Přírodovědecká fakulta Jihočeské univerzity

Bakalářská práce:

Vytvoření projektu fyzického zabezpečení objektu

Vypracoval: Bohuslav Dunovský

Školitel: Ing. Petr Šedivý

České Budějovice 2012

Bibliografické údaje

Dunovský B., 2012: Vytvoření projektu fyzického zabezpečení objektu

[Project of physical building security. Bc.. Thesis, in Czech.] – 50 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Anotace:
Úkolem této práce je provést analýzu vybrané části objektu v sídle firmy (název firmy je fiktivní), která se zabývá vývojem materiálu pro výrobu bankovek. Dokumentace části technologických postupů a receptur podléhá stupni utajení Důvěrné. Z těchto důvodů je nutné vytvořit v sídle firmy zabezpečený objekt a zabezpečenou oblast v souladu se zákonem 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, včetně pozdějších novelizací a souvisejících vyhlášek k ukládání, nakládání a tvorbě utajovaných informací do stupně utajení Důvěrné.

Abstract:
The aim of this work is to analyze the selected parts of the object in the company's headquarters (the company´s name is fictitious) which deals with the development of materials for the production of banknotes. The documentation of processes and formulas are subjected to the classification Confidential. For these reasons, it is necessary to create a secure headquarters' building and a secure area in accordance with law 412/2005 Coll., about protection of classified information and security capacity, including subsequent amendments and regulations related to storage, handling classified information and the creation of the classification Confidential.

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury. Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

Datum:

Podpis:

Poděkování:
Rád bych poděkoval panu ing. Petru Šedivému za cenné rady a pomoc při psaní bakalářské práce.

Obsah

1 Úvod

Zabezpečení objektu se v dnešní době stává předmětem zájmu jak fyzických, tak právnických osob s cílem ochránit majetek, budovy či duševní vlastnictví v nich uložené. K zabezpečení objektu je potřeba použít prostředky fyzického zabezpečení. V případě, že se v budově nachází materiály podléhající stupni utajení, je nutné při zabezpečení postupovat podle platných právních předpisů a norem, a to především podle zákona č. 412/2005, o ochraně utajovaných informací a bezpečnostní způsobilosti a s ním souvisejících vyhlášek. Dále i podle novely vyhlášky 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.

Cílem bakalářské práce je vytvořit projekt fyzického zabezpečení zabezpečeného objektu a zabezpečené oblasti firmy Security Printing (název je fiktivní) vyvíjející materiál používaný při výrobě bankovek. Při vývoji materiálu používá výrobní receptury, které podléhají stupni utajení Vyhrazené a Důvěrné. Zabezpečení proběhne technickými prostředky, jež jsou v souladu se seznamem certifikovaných prostředků NBÚ.

Fiktivní zabezpečená oblast byla umístěna do reálných kancelářských prostor v budově A, v areálu Jihočeské univerzity v Českých Budějovicích, ve kterých se v současné době nalézá studijní oddělení Přírodovědecké fakulty JČU.

Při zpracování projektu fyzické bezpečnosti objektu se postupuje podle struktury uvedené v novele vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. Nejprve se provede vyhodnocení hrozeb, které mohou pro daný objekt nastat a vést k neoprávněnému nakládání, odcizení, poškození či znehodnocení uložených dokumentů. Poté určíme kategorie zabezpečené oblasti a zabezpečeného objektu a jejich tříd. Podle struktury uvedené v novele vyhlášky č. 528/2005 Sb., ve znění vyhlášky č. 454/2011 Sb.. Bakalářská práce obsahuje popis způsobu používání opatření fyzické bezpečnosti. V této části se nachází i tabulka bodového ohodnocení opatření fyzické bezpečnosti. Dále následuje provozní řád a plán zabezpečení objektu a oblasti v krizových situacích.

2 Vyhodnocení rizik

2.1 Specifikace aktiv

Společnost Security Printing a.s. přichází do styku s utajovanými informacemi (UI), stupně utajení (SU) Vyhrazené a Důvěrné. Tyto informace u společnosti vznikají nebo jsou jí poskytovány. Jedná se zejména o speciální charakteristiky a receptury materiálů používané při výrobě bankovek. Dále jsou mezi UI zařazeny technické specifikace materiálů a polotvarů pro výrobu bankovek obsahující ochranné prvky. UI ve firmě je také dokumentace systému komplexního zabezpečení objektu, včetně mechanických zábran a kamerových systémů, kde se vyrábějí bankovky, doklady nebo ceniny. Rozsah přístupu společnosti k UI je vymezen podle § 20 odstavce 1 písmena a) i b) zákona č.412/2005 o ochraně utajovaných informací.

Mezi aktiva lze u společnosti zařadit:
- utajované informace
- nosiče utajovaných informací
    a) v listinné podobě
    b) v nelistinné podobě (na elektronických nosičích)
- poučené fyzické osoby (zaměstnanci společnosti) vlastnící OFO nebo oznámení o splnění podmínek pro přístup k UI SU Vyhrazené.

Společnost Security Printing pracuje s dokumenty SU Vyhrazené a Důvěrné, a to v listinné i nelistinné podobě. Společnost je držitelem IS, certifikovaným NBÚ a opravňuje ji k manipulaci s nelistinnými UI stupně Vyhrazené a Důvěrné. Tento IS schválila odpovědná osoba do provozu.

Zaměstnanci společnosti pracují na zakázkách, které jsou předmětem UI a o nichž je pravidelně informován NBÚ.

Odhadované množství zakázek, v rámci kterých se budou zaměstnanci seznamovat s UI nebo je budou zpracovávat, případně jim budou UI poskytovány:

Stupeň utajení (SU)	Počet UI za rok
SU Vyhrazené	100 až 200
SU Důvěrné	50 až 100

Při zpracování zakázek se někteří zaměstnanci mohou setkat s UI, nejčastěji ve SU Vyhrazené, v některých případech – ve SU Důvěrné. Dále se mohou zaměstnanci setkat s bezpečnostními opatřeními SU Důvěrné.

Při vzniku UI (případně UD) bude tato informace (dokument) vytvořena a zpracována v zabezpečené oblasti. V souladu s § 24, odstavce 5 zákona č. 412/2005 o ochranně utajovaných informací, lze UI v odůvodněných případech zpracovat i v objektu mimo zabezpečenou oblast, případně s písemným souhlasem bezpečnostního ředitele mimo objekt, a to v případě, pokud je zajištěno, že k utajované informaci nemá přístup neoprávněná osoba.

3 Stanovení jednotlivých hrozeb, zranitelnosti a jejich vyhodnocení

Důležité pro vyhodnocení jednotlivých hrozeb je zjištění, jakým hrozbám jsou utajované informace u společnosti vystaveny. U společnosti Security Printing se jedná převážně o níže popsané hrozby.

3.1 Hrozba neoprávněného nakládání s UI poučenými osobami.

Jedná se o úmyslné případně neúmyslné porušení povinnosti zaměstnanců, kteří byli poučeni odpovědnou osobou. Tyto povinnosti vyplývají ze Zákona č. 412/2005 Sb. o ochranné utajovaných informací a z prováděcích vyhlášek NBÚ.

Mezi nejčastější hrozby tohoto typu patří:

- vyzrazení UI z nedbalosti (neúmyslné)
- úmyslné vyzrazení UI

Vyzrazení UI z nedbalosti bývá nejčastěji formou předání UI osobě, která nesplňuje podmínky pro přístup k UI. Dále sem patří nedodržení bezpečnostních zásad a opatření při manipulaci s UI (např. nevrácení UD do úschovného objektu v zabezpečené oblasti po skončení manipulace s UD, nedbalou skartací UD, ztrátou UD a dalšími nepředvídanými skutečnostmi.)

Úmyslné vyzrazení UI bývá nejčastěji formou předání UI neoprávněné osobě, pořízení kopie UD a následné předání kopie neoprávněné osobě, či ústní sdělení UI neoprávněné

osobě. Úmyslné vyzrazení UI probíhá za účelem vlastního obohacení nebo využití informace pro svůj osobní prospěch.

I když je větší pravděpodobnost vyzrazení UI z nedbalosti, nelze zcela vyloučit ani úmyslné vyzrazení UI pověřenou osobou, a to například za úplatu či vyzrazení pod pohrůžkou násilí či jiné trestné činnosti vůči pověřené osobě nebo rodinným příslušníkům pověřené osoby.

Výše zmíněná rizika lze do jisté míry zmírnit důkladným výběrem zaměstnanců, kontrolou dodržování režimu stanoveného pro nakládání s UI, pravidelným školením, a kontrolou personální, administrativní a fyzické bezpečnosti. Na základě těchto skutečností byla míra rizika úmyslného vyzrazení UI označena jako nízká až střední. Míra neúmyslného vyzrazení UI byla označena jako střední.

Celkově lze tedy hrozbu nakládání s UI poučenými osobami označit jako **střední.**

3.2 Hrozba manipulace s UI neoprávněnou osobou

„Neoprávněnou osobou se rozumí fyzická nebo právnická osoba, která nesplňuje podmínky přístupu k utajovaným informacím stanovených zákonem 412/2005“ [1]

Hrozbu manipulace s UI neoprávněnou osobou nelze nikdy zcela vyloučit a to převážně ve spojitosti s násilnou trestnou činností, např.:

- vloupání do zabezpečené oblasti,
- přepadení zabezpečené oblasti,
- přepadení transportu UI mimo zabezpečenou oblast,
- nátlak na pracovníky, setkávající se s UI, pod pohrůžkou násilí na rodinných příslušnících pracovníka či na něm samotném,
- ztráta UI.

Hrozbu manipulace s UI neoprávněnou osobou lze zredukovat použitím prostředků fyzické, administrativní a personální bezpečnosti dle zákona č. 412/2005, o ochraně utajovaných informací. Dále umístěním zabezpečené oblasti na místo v budově, jež je nepovolaným osobám těžce přístupné.
Míru naplnění hrozby lze na základě výše uvedených skutečností vyhodnotit jako střední.

3.3 Hrozba poškození, zničení, či neoprávněného nakládání s UI při živelných katastrofách a haváriích

Při živelných katastrofách a technologických haváriích může dojít k poškození či zničení UI, například při:

- požáru v budově, v níž se nachází zabezpečená oblast, způsobeném selháním lidského faktoru při práci s otevřeným ohněm (např. při kouření), při zásahu budovy bleskem atd.

- živelné katastrofě, např. zaplavení budovy povodní, zasažení tornádem či větrnou bouří, sesuvem půdy, zemětřesením atd.

- selhání technického vybavení budovy, např. závadou elektroinstalace či spotřebiče zapojeného do elektrické sítě, poruchou vodovodních rozvodů v budově a následném zatopení zabezpečené oblasti.

Při těchto událostech může dojít k neoprávněnému nakládání s UI v důsledku porušení bezpečnostních opatření při živelné katastrofě. Z výše uvedených informací je zřejmé, že předejít lze pouze požáru v budově a selhání technického vybavení budovy. Tato rizika lze snížit pravidelnými kontrolami elektrických a vodovodních rozvodů, školením zaměstnanců a kontrolou dodržování požárních předpisů. Hrozbu poškození či zničení UI živelnou katastrofou nelze vyloučit, ale vzhledem k umístění objektu je toto riziko málo pravděpodobné.

Celkově lze považovat riziko hrozby neoprávněného nakládání s UI při živelných katastrofách za malou až střední.

3.4 Hrozba poškození, zničení UI následkem teroristického útoku

Tato hrozba může nabývat různých forem, například:

- pohrůžka umístění výbušného systému v areálu zabezpečené oblasti
- umístění a nález výbušného systému v areálu zabezpečené oblasti
- nález podezřelého předmětu v areálu zabezpečené oblasti
- fyzický útok jednotlivce nebo skupiny na zabezpečenou oblast
- obdržení podezřelého předmětu poštovní zásilkou

Vzhledem k umístění objektu, omezenému přístupu k zabezpečené oblasti nepovolaným osobám a povaze utajovaných informací, se kterými se v objektu nakládá, je míra hrozby poškození a zničení UI následkem teroristického útoku malá.

3.5 Hrozba vyzrazení UI prostřednictvím pasivního odposlechu či operativní techniky

Tato hrozba je spojena s náhodným, ale i cíleným pozorováním prostor zabezpečené oblasti, a to z okolních nezabezpečených oblastí (např. okolních budov). Hrozbě lze čelit například instalací žaluzií či privátních folií na okna v zabezpečené oblasti.

Dále se může jednat o nasazení odposlechové techniky do zabezpečené oblasti. Tomuto problému lze čelit pravidelným školením pracovníků a dodržováním všech režimových opatření. V závislosti na případném podezření na nasazení této techniky je nutno provést prohlídku zabezpečené oblasti proti nasazení odposlechové techniky.

Míra rizika této hrozby je malá až střední.

3.6 Hrozba vyzrazení UI z počítačového systému

Hrozba vyzrazení UI z počítačového systému může být způsobena neoprávněnou osobou, jež získá přístup k systému za účelem zcizení UI. Závažnost hrozby lze snížit pravidelným školením pracovníků, aktualizacemi používaného softwaru a dodržováním preventivních opatření při používání počítačového systému

3.7 Stanovení celkové míry rizika

Hrozba	**Míra rizika**
Hrozba neoprávněného nakládání s UI poučenými osobami	střední
Hrozba manipulace s UI neoprávněnými osobami	střední
Hrozba poškození, zničení UI při živelných katastrofách a haváriích	malá až střední
Hrozba zničení, poškození UI následkem teroristickém útoku	malá
Hrozba vyzrazení UI prostřednictvím pasivního odposlechu či operativní techniky	malá až střední
Hrozba vyzrazení UI z počítačového systému	střední
Celková míra rizika	**střední**

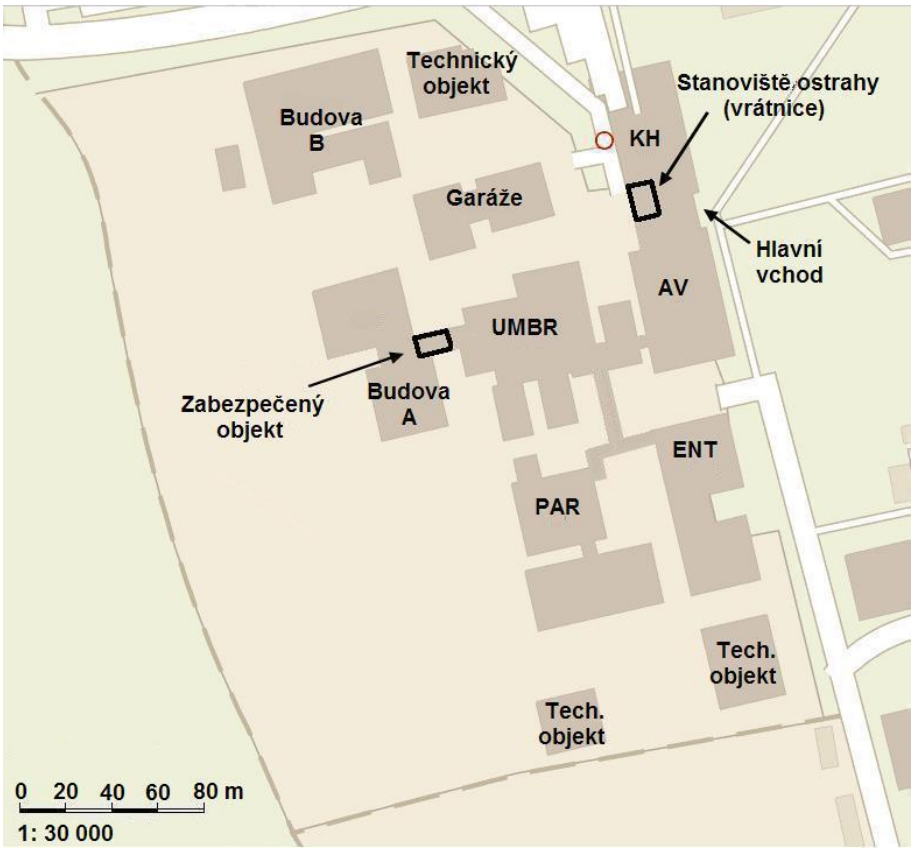
Tabulka 1: Stanovení míry rizika

Stanovení celkové míry rizika je základem pro projekt fyzické bezpečnosti. Jednotlivé hrozby byly klasifikovány dle pravděpodobnosti hrozby a předpokládaných následků stanovením míry rizika na malé, střední a velké. Na základě výše uvedených hrozeb byla stanovena celková míra rizika, a to jako **střední.** K minimalizaci jednotlivých rizik byla navržena bezpečnostní opatření fyzické i administrativní bezpečnosti.

4 Určení kategorií objektu a zabezpečených oblastí včetně jejich hranic a určení tříd zabezpečených oblastí

4.1 Popis areálu

Objekt, ve kterém se nachází sídlo firmy Security Printing je umístěn v areálu JČU v Českých Budějovicích Branišovská 31. Vlastníkem areálu je firma Security Printing.



Obrázek 1: Schéma areálu (zdroj: www.mapy.cz)

V areálu se nachází osm vícepatrových budov a několik menších technických objektů. Budovy KH, AV, ENT, PAR a UMBR jsou navzájem propojeny a jsou volně průchozí. Budova UMBR je propojena s budovou A, ale pouze stavebně - budovy nejsou průchozí. Budovy KH, B a ZEM mají shodně tři nadzemní podlaží, budovy AV, ENT, PAR, UMBR a budova A mají shodně čtyři nadzemní podlaží.

Do areálu vede hlavní vjezd z ulice Branišovská, zabezpečený vjezdovou závorou, obsluhovanou ze stanoviště ostrahy nacházející se vedle vjezdu do objektu mezi budovami KH a AV. V nočních hodinách se tento vjezd uzavírá bezpečnostními vraty. Stanoviště

ostrahy zároveň monitoruje hlavní vstup do areálu, nacházející se rovněž mezi budovami KH a AV, jež zároveň obě budovy spojuje.

Do areálu také vede servisní vjezd z ulice Studentská opatřený bezpečnostními vraty, která jsou trvale zamčena a otevírají se jen v případě poruch v areálu či jeho údržby.

Celý pozemek areálu je oplocen. Oplocení je tvořeno svařovanou železnou konstrukcí nebo pletivem.

Všechny vstupy do areálu jsou zabezpečený prostředky EZS a prostředky CCTV. Autorizace se provádí u vstupu do areálu a u vstupů do všech budov na základě osobní zaměstnanecké čipové karty.

V okolí areálu se na severní a východní straně nachází vícepodlažní obytné domy, na jižní a západní straně pak následují zemědělské plochy.

4.2 Stanovení objektu a jeho typu

Zabezpečený objekt se nachází v areálu JČU v budově A, ve druhém nadzemním podlaží, a to konkrétně v místnostech 311 a 311b.

Vstup do budovy A je nepřetržitě monitorován kamerovým systémem a vstup je možný pouze na základě zaměstnanecké čipové karty.

Průlezné otvory (okna) objektu se nacházejí ve výšce více než 5, 5 m nad terénem, ale lze k nim proniknout pomocí parapetu ze sousedních místností nebo se k nim slanit ze střechy budovy, na kterou lze proniknout ze sousední budovy. Proto **nesplňuje** požadavky na umístění průlezných otvorů.

Stropy, podlahy a stěny mají pevnou stavební konstrukci z betonu, respektive z cihel či tvárnic.

Část hranice zabezpečeného objektu, jež je shodná s opláštěním objektu je po stavebních úpravách, kdy došlo k zateplení budovy a výměně starých oken za okna plastová.

„Při určení typu objektu je rozhodující ta část hranice objektu, která má nejnižší odolnost.“ [2]

Na základě výše uvedeného byl objekt stanoven jako Objekt typ 1 **S3 = 1**

4.3 Stanovení hranic objektu

Hranice zabezpečeného objektu tvoří místnosti č. 311 a 311b. Tyto místnosti jsou umístěné v budově A, ve druhém nadzemním podlaží, v areálu JČU Branišovská 31, České Budějovice.

Nad zabezpečenou oblastí ve třetím nadzemním podlaží se nachází kancelářské prostory. Pod zabezpečenou oblastí, tj. v prvním nadzemním podlaží se nachází vchod do budovy.

Popis objektu:

Místnost č. 311. Severní stěna místnosti je téměř po celé délce vybavena okny ve výšce vyšší, než 5,5 metru nad terénem, ale lze se k nim dostat pomocí parapetu ze sousedních místností. Stěnu tvoří pevná stavební konstrukce. Severní stěna je z pevné stavební konstrukce. Východní stěna je rovněž vybavena téměř po celé délce okny, které jsou ve výšce větší než 5,5 metru nad terénem a nelze se k nim dostat pomocí parapetu či jiných stavebních prvků. Stěna je z pevné stavební konstrukce. Jižní stěnu tvoří lehká sádrokartonová stavební konstrukce, v níž jsou umístěny vchodové dveře do místnosti, jež jsou pevné konstrukce. Dále se zde nachází dveře vedoucí do místnosti 311b. Místnost sousedí na severu s budovou UMBR, která je oddělena pevnou stavební konstrukcí. Jižní stěnou sousedí s místností 312.

Místnost č. 311b. Severní stěna místnosti je z pevné stavební konstrukce. Nachází se zde okno ve výšce větší než 5,5m a je dostupné po parapetu z vedlejších místností. Severní stěnu tvoří lehká sádrokartonová konstrukce, ve které jsou dveře z pevné konstrukce vedoucí do místnosti 311. Východní a jižní stěnu tvoří lehká sádrokartonová konstrukce, za níž se nachází místnost 312.

Stanoviště ostrahy je umístěno cca 100m od hranice budovy, kde se nalézá zabezpečený objekt.

Hranice zabezpečeného objektu je vyznačena ve výkresové části technické dokumentace fyzické bezpečnosti.

4.4 Stanovení zabezpečené oblasti

Zabezpečená oblast se nachází uvnitř zabezpečeného objektu a to v prostorech místnosti č. 311b. Západní stěna je součástí opláštění budovy a nachází se zde okno opatřené žaluziemi a mechanickým zábranným systémem. Vzhledem k tomu, že zbylé stěny jsou z lehké sádrokartonové stavební konstrukce, byly opatřeny bezpečnostní příčkou technologie Duragips, obsahující vrstvy ocelového pozinkovaného plechu. Dveře vedoucí do zabezpečené oblasti jsou z pevné konstrukce a nevykazují žádné znaky opotřebení, které by mohly zabránit rozpoznání pokusu o násilné vniknutí do zabezpečené oblasti.

Hranice zabezpečené oblasti je vyznačena ve výkresové části technické dokumentace fyzické bezpečnosti.

„*Zabezpečené oblasti se podle nejvyššího stupně utajení utajované informace, která se v nich ukládá, zařazují do kategorií a) Přísně tajné, b) Tajné, c) Důvěrné, d) Vyhrazené. Zabezpečené oblasti se podle možnosti přístupu k utajované informaci zařazují do tříd*
a) třída I, kdy vstupem do této oblasti dochází k seznámení s utajovanou informací,
b) třída II, kdy vstupem do této oblasti nedochází k seznámení s utajovanou informací.“ [3]

Jelikož zabezpečená oblast slouží jako úložiště a prostor pro manipulaci s dokumenty do SU Důvěrné a protože při vstupu do zabezpečené oblasti nedochází k seznámení s utajovanými informacemi, je na základě výše uvedené části zákona zabezpečená oblast **kategorie Důvěrné třídy II.**

4.5 Popis zabezpečení objektu

Fyzická bezpečnost je soubor opatření, jejichž účelem je zamezit nepovolané osobě v přístupu do zabezpečených oblastí, ve kterých se mohou nacházet utajované informace nebo zabránit poškození, zničení či jinému znehodnocení těchto utajovaných informací.

Prostředky fyzické bezpečnosti mají za úkol následující:

- odradit pachatele od násilného vniknutí do objektu
- znemožnit pachateli násilné vniknutí do objektu
- ztížit a zpomalit postup pachatele
- umožnit včasné vyrozumění ostrahy a policie a tím zajistit dopadení pachatele

4.5.1 Úschovné objekty

V zabezpečené oblasti je umístěn jeden úschovný objekt. Jedná se o skříňový trezor TSS 125 M, certifikovaný NBÚ pro ukládání UI do SU Tajné a splňuje požadavky bezpečnostní třídy 1, podle normy ČSN EN 1143-1+A1 platnou od července 2009.

SS1 = 3 body

Úschovný objekt obsahuje zámek MAUER typu 2, který splňuje požadavky bezpečnostní třídy A, dle normy ČSN EN 1300+A1.

SS2 = 2 body

Celkové hodnocení úschovného objektu se vypočte vynásobením předchozích hodnot, tedy:

S1 = SS1 x SS2

S1 = 6 body

4.5.2 Zabezpečená oblast

Zabezpečená oblast se nachází v prostorách místnosti č. 311b. V severní stěně místnosti se nachází okno. Protože je okno dostupné po parapetu ze sousedních místností či po slanění ze střechy, bylo zabezpečeno mechanickým zábranným prostředkem (mříží). Mechanický zábranný prostředek splňuje podmínku, že jeho otvory „*…nesmí dovolit průchod šablony ve tvaru elipsy o rozměrech 250 mm x 150 mm a tloušťky 20 mm.“*[4] Okno je vybaveno roletou a privátní folií. Oblast je rovněž vybavena prostředky elektronické zabezpečovací signalizace, jejichž instalace odpovídá minimální hodnotě SS92 = 3.

Východní, jižní a západní stěnu tvoří lehká sádrokartonová stavební konstrukce, proto byly tyto stěny opatřeny bezpečnostní příčkou systému Duragips. Tento systém je certifikována podle ČSN P ENV 1627 a spadá do bezpečnostních tříd BT2 a BT3.

Dveře, vedoucí do zabezpečené oblasti, jsou pevné konstrukce typu Sherlock K330/2 certifikované dle bezpečnostní normy ČSN EN 1627 a protipožární normy ČSN EN 1634. Dveře neobsahují žádné znaky opotřebení, bránící v identifikaci pokusu o neoprávněný přístup.

Zabezpečená oblast má stěny z lehké stavební konstrukce, proto je oblast typu 1

SS3 = 1 bod

Dveře vedoucí do zabezpečené oblasti, obsahují bezpečnostní cylindrickou vložkou FAB 2402B a bezpečnostním kováním ROSTEX R1, v provedení koule z vnější strany a klika z vnitřní strany zabezpečeného objektu. Uzamykací systém a jeho komponenty splňují požadavky bezpečnostní třídy RC 4, podle ČSN EN 1627 a certifikaci NBÚ, proto je typu 3.

SS4 = 3 body

Celkové hodnocení zabezpečené oblasti

S2 = SS3 x SS4

S2 = 3 body

4.5.3 Hranice objektu

Hranice objektu je tvořena místností číslo 311 a zabezpečenou oblastí v místnosti 311b. Strop a podlaha objektu, stejně jako stěny orientované na západ, sever a východ, jsou z pevné stavební konstrukce. Stěna směřující na jih je z lehké sádrokartonové stavební konstrukce.

Okna objektu se nalézají ve výšce větší než 5,5 metru a není k nim přímý přístup terénních nerovností, stromů či okapů. Lze se k nim dostat pomocí parapetu ze sousedních místností. Rovněž je možné slanit k oknům ze střechy, jež je stavebně spojena se sousední budovou. Z důvodů nesplnění požadavků na umístění průlezných otvorů je objekt stanoven jako typu 1.

S3 = 1 bod

4.5.4 Systém kontroly vstupu do zabezpečené oblasti a zabezpečeného objektu

Zabezpečený objekt

Kontrola vstupu do zabezpečeného objektu je typu 2 a provádí se systémem typu SiPass, jež je certifikovaným pro způsobilost typu 2, splňující normu ČSN EN 50133-1. Kontrola vstupu je ovládána bezkontaktní čtečkou čipových identifikačních karet, umístěnou u vchodových dveří do zabezpečeného objektu. Ve vchodových dveřích se nachází certifikovaný magnetický kontakt IMKW6-10 napojený na zpožděnou smyčku EZS. Kontakt je po přiložení čipové identifikační karty na stanovenou dobu překlenut a umožní tak autorizované osobě vstup do objektu. Pokud se osoba neidentifikuje čipovou kartou, bude i přes deaktivaci EZS spuštěna poplachová signalizace na stanovišti ostrahy. Vstup do objektu je vybaven i mechanickou zábranou (tj. mechanickým zámkem umístěným ve vchodových dveřích).

Bodové ohodnocení

SS6 = 2 body

Zabezpečená oblast

Kontrola vstupu do zabezpečené oblasti je typu 2 a provádí se systémem typu SiPass, jež je certifikovaný pro způsobilost typu 2 a splňuje normu ČSN EN 50133-1. Kontrola vstupu je ovládána bezkontaktní čtečkou čipových identifikačních karet, umístěnou u vchodových dveří do zabezpečeného objektu. Ve vchodových dveřích se nachází certifikovaný magnetický kontakt IMKW6-10 napojený na zpožděnou smyčku EZS. Kontakt je po přiložení autorizované čipové identifikační karty na stanovenou dobu překlenut a umožní autorizované osobě vstup do objektu. Pokud se osoba neidentifikuje čipovou kartou, bude i přes deaktivaci EZS spuštěna poplachová signalizace na stanovišti ostrahy. Vstup do objektu je vybaven i mechanickou zábranou (tj. mechanickým zámkem umístěným ve vchodových dveřích).

Bodové ohodnocení

SS6 = 2 body

4.5.5 Režim návštěv v objektu

Návštěvy se po objektu pohybují pouze s doprovodem. Zároveň je vedena evidence údajů o návštěvách, obsahující osobní identifikační údaje návštěv a osob, jež návštěvy doprovázejí a časové údaje, kdy návštěvy proběhly. Zaměstnanci společnosti jsou v objektu viditelně označeni zaměstnaneckou identifikační kartou.

Bodové ohodnocení

SS7 = 3 body

Celkové hodnocení kontroly vstupů a režimu návštěv

S4 = SS6 + SS7

S4 = 5 bodů

4.5.6 Ostraha

Ostraha budovy A kde, se nachází zabezpečená oblast, se provádí nepřetržitě. Ostraha je prováděna pracovníky firmy Security Printing, která vlastní areál, v němž se budova A nachází. V pracovní době je ostraha vykonávána jedním pracovníkem ostrahy na recepci zároveň sloužící jako stanoviště ostrahy. Na stanoviště ostrahy jsou vyvedeny výstupy EZS zabezpečené oblasti a EZS, EPS a CCTV spadající pod zabezpečení areálu JČU. Mimo pracovní dobu ostrahu vykonávají dva pracovníci bezpečnostní služby. Jeden z pracovníků ostrahy provádí obchůzky areálu, v náhodném intervalu závislém na vnitřním provozu, ale nepřesahujícím 6 hodin. Ostraha pravidelně provádí kontrolu vnitřního prostoru areálu a budovy A, kde je umístěna zabezpečená oblast, v případě podezření provádí kontrolu i uvnitř ostatních budov v areálu. Ostraha nemá povolení ke kontrole prostor zabezpečeného objektu a zabezpečené oblasti. V případě potřeby ostraha kontaktuje osobu s povolením ke vstupu do zabezpečené oblasti. Rovněž kontroluje neporušenost a uzamčení dveří vedoucích do zabezpečené oblasti, také kontroluje neporušenost oken vedoucích do zabezpečeného objektu. V době trvání obchůzky se na stanovišti ostrahy neustále nachází druhý pracovník. Osoby vyskytující se v zabezpečené oblasti po pracovní době musí být předem oznámeny na recepci.

Stanoviště ostrahy se nachází do 100 m od zabezpečené oblasti.

Na základě výše uvedeného je možné vyhodnotit, že způsob ostrahy odpovídá typu 3.

SS8 = 3 body.

4.5.7 Zařízení EZS

V prostorách zabezpečené oblasti a zabezpečeného objektu jsou použitý prvky EZS a další komponenty splňující normu ČSN EN 50131-1 ed. 2 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy pro stupeň zabezpečení 2 nízké až střední riziko. Tísňový systém splňuje požadavky normy ČSN EN 50134-1 Poplachové systémy – Systém přivolání pomoci.

Jedná se o tyto prvky EZS

- ústředna EZS typ Siemens IC60M-8
- ovládací klávesnice IKP6 - 03
- detektor pohybu PIR typ IRM 270C
- detektory tříštění skla DL 500
- trezorové otřesové senzory ES 400
- magnetické kontakty IMKW6-10
- tísňová tlačítka HB 105
- opticko-kouřový hlásič požáru SD-282ST splňující normy ČSN EN 14604 a ČSN EN 54
- vnitřní siréna SA 913F umístěná před zabezpečenou oblastí

Použitá zařízení elektrické zabezpečovací signalizace musí splňovat požadavky norem řady ČSN EN (CLC/TS) 50131 – Poplachové zabezpečovací a tísňové systémy, a musí být ověřena jejich funkčnost zkouškou podle normy TNI 334591-3.

Revize použitých prvků EZS je prováděna každých 12 měsíců, což je doloženo v revizní zprávě nebo zprávě o provozní kontrole. Tento zápis se ukládá u odpovědné osoby (bezpečnostního ředitele nebo osoby jím pověřené).

Ústředna EZS je umístěna uvnitř zabezpečené oblasti v místnosti 311b. Z vnitřní strany vstupních dveří do zabezpečeného objektu se nachází klávesnice s LCD displejem umožňující vstup do objektu. Obdobně je tomu v případě vstupních dveří vedoucích do zabezpečené oblasti.

Prostředky EZS jsou zapojeny do různých smyček (zabezpečených proti přerušení) a připravených pro všechny nejpravděpodobnější případy narušení zabezpečeného objektu a oblasti.

- vstupní dveře do zabezpeč. objektu – jsou zde částečně zpožděné smyčky DVEŘE 1 (realizovaná magnetickými kontakty na dveřích) a PROSTOR 1 (realizovaná detektorem pohybu typu PIR), smyčky jsou zpožděné z důvodu možnosti aktivovat či deaktivovat EZS platným kódem na LCD klávesnici, zpoždění je realizováno ústřednou EZS, v případě příchodu je zpoždění smyčky DVEŘE 1 nahrazeno překlenutím smyčky od kontroly vstupu)
- vstupní dveře do zabezpeč. oblasti – jsou zde částečně zpožděné smyčky DVEŘE 2 (realizovaná magnetickými kontakty na dveřích) a PROSTOR 2 (realizovaná

detektorem pohybu typu PIR), smyčky jsou zpožděné z důvodu možnosti aktivovat či deaktivovat EZS platným kódem na LCD klávesnici, zpoždění je realizováno ústřednou EZS, v případě příchodu je zpoždění smyčky DVEŘE 2 nahrazeno překlenutím smyčky od kontroly vstupu)

- okna zabezpeč. objektu – jsou zde smyčky OKNO 1 (realizovaná magnetickými kontakty na oknech) a SKLO 1 (realizovaná detektory tříštění skla)
- okno zabezpeč. oblasti – jsou zde smyčky OKNO 2 (realizovaná magnetickým kontaktem na oknech) a SKLO 2 (realizovaná detektorem tříštění skla)
- úschovný objekt – jsou zde smyčky TREZOR 1 a TREZOR 2 (realizované otřesovými senzory)
- vlastní ochrana ústředny EZS – je zde smyčka USTREDNA (realizovaná systémovým tamper kontaktem)
- přivolání ostrahy při ohrožení – jsou zde smyčky POMOC 1 a POMOC 2 (realizovaná tísňovým tlačítkem)
- jiné možnosti narušení a pohybu v prostoru (probourání stěny atd.) – je zde smyčka POHYB 1 (realizovaná pohybovým senzorem v zabezpečeném objektu) a smyčka POHYB 2 (realizovaná pohybovým senzorem v zabezpečené oblasti)

SS91 = 2 body

V zabezpečené oblasti je instalací zařízení EZS zajištěna prostorová i plášťová ochrana a tísňový systém. Hlášení prostředků EZS a signalizace EPS je vyvedeno na stanoviště fyzické ostrahy.

SS92 = 3 body

Výpočet mezivýsledku bodového ohodnocení zařízení EZS

$$SS9 = (SS91 + SS92)/2 \text{ x } SS92/OBL$$

- OBL = bodová hodnota určená kategorií zabezpečené oblasti, tzn. OBL = 3 body

$$SS9 = (2 + 3)/2 \text{ x } 3/3 = 2,5$$

Výsledná hodnota se zaokrouhluje na celé číslo a maximální hodnota může být čtyři, proto:

SS9 = 3 body

Celkový výsledek bodového ohodnocení ostrahy a EZS

S5 = SS8 + SS9

S5 = 6 bodů

4.5.8 Ochrana perimetru

Ochrana perimetru je typu 1. To znamená: „*Fyzické bariéře typu 1 odpovídá oplocení bez speciálních bezpečnostních požadavků. Účelem tohoto oplocení je vyznačit hranice a zajistit minimální úroveň odrazení nebo odolnosti. Fyzická bariéra typu 1 může být tvořena jakýmkoliv typem materiálu.“* [5]

SS10 = 1 bodů

Hranice perimetru rovněž neobsahují kontrolu vstupu na všech přístupových bodech (SS11), nejsou prováděny namátkové vstupní a výstupní kontroly (SS12), hranice neobsahuje perimetrické detekční systémy (SS13). Neobsahuje bezpečnostní osvětlení vyplývající například z požadavků speciálního televizního systému na perimetru (SS14) a neobsahuje tedy ani prostředky CCTV (SS15).

SS11 = 0, SS12 = 0, SS13= 0, SS14= 0, SS15= 0

Celkové hodnocení ochrany perimetru

S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15

S6 = 0 bodů

4.5.9 Zařízení elektronické požární signalizace

Požární hlásič je zapojen do ústředny EZS a přes ni je signál veden na pracoviště určené pro stálý výkon ostrahy. Hlásiče jsou realizovány kouřovo-optickým senzorem SD-282ST, jež splňuje normu ČSN EN 54 – Elektrická požární signalizace a nacházejí se na stropech v místnosti 311 a v zabezpečené oblasti.

Zařízení EPS jsou bez bodového ohodnocení.

4.5.10 Zařízení fyzického ničení nosičů informací nebo dat

Zařízení fyzického ničení nosičů (skartovací stroj) je umístěno v zabezpečené oblasti a je realizován strojem Martin Yale 2000 CC řez (řez 3,8x48 mm), který je typu 2 a je určen pro ničení UI ve SU Důvěrné či nižší. Zařízení fyzického ničení nosičů informací nebo dat je certifikované NBÚ.

Zařízení fyzického ničení nosičů informací nebo dat je bez bodového hodnocení.

4.5.11 Zařízení proti pasivnímu a aktivnímu odposlechu utajovaných informací

„*Jednací oblast pro pravidelné projednávání utajovaných informací stupňů utajení Tajné a Přísně tajné je zabezpečena technickými prostředky proti pasivnímu a aktivnímu odposlechu utajované informace. Tato zařízení Úřad necertifikuje*.“[6]

Na základě výše uvedeného není nutné zabezpečit zabezpečený objekt a oblast prostředky proti odposlechu. Přesto je okno v zabezpečené oblasti vybaveno roletou a privátní folií zabraňující pasivnímu odposlechu.

5 Tabulka bodového ohodnocení opatření fyzické bezpečnosti zabezpečené oblasti

Záhlaví tabulky

Název zabezpečené oblasti: Zabezpečenou tvoří místnost č. 311b ve 2.NP v sídle společnosti Security Printing v budově A – Branišovská 1716/31d, České Budějovice

Název objektu UI: Hranici zabezpečeného objektu tvoří místnost č. 311 a zabezpečená oblast místnost č. 311b v sídle společnosti Security Printing v budově A – Branišovská 1716/31d, České Budějovice

Kategorie zabezpečené oblasti: Důvěrné

Třída zabezpečené oblasti: Třída II

Typ zabezpečené oblasti: Typ 1

Účel zabezpečené oblasti: V zabezpečené oblasti jsou uloženy UI SU Vyhrazené a Důvěrné, zároveň se v ní UI SU Vyhrazené a Důvěrné zpracovávají a vytvářejí. Zabezpečená oblast není využívána jako pracoviště se stálou přítomností zaměstnanců.

BEZPEČNOSTNÍ OPATŘENÍ	TYP	BODOVÉ OHODNOCENÍ
Úschovné objekty	☐ T. 4 – 4 body ☒ T. 3 – 3 body ☐ T. 2 – 2 body ☐ T. 1 – 1 bod	SS1= 3
Zámky úschovných objektů	☐ T. 4 – 4 body ☐ T. 3 – 3 body ☒ T. 2 – 2 body ☐ T. 1 – 1 bod	SS2= 2
Celkové hodnocení úschovného objektu a jeho zámku	S1 = SS1 x SS2	**S1= 6**
Zabezpečená oblast	☐ T. 4 – 4 body ☐ T. 3 – 3 body ☐ T. 2 – 2 body ☒ T. 1 – 1 bod	SS3= 1

Uzamykací systémy zabezpečené oblasti	☐ T. 4 – 4 body ☒ T. 3 – 3 body ☐ T. 2 – 2 body ☐ T. 1 – 1 bod	SS4= 3
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	S2 = SS3 x SS4	**S2= 3**
Zabezpečený objekt	☐ T. 4 – 5 bodů ☐ T. 3 – 3 body ☐ T. 2 – 2 body ☒ T. 1 – 1 bod	**S3= 1**
Kontrola vstupu	☐ T. 4 – 4 body ☐ T. 3 – 3 body ☒ T. 2 – 2 body ☐ T. 1 – 1 bod	SS6= 2
Režim návštěv v zabezpečeném objektu a) Návštěvy s doprovodem b) Návštěvy bez doprovodu c) Návštěvy bez kontroly	☒ ad a) – 3 bod ☐ ad b) – 1 bod ☐ ad c) – 0bodů	SS7 = 3
Celkové hodnocení kontroly vstupu	S4 = SS6 + SS7	**S4= 5**
Ostraha	☐ T. 5 – 5bodů ☐ T. 4 – 4 body ☒ T. 3 – 3 body ☐ T. 2 – 2 body ☐ T. 1 – 1 bod	SS8= 3
Zařízení elektrické zabezpečovací signalizace	☐ T. 4 – 4 body ☐ T. 3 – 3 body ☒ T. 2 – 2 body ☐ T. 1 – 1 bod	SS91= 2

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

ZABEZPEČENÁ OBLAST KATEGORIE Důvěrné	Míra rizika
	Střední
Povinné: (S1) + (S2) + (S3)	10
Povinné: (S4) + (S5)	11
Nepovinné: (S6)	0
Celkový výsledek	**21**

Hodnoty získané v tabulce porovnáme s tabulkou bodových hodnot pro nejnižší míry zabezpečení zabezpečené oblasti, podle bodu 12 Přílohy č. 1 novely Vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků:

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

Použité prostředky fyzické bezpečnosti vyhovují pro střední míru rizika a v zabezpečené oblasti kategorie Důvěrné splňují dané požadavky. Odpovědná osoba ověřila, že přijaté prostředky fyzické bezpečnosti, jež byly použity, splňují právní předpisy v oblasti ochrany UI a odpovídají projektu fyzické bezpečnosti.

6 Technická dokumentace fyzické bezpečnosti

6.1 Výkresová dokumentace

Podle přílohy č. 1 vyhlášky 528/2005 musí výkresová dokumentace obsahovat znázornění hranic zabezpečené oblasti a objektu a umístění technických prostředků fyzické bezpečnosti v nich umístěných. Výkresovou dokumentaci obsahuje příloha 1.

6.2 Dokumentace technických prostředků

Dokumentace technických prostředků obsahuje především výčet (název, počet, případně umístění) použitých technických prostředků umístěných v zabezpečené oblasti a objektu. Dále obsahuje čísla certifikátů instalovaných technických prostředků. Dokumentace také může obsahovat zápis o posouzení shody necertifikovaných technických prostředků z doby instalace s uvedením specifikace a způsobu používání, pokud se takové prostředky v zabezpečeném objektu a oblasti vyskytují .

6.3 Specifikace certifikovaných prostředků

Název technického prostředku	Počet	Číslo certifikátu	Popis (Funkce)
Mechanické zábranné prostředky:			
Skříňový trezor typ TSS 125 M	1	T0052/2010	Ukládání UI do stupně Důvěrné
Bezpečnostní protipožární dveře SHERLOCK K33/2	2	T0104/2011	Dveře do zabezpečeného objektu a zabezpečené oblasti
Zámková bezpečnostní cylindrická vložka FAB 2402B	2	T0043/2010	Součást dveří do zabezpečené objektu a zabezpečené oblasti
Bezpečnostní kování ROSTEX R1	2	T0078/2010	Součást dveří do zabezpečené objektu a zabezpečené oblasti

Systém kontroly vstupu:			
Řídící jednotka pro kontrolu vstupu	1	T3006/2009	Řídící jednotka pro kontrolu vstupu umístěná v zabezpečené oblasti
SiPass bezdotyková čtečka	2	T3006/2009	Kontrola vstupu bezkontaktní čtečkou do objektu UI a zabezpečené oblasti
Magnetický kontakt IMKW6-10	2	T1050/2009	Součást dveří do zabezpečeného objektu a zabezpečené oblasti
EZS - komponenty:			
Ústředna IC60M-8	1	T1108/2010	Ústředna s 8 programovatelnými výstupy a 16 vstupy
LCD klávesnice IKP6 - 03	1	T1108/2010	Deaktivuje / aktivuje magnetický kontakt D1 a detektor pohybu P1 v zabezpečeném objektu
LCD klávesnice IKP6 - 03	1	T1108/2010	Deaktivuje / aktivuje magnetický kontakt D2 a detektor pohybu P2 v zabezpečené oblasti
Magnetický kontakt IMKW6-10	7	T1106/2010	Detektor O1 na oknech v zabezpečeném objektu, O2 na oknech v zabezpečené oblasti
Detektor pohybu IRM 270C	2	T1054/2010	Detektor pohybu P1 v zabezpeč. objektu Detektor pohybu P2 v zabezpeč. oblasti
Detektor tříštění skla DL 500	3	T1097/2010	Akustický detektory tříštění skla O1 v zabezpečeném objektu Akustický detektor tříštění skla O2 v zabezpečené oblasti
Kouřový detektor požáru typ 2351E	2	T4009/2009	Detektor požáru 1 v zabezpečeném objektu Detektor požáru 2 v zabezpeč. oblasti
Tísňové tlačítko HB 105	2	T1063/2010	Tlačítka pro přivolání pomoci v zabezpeč. objektu a oblasti
Siréna SA 913F	2	Bez certifikace	Umístěná v recepci a před vstupem do zabezpečeného objektu

Otřesové trezorové čidlo ES 400	1	T1062/2010	Čidlo umístěné ve skříňovém trezoru
Skartovací stroj Martin Yale 2000 CC	1	T5022/2010	Stroj je umístěn v zabezpečené oblasti

7 Podmínky používání certifikovaných technických prostředků

„Technický prostředek pro ochranu utajovaných informací musí být nově pořízen v době platnosti jeho certifikátu.“ [7]

Po uplynutí doby platnosti certifikátu smí být prostředek pro ochranu utajovaných informací používán pouze za předpokladu, že prošel funkční zkouškou a je tedy plně funkční. Tyto kontroly jsou prováděny v časových intervalech nejméně 12 měsíců.

„*U mechanických zábranných prostředků a zařízení fyzického ničení nosičů informací a dat se funkční zkouška doloží zápisem podepsaným odpovědnou osobou nebo jí pověřenou osobou. U ostatních technických prostředků se funkční zkouška doloží protokolem o zkoušce (např. revizí, záznamem v provozní knize). Výsledek funkční zkoušky se ukládá u odpovědné osoby nebo jí pověřené osoby.“* [8]

U EZS a tísňového systému se provádí funkční zkouška podle normy TNI 334591-3. Záznam o zkoušce se ukládá u pověřené osoby.

U skartovacího stroje dojde v rámci funkční zkoušky nejen ke kontrole, ale i ke zkušební skartaci neutajovaného dokumentu. Bude vyhotoven záznam o funkční zkoušce.

V průběhu platnosti certifikátu NBÚ se provádí funkční zkouška, zajištěná odpovědnou osobou, nejpozději jednou za 12 měsíců. O takovéto zkoušce není povinností vést záznam.

8 Provozní řád

8.1 Pravidla pro vjezd a pohyb vozidel v areálu

Provozní řád řeší režim pohybu vozidel pouze po areálu, protože zabezpečený objekt tvoří dvě místnosti, jež nejsou dopravním prostředkům dostupné.

Do areálu vede hlavní vjezd z ulice Branišovská, který je zabezpečen vjezdovou závorou obsluhovanou ze stanoviště ostrahy, jenž je u ní umístěné. Po pracovní době (kolem 19:00) se vjezd uzavírá vraty. Případné otevření provádí ostraha objektu a o pohybu vozidel mimo pracovní dobu se vede záznam. Vjezd je povolen pouze vozidlům firmy Security Printing a nebo vozidlům předem ohlášených návštěv či zásobování. Ostraha vpouští firemní vozidla do areálu na základě vizuální identifikace. Vozidla návštěv (zásobování) musí být před vjezdem do areálu zkontrolována, zda se skutečně jedná o ohlášené vozidlo. Parkoviště návštěv se nachází zhruba 50m od hranic budovy, v níž se nalézá zabezpečená oblast.

Z ulice Studentská vede do areálu servisní vjezd. Tento vjezd je trvale zavřen vraty a je využíván pouze při opravách či stavebních úpravách v areálu. V případě použití tohoto vjezdu je o projíždějících vozidlech veden záznam.

8.2 Pravidla pro vstup a pohyb osob v budově A

Pracovníci firmy Security Printing se po budově pohybují volně, návštěvy a osoby nezaměstnané ve firmě se pohybují pouze s doprovodem. O výskytu osob v budově po pracovní době musí být informován službu vykonávající pracovník ostrahy.

Do budovy mohou osoby vstoupit hlavním vchodem v přízemí, případně vchody spojujícími budovu A s budovou B. Tyto vchody se nalézají v každém nadzemním podlaží, ale dveře, v nich umístěné, jsou trvale zamčeny (klíče se nacházejí na stanovišti ostrahy, u pověřené osoby a pro případ požáru jsou umístěny v prosklených bezpečnostních skříňkách po obou stranách vchodu). Všechny dveře obsahují magnetický kontakt, v případě neohlášeného otevření je spuštěna poplachová signalizace na stanovišti ostrahy. Ostraha pravidelně kontroluje uzamčení dveří.

Hlavní vchod do budovy je neustále monitorován systémem CCTV. Nachází se zde systém kontroly vstupu realizován bezkontaktní čtečkou čipových karet. Přístupovými kartami jsou vybaveni všichni pracovníci firmy Security Printing. V pracovní době mohou do

budovy vstupovat všichni zaměstnanci firmy. Po pracovní době je vstup umožněn pouze v doprovodu pracovníka ostrahy, jež má v tuto dobu jako jediný povolení ke vstupu do budovy, a to za účelem její kontroly.

Osobám nezaměstnaným ve firmě (návštěvám) je vstup do budovy A povolen pouze v doprovodu pracovníka, jenž si návštěvu vyžádal, či mu byla přidělena (návštěvu provází). Údaje o návštěvách se zaznamenávají na recepci. Cizím osobám je umožněn vstup do areálu za účelem firemních jednání, inspekcí, dodávky materiálu, či servisních a stavebních prací.

8.3 Pravidla pro vstup a pohyb osob v zabezpečeném objektu a oblasti

Vstup do zabezpečeného objektu a zabezpečené oblasti je umožněn pouze poučeným zaměstnancům vlastnícím oprávnění pro přístup k UI SU Důvěrné. Tito oprávněné osoby obdrží prostředky pro vstup do zabezpečené oblasti (klíče a hesla k systému EZS). Bezpečnostní ředitel vlastní seznam osob, jež obdrželi tyto prostředky, seznam je pravidelně aktualizován.

Poučené osoby na SU Vyhrazené mají přístup do zabezpečené oblasti pouze s doprovodem oprávněné osoby. Výjimečně jim může odpovědná osoba umožnit samostatný přístup do zabezpečené oblasti, ale v takovém případě musí být zajištěno, aby se takováto osoba neseznámila s UI stupně Důvěrné (UI stupně Důvěrné jsou v úložném objektu a osoby s nižším stupně oprávnění a poučení k nim nemají přístup). Ostatní poučené osoby mohou vstoupit do zabezpečeného objektu pouze v doprovodu osob vlastnících výše zmíněné oprávnění. Cizí osoba (návštěva) se musí při vstupu do zabezpečeného objektu či zabezpečené oblasti prokázat průkazem totožnosti. Pověřený zaměstnanec, s oprávněním k samostatnému vstupu do zabezpečeného objektu, jež provází návštěvu, či navštívený zaměstnanec musí cizí osobu zapsat do Knihy návštěv a vstupů, kam uvede její jméno, příjmení, číslo průkazu totožnosti, účel návštěvy, časové údaje kdy návštěva proběhla a jméno zaměstnance doprovázejícího návštěvu či navštíveného. Při odchodu cizí osoby se do Knihy návštěv uvede doba opuštění zabezpečené oblasti.

V zabezpečeném objektu se může návštěva nebo zaměstnanec (např. pracovník úklidové služby), jenž nemá oprávnění k přístupu k UI, zdržovat pouze v doprovodu osoby oprávněné ke vstupu do zabezpečeného objektu. V zabezpečené oblasti se může návštěva nebo zaměstnanec, jenž nemá oprávnění k přístupu k UI, zdržovat pouze v odůvodněném případě a to za doprovodu pracovníka vlastnícího oprávnění ke vstupu do zabezpečené oblasti

a oprávnění pro přístup k UI SU Důvěrné. Za návštěvu, či zaměstnance bez oprávnění, je po dobu jejich pobytu v zabezpečeném objektu zodpovědný pověřený pracovník provázející návštěvu, či navštívený zaměstnanec, jež má povinnost nenechat návštěvníka za žádných okolností v objektu samotného.

V zabezpečeném objektu se návštěva, či zaměstnanec bez oprávnění k přístupu k UI zdržují jen na dobu nezbytně nutnou. Po dobu jejich přítomnosti jsou UD uloženy v úschovném objektu.

Příslušníci HZS, inspektoři bezpečnosti práce, či Policie ČR mají do zabezpečeného objektu přístup v odůvodněných případech a po předložení jejich služebních průkazů. Musí být zapsáni do Knihy návštěv a doprovázeni zaměstnancem vlastnícím oprávnění k samostatnému vstupu do objektu. V případě události vyžadující včasný zásah osob bez oprávnění ke vstupu (např. havárie na vodovodním potrubí, požár poskytnutí lékařské pomoci atd.) mají osoby vykonávající tento zásah (pracovníci vodovodní společnosti, hasiči, zdravotníci atd.) umožněn vstup bez předložení průkazu totožnosti (nejsou uvedeni v knize návštěv).

Místnost, v níž se nachází zabezpečená oblast, je trvale uzavřena a v nepřítomnosti oprávněné osoby se uzamyká a zabezpečuje se aktivací EZS. Klíč a kódy k EZS vlastní pouze osoby oprávněné k samostatnému vstupu do zabezpečené oblasti, jejich seznam vlastní bezpečnostní ředitel. Osoby musí mít oprávnění k přístupu k UI SU Důvěrné. Před vstupem do místnosti se musí pracovník identifikovat na bezkontaktní čtečce kontroly vstupu umístěné před vstupem. Pokud tak neučiní, je i přes deaktivaci EZS spuštěna poplachová signalizace na stanovišti ostrahy.

O vstupu do zabezpečené oblasti je veden záznam, do kterého se uvádí:

- datum, čas, jméno a podpis osoby vstupující do objektu
- datum, čas, jméno a podpis osoby opouštějící objekt
- osoby, jimž byl umožněn vstup do objektu – uvádí se datum, čas, jejich jméno, důvod vstupu, podpis doprovázejícího pracovníka, za zápis odpovídá osoba, jež tento vstup umožnila

Úklid v zabezpečeném objektu se standardně provádí 1x týdně (v zabezpečené oblasti jednou za 14 dní). V závislosti na ročním období a v nezbytných případech je možné stanovit i větší počet termínů. V době úklidu je v zabezpečené oblasti stále přítomen oprávněný a poučený pracovník, jež o úklidu provede záznam do Knihy návštěv a vstupů.

8.4 Bezpečnostní opatření při vstupu a odchodu ze zabezpečeného objektu

Před vstupem do zabezpečeného objektu zkontroluje poučená oprávněná osoba neporušenost vstupních dveří a rámu. V případě zjištění poškození musí vyrozumět pracovníka ostrahy a bezpečnostního ředitele a o této události vyhotovit záznam.

Při vstupu do objektu musí pracovník použít čtečku kontroly vstupu umístěnou u vchodových dveří a následně klávesnicí, nacházející se v zabezpečeném objektu, deaktivovat systém EZS. Dále zkontroluje stav oken a vybavení místnosti.

V případě vstupu osoby, jež není pověřeným pracovníkem firmy Security Printing, musí ověřit její totožnost, důvod návštěvy a oprávnění ke vstupu do objektu. Musí provést zápis do Knihy návštěv a vstupů.

Před odchodem ze zabezpečeného objektu ověří pracovník uzavření všech oken a stav vybavení v místnosti. Zkontroluje, zda se v místnosti nenachází utajované dokumenty, pokud tomu tak je, neprodleně je vrátí do úschovného objektu, ale pokud se nejedná o dokumenty, se kterými pracoval, neprodleně vyrozumí bezpečnostního ředitele a dále se řídí jeho pokyny. S dokumenty se dále neseznamuje.

Při odchodu zaměstnanec aktivuje systém EZS, opustí místnost a následně uzamkne dveře do objektu.

Mimo pracovní dobu hlásí zaměstnanec vstup a odchod ze zabezpečeného objektu pracovníkovi ostrahy na recepci, kde je povinen se zapsat.

8.5 Bezpečnostní opatření při vstupu a odchodu ze zabezpečené oblasti

Před vstupem do zabezpečené oblasti zkontroluje poučená oprávněná osoba neporušenost vstupních dveří a rámu. V případě zjištění poškození musí vyrozumět pracovníka ostrahy a bezpečnostního ředitele a o této události vyhotovit záznam.

Při vstupu do objektu musí oprávněná osoba použít čtečku kontroly vstupu umístěnou u vchodových dveří a následně klávesnicí, nacházející se v zabezpečené oblasti, deaktivovat systém EZS. Dále zkontroluje stav okna, neporušenost zámku úschovného objektu a vybavení místnosti. Provede zápis o vstupu do místnosti.

V případě vstupu osoby, jež není oprávněným pracovníkem firmy Security Printing, nebo neoprávněné osoby, musí ověřit její totožnost, důvod návštěvy a oprávnění ke vstupu do objektu. Musí provést zápis do Knihy návštěv a vstupů. V závislosti k oprávnění osoby zabezpečit UI po dobu její přítomnosti v zabezpečené oblasti.

Před odchodem ze zabezpečené oblasti ověří pracovník uzavření všech oken a stav vybavení v místnosti. Zkontroluje, zda se v objektu nenachází utajované dokumenty, pokud tomu tak je, neprodleně je vrátí do úschovného objektu a pokud se nejedná o dokumenty, se kterými pracoval, neprodleně vyrozumí bezpečnostního ředitele, do jejich předání se s nimi dále neseznamuje a zamezí jejich poškození, ztrátě či vyzrazení jejich obsahu nepovolané osobě. Zkontroluje, zda je uzamčen úschovný objekt. Provede zápis o odchodu z místnosti.

Při odchodu zaměstnanec aktivuje systém EZS, opustí místnost a následně uzamkne dveře do objektu.

Mimo pracovní dobu hlásí zaměstnanec vstup a odchod ze zabezpečeného objektu pracovníkovi ostrahy na recepci, kde je povinen se zapsat.

8.6 Pravidla pro pohyb UI v objektu

Pravidla pro pohyb UI jsou tvořena vnitropodnikovou směrnicí, zabývající se administrativní bezpečností. Cílem této směrnice je stanovit takové postupy, jenž povedou k zajištění bezpečnosti UI při jejich zpracovávání, skartaci, přepravě a ukládání, v souladu se zákonem č. 412/2005, o ochraně utajovaných informací.

Zaměstnanci byli proškoleni, jak evidovat UI a jakým způsobem mají být UI přenášeny a jak zajistit jejich bezpečnou přepravu.

8.7 Pravidla pro používání technických prostředků, jejich provozní dokumentace

Technické prostředky používají zaměstnanci, kteří je potřebují k vykonávání své pracovní náplně a byli v jejich používání proškoleni bezpečnostním ředitelem. V případě nefunkčnosti technického prostředku sdělí pracovník, jenž odhalil nedostatek, tuto skutečnost bezpečnostnímu řediteli. Ten je zároveň povinen provádět pravidelné kontroly používaných technických prostředků umístěných v zabezpečené oblasti a předcházet tak případným závadám vedoucím například k snížení ochrany UI.

Systém kontroly vstupu a EZS používá pouze poučená osoba vlastnící identifikační kartu a platný kód. Všechny takové osoby byly proškoleny v manipulaci se systémem EZS a jak postupovat při poruše systému, případně dalších stavech, které mohou v rámci používání nastat. Osoby vlastnící tyto údaje a prostředky musí zamezit jejich ztrátě, záměně či získání a seznámení se s nimi neoprávněnou osobou. V případě takovéto události musí osoba neprodleně tuto skutečnost oznámit bezpečnostnímu řediteli.

Skartovací zařízení používají pouze osoby, jenž byli v jeho používání proškoleni. V zásadě by se mělo jednat o všechny osoby, kterým je umožněn samostatný vstup do zabezpečené oblasti. Skartace UI (UD) se provádí pouze na zařízení certifikovaném NBÚ. Po takovéto skartaci je možné UI (UD) považovat za běžný kancelářský odpad.

Bezpečnostní ředitel (pověřená osoba) zároveň provádí kontrolu i použitých mechanických prostředků (z důvodů koroze, opotřebení atd.). V případě zjištění závady zajistí v co nejkratší době výměnu či opravu poškozeného mechanického prostředku a po dobu oprav zajistí ochranu UI jiným způsobem shodným s plánem zabezpečení.

Provozní dokumentace technických prostředků se uchovává v zabezpečené oblasti a za její úplnost, dodržování stanovených termínů kontrol a revizí je zodpovědný bezpečnostní ředitel. Její součástí jsou dokumentace k systému EZS, ke skartačnímu zařízení, k úschovnému objektu, k mechanickému zámku dveří.

8.8 Pravidla pro manipulaci s klíči a identifikačními prostředky od vstupu do zabezpečené oblasti a klíči od úschovného objektu

Klíče od zabezpečeného objektu

Vstupní dveře do zabezpečeného objektu jsou osazeny jedním mechanickým bezpečnostním zámkem. Celkem existuje 6 klíčů od vchodových dveří. Čtyři z nich jsou vlastněny osobami, jež mají pracoviště v zabezpečené oblasti, jeden je vlastněn bezpečnostním ředitelem a jeden je uložen v zapečetěné krabičce v úschovném objektu rezervních klíčů na stanovišti ostrahy. Všechny klíče jsou opatřeny pořadovým číslem a jsou vlastněny pouze zaměstnanci, jenž mají oprávnění pro seznamování se s UI SU Důvěrné.

Klíče od zabezpečené oblasti

Vstupní dveře do zabezpečené oblasti jsou osazeny jedním mechanickým bezpečnostním zámkem. Celkem existují 4 klíče od vchodových dveří. Dva z nich jsou vlastněny osobami oprávněnými k samostatnému vstupu do zabezpečené oblasti, jeden vlastní bezpečnostní ředitel a jeden je uložen v zapečetěné krabičce v úschovném objektu rezervních klíčů na stanovišti ostrahy. Všechny klíče jsou opatřeny pořadovým číslem a jsou vlastněny pouze zaměstnanci, jenž mají oprávnění pro seznamování se s UI SU Důvěrné.

Pokud dojde ke ztrátě klíče k zabezpečenému objektu nebo oblasti, musí osoba, které klíč patřil, neprodleně vyrozumět bezpečnostního ředitele. Následně musí být provedena kontrola zabezpečené oblasti a objektu, kdy se bude zkoumat zejména neporušenost dveří, systému EZS, úschovného objektu a vybavení zabezpečeného objektu a oblasti. Poté proběhne výměna zámku spojená s náhradou klíčů.

Klíče od úschovného objektu

Klíče od úschovného objektu vlastní ve firmě Security Printing pouze dvě osoby. První z nich je bezpečnostní ředitel, jenž vlastní záložní klíč uložený v zapečetěném obalu. Druhým je pak evidenční pracovník, jenž je určen pro vydávání a přijímání UI uložených v zabezpečeném objektu.

V době nepřítomnosti oprávněné osoby lze úschovný objekt otevřít jen ve výjimečném případě a to odpovědnou osobou, nebo bezpečnostním ředitelem, za přítomnosti minimálně jednoho dalšího pracovníka firmy, obě osoby musí mít oprávnění ke vstupu do zabezpečené

oblasti a k seznamování s UI SU Důvěrné. O této události se vyhotoví záznam, kde bude uveden důvod otevření úschovného objektu, čas otevření a podpisy obou zúčastněných osob.

V případě dlouhodobé nepřítomnosti pracovníka se po rozhodnutí bezpečnostního ředitele předává klíč proti podpisu jeho určenému zástupci.

V případě, že dojde ke ztrátě jakéhokoli z klíčů, musí být o této události okamžitě informován bezpečnostní ředitel a musí urychleně dojít k výměně zámků úschovného objektu.

Kódy systému EZS

Pro ovládání systému EZS se používají dva druhy kódů:

První z nich je tzv. master kód, který se používá pro nastavení systému a práv jednotlivých uživatelů. Master kód je znám oprávněné osobě, odpovědné za nastavení systému. Jako záloha je tento kód uveden i v zapečetěné obálce, uložené v zabezpečeném objektu. V případě změny oprávněné osoby se vždy nastavuje nový master kód.

Druhý z nich je tzv. uživatelský kód, který vlastní každý pracovník oprávněný k přístupu do zabezpečeného objektu, respektive zabezpečené oblasti. Tento kód přiděluje pracovníkům oprávněná osoba vlastnící master kód. Platnost kódu zaniká, pokud pracovník pozbyl oprávnění k přístupu do zabezpečeného objektu či oblasti.

Bezpečnostní ředitel rozhodl, že podle zásad bezpečnostní politiky firmy je každý pracovník povinen minimálně jednou za rok požádat o změnu svého přístupového kódu.

V případě neočekávané nouzové situace je v úschovném objektu na stanovišti ostrahy vedle náhradních klíčů do zabezpečeného objektu a oblasti uložen i kód pro přístup do objektu a oblasti umístěný v zapečetěné obálce. Souhlas s použitím kódu vydává bezpečnostní ředitel, v případě jeho nedostupnosti oprávněná osoba odpovědná za nastavení systému. O použití záložního kódu je povinnost vyhotovit záznam, následně proběhne změna použitého kódu.

Identifikační bezkontaktní karty

Osobám s oprávněním k samostatnému vstupu do zabezpečeného objektu, respektive zabezpečené oblasti je mimo jednotlivých klíčů od místností přidělena i identifikační bezkontaktní karta systému kontroly vstupu. V případě ztráty bezkontaktní karty, je osoba povinna tuto skutečnost neprodleně oznámit bezpečnostnímu řediteli, jenž zajistí zablokování karty. Po dobu než je osobě vystavena nová bezkontaktní karta smí do zabezpečeného objektu vstupovat pouze v doprovodu jiné osoby s oprávněním k samostatnému vstupu do objektu. Svůj příchod osoba uvede do Knihy návštěv a vstupů s odůvodněním tohoto zápisu.

Poučené osoby mají zakázáno půjčovat své klíče či identifikační bezkontaktní karty jiným osobám, vyrábět jejich duplikáty a pokusit se v co největší míře předcházet jejich poškození či ztrátě. Pokud nastane nějaká z výše uvedených situací, je povinností poučené osoby nahlásit tuto událost bezpečnostnímu řediteli, jenž zajistí její nápravu a dočasný náhradní způsob ochrany UI.

8.9 Pravidla pro výkon ostrahy

Ostraha areálu firmy Security Printing, kde se v budově A nachází zabezpečená oblast, se provádí nepřetržitě a to v souladu s požadavky plynoucími z přílohy č. 1 vyhlášky č. 528/2005 o fyzické bezpečnosti a certifikaci technických prostředků. Ostraha je prováděna pracovníky firmy, jenž areál vlastní. V pracovní době je ostraha vykonávána jedním pracovníkem ostrahy na recepci, zároveň sloužící jako stanoviště ostrahy. Na stanoviště ostrahy jsou vyvedeny výstupy EZS zabezpečené oblasti a EZS, EPS a CCTV spadající pod zabezpečení areálu. Mimo pracovní dobu ostrahu vykonávají dva pracovníci bezpečnostní služby. Jeden z nich provádí v náhodném intervalu závislém na vnitřním provozu obchůzky areálu, doba intervalu nepřesahuje 6 hodin. Pracovníci nemají dovoleno samostatně vstupovat do zabezpečeného objektu a zabezpečené oblasti a nejsou osobami oprávněným k přístupu k UI.

Mezi povinnosti pracovníka ostrahy patří kontrola uzamčení všech dveří v areálu. Dále má povinnost kontrolovat všechny osoby vstupující do areálu, v něm se nacházející a vést o nich odpovídající záznamy. Jeho povinností je také hlásit havarijní situace v areálu a snažit se poskytnout odpovídající pomoc osobám v areálu a zasahujícím členům HZS, Policie, vodáren atd.

Oprávněná osoba s přístupem k UI je poučena odpovědnou osobou a během pracovní doby vykonává určitý druh fyzické ostrahy. Zejména jde o kontrolu uzamčení úschovného objektu, oken a vchodových dveří vedoucích do zabezpečené oblasti a zabezpečeného objektu. Kontroluje, zda se v objektu volně nenachází UI. Zjišťuje nedostatky prostředků fyzické bezpečnosti či technického vybavení zabezpečeného objektu, které mohou snížit ochranu UI či způsobit jejich poškození či zničení a v případě takovéhoto zjištění informovat bezpečnostního ředitele. Při mimořádné události neprodleně vyrozumět bezpečnostního ředitele či Policii ČR, HZS atd. V případě přepadení zabezpečeného objektu využít tísňového

systému (tísňového tlačítka) a případně, s ohledem na zdraví své a ostatních přítomných pracovníků, se pokusit o odražení útoku a zadržení pachatele.

Pokud dojde např. k pokusu o odcizení UI, nefunkčnosti prostředků fyzického zabezpečení či systému EZS a dalším nepředvídatelným událostem, jenž mohou vést ke snížení ochrany UI, vyhlašuje se tzv. **Stav ohrožení UI**. Stav vyhlašuje bezpečnostní ředitel, jenž může požádat o pomoc pracovníky ostrahy. Ti při odcizení UI provedou okamžité uzavření areálu a budovy A, provedou kontrolu bezpečnostních záznamů ze systému CCTV v budově a jejím okolí a osobní prohlídku osob, jenž se v areálu nachází. Při nefunkčnosti prostředků fyzického zabezpečení dojde až do doby odstranění nedostatků k posílení ostrahy budovy A, současně bude v zabezpečené oblasti přítomna minimálně jedna poučená osoba.

9 Plán zabezpečení objektu a zabezpečené oblasti v krizových situacích

Mimořádnou (krizovou) situací je *„stav, kdy bezprostředně hrozí, že dojde k vyzrazení nebo zneužití utajované informace“*[9] V případě firmy Security Printing se jedná především o situace popsané v části: 3. Stanovení jednotlivých hrozeb, zranitelnosti a vyhodnocení. Jsou to: hrozba neoprávněného nakládání s UI poučenými osobami; hrozba nakládání s UI neoprávněnou osobou; hrozba poškození, zničení, či neoprávněného nakládání s UI při živelných katastrofách a haváriích; hrozba poškození, zničení UI následkem teroristického útoku; hrozba vyzrazení UI prostřednictvím pasivního odposlechu či operativní techniky; hrozba vyzrazení UI z počítačového systému.

Společnost přijala opatření, kterými se snaží těmto mimořádným situacím předcházet a minimalizovat je. A to především důkladným výběrem zaměstnanců, jejich prověřením na trestní bezúhonnost, jejich pravidelným školením. Dále pak nainstalovanými prostředky fyzické bezpečnosti, režimovými opatřeními a ostrahou objektu, a také pravidelnými kontrolami jak použitých prvků fyzické bezpečnosti, tak i bezpečnosti personální a administrativní.

9.1 Pokyny k ochraně utajovaných informací v případě vzniku mimořádné události

Při zjištění mimořádné události (požáru, havárii inženýrských sítí) musí být okamžitě informován bezpečnostní ředitel, který následné řídí evakuaci zabezpečené oblasti a zajišťuje ochranu UI. V případě, že bezpečnostní ředitel, není v areálu přítomen, provádí tyto činnosti poučený zaměstnanec oprávněný k samostatnému vstupu do zabezpečené oblasti.

V případě propuknutí požáru (či havárie inženýrských sítí) se zaměstnanci řídí požární poplachovou směrnicí či interní směrnici pro mimořádné události. O takovéto mimořádné situaci v areálu firmy je nutné, kromě HZS, vyrozumět i Policii ČR.

V případě teroristického útoku nebo při stavu ohrožení učiní zaměstnanec, jenž se v té chvíli nachází v zabezpečeném objektu, nezbytná opatření k odvrácení hrozby a přivolání pomoci. Další pokyny v takovéto situaci pak vydává bezpečnostní ředitel, či jím pověřená osoba v součinnosti s pracovníky ostrahy a přivolané pomoci.

V případě živelné katastrofy se zaměstnanci řídí interní směrnicí pro mimořádné události v závislosti na rozsahu katastrofy.

Cílem opatření by mělo být zamezení přístupu a manipulace s UI nepovolanou osobou. Při zjištění takovéto skutečnosti nebo při jakékoli krizové situaci je povinností informovat bezpečnostního ředitele. Bezpečnostní ředitel (odpovědná osoba) je povinen skutečnost zaevidovat, vyhodnotit a neprodleně o ní vyrozumět NBÚ a orgánu či organizaci, jenž firmě UI poskytla. Dále musí do zprávy uvést opatření, která byla přijata k nápravě a prevenci takovýchto událostí.

9.2 Evakuace

Při vyhlášení evakuace musí začít osoby, s oprávněním k přístupu k UI, přítomné v zabezpečeném objektu s neprodlenou přípravou UI k evakuaci. Takovýto pokyn vydává bezpečnostní ředitel (odpovědná osoba). Pracovníci začnou UD ukládat do připravených schránek, jenž se v zabezpečeném objektu nachází v rámci platné legislativy a následně schránky vloží do úschovného objektu. Bezpečnostní ředitel mezitím vyhlásí stav ohrožení UI a vyhotoví dvě kopie seznamu UI. Jeden výtisk vloží do úschovného objektu a zbylý si ponechá. Následně se úschovný objekt uzamkne, aktivuje se systém EZS a uzamkne se i zabezpečená oblast. Zaměstnanci se dále řídí pokyny bezpečnostního ředitele a společně opustí budovu po vyznačených evakuačních trasách. V případě nepřítomnosti bezpečnostního ředitele či odpovědné osoby vede evakuaci jiná pověřená osoba.

10 Závěr

Z práce je patrné, že bezpečnost utajovaných informací má striktní pravidla. Bylo nejprve potřeba seznámit se se všemi zákony a vyhláškami potřebnými k řešení problematiky. Hlavním zdrojem informací se stala novela vyhlášky 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb., ve které je v příloze č. 1 uvedená přesná struktura projektu fyzické bezpečnosti a bodové ohodnocení jednotlivých certifikovaných prostředků. Z této struktury jsem v bakalářské práci vycházel. V práci byly použity pouze prostředky s platným bezpečnostním certifikátem uvedené ve Věstníku NBÚ.

Hlavním problémem v oblasti fyzické bezpečnosti bývá podcenění hrozícího rizika. Proto se práce poměrně podrobně věnuje analýze rizik, která mohou nastat a jejich následnému vyhodnocení.

Dalším problémem v oblasti fyzické bezpečnosti jsou v dnešní době i finanční náklady spojené s realizací projektu. Mnohdy jsou hlavním kritériem při jeho posuzování. V práci je přihlíženo k hodnotě uskladněných informací a jsou zváženy škody spojené s jejich případným odcizením, poškozením či zničením. Z těchto důvodů jsou náklady použité na prostředky fyzické bezpečnosti určené k zabezpečení zabezpečeného objektu a zabezpečené oblasti úměrné hodnotě uložených informací. Při jejich výběru nesmí dojít k snížení stupně ochrany, kterou pro jednotlivé stupně utajovaných informací stanovuje zákon.

V průběhu realizace projektu zabezpečené oblasti fiktivní firmy Security Printing došlo ke stavebním úpravám podle právních předpisů. Do okna místnosti, kde se nalézá zabezpečená oblast, byla umístěna mříž. Stěna z lehké stavební konstrukce byla zpevněna bezpečnostní příčkou.

Fyzické zabezpečení objektu je ovlivněno stále se zrychlujícím trendem vývoje elektronických zařízení, které se stávají dostupnější i pro menší subjekty a jsou používány ve stále větším množství.

Domnívám se, že se podařilo dosáhnout cíle práce, jímž bylo vytvoření projektu fyzického zabezpečení objektu podle platných zákonů a norem a zajistit efektivní ochranu uskladněných utajovaných informací.

11 Citace a seznam použitých zdrojů

[1] Zákon č. 412/2005 Sb. ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, , § 2, písm. h), IN: *Sbírka zákonů České republiky. 2005,* Dostupný také z: http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/uplne-zneni-zakona-c-4122005/

[2] Příloha č. 1 k novele vyhlášky č. 528/2005., ze dne 21. 12. 2011 o fyzické bezpečnosti a certifikaci technických prostředků ve znění vyhlášky č. 19/2008, str. 11, bod 3. Hranice objektu, Dostupná také z: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5282005/

[3]Zákon č. 412/2005 Sb. ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, § 25, odst. 1) a odst. 2), IN: *Sbírka zákonů České republiky. 2005,* Dostupný také z: http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/uplne-zneni-zakona-c-4122005/

[4]Příloha č. 1 k novele vyhlášky č. 528/2005., ze dne 21. 12. 2011 o fyzické bezpečnosti a certifikaci technických prostředků ve znění vyhlášky č. 19/2008, str. 8, odstavec 2. Zabezpečené oblasti a jejich uzamykací systémy, Dostupná také z: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5282005/

[5] Příloha č. 1 k novele vyhlášky č. 528/2005., ze dne 21. 12. 2011 o fyzické bezpečnosti a certifikaci technických prostředků ve znění vyhlášky č. 19/2008, str. 19, bod 6.1.4. Fyzická bariéra typ 1, Dostupná také z: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5282005/

[6]Příloha č. 1 k novele vyhlášky č. 528/2005., ze dne 21. 12. 2011 o fyzické bezpečnosti a certifikaci technických prostředků ve znění vyhlášky č. 19/2008, str. 19, bod 10. Zařízení proti pasivnímu a aktivnímu odposlechu utajovaných informací, Dostupná také z: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5282005/

[7][8]Příloha č. 1 k novele vyhlášky č. 528/2005., ze dne 21. 12. 2011 o fyzické bezpečnosti a certifikaci technických prostředků ve znění vyhlášky č. 19/2008, str. 24, bod 11. Podmínky používání certifikovaných technických prostředků po uplynutí doby platnosti jejich certifikátů, Dostupná také z: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5282005/

[9]Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů, str. 1, §2 Vymezení pojmů, písm. h), Dostupná také z: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5282005/

UHLÁŘ, J. *Technická ochrana objektů 2. díl: Technické zabezpečovací systémy 2*.Vyd. 2. Praha: Policejní akademie České republiky, 2009. ISBN 978-80-7251-313-0

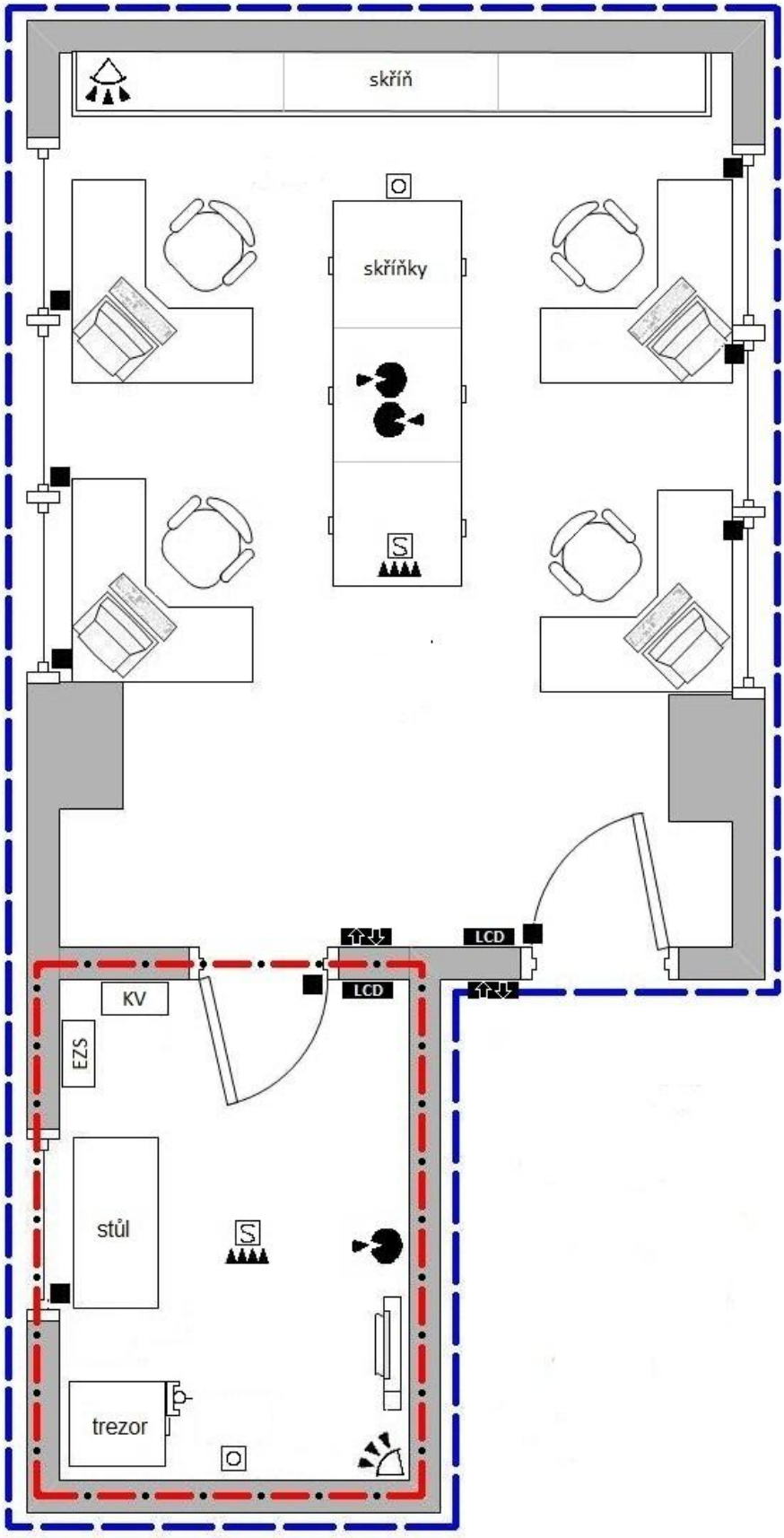
LÁTAL, I. a M. ŠTANTEJSKÝ. *Bezpečnostní zásady ochrany podniku*. Praha: Prospektum, 2001. ISBN 80-7175-091-3.

Trezorové normy. Jinova [online]. Jinova: Trezory a vše kolem nich© 2012 [cit. 2012-03-03]. Dostupné z: http://www.jinova.cz/trezorove-normy

Seznam certifikovaných technických prostředků. Národní bezpečnostní úřad [online].NBÚ© 2012 [cit.2012-03-03]. Dostupné z: http://www.nbu.cz/cs/informacni-centrum/seznamy/seznam-certifikovanych-technickych-prostredku/

Přílohy k nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb.

Příloha 1: Rozmístění prostředků fyzické bezpečnosti v zabezpečeném objektu a zabezpečené oblasti



Legenda

Zabezpečený objekt

Zabezpečená oblast

PIR čidlo

Detektor rozbití skla

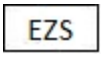
Požární čidlo

Magnetický kontakt

Otřesový senzor

Tísňové tlačítko

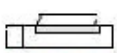
LCD klávesnice systému EZS



Ústředna systému EZS

Čtečka kontroly vstupu

Řídící jednotka kontroly vstupu



Skartační stroj

Příloha 2: Seznam použitých zkratek a pojmů

NBÚ Národní bezpečnostní úřad

UI utajovaná informace

UD utajovaný dokument

SU stupeň utajení

EZS elektronická zabezpečovací signalizace

EPS elektronická požární signalizace

CCTV (Closed-Circuit television) uzavřený televizní okruh využívající bezpečnostních kamer

OFO osvědčení fyzické osoby

ČSN označení českých technických norem

TNI technické normalizační informace

Tamper kontakt – magnetický kontakt detekující otevření, sejmutí krytu atd.

PIR (*Passive Infrared Sensor)* pasivní infračervené čidlo sloužící k detekci pohybu osob

Odpovědná osoba - osoba, která je ve firmě odpovědná za ochranu UI a je ji zákonem dáno plnění povinností z tohoto zákona vyplívajících

Bezpečnostní ředitel - *„Funkci bezpečnostního ředitele může vykonávat i odpovědná osoba sama, jinak je bezpečnostní ředitel přímo podřízen odpovědné osobě. Bezpečnostní ředitel zajišťuje a plní povinnosti stanovené mu písemně odpovědnou osobou v rozsahu tohoto zákon. Funkci bezpečnostního ředitel může vykonávat pouze osoba, která splňuje podmínky přístupu k UI takového SU, ke kterým bude mít při výkonu této funkce přístup.“* [1]

[1] Zákon č. 412/2005 Sb. ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, § 71 Bezpečnostní ředitel

Příloha 3: Tabulka cen použitých technických prostředků

Název	Cena za kus(v Kč)	Počet kusů	Celková cena (v Kč)
Úschovný objekt TSS 125 M	20 990	1	20 990
Trezorový zámek Mauer	1548	1	1 548
Bezpečnostní dveře Sherlock 330/2	13 154	2	26 308
Bezpečnostní kování Rostex R1	1 966	2	3 932
Cylindrická vložka FAB 2402B	1 500	2	3 000
Kontrola vstupu	5 100	2	10 200
Bezkontaktní čtečka karet	3 300	2	6 600
Ústředna EZS Siemens IC60M-8	4 692	1	4 692
Klávesnice IKP6 - 03	2 410	2	4 820
Detektor IMR 270C	3 439	2	6 878
Detektor rozbití skla DL 500	932	3	2 796
Otřesový senzor ES 400	2 890	1	2 890
Magnetické kontakty IMKW6-10	1 690	9	15 210
Tísňové tlačítko HB 105	390	2	780
Požární hlásič SD-282ST	732	2	1 464
Siréna SA 913F	583	1	583
Skartační stroj Martin Yale 2000 CC	5 342	1	5 342
Celková cena			**118 033**

Ceny jsou pouze orientační a jsou vybrány z různých zdrojů (většinou přímo od výrobců, či jejich výhradních prodejců) dne 2. 4. 2012. V případě výběru jiných technických prostředků nesmí být vybrány prostředky s menším bodovým ohodnocením, než výše uvedené, v opačném případě by došlo ke snížení hodnocení fyzické bezpečnosti zabezpečeného objektu a zabezpečené oblasti.