Bezpečnostní projekt v oblasti utajovaných informací

Security project in the area of classified information

Bc. Lukáš Breu

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. Lukáš BREU**
Osobní číslo:	**A09730**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní projekt v oblasti utajovaných informací**

Zásady pro vypracování:

1. **Práci zpracujte jako výukový materiál pro SBS.**
2. **Proveďte analýzu současného právního stavu v oblasti ochrany utajovaných informací v ČR, EU a NATO.**
3. **Popište problematiku provádění bezpečnostního posuzování.**
4. **Proveďte bezpečnostní posouzení konkrétního objektu v utajení V a D.**
5. **Navrhněte projekt fyzické bezpečnosti pro konkrétní objekt v utajení V a D.**
6. **Zpracujte napojení objektu na PCO, včetně sledování nadstandardních požadavků a havarijních stavů a implementace otřesového detektoru a bezdrátového tísňového tlačítka.**
7. **Práci doplňte grafickou a fotografickou dokumentací.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Zákon č. 412/2005 Sb. o ochraně utajovaných informací**
2. **KINDL, Jiří. Projektování bezpečnostních systémů I. díl. Zlín : Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-165-7**
3. **LAUCKÝ Vladimír. Technologie komerční bezpečnosti I. Zlín : Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-7318-194-0**
4. **LAUCKÝ Vladimír. Technologie komerční bezpečnosti II. Zlín : Univerzita Tomáše Bati ve Zlíně, 2007. ISBN 978-80-7318-631-9**
5. **UHLÁŘ, Jan. Technická ochrana objektů I. díl – Mechanické zábranné systémy. Praha : Policejní akademie České republiky, 2000. ISBN 80-7251-046-0**
6. **UHLÁŘ, Jan. Technická ochrana objektů II. díl – Elektrické zabezpečovací systémy. Praha : Policejní akademie České republiky, 2001. ISBN 80-7251-076-2**
7. **UHLÁŘ, Jan. Technická ochrana objektů III. díl – Ostatní zabezpečovací systémy. Praha : Policejní akademie České republiky, 2006. ISBN 80-7251-235-8**
8. **MUSIL, Jan; KONRÁD, Zdeněk; SUCHÁNEK, Jaroslav. Kriminalistika. Praha : C.H.Beck, 2004. ISBN 80-7179-878-9**

Vedoucí diplomové práce: **JUDr. Vladislav Štefka**
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

Záměrem této diplomové práce je vytvořit studijní materiál, který objasňuje legislativní úpravu ochrany utajovaných informací v ČR a základní zásady nakládání s utajovanými informacemi v EU a NATO, vysvětluje problematiku bezpečnostního posuzování a seznamuje s legislativní úpravou a faktickou podobou projektu fyzické bezpečnosti objektu, v němž jsou ukládány a zpracovávány utajované informace.

Klíčová slova: ochrana utajovaných informací, návrh poplachového zabezpečovacího a tísňového systému, bezpečnostní posouzení objektu, projekt fyzické bezpečnosti

ABSTRACT

The aim of this thesis is to provide study materials to introduce the legislation on security of classified information in the Czech Republic and elementary rules for handling classified information in the EU and NATO, it also clarifies processes of security evaluation and introduces the legislation and a real design of a physical security project for the building, where classified information is stored and handled.

Key words: security of classified information, design of intruder and hold-up alarm system, safety evaluation of a building, physical security project.

Poděkování:

Tímto děkuji vedoucímu diplomové práce panu JUDr. Vladislavu Štefkovi za cenné rady a připomínky při vytváření této diplomové práce. Zároveň bych tímto chtěl poděkovat panu Zdeňku Unčovskému za technické rady a konzultace při navrhování koncepce systému zabezpečení a v neposlední řadě své rodině, především manželce, za podporu po celou dobu mého studia.

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 23. 5. 2011

…….
podpis diplomanta

OBSAH

ÚVOD

Stejně jako pro 19. století užíváme pojmenování století páry nebo doba průmyslové revoluce, můžeme současnost pojmenovat dobou informací. Znalost a vlastnictví informací ovlivňují existenci každého podnikatelského subjektu. V rámci konkurenčního boje je důležité informace potřebné pro činnost společnosti nejen získávat, ale hlavně již získané informace chránit před jejich vyzrazením. Zvláštní pozornost pak vyžadují informace utajované. Ochrana utajovaných informací je poměrně specifickou oblastí ochrany informací. V případě zpracovávání utajovaných informací je nutné přijmout řadu opatření a splnit mnoho podmínek, aby byla zajištěna jejich řádná ochrana. Základním právním předpisem pro oblast ochrany utajovaných informací v České republice je zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů. Porušením stanovených povinností a pravidel při ochraně utajovaných informací dochází nejen ke spáchání přestupku nebo jiného správnímu deliktu, ale může dojít i ke spáchání trestného činu. Zákon č. 40/2009 Sb., trestní zákoník, uvádí hned tři trestné činy, jež je možné spáchat v souvislosti s porušením pravidel ochrany utajovaných informací. Jedná se o trestný čin Vyzvědačství podle § 316 trestního zákoníku, Ohrožení utajované informace podle § 317 trestního zákoníku a Ohrožení utajované informace z nedbalosti podle § 318 trestního zákoníku. Při práci s utajovanými informacemi by každý měl dobře znát podmínky a pravidla práce s těmito informacemi. Tato diplomová práce má za úkol seznámit čtenáře s hlavními zásadami, podmínkami a pravidly práce s utajovanými informacemi.

Jednou z nejdůležitějších oblastí ochrany utajovaných informací je oblast fyzické bezpečnosti. Fyzickou bezpečnost lze chápat jako systém opatření, která mají za úkol zabránit vyzrazení utajovaných informací. Oblast fyzické bezpečnosti tedy definuje základní požadavky na vybudování poplachových zabezpečovacích a tísňových systémů k ochraně utajovaných informací. Před vytvářením takových systémů je však nezbytné dobře se seznámit s objektem, ve kterém se bude tento systém vytvářet. Proto bude část práce věnována počáteční fázi návrhu poplachového zabezpečovacího a tísňového systému – bezpečnostnímu posouzení zabezpečovaného objektu. Po zřízení poplachového zabezpečovacího a tísňového systému objektu, který odpovídá požadavkům ochrany utajovaných informací, je nutné vypracovat a předložit ke schválení dokument o provedeném zabezpečení objektu a dalších přijatých opatřeních pro ochranu utajovaných informací – projekt fyzické bezpečnosti. Bez schváleného projektu fyzické bezpečnosti

daného objektu nelze v tomto objektu pracovat s utajovanými informacemi. Problematice vytváření projektu fyzické bezpečnosti bude věnována závěrečná část práce.

Hlavním úkolem této diplomové práce je vytvoření studijního materiálu, který objasní čtenáři základní zásady nakládání s utajovanými informacemi, dále přiblíží čtenáři problematiku bezpečnostního posuzování a seznámí jej s podobou projektu fyzické bezpečnosti objektu, v němž jsou ukládány a zpracovávány utajované informace.

I. TEORETICKÁ ČÁST

1 OCHRANA UTAJOVANÝCH INFORMACÍ

1.1 Ochrana utajovaných informací v EU a NATO

Legislativa pro oblast utajovaných informací EU a NATO je velice rozsáhlá. Není cílem této práce provést detailní analýzu jednotlivých právních norem EU a NATO. V této kapitole je proto uveden pouze přehled platných právních norem EU a NATO upravující problematiku ochrany utajovaných informací. Dále je uvedeno několik základních pravidel a definic týkajících se ochrany utajovaných informací v EU a NATO. Právní předpisy týkající se ochrany utajovaných informací v EU a NATO jsou k dispozici např. na webových stránkách Národního bezpečnostního úřadu ČR.

1.1.1 Právní úprava ochrany utajovaných informací v Evropské unii

Evropská unie je politické a ekonomické spojení 27 evropských států s přibližně 500 miliony obyvatel. Společné právo Evropské unie je základním pilířem integrace, přičemž jde o právní systém, který je nadřazen právním systémům jednotlivých členských zemí. Základními právními předpisy pro oblast ochrany utajovaných informací EU jsou Rozhodnutí rady EU ze dne 19. března 2001, kterým se přijímají bezpečnostní předpisy rady (2001/264/ES) a Rozhodnutí komise EU ze dne 29. listopadu 2001, kterým se mění její jednací řád (2001/844/ES, ESUO, Euratom). Rozhodnutí rady EU 2001/264/ES bylo novelizováno a doplněno:

- Rozhodnutím rady ze dne 10. února 2004, kterým se mění rozhodnutí 2001/264/ES, kterým se přijímají bezpečnostní předpisy Rady (2004/194/ES)
- Rozhodnutím rady ze dne 12. července 2005, kterým se mění rozhodnutí 2001/264/ES, kterým se přijímají bezpečnostní předpisy rady (2005/571/ES)
- Rozhodnutím rady ze dne 20. prosince 2005, kterým se mění rozhodnutí 2001/264/ES, kterým se přijímají bezpečnostní předpisy rady (2005/952/ES)
- Rozhodnutím rady ze dne 18. června 2007, kterým se mění rozhodnutí 2001/264/ES, kterým se přijímají bezpečnostní předpisy rady (2007/438/ES)

Rozhodnutí komise EU 2001/844/ES, ESUO, Euratom bylo novelizováno a doplněno:

- Rozhodnutím komise ze dne 3. února 2005, kterým se mění rozhodnutí 2001/844/ES, ESUO, Euratom (2005/94/ES, Euratom)

- Rozhodnutím komise ze dne 31. ledna 2006, kterým se mění rozhodnutí 2001/844/ES, ESUO, Euratom (2006/70/ES, Euratom)
- Rozhodnutím komise ze dne 2. srpna 2006, kterým se mění rozhodnutí 2001/844/ES, ESUO, Euratom (2006/548/ES, Euratom)

Uvedené předpisy EU vymezují základní zásady a minimální bezpečnostní normy, které musí orgány EU a členské státy odpovídajícím způsobem dodržovat tak, aby byla zajištěna bezpečnost a aby měl každý jistotu, že byly vytvořeny společné normy ochrany. Všechny členské státy EU musejí přijmout národní právní předpisy pro oblast utajovaných informací, které nebudou v rozporu s uvedenými normami EU. Každý členský stát musí vytvořit ústřední správní orgán pro oblast utajovaných informací, přičemž tyto orgány jsou povinny navzájem spolupracovat. Podle uvedených právních norem EU je utajovanou informací EU jakýkoli materiál a informace, jejichž neoprávněné vyzrazení by mohlo na různých stupních ohrozit zájmy EU nebo zájmy jednoho či více členských států nezávisle na tom, zda tyto informace pocházejí z EU nebo z členských států, třetích států nebo mezinárodních organizací. Mezi základní zásady ochrany utajovaných informací patří, aby k utajovaným informacím měly přístup pouze oprávněné osoby, tedy osoby, jež prošly bezpečnostní prověrkou (u stupně utajení CONFIDENTIEL UE a vyšší), a které tyto informace potřebují pro výkon své funkce nebo ke splnění svého úkolu. Utajované informace EU se klasifikují do čtyř stupňů utajení:

- TRÈS SECRET UE/EU TOP SECRET – informace a materiály, jejichž neoprávněné vyzrazení by mohlo výjimečně závažně poškodit základní zájmy Evropské unie nebo jednoho či více členských států,
- SECRET UE – informace a materiály, jejichž neoprávněné vyzrazení by mohlo vážně poškodit základní zájmy Evropské unie nebo jednoho či více členských států,
- CONFIDENTIEL UE – tento stupeň se použije pro informace a materiály, jejichž neoprávněné vyzrazení by mohlo poškodit základní zájmy Evropské unie nebo jednoho či více členských států,
- RESTREINT UE – informace a materiály, jejichž neoprávněné vyzrazení by mohlo být nevýhodné pro zájmy Evropské unie nebo jednoho či více členských států.

1.1.2 Právní úprava ochrany utajovaných informací v rámci Severoatlantické aliance

Severoatlantická aliance byla založena 4. dubna 1949 podpisem tzv. Washingtonské smlouvy. Jedná se o mezinárodní vojenskou organizaci se sídlem v Bruselu, která v současné době sdružuje 28 států Evropy a Severní Ameriky. Předpisy a dokumenty NATO jsou z části označené jako utajované informace. Neutajované předpisy NATO nejsou určeny k volné distribuci. V případě zájmu o seznámení se s neutajovanými předpisy NATO musí zájemce podat žádost Národnímu bezpečnostnímu úřadu ČR, ve které uvede důvod zájmu o daný předpis NATO. Výjimku tvoří některé dokumenty týkající se ochrany utajovaných informací, které jsou uveřejněny na webových stránkách Národního bezpečnostního úřadu ČR. V případě potřeby seznamovat se s utajovanými informacemi NATO musí zájemce splnit celou řadu podmínek a požadavků. Základním právním předpisem pro oblast utajovaných informací NATO je Sdělení generálního tajemníka C-M(2002)49 – Bezpečnost v rámci organizace Severoatlantické smlouvy ze dne 17. června 2002. Tento dokument byl novelizován a doplněn dokumenty C-M(2002)49-COR3, C-M(2002)49-COR6, C-M(2002)49-COR7 a C-M(2002)49-COR8. Součástí dokumentu C-M(2002)49 jsou Směrnice k otázkám personální bezpečnosti – AC/35-D/2000, Směrnice k otázkám fyzické (objektové) bezpečnosti – AC/35-D/2001, Směrnice k otázkám bezpečnosti informací – AC/35-D/2002, Směrnice k otázkám průmyslové bezpečnosti – AC/35-D/2003, Základní směrnice k otázkám INFOSEC[1] – AC/35-D/2004 a Řídící směrnice INFOSEC pro CIS[2] – AC/35-D/2005.

Mezi hlavní zásady ochrany utajovaných informací NATO patří, že členské země NATO a civilní a vojenské orgány NATO musejí zajistit dodržování schválených minimálních standardů uvedených v C-M(2002)49, aby byl zajištěn společný stupeň ochrany utajovaných informací mezi stranami. S utajovanými informacemi NATO je možné se seznamovat pouze v souvislosti s nezbytným plněním pracovních úkolů či úkolů

[1] *INFOSEC - aplikace bezpečnostních opatření určených k ochraně informací, které jsou zpracovávány, ukládány nebo předávány v komunikačních, informačních a jiných elektronických systémech, proti ztrátě důvěrnosti, integrity nebo dostupnosti, bez ohledu na to, zda by k ní mělo dojít náhodně nebo záměrně - úkolem je také zabránit ztrátě integrity nebo dostupnosti systémů samotných*

[2] *CIS – komunikační a informační systémy*

vyplývajících z funkce, přičemž pro seznamování s informacemi stupně utajení NATO CONFIDENTIAL a vyšší musí být provedena bezpečnostní prověrka osoby, která se má seznamovat. Utajované informace přitom musí být zabezpečeny vyváženým souborem bezpečnostních opatření včetně personálních, fyzických (objektových) bezpečnostních opatření a opatření k zajištění bezpečnosti informací a informačních a komunikačních systémů (INFOSEC), která platí pro všechny osoby s přístupem k utajovaným informacím a jejich nosičům a do veškerých prostor, ve kterých jsou takovéto informace uloženy. NATO definuje utajovanou informaci jako informaci nebo materiál, u nichž je stanoveno, že vyžadují ochranu proti neoprávněnému prozrazení a které byly takto označeny stupněm utajení. Utajované informace NATO jsou klasifikovány do čtyř stupňů:

- COSMIC TOP SECRET (CTS) – neoprávněné prozrazení takové informace by způsobilo NATO mimořádně vážnou škodu,
- NATO SECRET (NS) – neoprávněné prozrazení takové informace by způsobilo NATO vážnou škodu,
- NATO CONFIDENTIAL (NC) – neoprávněné prozrazení takové informace by poškodilo zájmy NATO,
- NATO RESTRICTED (NR) – neoprávněné prozrazení takové informace by bylo pro zájmy nebo působnost NATO nevýhodné.

V případě, že se jedná o utajovanou informaci týkající se oblasti zbraní hromadného ničení, přidává se k označení stupně utajení příznak ATOMAL. Dokumenty NATO obsahující neutajované informace jsou označovány příznakem NATO UNCLASSIFIED.

1.2 Ochrana utajovaných informací v ČR

Česká republika je od roku 1998 členem Severoatlantické aliance a od roku 2004 členem Evropské unie. Tak jako ostatní legislativa v právním pořádku České republiky musí být v souladu s právními předpisy NATO a EU i problematika ochrany utajovaných informací. Do roku 1998 byla problematika utajování informací na našem území upravena zejména v zákoně č. 102/1971 Sb., o ochraně státního tajemství. Tato právní norma však již nevyhovovala, proto ji od listopadu 1998 nahradil zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů. Jak uvádí Ivanka [1]: „Česká republika přijetím uvedeného zákona v roce 1998 jednoznačně deklarovala svůj úmysl

zapojit se do struktury organizace Severoatlantické smlouvy. Důležitou podmínkou tohoto zapojení byla právní úprava ochrany utajovaných skutečností, vyjadřující systém kompatibilní se systémy ochrany uplatňovanými v zemích Evropské unie a NATO.“. Jak dále Ivanka [1] uvádí: „Celý nový systém ochrany utajovaných informací je postaven na dvou základních principech:

- utajovat co nejméně, ale co nejkvalitněji,
- s utajovanými informacemi se mohou seznamovat pouze osoby, které je nezbytně nutně potřebují znát k výkonu povolání, funkce, apod.“.

Tyto dva základní principy jsou zakotveny i v současné právní úpravě problematiky ochrany utajovaných informací a tou je zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Zákon č. 412/2005 Sb. navázal na zákon č. 148/1998 Sb., přičemž rozšířil, upravil a zpřesnil podmínky pro přístup k utajovaným informacím a další požadavky na jejich ochranu. Prováděcími právními předpisy k zákonu č. 412/2005 Sb. jsou:

- nařízení vlády č. 522/2005 Sb. kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb.,
- vyhláška č. 523/2005 Sb. o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor,
- vyhláška č. 524/2005 Sb. o zajištění kryptografické ochrany utajovaných informací,
- vyhláška č. 525/2005 Sb. o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací,
- vyhláška č. 526/2005 Sb. o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti), ve znění vyhlášky č. 11/2008 Sb.,
- vyhláška č. 527/2005 Sb. o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti),

- vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.,
- vyhláška č. 529/2005 Sb. o administrativní bezpečnosti a o registrech utajovaných informací ve znění vyhlášky č. 55/2008 Sb.

V souvislosti s legislativními akty v oblasti ochrany utajovaných informací je potřeba ještě zmínit zákon č. 413/2005 Sb., o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, ze dne 21. září 2005, který pojednává, jak je již z názvu patrné, o změnách v některých zákonech v souvislosti s přijetím a nabytím účinnosti zákona č. 412/2005 Sb. Jako příklady zákonů, jichž se změny týkají, je možné uvést např. trestní zákon, trestní řád, občanský soudní řád či zákon o požární ochraně.

1.2.1 Úprava problematiky ochrany utajovaných informací podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ze dne 21. září 2005 nabyl účinnosti dne 1. ledna 2006. V platném znění je zákon ke dni 1. dubna 2011 rozdělen do devíti částí a obsahuje celkem 163 paragrafů. V následujících kapitolách bude proveden rozbor tohoto zákona včetně jeho prováděcích předpisů. Zákon a jeho prováděcí předpisy tvoří přesný a poměrně rozsáhlý komplex pravidel, podmínek a povinností, z nichž se pokusím vybrat to nejdůležitější pro potřeby této práce.

1.2.1.1 Předmět úpravy, základní ustanovení, vymezení pojmů

Zákon spolu s prováděcími právními předpisy upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k takovým informacím, požadavky na ochranu utajovaných informací, zásady pro stanovení a podmínky pro výkon citlivých činností a s tím spojený výkon státní správy. Zákon definuje utajovanou informaci jako takovou informaci, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné. Informace může být utajovanou pouze v případě, že je uvedená v seznamu utajovaných informací. Seznam utajovaných informací je uveden v nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb. Toto nařízení uvádí ve svých osmnácti přílohách seznamy utajovaných informací v oblasti působnosti jednotlivých ministerstev a dalších orgánů státního aparátu, jako jsou například Česká

národní banka, Národní bezpečnostní úřad, Správa státních hmotných rezerv či zpravodajské služby a to včetně uvedení stupně nebo rozsahu stupňů utajení jednotlivých informací. Při posuzování, jestli je informace informací utajovanou, je podle tohoto nařízení rozhodné, jestli případné vyzrazení nebo zneužití takové informace může způsobit újmu zájmům ČR nebo může být pro zájem ČR nevýhodná ve smyslu zákona č. 412/2005 Sb. Neoprávněnou osobu definuje zákon jako fyzickou nebo právnickou osobu, která nesplňuje podmínky přístupu k utajované informaci. Zákon definuje čtyři stupně klasifikace utajení informací:

- Přísně tajné, jestliže vyzrazení nebo zneužití takové informace může způsobit mimořádně vážnou újmu zájmům ČR,
- Tajné, jestliže vyzrazení nebo zneužití takové informace může způsobit vážnou újmu zájmům ČR,
- Důvěrné, jestliže vyzrazení nebo zneužití takové informace může způsobit prostou újmu zájmům ČR,
- Vyhrazené, jestliže vyzrazení nebo zneužití takové informace může být nevýhodné pro zájmy ČR.

Stupeň utajení informace, tedy její klasifikaci, provádí ten, kdo takovou informaci vytvořil, a to při vzniku této utajované informace. Zákon přesně definuje, co je mimořádnou újmou pro zájmy ČR (např. rozsáhlé ztráty na lidských životech a značné ohrožení vnitřního pořádku a bezpečnosti ČR), vážnou újmou pro zájmy ČR (např. značná škoda ČR ve finanční, měnové a hospodářské oblasti), prostou újmou pro zájmy ČR (např. ohrožení bezpečnosti jednotlivce) a nevýhodnost pro zájmy ČR (např. narušení bezpečnostních nebo zpravodajských operací). Mezi zájmy ČR, které by byly vyzrazením utajované informace příslušného stupně utajení ohroženy, patří zachování ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, zajištění mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života a zdraví fyzických osob.

1.2.1.2 Zajišťování ochrany utajovaných informací

Ochrana utajovaných informací je podle zákona zajišťována personální bezpečností, průmyslovou bezpečností, administrativní bezpečností, fyzickou bezpečností, bezpečností informačních a komunikačních systémů a kryptografickou ochranou. Jednotlivé formy ochrany utajovaných informací jsou v následujícím textu detailněji rozebrány.

Personální bezpečnost

Personální bezpečnost je zákonem definována jako výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro přístup takových osob k utajovaným informacím, jejich výchova a ochrana. Personální bezpečnost je zpracována v části druhé, hlava II, § 6 až 14 zákona. Problematiku personální bezpečnosti lze rozdělit do dvou částí, a to na podmínky přístupu k utajovaným informacím stupně utajení Vyhrazené a na podmínky přístupu k utajovaným informacím stupně utajení Přísně tajné, Tajné nebo Důvěrné.

S vyhrazenými utajovanými informacemi se může seznamovat pouze taková fyzická osoba, která nezbytně potřebuje přístup k těmto informacím k výkonu své funkce, je držitelem oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené, případně osvědčení nebo dokladu fyzické osoby a je poučena ve smyslu zákona. Fyzické osobě je Národním bezpečnostním úřadem vydáno oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené za předpokladu, že je tato fyzická osoba bezúhonná, je způsobilá k právním úkonům a musí jí být alespoň osmnáct let. Toto oznámení je platné zpravidla tři roky. Důvodem dřívějšího zániku platnosti tohoto oznámení je např. ztráta nebo odcizení oznámení, úmrtí nebo prohlášení osoby za mrtvou nebo pozbytí způsobilosti k právním úkonům či bezúhonnosti.

Přistupovat k utajovaným informacím stupně utajení Přísně tajné, Tajné nebo Důvěrné může pouze taková fyzická osoba, která nezbytně potřebuje přístup k těmto informacím k výkonu své funkce, je držitelem platného osvědčení fyzické osoby příslušného stupně utajení a je poučena ve smyslu zákona. Fyzická osoba může získat osvědčení pouze za předpokladu, že je státním občanem ČR nebo některého členského státu EU nebo NATO, dále splňuje podmínky bezúhonnosti, je věku alespoň osmnáct let a je způsobilá k právním úkonům. Dále tato fyzická osoba musí být osobnostně způsobilá a bezpečnostně spolehlivá. Všechny tyto podmínky pak musí splňovat po celou dobu platnosti osvědčení.

Bezpečnostní spolehlivost fyzické osoby se prokazuje tak, že u ní nebylo zjištěno bezpečnostní riziko, kterým je např. závažná či opakovaná činnost proti zájmům ČR, zařazení či spolupráce s bývalou StB, užívání jiné identity, pravomocné odsouzení pro trestný čin, porušení povinnosti při ochraně utajovaných informací či zřejmě nepřiměřené finanční nebo majetkové poměry vzhledem k řádně přiznaným příjmům. Platnost osvědčení fyzické osoby je pro stupeň utajení Přísně tajné pět let, pro stupeň utajení Tajné sedm let a pro stupeň utajení Důvěrné devět let. V případě, že fyzická osoba přestane splňovat podmínky pro vydání osvědčení, Národní bezpečnostní úřad okamžitě zruší platnost tohoto osvědčení. Dalšími důvody zániku platnosti osvědčení jsou např. odcizení nebo ztráta osvědčení, poškození a nečitelnost osvědčení či změna údajů v osvědčení.

Prezident republiky, poslanci a senátoři Parlamentu, členové vlády, Veřejný ochránce práv a zástupce Veřejného ochránce práv, soudci a prezident, viceprezident a členové Nejvyššího kontrolního úřadu disponují tzv. zvláštním přístupem k utajované informaci. To znamená, že tyto osoby mají přístup k utajované informaci všech stupňů utajení bez platného osvědčení fyzické osoby a poučení.

Prováděcím předpisem pro oblast personální bezpečnosti je vyhláška č. 527/2005 Sb. o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti).

Průmyslová bezpečnost

Problematika průmyslové bezpečnosti je v zákoně řešena v § 15 až 20. Průmyslovou bezpečnost lze definovat jako systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu se zákonem. Přístup k utajované informaci lze umožnit pouze takovému podnikateli, který nezbytně potřebuje takový přístup k výkonu své činnosti a je držitelem platného osvědčení podnikatele příslušného stupně utajení. Osvědčení může být podnikateli vystaveno pouze v případě, je-li podnikatel ekonomicky stabilní, bezpečnostně spolehlivý, schopný zabezpečit ochranu utajovaných informací, a pokud je odpovědná osoba držitelem platného osvědčení nebo oznámení fyzické osoby

pro požadovaný stupeň utajení. Podnikatel je pak povinen splňovat všechny tyto podmínky po celou dobu platnosti osvědčení podnikatele, v opačném případě toto osvědčení pozbyde platnosti. Osvědčení podnikatele je platné pro stupeň utajení Přísně tajné pět let, Tajné sedm let, Důvěrné devět let a Vyhrazené dvanáct let. Podnikatel nesplňuje podmínku ekonomické stability, jestliže např. mu hrozí nebo byla vyhlášena exekuce na majetek, podnikatel neplní finanční povinnosti vůči státu, fyzickým nebo právnickým osobám nebo podnikateli, neuhradil nedoplatek na dani z příjmů, zdravotním a sociálním pojištění. Bezpečnostní spolehlivost je v zákoně definována tak, že podnikatel nesplňuje podmínku bezpečnostní spolehlivosti, pokud je u něj zjištěno bezpečnostní riziko. Bezpečnostním rizikem ve smyslu zákona je pak např. činnost statutárního nebo kontrolního orgánu podnikatele proti zájmům ČR, uvedení nepravdivé informace nebo zamlčení důležité informaci při bezpečnostním řízení, personální nestabilita ve statutárním či kontrolním orgánu podnikatele, porušení povinností při ochraně utajovaných informací nebo v případě akciové společnosti existence jiné formy akcií, než jsou akcie na jméno.

Prováděcím předpisem pro oblast průmyslové bezpečnosti je vyhláška č. 526/2005 Sb. o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti), ve znění vyhlášky č. 11/2008 Sb.

Administrativní bezpečnost

Administrativní bezpečnost zákon specifikuje v § 21 až 23. Administrativní bezpečností se podle zákona rozumí systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi. Při vzniku utajované informace stanoví její původce stupeň utajení této informace a vyznačí jej na utajovanou informaci. Daný stupeň utajované informace pak platí po celou dobu existence této informace, pokud jej původce nezmění či nezruší. Původce utajované informace je dále povinen vyznačit svůj název, evidenční označení a datum vzniku utajované informace. Původci utajované informace je zákonem stanovena povinnost nejméně jednou za pět let prověřit, zda důvod utajování informace trvá. V případě, že původce utajované informace zruší nebo změní stupeň

utajení této informace, je povinen tuto změnu stupně utajení dané informace dát na vědomí všem příjemcům dané utajované informace.

Prováděcím předpisem je vyhláška č. 529/2005 Sb. o administrativní bezpečnosti a o registrech utajovaných informací ve znění vyhlášky č. 55/2008 Sb. Tato vyhláška stanovuje způsob vyznačení všech náležitostí na utajované informaci, administrativní pomůcky nutné při nakládání s utajovanými informacemi, podrobnosti k přepravě, přebírání, zapůjčování a pořizování kopií utajovaných informací. Dále je ve vyhlášce řešena problematika registrů utajovaných informací, problematika zajištění ochrany utajovaných informací při personálních změnách či zániku organizace a problematika manipulace s technickými zařízeními. Součástí vyhlášky je 12 příloh, ve kterých jsou uvedeny vzory administrativních pomůcek.

Fyzická bezpečnost

Zákon specifikuje podmínky fyzické bezpečnosti v § 24 až 34. Fyzickou bezpečnost zákon definuje jako systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat. V zákoně jsou jasně definována místa, kde lze pracovat s utajovanými informacemi. Nejčastějšími místy v souvislosti s manipulací s utajovanými informacemi jsou objekt, zabezpečená oblast a jednací oblast. Objektem se rozumí budova nebo jiný ohraničený prostor, ve kterém se nachází zabezpečená oblast nebo jednací oblast. Zabezpečená oblast je definována jako ohraničený prostor v objektu. Utajované informace se zpracovávají a ukládají v zabezpečených oblastech. Výjimečně lze utajované informace zpracovávat i mimo zabezpečenou oblast, ale jen v případě, že je zajištěno, že neoprávněná osoba nebude mít přístup k utajovaným informacím. Jednací oblastí zákon rozumí ohraničený prostor v objektu, přičemž utajované informace stupně utajení Přísně tajné a Tajné lze pravidelně projednávat pouze v jednací oblasti. Odpovědná osoba objektu, ve kterém se nacházejí utajované informace, je povinna zajistit, aby nedocházelo při projednávání k ohrožení nebo úniku utajovaných informací, zejména musí požádat o provedení kontroly, zda nejsou v jednací oblasti použity nedovolené technické prostředky k získávání informací. Zabezpečené oblasti se dělí do čtyř kategorií, do kategorií Přísně tajné, Tajné, Důvěrné nebo Vyhrazené, podle nejvyššího stupně projednávaných utajovaných informací v dané zabezpečené oblasti. Zabezpečené oblasti příslušných kategorií se dále dělí do dvou

tříd. Třída I zabezpečené oblasti je charakterizována tak, že vstupem do této zabezpečené oblasti dochází k seznámení s utajovanou informací. Naproti tomu vstupem do zabezpečené oblasti třídy II nedochází k seznámení s utajovanou informací. Neoprávněná osoba může vstoupit pouze do zabezpečené oblasti třídy II a to jen v doprovodu osoby, která má do této oblasti přístup.

Vstup do zabezpečených a jednacích oblastí a výstup z nich musí být kontrolován opatřeními fyzické bezpečnosti, kterými jsou střežení objektu nebo zabezpečené či jednací oblasti ostrahou, stanovení a všeobecné dodržování režimových opatření a použití technických prostředků.

Zákon přesně definuje požadavky na ostrahu pro jednotlivé kategorie zabezpečených oblastí:

- pro kategorie Přísně tajné – ostraha nejméně dvěma osobami u objektu,
- pro kategorie Tajné – ostraha nejméně jednou osobou u objektu a jednou další osobou, která provede v případě narušení rychlý zásah; zabezpečená oblast kategorie Tajné musí být vybavena technickými prostředky – elektrická zámková zařízení a systémy pro kontrolu vstupů, zařízení elektrické zabezpečovací signalizace a zařízení elektrické požární signalizace,
- pro kategorie Důvěrné – ostraha nejméně jednou osobou; zabezpečená oblast kategorie Důvěrné musí být vybavena technickými prostředky – elektrická zámková zařízení a systémy pro kontrolu vstupů a zařízení elektrické zabezpečovací signalizace,
- pro kategorie Vyhrazené – ostraha se zajišťuje pouze v rozsahu stanoveném odpovědnou osobou.

Obdobně je ostraha definována pro jednací oblasti pro projednávání utajovaných informací stupně utajení Přísně tajné a Tajné. Ostraha je dle zákona zajišťována zaměstnanci orgánu státu, právnické osoby nebo podnikající fyzické osoby, o jejichž objekt jde, příslušníky ozbrojených sil nebo ozbrojených sborů nebo příslušníky ozbrojených sil cizí moci anebo zaměstnanci bezpečnostní ochranné služby.

Režimová opatření jsou mimo jiné stanovení oprávnění osob pro vstup (resp. vozidel pro vjezd) do objektu, zabezpečené či jednací oblasti, stanovení způsobu manipulace s klíči a identifikačními prostředky ke vstupu, dále stanovení podmínek a způsobu kontroly osob v objektu, zabezpečené a jednací oblasti apod.

Technické prostředky zákon specifikuje zejména jako mechanické zábranné prostředky, elektrická zámková zařízení a systémy pro kontrolu vstupů, zařízení elektrické zabezpečovací signalizace, speciální televizní systémy, tísňové systémy, zařízení elektrické požární signalizace, zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů, zařízení fyzického ničení nosičů informací a zařízení proti pasivnímu a aktivnímu odposlechu utajované informace. Každý použitý certifikovaný nebo odpovědnou osobou schválený necertifikovaný technický prostředek má přiřazené bodové ohodnocení. Míra zabezpečení jednací a zabezpečené oblasti opatřeními fyzické bezpečnosti se určuje v závislosti na vyhodnocení rizik pomocí bodových hodnot těchto opatření. Opatření fyzické bezpečnosti musí odpovídat nejnižší míře zabezpečení jednací či zabezpečené oblasti a stanoví se v závislosti na stupni utajení utajovaných informací pravidelně v jednací oblasti projednávaných nebo na kategorii zabezpečené oblasti a na vyhodnocení rizik. Přitom se vyžaduje, aby bylo pravidelně ověřováno, zda použitá opatření fyzické bezpečnosti odpovídají projektu fyzické bezpečnosti a právním předpisům v oblasti ochrany utajovaných informací. Hodnocení rizik se musí provádět pravidelně, v případě potřeby je nezbytné míru opatření fyzické bezpečnosti upravit. Problematika vytváření projektu fyzické bezpečnosti bude detailně zpracována v samostatné kapitole.

Pro oblast fyzické bezpečnosti je prováděcím předpisem vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. Vyhláška stanovuje způsob ukládání utajovaných informací, požadavky na provádění ostrahy, podrobnosti režimových opatření, požadavky na jednotlivé technické prostředky, bodové ohodnocení opatření fyzické bezpečnosti a bodovou hodnotu nejnižší míry zabezpečení, pravidla a podmínky ověřování opatření fyzické bezpečnosti a vyhodnocení rizik a obsah provozního řádu a plánu zabezpečení v krizových situacích. Detailní rozbor vyhlášky bude vypracován v samostatné kapitole společně s problematikou projektu fyzické bezpečnosti.

Bezpečnost informačních a komunikačních systémů

Bezpečnost informačních nebo komunikačních systémů tvoří systém opatření, jejichž cílem je zajistit bezpečné nakládání s utajovanými informacemi v těchto systémech. Informačním systémem pro nakládání s utajovanými informacemi zákon rozumí jeden nebo více počítačů, jejich programové vybavení, periferní zařízení, správa tohoto

informačního systému a k tomuto systému vztahující se procesy nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací. Utajované informace v elektronické podobě je možné zpracovávat pouze v informačním a komunikačním systému certifikovaném Národním bezpečnostním úřadem. Komunikačním systémem pro nakládání s utajovanými informacemi zákon rozumí systém zajišťující přenos těchto informací mezi koncovými uživateli a zahrnující koncové komunikační zařízení, přenosové prostředí, kryptografické prostředky, obsluhu a provozní podmínky a postupy. Takový komunikační systém je možné provozovat pouze podle projektu bezpečnosti komunikačního systému schváleného Národním bezpečnostním úřadem.

Prováděcím předpisem je vyhláška č. 523/2005 Sb. o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. Vyhláškou jsou stanoveny požadavky na informační systémy nakládající s utajovanými informacemi a provádění jejich certifikace, požadavky na komunikační systémy nakládající s utajovanými informacemi a schvalování jejich projektů bezpečnosti, požadavky na ochranu utajovaných informací v kopírovacím zařízení, zobrazovacím zařízení a psacím stroji s pamětí, na ochranu utajovaných informací před jejich únikem kompromitujícím elektromagnetickým vyzařováním a požadavky na provádění certifikace stínících komor. Součástí vyhlášky jsou přílohy č. 1 a č. 2, které obsahují vzory certifikátu informačního systému respektive stínící komory, které potvrzují ověření a schválení jejich způsobilosti k nakládání s utajovanými informacemi.

Kryptografická ochrana

Kryptografickou ochranu tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací, aby nedošlo ke kompromitaci kryptografického materiálu. Kompromitace kryptografického materiálu znamená, že došlo k nakládání s kryptografickým materiálem, které by mohlo způsobit nebo způsobilo porušení ochrany utajovaných informací. Kryptografickým materiálem zákon rozumí kryptografický prostředek, klíčový materiál nebo kryptografickou písemnost. Kryptografický prostředek je utajovaný technický prostředek nebo softwarový produkt používaný ke kryptografické

ochraně, který musí být certifikován Národním bezpečnostním úřadem. Klíčový materiál je kryptografický klíč na odpovídajícím nosiči. Kryptografický klíč je utajovaný proměnný parametr nezbytný k jednoznačnému zašifrování, dešifrování nebo autentizaci dat. Kryptografická písemnost je listina nebo nosné médium obsahující utajované informace kryptografické ochrany.

Kryptografickou ochranu může provádět pouze pracovník pověřený k výkonu kryptografické ochrany, který je držitelem platného osvědčení fyzické osoby a současně držitelem osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Pro získání osvědčení o zvláštní odborné způsobilosti musí pověřený pracovník absolvovat školení a následně složit komisionální zkoušku, která ověří jeho teoretické a praktické znalosti z oblasti kryptografické ochrany. Školení a zkoušku organizuje zpravidla Národní bezpečnostní úřad. Osvědčení o zvláštní odborné způsobilosti má platnost pět let. Zákon dále upravuje podmínky pro přepravu a manipulaci s kryptografickým materiálem.

Prováděcím předpisem v oblasti kryptografické ochrany je vyhláška č. 524/2005 Sb. o zajištění kryptografické ochrany utajovaných informací. Vyhláška stanovuje podmínky provádění odborné zkoušky pro získání osvědčení zvláštní odborné způsobilosti, podrobnosti zajišťování kryptografické ochrany, manipulace s kryptografickým materiálem a administrativní náležitosti provádění kryptografické ochrany.

Ochrana před kompromitujícím elektromagnetickým vyzařováním, certifikace

Utajované informace stupně utajení Přísně tajné, Tajné a Důvěrné je nutné chránit před úniky, které by mohlo způsobit kompromitující elektromagnetické vyzařování. Ochrana před takovými úniky je prováděna zabezpečením elektrických a elektronických zařízení, zabezpečených oblastí nebo objektů. Národní bezpečnostní úřad provádí na základě podání žádosti ověřování, zda jsou objekty, zabezpečené oblasti a elektronická a elektrická zařízení způsobilá k provozu z pohledu ochrany utajovaných informací před vyzrazením kompromitujícím elektromagnetickým vyzařováním. Ověřování způsobilosti je prováděno měřením tohoto kompromitujícího vyzařování. Ochrana před takovým vyzařováním může být zabezpečována také certifikovanou stínící komorou.

Certifikace je ve smyslu zákona postup, při kterém Národní bezpečnostní úřad ověřuje způsobilost technických prostředků, informačních systémů, kryptografických prostředků a stínících komor k ochraně utajovaných informací a způsobilost kryptografických

pracovišť určených k výrobě a testování klíčového materiálu nebo distribuci kryptografického materiálu. Na základě ověření způsobilosti uvedených prostředků, systémů a pracovišť vydá Národní bezpečnostní úřad certifikát o způsobilosti. Tento certifikát je veřejnou listinou a v případě použití certifikovaného technického prostředku, informačního systému apod. je tato kopie příslušného certifikátu součástí projektu fyzické bezpečnosti daného objektu. Vydaný certifikát má omezenou platnost. Po skončení platnosti certifikátu, pokud není vydán opětovný certifikát o způsobilosti, nelze již informační systém, kryptografický prostředek, stínící komoru nebo kryptografické pracoviště chápat jako certifikované. Certifikovaný technický prostředek, který je použitý v rámci zabezpečení objektu, zabezpečených či jednacích oblastí, lze nadále používat i po skončení platnosti jeho certifikátu způsobilosti.

Prováděcím předpisem v oblasti certifikace je vyhláška č. 525/2005 Sb. o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, která stanovuje nezbytné náležitosti žádosti o certifikaci, potřebnou dokumentaci, vzory certifikátů, které jsou uvedeny v příloze č. 1 a č. 2 a způsoby a podmínky provádění certifikace.

1.2.1.3 Národní bezpečnostní úřad

Ústředním správním úřadem pro oblast ochrany utajovaných informací a oblast bezpečnostní způsobilosti je Národní bezpečnostní úřad (NBÚ). NBÚ byl zřízen zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, a to k 1. srpnu 1998. NBÚ se řídí zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. NBÚ vykonává státní správu v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti. Mezi hlavní úkony NBÚ podle zákona patří především rozhodování o vydání osvědčení fyzickým osobám a podnikatelům a případném zrušení platnosti těchto osvědčení, rozhoduje o vydání dokladů o bezpečnostní způsobilosti fyzickým osobám a případném zrušení platnosti těchto dokladů. NBÚ je hlavním orgánem státní správy pro plnění úkolů v oblasti ochrany utajovaných informací v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, Organizaci Severoatlantické smlouvy a z mezinárodních smluv, jimiž je Česká republika vázána. NBÚ je jako jediný oprávněn ve stanovených případech povolovat poskytování utajovaných informací v mezinárodním styku, vede ústřední registr utajovaných informací a schvaluje zřízení dalších registrů utajovaných

informací. NBÚ provádí nebo na základě dohod s jinými subjekty státní správy nebo soukromými subjekty zajišťuje certifikace technických prostředků, informačních systémů, kryptografických prostředků a pracovišť a stínících komor, dále zajišťuje a podílí se na výzkumu, vývoji a výrobě národních kryptografických prostředků, vývoji a schvalování národních šifrových algoritmů a vytváření národní politiky kryptografické ochrany. Na základě žádosti provozovatele objektu, ve kterém se vyskytují nebo budou vyskytovat utajované informace, NBÚ zjišťuje měření kompromitujícího elektromagnetického vyzařování. Součástí NBÚ jsou Národní středisko komunikační bezpečnosti, Národní středisko pro distribuci kryptografického materiálu, Národní středisko pro měření kompromitujícího elektromagnetického vyzařování a Národní středisko pro bezpečnost informačních systémů. V čele NBÚ je ředitel, který je přímo odpovědný předsedovi vlády nebo jím pověřenému členovi vlády. Kontrolu nad činností NBÚ vykonává zvláštní kontrolní orgán Poslanecké sněmovny Parlamentu ČR.

1.2.1.4 Povinnosti při ochraně utajovaných informací a správní delikty

Zákon jednoznačně uvádí povinnosti při ochraně utajovaných informací. V osmé části zákona v § 148 až 156 jsou taxativně vyjmenovány přestupky a správní delikty, jichž se mohou dopustit fyzické osoby, podnikající fyzické osoby, právnické osoby a podnikatelé v souvislosti s porušením pravidel a povinností v oblasti ochrany utajovaných informací. Zároveň jsou zde vyjmenovány pokuty za jednotlivé přestupky a správní delikty, které mohou být dle závažnosti protiprávního jednání ve výši od 50 000 Kč až do 5 000 000 Kč. Z přesného a podrobného vyjmenování povinností a protiprávního jednání a z výše pokut je jednoznačně patrné, jak velký má Česká republika zájem na dodržování pravidel ochrany utajovaných informací.

1.2.1.5 Přechodná a závěrečná ustanovení

V § 157 až 161 jsou uvedena přechodná a závěrečná ustanovení tohoto zákona, tedy vztah k ostatním právním předpisům, změny a zrušení vyjmenovaných právních norem a v posledním paragrafu je uvedena účinnost zákona dnem 1. ledna 2006.

1.3 Závěrem k právní úpravě problematiky utajování informací

V této kapitole byl nastíněn základní právní rámec oblasti ochrany utajovaných informací v EU a NATO, přičemž byly vyzdviženy některé základní zásady nezbytné pro plnění ochrany takových informací. Zároveň byl uveden přehled používaných klasifikací stupňů utajení v EU a NATO. Největší část této kapitoly je věnována platné legislativě ČR v oblasti utajovaných informací. V této části byl proveden detailnější rozbor z mého pohledu nejdůležitějších částí zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti ve znění pozdějších předpisů, včetně prováděcích právních předpisů tohoto zákona, vyjma problematiky týkající se projektu fyzické bezpečnosti, která bude zpracována v samostatné kapitole. V současné době se připravuje novelizace tohoto zákona, novelu zákona schválila vláda a současné době bude následovat proces schvalování v Poslanecké sněmovně Parlamentu ČR.

2 PROBLEMATIKA BEZPEČNOSTNÍHO POSUZOVÁNÍ

Poplachové zabezpečovací a tísňové systémy se navrhují a realizují především proto, aby bylo možné co nejvíce zabránit vzniku nebo alespoň snížit následky vzniku situací, při nichž dochází k porušení práv poškozených. V dnešní době jsou protiprávním jednáním v největší míře porušována práva majetková. Statistický přehled kriminality Policejního prezidia ČR za období od 1. ledna 2011 do 31. března 2011 uvádí celkový počet všech spáchaných trestných činů na území ČR 81 544, z čehož je 50 141 spáchaných majetkových trestných se způsobenou škodou ve výši 2 034 509 Kč. Z tohoto velkého počtu majetkových trestných činů jasně převažují krádeže prosté s počtem 29 727, následují je krádeže vloupáním v počtu 15 354. Jak uvádějí Musil, Konrád a Suchánek [2]: „Způsoby páchání krádeží jsou různorodé. Pachatelé nacházejí stále nové možnosti, způsoby a prostředky, kterými se snaží zmocnit cizích věcí, překonávat překážky a zabezpečovací zařízení.“. Rozsah předmětů útoků pachatelů majetkové trestné činnosti je velmi široký. Nejčastějším zájmem pachatelů jsou peníze, předměty běžného užitku, starožitnosti a umělecké předměty. Předměty běžného užitku si pachatel buď ponechává, nebo se je snaží prodat. Prodej uměleckých předmětů a starožitností už není tak jednoduchý, zvláště pak na území ČR. Prodej takových předmětů vyžaduje zpravidla jistý stupeň organizovanosti se zapojením překupníků a osob, pohybujících se v uměleckém prostředí. Odcizené peníze a peníze získané prodejem odcizených věcí pachatel použije pro vlastní potřebu, v dnešní době slouží tyto peníze často k nákupu alkoholu a drog.

Majetkovou trestnou činnost (krádeže) lze rozdělit do několika základních skupin:

- podle charakteru napadeného objektu – krádeže kapesní, krádeže vloupáním, krádeže motorových vozidel, krádeže prosté, krádeže v bytech, obchodech a kancelářích,
- podle vztahu pachatele k objektu – krádeže spáchané vnitřními pachateli (např. zaměstnanci), vnějšími pachateli a vnitřními a vnějšími pachateli ve spolupachatelství,
- podle stupně kvalifikovanosti – jednoduché a složité provedení,
- podle použití nástrojů – krádeže bez použití nástrojů, krádeže s použitím nástrojů,
- podle stupně příprav na krádeže – krádeže páchané po přípravě, krádeže bez přípravy.

Každý, kdo navrhuje a buduje zabezpečovací systémy, by měl mít alespoň základní povědomí o kriminalistice a kriminologii. Rozdílné požadavky budou na zabezpečení galerie a např. prodejny zemědělské techniky. Znalost těchto věd zásadně napomáhá při bezpečnostním posuzování a analýze rizik, která mohou zabezpečovanému objektu hrozit.

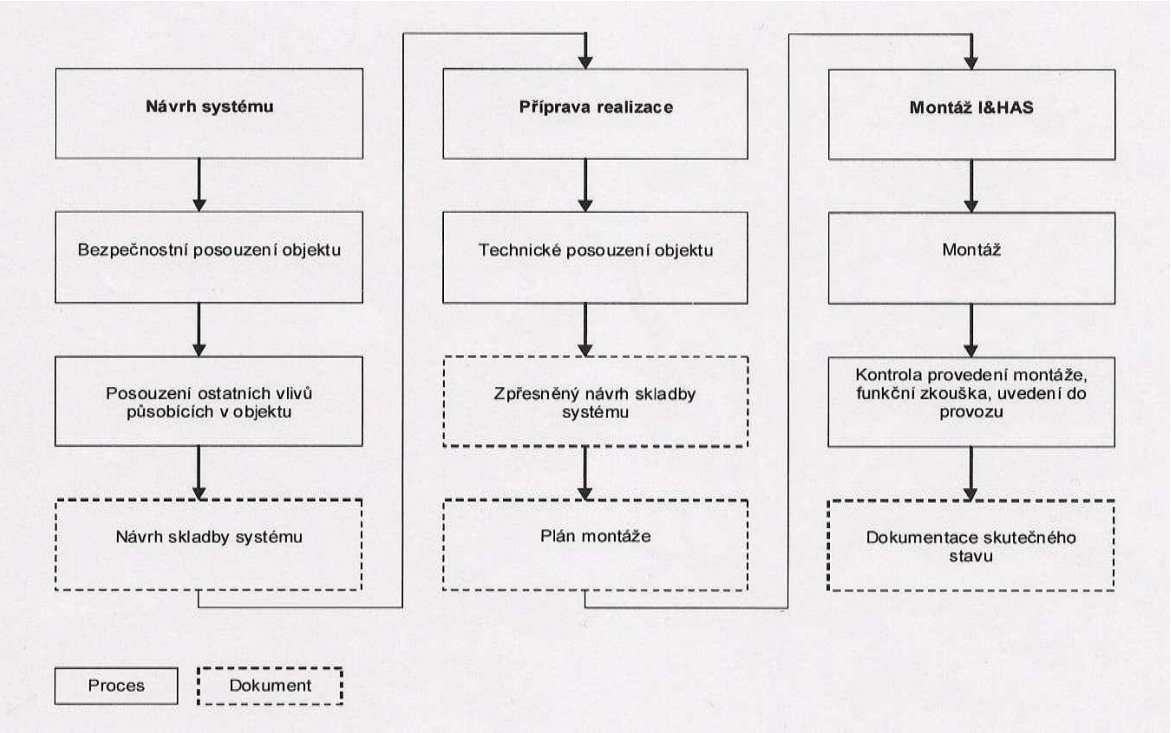
2.1 Návrh poplachových zabezpečovacích a tísňových systémů

Jednou z činností v oblasti bezpečnostního poradenství prováděného soukromými bezpečnostními službami je zřizování poplachových zabezpečovacích a tísňových systémů. Pro funkčně správné a kvalitně provedené zabezpečení objektu je nutné mít řadu zkušeností a širší rozhled nejen v oblasti bezpečnostních technologií. Proces zřizování poplachového zabezpečovacího a tísňového systému je možné rozdělit do několika základních fází:

- vypracování návrhu zabezpečení včetně zpracování cenové nabídky,
- zpracování projektu,
- instalace, oživení a kontrola funkčnosti systému,
- revize a pravidelné prohlídky,
- záruční servis a pozáruční péče o zákazníka.

Cílem návrhu poplachového zabezpečovacího a tísňového systému je především stanovení rozsahu systému a volba vhodných komponentů takového systému. Před začátkem vypracovávání návrhu poplachového zabezpečovacího a tísňového systému je nutné důkladně se seznámit s požadavky zákazníka, se zabezpečovaným objektem, se všemi vlivy, které mohou na zabezpečovaný objekt působit, s hodnotou a strukturou zabezpečovaného majetku, s přístupovými cestami apod. Jak uvádí Křeček [3]: „Důležité jsou zde jak formální, tak konkrétní informace a jejich strukturovaný záznam, který může později v rámci nabídkového řízení sloužit pro zpracování koncepce zabezpečení objektu (systémový návrh), aby bylo možno zpracovat nabídkovou cenu. Strategický význam zde má schopnost identifikace existujících nebezpečí, znalost událostí, jež se v této souvislosti již staly, a slabá místa objektu.“. První etapou návrhu takového systému je bezpečnostní posouzení objektu. Na základě poznatků zjištěných při provádění bezpečnostního posouzení konkrétního objektu se stanovuje potřebný stupeň zabezpečení a třídy prostředí jednotlivých komponent celého systému, případně pojistná třída. Výstupem fáze návrhu poplachového zabezpečovacího a tísňového systému je zpracování návrhu řešení systému (systémový návrh), např. počty, typy a umístění detektorů. Pojem bezpečnostní posouzení je definován v normě ČSN CLC/TS 50131-7. Podle této normy je účelem bezpečnostního posouzení odhalení faktorů, které mají vliv na volbu a umístění komponentů, v průběhu přípravy návrhu zabezpečovacího systému. Na základě detailní obhlídky objektu a lokality, ve které se objekt nachází, se stanovuje stupeň nebezpečí vzhledem k bezpečnostním

rizikům v dané lokalitě. Další ovlivňující faktory systémového návrhu mohou být odhaleny v průběhu technického posouzení objektu. Návrh poplachového zabezpečovacího a tísňového systému musí odpovídat míře rizika hrozícímu danému objektu. Na obrázku č. 1 je znázorněno schéma postupu zřizování poplachových zabezpečovacích a tísňových systémů podle normy ČSN CLC/TS 50131-7.



Obr. 1 Zřizování poplachových zabezpečovacích a tísňových systémů

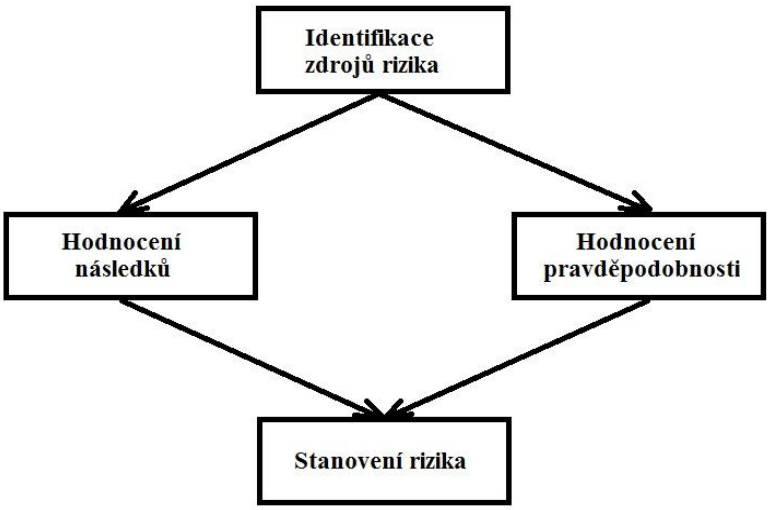
2.2 Analýza rizik

Analýza rizik, která hrozí nebo mohou hrozit zabezpečovanému objektu, je jednou ze základních činností procesu bezpečnostního posuzování. Analýzu rizik je možné definovat jako činnost, při které jsou stanovena zranitelná místa posuzovaného objektu a definovány hrozby působící na posuzovaný objekt a jeho aktiva, dále pravděpodobnost realizace těchto hrozeb a odhad jejich následků. Analýza rizik obsahuje:

- identifikaci aktiv – identifikace posuzovaného objektu a popis aktiv,
- stanovení hodnoty aktiv – určení významu a hodnoty aktiv, ohodnocení dopadu jejich případné ztráty či poškození na další činnost majitele těchto aktiv,

- identifikaci hrozeb a slabin – stanovení jevů a procesů, které mohou negativně ovlivnit hodnotu aktiv, určení slabých míst objektu, která mohou umožnit působení hrozeb,
- stanovení závažnosti hrozeb a míry zranitelnosti – určení pravděpodobnosti výskytu hrozby a míry zranitelnosti objektu vůči dané hrozbě.

Na obrázku č. 2 jsou znázorněny základní kroky prováděné při analýze rizik.



Obr. 2 Základní kroky analýzy rizik

Prostřednictvím analýzy rizik je možné určit míru rizika, které by případně mohlo hrozit posuzovanému objektu a následně stanovit stupeň zabezpečení tohoto objektu. Jak dále Křeček [3] uvádí: „Na základě předcházející analýzy je nutno ohodnotit všechna možná nebezpečí a zvážit celkové riziko dané kombinací faktorů vztahujících se ke střeženému majetku (potenciální nebezpečí) a faktorů vztahujících se k fyzické podstatě objektu (slabá místa). Úkolem hodnocení možných rizik je stanovit úroveň rizika, není-li možné nebezpečí v objektu zcela eliminovat a sejde-li se faktor potencionálního nebezpečí s faktorem slabých míst.“.

2.3 Stanovení potřebného stupně zabezpečení

Provedením analýzy rizik, tedy zjištěním potenciálních nebezpečí a slabých míst, dostáváme první podklady pro budoucí tvorbu návrhu poplachového zabezpečovacího

a tísňového systému. Při vytváření poplachových zabezpečovacích a tísňových systémů je nezbytné dodržovat normu ČSN EN 50131-1, která mimo jiné definuje čtyři stupně zabezpečení, čímž je zajištěna určitá jednotnost, univerzalita a flexibilnost při vytváření těchto systémů a zároveň odpovídající funkčnost a úroveň zabezpečení takových systémů. Nejnižší stupeň zabezpečení je stupeň 1, který odpovídá nízkému riziku a nejvyšší stupeň zabezpečení je stupeň 4, který odpovídá vysokému riziku. Stupeň zabezpečení celého poplachového zabezpečovacího a tísňového systému pak odpovídá prvku s nejnižším stupněm zabezpečení, který je v takovém systému obsažen. Stupně zabezpečení podle ČSN EN 50131-1 jsou:

- Stupeň 1 - Nízké riziko: předpokládá se, že vetřelec nebo lupič mají malou znalost I&HAS[3] a mají k dispozici omezený sortiment snadno dostupných nástrojů,
- Stupeň 2 - Nízké až střední riziko: předpokládá se, že vetřelec nebo lupič mají omezené znalosti I&HAS a používání běžného nářadí a přenosných přístrojů (např. multimetr),
- Stupeň 3 - Střední až vysoké riziko: předpokládá se, že vetřelec nebo lupič je obeznámen s I&HAS a mají rozsáhlý sortiment nástrojů a přenosných elektronických zařízení,
- Stupeň 4 - Vysoké riziko: předpokládá se, že vetřelec nebo lupič jsou schopni nebo mají možnost zpracovat podrobný plán vniknutí a mají kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících komponentů I&HAS. (Používá se, má-li zabezpečení prioritu před všemi ostatními hledisky.)

Výrobci komponentů poplachových zabezpečovacích a tísňových systémů označují své výrobky stupněm zabezpečení v souladu s touto normou. Důkazem o splnění požadavků této normy je pak posouzení zpravidla nezávislou akreditovanou zkušebnou a vydáním příslušného osvědčení. Projektant poplachových zabezpečovacích a tísňových systémů a zákazník pak mají jistotu, že komponenty systému mající příslušné osvědčení splňují podmínky pro zařazení do daného stupně zabezpečení.

---

[3] *I&HAS – Intruder and Hodl-up Alarm System = poplachový zabezpečovací a tísňový systém*

2.4 Stanovení míry rizika

Neexistuje jednoznačný předpis, který by stanovoval metodiku určování míry rizika, které hrozí jednotlivým objektům. Při návrhu vhodného stupně zabezpečení prvků poplachového zabezpečovacího a tísňového systému je nutné zvažovat mnoho aspektů, jako jsou např. lokalita, vlivy působící na objekt, chráněný majetek. Míru rizika, které hrozí zabezpečovanému objektu lze stanovit např. podle následujícího klíče:

- bytům, rodinným domům a jiným obytným objektům, nepojištěným na vysoké částky, se obvykle přiřazuje nízké a nízké až střední riziko, provádí se tedy zabezpečení komponenty stupně 1 až 2,
- kancelářím, dílnám, skladům, obchodům a restauracím, které nedisponují drahým vybavením a majetkem hrozí nejčastěji nízké až střední riziko, zabezpečení takových objektů se provádí komponenty stupně 2,
- objektům s cennými předměty, velkou hotovostí, šperky, omamnými látkami a zbraněmi lze přiřadit obvykle střední až vysoké riziko, zabezpečení se provádí komponenty stupně 3,
- vysoké riziko hrozí mincovnám, tiskárnám cenin, místům zpracování diamantů a zlata a jiným strategicky důležitým místům, jejichž zabezpečení se pak provádí komponenty stupně 4,
- pro pojištěné objekty je vhodné stanovit míru rizika v souladu s požadavky pojišťoven.

Stanovení míry rizika zabezpečovaného objektu se provádí jak na základě požadavků zákazníka a podmínek výkonu jeho činnosti, tak na základě poznatků zjištěných při bezpečnostním posouzení objektu. V praxi se zabezpečovaným objektů nejčastěji přiřazuje stupeň zabezpečení 2, tedy objektu hrozí s největší pravděpodobností nízké až střední riziko. Přiřazení stupně zabezpečení 4, tedy stanovení vysokého rizika hrozícího zabezpečenému objektu, se využívá v běžné praxi jen výjimečně.

2.5 Klasifikace prostředí

Na základě provedeného bezpečnostního posouzení objektu se určuje třída prostředí každého prvku systému podle prostředí, ve kterém se daný prvek systému bude nacházet. Při navrhování jednotlivých komponentů systému se tyto komponenty vybírají podle dané třídy prostředí. Jednotnost stanovení klasifikace prostředí, ve kterém jsou komponenty

poplachového zabezpečovacího a tísňového systému schopny plně fungovat, a označení dané klasifikace zajišťuje podobně jako u stanovení stupňů zabezpečení norma ČSN EN 50131-1. Tato norma definuje čtyři třídy prostředí:

- I. Vnitřní prostředí – obvykle se jedná vnitřní prostory o stálé teplotě, např. obytné nebo kancelářské objekty,
- II. Vnitřní všeobecné prostředí – obvykle jde o vnitřní prostory, ve kterých ale nemusí být stálá teplota, např. chodby, haly, schodiště, skladové prostory s nestálým vytápěním,
- III. Venkovní chráněné prostředí nebo prostředí s extrémními vnitřními podmínkami – obvykle jde o vnější prostředí budov, přičemž komponenty systému nejsou plně vystaveny povětrnostním vlivům,
- IV. Venkovní všeobecné prostředí – obvykle se jedná o vnější prostředí budov s plným vystavením prvků systému vnějším vlivům.

2.6 Bezpečnostní posouzení – identifikace možného nebezpečí a posouzení vlivů na poplachový zabezpečovací tísňový systém

Jak už bylo v předchozích podkapitolách uvedeno, před fází zpracování návrhu poplachového zabezpečovacího a tísňového systému je třeba provést vlastní bezpečnostní posouzení požadovaného objektu. Při provádění bezpečnostního posouzení je nezbytné zaměřit se především na následující aspekty:

- zabezpečené hodnoty – je třeba zhodnotit, jaká rizika hrozí zabezpečovanému majetku,
- stavební dispozice – posouzení stavební konstrukce, druhu a umístění budovy,
- minimální úroveň střežení pro poplachový zabezpečovací systém – odhad očekávaných způsobů narušení v jednotlivých místech objektu, na základě těchto odhadů stanovení stupně zabezpečení a skladby systému,
- minimální úroveň střežení pro tísňový zabezpečovací systém – takový systém užít pouze v případě nutnosti vyplývající z analýzy rizik,
- ostatní vlivy – posuzování stávajících a případných budoucích podmínek ve střeženém prostoru, posouzení vnitřních a vnějších vlivů.

Míra rizika narušení střeženého objektu a majetku závisí na mnoha faktorech a skutečnostech, které je třeba právě při bezpečnostním posouzení zjistit a následně tyto zjištěné faktory a skutečnosti zapracovat do návrhu poplachového zabezpečovacího

a tísňového systému tak, aby byla míra rizika narušení tohoto objektu a majetku minimalizována, případně zcela eliminována. Výčet faktorů a vlivů, které mohou ovlivnit tvorbu poplachového zabezpečovacího a tísňového systému jsou uvedeny v normě ČSN CLC/TS 50131-7 a jejích přílohách B až E. Uvedený přehled je však pouze informativní, při bezpečnostním posouzení je třeba zaměřit se na všechny vlivy a faktory vyskytující se v daném konkrétním posuzovaném objektu. Zjištěním a vzetím těchto ovlivňujících faktorů a vlivů v potaz a následným přizpůsobením navrhovaného poplachového zabezpečovacího a tísňového systému těmto vlivům a faktorům je zaručena odpovídající funkčnost systému. Už proto je nutná určitá zkušenost a širší rozhled při provádění bezpečnostního posuzování a následném navrhování poplachového zabezpečovacího a tísňového systému.

2.6.1 Faktory ovlivňující návrh poplachového zabezpečovacího a tísňového systému v souvislosti se zabezpečovaným majetkem

Mezi nejdůležitější faktory, které ovlivňují návrh poplachových zabezpečovacích a tísňových systémů, patří střežený majetek. Jedná se především o movitý majetek, u kterého hrozí odcizení. Dále je třeba přihlédnout i k faktu poškozování majetku. Stanovení míry rizika vloupání do zabezpečovaného objektu za účelem odcizení majetku a míry rizika poškození majetku závisí na charakteru střeženého majetku. Při bezpečnostním posuzování je tedy třeba zaměřit se na následující faktory, které mohou zásadním způsobem ovlivnit návrh poplachového zabezpečovacího a tísňového systému:

- druh majetku – snadnost zpeněžení, atraktivita pro pachatele, nebezpečí vloupání,
- hodnota majetku – maximální hodnota ztráty, následné výdaje související se ztrátou, osobní vztah k věcem,
- množství nebo velikost majetku – snadnost resp. náročnost odcizení a přepravy majetku, možnosti dalšího užívání nebo zpeněžení odcizeného majetku, snadnost přístupu do střežených prostor,
- historie krádeží v posuzovaném objektu – způsoby vloupání při předcházejících krádežích,
- nebezpečí způsobitelné majetkem – pro osoby a okolní prostředí, zneužití střeženého majetku,
- poškození majetku – riziko žhářství a vandalismu na střeženém majetku, následné psychologické problémy osob (obětí) po loupeži.

2.6.2 Faktory ovlivňující návrh poplachového zabezpečovacího a tísňového systému v souvislosti se zabezpečovanou budovou

Při bezpečnostním posuzování je značná pozornost věnována také obhlídce objektu s cílem identifikovat slabá místa objektu. Fyzická struktura posuzovaného objektu má významný vliv při vytváření návrhu poplachového zabezpečovacího a tísňového systému. Při posuzování fyzické struktury objektů s cílem identifikace slabých míst v rámci stavební dispozice objektu je třeba se zaměřit na následující:

- konstrukce objektu – stěny, střechy, podlahy a sklepení,
- otvory na obvodu objektu – konstrukce oken, dveří, střešních světlíků, ventilace a ostatních otvíraných částí pláště budovy, které by mohly usnadnit nepovolený vstup,
- režim provozu objektu – každodenní provoz či dlouhodobá neosídlenost objektů, přítomnost pracovníků ostrahy, přístup veřejnosti do střežených objektů, režim pro návštěvy,
- držitelé klíčů – přístup a dosažitelnost držitelů klíčů, evidence a uložení klíčů,
- posouzení lokality – kriminalita v oblasti, sousední budovy nebo stavby, které mohou usnadnit vloupání, rychlost reakce na signalizaci poplachu, blízkost nebo jiný vztah k sousedním objektům,
- stávající zabezpečení - kvalita a rozsah stávajících mechanických zabezpečovacích zařízení a poplachového zabezpečovacího a tísňového systému,
- historie krádeží, loupeží a výhružek – počet předcházejících incidentů ve střeženém objektu a způsoby jejich realizace,
- místní legislativa nebo předpisy – bezpečnostní požadavky, požární předpisy a požadavky na konstrukce budov, které mohou ovlivnit návrh poplachového zabezpečovacího a tísňového systému,
- prostředí střeženého objektu – městská zástavba, venkov, průmyslová oblast, typ osídlení, reliéf krajiny, nadmořská výška.

2.6.3 Vlivy působící na poplachový zabezpečovací a tísňový systém mající původ ve střežených objektech

Uvnitř střežených objektů může existovat celá řada faktorů ovlivňující výběr, umístění a nastavení komponentů systému (zejména detektorů). Mnoho z těchto ovlivňujících faktorů může uživatel objektu ovlivnit, např. provedením rekonstrukce, stavebních úprav apod. Následující přehled uvádí vlivy a podmínky vznikající uvnitř zabezpečovaných

objektů, které je nutné při bezpečnostním posuzování brát v úvahu, neboť mohou systém negativně ovlivnit:

- vodovodní potrubí – možný vliv pohybu vody v plastových potrubích při nasazení mikrovlnných detektorů,
- vytápění, vzduchotechnika, klimatizace – vliv turbulence vzduchu na detektory,
- vývěsní štíty, zavěšené předměty – vliv zavěšených předmětů s možností pohybu v zorném poli detektorů (např. záclony, rostliny),
- výtahy - vliv vibrací strojních zařízení (např. otřesová čidla),
- zdroje světla – kompaktní výbojky, zářivky mohou způsobit rušení mikrovlnných detektorů, světlomety vozidel a bodové reflektory nasměrované na čočky nebo zrcadla mohou ovlivnit činnost PIR detektorů,
- elektromagnetické rušení – zvážení vlivu okolních elektrických zařízení jako potencionálních zdrojů elektromagnetických rušení (např. svařovací soupravy, výbojkové komponenty, elektrické generátory a motory, domácí spotřebiče s elektromotory),
- vnější zvuky – vliv v případě nasazení ultrazvukových detektorů (kompresory, vzduchotechnika),
- domácí zvířata – vliv na detektory pohybu,
- průvan – vliv proudění vzduchu na ultrazvukové a PIR detektory (změny teploty, pohyb závěsů či záclon),
- uspořádání skladovaných předmětů – vliv z hlediska zastínění zorného pole detektoru nebo možnosti uvolnění předmětů a jejich následný pohyb v zorném poli detektoru,
- stavební konstrukce střežených objektů – zaměření se na konstrukci střech, stěn, podlah a sklepů, stav a usazení dveří a oken, ovlivnění detektorů vibracemi při montáži na lehké stavební materiály,
- zvláštní pozornost – vlivy působící na detektory na monitorování zasklení a stavebních konstrukcí,
- riziko planých poplachů u tísňových zařízení – volba umístění tísňových zařízení tak, aby nedocházelo k planým poplachům z hlediska pohybu osob.

2.6.4 Vlivy působící na poplachový zabezpečovací a tísňový systém mající původ vně střežených objektů

Vnější vlivy, které působí na zabezpečovaný objekt, nemá uživatel objektu obecně možnost ovlivnit. Jedná se o vlivy, které mohou negativně působit na sytém, a to i z relativně velkých vzdáleností. Tyto vlivy, mnohdy zdánlivě nesouvisející se zřizováním poplachových zabezpečovacích a tísňových systémů, je tedy také nezbytné brát v potaz při volbě a umístění jednotlivých komponentů těchto systémů. Pro jistotu správné funkce jednotlivých komponentů systému a systému jako celku, s ohledem na zjištěné vnější vlivy, je potřeba provést důkladný výběr jednotlivých komponentů systému a jejich následné umístění tak, aby byla zcela jistě vyloučena možnost působení vnějších vlivů. Jako příklady takových vnějších vlivů lze uvést:

- dlouhodobě působící faktory – např. silnice, železnice, metro, parkoviště, letecký koridor – není předpoklad změny za dlouhý časový úsek (roky),
- krátkodobě působící faktory – zejména vlivy výstavby v těsném sousedství,
- vlivy počasí – převažující a potencionální vlivy počasí,
- vysokofrekvenční rušení – zejména u bezdrátových komponent systému – např. vlivy televizních a rádiových vysílačů, radarů, základnových stanic systému mobilních telefonů,
- sousední objekty – vliv činnosti v sousedních objektech (vibrace, elektromagnetické rušení v průmyslových objektech),
- vlivy klimatických podmínek – výběr zařízení odpovídající místním klimatickým podmínkám (např. teplota, vlhkost),
- ostatní vnější vlivy – např. aktivity v přístupných vnějších částech objektu, v přilehlých částech rozsáhlejších komplexů budov, kulturní a sportovní akce v okolí.

2.7 Rozsah zabezpečení

Na základě poznatků zjištěných při bezpečnostním posouzení, zejména na základě provedené analýzy rizik, tedy zjištění slabých míst a potenciálních nebezpečí, se určuje minimální rozsah zabezpečení daného objektu. Pro každý stupeň zabezpečení jsou určená minimální místa posuzovaného objektu, u kterých je nezbytně nutné provést zabezpečení. V příloze F normy ČSN CLC/TS 50131-7 je uveden informativní minimální rozsah střežení.

Následující tabulka zobrazuje minimální rozsah střežení podle normy ČSN CLC/TS 50131-7.

Stupeň zabezpečení / **Místo střežení**	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Obvodové dveře	O	O	O+P	O+P
Okna		O	O+P	O+P
Ostatní otvory		O	O+P	O+P
Stěny				P
Stropy nebo střechy				P
Podlahy				P
Místnosti	T	T	T	T
Předmět (vysoké riziko)			S	S
O = střežení na otevření, P = střežení na průnik nebo proražení, S = specifický požadavek střežení, T = střežení na zachycení narušitele a pokrytí prostoru				

Tab. 1 Minimální rozsah zabezpečení

Tabulka minimálního rozsahu zabezpečení může sloužit jako základní, avšak nikoliv konečná pomůcka pro bezpečnostní posouzení při stanovení, které druhy narušení je pravděpodobné očekávat na jednotlivých místech střežených objektů. Navrhovaný systém pak musí odpovídat rizikům zjištěným a odhadnutým během bezpečnostního posouzení a odhadu pravděpodobných způsobů narušení s ohledem na předpokládané vybavení narušitele.

2.8 Zápis o bezpečnostním posouzení

Výstupem procesu bezpečnostního posuzování je zápis o bezpečnostním posouzení. Zápis o bezpečnostním posouzení objektu je tedy prvním dokumentem, ze kterého se následně vychází při návrhu konkrétního řešení poplachového zabezpečovacího a tísňového systému. Zápis o bezpečnostním posouzení by měl zejména obsahovat:

- druh, rozsah a objem majetku,
- vnější, vnitřní a další případné vlivy na objekt,

- stanovení stupně zabezpečení a klasifikace prostředí, případně pojistných tříd,
- stanovení typu ochrany a způsob předání poplachové informace,
- speciální požadavky a zvláštní opatření.

Do zápisu o bezpečnostním posouzení objektu se neuvádí všechny vlivy a faktory, které jsou uvedeny v normě ČSN CLC/TS 50131-7 a jejích přílohách, ale uvádějí se jenom ty, které lze očekávat v případě daného konkrétního objektu. Základní rozsah zápisu o bezpečnostním posouzení objektu, zejména u rozsáhlých systémů, je specifikován v technické normalizační informaci TNI 33 4591-1 – komentář k ČSN CLC/TS 50131-7 – část 1: Návrh EZS. Tento dokument zároveň doplňuje a upřesňuje možnosti řešení poplachových zabezpečovacích a tísňových systémů u těchto rozsáhlých systémů. Pro potřeby provedení zápisu o bezpečnostním posouzení u jednodušších systémů lze s výhodou využít Protokol o bezpečnostním posouzení objektu, který je přílohou podnikové normy PNJ 131 společnosti Jablotron Alarms a.s., případně doplněný o další poznatky zjištěné při procesu bezpečnostního posuzování.

II. PRAKTICKÁ ČÁST

3 BEZPEČNOSTNÍ POSOUZENÍ OBJEKTU

Poplachové zabezpečovací a tísňové systémy jsou navrhovány a zřizovány především z důvodu ochrany majetku proti odcizení, poškození a zneužití. Je tedy nadmíru důležité, aby jak návrh, tak i konečná dokumentace takového systému nebyly veřejným dokumentem, ale naopak, aby byla přijata opatření proti vyzrazení této dokumentace. Zvýšené opatrnosti je pak třeba dbát na dokumentaci týkající se zabezpečení objektů, v nichž jsou zpracovávány utajované informace. Zveřejnění dokumentace k zabezpečovacímu systému a režimových opatření ostrahy takového objektu by mohlo mít fatální důsledky. Z uvedených důvodů byl pro potřeby této práce vybrán v současné době nevyužívaný objekt, který byl navíc umístěn do jiné lokality, než ve které se skutečně nachází. Pro potřeby této práce nechť je objekt situován na adrese Lounská 236/I, Kolín a je vlastnictvím společnosti PFBVD, s.r.o., přičemž nejde o sídlo společnosti, nýbrž o nový objekt, který společnost zakoupila za účelem rozšíření své další činnosti. Společnost splňuje stanovené podmínky pro práci s utajovanými informacemi a hodlá se ucházet např. o státní zakázky, jejichž dokumentace by mohla obsahovat informace ve stupni utajení Vyhrazené a Důvěrné. Na obrázku č. 3 je označen posuzovaný objekt. Na obrázku č. 4 je vstupní brána do areálu, obrázky č. 5 až 9 zobrazují z několika pohledů posuzovaný objekt.

Obr. 3 Vyznačení posuzovaného objektu v lokalitě (zdroj: www.maps.google.com)

Obr. 4 Pohled na vstup do areálu

Obr. 5 Pohled na přední stranu objektu s vchodem

Obr. 6 Pohled na objekt z boku

Obr. 7 Pohled na bok a zadní část objektu

Obr. 8 Pohled z ulice na pravou a zadní část objektu a oplocení

Obr. 9 Pohled z ulice na levou a zadní část objektu a oplocení

3.1 Provedení bezpečnostního posouzení objektu

Objekt: PFBVD, s.r.o., Lounská 236/I, Kolín

Stanovení stupně zabezpečení : 1 (2) 3 Třída klasifikace prostředí : I (II) III IV

Typ objektu :					
Rodinný dům	□	Chata, Chalupa	□	Garáž	□
Byt činžovní	□	Byt – panelák	□	Byt v rod. domě	□
Kanceláře	✓	Obchod	□	Výrobní prostory	□
Umístění střežených prostor:					
Suterén	□	Přízemí	✓	1. Patro	✓
2. Patro	□	3. Patro a vyšší	□	Podkroví	□
Konstrukce objektu:					
Zděný	✓	Prefabrikát	□	Mont. ocelová hala	□
Dřevěná roubenka	□	UNIMO dřevěný	□	UNIMO ocelový	□
Dřevený – panel	□				
Konstrukce vnitřní:					
Zděný	✓	Smíšený	□	Dřevěná roubenka	□
Prefabrikát	□	Sádrokarton	□	Dřevěný panel	□
Konstrukce střechy:					
Štítová 90°	□	Štítová 120°	□	Rovná	□
Břidlice	□	Tašky	□	Plech rovný	✓
Eternit	□	Došky	□	Plech vlnitý	□
Kritická místa:					
Okna	□	Hlavní dveře	✓	Zadní dveře	□
Světlík	□	Střešní okno	□		
Poloha objektu:					
Řadová zástavba	□	O samotě stojící	□	Mírně svažitý terén	□
Do 100 m	✓	Rovný terén	✓	Prudký svah	□
Historie vloupání:					
1 x ročně	□	Vícekrát ročně	□	Dosud nevloupáno	✓
Speciální požadavky:					
Detektor kouře	✓	Detektor plynu	✓	Záplavový detektor	✓
Při poplachu zasahuje:					
Majitel	□	Agentura PCO	✓	Policie ČR	□
Soused	□	Hlídací agentura	✓	Městská policie	□
Reakce na poplach:					
Do 5 minut	□	Do 15 minut	✓	Více než 30 minut	□
Rušivé vlivy vnitřní:					
Ventilace, vzduchotech	□	Netěsnosti oken a dveří	✓	Zářivky, halog. osvětlení	✓
Rušivé vlivy vnější:					
Výtahy, el. motory	□	Vysílače AM, FM,TV, GSM	□	Těžká doprava, tramvaje	✓

Posouzení objektu a lokality:

Jedná se o bývalý vojenský objekt umístěný v areálu téměř obdélníkového tvaru o rozměrech cca 400 x 150 m. Areál je situován v klidné okrajové části města, v blízkosti areálu je zástavba rodinných domů, několik malých podnikatelských subjektů zaměřujících se na obchod, prodej a zajišťování služeb. Dále se v nedalekém okolí areálu nachází několik sportovně rekreačních objektů (fotbalový a atletický stadion, tenisové kurty). Areál je po celém svém obvodu oplocen plechovými výplněmi na zděné podezdívce, po celém obvodu je plot opatřen trojitým ostnatým drátem. Do areálu je jediný vjezd dvoukřídlými plechovými vraty. V areálu je dalších 10 budov, z nichž jedna je využívána jako zdravotnické středisko a ostatní budovy jsou v podstatě využívány jako skladové prostory. Areál je v nočních hodinách a ve dnech pracovního klidu uzavřen a monitorován bezpečnostní agenturou.

Posuzovaný objekt je postaven na rovinatém pozemku, jde o samostatně stojící cihlovou nepodsklepenou budovu s prvním a druhým nadzemním patrem. Budova má tvar obdélníku o rozměrech 40 x 12 m s vystoupením ve středu přední části budovy, kde je umístěn jediný vchod do budovy a vnitřní schodiště do patra. Střešní konstrukce budovy je tvořena dřevěným trámovím s krytinou z rovného plechu. Obvodové stěny budovy mají tloušťku minimálně 30 cm. Budova byla dlouhodobě nevyužívána, je nezbytné posoudit technický stav elektroinstalace, odpadů a rozvodů tepelné energie a vody. Celkový technický stav konstrukce budovy a střechy je dobrý.

V současné době není objekt vybaven žádným poplachovým zabezpečovacím a tísňovým systémem. V objektu bude prováděna vnitřní rekonstrukce, lze proto instalovat zabezpečovací systém založený na metalickém vedení napájení a signalizace. Výjimku pak bude tvořit bezdrátový tísňový hlásič.

Okenní otvory mají rozměr 100 x 215 cm, okenní otvor v průčelí objektu nad vstupními dveřmi má rozměr 180 x 160 cm, spodní okraj okenních otvorů v přízemí je ve výšce 1,6 m, spodní okraj okenních otvorů v patře je ve výšce 5,6 m. Všechna okna, kromě okna v průčelí nad vstupem do budovy, jsou tvořena spodní otevíratelnou částí a horní neotevíratelnou částí. Spodní část je tvořena dvoukřídlými dřevěnými dvojitými rámy s dvojskly o velikosti křídla 50 x 135 cm, horní část je tvořena dřevěným dvojitým rámem s dvojsklem o velikosti rámu 100 x 80 cm. Okno v průčelí objektu nad vstupními dveřmi je tvořeno trojkřídlým otevíratelným rámem s dvojskly.

Na všech oknech objektu jsou instalovány kovové mříže neznámého výrobce. Mříže jsou tvořeny ocelovými pruty čtvercového profilu o rozměrech 2 x 2 cm a velikosti ok maximálně 10 x 40 cm. Ukotvení mříží je přímé ve třech místech do obou svislých ostění každého okna. Mříže na všech oknech jsou v bezvadném technickém stavu. Některá okna jsou ve špatném technickém stavu, je nezbytné provést jejich opravu popřípadě výměnu. Z bezpečnostního hlediska je nevyhovující vstup do objektu a to zejména z důvodu nevyhovujícího technického stavu. Vstup do objektu je v současné době tvořen dvoukřídlými prosklenými dveřmi s cylindrickou vložkou FAB stupně bezpečnosti 1 – základní ochrana. Je nutné provést výměnu těchto dveří nejlépe za bezpečnostní dveře odpovídající třídy bezpečnosti. Pozornost je třeba věnovat zabezpečení šesti vikýřů a průlezu do půdního prostoru z chodby v patře budovy. Dále je třeba provést zabezpečení průlezu ke komínu. V blízkosti posuzovaného objektu je několik vzrostlých stromů, v současné době žádný nezasahuje nad prostor střechy budovy. Je nezbytné provádět pravidelnou kontrolu stavu okolních stromů a případně prořezání koruny stromu, který by zasahoval nad střechu budovy.

Druh, rozsah a objem majetku:

Předmětem činnosti v posuzovaném objektu bude pouze administrativní činnost. V objektu se nebude nacházet žádný cennější majetek, ale pouze běžné kancelářské vybavení. Předmětem zájmu případného pachatele by mohla být s největší pravděpodobností pouze výpočetní technika, která bude v objektu. Je potřeba vést přehlednou evidenci majetku objektu a provádět pravidelné inventury, pro předcházení větších ztrát vzniklých případnými krádežemi některým ze zaměstnanců. Vzhledem k faktu, že je areál ve všední dny v době od 18:00 do 6:00 hodin a ve dnech pracovního klidu uzavřen a celý oplocen pevným plotem doplněným o ostnatý drát, není předpoklad vzniku poškození střeženého objektu vandalismem.

Stanovení stupně zabezpečení a klasifikace prostředí:

Objekt bude využíván jako administrativní pracoviště. V objektu se tak nebude vyskytovat žádný neobvykle cenný majetek, jen cca 25 počítačových sestav, několik kusů multifunkčních tiskových zařízení a další běžné kancelářské vybavení. Ve druhém nadzemním patře objektu budou dvě zabezpečené oblasti ve smyslu zákona č. 412/2005

Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve kterých budou mimo jiné zpracovávány a ukládány utajované informace stupně utajení Vyhrazené a Důvěrné v listinných podobách. Na základě vyhodnocení míry rizika hrozící objektu s přihlédnutím na požadavky zabezpečení objektu podle zákona č. 412/2005 Sb. a příslušných právních předpisů lze předpokládat nízké až střední riziko narušení objektu, tedy lze stanovit požadovaný stupeň zabezpečení 2. Téměř všechny komponenty systému zabezpečení budou umístěny uvnitř objektu, který je trvale vytápěn a lze tedy stanovit třídu prostředí II – prostředí vnitřní všeobecné. Komponenty venkovní siréna s blikačem a venkovní čtečka systému kontroly vstupu musejí odpovídat třídě prostředí IV – prostředí venkovní všeobecné.

Při vytváření návrhu systému je třeba přihlédnout k požadavkům na ochranu utajovaných informací, zejména pak na fakt, že prostory musejí být zabezpečeny mechanickými zábrannými prostředky a střeženy poplachovým zabezpečovacím systémem certifikovaným Národním bezpečnostním úřadem. Do objektu je zavedena telefonní linka napojená na digitální telefonní ústřednu, je tedy možné využít napojení ústředny zabezpečovacího systému přes IP komunikátor. Komunikace mezi ústřednou zabezpečovacího systému a pultem centralizované ochrany může probíhat prostřednictvím Internetu. V lokalitě objektu je dostatečný signál všech tří mobilních operátorů pro použití GSM komunikátoru jako záložního prostředku přenosů mezi ústřednou zabezpečovacího systému a pultem centralizované ochrany. Dalším požadavkem zákona č. 412/2005 Sb. k ochraně utajovaných informací do stupně utajení Důvěrné je použití elektrických zámkových zařízení a systému pro kontrolu vstupů. Je tedy nezbytné do návrhu zabezpečovacího systému zapracovat systém pro kontrolu vstupů certifikovaný Národním bezpečnostním úřadem, který umožní na základě přidělení oprávnění jednotlivým zaměstnancům vstup těchto zaměstnanců do objektu a dalších prostor v souladu s podmínkami pro ochranu utajovaných informací. Systém pro kontrolu vstupů lze s výhodou využít pro potřeby evidence docházky zaměstnanců. Tato služba byla zákazníkovi při prvotní konzultaci požadavků na vytvoření zabezpečovacího systému navrhnuta a zákazník tuto službu požaduje. Při zpracovávání utajovaných informací do stupně utajení Důvěrné zákon č. 412/2005 Sb. požaduje kromě použití technických zabezpečovacích prvků také nepřetržité střežení objektu ostrahou. Podmínkou pro ostrahu objektu s utajovanými informacemi do stupně utajení Důvěrné je přítomnost nejméně jednoho člena ostrahy nepřetržitě v objektu. Objekt bude možné střežit pouze jedním

pracovníkem ostrahy, přičemž případné vyhlášení poplachu bude zároveň ústřednou zabezpečovacího systému signalizováno na pult centralizované ochrany (PCO), nejprve jen jako informace o mimořádném stavu ve střeženém objektu. Pracovník ostrahy pak bude mít určitý časový interval na vyřešení situace a deaktivaci poplachu. Pokud nebude poplach pracovníkem ostrahy deaktivován v daném časovém intervalu, PCO vyšle na místo zásahovou skupinu. Pro případ vzniku situace, kterou nebude pracovník ostrahy schopen evidentně zvládnout sám, bude vybaven bezdrátovým tísňovým tlačítkem. Po vyhlášení tísně bude na místo okamžitě vyslána zásahová skupina. Takto zpracovaná koncepce ostrahy vede ke splnění požadavků zákona a zároveň k ušetření nákladů na lidské zdroje při vícečlenné ostraze.

Vlivy působící na objekt:

Posuzovaný objekt se nachází v klidné lokalitě města zastavěné zčásti rodinnými domky a z části drobnými provozními a obchodními objekty. V blízkém okolí objektu se nachází komplex sportovně relaxačních objektů a městský park. Není zde předpoklad vlivu na poplachový zabezpečovací a tísňový systém za strany okolních objektů. V žádném z okolních objektů nejsou v současné době provozy, které by mohly ovlivnit systém. Město Kolín je klidnou lokalitou, geologicky neaktivní s převládajícími mírnými klimatickými podmínkami bez výrazných výkyvů počasí a extrémních teplot. Ve vzdálenosti cca 15 km od posuzovaného objektu se nachází vojenská základna taktického letectva v Čáslavi, přičemž dochází k občasným přeletům nadzvukových i podzvukových vojenských letadel nad lokalitou objektu. Tento fakt je třeba zahrnout v návrhu a realizaci poplachového zabezpečovacího a tísňového systému, zejména pak při nastavení citlivosti otřesových detektorů, aby se předešlo planým poplachům. Ve vzdálenosti cca 100 m od posuzovaného objektu se nachází jednokolejná neelektrifikovaná železniční trať, která je v současné době nevyužívána a ve střednědobém horizontu není pravděpodobné její využívání. Silniční doprava v lokalitě není nijak zvlášť exponovaná, silnice jsou využívány především pro osobní dopravu. Není pravděpodobný přílišný vliv silniční dopravy na funkčnost zabezpečovacího systému.

Základem zabezpečení posuzovaného objektu by měly být prvky plášťové a prostorové ochrany. Zabezpečovaný objekt je cihlová budova pevné konstrukce se stropy ve všech místnostech ve výšce minimálně 4 m. Nejvhodnější pro zajištění prostorové

a plášťové ochrany objektu bude použití PIR detektorů v kancelářích pod stropem a magnetických kontaktů – detektorů otevření vstupních dveří do objektu, dveří do dalších prostor, oken v obvodových stěnách objektu, vikýřů a průlezů na půdu a ke komínu. Plášťová ochrana bude zároveň zajištěna bezpečnostními vstupními dveřmi do objektu a mřížemi na oknech obvodových stěn objektu. Pro minimalizaci vzniku planých poplachů signalizací PIR detektory se doporučuje provést případnou montáž žaluzií nebo rolet do dvojitého rámu oken a zároveň provést kontrolu a utěsnění oken. Těmito opatřeními dojde k minimalizaci vzniku planých poplachů způsobených pohybem žaluzií apod. vlivem průvanu nebo sálání radiátorů umístěných pod oknem. Není předpoklad zastínění umístěných PIR detektorů. Při posuzování nebyly zjištěny vlivy ovlivňující činnost uvažovaných detektorů otevření.

Speciální požadavky a zvláštní opatření:

V objektu bude zaměstnáno cca 25 zaměstnanců provádějících administrativní činnost. Z důvodu výskytu utajovaných informací v zabezpečovaném objektu je nezbytné věnovat zvláštní pozornost výběru komponent zabezpečovacího systému, zejména pak vybírat technické prostředky certifikované Národním bezpečnostním úřadem. V zabezpečených oblastech ve druhém nadzemním podlaží budou dle přání zákazníka umístěny certifikované trezory pro ukládání listin s utajovanými informacemi, které mají být střeženy otřesovými detektory napojenými na ústřednu zabezpečovacího systému.

Zákazník požaduje v rámci vybudování zabezpečovacího systému i sledování havarijních stavů. V technické místnosti v prvním nadzemním patře je instalován plynový kotel na zemní plyn. V technické místnosti bude umístěn detektor unikajících výbušných plynů, zejména zemního plynu, jehož signalizace bude jednak opticko – akustická a jednak napojená na ústřednu zabezpečovacího systému. Ústředna zabezpečovacího systému po vyhlášení signalizace uzavře elektromagnetický ventil na přívodním potrubí zemního plynu. Zákazník dále požaduje instalaci detektorů pro signalizaci požáru. V každé místnosti objektu budou instalovány kombinované opticko – kouřové detektory k detekci vzniku požáru zjištěním přítomnosti kouře nebo zjištěním vysoké teploty. Detektor bude vznik požáru signalizovat rozsvícením LED diody a předáním signálu ústředně zabezpečovacího systému, která vyhlásí poplach. Pro případ porušení střešní krytiny nebo celé střešní konstrukce, v jehož důsledku by mohlo dojít k prosakování srážek

do kancelářských prostor s utajovanými informacemi, bude instalován u trezorů s uloženými utajovanými informacemi záplavový detektor se signalizací na ústřednu zabezpečovacího systému.

Další požadavky a opatření, poznámky:

Další požadavky zákazníka a případná opatření mající vliv na realizaci zabezpečovacího systému objektu budou se zákazníkem v průběhu realizace konzultovány.

4 PROJEKT FYZICKÉ BEZPEČNOSTI

Každý subjekt, který je ve smyslu zákona č. 412/2005 Sb. oprávněn nakládat s utajovanými informacemi, ať už se jedná např. o podnikatele či orgán státní správy, je povinen přijmout opatření nezbytná k zabezpečení a ochraně utajovaných informací předtím, než začne ve svých prostorách zpracovávat a ukládat utajované informace. Zpravidla to znamená zabezpečení objektu mechanickými zábrannými prostředky a instalací poplachového zabezpečovacího systému, případně i tísňového systému, instalací systému elektronické kontroly vstupu či speciálních televizních systémů a přijetím pravidel pro nakládání s utajovanými informacemi a pro pohyb zaměstnanců a návštěv v objektu s utajovanými informacemi. Subjekt je zároveň povinen vypracovat dokument, který obsahuje popis přijatých opatření k ochraně utajovaných informací. Tímto dokumentem je projekt fyzické bezpečnosti. Vypracovaný projekt fyzické bezpečnosti daného objektu musí být předložen ke kontrole přijatých opatření zpravidla Národnímu bezpečnostnímu úřadu. Následně proběhne fyzická kontrola přijatých opatření na místě a po schválení projektu fyzické bezpečnosti může teprve docházet k nakládání s utajovanými informacemi v daném objektu. Schválený projekt fyzické bezpečnosti se ukládá u odpovědné osoby nebo bezpečnostního ředitele.

4.1 Legislativní úprava vytváření projektu fyzické bezpečnosti

Projekt fyzické bezpečnosti je právně vymezen v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti v II. části, V. hlavě, § 32 a 33. Projekt fyzické bezpečnosti obsahuje jiné náležitosti v případě objektu s jednací oblastí, jiné náležitosti v případě objektu se zabezpečenou oblastí kategorie Vyhrazené a jiné náležitosti v případě objektu se zabezpečenou oblastí kategorie Přísně tajné, Tajné nebo Důvěrné. Projekt fyzické bezpečnosti objektu, ve kterém se nachází pouze zabezpečená oblast kategorie Vyhrazené, musí obsahovat:

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

Větší pozornost je upřena na zabezpečení objektů se zabezpečenými oblastmi kategorie Přísně tajné, Tajné nebo Důvěrné. Projekt fyzické bezpečnosti objektu, v němž se nachází takové zabezpečené oblasti, je rozsáhlejší a musí obsahovat zejména:

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

Obdobně rozsáhlé jsou projekty fyzické bezpečnosti pro objekty, v nichž se nachází jednací oblasti. V případě, že se v objektu nachází více zabezpečených oblastí, vypracuje se jen jeden projekt fyzické bezpečnosti pro všechny zabezpečené oblasti objektu a to i v případě, že jde o zabezpečené oblasti různých kategorií.

Prováděcím právním předpisem pro oblast fyzické bezpečnosti je vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. Vyhláška stanovuje bodové ohodnocení jednotlivých opatření fyzické bezpečnosti, uvádí nejnižší míru zabezpečení jednotlivých zabezpečených oblastí a jednacích oblastí, definuje základní metodu hodnocení rizik, uvádí další požadavky na opatření fyzické bezpečnosti a náležitosti certifikace technického prostředku.

Aby nebylo možné zaměnit významy důležitých pojmů užívaných při vytváření projektů fyzické bezpečnosti, jsou tyto pojmy jasně definovány v uvedené vyhlášce. Mezi nejdůležitější definované pojmy patří:

- objekt – budova nebo jiný ohraničený prostor, ve kterém se nacházejí zabezpečené nebo jednací oblasti,
- hranice objektu – plášť budovy, fyzická bariéra (oplocení) nebo jinak viditelně vymezená hranice,
- hranice zabezpečené oblasti nebo jednací oblasti – stavebně nebo jinak viditelně ohraničený prostor,
- vstup do objektu, zabezpečené oblasti nebo jednací oblasti – místo určené pro vstup a výstup osob a místo určené pro vjezd a výjezd dopravních prostředků,
- provozovatel objektu – odpovědná osoba popřípadě osoba jí k tomu pověřená,

- hrozba – možnost vyzrazení nebo zneužití utajované informace při narušení fyzické bezpečnosti,
- riziko – pravděpodobnost, že se určitá hrozba uskuteční,
- mimořádná situace – stav, kdy bezprostředně hrozí, že dojde k vyzrazení nebo zneužití utajované informace,
- technický prostředek – bezpečnostní prvek, jehož použitím se zabraňuje, ztěžuje nebo oznamuje narušení ochrany objektu, zabezpečené oblasti nebo jednací oblasti a dále ničí utajované informace,
- úschovný objekt – trezor, uzamykatelná skříň nebo jiná schránka,
- útočník – fyzická osoba, která vyvíjí činnost s cílem překonat technické prostředky a další překážky sloužící k zabezpečení ochrany utajovaných informací.

Zabezpečené oblasti a jednací oblasti ve smyslu zákona č. 412/2005 Sb. jsou zabezpečovány zejména kombinací opatření fyzické bezpečnosti, režimových opatření a ostrahou, a to v závislosti na stupni utajovaných informací, které se v daných oblastech nacházejí nebo projednávají. Přitom je třeba pravidelně ověřovat opatření fyzické bezpečnosti a opakovaně provádět vyhodnocení rizik, neboť situace daná při návrhu a realizaci zabezpečení a následného vytvoření a schválení projektu fyzické bezpečnosti se může v průběhu času výrazně měnit. Opatřeními fyzické bezpečnosti se rozumí především použití technických prostředků k zabezpečení objektu a zabezpečených a jednacích oblastí. Při zabezpečování jednotlivých objektů a oblastí je nutné, aby provozovatel objektu jasně stanovil hranici objektu, hranice zabezpečených oblastí a jejich zařazení do příslušné kategorie a třídy. Ve vyhlášce jsou pro jednotlivé kategorie zabezpečených oblastí stanoveny minimální technické prostředky, které je nezbytné použít k zabezpečení těchto oblastí. V zabezpečené oblasti kategorie Vyhrazené musejí být použity nejméně mechanické zábranné prostředky. Zabezpečená oblast kategorie Důvěrné musí být zabezpečena minimálně mechanickými zábranné prostředky a zařízením elektrické zabezpečovací signalizace. V zabezpečené oblasti kategorie Tajné a Přísně tajné musejí být použity mechanické zábranné prostředky, systémy pro kontrolu vstupů, zařízení elektrické zabezpečovací signalizace, speciální televizní systémy a zařízení elektrické požární signalizace. Pokud je však použit speciální televizní systém, nesmí tento systém narušit ochranu utajovaných informací. Speciální televizní systémy užívané v zabezpečených oblastech lze nahradit použitím tísňových systémů.

Pokud je v zabezpečené oblasti kategorie Důvěrné a vyšší zajištěna trvalá přítomnost pracujících osob, zabezpečuje se tato oblast především mechanickými zábrannými prostředky a elektrickou zabezpečovací signalizací nebo použitím tísňového systému. V případě umístění stálého stanoviště ostrahy v takové zabezpečené oblasti, není nutné používat zařízení elektrické zabezpečovací signalizace. Při ochraně utajovaných informací v objektu a zabezpečených a jednacích oblastech by se měly používat certifikované technické prostředky. Certifikaci provádí Národní bezpečnostní úřad, případně jiný subjekt na základě dohody uzavřené s Národním bezpečnostním úřadem. Necertifikované technické prostředky lze použít k zajištění ochrany zabezpečených oblastí kategorie Vyhrazené. K zajištění ochrany zabezpečených oblastí kategorie Důvěrné a vyšší lze necertifikované technické prostředky použít pouze v případě, že nesníží úroveň ochrany požadované pro daný stupeň. Utajované informace se ukládají v zabezpečených oblastech, případně v úschovném objektu, pokud je bodová hodnota tohoto úschovného objektu uplatněna v projektu fyzické bezpečnosti. Bodové hodnoty jednotlivých kategorií úschovných objektů jsou uvedeny v příloze č. 1 vyhlášky. Vyhláška dále ukládá povinnost umístit v objektu zařízení fyzického ničení nosičů informací. Pokud je hranice objektu totožná s hranicí zabezpečené oblasti, rozsah opatření fyzické bezpečnosti je určen požadavky na kategorii dané zabezpečené oblasti. V opačném případě, tedy pokud hranice objektu a zabezpečené oblasti nejsou totožné, je nutné provést zabezpečení na hranici objektu, kde se taková zabezpečená oblast nachází. Zabezpečení na hranici objektu je pak zajištěno:

- pro zabezpečenou oblast kategorie Vyhrazené mechanickými zábrannými prostředky,
- pro zabezpečenou oblast kategorie Důvěrné a Tajné – mechanickými zábrannými prostředky a zařízeními elektrické zabezpečovací signalizace,
- pro zabezpečenou oblast kategorie Přísně tajné – mechanickými zábrannými prostředky, zařízeními elektrické zabezpečovací signalizace a speciálními televizními systémy.

Obdobným způsobem, jako jsou stanoveny podmínky zabezpečení zabezpečených oblasti, jsou stanoveny podmínky zabezpečení jednacích oblastí a technických zařízení.

Režimová opatření vyhláška definuje jako:

- stanovení oprávnění osob a dopravních prostředků pro vstup do objektu, stanovení oprávnění osob pro vstup do zabezpečené oblasti a jednací oblasti a způsob kontroly těchto oprávnění,

- kontrolní opatření při vstupu do objektu, zabezpečených a jednacích oblastí a způsob kontroly těchto opatření,
- podmínky a způsob kontroly pohybu osob v objektu, zabezpečené oblasti a jednací oblasti a způsob kontroly a vynášení utajovaných informací z objektu, zabezpečené oblasti a jednací oblasti,
- režim manipulace s klíči a identifikačními daty,
- režim manipulace s technickými prostředky a jejich používání.

Pohyb osob a dopravních prostředků v objektu se zabezpečenou či jednací oblastí má svá přesná pravidla. Provozovatel objektu vydává seznam osob a dopravních prostředků, které mohou vstupovat, resp. vjíždět do objektu. Tento seznam je pak uložen u provozovatele objektu. Při vstupu do objektu, kde se nachází zabezpečená oblast kategorie Důvěrné a vyšší nebo jednací oblast kategorie Tajné a vyšší, se provádí kontrola vstupu těchto osob a zároveň se vede evidence údajů o návštěvách. U těchto objektů je povinně stanoven režim návštěv s doprovodem. V případě návštěvy osob neoprávněných k samostatnému vstupu do objektu se zabezpečenou nebo jednací oblastí kategorie Přísně tajné se ještě u těchto osob provádí kontrola na vyhledávání nebezpečných látek a předmětů.

Ve vyhlášce je dále definován režim manipulace s klíči a identifikačními daty jako systém a způsob označování, přidělování a odevzdávání, jejich úschovy a evidence, uložení duplikátů a způsob jejich použití. Režim manipulace s klíči a identifikačními daty k zabezpečené oblasti a k úschovnému objektu s utajovanými informacemi stupně utajení Vyhrazené stanoví provozovatel objektu. Klíče a identifikační data k zabezpečené a jednací oblasti a úschovnému objektu, v nichž se nachází utajované informace stupně utajení Vyhrazené se zvláštním režimem (např. KRYPTO) nebo utajované informace stupně utajení Důvěrné a vyšší, musejí být označeny a ukládají se zvláštním způsobem, který umožňuje kontrolu jejich použití a jejich výdej podléhá evidenci. Zabezpečená a jednací oblast a úschovný objekt musejí být v případě nepřítomnosti oprávněných osob uzamčeny. Osoby, které disponují s klíči a identifikačními daty je ukládají na stanoveném místě v objektu, pokud provozovatel objektu neurčí jinak. V případě ztráty klíčů či identifikačních dat musí být tato jejich ztráta neprodleně oznámena provozovateli objektu a musí být zajištěna náprava.

Pravidla a podmínky pro výkon ostrahy v objektech se zabezpečenými nebo jednacími oblastmi jednotlivých stupňů a bodová ohodnocení daného typu ostrahy jsou stanoveny v příloze č. 1 této vyhlášky.

Ve vyhlášce je dále definován pojem ověřování opatření fyzické bezpečnosti. Tímto se rozumí ověření, zda jednotlivá použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a právním předpisům v oblasti ochrany utajovaných informací. Ověřování těchto opatření je povinen provozovatel objektu nebo jím pověřená osoba provádět průběžně, nejméně však každých dvanáct měsíců.

Postup provádění vyhodnocení rizik je vyhláškou stanoven jako následující kroky:

- identifikace stupňů utajovaných informací a zjištění množství utajovaných informací, které se v objektu vyskytují nebo budou vyskytovat, zejména z hlediska následku jejich vyzrazení nebo zneužití,
- popis a vyhodnocení hrozeb, kterým jsou tyto utajované informace vystaveny,
- popis a vyhodnocení zranitelnosti utajovaných informací vůči těmto hrozbám,
- stanovení míry rizika, jako "malé", "střední" nebo "velké", na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací.

V závěru vyhláška stanovuje náležitosti žádosti o certifikaci technického prostředku a dobu platnosti certifikátu technického prostředku a náležitosti žádosti o uzavření smlouvy o zajištění činnosti provádění certifikace jiným subjektem, než je Národní bezpečnostní úřad.

Součástí vyhlášky jsou dvě přílohy. Příloha č. 1 je nepostradatelným dokumentem při vytváření projektu fyzické bezpečnosti. Tato příloha popisuje mimo jiné jednotlivá bodová ohodnocení nejnižší míry zabezpečení zabezpečené oblasti, jednací oblasti a zabezpečení technického zařízení. Dále jsou v této příloze uvedeny bodové hodnoty ostrahy objektu a struktura projektu fyzické bezpečnosti. V neposlední řadě uvádí způsob a podmínky používání technických prostředků po uplynutí doby platnosti certifikátů těchto prostředků. V příloze č. 2 je pak uveden vzor certifikátu technického prostředku.

Vyhláška nabyla účinnosti dnem 1. ledna 2006. Stejně jako zákon č. 412/2005 Sb. užívá vyhláška některé pojmy, které však již byly v bezpečnostní praxi nahrazeny jinými s obdobným významem. Např. pojem elektrická zabezpečovací signalizace (EZS) byl nahrazen pojmem poplachový zabezpečovací a tísňový systém (I&HAS) normou ČSN EN 50131-1. Při vytváření projektů fyzické bezpečnosti je však nezbytné dodržovat názvosloví podle zákona č. 412/2005 Sb. a jeho prováděcích právních předpisů.

4.2 Návrh projektu fyzické bezpečnosti

Projekt fyzické bezpečnosti

objektu společnosti PFBVD, s.r.o.

Lounská č.p. 236/I, Kolín

se zabezpečenými oblastmi kategorie

Vyhrazené a Důvěrné

I. URČENÍ OBJEKTU A ZABEZPEČENÉ OBLASTI

Obecný úvod

Projekt fyzické bezpečnosti objektu a v něm zřízených zabezpečených oblastí je realizován v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a vyhláškou č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

Adresa budovy s objektem, ve kterém se nacházejí zabezpečené oblasti kategorie Důvěrné a Vyhrazené je PFBVD, s.r.o., Lounská č.p. 236/I, Kolín. Vlastníkem budovy je společnost PFBVD, s.r.o., která je jediným uživatelem budovy. Jedná se o samostatně stojící nepodsklepenou budovu o dvou nadzemních podlažích, která je umístěna v oploceném areálu s jediným místem vstupu a vjezdu z ulice Lounská. Konstrukce budovy je cihlová o minimální síle obvodové stěny 30 cm. Střecha budovy je valbová s plechovou krytinou. Pod střechou budovy je půda. Budova je vytápěna ústředním topením s radiátory s vlastním plynovým kotlem. Do budovy není žádný vjezd. Do budovy je možné vstoupit jediným vchodem z prostor areálu. Vstupuje se dvoukřídlými uzamykatelnými protipožárními bezpečnostními dveřmi. Za vstupními dveřmi do objektu je vlevo umístěno stanoviště ostrahy objektu provádějící kontrolu vstupu do budovy. Schéma budovy s vyznačením hranice objektu, zabezpečených oblastí a prvků elektrického zabezpečovacího systému (dále jen EZS) je v příloze č. 1 tohoto projektu fyzické bezpečnosti.

Stanovení objektu

Objekt odpovídá typu 2 a nachází se v něm zabezpečené oblasti kategorie Vyhrazené a Důvěrné. Objekt tvoří první a druhé nadzemní podlaží budovy. Provozovatelem tohoto objektu je ředitel společnosti PFBVD, s.r.o., který odpovídá za ochranu utajovaných informací v rozsahu své kompetence. Objekt je tvořen těmito místnostmi:

1. nadzemní podlaží:
   - vstupní hala s chodbami a schodištěm – místnost č. 1
   - stanoviště ostrahy – místnost č. 2
   - kanceláře – místnost č. 3, 4, 7, 8, 9
   - WC – místnost č. 5
   - technická místnost s plynovým kotlem – místnost č. 6
2. nadzemní podlaží:
   - hala s průlezem na půdu – místnost č. 10
   - zabezpečená oblast kategorie Vyhrazené
     - chodba – místnost č. 11
     - kanceláře – místnost č. 12, 13. 14

zabezpečená oblast kategorie Důvěrné
- chodba – místnost č. 15
- kanceláře – místnost č. 16, 17, 18

Objekt je ohraničen v prvním nadzemním podlaží cihlovou obvodovou zdí budovy o síle více než 30 cm v nejslabším místě s okny zabezpečenými mechanickými zábrannými prostředky (pevná kovová mříž) a technickými prostředky EZS. Spodní hranice oken v prvním nadzemním patře je ve výšce 1,6 m nad úrovní terénu. Vstup do objektu je možný pouze bezpečnostními vstupními dveřmi opatřenými uzamykacím systémem a technickým prostředkem EZS. V druhém nadzemním podlaží je objekt ohraničen cihlovou obvodovou zdí budovy o síle více než 30 cm v nejslabším místě s okny zabezpečenými mechanickými zábrannými prostředky (pevná kovová mříž) a technickými prostředky EZS a průlezovým otvorem z haly na půdu zabezpečeným technickým prostředkem EZS. Spodní hranice oken v druhém nadzemním podlaží je výše než 5,5 m nad úrovní terénu.

Vstup do objektu je možný pouze v pracovní dny v době od 6:00 do 18:00 hodin vstupními dveřmi do budovy a dále kolem stanoviště ostrahy, na němž je minimálně jeden pracovník ostrahy, který zabezpečuje režim vstupu. Vstupní dveře do budovy jsou opatřeny čtecím zařízením elektronické kontroly vstupu. V pracovní době jsou vstupní dveře odemčeny, mimo tuto dobu jsou uzavřeny a uzamčeny, vstup do budovy je střežen ostrahou ze stanoviště ostrahy.

Objekt je zabezpečen kombinací režimových opatření, ostrahy a technických prostředků. Ostraha objektu je typu 2 a zajišťují ji pracovníci smluvní bezpečnostní ochranné služby nepřetržitě 24 hodin denně přítomností nejméně jednoho pracovníka ostrahy na stanovišti ostrahy u vstupu do budovy v kombinaci s napojením ústředny EZS střeženého objektu na pult centralizované ochrany. Pravidla pro výkon ostrahy a režimová opatření jsou stanovena v provozním řádu tohoto projektu fyzické bezpečnosti. Technické prostředky jsou použity ve formě kovových mříží na oknech objektu, zařízení systému elektronické kontroly vstupů (dále jen EKV) a prostředků EZS typu 2 s instalací typu 2 v rozsahu prostorové a plášťové ochrany objektu s použitím bezdrátového tísňového tlačítka pracovníka ostrahy.

Stanovení zabezpečených oblastí

V objektu jsou dvě zabezpečené oblasti:

- zabezpečená oblast V – zabezpečená oblast kategorie Vyhrazené, třídy II a typu 2. Zabezpečená oblast V je umístěna ve druhém nadzemním podlaží v místnostech č. 11, 12, 13 a 14. Hranice je tvořena levou stěnou haly z pohledu od schodiště a obvodovými stěnami levé části budovy. Stěny jsou z cihlového zdiva o tloušťce v nejslabším místě minimálně 30 cm. V obvodových stěnách budovy, jež tvoří hranici zabezpečené oblasti, jsou jednoduchá dřevěná okna, jejichž spodní hrana je výše než 5,5 m nad úrovní terénu. Okna jsou zabezpečena necertifikovanými mřížemi tvořenými ocelovými pruty čtvercového profilu o rozměrech 2 x 2 cm a velikosti ok maximálně 10 x 40 cm. Do zabezpečené oblasti V je jediný vchod z haly druhého nadzemního podlaží dvoukřídlými bezpečnostními protipožárními dveřmi Sherlock typ D2 F5/3 s elektronickým ovládáním zámku. Zabezpečená oblast V je střežena EZS – ústředna Magellan MG 5050 Paradox Variant typu 2 s instalací typu 2, která je umístěna na stanovišti ostrahy. V zabezpečené oblasti V je jeden úschovný objekt typu 3 Axi Mont CST 5 pro ukládání nosičů utajovaných informací a skartační zařízení typu 2 HSM 225.2. Vstup do zabezpečené oblasti V je střežen prostorovým PIR detektorem typu 2 Pro Plus (476) Paradox Variant a magnetickým kontaktem typu 3 3G-SM-60 Sentek Variant na vstupních dveřích. Vstup do zabezpečené oblasti V je umožněn přiložením identifikační karty oprávněného zaměstnance ke čtecímu zařízení systému EKV. Kanceláře v zabezpečené oblasti V jsou střeženy prostorovými PIR detektory typu 2 Pro Plus (476) Paradox Variant a magnetickými kontakty na otevíratelných částech rámů oken typu 3 3G-SM-60 Sentek Variant. Úschovný objekt utajovaných informací je střežen otřesovým detektorem typu 2 Paradox Variant Safe Protector 950. Uvedené prvky ESZ, úschovný objekt a skartační zařízení jsou certifikovány NBÚ. Zároveň je umístění úložného prostoru monitorováno záplavovým detektorem Variant WLD38R. Prostory zabezpečené oblasti V jsou dále monitorovány kombinovaným opticko – kouřovým a teplotním detektorem Variant FDR-36-SHR. Narušení prostoru je signalizováno na stanoviště ostrahy.
- zabezpečená oblast D – zabezpečená oblast kategorie Důvěrné, třídy II a typu 2. Zabezpečená oblast D je umístěna ve druhém nadzemním podlaží v místnostech č. 15, 16, 17 a 18. Hranice je tvořena pravou stěnou haly z pohledu od schodiště a obvodovými stěnami pravé části budovy. Stěny jsou z cihlového zdiva o tloušťce

v nejslabším místě minimálně 30 cm. V obvodových stěnách budovy, jež tvoří hranici zabezpečené oblasti, jsou jednoduchá dřevěná okna, jejichž spodní hrana je výše než 5,5 m nad úrovní terénu. Okna jsou zabezpečena necertifikovanými mřížemi tvořenými ocelovými pruty čtvercového profilu o rozměrech 2 x 2 cm a velikosti ok maximálně 10 x 40 cm. Do zabezpečené oblasti D je jediný vchod z haly druhého nadzemního podlaží dvoukřídlými bezpečnostními protipožárními dveřmi Sherlock typ D2 F5/3 s elektronickým ovládáním zámku. Zabezpečená oblast D je střežena EZS – ústředna Magellan MG 5050 Paradox Variant typu 2 s instalací typu 2, která je umístěna na stanovišti ostrahy. V zabezpečené oblasti D je jeden úschovný objekt typu 3 Axi Mont CST 5 pro ukládání nosičů utajovaných informací a skartační zařízení typu 2 HSM 225.2. Vstup do zabezpečené oblasti D je střežen prostorovým PIR detektorem typu 2 Pro Plus (476) Paradox Variant a magnetickým kontaktem typu 3 3G-SM-60 Sentek Variant na vstupních dveřích. Vstup do zabezpečené oblasti D je umožněn přiložením identifikační karty oprávněného zaměstnance ke čtecímu zařízení systému EKV. Kanceláře v zabezpečené oblasti D jsou střeženy prostorovými PIR detektory typu 2 Pro Plus (476) Paradox Variant a magnetickými kontakty na otevíratelných částech rámů oken typu 3 3G-SM-60 Sentek Variant. Úschovný objekt utajovaných informací je střežen otřesovým detektorem typu 2 Paradox Variant Safe Protector 950. Uvedené prvky ESZ, úschovný objekt a skartační zařízení jsou certifikovány NBÚ. Zároveň je umístění úložného prostoru monitorováno záplavovým detektorem Variant WLD38R. Prostory zabezpečené oblasti D jsou dále monitorovány kombinovaným opticko – kouřovým a teplotním detektorem Variant FDR-36-SHR. Narušení prostoru je signalizováno na stanoviště ostrahy.

II. VYHODNOCENÍ RIZIK

Specifikace aktiv

V objektu se vyskytují utajované informace stupně utajení Vyhrazené a Důvěrné ve formě listinných materiálů (písemnosti, předpisy, fotodokumentace) v počtu do cca 50 listů s utajovanými informacemi stupně utajení Vyhrazené a počtu do cca 50 listů s utajovanými informacemi stupně utajení Důvěrné.

Stanovení jednotlivých hrozeb a zranitelnosti

- Vyzrazení nebo zneužití utajované informace porušením povinnosti při její ochraně fyzickou osobou, která má přístup k utajované informaci.
- Vyzrazení utajované informace aktivní činností neoprávněné osoby za účelem získání utajované informace, a to pozorováním, odposlouchávání nebo bezprostředním přístupem k utajované informaci.
- Zánik utajované informace zničením jejího nosiče požárem nebo vodou.

Stanovení celkové míry rizika

Na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací je stanovena míra rizika - „malé riziko“.

III. ZPŮSOB POUŽITÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI

Tabulka bodového ohodnocení opatření fyzické bezpečnosti v zabezpečených oblastech V a D

Kategorie Vyhrazené, třída II (místnosti č. 11 - 14)

Kategorie Důvěrné, třída II (místnosti č. 15 - 18)

Účel zabezpečené oblasti: ukládání utajovaných informací v úschovném objektu

BEZPEČNOSTNÍ OPATŘENÍ	Typ	Bodové hodnocení
Úschovné objekty	▫ T3	SS1=3
Zámky úschovných objektů	▫ T2	SS2=2
Celkové hodnocení úschovného objektu a jeho zámku	S1=SS1xSS2	**S1=6**
Zabezpečené oblasti	▫ T2	SS3=2
Uzamykací systémy zabezpečené oblasti	▫ T1	SS4=1
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	S2=SS3xSS4	**S2=2**
Objekt	▫ T2	**S3=2**
Kontrola vstupu	▫ T3	SS6=3
Režim návštěv v objektu a) Návštěvy s doprovodem b) Návštěvy bez doprovodu c) Návštěvy bez kontroly	▫ Ad a)	SS7=3

Celkové hodnocení kontroly vstupu	S4=SS6+SS7	**S4=6**
Ostraha	▫ T2	SS8=2
Zařízení elektrické zabezpečovací signalizace	▫ T2	SS91=2
Instalace zařízení elektrické zabezpečovací signalizace	▫ T2	SS92=2
Mezivýsledek (SS 9)		SS9=2
Celkové hodnocení ostrahy a systému EZS	S5=SS8+SS9	**S5=4**
Fyzické bariéry	▫ -	SS10=0
Kontrola vstupu v přístupových bodech fyzické bariéry a) Kontrola je realizována b) Kontrola není realizována	▫ ad -	SS11=0
Namátkové vstupní a výstupní prohlídky a) Prohlídky jsou prováděny b) Prohlídky nejsou prováděny	▫ ad -	SS12=0
Perimetrický detekční systém (PDS)	-	SS13=0
Bezpečnostní osvětlení perimetru	-	SS14=0
Speciální televizní systém na perimetru	-	SS15=0
Celkové hodnocení ochrany perimetru	S6=(SS10xSS11)+SS12+SS13+SS14+SS15	**S6=0**
Celkové bodové ohodnocení	**S1+S2+S3+S4+S5+S6**	**20**

Tab. 2 Bodové ohodnocení opatření fyzické bezpečnosti v zabezpečených oblastech V a D

Přijatá opatření fyzické bezpečnosti pro kategorii zabezpečené oblasti – Vyhrazené a Důvěrné a míru rizika – malé riziko jsou **dostatečná.**

Technická dokumentace fyzické bezpečnosti

Výkresová dokumentace, která obsahuje vyznačení hranice objektu, hranic jednotlivých zabezpečených oblastí a rozmístění technických prostředků určených k ochraně utajovaných informací v objektu a zabezpečených oblastech je v příloze č. 1 tohoto projektu fyzické bezpečnosti.

Dokumentace technických prostředků, která obsahuje výčet použitých technických prostředků a základní údaje o certifikátech a zápisech o posouzení shody, je zpracovaná

formou tabulky v příloze č. 2 tohoto projektu fyzické bezpečnosti. Součástí dokumentace technických prostředků jsou kopie certifikátu Národního bezpečnostního úřadu a zápisy o posouzení shody.

IV. PROVOZNÍ ŘÁD

Pravidla pro režim pohybu osob v objektu

Oprávnění osoby k samostatnému vstupu do objektu schvaluje vedoucí objektu a těmto pracovníkům se vydává oprávnění ke vstupu do objektu (identifikační karta PFBVD, s.r.o.). Přehled oprávněných osob k samostatnému vstupu eviduje vedoucí objektu. Všichni pracovníci, kteří mají oprávnění ke vstupu do objektu, jsou povinni příchod a odchod do zaměstnání provést hlavním vchodem kolem stanoviště ostrahy za použití identifikační karty zaměstnance, kterou přiloží ke čtecímu zařízení u vstupních dveří do objektu. Oprávnění k samostatnému vstupu do objektu se prokazuje přidělenou výše uvedenou identifikační kartou. Oprávnění k vjezdu dopravních prostředků do objektu bez doprovodu není potřeba řešit, neboť do budovy objektu není možný vjezd dopravních prostředků. Návštěvou je každá osoba bez oprávnění k samostatnému vstupu. Návštěva je evidována v knize návštěv, která je umístěna u ostrahy při vchodu do objektu. Za zápis do knihy návštěv odpovídá společně ostraha objektu a navštívený (oprávněná osoba). Evidence návštěv obsahuje identifikační údaje návštěvy (jméno a příjmení, druh a číslo průkazu totožnosti), jméno a příjmení navštíveného a čas příchodu a odchodu návštěvy. Údaje v evidenci je možné zničit po uplynutí jednoho roku od jejich zápisu. Návštěvy se pohybují uvnitř objektu zásadně s doprovodem oprávněné osoby po celou dobu pobytu. Pokud návštěva jde na více pracovišť, musí být prvním doprovodem (oprávněnou osobu) předána další oprávněné osobě, jejíž pracoviště chce navštívit. Zpracovatelé utajovaných informací jsou povinni přijmout taková opatření, aby návštěvy neměly přístup k utajovaným informacím. Při údržbě a opravách zařízení v objektu je objednavatel opravy povinen zabezpečit doprovod pracovníků (návštěvy) oprávněnou osobou po celou dobu jejich činnosti – opravy, výstavby apod. Každý pracovník před odchodem ze své kanceláře prověří vypnutí elektrických spotřebičů a zavření a zajištění oken. Ve stanovené pracovní době, pokud je někdo na pracovišti, je vstup do objektu a zabezpečené oblasti uzavřen a střežení EZS zabezpečené oblasti je vypnuto. V ostatní dobu je vstup do objektu a zabezpečené oblasti uzavřen a uzamčen a EZS je zapnuta. Po skončení pracovní doby je

pracovník ostrahy povinen prověřit uzavření zabezpečených oblastí a zapne střežení EZS v objektu. Vstup do zabezpečené oblasti zamyká ten oprávněný pracovník, který z ní odchází jako poslední, poté co zkontroluje, zda se v ní ještě někdo nenachází.

Pravidla pro režim pohybu osob v zabezpečených oblastech

V zabezpečené oblasti se může samostatně pohybovat jen osoba, které bylo přiděleno oprávnění k samostatnému vstupu (dále jen „uživatel zabezpečené oblasti“). Uživatele zabezpečené oblasti určuje vedoucí objektu, který je za zabezpečenou oblast odpovědný a vede přehled uživatelů zabezpečené oblasti. Uživatel zabezpečené oblasti odpovídá za pohyb osob v zabezpečené oblasti podle stanovených pravidel a za řádné používání technických prostředků. Veškerý vstup do zabezpečené oblasti a výstup z ní je kontrolován uživatelem zabezpečené oblasti. Při vstupu do zabezpečené oblasti, u které jsou technické prostředky aktivovány, požádá uživatel ostrahu objektu o deaktivování EZS příslušné zabezpečené oblasti, zkontroluje neporušenost pečetě vstupních dveří, jejich uzamčení a bezvadný stav dveří. Po vstupu do zabezpečené oblasti zkontroluje neporušenost pečetě na úschovném objektu a případně stav oken na hranici zabezpečené oblasti. Vstup neoprávněné osoby a její pohyb v zabezpečené oblasti je možný pouze s doprovodem uživatele zabezpečené oblasti. Je nezbytné utajované informace před vstupem neoprávněné osoby zabezpečit jejich uložením a uzamčením v úschovném objektu a ukončit nebo přerušit jednání, jehož předmětem jsou utajované informace. Před odchodem ze zabezpečené oblasti, při kterém její uživatel opustí objekt, např. s ukončením pracovním doby, poslední uživatel zabezpečené oblasti zkontroluje předepsané uložení utajovaných informací, ověří uzavření a zajištění oken, vypnutí elektrických a jiných spotřebičů k zamezení vzniku požáru, uzamkne a zapečetí přidělený úschovný objekt a vstupní dveře. Zajistí u ostrahy aktivování EZS pro příslušnou zabezpečenou oblast. Klíče od vstupu do zabezpečené oblasti a klíč od úschovného objektu uloží do schránky, kterou zapečetí a uloží na určeném místě u ostrahy objektu (na schránce je vyznačeno, jaký klíč je zde uložen a seznam osob, které mohou schránku vyzvednout). Přítomnost uživatele v zabezpečené oblasti po pracovní době není možná.

Pravidla pro režim pohybu utajovaných informací v objektu

Utajované informace stupně utajení Vyhrazené a Důvěrné lze zpracovávat nebo s nimi jinak manipulovat pouze v objektu. Zpracovatel nebo ten, kdo manipuluje s utajovanými informacemi je povinen zabránit neoprávněné osobě v přístupu k nim, a proto zejména

neprojednává utajované informace za přítomnosti neoprávněné osoby, nesmí ztratit dispozici nad utajovanou informací a musí ověřit oprávnění osoby, jež se chce seznámit s touto utajovanou informací, k přístupu k utajované informaci. Předání nosiče utajované informace se provádí vždy oproti podpisu přebírající oprávněnou osobou. Pro ukládání utajovaných informací se zásadně užívají úschovné objekty v zabezpečených oblastech. V zabezpečených oblastech V i D se ukládají utajované informace v úschovném objektu typu 3 (Axi Mont CST 5) s uzamykatelným systémem typu 2. Úschovné objekty jsou označeny štítkem s uvedením stupně utajení. Ten, kdo utajovanou informaci zpracoval nebo vyřídil, anebo ji zpracovává či vyřizuje více dnů, ji vždy před skončením pracovní doby (resp. po ukončení práce s utajovanou informací) uloží do úschovného objektu příslušné zabezpečené oblasti.

Přeprava nebo přenášení utajované informace mimo objekt se provádějí za dodržení podmínek a pravidel stanovených vyhláškou č. 529/2005 Sb., o administrativní bezpečnosti a registrech utajovaných informací. Přeprava utajované informace stupně utajení Vyhrazené a Důvěrné se provádí kurýrní službou. Přenášení utajované informace stupně utajení Vyhrazené a Důvěrné provádí osoba, která má přístup k utajované informaci, v zalepené obálce nebo pevném obalu, na kterých je uveden název společnosti a stupeň utajení. Obálka nebo pevný obal se opatří nápisem „V případě nálezu neotvírejte a předejte neprodleně útvaru Policie ČR nebo Národnímu bezpečnostnímu úřadu!“. Utajovanou informaci stupně utajení Důvěrné lze přenášet pouze se souhlasem nadřízeného.

Ničení utajovaných informací provádí oprávněná osoba, která splňuje podmínky k seznamování s utajovanými informace stupně utajení Důvěrné nebo Vyhrazené a to zařízením fyzického ničení nosičů informací (dále jen skartovací stroj). K ničení listinných nosičů utajovaných informací je objekt vybaven skartovacími stroji typu 2 HSM 225.2, které jsou certifikovány NBÚ a označeny štítkem pro stupeň utajení Důvěrné a jsou umístěny v zabezpečených oblastech. Jiný než označený skartovací přístroj je zakázáno používat a skartovacím strojem pro ničení dokumentů příslušného stupně utajení je zakázáno ničit dokumenty vyšších stupňů utajení.

Pokyny pro užívání technických prostředků

Vstup do objektu je zabezpečen plnými dvoukřídlými bezpečnostními protipožárními dveřmi Sherlock typ D2 F5/3 typu 3 s uzamykacím systémem typu 2 v provedení „koule – koule“ (vše certifikováno NBÚ). Dveře jsou v pracovní době trvale uzavřeny

a otevírají se pro vstup i výstup pomocí čipové karty EKV (identifikační karta zaměstnance). V mimopracovní době (od 18:00 do 6:00 hodin) vstupní dveře do objektu zamyká pracovník ostrahy. Vstup do objektu je v pracovní době pod trvalým vizuálním dohledem pracovníka ostrahy. Vjezdová vrata do budovy ani do objektu nejsou. Okna na hranici objektu ve druhém nadzemním podlaží, kde jsou zabezpečené oblasti, jsou umístěna ve výšce více než 5,5 m nad úrovní terénu a jsou opatřena kovovou mříží a nelze k nim tedy jednoduše proniknout. Vstupní dveře do zabezpečené oblasti V ve druhém nadzemním podlaží vlevo od schodiště a vstupní dveře do zabezpečené oblasti D vpravo od schodiště jsou plné dvoukřídlé protipožární bezpečnostní dveře Sherlock typ D2 F5/3 typu 3 s uzamykacím systémem typu 2 v provedení „koule-koule“ (vše certifikováno NBÚ). V pracovní době jsou dveře uzavřeny a otevírají se pro vstup i výstup pomocí čipové karty EKV (karta zaměstnance). V mimopracovní době jsou dveře zabezpečené oblasti uzamčeny a zapečetěny. Za uzavření, uzamčení a zapečetění zabezpečené oblasti odpovídá poslední uživatel zabezpečené oblasti. Zamykatelné mříže na vstupu do zabezpečené oblasti nejsou instalovány.

Úschovné objekty typu 3 (Axi Mont CST 5) splňují podmínky pro ukládání utajovaných informací stupně utajení Vyhrazené a Důvěrné. V době nepřítomnosti uživatele zabezpečené oblasti, kterému byly přiděleny, jsou uzamčeny a v mimopracovní době i zapečetěny. Závadu úschovného objektu či poškození pečetě uživatel zabezpečené oblasti neprodleně oznámí vedoucímu objektu.

Systém EZS, který je instalován k ochraně objektu a zabezpečených oblastí, obsluhuje oprávněná osoba – ostraha budovy. Proškolení pracovníků ostrahy provádí správce EZS (pověřený pracovník ostrahy). Systém EZS typu 2 s instalací 2 je tvořen:

- ústřednou Magellan MG 5050 Paradox Variant typu 2 s instalací typu 2, doplněnou univerzálním IP komunikátorem Paradox Variant PCs300 (oboje na stanovišti ostrahy),
- PIR detektory Pro Plus (476) Paradox Variant typu 2 (kanceláře, chodby),
- magnetickými kontakty 3G-SM-60 Sentek Variant typu 3 (vstup do objektu, vstupy a okna zabezpečených oblastí, ostatní okna objektu a vikýře, průlez na půdu, průlez ke komínu),
- otřesovými detektory Paradox Variant Safe Protector 950 typu 2 (v zabezpečených oblastech pro ochranu utajovaných informací uložených v úschovných objektech),

- tísňovým bezdrátovým tlačítkem MCT201-868 Visonic Ltd. Honeywell typu 2 (ostraha objektu)
- kombinovanými opticko – kouřovými detektory Variant FDR-36-SHR (ve všech prostorách objektu),
- záplavovými detektory Variant WLD38R (v zabezpečených oblastech pro ochranu utajovaných informací uložených v úschovných objektech před zánikem vodou),
- detektorem unikajícího zemního plyn Variant GD-983-NG (v technické místnosti u kotle),
- vnitřní sirénou Variant SA 913 (na stanovišti ostrahy) a venkovní zálohovanou sirénou s blikačem Variant TEKNIM-720WR (pod střechou nad vchodem do objektu).

Pokyny pro používání EZS:

- proškolený pracovník ostrahy aktivuje a deaktivuje EZS v souladu s tímto provozním řádem,
- pracovník ostrahy vyhodnocuje a zapisuje výstupní hlášení technických prostředků EZS a na základě toho provádí úkony podle pravidel pro výkon služby a okamžitě informuje vedoucího objektu a pracovníka s nařízenou objektovou služební pohotovostí,
- správce EZS odpovídá za provozuschopnost EZS, za vedení provozní dokumentace, za kontrolu funkčnosti EZS a k tomu zejména:

1. vede přehled oprávněných osob a přiděluje oprávnění k ovládání EZS oprávněným osobám, oprávněná osoba si zvolí vlastní individuální číselný kód,
2. zajišťuje obměnu hesla periodicky, minimálně po 12 měsících jeho platnosti, a dále je-li heslo vyzrazeno nebo je podezření na jeho vyzrazení; oprávněná osoba je v těchto případech povinna si na jeho pokyn změnit individuální číselný kód a správce EZS o tom provede záznam do provozní knihy EZS,
3. vždy při personální změně z řad uživatelů EZS provádí jeho vyřazení ze systému,
4. zajišťuje neprodleně odstranění oznámených závad EZS,
5. zajišťuje provedení pravidelné kontroly funkčnosti EZS nejméně jednou za 12 měsíců, její zaznamenání do provozního deníku EZS a protokol o provedení pravidelné kontroly funkčnosti zakládá do provozní dokumentace.

Elektronická kontrola vstupu (EKV) je realizována na vstupu do objektu a na vstupech do zabezpečených oblastí V a D. Každý zaměstnanec má jasně stanoveno oprávnění, zda může vstupovat pouze do objektu nebo i do jednotlivých zabezpečených oblastí.

EKV (certifikována NBÚ typ 3) je tvořena:

- systémem kontroly vstupu Anet-Uni Control II napojeným na řídící PC na stanovišti ostrahy
- vnitřními čtečkami Anet Tango Uni na vstupu a výstupu zabezpečených oblastí a na výstupu z objektu
- venkovní čtečkou Anet Uni Reader-OTS na vstupu do objektu

Signalizace od čtecího zařízení EKV je vyvedena na řídící jednotku Anet-Uni Control II a na řídící PC umístěné na stanovišti ostrahy objektu. Po přiložení identifikační karty zaměstnance ke čtečce je provedeno ověřením oprávněnosti jeho vstupu. V případě, že je zaměstnanec oprávněn ke vstupu, provede řídící jednotka EKV uvolnění zajištění příslušných dveří pomocí elektronického ovládání zámku dveří a oprávněný zaměstnanec může vstoupit. Každé ověřování oprávněnosti se zaznamená do databáze systému EKV. Na poplachovou signalizaci narušení EKV reaguje ostraha objektu tím, že okamžitě provede kontrolu objektu a prověří, zda nedošlo k narušení objektu. Zároveň o vzniklé situaci vyrozumí vedoucího objektu. Další postup provádí dle pravidel pro výkon ostrahy.

Další pokyny pro používání EKV:

- oprávněná osoba prokazuje oprávnění k samostatnému vstupu a odchodu do a z objektu a zabezpečených oblastí přiložením bezkontaktní identifikační karty (průkaz zaměstnance) ke čtecímu zařízení.
- správce EKV odpovídá za provozuschopnost EKV, za vedení provozní dokumentace, za kontrolu funkčnosti EKV a k tomu zejména:
  1. dohlíží na řádné používání systému EKV, provozuje řídící jednotku a řídící PC systému EKV a zajišťuje jejich funkčnost,
  2. při zjištění závady systému EKV zajistí nápravu,
  3. nejméně jednou za 12 měsíců provádí kontrolu funkčnosti systému EKV spojenou se zápisem do provozního deníku EKV,
  4. vkládá do systému data oprávněných uživatelů na základě písemného požadavku vedoucího objektu,

5. vyřazuje na základě písemné žádosti vedoucího objektu uživatele, jímž bylo oprávnění ke vstupu zrušeno,
6. vede evidenci oprávněných uživatelů systému EKV, nejpozději do šestého dne každého kalendářního měsíce předá vedoucímu objektu evidenci docházky (příchodů a odchodů) oprávněných uživatelů do objektu včetně evidence přístupů do jednotlivých zabezpečených oblastí.

Závadu, havárii nebo nestandardní stav technických prostředků (např. poškození dveří, mříže, okna, pečetě, závada EZS nebo EKV) neprodleně oznámí pracovník, který je zjistil, vedoucímu objektu nebo podle povahy závady také správci EZS a EKV, kteří zajistí odstranění nežádoucího stavu.

Pravidla pro manipulaci s klíči

Označení klíčů od vstupních dveří objektu, zabezpečených oblastí a úschovných objektů a označení krabiček na klíče, obálek nebo pouzder s duplikáty klíčů:

- klíče od vstupních dveří do objektu jsou označeny štítkem a popisem jejich identifikace,
- klíče od vstupních dveří u zabezpečených oblastí jsou označeny štítkem, na kterém je číslo dveří a nápis „Zabezpečená oblast V" nebo „Zabezpečená oblast D"
- klíče od úschovných objektů v zabezpečených oblastech jsou označeny štítkem, na kterém je číslo místnosti, ve které se úschovný objekt nachází,
- krabička na klíče je označena nápisem „Zabezpečená oblast V" nebo „Zabezpečená oblast D" a číslem dveří zabezpečené oblasti,
- obálky nebo pouzdra s duplikáty klíčů od vstupních dveří u zabezpečených oblastí a od úschovných objektů, které se ukládají u vedoucího objektu, jsou označeny nápisem „Zabezpečená oblast V" nebo „Zabezpečená oblast D" a číslem dveří v zabezpečené oblasti.

Evidenci a přidělování klíčů zajišťuje vedoucí objektu. Evidence se vede podle druhu klíčů a obsahuje údaje o označení klíčů, o celkovém počtu k jednotlivým uzamykacím systémům, včetně počtu dodatečně vyrobených, dále komu byl klíč přidělen, datum a podpis o převzetí klíče a poznámky, např. o výrobě dalšího klíče, o poškození klíče, jeho ztrátě apod. Vedoucí objektu určí osoby oprávněné k vyzvedávání klíčů a k odemykání a zamykání zabezpečené oblasti a úschovného objektu. Tyto určené osoby si vyzvednou klíče od vstupních dveří zabezpečené oblasti před začátkem pracovní doby u ostrahy

objektu. Klíč od úschovného objektu si určená osoba po ukončení pracovní doby nebo při opuštění objektu uzavře do zapečetěné a označené schrány a tu uloží u ostrahy objektu. Za ochranu klíče proti jeho ztrátě nebo zneužití odpovídá každý, komu byl klíč přidělen. Vynášení klíče od vstupních dveří zabezpečené oblasti a od úschovného objektu mimo objekt je zakázáno.

Úschova klíčů se provádí podle těchto pravidel:

- Klíče od vstupních dveří do objektu jsou uloženy u ostrahy objektu. Duplikáty klíčů od vstupních dveří do objektu jsou uloženy u vedoucího objektu. Duplikáty nejsou určeny k běžnému používání, ale vydají se jen při poškození nebo ztrátě používaných klíčů, a to na dobu nezbytně nutnou k výměně zámku.
- Klíč od vstupních dveří zabezpečené oblasti používá určená osoba a ukládá jej v zapečetěné krabičce, kterou uloží u ostrahy objektu. Duplikáty klíčů od vstupních dveří zabezpečené oblasti jsou uloženy v zapečetěné obálce u vedoucího objektu. Duplikáty klíčů nejsou určeny k běžnému používání, ale vydají se jen při poškození nebo ztrátě používaných klíčů, a to na dobu nezbytně nutnou k výměně zámku a v případě krizových situací.
- Klíče od úschovného objektu používá určená osoba, která umožňuje ukládání nebo výdej nosičů utajovaných informací oprávněným osobám a ukládá je v označené zapečetěné krabičce, kterou uloží u ostrahy objektu. Duplikáty klíčů jsou uloženy v zapečetěné obálce, která je umístěna u vedoucího objektu.
- Ztrátu klíče nebo závadu na uzamykacím systému u dveří zabezpečené oblasti nebo u úschovného objektu a schránky, kde jsou klíče ukládány, jejich uživatel neprodleně oznámí vedoucímu objektu, který rozhodne o dočasných opatřeních k ochraně utajovaných informací a zajistí odstranění nežádoucího stavu. Nebude-li klíč nalezen, musí být pro další používání uzamykací systém vyměněn.
- Bezpečnostní karta ke klíči od certifikovaného bezpečnostního uzamykacího systému je uložena u evidence těchto klíčů. Za ochranu bezpečnostní karty před zneužitím odpovídá ten, kdo vede evidenci klíčů a používá ji k zajištění výroby dalších klíčů na základě oprávněného požadavku.

Pravidla pro výkon ostrahy

Objekt je nepřetržitě střežen nejméně jedním pracovníkem ostrahy. Ostrahu objektu včetně správy EZS a EKV zajišťují pracovníci smluvní bezpečnostní ochranné služby. V pracovní době od 6:00 do 18:00 hodin jsou k ostraze určeni dva pracovníci, jeden z nich střeží na stanovišti ostrahy při vstupu do budovy a druhý zajišťuje bezpečnost pracovníků objektu a plní pokyny vedoucího objektu. V mimopracovní době provádí ostrahu v objektu jeden pracovník ostrahy zpravidla na stanovišti ostrahy při vstupu do budovy. Dále je objekt střežen prostřednictvím systému EZS, jehož výstup je vyveden do místnosti ostrahy, která v případě narušení objektu provede zajištění objektu. Informace o vyhlášení poplachu z důvodu narušení nebo vzniku havarijního stavu je zároveň předána na pult centralizované ochrany (dále jen PCO) ve formě předpoplachové informace. Pracovník ostrahy je povinen v případě vyhlášení poplachu provést fyzickou kontrolu objektu pro zjištění příčiny vzniku poplachu a provedení nápravy. Na provedení kontroly a nápravy a následné deaktivace vyhlášeného poplachového stavu má pracovník ostrahy časový interval 5 minut. V případě neprovedení deaktivace poplachu se předpoplachová informace PCO změní na vyhlášení poplachu a na místo je vyslána zásahová skupina, která zajistí případného narušitele. Pracovník ostrahy má dále k dispozici pro případ nouze bezdrátové tísňové tlačítko, které použije v případě jakéhokoliv narušení objektu nebo havarijního stavu, které nemůže odvrátit vlastními silami. Použití tísňového tlačítka je okamžitě ústřednou ESZ i PCO vyhodnoceno jako poplach a na místo je vyslána zásahová skupina, která zajistí narušitele. Současně pracovník PCO informuje vedoucího objektu o vyhlášení poplachu a ten se dostaví na místo do 60 minut od vyrozumění pracovníkem PCO.

Systém kontroly vstupu EKV do objektu je typu 3 a tvoří jej uzamykací systémy v provedení „koule - koule“ v kombinaci s kontrolou vstupu ostrahou a doprovodem návštěv oprávněnými osobami. Pokud není vstup do objektu uzamčen, je neustále pod vizuální kontrolou pracovníka ostrahy objektu.

Ostraha – pracovník bezpečnostní ochranné služby plní zejména tyto úkoly:

- dohlíží na dodržování stanoveného režimu vstupu do objektu,
- obsluhuje EZS a vyhodnocuje výstupní hlášení EZS a EKV,
- kontroluje neporušenost a správnou činnost technických prostředků na hranicích objektu,

- střeží uložené schránky s klíči a manipulaci s nimi povolí jen vedoucímu objektu a držitelům klíče, ostatním zamezí jakoukoliv manipulaci bez přítomnosti vedoucího objektu,
- pokud jsou v objektu dva pracovníci ostrahy, provádí jeden z nich nepravidelné obchůzky uvnitř i vně objektu (nejméně před a po ukončení pracovní doby), při kterých prověřuje neporušenost technických prostředků, druhý pracovník provádí ostrahu na stanovišti ostrahy při vstupu do objektu,
- nahlásí zjištěnou nebo oznámenou závadu, havárii nebo nestandardní stav technických prostředků používaných k ochraně objektu, zajistí nápravu nebo věc oznámí vedoucímu objektu, případně správci EZS a EKV, kteří zajistí odstranění nežádoucího stavu a správce EZS (EKV) v případě závady zaznamená události v provozní dokumentaci EZS (EKV),
- prověřuje příčinu signalizovaného narušení a vzniku havarijní situace objektu nebo konkrétní zabezpečené oblasti prostřednictvím EZS a EKV a k tomu zejména:
  1. provede okamžitou fyzickou kontrolu v místě signalizovaného narušení a prověří stav mechanických zábranných prostředků a prostředků EZS v daném místě,
  2. při narušení objektu a zabezpečené oblasti neoprávněnou osobou provede opatření k jejímu zadržení za případného využití tísňového tlačítka pro přivolání zásahové skupiny, přičemž vyžádá prostřednictvím pracovníka PCO vyrozumění Policie ČR a vedoucího objektu,
  3. nebylo-li zjištěno žádné narušení, provede deaktivaci EZS a provedení deaktivace potvrdí pracovníkovi PCO, přičemž o signalizaci narušení vyrozumí vedoucího objektu následující pracovní den,
  4. při signalizaci vzniku havarijní situace (únik plynu, vznik požáru nebo havárie vody) prověří oblast signalizované havárie a přijme nezbytná opatření k ochraně utajovaných informací a dalšího majetku objektu, případně vyžádá prostřednictvím PCO vyrozumění vedoucího objektu a provedení zásahu Hasičského záchranného sboru.

Při plnění úkolů ostrahy zabezpečených oblastí není pracovník ostrahy oprávněn seznamovat se s utajovanými informacemi.

Zapojení EZS a napojení ústředny EZS na PCO

Objekt společnosti PFBVD, s.r.o., Lounská 236/I je střežen kombinací ostrahy a systému EZS založeném na certifikované ústředně EZS Magellan MG 5050 Paradox Variant typu 2 s instalací typu 2, na kterou jsou vyvedeny výstupy detektorů umístěných uvnitř objektu. Jedná se o hybridní ústřednu s možností zapojení až 32 standardních drátových nebo bezdrátových zón. Všechny komponenty systému, vyjma bezdrátového tísňového tlačítka ostrahy, jsou připojeny metalickým vedením napájení i signalizace umístěným pod omítkou. Ústředna obsahuje čtyři programovatelné výstupy. Jeden z programovatelných výstupů ovládá uzavírání elektromagnetického ventilu na přívodním potrubí zemního plynu ke kotli v případě signalizace úniku zemního plynu detektorem v technické místnosti. Ústředna je doplněna univerzálním IP komunikátorem Paradox Variant PCS300, který umožňuje komunikaci s PCO prostřednictvím sítě Internet. Komunikátor má vestavěný GSM modul a zároveň tak umožňuje v případě výpadku spojení prostřednictvím sítě Internet komunikovat s PCO prostřednictvím GPRS přenosů nebo SMS zpráv. Na pracovišti PCO je instalován IP/GPRS přijímač pro PCO Variant IPR 512, který umožňuje uvedenou komunikaci mezi ústřednou Magellan MG 5050 a PCO.

V. PLÁN ZABEZPEČENÍ OBJEKTU A ZABEZPEČENÉ OBLASTI V KRIZOVÝCH SITUACÍCH

Popis opatření k minimalizaci hrozeb a zranitelností uvedených ve vyhodnocení rizik

Hrozba vyzrazení nebo zneužití utajované informace porušením povinnosti při její ochraně fyzickou osobou, která má přístup k utajované informaci je dostatečně minimalizována vytvořením předepsaných podmínek personální, administrativní a fyzické bezpečnosti a to v takovém rozsahu, aby každá osoba, která má přístup k utajované informaci, s ní mohla v objektu bezpečně pracovat.

Hrozba vyzrazení utajované informace aktivní činností neoprávněné osoby za účelem získání utajované informace, a to pozorováním, odposlouchávání nebo bezprostředním přístupem k utajované informaci je dostatečně minimalizována kombinací bezpečnostních opatření fyzické bezpečnosti, která jsou podrobně stanovena v předchozích částech projektu.

K minimalizaci uvedených hrozeb vyzrazení utajované informace provádí vedoucí objektu pravidelné proškolování podřízených pracovníků k ochraně utajovaných informací a organizuje kontroly dodržování všech povinností, a to v intervalu nejméně jednou v každém kalendářním roce.

Hrozba zániku utajované informace zničením jejího nosiče požárem nebo vodou je minimalizována preventivními opatřeními, jako jsou proškolování protipožárních zásad, vytvoření Požární poplachové směrnice a Požárního evakuačního plánu budovy a jejich dodržováním ve všech prostorách objektu a umístěním úschovných objektů tak, aby případná havárie vodovodního systému neohrozila nosiče utajovaných informací. Za minimalizaci hrozby zániku utajované informace proškolováním protipožárních zásad všech zaměstnanců, a to nejméně jednou v každém kalendářním roce, zodpovídá pověřený pracovník smluvní bezpečnostní ochranné služby. Tento pracovník zároveň vytváří, vede a případně aktualizuje Požární poplachové směrnice a Požární evakuační plán budovy v souladu s příslušnou legislativní úpravou. Zároveň jsou jako součást EZS nainstalovány následující bezpečnostní prvky:

- Detektor hořlavých plynů umístěný v prostoru místnosti č. 6 pro detekci úniku zemního plynu vzniklého poruchou plynového kotle nebo přívodního potrubí.

  Po vyslání poplachového signálu detektoru hořlavých plynů ústředně EZS začne ústředna signalizovat nebezpečí úniku plynu v místnosti č. 6, neprodleně provede uzavření plynového potrubí prostřednictvím elektromagnetického ventilu a deaktivuje střežení magnetickými kontakty na rámu okna v místnosti č. 6 pro potřebu odvětrání plynu z místnosti.
- Kombinované opticko – kouřové a teplotní detektory umístěné ve všech místnostech objektu pro detekci zvýšené teploty a vzniku kouřových zplodin při vzniku požáru.

  Po vyslání poplachového signálu jednoho z detektorů v zabezpečených oblastech ústředně EZS ústředna začne signalizovat vznik požáru v dané zabezpečené oblasti a deaktivuje střežení zabezpečené oblasti pro potřebu uhašení vzniklého požáru a případného odvětrání prostoru zabezpečené oblasti.
- Záplavové detektory umístěné u úschovných objektů v zabezpečených oblastech pro ochranu uložených nosičů utajovaných informací.

Po vyslání poplachového signálu jednoho z detektorů v zabezpečených oblastech ústředně EZS začne ústředna signalizovat vznik nebezpečí zničení vodou v dané

zabezpečené oblasti a deaktivuje střežení zabezpečené oblasti pro potřebu ochránění úschovného objektu.

Pokyny pro ochranu utajovaných informací v případě vzniku mimořádné situace

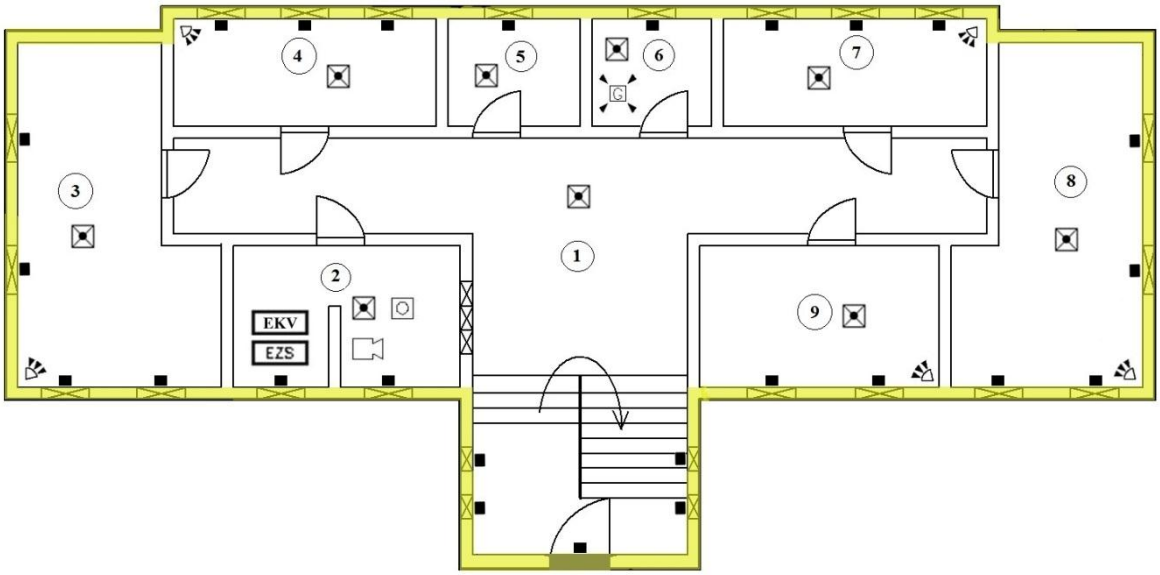
Opatření pro minimalizaci hrozby vyzrazení nebo zneužití utajované informace porušením povinnosti při ochraně utajované informace fyzickou osobou, která má přístup k utajované informaci jsou taková, že každý pracovník, který zjistil porušení povinností při ochraně utajovaných informací, je podle zákona č. 412/2005 Sb. povinen neprodleně toto oznámit vedoucímu objektu, který zajistí ohlášení zjištěného skutku na NBÚ a přijme opatření k odstranění příčin a nepříznivých následků.

Opatření pro minimalizaci hrozby vyzrazení utajované informace aktivní činností neoprávněné osoby za účelem získání utajované informace, a to pozorováním, odposlouchávánim nebo bezprostředním přístupem k utajované informaci jsou taková, že při zjištění jakékoliv aktivity neoprávněné osoby směřující k získání utajované informace, která se v objektu nachází, je každý pracovník povinen tomuto zabránit a neprodleně o tomto informovat vedoucího objektu, který rozhodne o dalších opatřeních. Při zjištění násilného vniknutí do objektu je každý pracovník, který vniknutí zjistil, povinen informovat o tom vedoucího objektu a uživatele zabezpečené oblasti a pokud možno zabránit dalšímu úniku utajovaných informací, které dosud nebyly vyzrazeny.

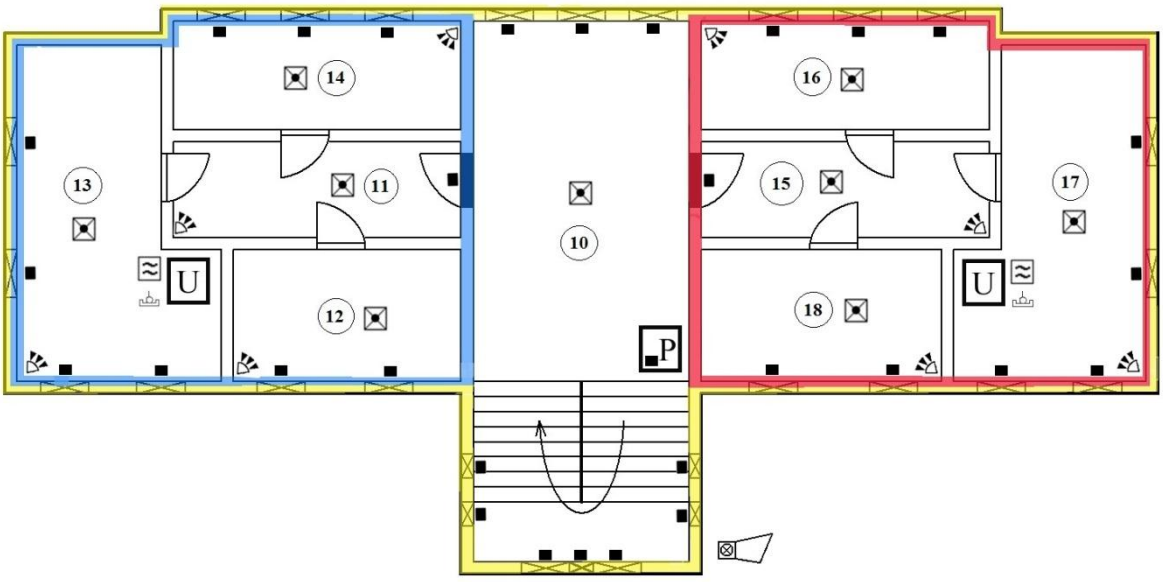
Hrozba zániku utajované informace zničením jejího nosiče požárem nebo vodou je minimalizována v závislosti na konkrétním vývoji mimořádné situace provedením přemístění utajovaných informací majících archivní hodnotu do bezpečí. K tomu účelu určení pracovníci přistaví služební vozidlo před budovu a naloží do něho evakuované utajované informace, které následně přepraví do zabezpečené oblasti buďto některému z útvarů Policie ČR nebo na NBÚ. Neumožní-li situace žádnou evakuaci, zajistí určení pracovníci v rámci daných možností, aby při likvidaci mimořádné situace a po ní, nedocházelo k vyzrazení utajovaných informací. Při havárii rozvodů vody a střešní konstrukce je nutné zamezit vniknutí vody do úschovných objektů nebo dočasně přemístit utajované informace mimo zasažený prostor a zajistit jejich bezpečnost. Dočasné přemístění utajovaných informací je třeba provést podle konkrétní situace buď v rámci objektu nebo mimo objekt do zabezpečené oblasti buďto některému z útvarů Policie ČR nebo na NBÚ.

Příloha č. 1 projektu fyzické bezpečnosti:

Schéma objektu s vyznačením hranice objektu, zabezpečených oblastí a prvků EZS



Obr. 10 Vyznačení hranice objektu a prvků zabezpečení v 1. nadzemním podlaží



Obr. 11 Vyznačení hranice objektu, zabezpečených oblastí a prvků zabezpečení ve 2. nadzemním podlaží

Legenda:

- vyznačení hranice objektu
- vyznačení hranice zabezpečené oblasti V
- vyznačení hranice zabezpečené oblasti D
- označení místnosti
- ústředna EZS
- řídící PC a jednotka EKV
- kombinovaný opticko – kouřový a teplotní detektor
- bezdrátové tísňové tlačítko ostrahy
- magnetický kontakt dveří a oken
- PIR detektor
- záplavový detektor
- otřesový detektor
- detektor úniku zemního plynu
- vnitřní siréna
- venkovní siréna s blikačem
- vstupní dveře do objektu a zabezpečených oblastí s magnetickým kontaktem a čtečkami identifikačních karet EKV
- úschovný objekt
- průlez na půdu s magnetickým kontaktem

Příloha č. 2 projektu fyzické bezpečnosti

Přehled použitých technických prostředků

Poř. číslo	Název technického prostředku	Počet	Certifikát č.	Umístění v zabezpečené oblasti nebo v objektu
1	Ústředna EZS Paradox Variant Magellan MG 5050	1	T1014/2010	Stanoviště ostrahy – místnost č. 2
2	Detektor otevření (magnetický kontakt) Sentek Variant 3G-SM-60	63	T1189/2008	Vstupní dveře, okna objektu a zabezpečených oblastí V a D, průlez na půdu, vikýře, průlez ke komínu
3	Detektor pohybu PIR Paradox Variant Pro Plus (476)	13	T1012/2010	Kanceláře objektu a místnosti zabezpečených oblastí V a D
4	Úschovný objekt Axi Mont CST 5	2	T0092/2009	Zabezpečená oblast V a D – kancelář 13 a 17
5	Otřesový detektor Paradox Variant Safe Protector 950	2	T1038/2009	Zabezpečená oblast V a D – kancelář 13 a 17
6	Bezpečnostní protipožární dveře Sherlock typ D2 F5/3	3	T0113/2010	Vstup do objektu a zabezpečených oblastí V a D
7	Systém kontroly vstupů – jednotka EKV Anet-Uni Control II	1	T3007/2010	Stanoviště ostrahy – místnost č. 2
8	Systém kontroly vstupů – vnitřní čtečka Anet Tango Uni	5	T3007/2010	Vstup a výstup zabezpečených oblastí V a D, výstup z objektu
9	Systém kontroly vstupů – venkovní čtečka Anet Uni Reader-OTS	1	T3007/2010	Vstup do objektu
10	Bezdrátové tísňové tlačítko ostrahy Visonic Ltd. Honeywell MCT201-868	1	T1103/2010	Ostraha objektu
11	Kombinovaný opticko – kouřový a teplotní detektor Variant FDR-36-SHR	18	-	Všechny místnosti objektu
12	Záplavový detektor Variant WLD38R	2	-	Zabezpečená oblast V a D – ochrana úschovných objektů
13	Detektor unikajícího plynu Variant GD-983-NG	1	-	Technická místnost – místnost č. 6

14	Vnitřní siréna Variant SA 913	1	-	Stanoviště ostrahy – místnost č. 2
15	Venkovní siréna s blikačem Variant TEKNIM-720WR	1	-	Vně objektu – průčelí budovy pod střechou

Tab. 3 Přehled použitých technických prostředků

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: T0113/2010

Bezpečnostní protipožární dveře SHERLOCK typ D2 F5/3
Bezpečnostní protipožární dveře SHERLOCK typ D2 F5/3 V
(Název a typové označení technického prostředku)

Výrobce: SHERLOCK, s.r.o.
Sídlo: Ľubovianska 7 - Bratislava, SR IČ: -
Držitel: SHERLOCK bezpečnostní dveře, s.r.o.
Sídlo: U Elektry 203/8 198 00 Praha 9 - Hloubětín IČ: 29018340

Tento certifikát potvrzuje ověření způsobilosti technického prostředku typu:
3
Bodové hodnocení technického prostředku podle přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků:
SS3=3, SS4=2

Platnost certifikátu do: 7.8.2011
Datum vydání certifikátu: 22.12.2010

Náměstek ředitele
Národního bezpečnostního úřadu
Jan Novák
012896

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
4

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

KOPIE

Obr. 12 Certifikát technického prostředku (zdroj: www.sherlock.cz)

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

PŘÍLOHU K CERTIFIKÁTU

Identifikační číslo: T0113/2010
Příloha číslo: 1

Bezpečnostní protipožární dveře SHERLOCK typ D2 F5/3, otevírané směrem do chráněného prostoru a Bezpečnostní protipožární dveře SHERLOCK typ D2 F5/3 V, otevírané směrem ven z chráněného prostoru, šířky 1250 mm, 1300 mm, 1400 mm, 1450 mm, 1500 mm, 1600 mm, 1650 mm, 1700 mm, 1800 mm, výšky 1970 mm, 2000 mm, 2100 mm, 2200 mm. Přehled komponent, kterými je možno certifikovaný výrobek osazovat, je uveden v příloze certifikačního protokolu C 158/2008, vydaného certifikačním orgánem č. 3025 společnosti TREZOR TEST s r.o. Tento přehled je k dispozici u držitele certifikátu. Výrobek je vyráběn v režimu akreditované certifikace od 7.8.2008.

Platnost certifikátu do: 7.8.2011
Datum vydání certifikátu: 22.12.2010

Otisk úředního razítka

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Náměstek ředitele
Národního bezpečnostního úřadu

Jan Novák

Certifikát a přílohu lze reprodukovat pouze společně.

KOPIE

Obr. 13 Příloha certifikátu technického prostředku

(zdroj: www.sherlock.cz)

ZÁVĚR

Cílem této diplomové práce bylo vytvořit studijní materiál pro potřeby všech, kteří se chtějí seznámit s problematikou ochrany utajovaných informací, bezpečnostního posuzování a vytváření projektů fyzické bezpečnosti. Práce je rozdělena na dvě základní části, na část teoretickou a část praktickou.

V teoretické části byl zpracován přehled legislativní úpravy ochrany utajovaných informací v rámci EU a NATO a ČR se zaměřením na seznámení se a vysvětlení z mého pohledu nejdůležitějších částí zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti a prováděcích právních předpisů k tomuto zákonu. Velká část pak byla věnována problematice fyzické bezpečnosti. Další kapitola teoretické části byla věnována problematice bezpečnostního posuzování, především vysvětlení pojmu bezpečnostní posuzování, jako první části návrhu poplachového zabezpečovacího a tísňového systému, definování rozsahu bezpečnostního posuzování a stanovení nezbytných částí a struktury procesu bezpečnostního posuzování.

V praktické části jsou pak využity poznatky získané při studiu problematiky bezpečnostního posuzování. Na základě těchto poznatků bylo vypracováno bezpečnostní posouzení konkrétního objektu, které bylo doplněno upřesňujícím popisem a fotodokumentací posuzovaného objektu. Druhá kapitola praktické části je věnována problematice vytváření projektu fyzické bezpečnosti. Podrobně je vysvětlena legislativní úprava problematiky vytváření projektů fyzické bezpečnosti. V závěrečné části byl vypracován návrh projektu fyzické bezpečnosti objektu, u kterého bylo provedeno bezpečnostní posouzení. Na základě provedeného bezpečnostního posouzení objektu s přihlédnutím k podmínkám ochrany utajovaných informací byl vytvořen imaginární poplachový zabezpečovací a tísňový systém posuzovaného objektu, včetně jeho napojení na pult centralizované ochrany prostřednictvím internetového připojení se zálohovou komunikací prostřednictvím GSM přenosů. Do systému zabezpečení byly zapracovány nadstandartní požadavky ve formě provozu poplachového zabezpečovacího a tísňového systému a systému elektronické kontroly vstupu s exportem údajů o vstupech pro potřeby evidence docházky zaměstnanců, který zabezpečují oprávnění pracovníci (správci) bezpečnostní agentury. Dále jsou systémem sledovány havarijní stavy – vznik požáru, únik zemního plynu a zaplavení trezorů s utajovanými informacemi vodou při havárii střešní konstrukce. Trezory s utajovanými informacemi jsou zároveň střeženy použitím

otřesového detektoru začleněného do systému. Ostraha objektu, tvořená nejméně jedním pracovníkem bezpečnostní agentury, je pro případ nouze vybavena bezdrátovým tísňovým tlačítkem. Uvedený poplachový zabezpečovací a tísňový systém je zapracován do projektu fyzické bezpečnosti jako jeden z prvků ochrany utajovaných informací v daném objektu.

Obecně není příliš jednoduché setkat se s dokumentací o bezpečnostním posouzení skutečných objektů a ještě menší je pravděpodobnost setkání se s projektem fyzické bezpečnosti skutečného objektu, proto by tato práce mohla být vhodnou pomůckou například pro začínající bezpečnostní pracovníky a studenty bezpečnostních oborů.

CONCLUSION

This thesis intends to provide study materials for everyone interested in security of classified information, security evaluation and designing of physical security projects. The thesis is divided into two parts – theoretical and practical.

Theoretical part presents the outline of the legislation on security of classified information in the EU, NATO and the Czech Republic and concentrates on introduction and explanation of those parts of the Protection of Classified Information and Security Qualification act No 412/2005COL and respective implementing regulations which I consider the most important. Big part is about the issue of physical security. Next chapter of the theoretical part focuses on security evaluation, especially on explanation what security evaluation as the first step when designing an intruder and hold-up alarm system really means, on defining the extent of security evaluation and specification of essential parts and structure of the security evaluation process.

The knowledge based on security evaluation studies is used in the practical part. This knowledge helped me to create security evaluation of a particular building, including a detailed description and photos of the evaluated building. The second chapter is about designing a physical security project. It explains in detail the legislation on designing physical security projects. The end of this part presents the design of a physical security project for the building, where security evaluation was done. This security evaluation of the building together with conditions concerning security of classified information served as a basis for creation of a mock intruder and hold-up alarm system for the evaluated building, including its connection to the alarm receiving center via Internet connection with back-up communication using GSM system. Special requirements such as operation of an intruder and hold-up alarm system and electronic check of entry with export of data concerning entry of employees to file their attendance were incorporated into the security system and are operated by authorized employees (administrators) from a security agency. The system also monitors emergency situations – fire, gas leak and when vaults with classified information are flooded due to a breakdown of the roof. The vaults containing classified information are also protected with a vibration detector integrated into the system. Building security, which consists of at least one security agency employee, has at their disposal a wireless emergency button for the case of emergency. This intruder and hold-up alarm system is incorporated into the physical

security project as one of the elements connected with security of classified information in a particular building.

In general, it is not easy to get hold of materials concerning security evaluation of real buildings and premises and even more difficult it is to get hold of a physical security project of a real building. Therefore, this thesis could be useful for example for new security employees and students specialized in security studies.

SEZNAM POUŽITÉ LITERATURY

Publikace:

[1] ČÍRTKOVÁ, Ludmila. *Kriminální psychologie*. Vyd. 1. Praha : Eurounion, 1998. 255 s. ISBN 80-85858-70-3.

[2] CHMELÍK, Jan a kol., *Rukověť kriminalistiky*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2005. 536 s. ISBN 80-86898-36-9

[3] IVANKA, Ján. *Systemizace bezpečnostního průmyslu I.* Vyd. 3. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 123 s. ISBN 978-80-7318-850-4.

[4] IVANKA, Ján. *Systemizace bezpečnostního průmyslu II*. Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 86 s. ISBN 978-80-7318-863-4.

[5] KARÁSEK, Tomáš. *European Union in a New* Security *Environment / edited by Tomáš Karásek*. Vydání 1. Praha : Univerzita Karlova, 2008. 130 s. ISBN 978-80-7378-075-3.

[6] KINDL, Jiří. *Projektování bezpečnostních systémů I. díl.* Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2004. 134 s. ISBN 80-7318-165-7.

[7] KŘEČEK, Stanislav a kol. *Příručka zabezpečovací techniky*. Vyd. 2. Blatná : [s.n.], 2003. 351 s. ISBN 80-902938-2-4.

[8] LAUCKÝ, Vladimír. *Bezpečnostní futurologie*. Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2007. 93 s. ISBN 978-80-7318-560-2.

[9] LAUCKÝ, Vladimír. *Speciální bezpečnostní technologie.* Vyd. 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 223 s. ISBN 978-80-7318-762-0.

[10] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I.* Vyd. 2. Zlín : Univerzita Tomáše Bati ve Zlíně, 2004. 64 s. ISBN 80-7318-194-0.

[11] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II.* Vyd. 2. Zlín : Univerzita Tomáše Bati ve Zlíně, 2007. 123 s. ISBN 978-80-7318-631-9.

[12] MUSIL, Jan; KONRÁD, Zdeněk; SUCHÁNEK, Jaroslav. *Kriminalistika*. Vyd. 2. Praha : C.H.Beck, 2004. 582 s. ISBN 80-7179-878-9.

[13] UHLÁŘ, Jan. *Technická ochrana objektů I. díl - Mechanické zábranné systémy*. Vyd. 1. Praha : Policejní akademie ČR, 2000. 150 s. ISBN 80-7251-046-0.

[14] UHLÁŘ, Jan. *Technická ochrana objektů II. díl - Elektrické zabezpečovací systémy*. Vyd. 1. Praha : Policejní akademie ČR, 2001. 205 s. ISBN 80-7251-076-2.

[15] UHLÁŘ, Jan. *Technická ochrana objektů III. díl – Ostatní zabezpečovací systémy*. Vyd. 1. Praha : Policejní akademie ČR, 2006. 246 s. ISBN 80-7251-235-8.

Legislativa, normy:

[1] Česká republika. Nařízení vlády ze dne 7. prosince 2005, kterým se stanoví seznam utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, 179, 522, s. 9950 - 9977. ISSN 1211-1244.

[2] Česká republika. Nařízení vlády ze dne 9. června 2008, kterým se mění nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In *Sbírka zákonů, Česká republika*. 2008, 77, 240, s. 3590 - 3592. ISSN 1211-1244.

[3] Česká republika. Vyhláška ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů, Česká republika*. 2005, 179, 528, s. 10079 - 10115. ISSN 1211-1244.

[4] Česká republika. Vyhláška ze dne 14. prosince 2005 o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, 179, 525, s. 10009 - 10014. ISSN 1211-1244.

[5] Česká republika. Vyhláška ze dne 14. prosince 2005 o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti). In *Sbírka zákonů, Česká republika*. 2005, 179, 526, s. 10015 - 10044. ISSN 1211-1244.

[6] Česká republika. Vyhláška ze dne 14. prosince 2005 o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti). In *Sbírka zákonů, Česká republika*. 2005, 179, 527, s. 10045 - 10078. ISSN 1211-1244.

[7] Česká republika. Vyhláška ze dne 14. prosince 2005 o zajištění kryptografické ochrany utajovaných informací. In *Sbírka zákonů, Česká republika*. 2005, 179, 524, s. 9994 - 10008. ISSN 1211-1244.

[8] Česká republika. Vyhláška ze dne 14. února 2008, kterou se mění vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. In *Sbírka zákonů, Česká republika*. 2008, 16, 55, s. 842 - 843. ISSN 1211-1244.

[9] Česká republika. Vyhláška ze dne 25. ledna 2008, kterou se mění vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In *Sbírka zákonů, Česká republika*. 2008, 9, 19, s. 454 - 459. ISSN 1211-1244.

[10] Česká republika. Vyhláška ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. In *Sbírka zákonů, Česká republika*. 2005, 179, 523, s. 9978 - 9993. ISSN 1211-1244.

[11] Česká republika. Vyhláška ze dne 7. ledna 2008, kterou se mění vyhláška č. 526/2005 Sb., o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti). In *Sbírka zákonů, Česká republika*. 2008, 5, 11, s. 386 - 388. ISSN 1211-1244.

[12] Česká republika. Zákon ze dne 11. června 1998 o ochraně utajovaných skutečností a o změně některých zákonů. In *Sbírka zákonů, Česká republika*. 1998, 52, 148, s. 6650 - 6672.

[13] Česká republika. Zákon ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In *Sbírka zákonů, Česká republika*. 2005, 143, 412, s. 7526 - 7576. ISSN 1211-1244.

[14] Česká republika. Zákon ze dne 21. září 2005 o změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti. In *Sbírka zákonů, Česká republika*. 2005, 143, 413, s. 7577 - 7596. ISSN 1211-1244.

[15] Česká republika. Zákon ze dne 8. ledna 2009 trestní zákoník. In *Sbírka zákonů, Česká republika*. 2009, 11, 40, s. 354 - 464. ISSN 1211-1244.

[16] ČSN CLC/TS 50131-7. *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 7: Pokyny pro aplikace*. Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009, 44 s.

[17] ČSN EN 50131-1. *Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky*. ed 2. Praha : Český normalizační institut, 2007, 40 s.

[18] ČSN EN 50133-1. *Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 1: Systémové požadavky*. Praha : Český normalizační institut, 2001, 28 s.

[19] ČSN EN 50133-7. *Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 7: Pokyny pro aplikace*. Praha : Český normalizační institut, 2000, 16 s.

[20] Komise Evropské unie. 2001/844/ES, ESUO, Euratom: Rozhodnutí Komise ze dne 29. listopadu 2001, kterým se mění její jednací řád (oznámeno pod číslem K(2001) 3031). In *Úřední věstník Evropské unie.* 2001, L 317, s. 1 – 55.

[21] Komise Evropské unie. 2005/94/ES, Euratom: Rozhodnutí Komise ze dne 3. února 2005, kterým se mění rozhodnutí 2001/844/ES, ESUO, Euratom. In *Úřední věstník Evropské unie.* 2005, L 31, s. 66 – 68.

[22] Komise Evropské unie. 2006/548/ES, Euratom: Rozhodnutí Komise ze dne 2. srpna 2006, kterým se mění rozhodnutí 2001/844/ES, ESUO, Euratom. In *Úřední věstník Evropské unie.* 2006, L 215, s. 38 – 43.

[23] Komise Evropské unie. 2006/70/ES, Euratom: Rozhodnutí Komise ze dne 31. ledna 2006, kterým se mění rozhodnutí 2001/844/ES, ESUO, Euratom. In *Úřední věstník Evropské unie.* 2006, L 34, s. 32 – 33.

[24] North Atlantic Council. AC/35-D/2000-REV6: Directive on Personnel Security, Note by the Chairman. *NATO Security Committee.* 2009. 17 s.

[25] North Atlantic Council. AC/35-D/2001-REV2: Directive on Physical Security, Note by the Chairman. *NATO Security Committee.* 2008. 13 s.

[26] North Atlantic Council. AC/35-D/2002-REV3: Directive on the Security of Information, Note by the Chairman. *NATO Security Committee.* 2006. 65 s.

[27] North Atlantic Council. AC/35-D/2003-REV4: Directive on Industrial Security, Note by the Chairman. *NATO Security Committee.* 2009. 68 s.

[28] North Atlantic Council. AC/35-D/2004-REV2: Primary Directive on INFOSEC, Note by the Chairman. *NATO Security Committee.* 2010. 30 s.

[29] North Atlantic Council. AC/35-D/2005-REV2: INFOSEC Management Directive for CIS, Note by the Chairman. *NATO Security Committee.* 2010. 31 s.

[30] North Atlantic Council. C-M(2002)49: Security within the North Atlantic Treaty Organisation (NATO), Note by the Secretary General. *NATO.* 2002. 60 s.

[31] North Atlantic Council. C-M(2002)49-COR3: Security within the North Atlantic Treaty Organisation, Corrigendum to C-M(2002)49 dated 17 June 2002 Amendment 3. *NATO.* 2006. 42 s.

[31] North Atlantic Council. C-M(2002)49-COR6: Security within the North Atlantic Treaty Organisation, Corrigendum to C-M(2002)49 dated 17 June 2002 Amendment 6. *NATO.* 2008. 20 s.

[33] North Atlantic Council. C-M(2002)49-COR7: Security within the North Atlantic Treaty Organisation, Corrigendum to C-M(2002)49 dated 17 June 2002 Amendment 7. *NATO.* 2009. 11 s.

[34] North Atlantic Council. C-M(2002)49-COR8: Security within the North Atlantic Treaty Organisation, Corrigendum to C-M(2002)49 dated 17 June 2002 Amendment 8. *NATO.* 2010. 22 s.

[35] Podniková norma PNJ 131. *Poplachové systémy – Pravidla zřizování poplachových zabezpečovacích a tísňových systémů objektů (PZTS)*. Jablotron Alarms, a.s., 2007, 20 s.

[36] Rada Evropské unie. 2001/264/ES: Rozhodnutí rady ze dne 19. března 2001, kterým se přijímají bezpečnostní předpisy Rady. In *Úřední věstník Evropské unie.* 2001, L 101, s. 1 – 66.

[37] Rada Evropské unie. 2004/194/ES: Rozhodnutí Rady ze dne 10. února 2004, kterým se mění rozhodnutí 2001/264/ES, kterým se přijímají bezpečnostní předpisy Rady. In *Úřední věstník Evropské unie.* 2004, L 63, s. 48 – 52.

[38] Rada Evropské unie. 2005/571/ES: Rozhodnutí Rady ze dne 12. července 2005, kterým se mění rozhodnutí 2001/264/ES, kterým se přijímají bezpečnostní předpisy Rady. In *Úřední věstník Evropské unie.* 2005, L 193, s. 31 – 36.

[39] Rada Evropské unie. 2005/952/ES: Rozhodnutí Rady ze dne 20. prosince 2005, kterým se mění rozhodnutí 2001/264/ES, kterým se přijímají bezpečnostní předpisy Rady. In *Úřední věstník Evropské unie.* 2005, L 346, s. 18 – 23.

[40] Rada Evropské unie. 2007/438/ES: Rozhodnutí Rady ze dne 18. června 2007, kterým se mění rozhodnutí 2001/264/ES, kterým se přijímají bezpečnostní předpisy Rady. In *Úřední věstník Evropské unie.* 2007, L 164, s. 24 – 29.

[41] *Statistický výkaz č. 1 - kriminalita za období od 1.1.2011 do 31.3.2011*. Praha : Policejní prezidium ČR, 2011.

Internetové zdroje:

[1] Google Maps – http://maps.google.com

[2] Jablotron Alarms, a.s. – http://www.jablotron.cz

[3] Národní bezpečnostní úřad – http://www.nbu.cz/cs

[4] Policie ČR – http://www.policie.cz

[5] Variant plus – http://www.variant.cz

[6] Sherlock – http://www.sherlock.cz

SEZNAM CITACÍ

[1] IVANKA, Ján. *Systemizace bezpečnostního průmyslu II*. Vydání 1. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 86 s. ISBN 978-80-7318-863-4.

[2] MUSIL, Jan; KONRÁD, Zdeněk; SUCHÁNEK, Jaroslav. *Kriminalistika*. Vydání 2. Praha : C.H.Beck, 2004. 582 s. ISBN 80-7179-878-9.

[3] KŘEČEK, Stanislav a kol. *Příručka zabezpečovací techniky*. Vydání 2. Blatná : Blatenská tiskárna, s.r.o., 2003. 351 s. ISBN 80-902938-2-4.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČR - Česká republika

ČSN CLC/TS - Technická specifikace CENELEC převzatá do národního systému norem ČR

ČSN EN - Evropská norma přejatá do národního systému norem ČR

EKV - Elektronická kontrola vstupu

EU - European Union – Evropská unie

EZS - Elektrická zabezpečovací signalizace (systém)

GPRS - General Packet Radio Service – mobilní datová služba

GSM - Global Systém for Mobile communications – globální systém pro mobilní komunikace

I&HAS - Intrusion and hold-up alarm systém – poplachový zabezpečovací a tísňový systém

IP - Internet protokol - protokol pro přenos dat

LED - Light Emitting Diode – světloemitující dioda

NATO - North Atlantic Treaty Organization – Severoatlantická aliance

NBÚ - Národní bezpečnostní úřad

PC - Personal Computer – osobní počítač

PCO - Pult centralizované ochrany

PIR - Passive Infrared – pasivní infračervený (detektor pohybu)

PNJ - Podniková norma Jablotron Alarms, a.s.

Sb. - Sbírka zákonů

SMS - Short Message Service – služba krátkých textových zpráv

StB - Státní bezpečnost

TNI - Technická normalizační informace

SEZNAM OBRÁZKŮ

SEZNAM TABULEK