především z důvodu z nízkého stupně bezpečnosti, který neodpovídá požadavkům NBÚ na ochranu utajovaných informací.

8 NÁVRH ZABEZPEČENÍ

Při návrhu zabezpečení budu vycházet z určení kategorií pro jednotlivé zabezpečené oblasti. V případě zabezpečené oblasti 1. NP je podmínkou použití minimálně MZS a PZS, v případě zabezpečení 2. NP je podmínkou jak využití MZS a PZS tak systémy pro kontrolu vstupů, EPS a speciální televizní systémy, které je možné nahradit tísňovým systémem. Pro zabezpečení jednacích oblastí určené kategorie je podmínkou použití všech již zmíněných systémů zabezpečení a navíc zařízení proti pasivnímu a aktivnímu odposlechu utajované informace.

8.1 Poplachový zabezpečovací a tísňový systém

8.1.1 Stupeň zabezpečení a rozsah střežení

Poplachový zabezpečovací systém bude chránit dvě zabezpečené oblasti kategorie důvěrné a tajné a jednu jednacích oblast kategorie tajné. V případě zabezpečené oblasti DŮVĚRNÉ bude zabezpečení odpovídat stupni 2 Nízké až střední a zabezpečené oblasti TAJNÉ stupni 3 Střední až vysoké podle ČSN CLC/TS 50 131 – 7. Podle stejné normy se určí i rozsah střežení podle jednotlivých stupňů zabezpečení. Rozsah střežení je závislý na vyhodnocení rizik konkrétního objektu, na vlivech vnitřního a vnějšího prostředí a samozřejmě na jeho stavební konstrukci.

8.1.2 Třída okolního prostředí

Třída I: Prostředí vnitřní. Jedná se prostředí, kde budou komponenty PZS umístěny ve stále vytápěných místnostech a kde se předpokládá, že teplota bude kolísat maximálně v rozmezí od +5 °C do +40 °C a relativní vlhkost se bude pohybovat okolo 75% bez kondenzace.

8.1.3 Použité prostředky

Při výběru komponent poplachového zabezpečovacího a tísňového systému budu vycházet z normy ČSN CLC/TS 50 131 - 7 pro stupeň zabezpečení 3 a 2, tato norma odpovídá požadavku NBÚ na bodovou hodnotu certifikovaného poplachového zabezpečovacího a tísňového systému $SS91 = 3$. Rozsah použitých komponent odpovídá bodové hodnotě NBÚ $SS92 = 2$ a 3 na instalaci zařízení elektrické zabezpečovací signalizace.

8.1.4 Ústředna PZTS

V objektu je navržen adresovatelný systém PZTS s možností rozšíření koncentrátory. Ústředna PZTS od firmy PARADOX typ EVO 192 je umístěna v druhém nadzemním podlaží v místnosti kancelář 2. V kovovém boxu je umístěna společně ústředna, napájecí zdroj, záložní baterie i jeden zónový expandér. Na dvojité vyvážené vstupy ústředny je přímo napojeno několik magnetických kontaktů, detektorů tříštění skla, PIR detektorů s antimaskingem, jeden tísňový hlásič a venkovní výstražné signalizační zařízení. Kompletní uspořádání je naznačeno v blokovém schématu ústředny ve výkresové dokumentaci. Z ústředny je dále vyvedena adresovatelná čtyřvodičová sběrnice do obou zabezpečených oblastí. Na tuto sběrnici jsou přímo napojeny ovládací klávesnice, rozšiřující moduly s 8 (v zapojení s ATZ 16) analogovými dvojitě vyváženými vstupy. Na tyto vstupy jsou připojeny magnetické kontakty oken a dveří, tísňové tlačítko, PIR detektory, duální PIR + MW detektory a akustické detektory tříštění skla. Na sběrnici jsou také připojeny moduly integrovaného přístupového systému.

Základní údaje ústředny PZTS	Hodnota
Dělení na podsystémy	8
Max. počet zón v systému	192
Max. počet modulů v systému	254
PGM výstupy na ústředně	4 x opto-relé 50 mA polarita +/-
PGM výstupy na ústředně	1 x relé 5A, 24 V
Počet uživatelských kódů	999
Maximální délka sběrnice	900 m
Proudový odběr ústředny	100 mA

Tabulka 10. Základní údaje ústředny [15]



Obrázek 4. Ústředna PZTS EVO 192 [15]

8.1.5 Detektory

8.1.5.1 Prostorová ochrana

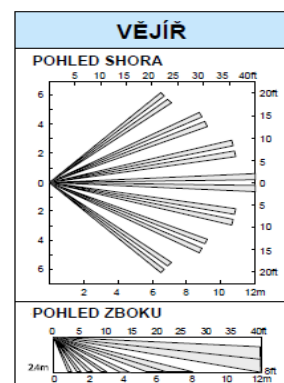
Tento způsob ochrany řeším použitím pasivních infračervených a duálních PIR + MW detektorů. Jednotlivé použité komponenty se liší podle kategorie zabezpečené oblasti. V rámci prvního nadzemního podlaží si vystačím s certifikovanými PIR detektory stupně zabezpečení 2. V druhém nadzemním podlaží již musím použít detektory pro stupeň zabezpečení 3.

1. nadzemní podlaží – zabezpečená oblast **DŮVĚRNÉ**

Pro uvedenou zabezpečenou oblast jsem vybral infračervený pasivní detektor OPTEX RX40QZD. Tento detektor splňuje certifikát NBÚ pro bodové hodnocení SS92 = 2. Detektor se vyrábí s půlkulovou čočkou a optikou Quad Zone Logic, která vytváří extrémně vysokou hustotu zón ve vertikálním směru, dvakrát vyšší ve srovnání s klasickými PIR detektory. Detektor použiju pro střežení všech místností prvního nadzemního podlaží. Vzhledem k charakteru vějíře PIR elementu, který dosahuje až 12 m do dálky pod úhlem 85°, si vystačím s jedním PIR do každé místnosti. Pouze v kanceláři 1 musím použít dva PIR, abych předešel „mrtvým zónám“.



Obrázek 5. PIR detektor OPTEX
RX40QZD [16]



Obrázek 6. PIR charakteristika
OPTEX RX40QZD [16]

2. nadzemní podlaží – zabezpečená oblast a jednací oblast **TAJNÉ**

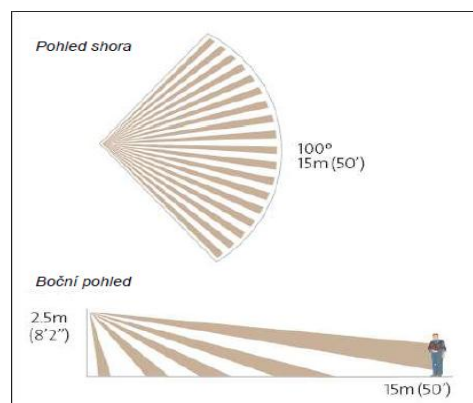
Podmínkou při výběru detektoru do uvedené zabezpečené oblasti byl především dostatečný dosah a odpovídající úhel pro detekci pohybu, který zajistí pokrytí celé plochy místnosti. Detektor by měl mít funkci antimasking a splňovat požadavky NBÚ na certifikaci výrobku.

Pro zabezpečení kanceláře 1, přes kterou je umožněn další postup neoprávněné osobě do ostatních kanceláří a do jednací oblasti, jsem použil PIR detektor od firmy RISCO typ RK800Q - G3. Tento detektor odpovídá požadavku na stupeň bezpečnosti 3. Výhodou tohoto typu detektoru je 2x dvojitý pyroelement, který umožňuje detekci 12 m do dálky v úhlu 100°. Abych dosáhl kompletního pokrytí kanceláře 1, musím zde umístit ještě stropní duální detektor od stejné firmy typ RK150DT – G3. Při výšce stropu 2,8 m je charakter detektoru kruh o průměru 8 m, který mi stačí pro pokrytí zbývajících prostorů kanceláře.

Pro zabezpečení všech ostatních kanceláří, včetně jednací oblasti si vystačím s jedním detektorem RK800Q - G3 na místnost.



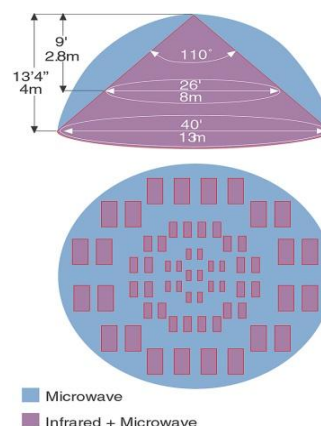
Obrázek 7. PIR detektor RISCO
RK800Q - G3 [16]



Obrázek 8. PIR charakteristika
RK800Q - G3 [16]



Obrázek 9. Duální PIR + MW
RISCO RK150DT – G3 [16]



■ Microwave

■ Infrared + Microwave

Obrázek 10. PIR + MW
charakteristika RK150DT – G3

8.1.5.2 Plášťová ochrana

Abych dodržel požadavky NBÚ na zabezpečení zabezpečených a jednacích oblastí je podmínkou použití plášťové ochrany. Rozsah použití je opět závislý na stupni zabezpečení pro jednotlivé kategorie. Plášťová ochrana představuje především magnetické kontakty do oken a obvodových dveří a ochranu skleněných ploch proti rozbití použitím detektorů tříštění skla.

1. nadzemní podlaží – zabezpečená oblast **DŮVĚRNÉ**

Magnetické kontakty jsem vybral pro stupeň zabezpečení 2 od firmy ASITA typ MAS273. Jedná se o plastový magnetický kontakt, který má dvě relé pro připojení do ústředny PZTS a zároveň do jiné technologie např. kontroly přístupu. Magnetické kontakty jsou umístěny ve všech oknech, balkonových dveřích a interiérových dveřích.

Detektory tříštění skla použiju do všech prostor zabezpečené oblasti. Z nabídky certifikovaných detektorů jsem vybral typ FG730 od výrobce HONEYWELL, který nabízí dosah až 9m. Detektor je schopen detekovat tříštění všech typů skel.



Obrázek 11. Magnetický kontakt
ASITA MAS273 [16]



Obrázek 12. Detektor tříštění
skla HONEYWELL FG730 [16]

2. nadzemní podlaží – zabezpečená oblast a jednacích oblast **TAJNÉ**

Pro druhé nadzemní podlaží jsem vybíral magnetické kontakty, které splňují požadavky NBÚ pro bodovou hodnotu $SS91 = 3$. K zabezpečení oken a interiérových dveří jsem použil výrobek od stejné firmy jako v 1. nadzemním podlaží, ale tentokrát typ MAS303, který přidává ochranu proti cizím magnetickým polím.

Detektorem tříštění skla zabezpečuju všechny prosklené plochy v 2. nadzemním podlaží. Použil jsem typ FG 1625TAS od výrobce HONEYWELL. Tento typ detektoru má maximální dosah 7,6 m a je možné jej připevnit jak na strop, tak na stěnu a splňuje certifikační předpoklady NBÚ.

8.1.5.3 Sabotážní ochrana

Ochrana jednotlivých komponent systému vůči nedovolené manipulaci, je zajištěna ochrannými spínači jednotlivých prvků (tamper). Všechny propojovací krabičky budou vybaveny také tamper kontakty. V rámci použití koncentrátorů s dvojitým vyvážení smyček je možné detekovat také sabotáž (přerušení, zkratování) vedení. Všechny prvky sabotážní ochrany jsou přiřazeny do 24h smyčky, zaznamenání sabotáže bez ohledu na stav systému.

8.1.6 Tísňový systém

Abych dodržel požadavky na fyzickou bezpečnost ochrany utajovaných informací podle kritérií NBÚ, je nutné použít do zabezpečené oblasti kategorie TAJNÉ prvky tísňové ochrany. Tento systém bude reprezentovat tísňové NC/NO výklopné tlačítko s pamětí poplachu a stíněným relé typ S3040/SR od výrobce SENTROL. Tísňový systém jsem umístil do nejkritičtějších míst a to do servrovy hosting centra a do jednacích místností.

8.1.7 Ovládání systému

Ovládání systému je zajištěno LCD klávesnicí K641 umístěnou v zádveří vchodových dveří do objektu. Její výhodou je LED indikace stavu, 1 zóna a 1 PGM. Pro každé podlaží zabezpečené oblasti použiju jednu klávesnici.



Obrázek 13. Tísňové tlačítko
S3040 [16]



Obrázek 14. Ovládací klávesnice
Paradox K641 [15]

8.1.8 Ohlašování poplachu a komunikace

Hlášení poplachu se může uskutečnit dvěma způsoby, pomocí výstražného signalizačního zařízení nebo pomocí poplachového přenosového systému.

- a) **Výstražné signalizační zařízení** reprezentuje venkovní akusticko-optická siréna TEKNIM – 720WR umístěn ve 2. nadzemním podlaží z jižní strany objektu. Siréna pracuje v režimu SAB, kdy při poplachu odebírá potřebný proud z AUX a baterie slouží jako případná záloha. Pro venkovní prostředí je umístěna do krytu IP44.



Obrázek 15. Akusticko-optická siréna TEKNIM – 720WR [17]

- b) **Poplachový přenosový systém** je zajištěn použitím GSM komunikátoru PCS200 pro ústředny PARADOX. GSM brána je schopna zajistit přenos kódovaných datových formátů ústředny na PPC v hlasovém pásmu GSM nebo GPRS. Komunikátor je schopný posílat uživateli SMS zprávy s identifikací poplachů na konkrétní zóně a přijímat zprávy pro uživatelské ovládání ústředny.



Obrázek 16. GSM komunikátor PCS200 [15]

Komunikace mezi ústřednou a uživatelem, popřípadě se servisním technikem je realizována pomocí ethernetového modulu IP 100, který umožňuje přístup a monitoring zabezpečovacího systému pomocí webového rozhraní nebo servisního software WinLoad. Zabezpečení komunikace je provedeno šifrou AES 256bit, MD5 a RC4.

8.1.9 Způsob vedení tras kabeláže

Abych zjistil potřebnou kabeláž pro celý systém, musím provést výpočet úbytku napětí na jednotlivých větvích. Napěťové poměry na vedení vychází z odporu vedení, který je dán použitým vodičem a z odebíraného proudu. Výpočet se provádí použitím Ohmova zákona.

Označení větve	ϕ [mm]	L [m]	R [Ω]	I_{\max} [A]	$U_{\Delta} = R \cdot I_{\max}$ [V]	$U_{\text{AUX}} = 13,8 - U_{\Delta}$ [V]	$U_{\text{BATERIE}} = 12 - U_{\Delta}$ [V]
Sběrnice 1	4x0,5	28,50	2,28	0,51	1,17	12,63	10,83
Sběrnice 2	4x0,5	30,00	2,40	0,30	0,72	13,08	11,28
Servrovna, 1. NP	4x0,22	5,50	1,10	0,01	0,01	13,79	11,99
Kancelář 2, 1. NP	4x0,22	20,50	4,10	0,04	0,15	13,65	11,85
Kancelář vedoucí, 1. NP	4x0,22	26,50	5,30	0,04	0,19	13,61	11,81
Kancelář 3, 1. NP	4x0,22	25,00	5,00	0,04	0,18	13,62	11,82
Kancelář 1	4x0,22	16,00	3,20	0,05	0,15	13,65	11,85
Kancelář 2, 2. NP	4x0,22	2,00	0,40	0,04	0,02	13,78	11,98
Jednací místnost, 2. NP	4x0,22	15,00	3,00	0,06	0,18	13,62	11,82
Kancelář 3, 2. NP	4x0,22	21,50	4,30	0,11	0,46	13,34	11,54
Servrovna host. centra, 2. NP	4x0,22	20,00	4,00	0,06	0,24	13,56	11,76

Tabulka 11. Hodnoty úbytku napětí na kabeláži

Kabeláž adresovatelné čtyřvodičové sběrnice a venkovní sirény bude natažena kabelem SYKFY 4x0,5. Pro propojení ostatních prvků postačuje kabel SYFK 4x0,22 nebo 4x0,5. Pro vedení střídavého napětí 230V/50 Hz použiju kabel CYKY 3x1,5.

Kabely jsou vedeny ve stěnách v ohebných elektroinstalačních PVC trubkách. V místech odbočení jsou použity propojovací krabíčky. Kabeláž k magnetickým kontaktům oken a dveří bude vedena ve vkladací liště.

8.1.10 Napájení a zálohování napájení

Systém PZTS bude napájen ze samostatně jištěných vývodů 230V/10A. Systém napájení a zálohování napájení by měl splňovat požadavky ČSN EN 50 131 – 1 [11] na dobu zálohování 60 hodin pro typ napájení A, kdy je energie dodávána z vnějšího zdroje (např.

sítě) a v případě jeho výpadku je energie dodávána z dobíjecího náhradního zdroje (akumulátor), který je automaticky dobíjen z vnějšího zdroje energie.

Pro výpočet kapacity záložního akumulátoru **KNZ** [Ah] použiju Rovnice 1. Abych mohl provést výpočet, musím určit proud systému odebíraný v klidovém stavu I_k [A], proud systému odebíraný při poplachu I_p [A] a dobu provozu na náhradní zdroj T [h].

$$KNZ = (T - 0,25) \cdot I_k + 0,25 \cdot I_p$$

Rovnice 1. Výpočet kapacity záložního akumulátoru

Před tím než spočítáme potřebný výkon zdroje, musíme nejprve určit nabíjecí proud akumulátoru I_D [A]. Toho dosáhneme použitím následující rovnice, kde **KNZ** [Ah] představuje kapacitu záložního akumulátoru, **0,8** je 80% jmenovité hodnoty napětí akumulátoru a 24 je maximální doba dobíjení na min. 80% kapacity.

$$I_D = (KNZ \cdot 0,8) \div 24$$

Rovnice 2. Dobíjecí proud akumulátoru

Nyní můžu spočítat potřebný výkon základního zdroje P_z [VA], použitím následující rovnice, kde U je jmenovité napětí 13,8 V, proud systému odebíraný při poplachu I_p [A] a nabíjecí proud akumulátoru I_D [A].

$$P_z = U \cdot (I_p + I_D)$$

Rovnice 3. Výkon základního zdroje

a) Výpočet výkonu základního zdroje a kapacity akumulátoru pro ústřednu

	Prvek PZTS	Typ	Počet	I_k [mA]	I_p [mA]
Výstup	ústředna	Digiplex EVO 192	1	110	110
Ústředna AUX max. 700 mA	detektor PIR	RK 800Q	3	36	117
	detektor tříštění skla	FG 1625TAS3	2	26	44
	klávesnice	K641	2	160	240
	tísňový hlásič	S 3040/SR	1	0	8
	expander 1	APR3 ZX8	1	29	31
	detektor PIR	RK 800Q	2	24	78
	duální PIR + MW stropní	RK 150DT	1	12	39
	tísňový hlásič	S 3040/SR	1	0	8
	detektor tříštění skla	FG 1625TAS3	2	26	44
Celkový proud				423	719

Tabulka 12. Velikost proudového odběru na výstupu ústředny PZTS

Po dosazení do rovnic jsem získal kapacitu akumulátoru **25,45 Ah**, nejbližší vyšší je **26 Ah**. Základní zdroj musí napájet i venkovní akustickou sirénu, která má při poplachu proudový odběr 450 mA. Výkon základního zdroje podle Rovnice 3 je **28,08 VA**, aby zdroj zvládl proudový odběr až 2 A, použiju **80 VA**. Siréna má vlastní baterii, která nezatěžuje baterii ústředny, výpočtem **0,41 Ah**, nejbližší vyšší je **1,3 Ah**.

b) Výpočet výkonu základního zdroje a kapacity akumulátoru pro komunikační zařízení

Výstup	Prvek PZTS	Typ	Počet	I_k [mA]	I_p [mA]
Ústředna SERIAL port	modul LAN/internet	IP MODUL 100	1	110	110
Ústředna SERIAL port	GSM komunikátor	PCS200 GSM/GPRS	1	60	600
Celkový proud				170	710

Tabulka 13. Velikost proudového odběru komunikačních zařízení

Po dosazení hodnot do příslušného vzorce získám vypočtenou hodnotu akumulátoru pro modul LAN i GSM komunikátor, vypočtená hodnota je **10,33 Ah**, nejbližší vyšší je **12 Ah**. Aby komunikátor s modulem nezatěžovali zdroj ústředny, zvolil jsem pro ně doplňkový zdroj PS 817 1,75A / 13,8V který je připojen do společného transformátoru ústředny.

c) Výpočet výkonu základního zdroje a kapacity akumulátoru pro expandéry 2,3

Výstup	Prvek PZTS	Typ	Počet	I_k [mA]	I_p [mA]
EX2 AUX	expander 2	APR3 ZX8	1	29	31
	detektor PIR	RX 40QZD	3	24	33
	detektor tříštění skla	FG 730	2	50	50
EX3 AUX	expander 3	APR3 ZX8	1	29	31
	detektor PIR	RX 40QZD	3	24	33
	detektor tříštění skla	FG 730	2	50	50
Celkový proud				206	228

Tabulka 14. Velikost proudového odběru na expandérech ústředny

Pro expandéry je nutné použít samostatný přídatný zdroj PS 817. V případě napájení z ústředny by došlo k překročení maximálního proudu z výstupu AUX, který je 700 mA. Oba expandéry by měli být podle výpočtu zálohovány baterií **12,35 Ah**, nejbližší vyšší je **18 Ah**. Přídatný zdroj je napojen do transformátoru 230/16V **20VA**, který zajistí dostatečný výkon pro celou část PZTS.

d) Výpočet výkonu základního zdroje a kapacity akumulátoru pro přístupové moduly

Prvek PZTS	Typ	Počet	I_k [mA]	I_p [mA]
přístupový modul	ACM 12	1	80	80
bezkontaktní čtečka	R870	1	39	65
elektromechanický zámek	ABLOY EL460	1	130	400
Celkový proud			249	545

Tabulka 15. Velikost proudového odběru pro jeden přístupový systém

Každý přístupový modul, který napájí jednu čtečku, jeden magnetický kontakt a jeden elektromechanický zámek musí mít svůj akumulátor. Podle výpočtu potřebuje jeden modul **15 Ah**, nejbližší vyšší je **18 Ah**. Výhodou přístupového modulu ACM 12 je možnost sdílet transformátor pro více přístupových modulů. Celkový odběr proudu při množství 3 moduly v jednom podlaží a jejich příslušenství je až 3,43 A, proto je nutné použít dostatečně dimenzované trafo, které mi výpočtem vyšlo **47,4 VA**, přesto použiju nejlépe **80 VA**.

8.1.11 Nastavení systému

Zabezpečovací a tísňový systém bude pracovat v základním dělení na 6 podsystémů.

- a) **1. Podsystém** – tento podsystém se vztahuje k prvnímu nadzemnímu podlaží a je jí místnost kancelář vedoucího, která je rozdělena do 4 zón. Zastřežení a odstřežení podsystému se provádí pomocí čtecího zařízení a přístupové karty a k nim přiřazených práv pro přístup.

Podsystém	Místnost	Číslo zóny	Prvek	Typ zóny
1	Kancelář vedoucí	1	magnetický kontakt oken	Okamžitá
1	Kancelář vedoucí	2	magnetický kontakt balk. dveří	Okamžitá
1	Kancelář vedoucí	3	PIR detektor	Okamžitá
1	Kancelář vedoucí	4	detektor tříštění skla	24h

Tabulka 16. Podsystém 1

- b) **2. Podsystém** – vztahuje se k prvnímu podlaží a její místnost servrovna. Podsystém tvoří jedna zóna, zastřežení a odstřežení podsystému je stejné jako v předchozím případě.

Podsystém	Místnost	Číslo zóny	Prvek	Typ zóny
2	Servrovna	5	PIR detektor	Okamžitá

Tabulka 17. Podsystém 2

- c) **3. Podsystem** – vztahuje se k prvnímu podlaží a spadají sem místnosti kancelář 1 až 3. Zastřežení a odstřežení podsystemu se provádí u vstupu do objektu pomocí čtecího zařízení a přístupové karty. Podsystem je možné zastřežit a odstřežit použitím ovládací klávesnice v zádveři vstupu do objektu.

Podsystem	Místnost	Číslo zóny	Prvek	Typ zóny
3	Kancelář 1	6	PIR detektor	Zpožděná
3	Kancelář 1	7	PIR detektor	Zpožděná
3	Kancelář 1	8	detektor tříštění skla	24h
3	Kancelář 1	9	magnetický kontakt oken	Okamžitá
3	Kancelář 2	10	PIR detektor	Okamžitá
3	Kancelář 2	11	magnetický kontakt dveře	Okamžitá
3	Kancelář 2	12	magnetický kontakt okna	Okamžitá
3	Kancelář 2	13	detektor tříštění skla	24h
3	Kancelář 3	14	detektor tříštění skla	24h
3	Kancelář 3	15	PIR detektor	Okamžitá
3	Kancelář 3	16	magnetický kontakt dveře	Okamžitá
3	Kancelář 3	17	magnetický kontakt balk. dveří	Okamžitá
3	Kancelář 3	18	magnetický kontakt okna	Okamžitá

Tabulka 18. Podsystem 3

- d) **4. Podsystem** – vztahuje se ke druhému nadzemnímu podlaží. Je tvořen místností servrovna hosting centra. Zastřežení a odstřežení podsystemu se provádí pomocí čtecího zařízení a přístupové karty a k nim přiřazených práv pro přístup.

Podsystem	Místnost	Číslo zóny	Prvek	Typ zóny
4	Servrovna hosting centra	19	magnetický kontakt oken	Okamžitá
4	Servrovna hosting centra	20	PIR detektor	Okamžitá
4	Servrovna hosting centra	21	tísňové tlačítko	24h
4	Servrovna hosting centra	22	detektor tříštění skla	24h

Tabulka 19. Podsystem 4

- e) **5. Podsystem** - vztahuje se ke druhému nadzemnímu podlaží. Je tvořen jednací a zasedací místnostní. Zastřežení a odstřežení podsystemu se provádí pomocí čtecího zařízení a přístupové karty a k nim přiřazených práv pro přístup.

Podsystém	Místnost	Číslo zóny	Prvek	Typ zóny
5	Jednací a zasedací	23	PIR detektor	Okamžitá
5	Jednací a zasedací	24	detektor tříštění skla	24h
5	Jednací a zasedací	25	magnetický kontakt oken	Okamžitá

Tabulka 20. Podsystém 5

- f) **6. Podsystém** – je realizován v druhém podlaží a tvoří ho 3 místnosti kancelář 1, kancelář 2 a kancelář 3. Zastřežení a odstřežení podsystému se provádí u vstupu do objektu pomocí čtecího zařízení a přístupové karty. Podsystém je možné zastřežit a odstřežit použitím ovládací klávesnice v zádveří vstupu do objektu.

Podsystém	Místnost	Číslo zóny	Prvek	Typ zóny
6	Kancelář 1	26	duální PIR+MW detektor	Zpožděná
6	Kancelář 1	27	PIR detektor	Zpožděná
6	Kancelář 1	28	detektor tříštění skla	24h
6	Kancelář 1	29	magnetický kontakt oken	Okamžitá
6	Jednací a zasedací	30	tísňové tlačítko	24h
6	Kancelář 2	31	PIR detektor	Okamžitá
6	Kancelář 2	32	magnetický kontakt dveře	Okamžitá
6	Kancelář 3	33	PIR detektor	Okamžitá
6	Kancelář 3	34	detektor tříštění skla	24h
6	Kancelář 3	35	magnetický kontakt okna	Okamžitá
6	Kancelář 3	36	magnetický kontakt dveře	Okamžitá

Tabulka 21. Podsystém 6

8.2 Integrovaný přístupový systém

Požadavky na přístupový systém v rámci fyzické ochrany utajovaných informací jsou uvedeny v příloze č. 1. k vyhlášce č. 528/2005 Sb. Abych dodržel minimální bodovou hodnotu nejnižší míry zabezpečení, realizuju systém kontroly vstupu typ 3, který musí být certifikovaný NBÚ a splňuje požadavky podle ČSN EN 50 133 – 1. [13]

Výhodou ústředny PZTS PARADOX EVO 192 je možnost rozšíření o různé druhy modulů. Při hledání vhodného přístupového systému, který by vyhovoval požadavkům na třídu přístupu B a třídu identifikace 2 jsem vybral modul kontroly přístupu DGP – ACM12.

8.2.1 Přístupový modul

Modul přístupu je připojen na sběrnici ústředny DIGIPLEX EVO192 a je umístěn podle výkresové dokumentace. Jeden modul slouží k vytvoření jednoho přístupového bodu použitím jedné čtečky, jednoho detektoru (magnetický kontakt nebo PIR detektor) pro

monitorování průchodu dveřmi, relé výstup na otvírání dveřního zámku a napájecí zdroj. Modul podporuje připojení čteček s výstupem WIEGAND 26bit a čteček s výstupem RS485 PARADOX. V jednom boxu je uložen přístupový modul, baterie a transformátor, který může být společný pro více modulů ACM 12.

Základní údaje modulu	Hodnota
Adresace modulu v systému	jedinečné číslo SN
Vstup pro čtečku	ano, 1 vnitřní/venkovní čtečku RS485
Rozhraní pro čtečky jiných výrobců	Wiegand 26 bit
Napájení	16 V~, 40 VA
Napájení	jeden transformátor pro více modulů
Max, proudový odběr z AUX výstupu	1A
Typ AUX výstupu	elektronická vratná pojistka 1,1 A
Dobíjecí proud záložního akumulátor	350/700 mA
Doporučený záložní akumulátor	12 V, 7 Ah/18 Ah
Proudový odběr modulu	max. 80 mA
Počet vstupů/zón	2, zóna CT (magnet), REX (detektor)
Tamper vstup	ano, NC tamper modulu
Programovatelný výstup PGM	ano, 1 x tranzistor 50 mA
Výstup pro otvírání dveřního zámku	ano, 1 x relé
Typ zdroje	spínaný

Tabulka 22. Modul přístupového systému [15]



Obrázek 17. Přístupový modul DGP – ACM12 [15]

8.2.2 Čtecí zařízení a přístupová karta

Pro čtení přístupových medií jsem použil bezkontaktní čtečku PARADOX R870. Tato čtečka podporuje formát WIEGAND 26 nebo 32bit.

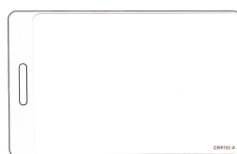
Pokud je čtečka připojena na napětí, začne její anténa nepřetržitě vysílat elektromagnetické budící pole. V okamžiku, kdy se karta vloží do tohoto pole, indukuje anténa toto pole a energii získanou indukcí napájí vnitřní obvody karty. Karta odvysílá svoje identifikační

číslo čtečky a ta vyhodnotí, zda se jedná o vysílání v korektním formátu. Pokud byl formát dat vyhodnocen jako správný, dojde ke zpracování a odeslání dat z čtečky do modulu, do kterého je připojena. Modul po sběrnici BUS pošle data do ústředny a ta vyhodnotí, zda karta má oprávnění k požadované akci.



Obrázek 18. Čtečka karet R870 [15]

Karta je přiřazena konkrétnímu uživateli, který její pomocí ovládá systém podle nastavení práv. Přiložením karty je možné otevírat dveře, vypínat a zapínat pod systémy. Uživatel může používat pouze jednu kartu.



Obrázek 19. Přístupová karta R207 [15]

8.2.3 Dveřní kontakt a elektromechanický zámek

Dveřní kontakt je v provedení magnet a je zapojen do vstupu čtečky zóna Z1 (CT). Detekuje otevření dveří a deaktivuje dveřní zámek. V případě, že je zařazena do ústředny PZS chová se jako 24h zóna a při neoprávněném vstupu vyvolá poplach. Neoprávněný vstup je otevření dveří bez přiložení karty.

Elektromechanický zámek bude použit od firmy ABLOY EL 460, který je vhodný pro vnitřní i venkovní rámové dveře. Tento typ zámku je samozamykacího charakteru, kdy při každém zavření dveří se automaticky vysune závora zámku. Zámek může být ovládán výstupním kontaktem ze čtečky karet, klávesnice atd. Zámek je vždy možné odemknout cylindrickou vložkou z obou stran dveří nebo stiskem kliky z vnitřní strany dveří – antipanic funkce. Použitý elektromechanický zámek splňuje bezpečnostní třídu 3 a bodové

hodnocení technického prostředku NBÚ SS4 = 2. Napájení zámku je jednotné 12 – 24 V DC a klidová spotřeba je 130 mA, maximální 400 mA



Obrázek 20. Elektromechanický zámek EL 460 [18]

8.2.4 Nastavení přístupu

- a) **Vstup kartou** – přiložením karty je aktivován dveřní zámek, aktivace je omezena dobou aktivace nebo ukončena rozpojením / sepnutím dveřního kontaktu.
- b) **Vstup s kartou s vypnutím podsystému** – přiložením karty dojde k vypnutí podsystému a k aktivaci dveřního zámku.
- c) **Násilné otevření dveří** – vyhlášení poplachu při narušení dveřního kontaktu bez předchozího přiložení karty.
- d) **Odchod klika / koule** – dveře se otevrou klikou a lze je otevřít pouze ze strany kliky, z vnější strany jsou dveře vybaveny koulí – v tomto případě nelze magnetický kontakt zařadit do hlídání.
- e) **Odchod a zapnutí podsystému kartou** – po uzavření dveří se ke čtečce přiloží dvakrát karta s intervalem 5s a dojde k zapnutí podsystému.
- f) **Přístup** – uživatel má nastaveno, do které skupiny dveří a s jakým časovým intervalem má přístup povolen.
- g) **Ukládání do historie** – odchod pomocí tlačítka nebo detektoru, poplach nezavřeno, násilně otevřeno.

Software NEWARE ACCES umožňuje kompletní správu přístupového modulu – programovat přístup, zadávat a mazat karty, stahovat historii, filtrovat události podle konkrétního uživatele, dveří, událostí, nastavovat časové rozvrhy.

8.3 Elektrická požární signalizace

Nutnost instalace elektrické požární signalizace vychází z normy ČSN 73 0875 Požární bezpečnost staveb – Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení. Podle části 4.2.1d) a 4.2.1e) této normy právní předpisy ani normativní požadavky nepožadují instalaci EPS. [14]

Výpočet v jakých objektech a prostorách musí být instalováno EPS, lze zjistit z rovnice nutnosti střežení požárního úseku, kde N je bezrozměrné číslo, j je součinitel charakteru posuzovaného prostoru, a_n součinitel pro nahodilé požární zatížení, o_s součinitel ohrožení osob, o_h součinitel ohrožení hodnot, o_v součinitel provozních vlivů. [9]

$$N = (j \cdot a_n + o_s \cdot o_h) \cdot o_v = (1,7 \cdot 1 + 0,9 \cdot 0,6) \cdot 1,25$$

Rovnice 4. Nutnost střežení požárního úseku

Po dosazení hodnot do vzorce jsem získal výsledek $N = 2,8$. V případě že je $N < 3$ nemusí být EPS instalována. Národní bezpečnostní úřad ale stanovuje podmínku instalace zařízení elektrické požární signalizace pro zabezpečené a jednací oblasti kategorie TAJNÉ a vyšší, proto musím realizovat EPS pro druhé nadzemní podlaží budovy.

8.3.1 Ústředna EPS

Pro druhé nadzemní podlaží je navržen analogový systém s certifikovanou ústřednou APOLLO F2 od výrobce NSC. Ústředna EPS je umístěna v druhém nadzemním podlaží v místnosti kancelář 2, která odpovídá hodnotě $a_n = 1$. Stupeň krytí ústředny IP = 42. Na analogovou hlásicí linku je připojeno sedm automatických hlásičů kouře optických nebo multisenzorových a tři tlačítkové hlásiče v místnostech servovna hostingového centra, jednací a zasedací místnost a kancelář 1. Všechny použité hlásiče jsou adresovatelné. Kompletní uspořádání je naznačeno v blokovém schématu ústředny ve výkresové dokumentaci. Ústředna komunikuje s PPC pomocí zařízení dálkového přenosu, z tohoto důvodu zde není vyžadována stálá obsluha ústředny.

Základní údaje ústředny EPS	Hodnota
Napájení	230 V AC, 50 Hz
Výstupní napětí	24 V DC
Odběr v klidu	100 mA
Počet hlásičů + sirén na smyčku	126
Doporučený linkový kabel	JY-(ST)Y 2x2x0,8 / až 3 km

Tabulka 23. Základní technické parametry ústředny EPS [19]

8.3.2 Způsob detekce požáru

Automatické hlásiče budou umístěny v prostoru podle výkresové dokumentace. Rozmístění a počet automatických hlásičů je posouzeno zvlášť pro každý prostor objektu. Společný charakter pro všechny prostory objektu je výška stropu v místnosti 2,8 m a jeho rovinný charakter s úhlem svíraným s vodorovnou rovinou stavby a stropem do 15°. Celková plocha chráněných prostor je přibližně 230 m². Maximální hlídaná plocha pro jeden kouřový hlásič je při výšce stropu do 6 m, 60 m².

Umístění tlačítkových hlásičů je realizováno ve třech místech objektu, vždy v zádveři konkrétních místností ve výšce 1,3 m nad podlahou.

Místnost	Plocha [m ²]	Druh hlásiče	Počet hlásičů
Kancelář 2	13,5	automatický kouřový multisenzorový	1
Jednací a zasedací	29,25	automatický kouřový multisenzorový, tlačítkový	2
Kancelář 1	113,6	automatický kouřový optický a multisenzorový, tlačítkový	4
Kancelář 3	40,47	automatický kouřový multisenzorový	1
Servrova hosting centra	32,4	automatický kouřový multisenzorový, tlačítkový	2

Tabulka 24. Rozdělení hlásičů požáru do místností

- Automatický hlásič kouřový** – typ hlásiče XP 95, dodává se s obyčejnou paticí nebo s paticí s izolátorem, tento hlásič se vyrábí s krytím IP 43,
- Automatický hlásič multisenzorový** – typ hlásiče XP95, kombinace optického a teplotního senzoru, krytí IP 43,
- Tlačítkový hlásič** – povrchový s izolátorem, krytí IP 53.

Číslo hlásící linky	Číslo skupiny hlásiče	Druh hlásiče
1	1	automatický kouřový multisenzorový
1	2	tlačítkový
1	3	automatický kouřový optický

Tabulka 25. Rozdělení hlásičů do hlásící linky a skupiny

8.3.3 Signalizace poplachu

Poplach bude signalizován jednostupňově, bude vyhlášen všeobecný poplach a zároveň bude uskutečněn přenos pomocí ZDP na PPC. Všeobecný poplach bude signalizován akusticky pomocí sirény umístěné v kanceláři 1.

Přenos na PPC zajistí radiový objektový vysílač RADOM STX 23, který je určen pro komunikaci s ústřednou EPS. Oba tyto systémy spolu komunikují pomocí sériového rozhraní RS232.

8.3.4 Vedení kabeláže

Pro linkový rozvod EPS jsou navrženy kabely samozhášivé J-Y(St)Y 2x2x0,8 mm, které jsou doporučeny výrobcem EPS. Kabely pro ovládání požárně bezpečnostních zařízení musí být v provedení zajišťujícím jejich funkčnost při požáru. Pro spojení se sirénou bude použit bezhalogenový kabel JE-H(St) H E30/60 1x2x0,8 mm s omezenou funkčností minimálně 30 minut. Kabelová vedení budou uložena v trubkách pod omítkou nebo na povrchu v pevných trubkách.

Druh kabelu	Typ kabelu	Délka hlásicí linky [m]	Odpor smyčky [Ω /m]	Celkový odběr prvků na lince [A]
samozhášivý	J-Y(St) Y 2x2x0,8 mm	57,8	0,0732	0,105

Tabulka 26. Vedení hlásicí linky EPS

Druh kabelu	Typ kabelu	Délka smyčky [m]	Odpor smyčky [Ω /m]	Celkový odběr prvků na lince [A]
ohniodolný	JE -H(St)H 1x2x0,8 mm	3,4	0,0732	max. 0,035

Tabulka 27. Vedení smyčky pro signalizaci poplachu sirénou

8.3.5 Napájení a zálohování napájení

Systém EPS bude napájen ze samostatně jištěných vývodů 230V/10A. Ústředna disponuje vlastním zdrojem napájení umístěným v krytu ústředny. Provozní napětí ústředny je 24 DC. Záložní napájecí zdroj musí udržet systém ve funkci alespoň 72 hodin při výpadku hlavního zdroje napájení. Pro výpočet kapacity záložního akumulátoru použiju stejný vzorec jako v kapitole 8.1.10. Výsledná kapacita záložního akumulátoru vyšla **7,9 Ah**, nejbližší vyšší je **12 Ah**. Akumulátor je uložen ve stejném krytu s ústřednou. Maximální proudový odběr systému je pouze 0,14 A, odpor hlásicí linky při vzdálenosti 57,8 m je **4,22 Ω** .

8.4 Mechanické zábranné systémy

Pro ukládání utajovaných informací ve formě tištěných dokumentů nebo kompaktních disků použiju skříňové trezory, které odpovídají certifikačním požadavkům NBÚ a splňují bezpečnostní třídu pro danou zabezpečenou oblast.

Zabezpečenou oblastí byl zvolen typ 2, proto použiju pro zabezpečení oken, dveří a uzávěrů mechanické zábranné prostředky bezpečnostní třídy 2 nebo vyšší abych dodržel minimální bodovou hodnotu ZO.

8.4.1 Zabezpečená oblast kategorie Důvěrné

Jelikož jsem v této zabezpečené oblasti navrhl systém kontroly vstupu, musím použít vhodné a certifikované bezpečnostní dveře, elektromechanický zámek, bezpečnostní kování a cylindrickou vložku. Jako dodavatele bezpečnostních dveří jsem zvolil firmu SHERLOCK, jejíž certifikované výrobky jsou přímo vyráběné pro kombinaci s elektromechanickým zámkem od firmy ASSA ABLOY.

Pro vstupy do místností kde, nebude realizován přístupový systém, jsem zvolil bezpečnostní dveře od stejného výrobce jako v případě dveří pro kontrolu vstupu. Uzamykací systém tvoří bezpečnostní souprava od firmy FAB.

Pro ochranu oken jsem zvolil certifikovaný uzamykací systém od firmy ADLO, který je možné nainstalovat na stávající plastová okna a balkonové dveře v objektu.

Pro ukládání utajovaných informací jsem zvolil skříňový trezor od firmy PROFIKON.

Druh MZS	Výrobce	Typ	Bezpečnostní třída	NBÚ	Počet
Bezpečnostní dveře pro kontrolu vstupu	Sherlock	F6/2 Abloy	2	SS3 = 2 SS4 = 1	5
Elektromechanický zámek	ASSA ABLOY	ABLOY EL 460	3	SS4 = 2	5
Bezpečnostní kování	ASSA ABLOY	IKON SX48	4	SS4 = 3	5
Cylindrická vložka	FAB	CONTROL	3	SS4 = 2	5
Zárubně	Sherlock	CG6			5

Tabulka 28. Bezpečnost dveří pro kontrolu vstupu

Druh MZS	Výrobce	Typ	Bezpečnostní třída	NBÚ	Počet
Bezpečnostní dveře klasické	Sherlock	F6/2 PLUS	2	SS3 = 2 SS4 = 1	2
Zadlabávací zámek	MUL -T- LOCK		2	SS4 = 1	2
Bezpečnostní kování	FAB	S1/90	3	SS4 = 2	2
Cylindrická vložka	FAB	2018N	3	SS4 = 2	2
Zárubně	Sherlock	CG6			

Tabulka 29. Bezpečnost dveří pro zabezpečenou oblast Důvěrné

Úschovný objekt	Výrobce	Typ	Bezpečnostní třída	NBÚ	Počet
Skříňový trezor	Profikon	Neptun	0	SS1 = 2 ; SS2=2	1

Tabulka 30. Úschovný objekt pro zabezpečenou oblast Důvěrné

Druh MZS	Výrobce	Bezpečnostní třída	Počet
Zabezpečení oken	Adlo	3	12

Tabulka 31. Uzamykací systém oken



Obrázek 21. Bezpečnostní zamykání oken ADLO [20]

8.4.2 Zabezpečená oblast Tajné

Zabezpečení mechanickými zabranými systémy pro tuto kategorii je v podstatě totožné pouze se liší třídou bezpečnosti a u dveří počtem jisticích bodů, kterými jsou dveře zajištěny v zárubni. Dveře pro kontrolu vstupu a zabezpečení oken jsou totožné v obou podlažích.

Druh MZS	Výrobce	Typ	Bezpečnostní třída	NBÚ	Počet
Bezpečnostní dveře klasické	Sherlock	F6/3	3	SS3 = 3 SS4 = 2	2
Zadlabávací zámek	MUL -T- LOCK		3	SS4 = 2	2
Bezpečnostní kování	FAB	S1/90	3	SS4 = 2	2
Cylindrická vložka	FAB	2018N	3	SS4 = 2	2
Zárubně	Sherlock	CG6			

Tabulka 32. Bezpečnost dveří pro zabezpečenou oblast Tajné

Úschovný objekt	Výrobce	Typ	Bezpečnostní třída	NBÚ	Počet
Skříňový trezor	Profikon	Salvus 1	1	SS1 = 3; SS2=2	1

Tabulka 33. Úschovný objekt pro zabezpečenou oblast Tajné

8.4.3 Zabezpečení jednací oblasti Tajné

Jednací oblast vyžaduje podle požadavků NBÚ použití oken a dveří s ještě vyšší bezpečnostní třídou než je tomu v případě obou zabezpečených místností.

Druh MZS	Výrobce	Typ	Bezpečnostní třída	NBÚ	Počet
Bezpečnostní dveře pro kontrolu vstupu	Sherlock	F6/4 Abloy	4	SS3 = 4 SS4 = 3	1
Elektromechanický zámek	ASSA ABLOY	ABLOY EL 460	3	SS4 = 2	1
Bezpečnostní kování	ASSA ABLOY	IKON SX48	4	SS4 = 3	1
Cylindrická vložka	FAB	DYNAMIC	4	SS4 = 3	1
Zárubně	Sherlock	CG6			1

Tabulka 34. Bezpečnost dveří pro jednací oblast Tajné

Jednací oblast musí být chráněna proti odezírání z míst nacházejících se vně jednací oblasti. K tomuto účelu poslouží certifikovaná bezpečnostní roleta od firmy LIBRAX.

Druh MZS	Výrobce	Typ	Bezpečnostní třída	NBÚ	Počet
Zabezpečení oken - roleta	Librax	RL-P	3	SS3 = 3 SS4 = 2	1

Tabulka 35. Bezpečnostní roleta pro jednací oblast Tajné

8.5 Technická ochrana proti aktivnímu a pasivnímu odposlechu

Jednací oblast pro pravidelné projednávání utajovaných informací stupně utajení Tajné je podle požadavků NBÚ povinné zabezpečit proti pasivnímu a aktivnímu odposlechu certifikovanými technickými prostředky.

- a) **Kontrola radiového spektra** – cílem je odhalit radiové odposlechové prostředky umístěné v chráněném prostoru. Jsou to pásmové automaticky přesaditelné přijímače – lokátory s automatickou detekcí nejsilnějšího signálu. Výchylka měřeného signálu je zobrazena na ručičkovém měřicím přístroji nebo indikací LED diod. Takovým certifikovaným přístrojem je **MRA – 3**, paměťový radiový analyzátor, který pracuje v pásmu od 43 MHz do 2,7 GHz. Jednotlivé signály umí vyladit, poslouchat a změřit jejich kmitočet. Zkontrolované rádiové spektrum, které

neodhalilo žádnou štěnici, je uloženo do paměti a každých 6 sekund porovnávána s aktuálními signály. Přítomnost nového signálu je vyhodnocena poplachovou signalizací.

- b) **Zašumění prostoru** – účelem zašumění je zajistit ochranu prostoru proti odposlechu využívajícího všech forem snímání zvuku z oken, zdí případně i z jiných předmětů pokud útočníkův systém využívá jako průnik do prostoru okna nebo zdi místnosti. Pro zašumění prostoru se použije šumový generátor **SNG**, ke kterému je připojeno 2 – 12 nízkoimpedančních reproduktorů nebo 100 piezokeramických akustických měničů nebo jejich kombinace. Ty jsou potom instalovány na vnitřní strany nábytku, stolů a dalších předmětů.

8.6 Zařízení fyzického ničení nosičů informací

Zařízení fyzického ničení informací typ 3 jsou určena pro ničení utajovaných informací stupně utajení Tajné nebo nižší. Toto zařízení bude instalováno v druhém nadzemním podlaží v blízkosti jednací místnosti. Požadavkem na zařízení typu 3 je zničení informací papírového charakteru, filmu z polyesteru, kovu umělé hmoty nebo identifikační karty. Vybral jsem certifikované zařízení od firmy XERTEC typ INTIMUS 120CC4.



Obrázek 22. Skartovací zařízení INTIMUS 120CC4 [21]

8.7 Bodové porovnání realizovaného a požadovaného zabezpečení

Pro každou zabezpečenou oblast a jednacích oblast stanovím bodové hodnocení opatření fyzické bezpečnosti a porovnáji ji s minimální bodovou hodnotou určenou Národním bezpečnostním úřadem pro jednotlivé kategorie zabezpečených a jednacích oblastí. Konkrétní tabulka pro každou zabezpečenou oblast je umístěna v příloze tři.

8.8 Soupiska použitých prvků

Pro přehlednější orientaci v této práci jsem vytvořil soupisku prvků, která obsahuje druh systému zabezpečení, typ komponenty podle značení výrobce zařízení a počet který je použit. Dále je v soupisce znázorněna jednotková cena a celková cena zabezpečovacího systému podle druhu. Do ceny není započítána kabeláž. Soupiska použitých prvků je umístěna v přílohové části této práce.

ZÁVĚR

Cílem práce bylo realizovat technickou ochranu utajovaných informací podle vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.

Na samém začátku projektu bylo důležité stanovit několik zásadních informací, které se dále projevily v celém návrhu systému zabezpečení. V první řadě bylo nutné určit aktiva společnosti, které je nutné chránit a velikost újmy, která by vznikla při neoprávněné manipulaci s utajovanou informací. V dalších krocích se postupně určila velikost ohrožení, zranitelnost objektu a celková míra rizika v objektu. Na základě těchto informací se mohlo určit bodové hodnocení bezpečnosti pro určený objekt.

V další fázi projektu se stanovil typ objektu, jeho hranice, typ zabezpečené oblasti a jednacích oblastí včetně jejich kategorií a tříd. Neméně důležité bylo zhodnocení původního stavu zabezpečení objektu.

Jakmile jsem určil všechny důležité faktory, mohl jsem přistoupit k samotnému návrhu zabezpečení. Nejdříve jsem si určil stupeň zabezpečení a předpokládaný rozsah střežení podle kategorie zabezpečené oblasti a současně jsem určil třídu prostředí, ve které budou všechny prvky ochrany pracovat. Výběr druhu ochrany závisel na kategorii zabezpečené oblasti. V zabezpečené oblasti 1. NP jsem realizoval PZS, MZS i kontrolu vstupů, v druhém nadzemním podlaží jsem realizoval stejný systém ochrany a navíc elektrickou požární signalizaci. Podle požadavků Národního bezpečnostního úřadu jsem musel do zabezpečené oblasti Tajné navrhnout zařízení fyzického ničení nosičů informací a pro jednacích oblast Tajné zajistit ochranu proti aktivnímu a pasivnímu odposlechu.

Nejdůležitější a zároveň nejproblematictější bylo vyhledat certifikované technické prostředky, které vyhovují danému stupni zabezpečení. To se samozřejmě projevilo na ceně jednotlivých prvků systému. Nejnákladnější byla realizace mechanických zabraných systémů, kde především bezpečnostní dveře a jejich příslušenství zvedlo koncovou cenu do závratných výšek.

Samostatnou kapitolou byl návrh elektrické požární signalizace, která by podle uvedeného výpočtu nemusela být realizována, ale NBÚ ji přesto předepisuje pro zabezpečené oblasti kategorie Tajné. Realizoval jsem proto tento systém do uvedené oblasti, přesto bych doporučil její rozšíření do celého objektu bez ohledu na kategorii zabezpečené oblasti.

ZÁVĚR V ANGLIČTINĚ

The aim was implement the technical protection of classified information pursuant to Decree No. 528/2005 Coll. On physical security and certification of technical equipment, as amended by Decree No. 19/2008 Coll.

At the very beginning of the project was important to provide some essential information, which is also reflected in its security system design. First, it was necessary to determine the company's assets, which must be protected and the size of the harm that would result from the unauthorized use of classified information. The next step is to determine the size gradually threat, vulnerability and building the overall risk level in the building. Based on this information could identify scores of security for the specified object.

In the next phase of the project to determine the type of object, its boundaries, type the security area and meeting area, including the categories and classes. Equally important was to assess the security status of the original object.

Once I set all the relevant factors, I could proceed to the actual security design. First I determine the security level and the expected scope of surveillance by the category secure area while I set the class environment in which all elements of the protection work. Selection of protection depended on the category of protected areas. The secure area 1 NP I realized IAS, MZS and control inputs on the second floor, I realized the same protection system, plus an electric fire alarm. As required by the National Security Bureau, I had to secure the secret to design equipment for physical destruction of media and the secret meeting area to ensure protection against active and passive eavesdropping. The most important and also most problematic to find a certified technical resources to meet the given security level. This is obviously reflected in the price of individual components of the system. The most expensive was the implementation of seized mechanical systems, especially where the security doors and accessories retail price rose to dizzying heights.

A separate chapter of the proposal was a fire alarm, which, according to that calculation may not be realized, but it still prescribes the National security agency to secure the secret category. I realized why this system in that area, I'd still recommend its extension to the entire building, irrespective of category of protected areas.

SEZNAM POUŽITÉ LITERATURY

- [1] MUSIL, Rudolf. *Ochrana utajovaných skutečností*. 1. Praha: Eurounion, 2001. 379 s. ISBN 80-85858-93-2.
- [2] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.
- [3] Národní bezpečnostní úřad: *Podnikatel a bezpečnostní řízení* [online]. 2005 [cit. 2011-05-17]. Obecně k průmyslové bezpečnosti. Dostupné z WWW: <<http://www.nbu.cz/cs/ochrana-utajovanych-informaci/prumyslova-bezpecnost/obecne-k-prumyslove-bezpecnosti/>>.
- [4] Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.
- [5] Příloha č. 1 k vyhlášce č. 528/2005 Sb., ve znění vyhlášky č. 19/2008 Sb.
- [6] Cleverandsmart [online]. 2008 [cit. 2011-05-17]. *Analýza rizik: kvalitativní analýza rizik*. Dostupné z WWW: <<http://www.cleverandsmart.cz/analyza-rizik-kvalitativni-analyza-rizik/>>.
- [7] HOFREITER, Ladislav. *Zásady a principy analýzy rizik v oblasti fyzickej a objektovej bezpečnosti* [online]. Žilina: Fakulta špeciálneho inžinierstva ŽU v Žiline, 2006. 34 s. Metodika. Žilinská univerzita v Žiline. Dostupné z WWW: <nbusr.sk>.
- [8] FRYŠAR, Miroslav. Moderní řízení: Ochrana majetku a informací [online]. 12. 9. 2003 [cit. 2011-05-17]. *Postup při návrhu a realizaci bezpečnostního systému*. Dostupné z WWW: <http://modernirizeni.ihned.cz/c4-10007700-13346220-600000_detail-postup-pri-navrhu-a-realizaci-bezpecnostniho-systemu>.
- [9] KINDL, Jiří. *Projektování bezpečnostních systémů I*. Zlín: Univerzita Tomáše Bati, 2007. 134 s. ISBN 978-80-7318-554-1.
- [10] KŘEČEK, Stanislav. *Průručka zabezpečovací techniky*. 3. [s.l.] : Cricetus, 2006. 313 s. ISBN 80-902938-2-4.
- [11] ČSN EN 50131-1, Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky

- [12] ČSN CLC/TS 50131-7, Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace
- [13] ČSN EN 50133-1, Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 1: Systémové požadavky
- [14] ČSN 73 0875, Požární bezpečnost staveb – Stanovení podmínek pro navrhování elektrické požární signalizace v rámci požárně bezpečnostního řešení
- [15] *EUROSAT CS* [online]. 2011 [cit. 2011-05-21]. Dostupné z WWW: <www.eurosat.cz>.
- [16] *ADI GLOBAL DISTRIBUTION* [online]. 2011 [cit. 2011-05-21]. Dostupné z WWW: <www.adiglobal.cz>.
- [17] *SEGURO s.r.o.* [online]. 2009 [cit. 2011-05-21]. Dostupné z WWW: <www.seguro.cz>.
- [18] *ASSA ABLOY* [online]. 2011 [cit. 2011-05-21]. Dostupné z WWW: <www.assaabloy.cz>.
- [19] *EUROALARM* [online]. 2011 [cit. 2011-05-21]. Dostupné z WWW: <www.euroalarm.cz>.
- [20] *ADLO* [online]. 2002 [cit. 2011-05-21]. Dostupné z WWW: <www.adlo.cz>.
- [21] *XERTEC* [online]. 1991 [cit. 2011-05-21]. Dostupné z WWW: <www.xertec.cz>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

NBÚ	Národní bezpečnostní úřad
UI	Utajovaná informace
IS	Informační systém
Z	Zranitelnost objektu
ZO	Zabezpečená oblast
JO	Jednací oblast
PZS	Poplachový zabezpečovací systém
PZTS	Poplachový zabezpečovací a tísňový systém
EPS	Elektrická požární signalizace
PCO	Pult centralizované ochrany
PPC	Poplachové přijímací centrum
NP	Nadzemní podlaží
PIR	Pasivní infračervený detektor pohybu
MZS	Mechanický zábranný systém
ATZ	Připojení dvou detektorů po jednom páru vyhodnocovacích vodičů
MW	Microwave – mikrovlnný detektor pohybu
PGM	Programovatelný výstup
NC	Normal close
NO	Normal open
LCD	Liquid crystal display – displej z tekutých krystalů
AUX	Napájecí výstup ústředny
IP	Stupeň krytí
GSM	Globální systém pro mobilní komunikaci
GPRS	Mobilní datová služba

SMS	Krátká textová zpráva
AES	Označení pro symetrickou blokovou šifru
MD5	Hašovací funkce
RC4	Generátor pseudonáhodných bitů
KNZ	Kapacita náhradního akumulátoru
LAN	Local area network – lokální počítačová síť
EX	Expander
ČSN	Česká státní norma
EN	Evropská norma
BUS	Adresovatelná sběrnice
DC	Stejnoseměrný proud
ZDP	Zařízení dálkového přenosu
RS232	Sériové komunikační rozhraní
LED	Light Emitting Diode – dioda emitující světlo

SEZNAM OBRÁZKŮ

Obrázek 1. Algoritmus hodnocení zranitelnosti chráněného prostoru [7].....	22
Obrázek 3. Příklad určení míry rizika ohrožení utajovaných informací [7]	24
Obrázek 2. Postup při stanovení míry rizika.....	24
Obrázek 4. Ústředna PZTS EVO 192 [15]	45
Obrázek 5. PIR detektor OPTEX RX40QZD [16]	46
Obrázek 6. PIR charakteristika OPTEX RX40QZD [16].....	46
Obrázek 7. PIR detektor RISCO RK800Q - G3 [16]	47
Obrázek 8. PIR charakteristika RK800Q - G3 [16].....	47
Obrázek 9. Duální PIR + MW RISCO RK150DT – G3 [16]	47
Obrázek 10. PIR + MW charakteristika RK150DT – G3 [16]	47
Obrázek 11. Magnetický kontakt ASITA MAS273 [16].....	48
Obrázek 12. Detektor tříštění skla HONEYWELL FG730 [16]	48
Obrázek 13. Tísňové tlačítko S3040 [16]	49
Obrázek 14. Ovládací klávesnice Paradox K641 [15].....	49
Obrázek 15. Akusticko-optická siréna TEKNIM – 720WR [17]	50
Obrázek 16. GSM komunikátor PCS200 [15]	50
Obrázek 17. Přístupový modul DGP – ACM12 [15].....	57
Obrázek 18. Čtečka karet R870 [15]	58
Obrázek 19. Přístupová karta R207 [15]	58
Obrázek 20. Elektromechanický zámek EL 460 [18].....	59
Obrázek 21. Bezpečnostní zamykání oken ADLO [20]	64
Obrázek 22. Skartovací zařízení INTIMUS 120CC4 [21]	66

SEZNAM TABULEK

Tabulka 1. Postup hodnocení ohrožení	21
Tabulka 2. Příklad matice hodnocení zranitelnosti	23
Tabulka 3. Identifikace aktiv a stupně utajení	38
Tabulka 4. Soupiska ohrožení objektu	39
Tabulka 5. Matice zranitelnosti objektu	40
Tabulka 6. Výsledná míra rizika v objektu	40
Tabulka 7. Bodové hodnoty zabezpečené oblasti [5]	41
Tabulka 8. Bodové hodnoty jednacích oblastí [5]	41
Tabulka 9. Bodové hodnoty zabezpečené oblasti kategorie Důvěrné [5]	41
Tabulka 10. Základní údaje ústředny [15]	45
Tabulka 11. Hodnoty úbytku napětí na kabeláži	51
Tabulka 12. Velikost proudového odběru na výstupu ústředny PZTS	52
Tabulka 13. Velikost proudového odběru komunikačních zařízení	53
Tabulka 14. Velikost proudového odběru na expandérech ústředny	53
Tabulka 15. Velikost proudového odběru pro jeden přístupový systém	54
Tabulka 16. Podsystem 1	54
Tabulka 17. Podsystem 2	54
Tabulka 18. Podsystem 3	55
Tabulka 19. Podsystem 4	55
Tabulka 20. Podsystem 5	56
Tabulka 21. Podsystem 6	56
Tabulka 22. Modul přístupového systému [15]	57
Tabulka 23. Základní technické parametry ústředny EPS [19]	60
Tabulka 24. Rozdělení hlásičů požáru do místností	61
Tabulka 25. Rozdělení hlásičů do hlásicí linky a skupiny	61
Tabulka 26. Vedení hlásicí linky EPS	62
Tabulka 27. Vedení smyčky pro signalizaci poplachu sirénou	62
Tabulka 28. Bezpečnost dveří pro kontrolu vstupu	63
Tabulka 29. Bezpečnost dveří pro zabezpečenou oblast Důvěrné	64
Tabulka 30. Úschovný objekt pro zabezpečenou oblast Důvěrné	64
Tabulka 31. Uzamykací systém oken	64
Tabulka 32. Bezpečnost dveří pro zabezpečenou oblast Tajné	64

Tabulka 33. Úschovný objekt pro zabezpečenou oblast Tajné.....	65
Tabulka 34. Bezpečnost dveří pro jednací oblast Tajné	65
Tabulka 35. Bezpečnostní roleta pro jednací oblast Tajné	65

SEZNAM ROVNIC

Rovnice 1. Výpočet kapacity záložního akumulátoru	52
Rovnice 2. Dobíjecí proud akumulátoru	52
Rovnice 3. Výkon základního zdroje.....	52
Rovnice 4. Nutnost střežení požárního úseku.....	60

SEZNAM PŘÍLOH

Příloha P I: Soupiska a hodnocení ohrožení

Příloha P II: Stanovení hranic zabezpečených a jednacích oblastí

Příloha P III: Bodové porovnání realizovaného a požadovaného zabezpečení

Příloha P IV: Soupiska použitých prvků

Příloha P V: Výkresová dokumentace

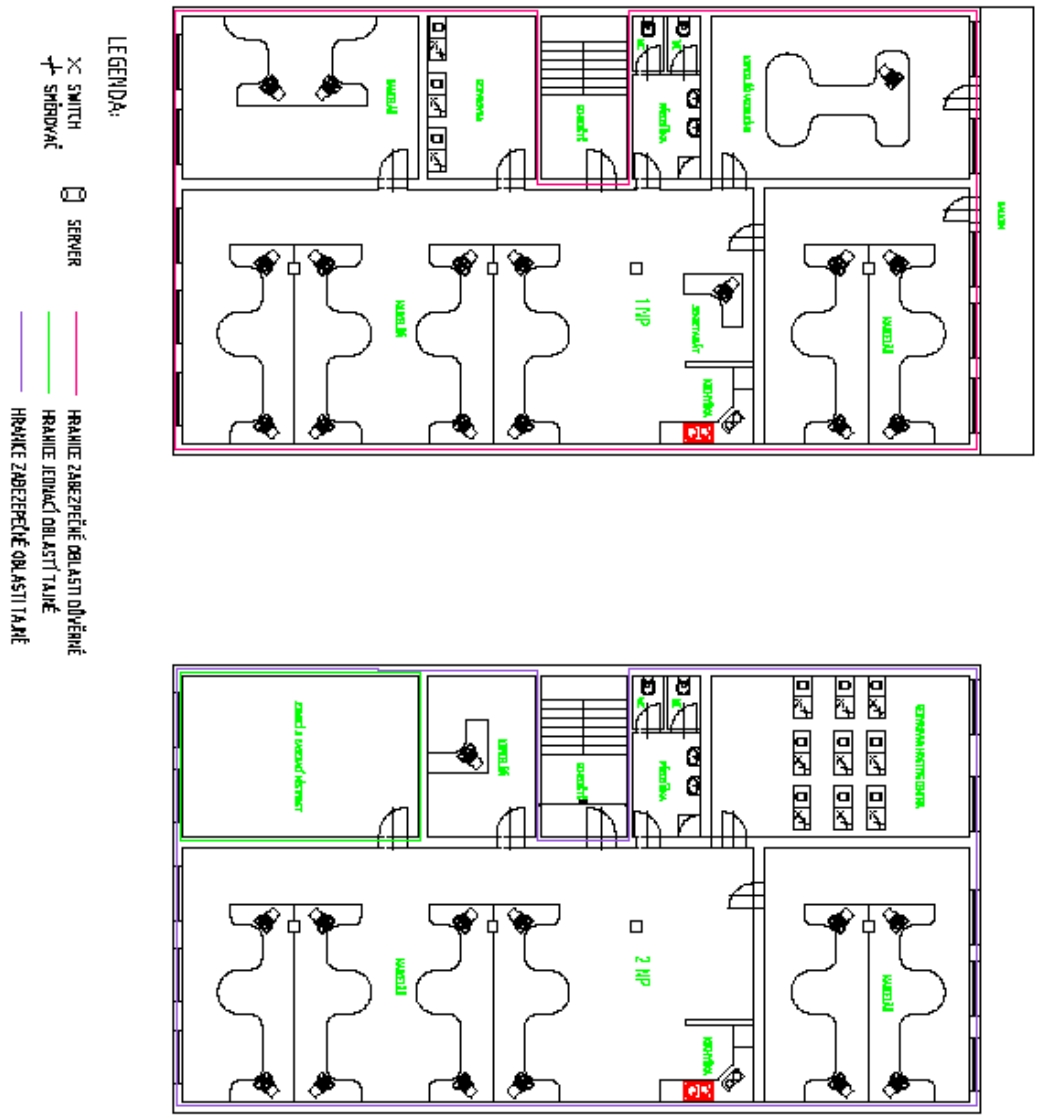
Příloha P VI: Certifikáty technických prostředků (uloženo na CD)

PŘÍLOHA P I: SOUPISKA A HODNOCENÍ OHROŽENÍ

Ohrožení		Zdroj	Motivace, záměr, příčina	Výskyt případu v minulosti (ANO/NE)	Hodnocení (0; M; S; V)
Z hlediska polohy a umístění objektu	O ₁	Výrobní objekty	Havárie, zdroje nebezpečných látek		
	O ₂	Stacionární zdroje nebezpečných látek			
	O ₃	Mobilní zdroje nebezpečných látek	Blízkost komunikace a rozvodu		
	O ₄	Dopravní nehody	Blízkost komunikace, železnice, leteckého koridoru		
	O ₅	Jaderné zařízení	Havárie		
	O ₆	Vodní nádrže	Protržení hráze, záplavová oblast		
Zabezpečení ochrany objektu	O ₇	Náhodný lupič	Zisk		
	O ₈	Lupič s přípravou	Zisk, pomsta		
	O ₉	Vandalismus	Poškození majetku		
	O ₁₀	Návštěvy	Zisk, zvědavost, nedostatečná režimová opatření		
	O ₁₁	Dodavatelé			
Činnost cizích zpravodajských služeb, teroristických a zločineckých organizací	O ₁₂	Cizí zpravodajské služby	Poškození politických, ekonomických a vojenských zájmů		
	O ₁₃	Komerční zpravodajské služby			
	O ₁₄	Teroristi	Pomsta, vydírání, strach		
	O ₁₅	Odpůrci	Poškození zájmů		
	O ₁₆	Skupina organizovaného zločinu	Zisk, pomsta, poškození zájmů		
	O ₁₇	Záškodníci	Pomsta, poškození zájmů, sabotáž		
Technické poruchy	O ₁₈	Rozvod el. Energie	Havárie, požár, záplavy, plyn, sabotáž		
	O ₁₉	Rozvod vody			
	O ₂₀	Rozvod a zásobníky plynu			
	O ₂₁	Ústřední vytápění			

Zaměstnanci	O ₂₂	Vlastní zaměstnanci - oprávněné osoby	Zisk, nedbalost, neznalost, vydírání		
	O ₂₃	Vlastní zaměstnanci - neoprávněné osoby	Pomsta, zisk, vydírání, nedostatečná ochrana		
	O ₂₄	Servisní služby, obslužný personál	Zisk, častý pohyb v objektu, nedostatečná ochrana		
	O ₂₅	Pracovníci fyz. ochrany	Zisk, nedbalost, vydírání, neoprávněný přístup		
Okolní objekty	O ₂₆	Výrobní objekty zdroje nebezpečných látek	Havárie, blízkost zdroje nebezpečných látek		
Výjimečný a nouzový stav	O ₂₇	Povodně a záplavy	Blízkost vodního toku, povodňová oblast		
	O ₂₈	Požár	Blesk, sabotáž, havárie		
	O ₂₉	Sesuvy půdy	Geologické podmínky		
	O ₃₀	Narušení veřejného pořádku	Extremismus, sociální nepokoje		

**PŘÍLOHA P II: STANOVENÍ HRANIC ZABEZPEČENÝCH A
JEDNACÍCH OBLASTÍ**



PŘÍLOHA P III: BODOVÉ POROVNÁNÍ REALIZOVANÉHO A POŽADOVANÉHO ZABEZPEČENÍ

Název zabezpečené oblasti:	1. nadzemní podlaží	
Kategorie a třída:	Důvěrné, II.	
Účel:	Ukládání, zpracování	
Bezpečnostní opatření	Typ	Bodové hodnocení
Úschovné objekty	T. 2 - 2 body	SS1 = 2
Zámky úschovných objektů	T. 2 - 2 body	SS2 = 2
Úschovný objekt včetně uzamykacího systému	0	S1 = 0
Celkové hodnocení úschovného objektu a jeho zámku	$S1 = SS1 \times SS2$	S1 = 4
Zabezpečená oblast	T. 2 - 2 body	SS3 = 2
Uzamykací systém zabezpečené oblasti	T. 1 - 1 bod	SS4 = 1
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	$SS2 = SS3 \times SS4$	S2 = 2
Objekt	T. 3 - 3 body	S3 = 0
Kontrola vstupu	T. 3 - 3 body	SS6 = 3
Režim návštěv v objektu a) s doprovodem	ad a) 3 body	SS7 = 3
Celkové hodnocení kontroly vstupu	$S4 = SS6 + SS7$	S4 = 6
Ostraha	T. 1 - 1 bod	SS8 = 1
Zařízení PZS	T. 3 - 3 body	SS91 = 3
Instalace PZS	T. 2 - 2 body	SS92 = 2
Mezivýsledek (SS9)	$SS9 = (SS91 + SS92) / 2 \times SS92 / OBL$	SS9 = 3
Celkové hodnocení ostrahy a systému PZS	$S5 = SS8 + SS9$	S5 = 4
Fyzické bariéry	0	SS10 = 0
Kontrola vstupu v přístupových bodech fyzické bariéry b) kontrola není realizována	ad b) 0 - bodů	SS11 = 0
Namátkové vstupní a výstupní prohlídky b) nejsou prováděny	ad b) 0 - bodů	SS12 = 0
Perimetrický detekční systém PDS	0	SS13 = 0
Bezpečnostní osvětlení perimetru	0	SS14 = 0
Speciální televizní systém na perimetru	0	SS15 = 0
Celkové hodnocení ochrany perimetru	0	S6 = 0
Celkové hodnocení zabezpečené oblasti	S1 + S2 + S3 + S4 + S5	16
Nejnižší míra zabezpečení		16

Název zabezpečené oblasti:	2. nadzemní podlaží	
Kategorie a třída:	Tajné, II.	
Účel:	Ukládání, zpracovávání	
Bezpečnostní opatření	Typ	Bodové hodnocení
Úschovné objekty	T. 2 - 3 body	SS1 = 3
Zámky úschovných objektů	T. 2 - 2 body	SS2 = 2
Úschovný objekt včetně uzamykacího systému	0	S1 = 0
Celkové hodnocení úschovného objektu a jeho zámku	$S1 = SS1 \times SS2$	S1 = 6
Zabezpečená oblast	T. 2 - 2 body	SS3 = 2
Uzamykací systém zabezpečené oblasti	T. 2 - 2 body	SS4 = 2
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	$SS2 = SS3 \times SS4$	S2 = 4
Objekt	T. 3 - 3 body	S3 = 0
Kontrola vstupu	T. 3 - 3 body	SS6 = 3
Režim návštěv v objektu a) s doprovodem	ad a) 3 body	SS7 = 3
Celkové hodnocení kontroly vstupu	$S4 = SS6 + SS7$	S4 = 6
Ostraha	T. 1 - 1 bod	SS8 = 1
Zařízení PZS	T. 3 - 3 body	SS91 = 3
Instalace PZS	T. 3 - 3 body	SS92 = 3
Mezivýsledek (SS9)	$SS9 = (SS91 + SS92) / 2 \times SS92 / OBL$	SS9 = 3
Celkové hodnocení ostrahy a systému PZS	$S5 = SS8 + SS9$	S5 = 4
Fyzické bariéry	0	SS10 = 0
Kontrola vstupu v přístupových bodech fyzické bariéry b) kontrola není realizována	ad b) 0 - bodů	SS11 = 0
Namátkové vstupní a výstupní prohlídky b) nejsou prováděny	ad b) 0 - bodů	SS12 = 0
Perimetrický detekční systém PDS	0	SS13 = 0
Bezpečnostní osvětlení perimetru	0	SS14 = 0
Speciální televizní systém na perimetru	0	SS15 = 0
Celkové hodnocení ochrany perimetru	0	S6 = 0
Celkové hodnocení zabezpečené oblasti	S1 + S2 + S3 + S4 + S5	20
Nejnižší míra zabezpečení		20

Název zabezpečené oblasti:	2. nadzemní podlaží	
Kategorie a třída:	Tajné, II.	
Účel:	Projednávání	
Bezpečnostní opatření	Typ	Bodové hodnocení
Úschovné objekty	T. 2 - 3 body	SS1 = 0
Zámky úschovných objektů	T. 2 - 2 body	SS2 = 0
Úschovný objekt včetně uzamykacího systému	0	S1 = 0
Celkové hodnocení úschovného objektu a jeho zámku	$S1 = SS1 \times SS2$	S1 = 0
Zabezpečená oblast	T. 3 - 3 body	SS3 = 3
Uzamykací systém zabezpečené oblasti	T. 2 - 2 body	SS4 = 2
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	$SS2 = SS3 \times SS4$	S2 = 6
Objekt	T. 3 - 3 body	S3 = 0
Kontrola vstupu	T. 3 - 3 body	SS6 = 3
Režim návštěv v objektu a) s doprovodem	ad a) 3 body	SS7 = 3
Celkové hodnocení kontroly vstupu	$S4 = SS6 + SS7$	S4 = 6
Ostraha	T. 1 - 1 bod	SS8 = 1
Zařízení PZS	T. 3 - 3 body	SS91 = 3
Instalace PZS	T. 3 - 3 body	SS92 = 3
Mezivýsledek (SS9)	$SS9 = (SS91 + SS92) / 2 \times SS92 / OBL$	SS9 = 3
Celkové hodnocení ostrahy a systému PZS	$S5 = SS8 + SS9$	S5 = 4
Fyzické bariéry	0	SS10 = 0
Kontrola vstupu v přístupových bodech fyzické bariéry b) kontrola není realizována	ad b) 0 - bodů	SS11 = 0
Namátkové vstupní a výstupní prohlídky b) nejsou prováděny	ad b) 0 - bodů	SS12 = 0
Perimetrický detekční systém PDS	0	SS13 = 0
Bezpečnostní osvětlení perimetru	0	SS14 = 0
Speciální televizní systém na perimetru	0	SS15 = 0
Celkové hodnocení ochrany perimetru	0	S6 = 0
Celkové hodnocení zabezpečené oblasti	S1 + S2 + S3 + S4 + S5	16
Nejnižší míra zabezpečení		16

PŘÍLOHA P IV: SOUPISKA POUŽITÝCH PRVKŮ

Poplachový zabezpečovací a tísňový systém				
Prvek	Typ	Počet	Cena/ks [Kč]	Cena [Kč]
Ústředna PZTS	Digiplex EVO 192	1	4500	4500
Rozšiřující expandéry zón	ZX8	3	1299	3897
PIR	RX40QZD	6	470	2820
PIR	RK800Q -G3	5	1190	5950
PIR + MW stropní	RK150DT	1	2280	2280
Magnetický kontakt	MAS273	27	200	5400
Magnetický kontakt	MAS303	25	298	7450
Detektor tříštění skla	FG730	4	500	2000
Detektor tříštění skla	FG 1625TAS	4	890	3560
Tísňové tlačítko	S30/40 SR	2	874	1748
LCD klávesnice	K641	2	2599	5198
Akusticko-optická siréna	720WR	1	999	999
GSM komunikátor	PCS200	1	5299	5299
IP LAN komunikátor	IP100	1	3333	3333
Doplňkový napájecí zdroj	PS 817	2	429	858
Transformátor	80VA, 20VA	2	469, 269	738
Akumulátor	26 Ah	1	1199	1199
Akumulátor	12 Ah	1	710	710
Akumulátor	18 Ah	1	799	799
BOX	Esprit BOX D	1	599	599
			Cena celkem	59337

Integrovaný přístupový systém				
Prvek	Typ	Počet	Cena/ks [Kč]	Cena [Kč]
Přístupový modul	ACM 12	6	2895	17370
Přístupová karta	R207	1	100	100
Bezkontaktní čtečka karet	R870	6	1999	11994
Elektromechanický zámek	EL 460	6	11150	66900
Transformátor	80VA	2	469	938
Akumulátor	18 Ah	6	799	4794
			Cena celkem	102096

Mechanické zábranné systémy				
Prvek	Typ	Počet	Cena/ks [Kč]	Cena [Kč]
Bezpečnostní dveře pro kontrolu vstupu	F6/2 Abloy	5	18127	90635
Bezpečnostní dveře pro kontrolu vstupu	F6/4 Abloy	1	27496	27496
Bezpečnostní dveře klasické	F6/2 PLUS	2	19446	38892
Bezpečnostní dveře klasické	F6/3	2	24000	48000
Bezpečnostní kování	IKON SX48	6	4430	26580
Bezpečnostní kování	S1/90	4	1729	6916
Cylindrická vložka	2018N	4	1500	6000
Cylindrická vložka	CONTROL	5	688	3440
Cylindrická vložka	DYNAMIC	1	946	946
Bezpečnostní roleta	RL - P	1	pouze na objednávku	
Bezpečnostní zámek oken	Adlo	20	3700	74000
Skříňový trezor	Neptun	1	10500	10500
Skříňový trezor	Salvus 1	1	21000	21000
Bezpečnostní zárubně	CG6	10	2690	26900
			Cena celkem	381305

Zařízení fyzického ničení nosičů informací	Typ	Počet	Cena [Kč]
Skartovací stroj	INTIMUS 120CC4	1	31 900

Ochrana proti aktivnímu a pasivnímu odposlechu	Typ	Počet	Cena [Kč]
Kontrola radiového spektra	MRA - 3	1	28488
Šumový generátor	SNG	1	13 980
		Cena celkem	42468

Elektrická požární signalizace				
Prvek	Typ	Počet	Cena/ks [Kč]	Cena [Kč]
Ústředna	Apollo F2	1	29245	29245
Požární hlásič kouřový multisenzorový	XP95	4	1510	6040
Požární hlásič kouřový multisenzorový s izolátorem	XP95	1	1624	1624
Požární hlásič manuální tlačítkový	XP95	3	1782	5346
Požární hlásič optickokouřkový	XP95	2	1367	2734
Patice pro hlásiče	XP95	6	88	528
Patice pro hlásiče s izolátorem	XP96	1	436	436
Zařízení dálkového přenosu	RADOM STX 23	1	20240	20240
Akumulátor	12 Ah		710	0
Siréna	SONOS	1	624	624
			Cena celkem	66817

PŘÍLOHA P V: VÝKRESOVÁ DOKUMENTACE