Využití technických zabezpečovacích systémů při ochraně utajovaných informací

The use of security systems to protect classified information

Bc. Michal Roubal

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

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

Jméno a příjmení:	**Bc. Michal ROUBAL**
Osobní číslo:	**A09690**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Využití technických zabezpečovacích systémů při ochraně utajovaných informací**

Zásady pro vypracování:

1. **Pojednejte o národní legislativní úpravě v oblasti ochrany utajovaných informací (OUI).**
2. **Analyzujte požadavky na realizaci opatření fyzické bezpečnosti zabezpečených a jednacích oblastí.**
3. **Specifikujte požadavky na zabezpečovací systémy z hlediska OUI.**
4. **Pojednejte o certifikaci technických prostředků pro účely OUI.**
5. **Vypracujte návrh opatření fyzické bezpečnosti zabezpečené oblasti se stupněm utajení TAJNÉ.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **412/2005 Sb. Zákon ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti.**
2. **528/2005 Sb. Vyhláška ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků.**
3. **Fyzická bezpečnost (technické prostředky a další prvky fyzické bezpečnosti a jejich certifikace) [online]. Praha: NBÚ, 2010 [citováno 2011-01-24]. Dostupné z URL [http://www.nbu.cz].**
4. **Zpracování projektu fyzické bezpečnosti pro orgány státu a právnické i podnikající fyzické osoby. [online]. Ostrava: F.S.C. Bezpečnostní poradenství, 2010 [citováno 2011-01-24]. Dostupné z URL [http:// http://www.fsc-ov.cz].**
5. **Ochrana utajovaných informací.. [online]. Brno: DRAKAS, 2009 [citováno 2011-01-24]. Dostupné z URL [http:// http://www.drakas.cz].**

Vedoucí diplomové práce:	**Ing. Jan Valouch, 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

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem diplomové práce je vypracování analýzy a specifikace požadavků na zabezpečovací systémy z hlediska ochrany zabezpečených oblastí v souladu s ustanoveními relevantních předpisů. Součástí práce je analýza procesu certifikace prvků zabezpečovacích systémů a souhrnný přehled doporučení pro dodavatele zabezpečovacích systémů subjektům zabezpečujícím ochranu utajovaných informací. Stěžejním výstupem práce je vypracování návrhu zabezpečení zabezpečené oblasti určené kategorie stupně utajení TAJNÉ.

Klíčová slova: analýza, certifikace prvků, návrh, zabezpečovací systém

ABSTRACT

The aim of this thesis is an analysis and specification of security systems for the protection of secured areas in accordance with the provisions of relevant laws. An analysis of the process of certification of safety systems and a summary of recommendations for suppliers of security systems operators providing protection of classified information. The main output of this work is the drafting of security for the secured category SECRET level.

Keywords: analysis, certification of components, design, security system

Děkuji svému vedoucímu diplomové práce panu Ing. Janu Valouchovi, Ph.D. za jeho odborné vedení, konzultace, rady a věcné poznatky, které mi poskytoval během psaní 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

Problematika technického zabezpečení jako jedna ze součástí ochrany utajovaných informací je v současné době velmi důležitá, protože porušení zásad manipulace ochrany utajovaných skutečností může mít velice negativní dopad na firmu, které se tyto informace týkají. Problém je hlavně v tom, že některé společnosti to berou na lehkou váhu. Každá firma týká se to především státních institucí, by měla vyčlenit část financí pro tuto oblast, jelikož jsou 4 stupně utajení tak každé bude stát jiný finanční obnos. Tyto informace jsou uloženy v prostorech kde jsou dostatečně zabezpečeny jak technickými prostředky tak fyzickou ostrahou a řeší se přístup k nim. Proto cílem diplomové práce je zajistit pro dodavatelské subjekty souhrnný přehled a doporučení jak zabezpečit utajovanou informaci týká se to hlavně techniky a osob a manipulace je věc zákazníka. Práce se také bude zabývat analýzou procesu certifikace technických prostředků zabezpečovacích systémů. Společnosti, které disponují utajovanými informacemi prochází jednou za určitý časový interval auditem, který se týká ověření shody, realizace technických prostor určený k manipulaci a ukládání utajovaných informací po dokončení montážní firmou a taky projektem fyzické bezpečnosti. Hlavní problémem utajovaných informací je jejich únik například nedávná kauza wikileaks, někteří lidé to brali jako 11. září pro světovou diplomacii. Tato kauza odhalila jak je nebezpečné podceňovat zabezpečení citlivých informací. Únik utajovaných dat v komerční oblasti nezpůsobí takovou rozruch avšak pro firmy to může mít likvidační následky například vyzrazením know-how nebo odhalení strategických záměrů. Firmy se v současné době hodně zajímají hrozbami vnějšího charakteru, ale tímto podceňují útoky ze strany zaměstnanců. Citlivá data je třeba chránit a okamžitě reagovat na podezřelé chování jakéhokoli uživatele. Za porušení zásad OUI hrozí sankce ve výši několik desítek milionů korun.

Oblasti, kterých se utajované informace dotýkají:

- obrana,

- státní správa,

- hmotné rezervy,

- objekty kritické infrastruktury a další.

I. TEORETICKÁ ČÁST

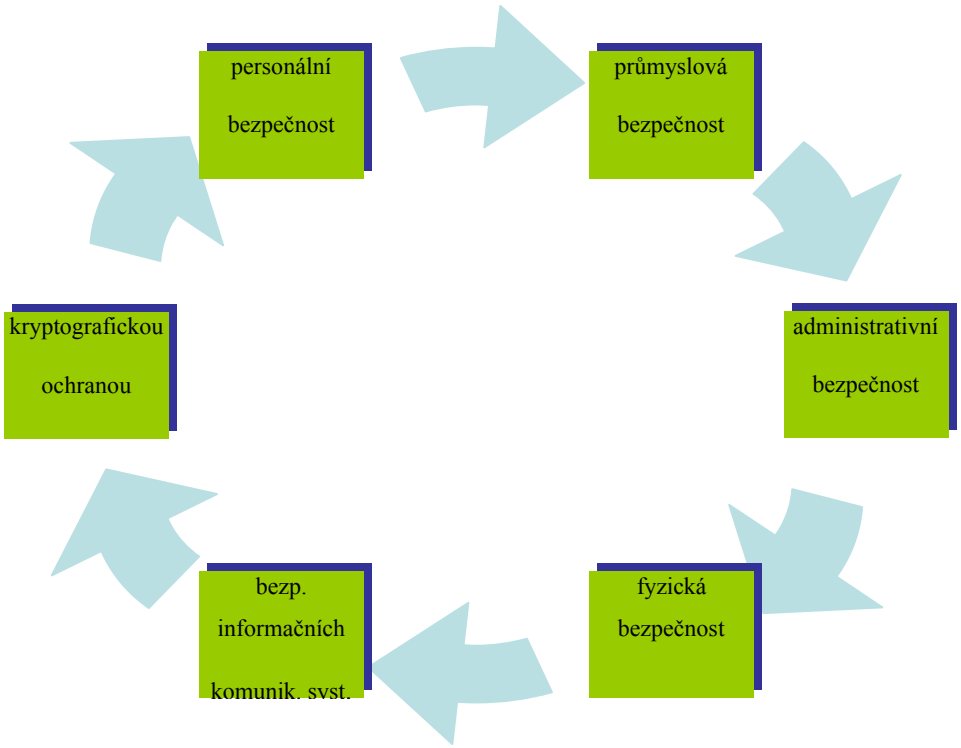
1 LEGISLATIVNÍ RÁMEC

Problematiku ochrany utajovaných informací v národní právním řádu řeší zákon 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen zákon o ochraně utajovaných informací). Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, určuje podmínky pro přístup k nim a dále požadavky na jejich ochranu. Státním orgánem odpovědným za utajovanou informaci je NBÚ (národní bezpečnostní úřad). Tento úřad je ústředním správním orgánem pro oblast ochrany utajovaných informací a bezpečnostní způsobilosti. Utajovaná informace může být v jakékoliv podobě a na jakémkoliv médiu, jestliže dojde k vyzrazení nebo odcizení této utajované informace může to způsobit vážnou újmu svrchovanosti a územní celistvosti České republiky. Potřeba ochrany utajovaných informací je velká, protože žádná společnost nemá zájem o trvalé, dočasné hrozby nebo dokonce krize, která vede vždy k materiálním, finančním a lidským ztrátám. Většina společností tuto situaci velmi podceňuje vůbec neví jak tomu předcházet a neví základní věc, jak se chovat jestliže tato krizová situace nastane zneužitím jejich utajovaných informací. Prevence může předejít - zamezit - a odvrátit, jelikož může selhat lidský faktor je třeba využít technických prostředků k ochraně utajovaných informací. Při posuzování míry rizika si musíme odpovědět na základní otázky co musíme chránit (budova, zaměstnanci, nebezpečné látky v objektu, vybavení, utajované informace) a dále si musíme uvědomit proč to chránit nebo před kým až poté si můžeme zvolit opatření a kombinaci technických prostředků.

1.1 Fyzická bezpečnost v rámci utajovaných informací

Fyzická bezpečnost tvoří jeden z důležitých typů ochrany utajovaných informací, ověřuje podmínky pro přístup k nim a její úkolem je chránit tyto utajované informace. Nasazení technických zabezpečovacích systémů spadá především do této oblasti.

Druhy zajištění utajovaných informací:



Obr. č.1 Druhy zajištění informací

a) personální bezpečností, kterou tvoří výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím, jejich výchova a ochrana,

b) průmyslovou bezpečností, kterou tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu s tímto zákonem,

c) administrativní bezpečností, kterou tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi,

d) fyzickou bezpečností, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat,

e) bezpečností informačních nebo komunikačních systémů, kterou tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému,

f) kryptografickou ochranou, kterou tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací. [1]

Technická opatření mohou být podpořena nebo degradována lidským faktorem. Tím je myšleno jeho úmyslným pochybením nebo nedbalostí a proto musíme vedle typů technické ochrany taky věnovat pozornost výběru fyzických osob, která pracují s utajovanými informacemi, ale rovněž taky osob, které se přímo podílejí na procesu fyzické ochrany, včetně technického zabezpečení. Tím jsou obchodní společnosti, které se podílejí na zakázce, provádí navrch zabezpečení, montáž, servis PZS (poplachový zabezpečovací systém).

Technické prostředky fyzické ochrany se dělí:

- mechanické a technické prostředky,

Dále se rozdělují na mechanické zábranné systémy (plášťové, předmětové, obvodové) a technické prostředky ochrany (EZS, EPS, kamerové systémy, ústředny, PCO, přenos.zař.)

- organizační a režimová opatření,

- fyzická ostraha.

V dnešní době je velký problém získat kvalitní a správně motivované zaměstnance. Motivace se odráží hlavně na špatných platových podmínkách toto se odráží na kvalitě a dalšího procesního růstu.

Osoby nebo podnikatelé, jestliže chtějí manipulovat s utajovanými informacemi musí dle zákona 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti splňovat podmínky pro vydání osvědčení, které jsou níže uvedeny.

a.) Podmínky pro vydání osvědčení **fyzické osoby**:

- fyzické osoba musí být občanem České republiky nebo státu Evropské unie nebo Organizace severoatlantické smlouvy

- bezúhonnost,
- dosažení věku minimálně 18let,
- poučen právním úkonům,
- bezpečnostně spolehlivá,
- netrpí žádnou vadou, která by mohla mít vliv na jeho spolehlivost,

Toto oznámení zaniká jestli-že:

- osoba porušila jednu z podmínek pro vydání osvědčení,
- ukončení služebního poměru,
- trestný čin(odcizení, znehodnocení),
- úmrtí. [1]

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
Pošt. přihr. 49
150 06 Praha 56

OSVĚDČENÍ

fyzické osoby

Certificate of Security Clearance/Certificat d´habilitation personnelle

ČÍSLO: NBÚ-071431
Number/Numéro

Jméno a příjmení: Václav TOULEC
Name and Surname
Nom et prénom

Rodné příjmení: Toulec
Maiden Name
Nom de naissance

Datum narození: 24.11.1964
Date of Birth
Date de naissance

Rodné číslo: [redacted]
Personal No.
Numéro d'identification personnelle

Místo narození: Praha 4
Place of Birth
Lieu de naissance

Státní občanství: Česká republika
Nationality
Nationalité

Stupeň utajení: DŮVĚRNÉ
Classification Level CONFIDENTIAL
Niveau de classification CONFIDENTIEL DEFENSE

Datum vydání: 8.12.2008
Date of Issue
Date de délivrance

Platnost od: 8.12.2008
Valid from
Validité à partir de

Platnost do: 7.12.2017
Date of Expiry
Date d'expiration

Podpis oprávněného zástupce
Signature of the Competent Representative
Signature du représentant autorisé

Otisk úředního razítka
Official Stamp/Cachet officiel

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD 13

036593

Obr. 1. Certifikát osvědčení fyzické osoby [3]

b.) Podmínky pro vydání osvědčení **podnikatele**:

- bezpečnostně spolehlivý,

- ekonomicky zajištěný,

- je schopen zabezpečit ochranu utajovaných informací,

- odpovědná osoba musí být držitelem osvědčení fyzické osoby nejméně pro takový stupeň pro, který žádá podnikatel, [1]

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD ČESKÉ REPUBLIKY
(NATIONAL SECURITY AUTHORITY OF THE CZECH REPUBLIC/
AUTORITÉ NATIONALE DE LA SÉCURITÉ DE LA RÉPUBLIQUE TCHÈQUE)
Pošt. přihr. 49
150 06 Praha 56

Národní bezpečnostní úřad České republiky vydává podle § 121 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
(The National Security Authority of the Czech Republic issues according to Section 121 of Act No. 412/2005 Coll., on protection of classified information and security capacity / L'Autorité Nationale de la Sécurité de la République tchèque délivre d'après l'article 121 de la Loi n°. 412/2005 Recueil des lois, relative à la protection des informations classifiées et d'aptitude de sécurité)

OSVĚDČENÍ
podnikatele
(CERTIFICATE of Facility Security Clearance / CERTIFICAT d'habilitation d'entreprise)

Číslo / Number / Numéro: 001306

Držitel osvědčení / Holder of certificate / Possesseur du certificat:

StringData, s.r.o.
IČ: 496 80 331
Praha 2 - Vinohrady, Na Švihance 8

Toto osvědčení umožňuje přístup k utajované informaci nejvýše stupně utajení
(This certificate allows access to classified information up to the level / Ce certificat permets l'accès aux informations classifiées jusqu'au niveau)

VYHRAZENÉ/RESTRICTED/DIFFUSION RESTREINTE
(stupeň utajení / Level of classification / Niveau de classification)

Forma přístupu / Form of access / Forme d'accès:
Na základě tohoto osvědčení má podnikatel podle § 20 odst. 1 zákona č. 412/2005 Sb., přístup k utajované informaci:
a) která u něho vzniká, nebo je mu poskytnuta, nebo
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.
This certificate allows access of the facility to classified information according to Section 20(1) of Act No. 412/2005 Coll.:
a) is originated by or released to the facility, or
b) is not originated by or released to the facility, but which is accessible by employees of the facility or persons acting on behalf of or for the facility, in connection with performance of work or other activities for the facility on the basis of the contract.
D'après l'article 20.1 de la Loi n°. 412/2005 Recueil des lois, ce certificat permet l'accès à l'information classifiée à l'entreprise:
a) quand celle-ci se produisse ou elle lui est fournie
b) quand celle-ci ne se produisse pas ou elle ne lui est pas fournie, mais à la quelle ont l'accès les employés de l'entreprise ou les personnes agissant au nom ou pour l'entreprise conformément à leurs travail ou autre activité pour l'entreprise suite au contrat.

Datum vydání / Date of issue / Date de délivrance: **11.3.2010**

Platnost do / Valid until / Validité jusqu'à: **10.3.2022**

otisk úředního razítka / Official stamp / Cachet officiel:
podpis oprávněného zástupce / Signature of the NSA's authorized representative / Signature du représentant de l'ANS:
001422

Obr. 2. Certifikát osvědčení podnikatele [4]

1.2 Objekty, zabezpečené oblasti a jednací oblasti

Pro ochranu utajovaných informací se určují objekty, zabezpečené oblasti a jednací oblasti.

Objekty

Objektem se rozumí budova nebo jiný stavební prostor, kde se ukládají nebo dochází k manipulaci s utajovanými informacemi.

Tyto utajované informace se zpracovávají:

- v objektu, který se může nacházet mimo zabezpečenou oblast, ale to je tehdy pokud je dostatečně zajištěna bezpečnost, aby k utajovaným informacím neměla přístup neoprávněná osoba,

- v zabezpečených oblastech,

- mimo objekt, ale to jenom za předpokladu písemného souhlasu odpovědné osoby

Utajované informace se ukládají v zabezpečených oblastech ve, kterých se nacházejí trezory, bezpečnostní skříně nebo schránky, které musí odpovídat určitým normám (kvalita materiálu, kvalita zabezpečení). [1]

Zabezpečené oblasti:

Zabezpečenou oblastí se rozumí prostor, kde se ukládají nebo zpracovávají utajované informace.

Zabezpečené oblasti se podle stupně utajení dělí do kategorií:

- vyhrazené,

- důvěrné,

- tajné,

- přísně tajné.

Také se dělí podle možnosti přístupu nim:

- fyzická osoba, která vstupuje do zabezpečené oblasti, kde dochází k seznámení s utajovanou informací,

- fyzická osoba, která vstupuje do zabezpečené oblasti, kde nedochází k seznámení s utajovanou informací;

Každý vstup a výstup musí být kontrolován a samozřejmě tento přístup musí být za doprovodu pověřené osoby, která má vstup do oblasti povolen.

V zabezpečované oblasti nelze ukládat utajované informace jiného podnikatele!

Práce v zabezpečených oblastech:

Pro práci v zabezpečovaných oblastech musí být aplikované přesné bezpečnostní postupy:

- analýza rizik v zabezpečovaných oblastech,

- audit,

- vypracování projektu ochrany,

- vytvoření bezpečnostních procesů a řádné proškolení zaměstnanců,

- vytvoření bezpečnostních procesů pro dodavatele. [5]

Zabezpečené oblasti se dělí na 5 typů dle materiálu, který tvoří jejich obvod:

Tab. 1. Používaný materiál u různých typů zabezpečené oblasti

	Typ 0	**Typ 1**	**Typ 2**	**Typ 3**	**Typ 4**
použitý materiál stěny, stropy podlahy	sádrokarton	sádrokarton	zděná stěna	zděná stěna	zděná stěna
	plech	plech	tl. 100-150mm	tl. < 150mm	tl. < 300mm
	plast	plast	vystužený	vyst. Beton	vyst. Beton
	dřevo	dřevo	beton do	do 150mm	do 150mm
	sklo	sklo/bezp fól.	100mm	okna/dveře tř.3	okna/dveře tř.4,5
				ČSN P ENV1627	ČSN P ENV1627

Obr. 3. Úložna klíčů zabezpečené oblasti [6]

Jednací oblasti:

Jednací oblast se nachází uvnitř objektu. O tuto oblast se starají odpovědné osoby, které musí zajistit, aby nedošlo k úniku informací, které jsou v oblasti projednávány. Odpovědné osoby jsou jednou za určitý interval povinny požádat příslušný úřad o provedení kontroly, zda v jednací oblasti nedochází k úniku utajovaných informací, pomocí technický prostředků. Tuto kontrolu provádí zpravodajské služby a policie České republiky. Samozřejmostí musí být, že vstupy a výstupy jednací oblasti jsou kontrolovány technickými zařízeními a fyzickou ostrahou.

Při obranné prohlídce musí být nasazeny technické prostředky proti pasivnímu a aktivnímu odposlechu utajované informace. Obranná prohlídka se musí provádět vždy po neautorizovaném vstupu nebo po odchodu pracovníků, kteří provádějí údržbu nebo úpravy v jednací oblasti dělali.

Obr. 4. Jednací oblast [7]

1.3 Opatření fyzické bezpečnosti

Opatřeními fyzické bezpečnosti jsou:

- ostraha,

- režimová opatření,

- technické prostředky.

Fyzická ostraha objektu

Zabezpečuje se vyškolenými zaměstnanci provozovatele objektu, příslušníky ozbrojených sil, ozbrojených sborů nebo zaměstnanci pověřené bezpečnostní ochranné služby. U důležitých objektů se fyzická ostraha objektu zajišťuje nepřetržitě. Fyzickou ostrahu objektu zajišťují na stanovišti určeném pro stálý výkon fyzické ostrahy objektu nejméně 2 pracovníci fyzické ostrahy objektu. Délka přístupové trasy od stanoviště určeného pro stálý výkon fyzické ostrahy objektu ke vstupu do nejvzdálenější zabezpečené oblasti nesmí být větší než 500 metrů. Na stanoviště určené pro stálý výkon fyzické ostrahy objektu jsou vyvedena výstupní hlášení technických prostředků. Objekty kategorie přísně tajné se zajišťuje nejméně dvěma osobami, tajné jednou osobou u objektu a druhou osobou, která vyhlásí poplach nebo jinak zasáhne jsou-li utajované informace narušeny a důvěrné u této kategorie stačí pouze jedna osoba. [8]

Režimová opatření

V rámci režimových opatření zajišťujeme :

- Vstup a výstup osob a vjezdu a výjezdu dopravních prostředků, který stanoví: oprávnění osob a dopravních prostředků pro vstup a vjezd do objektu, výstup a výjezd z objektu a způsob kontroly,

- Podmínky a způsob kontroly vynášení a vnášení věcí nebo utajovaných skutečností z objektu,

- Pohybu osob, věcí, dopravních prostředků a utajovaných skutečností v objektu a jeho jednotlivých částech v pracovní a mimopracovní době,

- Manipulace s klíči, identifikačními prostředky a médii, které se používají pro systémy zabezpečení vstupů, kterým se zejména určuje systém a způsob označování, přidělování a odevzdávání klíčů, jejich úschovy a evidence, uložení duplikátů a způsob jejich použití,

- Manipulace s technickými prostředky a jejich používání. [8]

Oprávnění ke vstupu do objektu

Oprávnění ke vstupu vjezdu do objektu vydává provozovatel objektu nebo jiná pověřená osoba. Vstup osob nebo vozidel do objektu se prokazují takovým způsobem, která určí

jejich jednoznačnou identifikaci. Seznam osob které vstupují do objektu nebo dopravní prostředky evidují pověřené osoby, které se ve většině případů nachází na vrátnici. Provozovatel stanoví v provozním řádu opatření, které zabrání návštěvám nebo zaměstnancům z jiného oddělení, aby nedošlo k neoprávněnému seznámení s utajovanými informacemi. Za dodržování těchto opatření je zodpovědná osoba, která osoby doprovází, protože ve většině důležitých objektech je návštěvám povolen pohyb jen s doprovodem.

Kontrolní opatření při vstupu do objektu

Kontrolu vstupu osob a vjezdu dopravních prostředků provádí fyzická ostraha nebo jiná pověřená osoba, kterou určí majitel objektu. Při kontrole se používají certifikované technické prostředky. [8]

Technické prostředky

Technickým prostředkem se rozumí zařízení, jehož použitím se zabraňuje, stěžuje nebo oznamuje narušení ochrany objektu.

Mechanické zábranné prostředky, kterými jsou úschovné objekty, zámky, dveře, mříže, fólie, bezpečnostní rámy a skla, elektrická zámková zařízení a systémy pro zabezpečení vstupů do objektů a zabezpečených oblastí.

Mezi technické prostředky řadíme :

- ACS systémy: zařízení elektrické zabezpečovací signalizace sloužící ke zjišťování a vyhodnocování neoprávněného vstupu,

- PZS: speciální televizní systémy pro snímání, přenos a zobrazování pohybu osob a dopravních prostředků v objektech,

- CCTV systémy: tísňové systémy, zejména tísňové hlásiče, které fungují jako součást elektrické zabezpečovací signalizace,

- Tísňové systémy,

- EPS systémy: detektory látek nebo zařízení sloužící zejména k vyhledávání kovů, zařízení fyzického ničení nosičů informací,

- Skart systémy: zařízení proti pasivnímu a aktivnímu odposlechu utajované skutečnosti z míst vně objektu,

- Zařízení fyzického ničení nosičů informací. [8]

Míra zabezpečení jednací oblasti a zabezpečené oblasti opatřeními fyzické bezpečnosti se určuje pomocí bodových hodnot, bodové hodnocení se přiřazuje certifikovaným a necertifikovaným technickým prostředkům tyto hodnoty a nejnižší míry zabezpečení jsou stanoveny prováděcím právním předpisem. Opatření fyzické bezpečnosti nebo kombinace těchto opatření musí odpovídat nejnižší míře zabezpečení jednací oblasti nebo zabezpečené oblasti, která se stanoví v závislosti na vyhodnocení rizik a na stupni utajení utajovaných informací, které jsou v jednací oblasti pravidelně projednávány.

1.4 Projekt fyzické bezpečnosti

Projekt fyzické bezpečnosti se vytváří pokud se v objektu nachází oblasti kategorie důvěrné, tajné, přísně tajné. Obsahem je návrh systému ochrany utajovaných informací. Představuje seznámení se specifiky orgánu státu nebo podnikatele, poskytnutí nezbytných podkladových materiálů a vytipování optimálních prostor určených pro manipulaci s utajovanými informacemi. Tyto jsou vytipovány s ohledem na minimální náklady spojené s jejich technickým zabezpečením, tak s ohledem na provozní potřeby uživatele. Rovněž je přihlédnuto k stávajícímu využití prostor. Na závěr je společně s uživatelem zvolena optimální varianta určení "objektu", zabezpečené oblasti a jejich zabezpečení. Součástí je i nezbytná koordinace při výběru z nabídek dodavatelů technologií a služeb.

Tento projekt musí obsahovat :

- určení tříd zabezpečených oblastí, určení objektu včetně hranic,

- vyhodnocení rizik,

- způsob použití fyzické bezpečnosti,

- provozní řád objektu,

- plán zabezpečení objektu a zabezpečených oblastí v krizových situacích.

Projekt fyzické bezpečnosti kategorie vyhrazené obsahuje :

- určení tříd zabezpečených oblastí, určení objektu včetně hranic,

- způsob opatření fyzické bezpečnosti.

Projekt fyzické bezpečnosti pro jednací oblast obsahuje :

- určení objektu a jednací oblasti, včetně jejich hranic,

- vyhodnocení rizik,

- způsob použití opatření fyzické bezpečnosti,

- provozní řád objektu,

- plán zabezpečení objektu a jednací oblasti v krizových situacích.

Určení objektu a jednací oblasti, včetně jejich hranic. Jedná se část projektu fyzické bezpečnosti, která nám stanovuje požadavky na objekt.

- určení typu objektu, stanovení jeho kategorie a hranic,

- popis zabezpečení,

- stanovení zabezpečených oblastí, určení typu a jejich tříd,

- popis zabezpečení (technické zabezpečení, režimová ochrana, fyzická ochrana, hodnocení bezpečnostních opatření). [9]

Vyhodnocení rizik zahrnuje

- stanovení míry a rizika,

- vyhodnocení hrozeb a zranitelnosti,

- specifikace aktiv.

Způsob použití opatření fyzické bezpečnosti:

- hodnocení bezpečnostních opatření pro každou zabezpečenou oblast,

- výkresovou dokumentaci, která zahrnuje vyznačení hranic, specifikaci použitých technických prostředků,

- způsob použití technických prostředků, parametry a jejich údaje,

- certifikáty použitých technických prostředků certifikovaných NBÚ,

- prohlášení o shodě pro technické prostředky necertifikované NBÚ včetně způsobu jejich použití. [9]

Na závěr zahrnujeme implementaci projektu fyzické bezpečnosti do podmínek klienta. Součástí je spolupráce s dodavateli technického zabezpečení nebo zajištění dodávek subdodavatelem, který je vybrán klientem. Dále je provedeno školení osoby odpovědné za ochranu utajovaných informací a jednotlivých uživatelů. Podle požadavků klienta je možné provést také školení všech zaměstnanců, školení ostrahy. Také je provedeno ověření shody realizace opatření fyzické bezpečnosti s projektem fyzické bezpečnosti. Dojde-li v průběhu realizace zabezpečení ke změnám, jsou zapracovány přímo do projektu fyzické bezpečnosti nebo formou dodatku. [9]

Plán zabezpečení objektu a jednací oblasti v krizových situacích:

Plán zabezpečení objektu a jednacích oblastí stanovuje základní postupy, kdy dochází k ohrožení utajovaných informací. Plán obsahuje:

- opatření k minimalizaci hrozeb a zranitelnosti utajovaných informací

- pokyny a postupy pro ochranu utajovaných informací při vzniku mimořádné situace

Opatření jsou stanovena na požadavcích klienta. Součástí zpracování je pořízení knihy návštěv a klíčů. Projekt je nejprve vypracován v tzv. pracovní verzi, která je konzultovaná s klientem a na základě toho je vyhotovena konečná verze čistopis. V zavedení systému jakosti ISO 9001 se na zpracování projektu podílejí 2 osoby (konzultanti) specialisté na fyzickou bezpečnost. První z nich je zpracovatelem a druhý oponentem. V závěru je jejich projekt ověřen manažerem produktu a předán výstupní kontrole. [9]

Dílčí závěr:

V této kapitole jsme provedl výčet základních pojmů, které jsou spíše pro seznámení. Bezpochybně mezi ně patří druhy utajovaných informací, podmínky pro vydání osvědčení fyzické osoby a podnikatele včetně vzorů certifikátů jak by měly vypadat. V další části této kapitoly jsem popsal co to je zabezpečená oblast a jednací oblast a dále jsem se zabýval důležitou částí opatření fyzické bezpečnosti. Uvedení kapitoly má důležitý význam, protože touto částí jsou definovány co je to ostraha jaké je režimové opatření a hlavně technické prostředky, kdy se těmito prostředky zabývám v praktické části pro zabezpečenou oblast pro stupeň tajné. Další částí je projekt fyzické bezpečnosti. Jedná se o takové seznámení jak by měl projekt fyzické bezpečnosti vypadat a co by měl obsahovat.

2 ANALÝZA POŽADAVKŮ NA TECHNICKÉ PROSTŘEDKY

Problematiku těchto požadavků řeší v národním právním řádu Vyhláška č.528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků (dále jen Vyhláška o fyzické bezpečnosti) která upravuje opatření fyzické bezpečnosti, nejnižší míru zabezpečení zabezpečené oblasti, metodu hodnocení rizik a certifikaci technických prostředků.

Vyhláška představuje rovněž směrnici jak postupovat při realizaci projektu fyzické bezpečnosti a účelem je poskytnout informace jak tento projekt realizovat.

Pojmy vyhlášky:

- objektem je budova nebo jiný ohraničený prostor ve kterém se nachází zabezpečená oblast,

- hranicí objetu je myšlen plášť budovy,

- hranicí zabezpečené oblasti nebo jednací oblasti je stavebně ohraničený prostor,

- vstup a výstup zabezpečené oblasti a jednací oblasti je místo určené příslušným osobám nebo jeho doprovodu,

- provozovatelem objektu je odpovědná osoba,

- při narušení fyzické bezpečnosti hrozí odcizení zneužití utajované informace,

- mimořádnou situací se rozumí pokud dojde k vyzrazení nebo zneužití utajovaní informace,

- použití technických prostředků se zabraňuje, oznamuje narušení nebo odcizení utajované informace,

- úschovný objekt trezor, skříň, uzamykatelná schránka,

- útočníkem je fyzická osoba, která se snaží překonat zabezpečení zabezpečené oblasti nebo jednací oblasti za účelem odcizení a následně zneužití utajované informace. [2]

2.1 Ověřování opatření fyzické bezpečnosti a vyhodnocení rizik

Ověřování opatření fyzické bezpečnosti znamená zda jednotlivá opatření fyzické bezpečnosti a také vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a předpisům z oblasti utajovaných informací. Na základě tohoto provádí ověření provozovatel nebo pověřená osoba objektu nejméně každých 12 měsíců.

Vyhodnocení rizik se provádí

a) identifikací stupňů utajovaných informací a zjištěním množství utajovaných informací, které se v objektu vyskytují nebo budou vyskytovat, zejména z hlediska následku jejich vyzrazení nebo zneužití,

b) popisem a vyhodnocením hrozeb, kterým jsou tyto utajované informace vystaveny,

c) popisem a vyhodnocením zranitelnosti utajovaných informací vůči těmto hrozbám,

d) stanovením míry rizika, jako "malé", "střední" nebo "velké", na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací.

V případě změny opatření fyzické bezpečnosti provozovatel objektu nebo jím pověřená osoba neprodleně zajistí shodu s projektem fyzické bezpečnosti. [2]

V příloze č.1 vyhlášky 528/2005 o fyzické bezpečnosti a certifikaci technických prostředků je rozdělení jednotlivých systému požadovaných oblastí značeno formou S nebo SS. Toto značení je u každého technického zařízení pro zabezpečení zabezpečené oblasti nebo jednací oblasti, které určuje hodnotu a typ. Hodnoty nám slouží k tomu jak vypočítat příslušnou kategorii z tabulky míry rizik pro určitý stupeň. Podrobnější počítání se bude řešit v praktické části diplomové práce.

Příklad pro stupeň přísně tajné:

Tab. 2. Tabulka bodových hodnot nejnižší míry zabezpečení [10]

ZABEZPEČENÁ OBLAST KATEGORIE Přísně Tajné	Míra rizika		
	malá	střední	velká
Povinné : (S1) + (S2) + (S3)	10	11	13
Povinné : (S4) + (S5) *	6	7	7
Nepovinné : (S6)	4	5	5
Celkový výsledek	**20**	**23**	**25**

Bezpečnostní opatření jsou typově a bodově ohodnoceny. Mezi bezpečnostní opatření spadají:

- úschovné objekty, zámky úschovných objektů, úschovné objekty včetně uzamykacího systému, zabezpečené oblasti, uzamykací systémy zabezpečené oblasti, objekt, kontrola vstupu, režim návštěv objektu, ostraha, zařízení elektrické zabezpečovací signalizace, instalace PZS, fyzické bariéry, kontrola vstupu v přístupových bodech, osvětlení perimetru, speciální televizní systém perimetru. [10]

2.2 Zabezpečení zabezpečené oblasti

Zabezpečení zabezpečené oblasti:

Hranici zabezpečené oblasti a její zařazení do příslušné kategorie[6)] a třídy stanoví provozovatel objektu. Hranici objektu stanoví provozovatel objektu.

Zabezpečení zabezpečené oblasti a hranice objektu je zajišťováno kombinací opatření fyzické bezpečnosti.

Rozsah použití technických prostředků k zabezpečení zabezpečené oblasti se stanoví v závislosti na kategorii a třídě dané zabezpečené oblasti a vyhodnocení rizik.

- *pro kategorii **Vyhrazené** - mechanické zábranné prostředky,*

- *pro kategorii **Důvěrné** - mechanické zábranné prostředky a zařízení elektrické zabezpečovací signalizace,*

- *pro kategorii **Tajné a Přísně tajné** - mechanické zábranné prostředky, systémy pro kontrolu vstupů, zařízení elektrické zabezpečovací signalizace, speciální televizní systémy, zařízení elektrické požární signalizace.*

*Zabezpečené oblasti kategorie **Důvěrné a vyšší**, v nichž je zajištěna trvalá přítomnost zde pracujících osob, se zabezpečují zejména mechanickými zábrannými prostředky a zařízením elektrické zabezpečovací signalizace a nebo tísňovým systémem. Plní-li tyto zabezpečené oblasti současně úlohu stanovišť určených pro stálý výkon ostrahy, nemusí být*

vybaveny zařízeními elektrické zabezpečovací signalizace. Při použití speciálních televizních systémů nesmí být narušena ochrana utajovaných informací.

K zajištění ochrany zabezpečených oblastí kategorie Vyhrazené se používají certifikované nebo necertifikované technické prostředky.

K zajištění ochrany zabezpečených oblastí kategorie Důvěrné a vyšší se používají certifikované technické prostředky. Necertifikované technické prostředky lze použít pouze za předpokladu, že nesníží úroveň ochrany požadované pro daný stupeň utajení.

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. [2]

Požadavky na PZS

Požadavky na technické prky vychází z přílohy č. 1 vyhlášky 528/2005 Sb.

Každý prvek má svůj specifický symbol, který se značí hodnotou S nebo SS. Tyto hodnoty mají různé bodové ohodnocení, pro jednotlivé typy, protože následný výpočet zabezpečení zabezpečené oblasti nebo jednací oblasti pro důvěrné - přísně tajné, musí vycházet z těchto stanovených bodových hodnot.

Například SS91 znamená, že se jedná o prvky poplachových zabezpečovacích systémů a jaký zvolíme typ záleží na našich požadavcích.

Tab. 3. Požadavky na PZS dle různých typů

Označení a body	PZS typ 4	PZS typ 3	PZS typ 2	PZS typ 1
SS91 = 4body	ČSN EN 50131-1	ČSN EN 50131-1	ČSN EN 50131-1	Tento typ
SS91 = 3body	stupeň zabezp.	střední až	nízké až	není
SS91 = 2body	vysoké riziko	vysoké	střední	certifikovaný
SS91 = 1body	ČSN EN 50134-1	ČSN EN 50134-1	ČSN EN 50134-1	úřadem

Požadavky na instalaci PZS

Tab. 4. Požadavky na instalaci PZS dle různých typů

Označení a body	PZS typ 4	PZS typ 3	PZS typ 2	PZS typ 1
SS92 = 4body	prostorová	prostorová	prostorová	Je realizovaná
SS92 = 3body	plášťová	plášťová	plášťová	v rozsahu
SS92 = 2body	tísňový systém	tísňový systém	průlezné otvory	prostorové
SS92 = 1body	otřesová čidla		nad 5,5m	ochrany

Výpočet hodnoty SS9, kterou potřebujeme do bodového hodnocení se vypočítá pomocí tohoto vzorce. Maximální hodnota výsledku může být 4. Je-li v zabezpečené oblasti trvalá přítomnost jedné osoby nemusí se instalovat zařízení PZS, v tomto případě je hodnota

SS9 = 4.

SS9 = (SS91+SS92)/2xSS92/OBL OBL.. bodová hodnota zabezpečené oblasti

Tab. 5. Bodová hodnota zabezpečené oblasti [10]

Kategorie zabezpečené oblasti	Bodová hodnota **OBL**
Přísně tajné	4 body
Tajné	3 body
Důvěrné	2 body
Vyhrazené	1 bod

Požadavky na ACS

Systém kontroly vstupu musí být certifikovaný úřadem u typu 2-4 musí být výstupní poplachový signál vyveden na celé stanoviště ostrahy.

Tab. 6. Požadavky na ACS dle různých typů

Označení a body	ACS typ 4	ACS typ 3	ACS typ 2	ACS typ 1
SS6 = 4body	ČSN EN 50133-1	ČSN EN 50133-1	ČSN EN 50133-1	Uzamykatelná
SS6 = 3body	třída přístupu B	třída přístupu B	třída přístupu A	mechanická
SS6 = 2body	třída identifik. 3	třída identifik. 2	třída identifik. 1	zábrana
SS6 = 1body	na všech vstup.	na všech vstup.	na všech vstup.	na všech vstup.

Požadavky na CCTV

Tyto systémy slouží pro přenos, snímání a zobrazování pohybu osob a dopravních prostředků a musí být certifikované úřadem. U speciálních televizních systému se certifikují kamery a řídící jednotky. [10]

Požadavky na EPS

Hlásiče musí být zapojeny do ústředny EPS nebo do ústředny PZS. V obou případech musí být vyveden signál poplachu na stanoviště ostrahy. EPS musí být certifikováno úřadem a splňovat požadavky norem. [10]

Tab. 7. Požadavky na EPS

ČSN EN 54-1	EPS - úvod
ČSN EN 54-2	EPS - ústředna
ČSN EN 54-3	EPS - Sirény
ČSN EN 54-4	EPS - Napájecí zdroj
ČSN EN 54-5	EPS - Hlásiče teplot
ČSN EN 54-6	EPS - Hlásiče kouře
ČSN EN 54-7	EPS - Tlačítkové hlásiče

Požadavky na trezory (úschovné objekty)

U typu 3-4 se jedná o trezory, trezorové dveře a komorové trezory kde může být uložen kryptografický materiál, kdy musí být vybaven třípolohovým kombinačním zámkem.

Tab. 8. Požadavky na trezory dle různých typů

Označení a body	Trezor typ 4	Trezor typ 3	Trezor typ 2	Trezor typ 1
SS1 = 4body	ČSN EN 1143-1	ČSN EN 1143-1	ČSN EN 1143-1	Ocelová skříň
SS1 = 3body	bez. Třída 2	bez. Třída 1	bez. Třída 0	třístranný
SS1 = 2body	zámek tř. A	zámek tř. A	zámek tř. A	rozvorový
SS1 = 1body	ČSN EN 1300	ČSN EN 1300	ČSN EN 1300	mechanismus

Tab. 9. Požadavky na úschovný objekt dle různých typů

Označení a body	Trezor typ 1A	Trezor typ 1B	Trezor typ 1C	Trezor typ 1T	Trezor typ T	Trezor typ 0
S1 = 1body	uzamykací	uzamykací	uzamykací	Není certifik.	Je certifik.	Není certifik.
S1 = 2body	systém	systém	systém	úřadem	úřadem a	pevná konstr.
S1 = 3body	bezp. Třída Z1	bezp. Třída Z2	bezp. Třída Z3	posuzuje	musí splňovat	schránka
S1 = 1body	ČSN 91 6012	ČSN 91 6012	ČSN 91 6012	provozovatel	požad. 1T	kancel. Nábytek
S1 = neuvedeno						
S1 = 0body						

Požadavky na zařízení fyzického ničení nosičů informací

Rozlišujeme několik typů zařízení fyzických ničení nosičů informací, které jsou určeny k ničení utajovaných informací.

TYP 4:

Tyto zařízení fyzického ničení nosičů utajovaných informací jsou určena pro stupně přísně tajné nebo nižší a jsou certifikovány úřadem. Všechny tyto typy nemají bodové ohodnocení.

Tab. 10. Požadavky na zařízení fyzického ničení nosičů informací typ 4 [10]

Nosič informací	Velikost odpadních částic	
Např. papír, film z polyesteru s uložením informace v originální velikosti, kov, umělá hmota, identifikační karty	šířka částic	≤ 0,8 mm
	délka částic	≤ 13,0 mm
Např. film z polyesteru s uložením informace ve zmenšené velikosti, jako mikrofilm, čipové karty	plocha částic	≤ 0,2 mm^2

TYP 3:

Zařízení fyzického ničení nosičů utajovaných informací určeny pro tajné nebo nižší a jsou certifikovány úřadem.

Tab. 11. Požadavky na zařízení fyzického ničení nosičů informací typ 3 [10]

Nosič informací	Velikost odpadních částic	
Např. papír, film z polyesteru s uložením informace v originální velikosti, kov, umělá hmota, identifikační karty	šířka částic	≤ 2,0 mm
	délka částic	≤ 15,0 mm
Např. film z polyesteru s uložením informace ve zmenšené velikosti, jako mikrofilm, čipové karty	plocha částic	≤ 0,5 mm^2

TYP 2:

Zařízení fyzického ničení nosičů utajovaných informací určeny pro důvěrné nebo nižší a jsou certifikovány úřadem.

Tab. 12. Požadavky na zařízení fyzického ničení nosičů informací typ 2 [10]

Nosič informací	Velikost odpadních částic		
Např. papír, film z polyesteru s uložením informace v originální velikosti, kov	křížový řez	šířka částic	≤ 4,0 mm
		délka částic	≤ 80,0 mm
	přímý řez	šířka pruhu	≤ 2,0 mm
		délka pruhu	≤ 297,0 mm
		plocha částic*	≤ 320,0 mm^2
Umělá hmota, např. identifikační karty	šířka částic		≤ 4,0 mm
	délka částic		≤ 80,0 mm
Např. film z polyesteru s uložením informace ve zmenšené velikosti, jako mikrofilm, čipové karty	plocha částic		≤ 1,0 mm^2

TYP 1:

Zařízení fyzického ničení nosičů utajovaných informací určeny pro vyhrazené.

Tab. 13. Požadavky na zařízení fyzického ničení nosičů informací typ 1 [10]

Nosič informací	Velikost odpadních částic		
Např. papír, film z polyesteru s uložením informace v originální velikosti, kov	přímý řez	šířka pruhu	≤ 6,0 mm
		délka pruhu	neomezena
		plocha částic*	≤ 320,0 mm^2

TYP 0:

Jsou určeny pro ničení utajovaných informací přísně tajné nebo nižší. K ničení se používá pálení nebo roztavení, přičemž teplota musí vést k úplnému zničení utajované informace a nemožnosti obnovení. [10]

Uzamykací systémy zabezpečené oblasti:

Uzamykacím systémem se rozumí systémy mechanických zábranných prostředků zejména zámky, dveře, mříže, folie, skla a další bezpečnostní konstrukční a stavební prvky. Mechanickými zábrannými prostředky se zabezpečují průlezné otvory, které dovolí průchod o níže uvedených rozměrech:

Tab. 14 . Rozměry průlezných otvorů [10]

Průlezný otvor	Rozměr
obdélník	400mmx250mm
elipsa	400mmx300mm
kruh	průměr 350mm

Tab. 15. Uzamykací systémy dle různých typů

Uzamykací systém typ 0	Uzamykací systém typ 1	Uzamykací systém typ 2	Uzamykací systém typ 3	Uzamykací systém typ 4
není	Certifikovaný úřadem	Certifikovaný úřadem	Certifikovaný úřadem	Certifikovaný úřadem
Certifikovaný úřadem	uzam. Syst. A jeho	uzam. Syst. A jeho	uzam. Syst. A jeho	uzam. Syst. A jeho
	komponenty	komponenty	komponenty	komponenty
	bezp. Tř. 2	bezp. Tř. 3	bezp. Tř. 4	bezp. Tř. 5
	ČSN P ENV 1627	ČSN P ENV 1627	ČSN P ENV 1627	ČSN P ENV 1627

Zabezpečení jednacích oblastí:

Hranici jednací oblasti a hranici objektu stanoví provozovatel objektu.

Zabezpečení jednací oblasti a hranice objektu je zajišťováno kombinací opatření fyzické bezpečnosti.

Rozsah použití opatření fyzické bezpečnosti k zabezpečení jednací oblasti se stanoví v závislosti na stupni utajovaných informací, které jsou v jednací oblasti pravidelně projednávány a na vyhodnocení rizik.

Jednací oblasti pro pravidelné projednávání utajovaných informací stupňů utajení Tajné a Přísně tajné, se zabezpečují mechanickými zábrannými prostředky, systémy pro kontrolu vstupů, zařízeními elektrické zabezpečovací signalizace, speciálními televizními systémy, zařízeními elektrické požární signalizace, zařízeními proti pasivnímu a aktivnímu odposlechu utajované informace.

Speciální televizní systémy lze nahradit tísňovými systémy.

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

Zabezpečení jednací oblasti se dále provádí na hranici objektu, ve kterém se tato oblast nachází. Rozsah použití technických prostředků je stanoven v závislosti na stupni utajovaných informací, které jsou v jednací oblasti pravidelně projednávány a na základě vyhodnocení rizik a dále s ohledem na charakter hranice objektu. Hranice objektu je zabezpečena mechanickými zábrannými prostředky, zařízením elektrické zabezpečovací signalizace a speciálním televizním systémem.

V objektu se umísťuje zařízení fyzického ničení nosičů informací.

V případě, že hranice objektu je totožná s hranicí jednací oblasti, je rozsah použití opatření fyzické bezpečnosti určen požadavky na zabezpečení jednací oblasti. [2]

Fyzický bezpečnostní perimetr:

Prostory ve kterých dochází k manipulaci nebo kontaktu s utajovanými informacemi musí být zabezpečeny dle požadavků stupně utajení. Tento prostor lze zabezpečit fyzickou ostrahou nebo detektory.

Řešení:

- vypracování projektu ochrany,

- audit současného stavu,

- analýza prostorů , které můžou být narušeny,

- dodávka a montáž prvků,

- proškolení zaměstnanců.

Kontrola vstupu a pohybu osob:

Do zabezpečených oblastí mají přistup pouze oprávněné osoby, ale i přesto musí být tyto oblasti chráněny fyzickou ostrahou, elektronickou kontrolou vstupu a nebo jejich vhodnou kombinací.

Řešení:

- vypracování projektu režimových opatření,

- rozdělení prostorů do jednotlivých zón,

- zabezpečení bezpečnostní službou,

- přístupová oprávnění.

Obr. 5. Fyzická ostraha objektu [11]

Ochrana před hrozbami přírodního charakteru:

Pro zabezpečení ochrany proti požárům, povodním, vichřicím, zemětřesením, výbuchem musí být aplikovány opatření v krizové situaci.

- audit současného stavu,

- projektování EPS,

- projektování PZS,

- instalace podpůrných PZS prostředků (detektory zaplavení, úniku plynu, otřesové detektory),

- vypracování krizového plánu.

2.3 Zabezpečení technického zařízení

Technické zařízení, které obsahuje utajovanou informaci stupně důvěrné a vyšší se ukládá v zabezpečené oblasti. Hranici, rozsah a způsob použití technických prostředků této oblasti stanovuje provozovatel objektu, aby zajistil informovanost ostrahy o narušení útočníkem, aby jej zpomalil nebo mu úplně zabránil cestu k utajované informaci v technickém zařízení. Zabezpečení je zajišťováno kombinací opatření fyzické bezpečnosti. K zajištění ochrany oblasti a objektu se používají certifikované i necertifikované prostředky, ale většina provozovatelů se přikloní spíše k těm certifikovaným.

Typy fyzické ostrahy:

- **strážní a recepční služba** – denní i noční provoz, pravidelná kontrola objektu, kontrola vozidel, evidence,

- **ostraha objektů** – kontrolní pochůzková činnost, spolehliví pracovníci ostrahy vybaveni donucovacími prostředky, cvičenými psy,
- **pořadatelská služba** – ostraha při hudebních, sportovních či jiných produkcích;
- **bodyguarding** – osobní ochrana osob; přímá ochrana zákazníka před fyzickým či verbálním napadením,
- **doprovod** – ochrana při přepravě finanční hotovosti a cenin;

Pro ochranu technického zařízení, které obsahuje utajovanou informaci stupně **důvěrné** se stanovuje ostraha typu 4 nebo vyšší, kde spadají příslušníci ozbrojených sil nebo ozbrojených sborů. Ostraha provádí obchůzky v pravidelných intervalech ne větším jak 6 hodin, v noci se samozřejmě četnost obchůzek zvyšuje. V době obchůzek musí zůstat vždy alespoň jedna osoba na stanovišti.

Pro ostrahu technického zařízení obsahující utajovanou informaci stupně **tajné** je použita zase ostraha typu 4, ale s jedním rozdílem, že obchůzky se vykonávají v pravidelném intervalu větším něž 4 hodiny.

Pro ostrahu technického zařízení obsahující utajovanou informaci stupně **přísně tajné** je použita ostraha typu 5, pod kterou spadají příslušníci ozbrojených sil nebo sborů. Ostraha provádí obchůzky po náhodných trasách v intervalu ne větší než 2 hodiny. V době obchůzek musí zůstat vždy alespoň jedna osoba na stanovišti.

Povinnosti provozovatele objektu je stanovit limity pro ostrahu, které se musí dodržet při zásahu proti útočníkovy na základě překážek a druhu technických prostředků, které útočník musí překonat k utajované informaci. Zásah ostrahy proti tomuto útočníkovy je prováděn minimálně dvěma fyzickými osobami v jakémkoli místě objektu, kde došlo k poplachu. Ostraha provádí zásah proti útočníkovy v časovém limitu, který stanovil provozovatel objektu. Tyto limity musí být pravidelně prověřovány a uvádí se v projektu fyzické bezpečnosti. [2]

Dílčí závěr :

Výše uvedená kapitola řeší základní údaje o problematice zabezpečení zabezpečených oblastí, zabezpečení jednacích oblastí a zabezpečení technického zařízení. Důležitou částí v této kapitole jsou požadavky na technické prostředky, kdy jsem znázornil tabulkově kolik bodů a jaké značení má každý typ a druh technického prostředku. Kapitola dále řeší ověřování opatření fyzické bezpečnosti a jak se provádí vyhodnocení rizik.

3 CERTIFIKACE TECHNICKÝCH PROSTŘEDKŮ

3.1 Úvod

Certifikací technických prostředků se rozumí způsobilost zařízení k ochraně utajovaných informací, posouzení technický parametrů a vystavení certifikátu na základě vypracovaného odborného posudku akreditované zkušební laboratoře.

Certifikace je činnost :

- autorizované osoby - právnická osoba, která je provádí certifikaci v rozsahu vymezeném technickým předpisem,

- akreditované osoby - prováděna na žádost výrobce nebo jiné osoby, při níž se osvědčí, že výrobek nebo jeho výroba případně jeho opakované použití jsou v souladu s certifikáty technických požadavků.

3.2 Společná ustanovení certifikace

Certifikace je postup, kterou na základě žádosti a splnění požadavků provádí NBÚ a ověřuje:

- způsobilost technického prostředku utajovaných informací,

- způsobilost informačního systému k nakládaní utajovaných informací,

- způsobilost kryptografického prostředku k ochraně utajovaných informací,

- způsobilost kryptografického pracoviště,

- způsobilost stínící komory k ochraně utajovaných informací,

Jestliže není zajištěna tato způsobilost úřad rozhodne o nevydání certifikátu. Odvolání proti tomuto rozhodnutí je nepřípustné. Vydání posudku ověřování způsobilosti, může úřad uzavřít s orgánem státu nebo podnikatelem smlouvu, která se týká všech kromě způsobilosti technických prostředků utajovaných informací, ale taky může dojít k situaci, kdy tato smlouva neplatí, protože ověřování způsobilosti z důvodu utajení nelze provést. Toto ověření může být provozováno zpravodajskými službami, které ve výsledku předají všechny patřičné podklady úřadu. Seznam orgánů nebo podnikatelů, kteří mají smlouvu s úřadem je zveřejněn ve věštníku úřadu. [1]

3.3 Certifikáty

Certifikát vystavuje Národní bezpečnostní úřad (NBÚ) na základě žádosti výrobce, zákazníka, dovozce, prodejce v souladu s vyhláškou 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků.

Certifikáty vydané autorizovanou osobou se využívají při posuzování shody a certifikáty vydané akreditovanou osobou lze využít jako podklad pouze v případě, jestli je k posouzení schody oprávněn výrobce, dovozce.

Základem je popsat certifikaci výrobků, jejichž výstup využívá Národní bezpečnostní úřad pro certifikaci technických prostředků podle zákona č.412/2005 sb. [1]

Certifikáty technického prostředku musí obsahovat :

- evidenční číslo,

- název a typ technického prostředku,

- identifikaci výrobce, identifikačním číslem osoby,

- identifikaci držitele certifikátu,

- datum vydáni a platnosti certifikátu,

- hodnocení prostředku,

- podpis pověřeného zástupce úřadu, který musí mít oprávnění a otisk razítka. [1]

Certifikáty informačního systému k nakládání utajovaných informací musí obsahovat:

- evidenční číslo,

- identifikaci držitele certifikátu,

- datum vydání a platnosti certifikátu,

- podpis pověřeného zástupce úřadu, který musí mít oprávnění a otisk razítka,

- stupeň utajení, pro který byla tato způsobilost informačního systému ověřena. [1]

Certifikáty kryptografického prostředku musí obsahovat:

- evidenční číslo,

- identifikaci držitele certifikátu,

- datum vydání a platnosti certifikátu,

- podpis pověřeného zástupce úřadu, který musí mít oprávnění a otisk razítka,

- identifikaci kryptografického prostředku,

- identifikace výrobce kryptografického prostředku,

- stupeň utajení , pro který byla způsobilost kryptografického prostředku schválena. [1]

Certifikáty kryptografického pracoviště musí obsahovat:

- evidenční číslo,

- identifikaci držitele certifikátu,

- datum vydání a platnosti certifikátu,

- podpis pověřeného zástupce úřadu, který musí mít oprávnění a otisk razítka,

- identifikaci a specifikaci kryptografického pracoviště,

- rozsah způsobilosti kryptografického pracoviště. [1]

Certifikáty stínící komory musí obsahovat:

- evidenční číslo,

- identifikaci držitele certifikátu,

- datum vydání a platnosti certifikátu,

- podpis pověřeného zástupce úřadu, který musí mít oprávnění a otisk razítka,

- identifikaci stínící komory,

- identifikace výrobce stínící komory,

- stupeň utajení , pro který byla způsobilost stínící komory schválena. [1]

Vzor certifikátu:

Příloha č. 2 k vyhlášce č. …/2005 Sb.

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
Pošt. přihr. 49
150 06 Praha 56

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

C E R T I F I K Á T

technického prostředku

Evidenční číslo: ……..

……..
(Název a typové označení technického prostředku)

Výrobce:
Sídlo/trvalý pobyt/ místo podnikání/adresa: IČ/ rodné číslo
Držitel:
Sídlo/trvalý pobytu/místo podnikání/adresa: IČ/ rodné číslo:

Tento certifikát potvrzuje ověření způsobilosti technického prostředku typu:

……

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

……..

Platnost certifikátu do:
Datum vydání certifikátu:

Otisk úředního razítka

Podpis oprávněného zástupce

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

40

Obr. 6. Vzor certifikátu [10]

3.4 Náležitosti žádosti o certifikaci technického prostředku

O certifikaci technického prostředku žádáme NBÚ a musí obsahovat :

- identifikaci žadatele

1. *obchodní firmou, popřípadě názvem, sídlem a identifikačním číslem, je-li žadatelem právnická osoba,*
2. *obchodní firmou, popřípadě jménem a příjmením, případně odlišujícím dodatkem, trvalým pobytem a místem podnikání, liší-li se od trvalého pobytu, datem narození a identifikačním číslem, je-li žadatelem fyzická osoba, která je podnikatelem, nebo*
3. *názvem, sídlem, identifikačním číslem a jménem a příjmením odpovědné osoby, jde-li o orgán státu.*

- výčet a označení technických prostředků a seznam předkládané dokumentace.

K žádosti podle odstavce 1 se přiloží tato dokumentace

specifikace a popis technického prostředku,

prohlášení o nezávadnosti či shodě technického prostředku[8)],

certifikát shody nebo prohlášení o stejném složení a provedení technického prostředku, které obsahuje prohlášení výrobce, že technický prostředek bude vyráběn ve stejném složení a provedení, jak byl specifikován v posudku. [2]

Žádost o certifikaci technického prostředku a platnost certifikátu:

O certifikaci technického prostředku musí písemně zažádat výrobce, dovozce, distributor nebo uživatel technického prostředku na příslušném úřadu. Tento úřad stanovuje dobu platnosti certifikátu technického prostředku tato doba se pohybuje maximálně do 5 let. Seznam technických prostředků u kterých výrobci žádají certifikáty se nachází ve věštníku úřadu. Platnost tohoto certifikátu může zaniknout jestliže uplynula doba jeho platnosti nebo na žádost úřadu jestliže zjistí, že technický prostředek nesplňuje dané požadavky.

Úřad stanovuje jednu výjimku, jestliže uplyne doba platnosti technického prostředku k ochraně utajovaných informací, tento výrobek se může nadále používat. [1]

Žádost o certifikaci informačního systému a platnost certifikátu:

O certifikaci informačního systému písemně žádá úřad provozovatel IS, orgán státu nebo podnikatel, který bude informační systém provozovat. Pravidla jsou pořád stejná tak jako u technického prostředku tzn. ten kdo požádal o certifikaci musí předložit na úřad žádost a příslušnou dokumentaci nezbytnou pro provedení certifikace. Dobu platnosti certifikátu stanovuje úřad.

Platnost tohoto certifikátu je pro stupně utajení :

- přísně tajné a tajné maximálně 2 roky,

- důvěrné maximálně 3 roky,

- vyhrazené maximálně 5 let.

Platnost tohoto certifikátu zaniká jestliže uplyne doba jeho platnosti, zánikem osvědčení podnikatele nebo rozhodnutí úřadu o jeho platnosti. Jestli chce podnikatel nebo orgán státu dále používat informační systémy jejichž platnost propadla, musí požádat písemně úřad o certifikaci. 6 měsíců předem je maximální doba, kdy můžeme požádat znovu o certifikaci informačního systému. [1]

Žádost o certifikaci kryptografického systému a platnost certifikátu:

O certifikaci kryptografického prostředku písemně žádá u úřadu podnikatel nebo orgán, u kterého bude kryptografické pracoviště. Jestliže žádá podnikatel musí být držitelem platného osvědčení. Úřad stanovuje maximální dobu platnosti certifikátu kryptografického systému na 3 roky. Platnost certifikátu zaniká jestliže uplyne doba jeho platnosti, na žádost úřadu, zánikem platnosti osvědčení a zrušením orgánu státu. Jestli má zájem podnikatel nebo orgán státu dále používat kryptografické pracoviště jejichž platnost propadla, musí požádat písemně úřad o certifikaci. Tato žádost musí být podána 6 měsíců předem jedná se o maximální dobu, kdy můžeme požádat znovu o certifikaci kryptografického pracoviště.

Úřad je povinen rozhodnout o certifikaci kryptografického pracoviště do 6 měsíců ve zvláštních případech do 1 roku. [1]

Žádost o certifikaci stínící komory a platnost certifikátu:

O certifikaci stínící komory písemně žádá u úřadu podnikatel nebo orgán státu, u kterého se předpokládá používání stínící komory. Ten kdo požádal o certifikaci musí být v jejím průběhu předložena dokumentace nezbytná pro provedení certifikace. Platnost certifikátu stínící komory stanovuje úřad maximálně na 5let. Platnost certifikátu zaniká jestliže uplyne doba jeho platnosti, zánikem planosti osvědčení, zrušením orgánu státu a na žádost úřadu. Opakovaná žádost o certifikaci stínící komory musí být předložena 12 měsíců před uplynutím doby jeho platnosti.

Komponenty PZS spadají do certifikace technických prostředků. Detektory mají samozřejmě certifikaci pro evropský trh pod značkou **CE,** nicméně jsou testovány v akreditovaných zkušebnách a podle výsledků zkoušek a platných evropských standardů tříděny do bezpečnostních kategorií. [1]

3.5 Certifikační postup a audit

Cílem certifikace je dodržování funkční jakosti, který je začleněn do organizace od vedení až po posledního dělníka.

Jakmile je nabídka klientem akceptována, je přijetí nabídky potvrzeno ze strany certifikační společnosti.
Fáze auditu číslo 1 bude provedena u všech nových klientů a zahrnuje následující:

1. *Přezkoumání dokumentace systému řízení;*
2. *Ověření adresy sídla společnosti a specifických podmínek v místě podnikání. Osobní jednání s klientem týkající se zhodnocení připravenosti organizace pro pokračování auditu fází číslo 2;*
3. *Přezkoumání stavu společnosti a seznámení s požadavky souvisejícími s normou (standardem) s ohledem na na identifikaci klíčových výkonnostních parametrů, procesů, cílů a činností managementu řízení;*

4. *Získání nezbytných informací týkajících se rozsahu certifikace systému řízení, procesů a místa činnosti klienta a dalších právních, regulačních a statutárních aspektů (např. kvalita, životní prostředí, rizika);*
5. *Přezkoumání alokace zdrojů a projednání podrobností týkajících se druhé fáze auditu;*
6. *Na základě dostatečného seznámení se systémem řízení a prováděnými procesy v organizaci bude v souladu s možnými významnými aspekty navržen plán pro provedení auditu ve fázi číslo 2;*
7. *Zhodnocení plánu a plnění interních auditů a přezkoumání managementem a zhodnocení úrovně implementace managementu řízení v organizaci.*
8. *První fáze auditu bude provedena v místě podnikání klienta za účelem dosažení cílů a záměrů uvedených výše.*

Po provedení první fáze auditu bude vypracována zpráva z auditu a následně předána klientovi. Zjištění budou klientovi vysvětlena a zaznamenána ve zprávě z auditu. Potenciální neshody označené v první fázi auditu mohou zapříčinit vznik nesouladu či neshody se standardem ve druhé fázi auditu.

Fáze auditu číslo 2 bude provedena za účelem zhodnocení implementace systému řízení a účinnosti systému řízení zákazníka. Zahrnuje následující:

1. *Informace a záznamy o shodě systémové dokumentace se všemi požadavky normy;*
2. *Monitorování, měření, reportování a vyhodnocování vůči klíčovým parametrům a cílům;*
3. *Prověření systému řízení zákazníka a soulad s legislativou;*
4. *Kontrola funkčnosti řízení procesů;*
5. *Interní audit a přezkoumání managementem;*
6. *Zodpovědnost vedení organizace za firemní politiku;*

7. *Provázání mezi normativními požadavky, předpisy, plněním plánů a cílů a dalších právních požadavků, odpovědnosti, způsobilosti zaměstnanců a činnostmi včetně interních auditů a závěrů.*

Po ukončení druhé fáze auditu, provedou členové audit týmu zhodnocení a analýzu všech informací a záznamů získaných během první a druhé fáze auditu včetně interních auditů a závěrů.
Na závěr auditu bude vypracována zpráva z auditu a předána klientovi.

- *Pokud nejsou zjištěny nedostatky (neshody či nesoulad s normou), vedoucí auditor doporučí registraci společnosti.*
- *Pokud jsou zjištěny méně závažné nedostatky (nesoulad s normou), musí je zákazník odstranit dříve, než bude možno předat doporučení k registraci společnosti.*
- *Pokud jsou zjištěny větší nedostatky (neshody), musí je zákazník odstranit a bude nutné opakování auditu v omezeném rozsahu činnosti klienta za účelem ověření, že byly nedostatky odstraněny. Po té může vedoucí auditor vydat doporučení k registraci společnosti.*
- *Jakmile je doporučena registrace společnosti a je vydán certifikát, přechází zákazník do režimu dozorového auditu. U menších firem může představovat pouhou jednodenní návštěvu dozoru za rok. Avšak u větších klientů a v závislosti na počtu certifikovaných norem může být potřeba pracovních dní pro provedení dozoru větší - viz poznámky níže.*

Po uplynutí tříletého období je prováděno nové přezkoumání, aby bylo zajištěno, že je vše v pořádku a aby mohl být vydán nový certifikát pro další tříleté období.
Před ukončením tříletého období certifikace je provedeno přezkoumání zpráv z auditu za předcházející tři roky. Opětovné posouzení auditu zajišťuje, že může být vydán nový certifikát s platností na další tříleté období. Recertifikační audit může zahrnovat první fázi auditu v případě, kdy dojde k významným změnám v systému řízení organizace (např. změny v legislativě). [12]

3.6 Podmínky nasazení technických prostředků pro zabezpečení zabezpečené oblasti

Daný výrobek můžeme použít k ochraně utajovaný informací pokud splňuje požadavky, který mu stanoví vyhláška 528/2005 Sb.

Výrobek označený značkou CE by měl splňovat všechny požadavky evropského práva na technickou bezpečnost. Zaručuje výrobku vstup na trhy všech států EU, ale neznamená, že výrobek je absolutně bezpečný.

Technická bezpečnost

- tvoří systém opatření k zabezpečení utajovaných informací technickými prostředky,

- k ochraně utajovaných informací musí být použity technické prostředky certifikované úřadem nebo jinou pověřenou organizací. Ostatní technické prostředky lze použít jen doplňkově za podmínky, že jejich užitím nedojde ke snížení úrovně ochrany požadovaný pro daný stupeň utajení,

- úřad stanoví právním předpisem opatření, technické prostředky a jejich použití při ochraně utajovaných informací.

Technické prostředky se dělí:

Podle předmětu který mají chránit

- Technické prostředky k ochraně života, zdraví (zbraně, vesty),
- Technické prostředky k ochraně majetku (zámky, ploty, PZS),
- Technické prostředky k ochraně informací (trezory, kryptografická bezpečnost)

Podle technického principu:

- MZS,
- Elektrické a elektronické systémy,

Ostatní technické prostředky (hasící přístroje, ochranné oděvy)

3.7 Konkrétní výrobky pro zabezpečení utajovaných informací

NBÚ uveřejňuje seznam výrobků pro zabezpečení utajovaných informací, který slouží pro snažší orientaci projektantů, montážních firem, dodavatelů. Tento seznam také slouží pro kontrolu jestli daný výrobek, který chceme použít a je v seznamu certifikovaných technických prostředků. Certifikace nám ověřuje předpoklady k úspěšnosti, ale nemůžeme tvrdit, že certifikovaná organizace bude určitě úspěšná. Výběr konkrétního výrobku záleží na tom co chceme zabezpečit a čím to chceme zabezpečit.

V seznamu který uveřejňuje NBÚ jsou (ACS, MZS, CCTV, EPS, PZS + tísňové systémy, zařízení fyzického ničení nosičů informací, zařízení proti aktivnímu a pasivnímu odposlechu, zařízení k vyhledávání nebezpečných látek nebo předmětů. Každá společnost musí mít certifikát schválený NBÚ ke způsobilosti použití výrobků, které spadají do příslušných kategorií v seznamu.

Ukázka certifikátu schváleným NBÚ:

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
Pošt. přihr. 49
150 06 Praha 56

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

CERTIFIKÁT
technického prostředku
Evidenční číslo: T3011/2007

Systém kontroly vstupů
ANeT-UNI-II
(Název a typové označení technického prostředku)

Výrobce: ANeT-Advanced Network Technology, s.r.o.
Sídlo: Šumavská 35, 658 56 Brno, IČ: 47916923

Držitel: ANeT - Advanced Network Technology, s.r.o.
Sídlo: Šumavská 35, 658 56 Brno, IČ: 47916923

Tento certifikát potvrzuje ověření způsobilosti technického prostředku typu:
2 - 4

Bodové hodnocení technického prostředku podle přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků:
V závislosti na realizaci systému SS6=2 až 4 body.

Platnost certifikátu do: 9.3.2010
Datum vydání certifikátu: 2.8.2007

Náměstek ředitele
Národního bezpečnostního úřadu
Ing. Jaroslav ŠMÍD

011054

Přílohy 1/1
(Příloha je nedílnou součástí certifikátu a lze je reprodukovat pouze společně)

Obr. 7. Vzor certifikátu technického prostředku [13]

3.8 Podmínky používání technických prostředků po uplynutí doby jejich platnosti

Technický prostředek nesmí být po uplynutí platnosti certifikátu pro ochranu utajovaných informací pořízen nebo nově nasazen. Technický prostředek může být nově nasazován jen v případě, jestli je doloženo, že byl v době platnosti technický prostředek nasazen nebo pořízen stejným orgánem státu, právnické osoby nebo podnikatele, u kterého je prováděno další nasazení. Tyto technické prostředky jejichž platnost vypršela mohou být znova používány za podmínky, že jsou plně funkční a tato funkčnost je ověřena funkční zkouškou.

U mechanických zábranných prostředků a zařízení fyzického ničení informací se tato funkční zkouška doloží zápisem podepsaným provozovatelem nebo jeho pověřenou osobou. U ostatních technických prostředků se tato zkouška doloží formou protokolů o zkoušce. [10]

Dílčí závěr :

Výše uvedená kapitola analyzuje rozbor prvků, které se používají do zabezpečených oblastí, jednacích oblastí nebo nám slouží pro projekt zabezpečení musí mít certifikáty, které jsou schváleny NBÚ. Dále kapitola řeší co je certifikát, druhy certifikátů a co musí obsahovat pro různé prostředky. Také se zde proveden rozbor jak by měl vypadat certifikát a jaké jsou náležitosti žádosti o certifikaci technického prostředku, co je to certifikační proces a jaké jsou výrobky pro zabezpečení utajovaných informací. Poslední podkapitola se zabývá řešením podmínek pro používání technických prostředků, jestliže doba jejich platnosti uplyne.

II. PRAKTICKÁ ČÁST

4 NÁVRH OPATŘENÍ FYZICKÉ BEZPEČNOSTI ZABEZPEČENÉ OBLASTI STUPĚŇ TAJNÉ

Návrh opatření fyzické bezpečnosti zabezpečené oblasti se stupněm utajení TAJNÉ, vychází z ustanovení zákona 412/2005 sb. o ochraně utajovaných informací a bezpečnostní způsobilosti a také z vyhlášky 528/2005 sb. o fyzické bezpečnosti a certifikaci technických prostředků a přiložené přílohy číslo 1 této vyhlášky.

Projekt fyzické bezpečnosti pro stupeň TAJNÉ musí obsahovat:

- vyhodnocení rizik,

- určení objektů, zabezpečené oblasti a jednací oblasti včetně jejich hranic a určení kategorií a tříd těchto oblastí,

- způsob opatření fyzické bezpečnosti,

K zabezpečení oblasti stupeň TAJNÉ jsou potřeba následující prostředky PZS, ACS, MZS, CCTV a EPS.

Tento projekt slouží také jako součást pro výběr dodavatele zabezpečení. Zpracovatel musí splnit veškeré legislativní požadavky na způsobilost projektanta.

Nedostatky v projektu, kterých je nutné se vyvarovat:

- projekt musí zpracovávat jedna pověřená společnost,

- technologie použitá v projektu je dostupná pouze této pověřené společnosti,

- nákladové položky můžou být nadhodnoceny,

- projekt nemusí odpovídat novým normám,

- nedostatečně platná legislativa nebo je aplikovaná nesprávně,

- zpracování projektu nepředchází bezpečnostní posouzení,

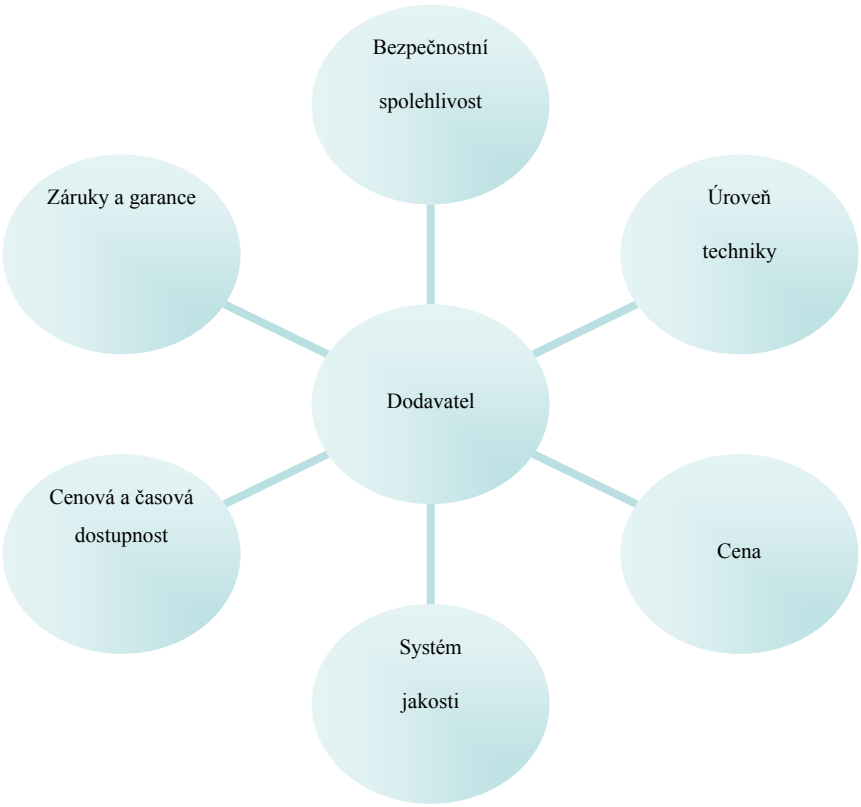
- projekt nerespektuje pojistné podmínky klienta,

Největším chybou při výběru bývá, že pověřená společnost s nejnižší cenovou nabídkou na jeho zpracování projekt realizuje a náklady bývají vyšší než ceny na trhu v České republice.

Samozřejmě hotový projekt zabezpečení se musí podrobit zkušebnímu provozu, který je nejen otázkou ověření spolehlivosti a bezporuchovosti použité technologie, ale i schopnosti uživatelů systém využívat. Ve zkušebním provozu je nutné zpracovat provozní řád, plán revizí, údržby a kontrol.

K provozu bezpečnostního systému vyžadujeme pravidelný servis, pravidelné revize, ale také hodnocení účinnosti nasazeného systému. Doplnění zařízení do tohoto systému obvykle navrhuje specialista na bezpečnostní systémy ve spolupráci s uživatelem. [14]

Na jaké zásady by jsme při výběru dodavatelů neměli zapomínat:



Obr. 8. Zásady při výběru dodavatelů

4.1 Struktura projektu fyzické bezpečnosti pro zabezpečenou oblast kategorie TAJNÉ

4.2 Vyhodnocení rizik

Úkolem hodnocení rizik je stanovit úroveň možného rizika, není-li možné zcela eliminovat nebezpečí v objektu, slabé místa se stanou potencionálním nebezpečím. Riziková analýza

určuje rovnováhu nebezpečí odpovídající pravděpodobnosti, jenž je dána s rozsahem odpovídajících škod. Tato pravděpodobnost se nechá odvodit s analýzy nebezpečí ohodnocením možných scénářů. Tyto scénáře jsou dány atraktivitou objektu pro pachatele, náklady na přípravu, rizikem pachatele a provedení trestného činu. [24]

Pravděpodobnost vniknutí je závislá na vnějších okolnostech, které jsou například:

- změna okolního prostředí,

- změna potřeb,

- změna politického klimatu,

- změna podnikového klimatu.

Tab. 16. Matice pro kvalifikaci rizik [24]

Následky škod				
Katastrofální	3	4	4	4
Značné	2	3	3	4
Nepatrné	1	2	3	3
Nevýznamné	1	1	2	3
	Nepravděpod.	výjímečné	pravděpodob.	předpokládané
	PRAVDĚPODOBNOST VZNIKU NEBEZPEČNÉ UDÁLOSTI			

Objekt je zabezpečen převážně PIR detektory, které se nachází v učebnách, přízemí a na všech chodbách.

V okolí objektu se nenachází žádné větší společenské kluby až na hospodu Bamboo, která je hned naproti školy. Tato hospoda je navštěvována spíše studenty v odpoledních i večerních hodinách a nedochází tam k žádným potyčkám a ani v okolí této oblasti nedochází k velkému vandalismu.

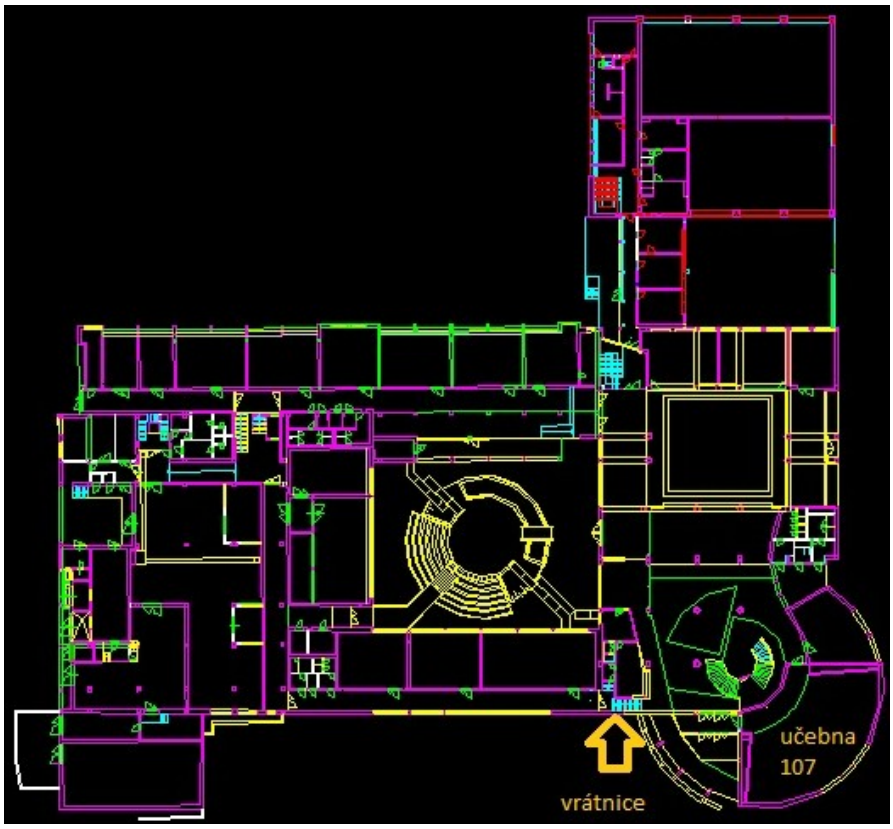
Největším problémem je sídliště, které se nachází několik stovek metrů od naší školy, které je nechvalně známá část města Zlín. Toto sídliště obývá více něž 30tisíc lidí a v noci se toto území i okolí, kde můžeme zahrnout naši školu mění na území zlodějů, násilníků, vandalů. Na tomto sídlišti podle policejních statistik dojde každých 70minutu k porušení zákona. Toto číslo je obrovský problém, protože jak si můžete všimnout na obrázku v okolí jen jedna stanice městských strážníků, kdy hlavně ve večerních hodinách nemají šanci toto území uhlídat. Díky tomuto hustě obydlenému sídlišti není náš objekt zrovna na nejlepším místě Zlína.

Obr. 9. Možná rizika okolí budovy U5

V této podkapitole se nejedná o kompletní vyhodnocení rizik, ale pouze o ukázku.

4.3 Určení objektu zabezpečené oblasti

Pro zabezpečení zabezpečené oblasti tajné jsem pro návrh vybral učebnu 51/107, která se nachází v budově U5 Fakulty aplikované informatiky univerzity Tomáše Bati, jejichž adresa je Nad Stráněmi 4511, 760 01 Zlín. Tato budova se skládá z osmi pater a 2 tělocvičen. Budova obsahuje dva vchody jeden pro zaměstnance, kde se dá dostat jen pomocí přístupové karty a druhý hlavní (veřejný), který se nachází kousek od učebny, která nám bude sloužit pro výuku, při které budou používány i informace utajovaného charakteru.



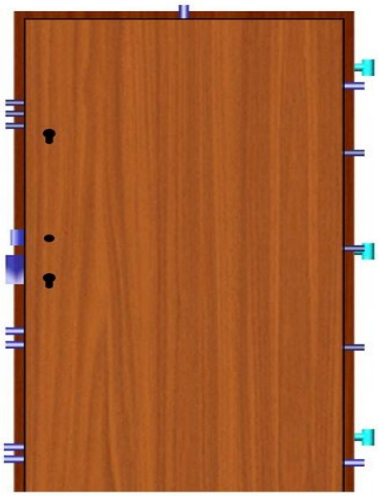
Obr. 10. Technický výkres budovy U5 [23]

Naše učebna kde se bude pracovat s utajovanými informacemi se nachází hned po pravé straně od vchodu do školy vedle vstupu na schodiště do prvního patra budovy. Na obrázku se nachází vstupní dveře do naší místnosti, ale pro naše použití jsou nevhodné, proto musíme instalovat bezpečnostní dveře příslušné třídy.

Obr. 11. Vchodové dveře do 51/107

Pro naši zabezpečenou oblast jsem zvolil dveře od firmy BEDEX Vario EL VD 3 s požární odolností EI 30D1. Tyto bezpečnostní dveře jsou vhodné do stávajících i nových zárubní. Vyrábí se otevíratelné Do i Ven z chráněného prostoru s možností elektronické kontroly vstupu. Tyto dveře se dají otevřít za pomocí čipové karty nebo bezpečnostního kódu, který má oprávněná osoba. Tyto dveře jsou určeny pro stupeň tajné a spadají bezpečnostní třídy 3.

Jejích konstrukce je ocelová s jeklovým rámem a speciálními vnitřními výztuhami. Tyto dveře mají 7 aktivních 3 pasivní uzamykací čepy. Jsou vybaveny vnitřním antikorozním protipožárním nátěrem, mají desetibodový zajišťovací mechanismus. Výroba těchto dveří je na zakázku.



Obr. 12. Dveře BEDEX VARIO [22]

Bezpečnostní třída podle normy ČSN P ENV 1627 a navazujících	2	3	4
Certifikát NBÚ podle z. č. 412/2005 pro	důvěrné	tajné	přísně tajné
Nutnost zárubní	není	není	ano
Požární odolnost	ano	ano	ano
Šířka 80–90	ano	ano	ano
Dvoukřídlé	ne	ano	ano
Atypické rozměry	ne	ano	ano
Otevírané ven	ne	ano	ne
Obložení	hladké	hladké bez kazety	hladké bez kazety

Obr. 13. Bezpečnostní třída pro bezpečnostní dveře [22]

Největším problémem jsou okna do naší učebny, protože se nachází asi 1,5m nad terénem tak jejich zranitelnost je velmi vysoká. Pro zabezpečení těchto oken nám poslouží bezpečnostní rolety, i když tam jsou už nějaké instalovány nevím o jaký typ se jedná.

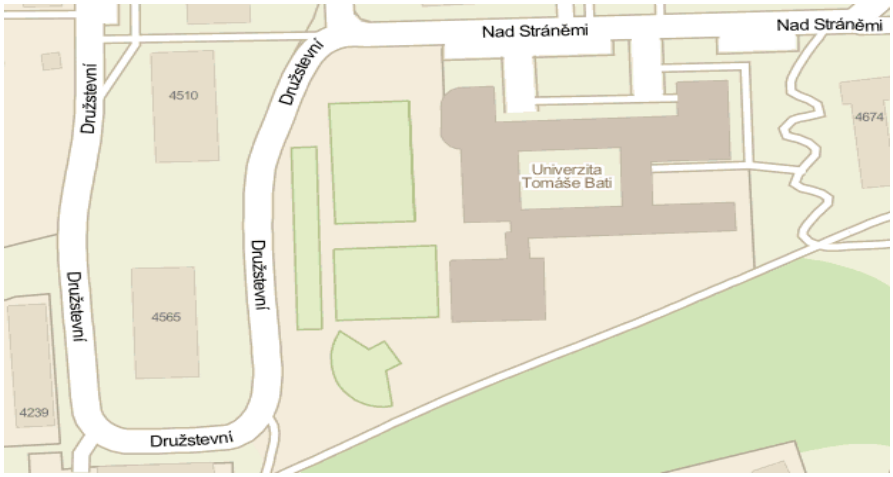
Obr. 14. Okna učebny 51/107

Bezpečnostní rolety pro naši zabezpečenou oblast jsem zvolil rolety GARANT. Tyto rolety jsou speciálně vyvinuté pro požadavky vysoké odolnosti proti vniknutí. Roleta je certifikována v bezpečnostní třídě 3 podle ČSN P ENV 1627 a dle zákona o 412/2005sb. je určena pro stupeň tajné. Lamely rolety jsou vyrobeny z hliníkového protlačovaného profilu CD 40 a dosedací lišta se skládá ze dvou vzájemně prošroubovaných profilů s ocelovou výztuhou. Ovládání této rolety je za pomocí 230V motoru a bezpečnostní vodící lišty jsou rovněž vyztuženy ocelovou deskou.

Obr. 15. Rolety GARANT [25]

Vrátnice nám slouží k úschovně klíčů a hlavně bude jako stanoviště fyzické ostrahy, ve kterém se nachází jeden příslušník, který bude pořád k dispozici na vrátnici a jehož úkolem je sledovat monitorovací systém, vydávat klíče a hlavně bude u ústředny PZS, protože při vyhlášení poplachu musí být fyzická ostraha ihned informována o pokusu nebo vniknutí do místnosti našeho objektu. Druhý příslušník ostrahy bude mít za úkol obchůzky a jeho prioritním úkolem bude kontrolovat legitimaci osob, které do místnosti s utajovanými informacemi mají povolen přístup, zamykání/odemykání této místnosti a po ukončení zasedání její kontrola.

Okolí objektu si můžete všimnout na znázorněné základní mapě a foto mapě části jižních svahů.



Obr. 16. Základní mapa okolí budovy U5

Obr. 17. Foto mapa okolí budovy U5

4.4 Tabulka bodového ohodnocení opatření fyzické bezpečnosti zabezpečené oblasti

Jelikož se bude jednat o školní učebnu pro stupeň utajení tajné, tak míra rizika bude stanovena na **velkou,** protože okolí našeho objektu je kritické a příčinou hustě obydleného sídliště.

Tab. 17. Tabulka bodového ohodnocení zabezpečené oblasti TAJNÉ [10]

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**

- S5** - znamená, že hodnota musí dosáhnout alespoň 4 bodů.

- u kategorie tajné může být pouze jedna z hodnot S1-S3 rovna 0.

Hodnoty proměnných S1-S6 získáme z níže uvedené tabulky a toto je následně nutné porovnat s tabulkou, podle které se snadno vypočítá míra rizika. Na základě tohoto porovnání stanovím, jestli jsou přijatá opatření fyzické bezpečnosti pro danou míru rizika a zabezpečenou oblast **tajná** vyhovující.

Tab. 18. Tabulka bodového ohodnocení opatření fyzické bezpečnosti [10]

BEZPEČNOSTNÍ OPATŘENÍ	TYP	BODOVÉ OHODNOCENÍ
Úschovné objekty	▫ T. 4 – 4 body ▫ T. 3 – 3 body ▫ T. 2 – 2 body ▫ T. 1 – 1 bod	SS1=
Zámky úschovných objektů	▫ T. 4 – 4 body ▫ T. 3 – 3 body ▫ T. 2 – 2 body ▫ T. 1 – 1 bod	SS2=
Úschovný objekt včetně uzamykacího systému,	▫ T. 1A – 1 bod ▫ T. 1B – 2 body ▫ T. 1C – 3 body ▫ T. 1T – 1 bod ▫ T. T – neuvedeno	S1=
Celkové hodnocení úschovného objektu a jeho zámku	S1 = SS1 x SS2	S1=
Zabezpečené oblasti	▫ T. 4 – 4 body ▫ T. 3 – 3 body ▫ T. 2 – 2 body ▫ T. 1 – 1 bod	SS3=
Uzamykací systémy zabezpečené oblasti	▫ T. 4 – 4 body ▫ T. 3 – 3 body ▫ T. 2 – 2 body ▫ T. 1 – 1 bod	SS4=
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	S2 = SS3 x SS4	S2=
Objekt	▫ T. 4 – 5 bodů ▫ T. 3 – 3 body ▫ T. 2 – 2 body ▫ T. 1 – 1 bod	S3=
Kontrola vstupu	▫ T. 4 – 4 body ▫ T. 3 – 3 body ▫ T. 2 – 2 body ▫ T. 1 – 1 bod	SS6=
Režim návštěv v objektu a) Návštěvy s doprovodem b) Návštěvy bez doprovodu c) Návštěvy bez kontroly	▫ ad a) – 3 bod ▫ ad b) – 1 bod ▫ ad c) – 0bodů	SS7=
Celkové hodnocení kontroly vstupu	S4 = SS6 + SS7	S4=
Ostraha	▫ T. 5 – 5bodů ▫ T. 4 – 4 body ▫ T. 3 – 3 body ▫ T. 2 – 2 body ▫ T. 1 – 1 bod	SS8=
Zařízení elektrické zabezpečovací signalizace	▫ T. 4 – 4 body ▫ T. 3 – 3 body ▫ T. 2 – 2 body ▫ T. 1 – 1 bod	SS91=

Instalace zařízení elektrické zabezpečovací signalizace	▫ T. 4 – 4 body ▫ T. 3 – 3 body ▫ T. 2 – 2 body ▫ T. 1 – 1 bod	SS92=
Mezivýsledek (SS 9)		SS9=
Celkové hodnocení ostrahy a systému EZS	S5 = SS8 + SS9	S5=
Fyzické bariéry	▫ T. 7- 12 bodů ▫ T. 6 – 9 bodů ▫ T. 5 – 7 bodů ▫ T. 4 – 4 body ▫ T. 3 – 3 body ▫ T. 2 – 2 body ▫ T. 1 –1 bodů	SS10=
Kontrola vstupu v přístupových bodech fyzické bariéry a) Kontrola je realizována b) Kontrola není realizována	▫ ad a) – 1 bod ▫ ad b) – 0 bodů	SS11=
Namátkové vstupní a výstupní prohlídky a) Prohlídky jsou prováděny b) Prohlídky nejsou prováděny	▫ ad a) – 1 bod ▫ ad b) – 0 bodů	SS12=
Perimetrický detekční systém (PDS)	2 body	SS13=
Bezpečnostní osvětlení perimetru	2 body	SS14=
Speciální televizní systém na perimetru	2 body	SS15=
Celkové hodnocení ochrany perimetru	S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15	S6=

5 NÁVRH PROSTŘEDKŮ PRO ZABEZPEČENÍ UČEBNY 51/107 PRO UTAJOVANÉ INFORMACE TAJNÉ

Návrh prostředků pro učebnu 51/107 bude vycházet z bodového ohodnocení přílohy č.1 vyhlášky 528/2005 Sb.

Dle přílohy zde navrhuji:

- úschovný objekt, zámek pro trezor, určuji typ zabezpečené oblasti, uzamykací systém, hranice objektu, systém kontroly vstupu, režim návštěv v objektu, ostrahu, poplachový zabezpečovací systém, kamerový systém, elektrickou požární signalizaci, požární poplachové zařízení, hlásiče teploty, kouře a tlačítkové, zařízení fyzického ničení nosičů informací.

5.1 Úschovný objekt (trezor)

Tento trezor je nejmenší stěnový trezor, který je vhodný do naší učebny a bude nám sloužit pro uložení utajovaných dokumentů a jiných nosičů.

Obr. 18. Úschovný objekt [15]

Tento trezor je určen pro ochranu utajovaných informací stupně TAJNÉ a je certifikován NBÚ. Přesně splňuje naše požadavky je to nejmenší stěnový trezor pro uložení dokumentů maximálního formátu A4.

Obr. 19. Zámek pro trezor [16]

Tento úschovný objekt je určen pro typ 3 jehož zámek je typu 2.

Vypočítání bodového ohodnocení:

SS1 = 3body ; SS2 = 2body

Dle tabulky bodového ohodnocení můžeme vypočítat naše potřebné S1.

S1 = SS1 x SS2 = 3 x 2 = 6bodů

Zabezpečená oblast :

Dle přílohy č.1 z vyhlášky 528/2005 sb. jsem stanovil zabezpečenou oblast TYP 1.

Jedná se o oblast jejichž stěny, podlahy jsou lehké stavební konstrukce, které obsahují například (sádrokarton,dřevo, plastické tvrzené hmoty, profilový plech, sklo opatřené bezpečnostní fólií). Průlezné otvory musí být zabezpečeny mechanickými zábrannými prostředky, chráněny certifikovanými prostředky PZS. Průlezné otvory, kde nejsou kladeny požadavky na zabezpečení se musí nacházet 5.5m nad terénem, ale jelikož naše průlezné otvory se jsou 2m nad zemí, tak musí být zabezpečeny MZS. Do naší místnosti nelze proniknout ze střechy nebo pomocí okapů, terénních nerovností a ze stromů. Mechanické zábranné prostředky musí být pevné konstrukce a nesmí vykazovat znaky opotřebení.

Bodové ohodnocení tohoto typu je :

SS3 = 1bod

5.2 Uzamykací systém

Uzamykací systém jsem zvolil typ ochrany 2. Tento uzamykací systém je certifikován úřadem a samotný systém a jeho komponenty musí splňovat požadavky bezpečnostní třídy 3 podle ČSN P ENV 1627.

Bodové ohodnocení typu je :

SS4 = 2 body

Výpočet důležité hodnoty S2 vypočítáme za pomocí těchto dvou bodový ohodnocení.

Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému :

S2 = SS3 x SS4 = 1 x 2 = 2 body

Obr. 20. Uzamykací systém FAB [17]

- výrobek certifikován v bezpečnostní třídě 3,

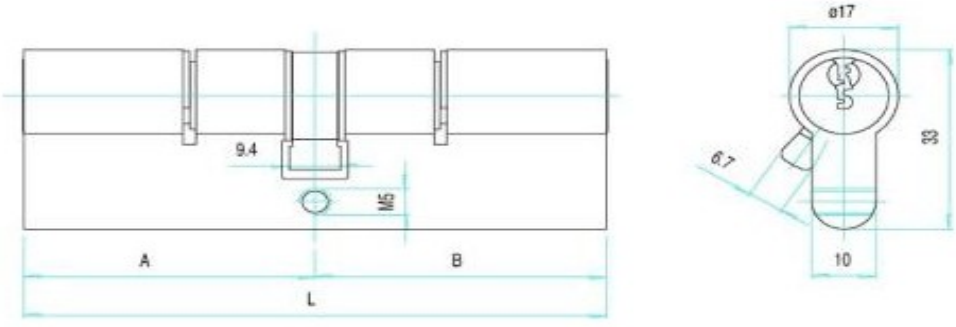
- splňuje požadavky NBÚ typu 2,

- právní ochrana kopírování klíče,

- délka cylindrické vložky od 59mm,

- povrchová úprava saténový nikl

Technický nákres této vložky:



Obr. 21. Technický nákres FAB [17]

5.3 Hranice objektu

Hranici objektu jsem zvolil ochranu typu 2, kdy průlezné otvory musí být zabezpečeny mechanickými zábrannými prostředky nebo PZS minimálně SS92=1. Tato podmínka může platit, pokud se průlezné otvory nachází 2m nad terénem.

Bodové ohodnocení tohoto typu je :

S3 = 2 body

Výpočet první části míry rizika:

Dle tady těchto výsledků bodových ohodnocení můžeme vypočítat, podle tabulky míry zabezpečení fyzické bezpečnosti pro stupeň tajné kdy jsme skutečně docílili našeho stanoveného rizika velká 10ti bodů.

S1 + S2 + S3 = 6 + 2 + 2 = **10 bodů**

5.4 Systém kontroly vstupu

Vstup do zabezpečené oblasti navrhuji realizovat pomocí produktu, který rozšiřuje systém pro ústředny PZS od firmy Galaxy. Tento modul je propojen s ústřednou PZS pomocí sběrnice RS 485. Kontrola vstupu je realizována na vstupu do zabezpečené oblasti. Výstupní poplachový signál tohoto systému musí být vyveden na stálé pracoviště ostrahy.

Obr. 22. Kontrola vstupu [18]

Technické parametry:

- na 2 připojitelné čtečky,

- třída prostředí 2,

- kompatibilita s ústřednou GALAXY;

Tento modul od firmy Honeywell je kompatibilní s naší ústřednou PZS a je certifikován NBÚ SS6 = 2 až 6 bodů což nám vyhovuje. Já jsem si zvolil tento modul do kategorie ochrany typu 2.

Bodové ohodnocení toho typu je SS6 = 2body.

U vstupu do zabezpečené oblasti bude čtečka s připojením na sběrnici RS 485. Tato čtečka je dodávána jako součást příslušenství naší použité PZS ústředny.

Obr. 23. Bezkon.čtečka [18]

Technické parametry:

- kompatibilita s GALAXY,

- připojení pomocí linky RS- 485,

- krytí IP 67;

5.5 Režim návštěv v objektu

Režim návštěv v přízemí je stanoven typem 1 zahrnuje, že návštěvy, které mají přístup do objektu bez doprovodu, musí být viditelně označeny, tudíž v tomto případě musí být viditelně označeni i všichni zaměstnanci objektu. V přízemí objektu bude vedena evidence údajů o návštěvách , která obsahuje osobní identifikaci návštěv a časové údaje návštěv v objektu.

Bodové ohodnocení toho typu je :

SS7 = 1 bod

Díky těmto dvěma hodnotám si můžeme vypočítat potřebné S4.

Celkové hodnocení kontroly vstupu :

S4 = SS6 + SS7 = 2 + 1 = 3 body

5.6 Ostraha

Ostraha je stanovena typem 2, kdy objekt zabezpečují orgány státu , právnické osoby, fyzické osoby, příslušníci ozbrojených sil, ozbrojených sborů nebo zaměstnanci bezpečnostní ochranné služby. U tohoto typu ostrahy nejsou vyžadovány obchůzky.

Bodové ohodnocení toho typu je :

SS8 = 2 body

Zde uvedu typový příklad značení certifikace a posouzení PZS, které jsou uvedeny na stránkách většiny výrobců a prodejců technických prvků.

Typový příklad značení prodejce o certifikaci technického prostředku

Vzal jsem typový příklad ústředny, kde internetový prodejce na obrázku uvádí certifikáty a posouzení k produktům, které prodává. Produkty, které chceme použít k ochraně utajovaných informací musí být samozřejmě certifikovány národním bezpečnostním úřadem, který vydá na základě hodnocení příslušný certifikát pokud to prodejce, kupující osoba nebo montáží firma podcení a bude instalovat necertifikované zařízení nebo dokonce zařízení s propadlým certifikátem, tak samozřejmě pro tyto subjekty hrozí sankce.

ČSN EN 50131-1 stupeň 2

- horní šipka znázorňuje, že tento certifikát vydává zkušebna technických prostředků střežení na základě posouzení dle uvedené normy. Tato ústředna je pro stupeň zabezpečení 2 **nízké - střední riziko,**

- dolní šipka znázorňuje , že tento certifikát vydává národní bezpečnostní úřad. Tento certifikát potvrzuje ověření technické způsobilosti typu 2, které musí splňovat požadavky dle ČSN EN 50131-1 jak je uvedeno nahoře a tísňový systém musí splňovat požadavky dle ČSN EN 50134-1.

Obr. 24. Značení certifikace PZS ústředny [18]

Dle tabulky, která přiřazuje kategorie k typům technických prostředků, z našeho příkladu nám vychází, že ústředna na obrázku je certifikována pro kategorii stupně **důvěrné**.

Tab. 19 . Tabulka přiřazení kategoriím k typům technických prostředků PZS [10]

Tabulka přiřazení kategorií k typům technických prostředků EZS

Typ technického prostředku EZS	Stupeň utajení pro který byla schválena způsobilost je vypsán slovy nebo vypsaná zkratkou		Bodová hodnota
	do 31.12. 1999	od 1.1. 2000	
Typ 4	-	„PT“	4 body
Typ 3	„PŘÍSNĚ TAJNÉ“	„T“	3 body
Typ 2	„DŮVĚRNÉ“	„D“	2 body

5.7 Zařízení PZS

Ústřednu PZS jsem zvolil na základě posouzení uváděných parametrů ve srovnání s požadavky pro zabezpečenou oblast stupeň tajné. Toto zařízení je certifikováno NBÚ, které splňuje požadavky ČSN EN 50131-1 stupeň zabezpečení střední až vysoké riziko. Ústředna obsahuje barevný dotykový displej, který zpřehledňuje a zjednodušuje uživatelské ovládání systému.

Obr. 25. Použitá PZS ústředna [18]

Bodové ohodnocení tohoto typu je :

SS91 = 3 body

Instalace zařízení poplachového zabezpečovacího systému :

Tato instalace bud řešena pro TYP 3, kdy realizace toho systému j v rozsahu zabezpečené oblasti:

- prostorová ochrana,

- plášťová ochrana,

- tísňový systém,

Bodové ohodnocení toho typu je :

SS92 = 3 body

Z těchto bodových hodnot potřebujeme vypočítat SS9. Jedná se o mezivýsledek.

SS9 = (SS91 + SS92)/2 x SS92/OBL OBL..... 3 protože se jedná o stupeň tajné

SS9 = (3 + 3)/2 x 3/3

SS9 = 3 body

Celkové hodnocení ostrahy a systému PZS :

S5 = SS8 + SS9

S5 = 2 + 3 = **5 bodů**

Bodové hodnoty, které jsou povinné musíme dopočítat pro stupeň tajné:

S4 + S5 = 8 bodů

Míra rizika je stanovena velká, pro stupeň tajné je to hodnota 5 nám vyšlo 8, tento výsledek může být větší tabulková hodnota je jen orientační.

5.8 CCTV

Tyto systémy slouží pro snímání, přenos a zobrazování pohybu osob, dopravních prostředků a musí být certifikované úřadem. Předmětem certifikace těchto zařízení jsou kamery a řídící jednotky.

Pro naše zabezpečení použijeme dvě venkovní kamery , které se budou nacházet jedna u venkovních oken a druhá bude na vstupu do objektu. Tyto kamery od společnosti Samsung splňují naše požadavky, protože jsou určeny do neosvětlených venkovních prostor, mají přisvětlení do 30m díky IR LED mají velmi dobré rozlišení a hlavně pro nás důležitý aspekt, že detekují pohyb.

Obr. 26. Venkovní kamera [18]

Technické parametry:

- barevná venkovní kamera,

- rozlišení barva : 600TV řádků a ČB 700TV řádků,

- komunikační rozhraní RS-485 koaxiální řízení;

K programovaní těchto kamer nám slouží klávesnice od společnosti Samsung, která je propojena pomocí koaxiálního kabelu nebo RS 485.

Obr. 27. Samsung klávesnice [18]

Vnitřní kameru jsem zvolil také od společnosti Samsung. Tato kamera se bude nacházet nad vstupem do naší zabezpečené oblasti. Jedná se o kameru s IR LED přísvitem do 20m, je ideální do neosvětlených prostor.

Obr. 28. Vnitřní kamera [18]

Technické parametry :

- rozlišení 600TV řádků,

- IR přísvit 20m,

Tento monitor je určen pro kamerové systémy, který obsahuje 2x průchozí video vstup, 1 VGA vstup a audio vstup.

Obr. 29. LCD monitor [18]

Technické parametry:

- 17" monitor,

- rozlišení 1280x1024,

- spotřeba 42W;

Pro nahráváni jsem zvolil digitální videorekordér s rychlostí obrázků 100obr/s, obsahuje 8x video vstupy, 500gb HDD. Tento rekordér je vhodný pro středně náročné aplikace.

Obr. 30. Videorekordér [18]

Technické parametry :

- formát komprese H.264,

- počet video vstupů 8,

- počet audio výstupů 4,

- ovládání RS-485;

5.9 Zařízení elektrické požární signalizace:

Ústřednu pro elektrickou požární signalizaci jsem vybral NSC Apollo F2, protože se jedná o ústřednu, která má platný certifikát NBÚ a splňuje naše požadavky.

Obr. 31. EPS ústředna [19]

Skříň této ústředny je jednoduchá pro montáž v podobě pantů, sklopného a odnímatelného předního panelu, takže technik nemá problém dostat se k připojovacím svorkám.

Pomocí LCD displeje a funkčních tlačítek lze ovládat dynamicky všechny postupy. Nápisy na čelním panelu jsou vyměnitelné a umožňují vložení jiné jazykové verze. Tato ústředna obsahuje svůj napájecí zdroj i baterii.

- požární poplachové zařízení "siréna" :

Nejmenší doporučení pro stupeň tajné je IP krytí 62. Tato siréna splňuje naše požadavky, i když svým zbarvením není vhodná na bílou zeď.

Obr. 32. Siréna [20]

Technické parametry :

- napájení 9-60V DC,

- krytí IP 65,

- počet tónů 32;

- hlásiče teplot - bodové hlásiče

Zvolil jsem hlásič třídy A1R od firmy Honeywell. Jedná se o konvenční teplotní diferenciální hlásič, nominální teplota 58°C, který je certifikován NBÚ.

Obr. 33. Hlásič teploty [18]

Technické parametry :

- napájení 30 Vss,

- odběr klidový 0,17mA,

- odběr maximální 80mA;

- hlásiče kouře - hlásiče bodové

Tento optický detektor kouře jsem zvolil rovněž od firmy Honeywell. Jedná se o konvenční optický detektor kouře s dorovnáváním citlivosti, který má dvojbarevnou programovatelnou LED signalizující poplach, zaprášení a poruchu detektoru.

Obr. 34. Hlásič kouře [18]

Technické parametry :

- napájecí napětí 30 Vss,

- odběr klidový 0,16 mA,

- odběr maximální 80 mA;

- tlačítkové hlásiče

Vybral jsem tlačítkový hlásič Ex XP95 od firmy Apollo. Je určený pro teploty -20 až 60 stupňů. Tento hlásič bude umístěn u vchodu do zabezpečené místnosti, na vrátnici a uvnitř místnosti.

Obr. 35. Tlačítkový hlásič [18]

5.10 Zařízení fyzického ničení nosičů informací :

Jedná se o profesionální skartovačku, určena pro skartování důvěrných dokumentů, kreditních karet a také CD/DVD disků. Je navržena pro pracovní oblasti s vysokými požadavky na ochranu dat, tudíž splňuje naše požadavky a lze ji použít do zabezpečené oblasti stupeň tajné, protože je certifikována NBÚ.

Obr. 36. Skartovačka [21]

Technické parametry:

- Certifikována NBÚ tajné,

- list formátu A4 rozřeže až na 3000 kousků,

- skartuje v příčném řezu 2x8mm;

Dílčí závěr :

Praktická část řeší návrh technických prostředků zabezpečené oblasti tajné, která by se mohla nacházet na fakultě U5, ale důležitým hodnocením bylo stanovit si míru rizika, tu jsem určil na velkou, jelikož v okolí budovy se nachází hodně zalidněné a problémové sídliště a objekt není moc zabezpečen. Technické prostředky, které jsem použil mají platný certifikát NBÚ a jsou určeny pro zabezpečené oblasti požadovaného stupně, které jsem následně dle vyhlášky bodově vyhodnotil. V této části je proveden návrh co použít a jaké se kladou požadavky na projekt pro oblast stupeň tajné, jaké jsou nedostatky projektu a kterých důležitých faktorů by jsme se měli vyvarovat. Dále jsou zde poznatky na jaké zásady by jsme při výběru dodavatelů neměli zapomínat.

ZÁVĚR

V první řadě je potřeba si uvědomit, že vhodná volba montážní firmy, výběr kvalitních certifikovaných technických zařízení vede k lepší ochraně před vloupáním, pokusu o vloupání. Musíme brát na vědomí, že v našem objektu se nachází utajované informace, jejichž odcizení, či únik je nepřípustné, ale samozřejmě může k tomu dojít. Proto by měl provozovatel objektu brát na vědomí zabezpečení této zabezpečené oblasti. Zabezpečení technickými prostředky je velmi náročné hlavně finančně. Míra zabezpečení technickými prostředky má velkou váhu, ale samozřejmě musíme brát v úvahu loajalitu zaměstnanců, protože kvalita zabezpečení neovlivní pokud zaměstnanci nedodržují určitý kodex společnosti.

Podmínkou nasazení technických prostředků je část certifikace, které je nesmírně důležitá pro prostředky, protože jestli chceme použít do zabezpečené oblasti nebo jednací oblasti tyto prvky musí být náležitě certifikovány NBÚ. Podkapitolou byli také náležitosti certifikace, jak zažádat o certifikát , co má obsahovat a kdo ho může dostat.

Hlavní výsledky práce jsou v provedeném návrhu zabezpečení zabezpečené oblasti. V tomto návrhu bylo řešeno jaké technické prostředky použít, podle čeho je počítat a jaké jsou pro náš stupeň na ně kladeny požadavky.

Kvalitně nasazené zabezpečovací prvky vyžadují od pachatele takové úsilí na jeho psychickou i fyzickou stránku, že se ve většině případů rozhodne pro jiný technicky slabší objekt. Proto je kladen důraz na zabezpečení objektů v takové výši, která je oproti cennosti celkovému majetku zanedbatelná.

Diplomová práce se také zabývá fyzickou bezpečností, jaké jsou kladeny požadavky na ostrahu, protože se nemůžeme spoléhat jen na technické prostředky. Na tyto prostředky musí dohlížet proškolený personál, aby mohl v případě vyhlášení poplachu ihned zakročit a zamezit tak odcizení utajovaných informací, protože spoléhat se jen na technické prostředky nemůžeme. V dnešní době kriminalita značně roste a hlavní příčinou jsou nově používané technologie v oblasti techniky, které slouží ke krádežím. Také nesmíme podceňovat pachatele, protože není problém si v relativně krátkém intervalu sehnat potřebnou techniku pro krádež.

Přínosem této práce je seznámení se s utajovanými informacemi, určuje pravidla jak s nimi zacházet, jaký je kladen důraz na certifikaci a na návrh zabezpečení oblasti.

ZÁVĚR V ANGLIČTINĚ

First of all you need to realize that an appropriate choice of installers, a selection of quality certified technical equipment leads to better protection against burglary, attempted burglary. We take note that our object is classified information, the theft or leakage is unacceptable, but of course can happen. Therefore, the facility should take note of the security to the secured area. Technical security equipment is very difficult especially financially. The rate of technical security means a lot of weight, but of course we take into account employees' loyalty, because the quality does not affect security if employees do not comply with a code of society.

Condition for the deployment of technical resources is part of the certification, which is extremely important for the funds, because if we want to use the secure area or meeting the following elements must be properly certified by the NBÚ. Subchapter were also certification requirements, how to apply for a certificate, you must contain and who it can get.

The main results of the work carried out in the draft security security area. In this proposal, which was solved by technical means used, how to count and what are our degree requirements imposed upon them.

Well-deployed security features require the offender such effort on his mental and physical training that in most cases opt for other technically weaker object. Therefore, the emphasis is on building security in an amount that is compared to the total equivalence property is negligible.

The thesis also deals with physical security, which are requirements for security, because we can´t rely on technical means. These funds must be supervised by trained staff, so when the alarm immediately intervene and prevent theft of classified information, because relying only on the technical means can´t. Today, crime is rising significantly and the main reason is new technology used in the techniques used to steal. Also, offenders must not be underestimated, because it is not a problem in a relatively short interval to obtain the necessary equipment for theft.

The contribution of this work is to get acquainted with classified information establishes the rules for how to handle it, what is the emphasis on certification and security on the proposal.

SEZNAM POUŽITÉ LITERATURY

[1] 412/2005 Sb. Zákon ze dne 21.září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti

[2] 528/2005 Sb. Vyhláška ze dne 14.prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků

[3] *Klubpersonalistu* [online]. 2009 [cit. 2011-05-22]. Certifikáty ISO nbu. Dostupné z WWW: <www.rskppraha.klubpersonalistu.cz>.

[4] *Stringdata* [online]. 2009 [cit. 2011-05-22]. Stringdata, s.r.o. Dostupné z WWW: <http://www.stringdata.cz/>.

[5] *Zabezpečená oblast* [online]. 2010 [cit. 2011-05-22]. Coverit. Dostupné z WWW: <http://www.coverit.sk>.

[6] *Raisa* [online]. 2011 [cit. 2011-05-22]. Úložna klíčů. Dostupné z WWW: <http://www.raisa.cz>.

[7] *Av- prezentace* [online]. 2010 [cit. 2011-05-22]. Jednací oblast. Dostupné z WWW: <www.av-prezentace.cz/>.

[8] *Survivor* [online]. 2011 [cit. 2011-05-22]. Zabezpečení objektu. Dostupné z WWW: <http://www.survivor.cz>.

[9] *F.C.S.* [online]. 2010 [cit. 2011-05-22]. Zpracovaní projektu fyzické bezpečnosti. Dostupné z WWW: <http://www.fsc-ov.cz>.

[10] 528/2005 Sb. Vyhláška ze dne 14.prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků, příloha vyhlášky č.1

[11] *One security s.r.o.* [online]. 2011 [cit. 2011-05-22]. Bezpečnostní agentura. Dostupné z WWW: <http://www.onesecurity.cz>.

[12] *Certifikujeme* [online]. 2010 [cit. 2011-05-22]. Postup při certifikaci. Dostupné z WWW: <http://www.certifikujeme.cz>.

[13] *Anet* [online]. 2010 [cit. 2011-05-22]. Certifikát. Dostupné z WWW: <http://www.anet.eu>.

[14] *Drakas* [online]. 2011 [cit. 2011-05-22]. Projekt fyzické bezpečnosti. Dostupné z WWW: <http://www.drakas.cz>.

[15] *Keymart* [online]. 2011 [cit. 2011-05-22]. Trezory. Dostupné z WWW: <http://trezory-keymart.cz/>.

[16] *Sherlock* [online]. 2011 [cit. 2011-05-22]. Bezpečnostní dveře . Dostupné z WWW: <http://www.sherlock.cz/>.

[17] *Fab* [online]. 2010 [cit. 2011-05-22]. Fab. Dostupné z WWW: <http://www.fab.cz/>.

[18] *Adiglobal* [online]. 2011 [cit. 2011-05-22]. Global distribution. Dostupné z WWW: <http://www.adiglobal.cz>.

[19] *ICS systémy s.r.o.* [online]. 2003 [cit. 2011-05-22]. Ústředna EPS. Dostupné z WWW: <http://www.ics-kv.cz>.

[20] *Euroalarm* [online]. 2007 [cit. 2011-05-22]. Zabezpečovací technika. Dostupné z WWW: <http://www.euroalarm.cz/>.

[21] *Nejceny* [online]. 2011 [cit. 2011-05-22]. Kancelářská skartovačka. Dostupné z WWW: <http://www.nej-ceny.cz>.

[22] *Bezpečnostní dveře* [online]. 2010 [cit. 2011-05-22]. Herakles. Dostupné z WWW: <http://www.he.cz/>.

[23] Výukový materiál z předmětu Projektování integrovaných systémů, Ing. Petr Kováč

[24] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. Vyd. 3. aktualiz. S.l. : Cricetus, 2006. 313 s. ISBN 80-902938-2-4(brož.).

[25] *Bezpečnostní rolety* [online]. 2011 [cit. 2011-05-22]. Invence.net. Dostupné z WWW: <http://www.invence.net>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

MZS Mechanické zábranné systémy

EPS Elektrická požární signalizace

PZS Poplachový zabezpečovací systém

ČSN Česká státní norma

BT Bezpečnostní třída

SEZNAM OBRÁZKŮ

SEZNAM TABULEK