

Přírodovědecká fakulta Jihočeské univerzity

Bakalářská práce:

Vytvoření projektu fyzické bezpečnosti

Vypracovala: Kateřina Schneiderová

Školitel: Ing. Petr Šedivý

České Budějovice 2011

Bibliografické údaje

Schneiderová K., 2011: Vytvoření projektu fyzické bezpečnosti.

[Physical security precautions B.A. Thesis, in Czech.] – 31 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Anotace

Vytvoření systému opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajované informaci, nebo alespoň zaznamenat pokus o něj. Je nutné vybrat fyzické osoby, které budou mít přístup k utajované informaci, jejich výchova a obrana. Nakonec nesmíme zapomenout na administrativní bezpečnost - systémová opatření při tvorbě, příjmu, evidenci, zpracování, ukládání, přepravě a archivaci utajovaných informací.

Abstrakt

Creating a system of measures to prevent unauthorized person or impede access to classified information, or at least attempt to record it. You must select individuals who will have access to classified information, training and defence. Finally, we must not forget the administrative security – system measures in the production, reception, registration, processing, storage, transport and archiving of classified information.

Prohlašuji, že svoji bakalářskou práci jsem vypracovala 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 – v úpravě vzniklé vypuštěním vyznačených částí archivovaných Přírodovědeckou fakultou - 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.

V Českých Budějovicích dne 1. 3. 2011

Podpis:

Poděkování

Ráda bych poděkovala panu Ing. Petrovi Šedivému za konzultace a odbornou asistenci.

Obsah

1	Úvod	1
2	Metodika.....	2
2.1	Zadání práce	2
2.2	Pojmy	2
2.3	Stanovení míry rizika	3
2.4	Stanovení objektu	3
2.5	Technické prostředky zabezpečeného objektu	4
2.6	Stanovení zabezpečené oblasti	4
2.7	Technické prostředky zabezpečené oblasti	5
2.8	Certifikace	5
2.9	Tabulka bodového ohodnocení	6
2.10	Technická dokumentace fyzické bezpečnosti	10
2.11	Uplynutí doby platnosti certifikátu	10
2.12	Funkční zkouška	10
2.13	Provozní řád	11
2.14	Ostraha	13
2.15	Stav ohrožení	13
2.16	Kontrola zabezpečené oblasti	14
2.17	Mimořádná situace	14
3	Ochrana dokumentů	17
4	Národní bezpečnostní úřad	18
4.1	NBÚ	18
4.2	Věstník	18
4.3	Fyzická bezpečnost	19
4.4	Certifikace	19
5	Kalkulace.....	20
6	Závěr.....	22
7	Slovníček pojmů.....	23
8	Bibliografie.....	24
9	Příloha	26

1 Úvod

Ochrana utajovaných informací je oblastí ochrany informací, která je v současnosti vymezena a upravena zákonem č. 412/2005 Sb. o ochraně utajovaných informací a bezpečnostní způsobilosti. Ačkoli je tato problematika dostatečně obsažena v zákonu a v dalších právních předpisech, je natolik složitá, že její zvládnutí vyžaduje jak specifické znalosti, tak praktické zkušenosti.

Nezbytným předpokladem pro úspěšné bezpečnostní řízení je bezchybná realizace přijatých opatření v oblastech administrativní, fyzické, personální, informační, komunikační, kryptografické a průmyslové.

Řádné fyzické zabezpečení dat musí odolat zlodějům i lidem z vlastních řad. Musí se také zajistit ochrana před haváriemi nebo živelnými pohromami. Nesmí se zapomínat ani na prevenci a minimalizaci chemického nebo fyzického poškozování dokumentů nebo jejich rozpadu.

Systém se zabezpečuje od běžných a dostupnějších prostředků k těm méně známým a méně dostupným. Pokud budeme systém správně zabezpečovat, dokážeme tím předejít útokům od útočníků. Při vytváření zabezpečení bereme na vědomí, že útočníci mají určité schopnosti a vědomosti, vybavení a prostředky. V případě, že se bude dodržovat správný postup při zabezpečování, snižuje se tím riziko útoku. Zneužití údajů je v dnešní době velmi nebezpečné, a proto je třeba tématu bezpečnost věnovat velkou pozornost. Je důležité uvědomit si, že při zvyšování zabezpečení dochází ke snižování komfortu. Neměl by se opomíjet fakt, že dochází nejen k vylepšování technik zabezpečení, ale také ke zlepšování schopností útočníků.

Při vybírání zabezpečovacího systému by neměla být hlavním kritériem cena, i když ta je hodně důležitá. Cena by měla být v poměru k hodnotě majetku, který chceme chránit. Finanční náklady se odvíjí od ceny nemovitostí a jejího vybavení. Je tedy rozdíl, jestli chceme chránit byt, rodinný dům nebo komerční objekt. Jistě bychom na zabezpečení neměli šetřit. Spolehlivý a kvalitní zabezpečovací systém by měl být normalizován a schválen Českou asociací pojišťoven.

V dnešní době se mnohem častěji než o fyzické bezpečnosti hovoří o ochraně osobních údajů. Pokud fyzická osoba může být ze shromážděných údajů přímo nebo nepřímo identifikována, pak jsou tyto údaje údaji osobními. Znakem osobního údaje tedy je, že seskupením údajů vznikne taková identifikace subjektu, která nelze zaměnit s jiným subjektem.

Jelikož s ochranou osobních údajů se každý z nás setkává téměř denně, zajímalo autorku, jak se pracuje v oboru fyzického zabezpečení. Jako cíl práce se zaměřila na seznámení se s problematikou, a poté vytvoření projektu fyzické bezpečnosti s pomocí odborníka. Hlavním důvodem bylo získat praktické zkušenosti a vědění o tom, jak to funguje v praxi.

2 Metodika

2.1 Zadání práce

Při určení objektů a zabezpečených oblastí včetně jejich hranic a určení kategorií, tříd a bodového ohodnocení se používá příloha č. 1 k vyhlášce č. 528/2005 Sb., ve znění vyhlášky č. 19/2008 Sb., jako pomocnou příručku či materiál, ve kterém najdeme přesný postup při vytváření projektu fyzické bezpečnosti.

Projekt fyzické bezpečnosti byl vytvořen pro fiktivní společnost UAI, a.s., která získala státní zakázku na vyhodnocení dislokačních plánů z pohledu ohrožených lokalit živelnou pohromou. Státní zakázka se zabývá pouze papírovými dokumenty SU Důvěrné v rozsahu cca padesáti dokumentů. Firma má sídlo v administrativním objektu a na zakázce pracuje šest osob, které mají osvědčení na SU Důvěrné. Firma v souladu se ZOUI absolvovala bezpečnostní řízení na NBÚ a bylo jí vydáno osvědčení na seznamování s UI SU Důvěrné. Toto osvědčení je nutné rozšířit na tvorbu a ukládání UI do SU Důvěrné tak, aby společnost splňovala podmínku podle § 16 odst. 1 písm. c) ZOUI zajištěním ochrany UI personální, administrativní a fyzickou bezpečností a bezpečností IS. Tento dokument řeší oblast fyzické bezpečnosti. Fyzickou bezpečností je ve společnosti chápán systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k UI, popřípadě přístup nebo pokus o něj zaznamenat.

Takto upravený projekt fyzické bezpečnosti bude vyhovovat požadavkům na zajištění bezpečnosti osobních a důvěrných informací dle zákona č. 101/2000 Sb. ochrana osobních dat a dle zákona č. 513/1991 Sb. a dle zákona č. 514/1991 Sb. Obchodní zákoník.

2.2 Pojmy

Je důležité uvědomit si, co jednotlivé pojmy znamenají:

- objektem budova nebo jiný ohraničený prostor, ve kterém se nacházejí zabezpečené nebo jednací oblasti
- hranicí zabezpečené oblasti nebo jednací oblasti stavebně nebo jinak viditelně ohraničený prostor
- vstupem do objektu, zabezpečené oblasti nebo jednací oblasti místo určené pro vstup a výstup osob a místo určené pro vjezd a výjezd dopravních prostředků
- dopravními prostředky pozemní, podzemní, vzdušné a vodní prostředky určené k přepravě osob, předmětů a materiálu
- provozovatelem objektu odpovědná osoba popřípadě osoba jí k tomu pověřená
- hrozbou možnost vyzaření nebo zneužití utajované informace při narušení fyzické bezpečnosti
- rizikem pravděpodobnost, že se určitá hrozba uskuteční
- mimořádnou situací stav, kdy bezprostředně hrozí, že dojde k vyzaření nebo zneužití utajované informace
- technickým prostředkem bezpečnostní prvek, jehož použitím se zabraňuje, ztěžuje nebo oznamuje narušení ochrany objektu, zabezpečené oblasti nebo jednací oblasti a dále ničí utajované informace
- úschovným objektem trezor, uzamykatelná skříň nebo jiná schránka stanovená v příloze č. 1 této vyhlášky

- technickým zařízením vojenský materiál, zejména elektronická, foto-technická, chemická, fyzikálně-chemická, radiotechnická, optická a mechanická vojenská technika a vojenská výzbroj, který obsahuje utajovanou informaci
- útočником fyzická osoba, která vyvíjí činnost s cílem překonat technické prostředky a další překážky sloužící k zabezpečení ochrany utajovaných informací. [1]

2.3 Stanovení míry rizika

Při zabezpečování objektu je v podstatě prováděna prevence. Je velmi důležité uvědomit si potenciální nebezpečí. Proto se v projektu fyzické bezpečnosti stanovují jednotlivé hrozby a zranitelnosti. Při stanovení hrozeb se musí brát na vědomí, kdo může být potenciální útočník, a jak se před ním bránit, ale také důvod útoku (vyzrazení). Vyzrazení může být neúmyslné, ale i úmyslné za účelem např. zisku. Z toho vyplývá, že k dobrému zabezpečení patří i důkladný výběr pracovníků, kteří budou mít přístup k UI, jejich školení a kontrola. Proto byla v projektu fyzické bezpečnosti stanovena hrozba neoprávněného nakládání s UI jak poučenou osobou, tak i osobou nepovolanou. Při ohrožení dokumentů živelnou pohromou může dojít k poškození nejen ohněm, kouřem, vodou a při jejich odstraňování, ale existuje i hrozba neoprávněného nakládání s UI při porušení bezpečnostních opatření při živelné pohromě. Poslední velkou hrozbou je hrozba vyzrazení UI pasivním odposlechem nebo operativní technikou. Tato hrozba se dá minimalizovat pravidelným prováděním kontrol a dodržováním režimových opatření.

U jednotlivých hrozeb se musí určit míra rizika (malá, střední, velká), ze které vyplývá celková míra rizika. Tato celková míra rizika je důležitá z pohledu fyzické bezpečnosti, protože na základě toho se dále porovnávají bodová ohodnocení přijatých opatření fyzické bezpečnosti s tabulkou hodnot nejnížší míry zabezpečení zabezpečené oblasti, viz příloha. Celková míra rizika byla stanovena na hodnotu střední. Když se podíváme do tabulky hodnot nejnížší míry zabezpečení zabezpečené oblasti SU Důvěrné, vidíme, že bodové hodnocení přijatých opatření fyzické bezpečnosti musí být minimálně 14 bodů.

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

Tabulka 3.1: Tabulka bodových hodnot nejnížší míry zabezpečení zabezpečené oblasti

2.4 Stanovení objektu

Objekt se zabezpečenou oblastí se nachází v areálu fiktivní firmy UAI, a.s. v areálu JČU v Českých Budějovicích. V areálu se nachází tři administrativní budovy B1, B2, B3 a dvě garáže. Zabezpečenou oblastí je místnost ve 3. NP budovy B1.

Při určení objektu je rozhodující ta část objektu, která má nejnížší odolnost. Stěny, podlahy a stropy mohou být pevné stavební konstrukce, lehké stavební konstrukce nebo vylehčené konstrukce, která pouze chrání před větrem. Objekt, místnosti č. 307 a č. 308, je lehké stavební konstrukce a má průlezný otvor. I přesto, že byla splněna podmínka, že průlezný otvor se nachází více jak 5,5 m nad terénem a nelze k němu jednoduše proniknout,

byly provedeny stavební úpravy a všechny průlezné otvory byly nahrazeny lehkou sádrokartonovou konstrukcí z důvodu většího zabezpečení.

Další důležitá část je stanovení hranic objektu. Hranice zabezpečeného objektu tvoří dvě místnosti č. 329 a č. 309b. Obě místnosti jsou administrativní. Stropy a stěny jsou pevné stavební konstrukce. Jelikož se obě místnosti nachází ve 3. NP, opět splňují podmínku, že spodní hranice průlezného otvoru, tedy okna, se nachází více jak 5,5 m nad terénem a nelze k němu jednoduše proniknout. V okamžiku, kdy se provede kontrola, že objekt a jeho hranice splňují výše uvedené požadavky, může se určit, že takto ohraničený objekt splňuje podmínky objektu typu 2 s bodovým hodnocením 2 body dle vyhlášky 528/2005 Sb. Bodové hodnocení je podrobněji vysvětleno níže.

2.5 Technické prostředky zabezpečeného objektu

Objekt je jedna místnost na dvou místech oddělená lehkou sádrokartonovou zdí. Tím opticky rozděluje místnost na tři části. Objekt má šest oken, každé z nich je zabezpečeno certifikovaným detektorem rozbití skla Glass Trek typu 3 (3 body).

V místnosti se nachází tři detektory pohybu rozmístěné tak, aby pokryly celou plochu místnosti č. 308. V objektu je umístěno jedno tísňové tlačítko. To je používáno zaměstnanci při pocitu osobního ohrožení. Zařízením elektrické požární signalizace je kouřový detektor umístěný na stropě v místnosti č. 308. Hlásič je certifikovaný NBÚ. Vstup do objektu je ovládán klávesnicí, která se nachází za dveřmi uvnitř objektu. Kontrola jediného možného vstupu do zabezpečeného objektu je typu 2 (2 body). Tato kontrola vstupu je ovládána bezkontaktní čtečkou karet, kterou je umístěna před vstupní dveře zabezpečeného objektu. Oprávněná osoba se tedy musí identifikovat kartou na čtečce. Pokud se neidentifikuje, bude přes deaktivaci EZS spuštěn poplachový signál na stanovišti ostrahy v recepci budovy B1. Všechny použité technické prostředky splňují podmínku certifikace a certifikáty jsou platné.

2.6 Stanovení zabezpečené oblasti

Určení typu zabezpečené oblasti je, stejně jako u určení objektu, dáno nejméně odolným prvkem její hranice. Zabezpečenou oblastí je jedna místnost č. 307. Do této místnosti se vstupuje jedním vchodem ze zabezpečeného objektu. Sousedí tedy s místností č. 308 a ze západní strany s místností č. 329. Jižní stěna, ve které je průlezný otvor, okno vybavené žaluziemi, je součástí opláštění budovy. Okno splňuje podmínky, že se nachází více jak 5,5 m nad terénem a nelze k němu jednoduše proniknout ze střechy nebo za pomoci hromosvodů, okapů, stromů...

Zabezpečená oblast prošla stavební úpravou a skleněná výplň, mimo okna, byla nahrazena lehkou stavební konstrukcí. Oblast slouží nejen jako pracoviště s UI, ale také jako jejich úložna. Musí být proto vybavena potřebnými technickými prostředky. Technické prostředky musí být certifikované, jelikož to ukládá zákon 412/2005 Sb.

Fyzickou bezpečnost tvoří systém opatření, jehož cílem je zabránit nepovolané osobě v přístupu do zabezpečené oblasti nebo zabránit poškození, znehodnocení, zničení či jinému ohrožení UI. Fyzická bezpečnost je soubor opatření, který zabraňuje neoprávněnému nakládání s UI nebo vniknutí nepovolané osoby do zabezpečené oblasti.

Vytvoření fyzické bezpečnosti má:

- odradit pachatele
- znemožnit pokus o vloupání
- ztížit postup pachatelů

- zajistit zásah bezpečnostních složek, a tím zvýšit pravděpodobnost dopadení.

2.7 Technické prostředky zabezpečené oblasti

Zabezpečená oblast je vybavena skříňovým trezorem typu ASJ 1/I certifikovaným NBÚ do 20. 5. 2013. Tento úschovný objekt je typu 3 (3 body) a je osazen certifikovaným zámkem typu 2 (2 body). Zámek splňuje požadavky bezpečnostní třídy B dle ČSN EN 130. Skříňový trezor je zabezpečen otřesovým detektorem SAFE PROTECTOR (950) typu 3 (3 body).

Certifikované bezpečnostní protipožární dveře typu PYROSAFE jsou pevné konstrukce, nevykazují žádné známky poškození, které by mohly bránit pokusům identifikovat neoprávněný vstup. Dveře do zabezpečené oblasti jsou osazeny bezpečnostní cylindrickou vložkou 2502 BDN SGHK 4 DYNAMIC PLUS a uzamykací systém je typu 3 (3 body). Zámek je certifikovaný NBÚ a jeho komponenty splňují požadavky bezpečnostní třídy 4 podle ČSN P ENV 1627. Jediné okno je zabezpečeno detektorem rozbití skla Glass Trek typu 3 (3 body) a je vybaveno žaluziemi. V zabezpečené oblasti se nachází detektor pohybu umístěný tak, aby pokryl celou plochu oblasti. Oblast je vybavena certifikovaným skartačním strojem REXEL MERCURY, který je nutný pokud se pracuje s papírovými dokumenty.

Ke vstupu do oblasti se používá jediný možný vchod. Kontrola vstupu ACS – LINE je typu 2. Kontrola vstupu je ovládána bezkontaktní čtečkou karet, která je umístěna před vstupními dveřmi do zabezpečeného oblasti. Pokud se tedy oprávněná osoba neidentifikuje kartou na čtečce, bude přes deaktivaci EZS přenesen signál na stanoviště ostrahy. Certifikovaný kouřový detektor je umístěný na stropě zabezpečené oblasti.

V objektu i zabezpečené oblasti se nachází zařízení elektrické zabezpečovací signalizace včetně komponent, které splňují požadavky podle ČSN EN 50 134 - 1 pro stupeň zabezpečení 3 (střední až vysoké riziko). Ústředna je nainstalovaná v zabezpečené oblasti, tedy v místnosti č. 308.

O jednotlivých komponentech byla zmínka již výše, jedná se o:

- ústředna EZS DIGIPLEX EVO 192 PARADOX SECURITY SYSTEMS
- detektor pohybu PIR
- tísňová tlačítka ELM-PA-G3-W
- detektor otřesu SAFE PROTECTOR
- detektor rozbití skla GLASS TREK
- magnetické kontakty MAS 353
- hlásič požáru kouřový optický 2351E
- ovládací klávesnice PSD-CJ 1000
- siréna instalovaná na chodbě před vstupem do zabezpečeného objektu a na stálém stanovišti ostrahy

Všechny technické prostředky splňují podmínku certifikace a jsou platné.

2.8 Certifikace

Seznam certifikovaných technických prostředků zveřejňuje Věstník. Věstník je periodická publikace, kterou vydává Národní bezpečnostní úřad pro veřejnost. Obsahuje řadu důležitých informací z oblasti ochrany UI a bezpečnostní způsobilosti. Důraz je kladen na informace, které svým charakterem vymezuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, zejména § 137 písm. g. Současně Věstník informuje o řadě

zásadních opatření, které přijal Národní bezpečnostní úřad, včetně komentářů a stanovisek k novým právním předpisům v uvedených oblastech. Věstník vychází dle potřeb NBÚ a čtenářského zájmu, nejméně však dvakrát do roka. [5]

U každého technického prostředku ve Věstníku nalezneme:

- evidenční číslo (číslo certifikátu)
- název
- označení
- výrobce
- držitel (jméno a kontakt)
- kategorie
- bodové hodnocení
- platnost certifikátu

Tyto základní informace umožňují dobrou orientaci v dokumentu, díky které si každý může vybrat takový certifikovaný technický prostředek, který odpovídá bodovému hodnocení, které si sám určil, aby splnil podmínky zabezpečení na určitý SU. Jelikož Věstník zobrazuje kontaktní údaje poskytovatele technických prostředků, je proto velice jednoduché zažádat o certifikát, který je třeba doložit v projektu fyzické bezpečnosti.

Společnosti, které poskytují certifikované prostředky, jsou ochotné na požádání zaslat kopie certifikátů. Některé společnosti dokonce poskytují kopie certifikátů na svých webových stránkách, jsou tedy volně k stažení.

2.9 Tabulka bodového ohodnocení

Po zvolení všech bezpečnostních opatření, tj. vybrání vhodných certifikovaných technických prostředků, provedení lehkých stavebních úprav atd., se vyplnila tabulka bodového ohodnocení opatření fyzické bezpečnosti takto:

<p>Název: Místnost 307 ve 3. NP, budova B1 v sídle společnosti UAI, a.s., Branišovská 31, České Budějovice</p> <p>Kategorie: Důvěrné</p> <p>Třída: Třída II</p> <p>Typ: Typ 2</p> <p>Účel zabezpečené oblasti: Místnost č. 307 slouží jako úložna UI SU Vyhrazené nebo Důvěrné a pro zpracování nebo vytváření UI SU Vyhrazené nebo Důvěrné.</p>		
BEZPEČNOSTNÍ OPATŘENÍ	TYP	BODOVÉ OHODNOCENÍ
Úschovné objekty	<input type="checkbox"/> T. 4 – 4 body <input checked="" type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS1= 3

Zámky úschovných objektů	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input checked="" type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS2= 2
Celkové hodnocení úschovného objektu a jeho zámku	$S1 = SS1 \times SS2$	S1= 6
Zabezpečené oblasti	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input checked="" type="checkbox"/> T. 1 – 1 bod	SS3= 1
Uzamykací systémy zabezpečené oblasti	<input type="checkbox"/> T. 4 – 4 body <input checked="" type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS4= 3
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	$S2 = SS3 \times SS4$	S2= 3
Objekt UI	<input type="checkbox"/> T. 4 – 5 bodů <input type="checkbox"/> T. 3 – 3 body <input checked="" type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	S3= 2
Kontrola vstupu	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input checked="" type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS6= 2
Režim návštěv v objektu UI a) Návštěvy s doprovodem b) Návštěvy bez doprovodu c) Návštěvy bez kontroly	<input checked="" type="checkbox"/> ad a) – 3 bod <input type="checkbox"/> ad b) – 1 bod <input type="checkbox"/> ad c) – 0bodů	SS7 = 3
Celkové hodnocení kontroly vstupu	$S4 = SS6 + SS7$	S4= 5
Ostraha	<input type="checkbox"/> T. 5 – 5bodů <input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input checked="" type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS8= 2
Zařízení elektrické zabezpečovací signalizace	<input type="checkbox"/> T. 4 – 4 body <input checked="" type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS91= 2
Instalace zařízení elektrické zabezpečovací signalizace	<input type="checkbox"/> T. 4 – 4 body <input checked="" type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS92= 3
Mezivýsledek (SS 9)		SS9= 2

Celkové hodnocení ostrahy a systému EZS	S5 = SS8 + SS9	S5= 4
Fyzické bariéry	<input type="checkbox"/> T. 7- 12 bodů <input type="checkbox"/> T. 6 – 9 bodů <input type="checkbox"/> T. 5 – 7 bodů <input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input checked="" type="checkbox"/> T. 1 –1 bodů	SS10= 1
Kontrola vstupu v přístupových bodech fyzické bariéry a) Kontrola je realizována b) Kontrola není realizována	<input type="checkbox"/> ad a) – 1 bod <input checked="" type="checkbox"/> ad b) – 0 bodů	SS11= 0
Namátkové vstupní a výstupní prohlídky a) Prohlídky jsou prováděny b) Prohlídky nejsou prováděny	<input type="checkbox"/> ad a) – 1 bod <input checked="" type="checkbox"/> ad b) – 0 bodů	SS12= 0
Perimetrický detekční systém (PDS)	2 body	SS13= 0
Bezpečnostní osvětlení perimetru	2 body	SS14= 0
Celkové hodnocení ochrany perimetru	S6 = (SS10 x SS11) + SS12 + SS13 + SS14 + SS15	S6= 0

Tabulka 3.2: Tabulka bodového ohodnocení opatření fyzické bezpečnosti

Záhlaví tabulky musí obsahovat:

- název zabezpečené oblasti
- kategorii zabezpečené oblasti
- třídu zabezpečené oblasti
- druh jednacích oblastí
- účel, ke kterému má zabezpečená oblast sloužit

Tabulku bodového ohodnocení opatření fyzické bezpečnosti se musí zpracovat pro každou zabezpečenou oblast. Každé bezpečnostní opatření má svůj název, typ (počet bodů) a bodové hodnocení. Jednotlivé body se mezi sebou podle vzoru v tabulce buď vynásobí, nebo sečtou. Poté se celkové hodnoty, získané vyplněním tabulky bodového ohodnocení opatření fyzické bezpečnosti v zabezpečené oblasti, porovnají s tabulkou bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti.

Bodové ohodnocení se přiděluje těmto bezpečnostním opatřením:

Povinné:

- úschovné objekty (SS1)
- zámky úschovných objektů (SS2)

- úschovný objekt včetně uzamykacího systému (S1)
- zabezpečené oblasti (SS3)
- uzamykací systémy zabezpečené oblasti (SS4)
- objekt (S3)
- kontrola vstupu (SS6)
- režim návštěv v objektu (SS7)
- ostraha (SS8)
- zařízení elektrické zabezpečovací signalizace (SS91)
- instalace zařízení elektrické zabezpečovací signalizace (SS92)

Nepovinné:

- fyzické bariéry (SS10)
- kontrola vstupu v přístupových bodech fyzické bariéry (SS11)
- namátkové prohlídky, vstupní, výstupní (SS12)
- perimetrický detekční systém (SS13)
- osvětlení perimetru (SS14)
- televizní systém na perimetru (SS15)

Jak je uvedeno v tabulce 1, existuje šest proměnných S1 – S6, které se získají po dosažení hodnot do jednotlivých jednoduchých vzorečků v tabulce bodového ohodnocení.

$$S1 = SS1 \times SS2$$

$$S2 = SS3 \times SS4$$

$$S3 = \text{objekt}$$

$$S4 = SS6 \times SS7$$

$$S5 = SS8 \times SS9;$$

$$S6 = (SS10 \times SS11) + SS12 + SS13 + SS14 + SS15$$

Teď se celkové hodnoty S1 – S6, získané vyplněním tabulky bodového ohodnocení opatření fyzické bezpečnosti v zabezpečené oblasti, porovnají s tabulkou bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti (Tabulka 1).

Zabezpečená oblast kategorie Důvěrné	Míra rizika
	střední
Povinné: (S1) + (S2) + (S3)	11
Povinné: (S4) + (S5)	9
Nepovinné: (S6)	0
Celkový výsledek	20

Tabulka 3.3: Tabulka bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti

Je vidět, že přijatá opatření fyzické bezpečnosti jsou pro střední míru rizika a pro kategorii zabezpečené oblasti SU Důvěrné dostačující a splňují dané požadavky. Ověření, že provedená opatření fyzické bezpečnosti odpovídají projektu fyzické bezpečnosti, kontroluje provozovatel objektu.

2.10 Technická dokumentace fyzické bezpečnosti

Technická dokumentace fyzické bezpečnosti se dělí do dvou částí:

- výkresová dokumentace
- dokumentace technických prostředků

Výkresová dokumentace je v podstatě obrázek, který obsahuje především vyznačení hranic objektu, zabezpečené oblasti nebo jednacích oblastí. Zakresluje se rozmístění technických prostředků v objektu a zabezpečené oblasti.

Dokumentace technických prostředků je tabulka obsahující seznam použitých technických prostředků, jejich název, počet, číslo certifikátu a jednoduchý popis, popř. umístění. Mezi základní údaje u certifikovaných technických prostředků patří kopie a přílohy z doby instalace. U necertifikovaných technických prostředků uvádí zápis o posouzení shody z doby instalace.

2.11 Uplynutí doby platnosti certifikátu

Po uplynutí doby platnosti certifikátu se nesmí technický prostředek pořizovat ani nově nasazovat. Technický prostředek může být nově nasazen jen v případě, že byl pořízen v době platnosti certifikátu NBÚ. Tato skutečnost musí být doložena. Nasazení prostředku je ovlivněno provedením funkční zkoušky technického prostředku ke dni nasazení. Zápis o výsledku se ukládá u odpovědné osoby. Po uplynutí doby platnosti certifikátu mohou být technické prostředky použity jen v případě, že se po provedení funkční zkoušky prokáže, že je prostředek plně funkční. U mechanických zábranných prostředků a zařízení fyzického ničení UI se funkční zkouška dokládá zápisem o provedení funkční zkoušky, za kterou se zaručuje odpovědná osoba. U ostatních technických prostředků se funkční zkouška dokládá revizní zprávou nebo záznamem v provozní knize. Funkční zkouška se provádí minimálně jednou za dvanáct měsíců.

2.12 Funkční zkouška

Provádění funkčních zkoušek v době platnosti certifikátu NBÚ k technickému prostředku zajišťuje odpovědná osoba. Kontroluje se funkčnost všech prostředků, které jsou instalovány za účelem ochrany UI. Funkční zkouška u těchto prostředků se musí provádět každých dvanáct měsíců. O této kontrole nemusíme vést žádné záznamy.

Provádění funkční zkoušky u technických prostředků, u kterých skončila platnost certifikátu NBÚ, je nezbytné provádět každých dvanáct měsíců. O provedení funkční zkoušky rozhoduje odpovědná osoba, u které se také ukládá záznam o provedení funkční zkoušky. Při kontrole mechanických zábranných prostředků se kontrolor zaměřuje na kontrolu funkčnosti, ale i neporušenosti, včetně zámků, aby se dalo identifikovat pokusy o vniknutí. Funkční zkouška elektrické bezpečnostní signalizace a tísňového systému se provádí dle TNI 33 45 91 – 3. Zkouška je prováděna vždy každý rok při pravidelné revizi. Záznam je tedy uveden v revizní zprávě, může se zaznamenat i do provozní knihy. Tento záznam se opět uchovává u odpovědné osoby. Funkční kontrola se provádí i na zařízení fyzického ničení nosičů informací umístěné v zabezpečené oblasti. Je třeba zkontrolovat nejen stav skartovače, ale musí se provést i zkušební skartace neutajovaného dokumentu. Výstupní částice bude přeměřena. Certifikát skartovacího stroje obsahuje informaci o rozměrech řezu, které musí skartovací stroj splňovat. Odpovědná osoba tedy ověří, že rozměry splňují rozměry uvedené

v certifikátu NBÚ. Částice splňující rozměry se přikládá k zápisu o provedení funkční zkoušky, který se ukládá u odpovědné osoby.

U mechanických zábranných prostředků, které v době pořízení nebyly certifikovány NBÚ, musí být certifikát nahrazen zápisem o posouzení shody odpovědnou osobou. Funkční zkouška se u takových prostředků provádí stejně, jako u prostředků, jejichž platnost certifikátů ještě nevypršela.

2.13 Provozní řád

Provozní řád je souhrn administrativních a organizačních opatření, který musí obsahovat pravidla pro režim pohybu osob i návštěv a dopravních prostředků v areálu, objektu a zabezpečené oblasti, pravidla pro režim pohybu utajovaných informací v zabezpečeném objektu. V provozním řádu by měla obsahovat dokumentaci k technickým prostředkům, která obsahuje pokyny pro používání technických prostředků, datum jejich instalace, stanovení kontrol funkčnosti. Jedná se tedy např. o provozní knihy, návody k obsluze technických prostředků. V provozním řádu jsou obsažena i pravidla pro manipulaci s klíči. To zahrnuje jak klíče od vstupů do objektu, zabezpečených oblastí nebo jednacích oblastí, klíče od úschovných objektů, tak klíče od elektrického zabezpečovacího systému, tedy zahrnuje i čipové karty. Tato pravidla se zabývají označováním, přidělováním, odevzdáváním, úschovou a evidencí klíčů. Z důvodu větší bezpečnosti se doporučuje uchovávat klíče i jejich duplikáty v zabezpečeném objektu, pokud se určí, že klíče budou uchovány mimo zabezpečený objekt, dodržují se bezpečnostní pravidla manipulace s klíči mimo objekt. Součástí provozního řádu jsou pravidla pro výkon ostrahy. Musí se stanovit počet členů, především pravidla pro způsob jejich výkonu.

Při vytváření provozního řádu bylo tedy potřeba zaměřit se na pravidla vjezdu a pohybu dopravních prostředků do areálu, i přesto, že zabezpečená oblast se nachází ve 3. NP, a tak se problém kontroly vjezdu do areálu neřeší. Vjezd do garáží je ale povolen pouze služebním vozům. Pravidla pro režim vstupu a pohybu osob v budově B1 je zabezpečeno tím, že lidé, kteří se pohybují samostatně, jsou pouze pracovníci, jelikož jsou vybaveny osobními kartami. Ostatní osoby, tedy návštěvy, se smí pohybovat pouze v doprovodu a jejich příchod a odchod je evidován v záznamové knize uložené na recepci. Do budovy smí v podstatě vstupovat osoby pouze za účelem návštěv, služebních jednání a dodavatelských služeb. Pravidla pro režim pohybu osob v objektu a zabezpečené oblasti je přísnější. Pohyb po objektu a zabezpečené oblasti mají pouze osoby, které mají oprávnění k přístupu na stupeň utajení Vyhrazené a Důvěrné. Ti obdrželi prostředky, které jim umožní vstup do objektu. Ostatní smí vstupovat do objektu pouze v jejich přítomnosti a vše je zaznamenáno v návštěvní knize uložené na recepci v přízemí budovy B1. Do návštěvní knihy se zaznamenává jméno, příjmení, číslo dokladu totožnosti, firma, důvod návštěvy a jméno osoby, se kterou se bude jednat. Osoby se smí zdržovat v oblasti pouze po dobu nezbytně nutnou pro výkon jeho činnosti. Za umožnění vstupu do oblasti je odpovědný oprávněný pracovník, který nesmí nechat pracovníka nebo návštěvníka samotného, čímž se zajišťuje, že do oblasti nemá přístup nepovolaná osoba. Po skončení návštěvy se eviduje odchod návštěvy. Zvláštní kapitolou jsou Policie ČR, orgány státního požárního dozoru a inspektoři bezpečnosti práce. Těm je vstup povolen po předložení služebního průkazu a zapsáním příchodu a později odchodu do knihy návštěv. Podobně je tomu i u zdravotní služby, plynáren a kanalizačních služeb. Těm je vstup povolen bez předložení průkazu, pokud je účelem vstupu poskytnutí první pomoci nebo rychlý a nezbytný zásah. Jakýkoli vstup do zabezpečené oblasti se eviduje. Zapisuje se odemčení a uzamčení místnosti, to znamená zapnutí a vypnutí EZS, datum, čas jméno, podpis a důvod návštěvy. Dále jsem stanovila bezpečnostní a kontrolní opatření při vstupu

do zabezpečeného objektu. Tato opatření má na starosti poučený zaměstnanec, který musí dodržovat pravidla, jako jsou:

- před vstupem do místnosti ověřit neporušenost vstupních dveří a rámu, v případě zjištění rozporu, povolat ostrahu a provést záznam do dokumentace
- při odemčení místnosti požit osobní kartu pro kontrolu vstupu, vypnout EZS, zkontrolovat okna, dveře, vybavení
- při povolení vstupu jiné osoby, ověřit její totožnost a zapsat vše do knihy návštěv
- při odchodu kontroluje okna a především opět aktivuje EZS

Stejná opatření provádí i poučený zaměstnanec při vstupu do zabezpečené oblasti. Důležitým opatřením bylo stanovení pravidel pro režim pohybu UI v zabezpečeném objektu. To zahrnuje opatření přijímání, evidenci, zpracování, přepravu, ukládání, vyřazování, skartaci, archivaci a případně i manipulaci v souladu s platnou legislativou, především ZOUI a vyhláškou 19/2008 Sb. Aby docházelo k dodržování opatření, je třeba provádět školení osob a jejich kontrola. Další neméně důležitou dokumentací je dokumentace k technickým prostředkům. Ta zahrnuje pravidla pro jejich používání, čímž se mimo jiné předchází k jejich rychlému opotřebení nebo znehodnocení, popřípadě úplnému zničení, kterým by mohlo dojít ke snížení úrovně OUI. Pokud se přece jen stane, že dojde k jednomu z výše uvedených narušení, poučená osoba je povinna informovat odpovědnou osobu. Odpovědná osoba má povinnost provádět pravidelné kontroly všech instalovaných prostředků, které jsou v zabezpečeném objektu. Kontroluje funkce, poškození, ale i korozi apod. V případě zjištění poruchy musí zajistit co nejrychlejší odstranění škody. Jak jsem uvedla v projektu fyzické bezpečnosti, viz příloha, systém EZS a kontrolu vstupu smí využívat pouze poučené osoby. Poučená osoba je proškolená a má kód pro obsluhu EZS. Tyto osoby musí zabránit seznámení se s kódem nepovolaným osobám. V případě ztráty kódu nebo vyzrazení musí tyto skutečnosti nahlásit odpovědné osobě. Všechny poučené osoby jsou proškoleny z obsluhy skartovacího zařízení. Poučené osoby jsou povinni skartovat dokumenty určené k likvidaci pouze na zařízení certifikovaném NBÚ. Provozní dokumentaci k technickým prostředkům tvoří dokumentace úschovných objektů, dokumentace EZS, dokumentace skartačního zařízení a dokumentace (karta) bezpečnostního zámku dveří. Za úplnost provozní dokumentace, dodržení termínů kontrol funkčnosti a revizí odpovídá bezpečnostní ředitel. Záznam o vstupu a odchodu ze zabezpečené oblasti byl umístěn tak, aby k němu měl přístup každý oprávněný pracovník, který musí provádět nařízené záznamy. Dalším z uvedených pravidel jsou pravidla pro manipulaci s klíči a vstupními kódy zahrnuje:

- klíče od zabezpečeného objektu
- klíče od zabezpečené oblasti
- klíče a číselné kombinace od úschovného objektu
- kódy EZS a identifikační karty s rozlišením povolené zóny
- klíče a číselné kombinace od přenosných schránek

Existuje 5 klíčů od vstupních dveří, přičemž každý má přiděleno pořadové číslo 1 až 5 (č. 1 - pracovník pověřený vedením jednacího protokolu, č. 2 - bezpečnostní správce IS, č. 3 - odpovědná osoba, č. 4 - pomocný klíč uložený v trezoru, č. 5 nouzový duplikát v zapečetěné krabičce v trezoru záložních klíčů správy). Ztráta jakéhokoli klíče se musí okamžitě oznámit odpovědné osobě. Ta zajistí, že se provede kontrola neporušenosti dveří, zámku a prostor zabezpečené oblasti. I přesto se musí, co nejrychleji, vyměnit všechny zámky od ztraceného klíče. Zaměstnanci jsou poučeni o tom, že nesmí klíče půjčovat, poškodit je nebo ztratit, ani dělat kopie.

Při stanovení pravidel provozního řádu bylo důležité uvědomit si, že se s dokumenty zachází i mimo zabezpečenou oblast, že je možné je přepravovat, a proto se musí zajistit bezpečnostní přenosné schránky pro ochranu utajovaných dokumentů během přepravy. Vybrala jsem takové schránky, které jsou vybaveny mechanickými nebo kombinačními zámky. Duplikáty klíčů a číselné kombinace schránek jsou uloženy v zalepené obálce v úschovném objektu. Z toho je zřejmé, že klíče od zabezpečené oblasti podléhají vyššímu zabezpečení než ostatní klíče.

2.14 Ostraha

Dle přílohy č. 1 k vyhlášce č.528/2005 Sb., ve znění vyhlášky 19/2008 Sb. byla vybrána ostraha typu 2. Pravidla pro výkon ostrahy jsou nutná, pokud se v zabezpečené oblasti nachází dokumenty SU Důvěrné a vyšší. I přesto, že pro dokumenty SU Důvěrné a Vyhrazené lze použít ostrahu typu 1, dá se předpokládat, že se UI mohou do budoucna rozšířit na SU Tajné a vyšší, proto jsem vybrala ostrahu typu 2 bez obchůzek. Ostrahu mohou provádět zaměstnanci orgánu státu, fyzické nebo právnické osoby, jejichž objektu se to týká. Nevylučují se ani zaměstnanci bezpečnostní služby. U zvoleného typu ostrahy nejsou povinné bezpečnostní obchůzky. Ve fiktivním areálu UAI, a.s. je zajištěna nonstop fyzická ostraha zabezpečené oblasti prostřednictvím ostrahy, která se nachází v přízemí budovy B1 na recepci. Pracovníci ostrahy jsou poučené osoby, které mají oprávnění ke vstupu k UI SU Důvěrné. Na recepci, tedy na centrálu ostrahy je vyvedena signalizace poplachu elektrické zabezpečovací signalizace objektu i oblasti. Pracovníkům ostrahy je na centrálu vyvedena EZS budovy B1, elektrická požární signalizace a monitor pro sledování kamer z průmyslové zóny.

Pracovníkovi se v rámci provozního řádu stanovila tyto povinnosti:

- kontrola zamčení vstupních dveří
- kontrola osob pohybujících se v budově
- obsluha všech technických prostředků ostrahy budovy
- vedení záznamů
- hlášení havarijních událostí na dispečink
- přiměřené poskytnutí informací nebo pomoci v nouzi osobám v budově B1

2.15 Stav ohrožení

Stav ohrožení se vyhláší v případě pocitu nebo zjištění zvýšeného rizika. Rizikem může být pokus o neoprávněný vstup do zabezpečené oblasti a s tím spojený pokus o odcizení utajovaných dokumentů. Jedná se ale i zjištění nefunkčnosti technických prostředků nebo změna bezpečnostní situace a snížení bezpečnosti. Stav ohrožení vyhláší odpovědná osoba. Aby nedošlo k odcizení utajovaných dokumentů, zaměstnanci bezpečnostní služby uzavřou všechny vstupy do budovy a zamezí dalším návštěvám vstup a lidem uvnitř k odchodu z budovy do té doby, než se provedou důsledné kontroly. Když se naleznou UI mimo zabezpečenou oblast, je pracovník, který dokumenty našel povinen informovat odpovědnou osobu a musí zajistit, aby se dokumenty nedostaly do rukou neoprávněným osobám. Samozřejmě ani on sám se nesmí s UI seznamovat.

2.16 Kontrola zabezpečené oblasti

Kontrola zabezpečené oblasti se provádí každý kalendářní rok. Postupuje se podle plánu kontrol, který má na starosti vypracovat odpovědná osoba. Jedná se kontroly, jako jsou kontrola ukládání protokolů o ověření funkční zkoušky, revizní záznamy, záznamy v provozní knize, návštěvní knize apod. Důležitou částí je kontrola klíčů, musí se zkontrolovat jejich uložení a správná manipulace. To zahrnuje i kontrolu vstupu do oblasti, tedy kontrolu evidencí návštěv. Odpovědná osoba musí ověřit, zda jednotlivá opatření fyzické bezpečnosti odpovídají projektu fyzické bezpečnosti. V případě, že dojde k aktualizaci, musí dohlédnout na to, aby se změny projevily i v projektu fyzické bezpečnosti. Po provedení všech kontrol a ověření všech opatření musí odpovědná osoba vypracovat Záznam o kontrole.

Záznam o kontrole zabezpečená oblast

Byla provedena kontrola zabezpečené oblasti s tímto výsledkem:

1. byl prostudován projekt fyzické bezpečnosti a odpovídá skutečnému stavu
2. celková míra rizik zůstává střední
3. byla provedena funkční zkouška:
 - a. EZS
 - b. zámku a neporušenosti vstupních dveří do zabezpečené oblasti
 - c. zámky a těla úschovných objektů (trezorů)
 - d. funkční zkouška skartovacího stroje

Výsledek kontroly:

Datum:

Podpis odpovědné osoby (bezpečnostního ředitele):

Ukázka 3.1: Provedení záznamu o kontrole

2.17 Mimořádná situace

Mimořádnou situaci definuje vyhláška NBÚ č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků v § 2, písm. i), a to jako stav, kdy bezprostředně hrozí, že dojde k vyzrazení nebo zneužití UI. Týká se:

- neoprávněné nakládání s UI poučenými osobami (úmyslně i neúmyslně)
- neoprávněné nakládání s UI nepovolanou osobou (vniknutím do zabezpečené oblasti, odcizení klíčů, úmyslné způsobení havárie)
- neoprávněné nakládání s UI při havárii (požár, toxické látky, průmyslová havárie, výbuch plynu, apod.)
- neoprávněné nakládání s UI při teroristickém útoku nebo vandalismu (telefonická pohružka, demonstrace, nepokoje, apod.)

- únik UI z IS, riziko zničení dat
- vyzrazení UI pasivním odposlechem, nasazením operativní techniky

Společnost se snaží riziko vzniku mimořádných situací minimalizovat:

- pečlivým výběrem zaměstnanců a jejich prověřením v rámci bezpečnostního řízení
- pravidelným školením
- umístěním zabezpečené oblasti v budově do místa, které není běžně dostupné
- důslednou pravidelnou kontrolní činností všech opatření personální, administrativní a fyzické bezpečnosti, včetně opatření bezpečnosti IS
- opatřeními fyzické bezpečnosti (technickými prostředky, režimovými opatřeními a ostrahou)

Pro řešení mimořádných situací a snížení škod v případě jejich vzniku je rozhodující:

- včasnost rozpoznání možného rizika ohrožení UI
- úroveň realizace opatření
- rychlost řešení
- rychlost informování subjektů
- schopnost obnovit standardní stav OUI na úroveň před vznikem takové situace

Pokyny a postup pro OUI v případě vzniku krizové situace:

- rychle analyzovat druh krizové situace
- vyhlásit stav ohrožení UI
- uzavřít úložný objekt
- zvolit optimální řešení s cílem ochrany lidských životů a docílení co nejmenší škody
- informovat odpovědnou osobu o vzniku krizové situace, paralelně informovat ostrahu
- realizovat opatření k odstranění následků krizové situace
- zabezpečit OUI do doby obnovy standardního stavu
- provést analýzu příčin vzniku krizové situace a navrhnout nápravná a preventivní bezpečnostní opatření
- neposkytovat informace o krizových situacích nepovolaným osobám s odvoláním na odpovědnou osobu

Nesmí se zapomínat na stanovení povinností osob při řešení mimořádné situace. Jedná se o zaměstnance, bezpečnostního ředitele nebo odpovědné osoby. Mezi tyto povinnosti patří např. zamezení neoprávněné manipulaci s utajovanou informací, zabezpečení zabezpečeného objektu a oblasti, vyhodnocení situace, zvážení následků a přijetí opatření k řešení mimořádné situaci.

Při havárii inženýrských sítí (voda, plyn, elektroinstalace) a při vzniku požáru (jiné živelné pohromy) je potřeba ihned uvědomit nejen odpovědnou osobu, ale také Policii ČR a podle rozsahu požáru a stupně nebezpečí ohrožení také plynárenskou, vodárenskou a energetickou společnost. Nesmí se zapomínat ani na mimořádnou situaci, kterou může být teroristický. Další postup a případné zajištění UI před zneužitím nebo vyzrazením a jejich následnou obnovu řídí bezpečnostní ředitel společnosti nebo jím pověřená - poučená osoba.

Hlavním cílem je zamezení přístupu nebo v rámci likvidace katastrofy k přístupu nebo manipulaci s UI neoprávněnými osobami. Při zjištění neoprávněného nakládání nebo ztrátě UI je odpovědná osoba povinna tyto skutečnosti bez zbytečného odkladu oznámit písemně NBÚ, včetně opatření přijatých k nápravě. Veškerá tato zjištění neoprávněného nakládání nebo ztráty musí být odpovědnou osobou neprodleně evidována a vyhodnocována. Další povinností je seznámit se s pravidly vyhlášení stavu ohrožení UI a následně všechna stanovená opatření dodržovat. Další možností řešení mimořádné situace je evakuace. Při ní se musí dodržovat pravidla v souladu s platnou legislativou týkající se přenosu utajovaných dokumentů. Poučené osoby tedy uloží UI do přenosných schránek připravených v souladu s platnou legislativou a směrnicí zajišťující administrativní bezpečnost, a tyto přenosné schránky uloží do úschovného objektu, který řádně uzavřou a uzamknou. K UI uloženým do úschovných schránek se přiloží seznam obsažených UI. Zabezpečená oblast se uzamkne a aktivuje se EZS.

3 Ochrana dokumentů

Havárie a živelné pohromy negativně ovlivňují životnost dokumentů. Během požárů dochází k poškození dokumentů nejen ohněm, kouřem a sazemi, ale i hasícími prostředky. Základem prevence před živelnými pohromami je průzkum a definice konkrétních rizikových faktorů, např. umístění v záplavové oblasti, stav hydrantů, střech a okapů, stav vodní a topenářské instalace, stav protipožárního a hasícího vybavení, apod.

Mezi zdroje ohrožení patří také chybné úložiště, nevhodná manipulace, hmyz, příliš intenzivní světlo atd. Při nízké teplotě hrozí nebezpečí kondenzace vody na povrchu dokumentů. Při vysoké teplotě se snižuje celková mechanická odolnost a podporují se mikrobiální činnosti, tedy plísně. Ani prudké výkyvy, kterými dochází k rozpínání a smršťování, popř. praskání povrchu dokumentů nejsou žádoucí. U papírových dokumentů se uvádí přijatelná teplota vzduchu a relativní vlhkost vzduchu:

- teplota: 18 ± 2 °C
- relativní vlhkost: $50 \pm 5\%$

V dnešní době již existují osvědčené metody, jak stabilizovat parametry klimatu. U teploty jde především o klimatizaci, větrání a udržování izolace. Při nízké vlhkosti se musí zajistit zvlhčovače a při vysoké vlhkosti odvlhčovače. Opět se dodržuje větrání a izolace. Klimatizace a proudění vzduchu chrání i před látkami znečišťující ovzduší. Dalším parametrem je ochrana před světlem. Před světlem chrání dokumenty UV – folie, žaluzie, rolety a důležité je i správné osvětlení, nejlépe zdroj světla s UV – filtrem

Dokumenty je třeba chránit před poškozením vodou, ohněm, mrazem, chemikáliemi, světlem. Dobrou prevencí je ovšem i vybavení ochrannými pomůckami jako jsou různé fólie, polyetylenové sáčky, základní nářadí, čisticí prostředky nebo ochranný oděv. Je třeba si uvědomit, že tyto ochranné prostředky nejsou certifikované NBÚ, nesplňují tedy žádná kritéria a toto zabezpečení se nehodnotí žádným bodovým hodnocením. Jedná se pouze o jinou formu prevence, kterou se může utajovaný dokument chránit bez ohledu na legislativní rámec a opatření stanovená NBÚ. Způsob, kterým dochází k poničení utajovaných dokumentů a o kterém ještě nebyla zmínka, je kopírování. Kopírování může dokument výrazně poničit, proto by měl být originál ušetřen od častého kopírování.

Před živelnými pohromami se nelze ubránit, lze je ovšem předvídat a provést alespoň drobné preventivní opatření. Známou mezinárodní organizací, která má poslání poskytovat pomoc a ochranu při ohrožení světového kulturního dědictví přírodními katastrofami je Mezinárodní komitét Modrý štít – ICBS (International Committee of the Blue Shield). Společnost funguje od poloviny roku 1996 a jejími hlavními úkoly jsou prevence před pohromami a rychlá opatření během stavu nouze. Český komitét Modrý štít – ČKMS vznikl v roce 2000. ČKMS sdružuje instituce pečující o kulturní odkazy, např. Česká archivní společnost.

4 Národní bezpečnostní úřad

4.1 NBÚ

Stanovení fyzické bezpečnosti utajovaných informací a dokumentů poskytuje Národní bezpečnostní úřad – NBÚ. Mezi jeho hlavní úkoly patří:

- rozhoduje o vydání osvědčení fyzické osoby, osvědčení podnikatele a o vydání dokladu o bezpečnostní způsobilosti fyzické osoby a o zrušení platnosti osvědčení fyzické osoby, osvědčení podnikatele a dokladu
- plní úkoly 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
- ve stanovených případech povoluje poskytování utajovaných informací v mezinárodním styku
- vede ústřední registr a schvaluje zřízení registrů,
- provádí výkon státního dozoru a ukládá sankce za nedodržení povinností stanovených zákonem,
- zajišťuje činnost Národního střediska komunikační bezpečnosti, Národního střediska pro distribuci kryptografického materiálu, Národního střediska pro měření kompromitujícího elektromagnetického vyzařování a Národního střediska pro bezpečnost informačních systémů, které jsou jeho součástí,
- provádí certifikace technického prostředku, informačního systému, kryptografického prostředku, kryptografického pracoviště a stínicí komory,
- zajišťuje výzkum, vývoj a výrobu národních kryptografických prostředků,
- vyvíjí a schvaluje národní šifrové algoritmy a vytváří národní politiku kryptografické ochrany

4.2 Věstník

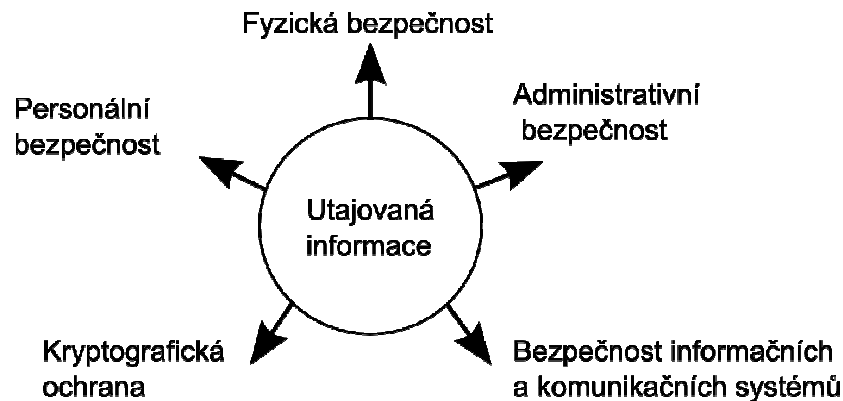
Seznam certifikovaných technických prostředků zveřejňuje Věstník. Věstník je periodická publikace, kterou vydává Národní bezpečnostní úřad pro veřejnost, nejméně dvakrát do roka.

U každého technického prostředku ve Věstníku nalezneme:

- evidenční číslo (číslo certifikátu)
- název
- označení
- výrobce
- držitel (jméno a kontakt)
- kategorie
- bodové hodnocení
- platnost certifikátu

Tyto základní informace umožňují dobrou orientaci v dokumentu, díky které si každý může vybrat takový certifikovaný technický prostředek, který odpovídá bodovému hodnocení, které si sám určil, aby splnil podmínky zabezpečení na určitý SU.

4.3 Fyzická bezpečnost



Obrázek 5.1: Utajovaná informace

Fyzická bezpečnost je zajištěna nejen bezpečností fyzickou, ale jak je vidět na obrázku, také bezpečností personální, administrativní, bezpečností informačních a komunikačních systémů, kryptografickou ochranou a průmyslovou bezpečností. Vytvoření fyzické bezpečnosti znamená vytvořit systém opatření, která nepovolane osobě zabrání nebo ztíží přístup k utajované informaci.

Vytvoření fyzické bezpečnosti má:

- odradit pachatele
- znemožnit pokus o vloupání
- ztížit postup pachatelů
- zajistit zásah bezpečnostních složek, a tím zvýšit pravděpodobnost dopadení

Vytvoření bezpečnostních opatření se popisuje v projektu fyzické bezpečnosti, který je zpracovaný podle specifikace uvedené v příloze č. 1 vyhlášky č. 528/2005 Sb. ve znění vyhlášky č. 19/2008 Sb. Poté se projekt fyzické bezpečnosti musí dát na NBÚ k posouzení a schválení. Projektem fyzické bezpečnosti je tedy dokument, který definuje použité bezpečnostní prvky a uvádí, jaká byla vytvořena bezpečnostní opatření. Vytvoření projektu fyzické bezpečnosti znamená nejen seznámení se s technickými prostředky, ale hlavně s legislativním rámcem oblasti, pro kterou je zabezpečení prováděno (v našem případě jsou to utajované informace dle zák. 412/2005 Sb.). Teprve potom lze vytvořit kvalitní projekt.

4.4 Certifikace

Při certifikaci technických prostředků dochází k hodnocení technických parametrů technických zařízení, která jsou používána k ochraně utajovaných informací. Jedná se o odborný posudek. Certifikát může obsahovat přílohu. V příloze certifikátu se uvádí složení, podmínky pro použití nebo omezující skutečnosti apod. Certifikát se vydává pro jednotlivý technický prvek. Je vydáván na žádost podnikatele, společnosti nebo fyzické osoby, která prostředek bude používat. Po uplynutí doby platnosti se nesmí technický prvek používat, pokud není provedena funkční zkouška. Seznam certifikovaných technických prostředků zveřejňuje Věstník.

5 Kalkulace

Název	Počet kusů	Cena za kus/Kč	Cena celkem/Kč
Bezpečnostní dveře	2	3 200	6 400
Skříňový trezor	1	36 000	36 000
Zámková vložka	2	1 500	3 000
Kontrola vstupu	2	4 850	9 700
Bezdotyková čtečka	2	3 200	6 400
Magnetický kontakt	8	650	5 200
Ústředna	1	12 605	12 605
Klávesnice	2	1 800	3 600
Detektor otřesu	1	3 990	3 990
Detektor pohybu	4	1 630	6 520
Detektor rozbití skla	5	1 420	7 100
Detektor požáru	2	1 710	3 420
Tísňové tlačítko	2	450	900
Siréna	2	490	980
Čipové karty	8	118	944
Skartační stroj	1	4 500	4 500
Stavební úpravy a montáž	1	60 000	60 000
Revizní zpráva	1	6 000	6 000
Celkem			177 259

Tabulka 6.1: Tabulka nákladů na zabezpečení objektu

Výše uvedená tabulka obsahuje spíše katalogové ceny a ceny získané z e-shopů. Přesněji lze cenu získat např. tím, že si nabídku necháme udělat od dodavatelské firmy. Cena lze snížit jiným umístěním prvků nebo použitím méně silných prostředků. Může se dosáhnout až 25% snížení ceny (odhadem). Pokud se použijí méně silné technické prostředky, dochází tím ke snížení bodového hodnocení. Proto je třeba dávat si pozor, aby nedošlo ke snížení bodového ohodnocení natolik, že by bodové hodnocení přijatých opatření fyzické bezpečnosti nesplňovalo minimální bodové ohodnocení tabulky hodnot nejnižší míry zabezpečení zabezpečené oblasti. Další, téměř nezbytnou, možností je odborná konzultace na NBÚ. NBÚ vydává Úřadem schválený projekt bezpečnosti komunikačního systému. Po předložení všech dokumentů a zkontrolování uskutečnění zabezpečení může NBÚ schválit projekt bezpečnosti. Pokud tedy dojde k jakékoli úpravě zabezpečení v projektu fyzické bezpečnosti, je třeba schválení NBÚ. Ať už je důvodem použití bezpečnostních prvků nižšího hodnocení, a tím snížení celkové ceny nákladů, nebo např. nahrazení jednotlivých prvků. V uvedeném projektu fyzické bezpečnosti může dojít ke snížení ceny např. tím, že místo stavebních úprav

a nahrazením všech průlezných otvorů (mimo oken) lehkou stavební konstrukcí, se jednotlivé průlezné otvory zabezpečí pouze mřížemi. V rámci úprav vedoucích ke snižování nákladů nesmí dojít ke snížení bezpečnosti zabezpečené oblasti. Není proto možné nahradit certifikovaný technický prostředek za necertifikovaný, jelikož takový by nesplňoval podmínky přílohy č. 1 k vyhlášce 528/2005 Sb., ve znění vyhlášky č. 19/2008 Sb., jeho bodové hodnocení by bylo 0, a tím by se snížila míra zabezpečení zabezpečené oblasti. Jinou možností je zvolení takové zabezpečené oblasti, u které není potřeba provádět stavební úpravy, a tím nenavyšovat náklady. Cena by neměla být hlavním kritériem při výběru zabezpečení, avšak nutno podotknout, že je většinou považována za jednu z nejdůležitějších kritérií.

6 Závěr

Cílem práce bylo vytvoření projektu fyzické bezpečnosti. Vytvoření projektu fyzické bezpečnosti znamená nejen seznámení se s technickými prostředky, ale především seznámení se s legislativním rámcem oblasti, pro kterou je zabezpečení prováděno. V tomto konkrétním případě jsou to utajované informace, jedná se tedy o zákon 412/2005 Sb. Teprve po seznámení se s legislativou lze vytvořit kvalitní projekt.

Při vypracovávání projektu bylo striktně dodržováno postupu uvedeného v příloze č. 1 k vyhlášce 528/2005 Sb., ve znění vyhlášky č. 19/2008 Sb. Byly vybrány pouze technické prostředky uvedené ve Věstníku, jejichž platnost certifikátů vydaných k 1. lednu 2010 je stanovena do 31. prosince 2012. Nejdříve došlo k určení hrozeb a stanovení celkové míry rizika stupně utajení Důvěrné na hodnotu střední, tedy 14 bodů. Po zvolení zabezpečené oblasti a technických prostředků, které budou sloužit k ochraně utajovaných informací, došlo k ohodnocení zabezpečení na 20 bodů. Je vidět, že přijatá opatření fyzické bezpečnosti jsou pro střední míru rizika a pro kategorii zabezpečené oblasti SU Důvěrné dostačující a splňují dané požadavky. Při vytváření projektu fyzické bezpečnosti nedošlo k zanedbání žádného z jednotlivých bodů, které nám vyhláška ukládá. Dá se říci, že projekt fyzické bezpečnosti splňuje všechny podmínky a mohl by být schválen NBÚ. Tedy cíle bakalářské práce byly splněny.

Zneužití údajů je v dnešní době velmi nebezpečné, a proto je třeba tématu bezpečnost věnovat velkou pozornost. V případě, že se bude dodržovat správný postup při zabezpečování, snižuje se tím riziko útoku. K tomu je určený právě projekt fyzické bezpečnosti. Při zohlednění legislativního rámce lze princip projektu fyzické bezpečnosti využít např. při ochraně osobní údajů, obchodního tajemství apod.

Vytvoření fyzické bezpečnosti má za úkol odradit útočníka před vniknutím do objektu. Po dobu trvání projektu většinou nedochází k ověření míry bezpečnosti reálným útokem, a proto se musí udržovat nadšení pracovníků, finanční podpora a nepřetržitá kontrola efektivního zabezpečení i po několik let. Je proto důležité věřit v efektivitu projektu fyzické bezpečnosti a dodržovat jej.

7 Slovníček pojmů

- UI – utajovaná informace
- OUI – ochrana utajovaných informací
- SU – stupeň utajení
- FO – fyzická osoba
- NP – nadzemní podlaží
- EZS – elektrická zabezpečovací signalizace
- NBÚ – Národní bezpečnostní úřad
- V – Vyhrazené
- D – Důvěrné

- ZOUI – zákon č 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti v platném znění

8 Bibliografie

- [1] *Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. / Prováděcí právní předpisy / Právní předpisy / Národní bezpečnostní úřad* [online]. 2005 [cit. 2011-04-19]. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. Dostupné z WWW: <<http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5282005/>>
- [2] KORHOŇ, Miloš. *Havárie a živelné pohromy* [online]. [s.l.], 2005. 34 s. Oborová práce. Vědecká knihovna
- [3] MCIIWAINE, John. *Živelné pohromy a havárie - prevence a plánování* [online]. [s.l.], 2007. 68 s. Absolventská práce. University College London
- [4] KORHOŇ, Miloš. *Ochrana dokumentů* [online]. [s.l.], 2005. 26 s. Oborová práce. Vědecká knihovna
- [5] *Věstník / O nás / Národní bezpečnostní úřad* [online]. 2005 [cit. 2011-04-19]. Věstník. Dostupné z WWW: <<http://www.nbu.cz/cs/o-nas/vestnik/>>
- [6] *Hlavní úkoly / O nás / Národní bezpečnostní úřad* [online]. 2005 [cit. 2011-04-19]. Hlavní úkoly. Dostupné z WWW: <<http://www.nbu.cz/cs/o-nas/hlavni-ukoly-nbu/>>
- [7] *Informace k certifikačnímu postupu NBÚ / Certifikační postup NBÚ - verze 2010 / Certifikace / Fyzická bezpečnost (technické prostředky a další prvky fyzické bezpečnosti a jejich certifikace) / Ochrana utajovaných informací / Národní bezpečnostní úřad* [online]. 2005 [cit. 2011-04-19]. Informace k certifikačnímu postupu NBÚ. Dostupné z WWW: <<http://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost/certifikace/certifikacni-postup-nbu/informace-k-certifikacnimu-postupu-nbu/>>
- [8] *Projekt bezpečnosti – Postup hodnocení / Bezpečnost komunikačních systémů / Ochrana utajovaných informací / Národní bezpečnostní úřad* [online]. 2005 [cit. 2011-04-19]. Projekt bezpečnosti – Postup hodnocení. Dostupné z WWW: <<http://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-komunikacnich-systemu/projekt-bezpecnosti-postup-hodnoceni/>>
- [9] *DRAKAS s.r.o. - projekt fyzické bezpečnosti* [online]. 2011 [cit. 2011-04-19]. PROJEKT FYZICKÉ BEZPEČNOSTI. Dostupné z WWW: <PROJEKT FYZICKÉ BEZPEČNOSTI>
- [10] *RAC - Download* [online]. 2010 [cit. 2011-04-19]. Risk Analysis Consultants. Dostupné z WWW: <<http://www.rac.cz/rac/homepage.nsf/CZ/Downloadx>>
- [11] *Právní předpisy / Národní bezpečnostní úřad* [online]. 2005 [cit. 2011-04-19]. Právní předpisy. Dostupné z WWW: <<http://www.nbu.cz/cs/pravni-predpisy/>>
- [12] *Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor / Prováděcí právní předpisy / Právní předpisy / Národní bezpečnostní úřad* [online]. 2005 [cit. 2011-04-19]. >Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. Dostupné z WWW: <<http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5232005/>>

- [13] *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. / Prováděcí právní předpisy / Právní předpisy / Národní bezpečnostní úřad [online]. 2005 [cit. 2011-04-19]. 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. Dostupné z WWW: <<http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5262005/>>*
- [14] *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) / Prováděcí právní předpisy / Právní předpisy / Národní bezpečnostní úřad [online]. 2005 [cit. 2011-04-19]. 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). Dostupné z WWW: <<http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5272005/>>*
- [15] *Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. / Prováděcí právní předpisy / Právní předpisy / Národní bezpečnostní úřad [online]. 2005 [cit. 2011-04-19]. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. Dostupné z WWW: <<http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5282005/>>*
- [16] *Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb. / Prováděcí právní předpisy / Právní předpisy / Národní bezpečnostní úřad [online]. 2005 [cit. 2011-04-19]. Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb. Dostupné z WWW: <<http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5292005/>>*

Příloha – Projekt fyzické bezpečnosti

Projekt fyzické bezpečnosti společnosti UAI, a.s.

Zpracovala: Kateřina Schneiderová

**České Budějovice
1. března 2011**

POUŽITÉ ZKRATKY:	4
1. ÚVOD	5
2. VYHODNOCENÍ RIZIK	6
2.1. Specifikace aktiv	6
2.2. Stanovení jednotlivých hrozeb a zranitelností a jejich vyhodnocení včetně stanovení celkové míry rizika	6
2.2.1. Hrozba neoprávněného nakládání s UI poučenými osobami	6
2.2.2. Hrozba neoprávněného nakládání s UI nepovolnou osobou	7
2.2.3. Hrozba neoprávněného nakládání s UI při živelné pohromě či havárii	7
2.2.4. Hrozba vyzrazení UI pasivním odposlechem a nasazením operativní techniky	7
2.3. Stanovení celkové míry rizika.....	7
3. URČENÍ OBJEKTU A ZABEZPEČENÉ OBLASTI VČETNĚ JEJICH HRANIC, URČENÍ KATEGORIE A TŘÍDY ZABEZPEČENÉ OBLASTI	9
3.1. Popis areálu UAI, a.s.....	9
3.2. Stanovení objektu a jeho typu	9
3.3. Stanovení hranic objektu.....	10
3.4. Stanovení zabezpečené oblasti a její hranice.....	10
3.5. Popis zabezpečení objektu a zabezpečené oblasti	10
3.5.1. Úschovné objekty a zámek	11
3.5.2. Zabezpečená oblast	11
3.5.3. Hranice objektu	11
3.5.4. Systém kontroly vstupu do zabezpečeného objektu a oblasti	11
3.5.5. Režim návštěv v objektu	12
3.5.6. Ostraha	12
3.5.7. Zařízení elektrické zabezpečovací signalizace	12
3.5.8. Ochrana perimetru	13
3.5.9. Zařízení elektrické požární signalizace	13
4. TABULKA BODOVÉHO OHODNOCENÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI V ZABEZPEČENÉ OBLASTI	14
5. TECHNICKÁ DOKUMENTACE FYZICKÉ BEZPEČNOSTI	17
5.1. Výkresová dokumentace	17
5.2. Dokumentace technických prostředků	17
5.3. Specifikace certifikovaných prostředků	17
6. PODMÍNKY POUŽÍVÁNÍ TECHNICKÝCH PROSTŘEDKŮ PO UPLYNUTÍ DOBY PLATNOSTI JEJICH CERTIFIKÁTŮ:	18
6.1. Po uplynutí doby platnosti certifikátu	18
6.2. Pravidla pro provádění funkčních zkoušek jednotlivých technických prostředků	19
7. PROVOZNÍ ŘÁD	19
7.1. Pravidla pro režim vjezdu a pohybu dopravních prostředků do areálu	19

7.2. Pravidla pro režim vstupu a pohybu osob v budově B1	19
7.3. Pravidla pro režim pohybu osob v objektu a v zabezpečené oblasti	19
7.4. Bezpečnostní a kontrolní opatření při vstupu do zabezpečeného objektu	20
7.5. Bezpečnostní a kontrolní opatření při vstupu do zabezpečené oblasti	20
7.6. Pravidla pro režim pohybu UI v zabezpečeném objektu	20
7.7. Provozní dokumentace k technickým prostředkům - pravidla pro jejich používání	21
7.8. Pravidla pro manipulaci s klíči	21
7.9. Pravidla pro výkon ostrahy	22
8. DALŠÍ OPATŘENÍ V OBLASTI FYZICKÉ BEZPEČNOSTI	23
9. PLÁN ZABEZPEČENÍ OBJEKTU A OBLASTI V KRIZOVÝCH SITUACÍCH.....	24
9.1. Zásady obecného postupu při řešení mimořádné situace	25
9.2. Povinnosti poučených zaměstnanců při řešení mimořádné situace	25
9.3. Povinnosti bezpečnostního ředitele (odpovědné osoby)	25
9.4. Pokyny pro ochranu UI v případě vzniku mimořádné situace	26
9.5. Vyhlášení stavu ohrožení UI	26
9.6. Evakuace	27
PŘÍLOHA A - ROZMÍSTĚNÍ TECHNICKÝCH PROSTŘEDKŮ V ZABEZPEČENÉM OBJEKTU A ZABEZPEČENÉ OBLASTI	28
PŘÍLOHA B - CERTIFIKÁTY TECHNICKÝCH PROSTŘEDKŮ.....	30

Použité zkratky:

UI – utajovaná informace

OUI – ochrana utajovaných informací

SU – stupeň utajení

FO – fyzická osoba

NP – nadzemní podlaží

EZS – elektrická zabezpečovací signalizace

OBL – bodová hodnota určená kategorií zabezpečené oblasti

NBÚ – Národní bezpečnostní úřad

V – Vyhrazené

D – Důvěrné

ZOUI – zákon č 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti v platném znění

1. Úvod

Společnost UAI, a.s. získala státní zakázku na vyhodnocení dislokačních plánů z pohledu ohrožených lokalit živelnou pohromou. Státní zakázka předpokládá práci pouze s papírovými dokumenty SU Důvěrné v rozsahu cca padesáti dokumentů. Firma má sídlo v administrativním objektu a na zakázce pracuje tým o šesti osobách, které již mají osvědčení na SU Důvěrné.

Firma v souladu se ZOUI již absolvovala bezpečnostní řízení na NBÚ a bylo jí vydáno osvědčení podnikatele na seznamování s UI SU Důvěrné. Toto osvědčení je nutné rozšířit na tvorbu a ukládání UI do stupně utajení Důvěrné tak, aby společnost UAI, a.s. splňovala podmínku podle § 16 odst. 1 písm. c) ZOUI zajištěním ochrany UI personální, administrativní a fyzickou bezpečností a bezpečností IS. Tento dokument řeší oblast fyzické bezpečnosti. Fyzickou bezpečností je ve společnosti chápán systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k UI, popřípadě přístup nebo pokus o něj zaznamenat.

2. Vyhodnocení rizik

2.1. Specifikace aktiv

Společnost UAI, a.s. má přístup k UI SU Vyhrazené a Důvěrné, které u ní vznikají, nebo jsou jí poskytovány a zároveň má možnost seznamovat se s UI stejného SU i u zákazníků v souvislosti s výkonem pracovní nebo jiné činnosti pro podnikatele na základě smlouvy (vybraní zaměstnanci společnosti nebo osoby jednající jménem společnosti). Společnost UAI, a.s. má souhlas pro přístup, poskytování, ukládání a vznik v souladu s § 20, odst. 1, písm. a) i b) ZOUI (Vyhrazené, Důvěrné).

Mezi aktiva u společnosti UAI, a.s. patří:

- UI
- nosiče datových informací v listinné podobě
- poučené FO (zaměstnanci společnosti nebo vlastníci oznámení o splnění podmínek pro přístup k UI SU Důvěrné.)

Zaměstnanci společnosti pracují na zakázkách, jejichž předmětem jsou UI. Přehled těchto zakázek je pravidelně oznamován NBU.

Odhad předpokládaného počtu zakázek za rok, v rámci kterých se budou pracovníci seznamovat nebo zpracovávat UI, nebo jim UI budou poskytovány:

SU	Počet zakázek	Počet UI
Vyhrazené	0 - 3	0 - 100
Důvěrné	0 - 1	0 - 5

Při realizaci některých zakázek může dojít u některých zaměstnanců k seznámení, vzniku nebo poskytnutí UI při přípravě nebo realizaci zakázky, poskytování servisu apod. Pracovníci nejčastěji přicházejí do styku s UI SU Vyhrazené, v některých případech i SU Důvěrné.

V případě vzniku UI, budou tyto UI zpracovávány v zabezpečené oblasti nebo se souhlasem odpovědné osoby i mimo zabezpečenou oblast, pokud je v souladu s § 24, odst. 5 ZOUI zajištěno, že k UI nemá přístup neoprávněná osoba.

2.2. Stanovení jednotlivých hrozeb a zranitelností a jejich vyhodnocení včetně stanovení celkové míry rizika

2.2.1. Hrozba neoprávněného nakládání s UI poučenými osobami

Jedná se o úmyslné nebo neúmyslné porušení povinností pracovníků poučených odpovědnou osobou, které vyplývají z ZOUI a Vyhlášek NBU.

Nejčastěji se jedná o vyzrazení UI:

- z nedbalosti
- nedodržení bezpečnostních zásad a opatření
- za účelem vlastního obohacení

Větší pravděpodobností vyzaření UI je z nedbalosti. Riziko úmyslného vyzaření nelze vyloučit, ale je malé. Pravděpodobnější je vyzaření UI pod nátlakem. Rizika této skupiny jsou minimalizovány pečlivým výběrem zaměstnanců, pravidelným školením a důkladnou pravidelnou kontrolní činností.

Na základě těchto skutečností považuje společnost míru rizika neoprávněného nakládání s UI poučenými osobami jako malou až střední.

2.2.2. Hrozba neoprávněného nakládání s UI nepovolanou osobou

Jedná se o riziko seznámení se s UI nepovolanou osobou, aniž by poučení zaměstnanci společnosti porušili povinnosti. Rizika jsou v tomto případě spojena s trestnou činností, a to vloupáním do zabezpečené oblasti, přepadením poučené osoby manipulující s UI v zabezpečené oblasti i mimo zabezpečenou oblast, přepadením při přenášení a přepravě mimo zabezpečenou oblast společnosti. Další formou rizika je nátlak na poučenou osobu pod pohrůžkou násilí nebo vydíráním poučené osoby.

Míra rizika neoprávněného nakládání s UI je tedy snížena zejména umístěním zabezpečené oblasti v budově do místa, které není běžně dostupné a dalšími opatřeními fyzické bezpečnosti. Na základě těchto skutečností lze míru tohoto rizika považovat za střední.

2.2.3. Hrozba neoprávněného nakládání s UI při živelné pohromě či havárii

Existuje hrozba poškození nebo zničení UI požárem, výbuchem plynu a následným požárem nebo jinými živly. Při živelné pohromě může také dojít k neoprávněnému nakládání s UI v důsledku porušení bezpečnostních opatření při živelné pohromě. Při takové pohromě se mohou stát UI volně přístupné nebo může dojít k jejich zničení. Havárie může vzniknout např. v důsledku autonehody vozidla s nebezpečným nákladem. Tyto havárie by mohly omezit možnosti poučených osob nebo ostražky bezpečnostní agentury provádět OUI.

Rizika této skupiny jsou minimalizována na základě opatření specifikovaných v plánu zabezpečení objektu a zabezpečené oblasti v krizových situacích. Společnost považuje míru rizika neoprávněného nakládání při živelné pohromě za malou až střední.

2.2.4. Hrozba vyzaření UI pasivním odposlechem a nasazením operativní techniky

Tato hrozba je spojena s formou odposlechu nebo odezírání z prostor mimo zabezpečenou oblast. Ochrana před tímto rizikem spočívá v režimových a technických opatřeních, která znemožňují již samotnou instalaci a následně použití těchto prostředků.

Případnému odezírání je zabráněno umístěním zabezpečené oblasti do 3.NP. V zabezpečené oblasti se nachází jedno okno, přičemž za oknem je stahovací venkovní žaluzie, která se ovládá elektricky zevnitř zabezpečené oblasti. Tato žaluzie je určena pouze pro toto okno. Tato žaluzie zabrání jakékoliv možnosti odezírání.

Míra tohoto rizika je malá a toto riziko je minimalizováno pravidelným prováděním školení poučených osob a dodržováním všech režimových opatření a rozhodnutím, že v případě jakéhokoliv podezření bude provedena obranná prohlídka prostřednictvím NBÚ, a to na základě žádosti odpovědné osoby.

2.3. Stanovení celkové míry rizika

Odpovědná osoba posuzovala zejména druh, SU a rozsah UI, specifika manipulace s UI a jejich zranitelnosti vůči uvedeným hrozbám. Jednotlivá rizika byla klasifikována dle

reálnosti uplatnění hrozby a způsobených následků stanovením míry rizika na malé, střední nebo velké. V návaznosti na výše uvedený popis hrozeb a vyhodnocení zranitelnosti vůči hrozbám byla stanovena míra jednotlivých rizik. Na základě toho byla stanovena celková míra rizika jako **střední**.

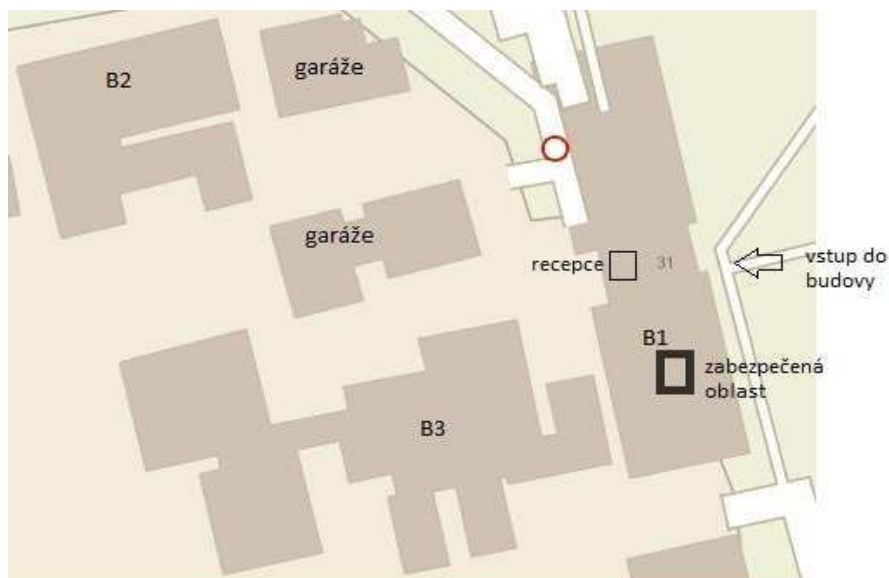
Tato celková míra je důležitá z pohledu fyzické bezpečnosti, protože na základě toho se dále porovnávají bodová ohodnocení přijatých opatření fyzické bezpečnosti s tabulkou hodnot nejnižší míry zabezpečení zabezpečené oblasti.

3. Určení objektu a zabezpečené oblasti včetně jejich hranic, určení kategorie a třídy zabezpečené oblasti

3.1. Popis areálu UAI, a.s.

Sídlo společnosti UAI, a.s. se nachází v areálu JČU v Českých Budějovicích 2, Branišovská 1160/31. Vlastníkem tohoto areálu je společnost UAI, a.s., IČO 01234567.

Schéma areálu:



Areál se skládá ze tří rozdílných vícepatrových administrativních budov označených B1, B2, B3. Do areálu je jeden vjezd z ulice Branišovská. Do objektu B1 se vstupuje hlavním vchodem z ulice Branišovská. V objektu B1 se ve 3. NP nachází zabezpečený objekt se zabezpečenou oblastí.

Všechny vstupy jsou zajištěny EZS s kamerovým systémem a autorizace se provádí pomocí čipové karty. Areál je pod nepřetržitou kontrolou ostrahy. Hlavní stanoviště ostrahy je v přízemí na recepci v budově B1.

Budovy B2, B3 sousedí ze západní strany s budovou B1.

Budova B2 je přízemní s jedním vstupem zajišťující vstup pouze po identifikaci čipovou kartou.

Budova B3 má 4NP. Její jediný vstup je nepřetržitě kontrolován kamerovým systémem a vstup do prostoru jednotlivých pater je po identifikaci čipovou kartou.

3.2. Stanovení objektu a jeho typu

Zabezpečený objekt je umístěn v areálu UAI, a.s. budova B1 ve 3. NP. Zabezpečený objekt tvoří vnější hranice místností č. 308 a č. 307. Podlahy a stropy jsou pevné stavební konstrukce z cihel. Stěny jsou lehké stavební konstrukce.

Hranice objektu splňují podmínky, že spodní okraje průlezného otvoru (okna) jsou více jak 5,5 m nad terénem a nelze k nim jednoduše proniknout ze střechy nebo za pomoci hromosvodů, okapů, parapetů, jiných stavebních prvků, terénních nerovností, stromů či jiných staveb.

Hranice objektu je po stavebních úpravách, kde veškeré skleněné výplně mimo okna byla nahrazena lehkou sádrokartonovou konstrukcí.

Při určení typu objektu je rozhodující ta část hranice objektu, která má nejnižší odolnost.

Z tohoto důvodu byl stanoven objekt typu S3 = 2.

3.3. Stanovení hranic objektu

Hranici zabezpečeného objektu tvoří místnost č. **329** a místnost č. **309b** umístěné v budově B1 ve 3. NP v areálu UAI, a.s., Branišovská 31, České Budějovice. Stropy a podlahy jsou betonové stavební konstrukce. V místnostech pod zabezpečeným objektem, v 2. NP budovy B1 jsou administrativní místnosti.

Místnost č. **329** se nachází na západní straně. V místnosti jsou dvě okna vybavena žaluziemi. Okna jsou umístěna více než 5,5 m nad terénem. Vstupní dveře do místnosti jsou pevné konstrukce a východní stěna je součástí zabezpečeného objektu.

Místnost č. **309b** se nachází na severní straně. V místnosti je jedno okno vybavené žaluziemi. Okna jsou umístěna více než 5,5 m nad terénem. Vstupní dveře jsou pevné konstrukce. Jižní strana místnosti je součástí zabezpečeného objektu.

Obě místnosti sousedí s administrativními místnostmi a jsou oddělené lehkou sádrokartonovou konstrukcí.

Hranice objektu i zabezpečené oblasti je zakreslena do výkresové části technické dokumentace fyzické bezpečnosti.

3.4. Stanovení zabezpečené oblasti a její hranice

Zabezpečená oblast, místnost č. **307** se nachází v zabezpečeném objektu a sousedí s místností č. **329**. Jižní stěna hranice zabezpečené oblasti je součástí opláštění budovy. Zabezpečená oblast má jedno okno, vybavené žaluziemi. Hranice zabezpečené oblasti je lehké stavební konstrukce. Zabezpečená oblast prošla stavební úpravou a skleněná výplň, mimo oken, byla nahrazena lehkou stavební konstrukcí. Dveře do zabezpečené oblasti jsou pevné konstrukce s požární odolností. Dveře nevykazují znaky poškození nebo opotřebení, které by mohlo znemožnit identifikovat pokusy o neoprávněný vstup.

Hranice objektu i zabezpečené oblasti jsou zakresleny do výkresové části technické dokumentace fyzické bezpečnosti.

Zabezpečenou oblast tvoří jedna místnost č. **307**. Zabezpečená oblast slouží jako úložna a pracoviště s UI certifikovanými na SU Důvěrné.

Zabezpečená oblast je vybavena skartačním strojem REXEL MERCURY RSM1130. Tento skartovač je nutný, jelikož se jedná o papírové dokumenty.

Zabezpečená oblast je kategorie Důvěrné, třídy II ve smyslu § 25, odst. 1, písm. c) a odst. 2, písm. b) ZOUI, tj. vstupem do zabezpečené oblasti nedochází k seznámení s UI.

3.5. Popis zabezpečení objektu a zabezpečené oblasti

Fyzickou bezpečnost tvoří systém opatření, jehož cílem je zabránit nepovolané osobě v přístupu do zabezpečené oblasti nebo zabránit poškození, znehodnocení, zničení či jinému ohrožení UI. Fyzická bezpečnost je soubor opatření, který zabraňuje neoprávněnému nakládání s UI nebo vniknutí nepovolané osoby do zabezpečené oblasti.

Vytvoření fyzické bezpečnosti má:

- odradit pachatele od úmyslu provést vloupání do zabezpečené oblasti
- znemožnit pokus o vloupání
- ztížit postup pachatelů
- zajistit zásah bezpečnostních složek, a tím zvýšit pravděpodobnost dopadení

3.5.1. Úschovné objekty a zámek

V zabezpečené oblasti se nachází skříňový trezor typu ASJ 1/I, který je certifikován NBÚ do 20. 5. 2013. Tento úschovný objekt typu 3 je osazen zámkem typu 2 certifikovaný NBÚ. Zámek splňuje požadavky bezpečnostní třídy B dle ČSN EN 1300.

SS1 = 3 body

SS2 = 2 body

(S1) = SS1 x SS2 = 6

3.5.2. Zabezpečená oblast

Zabezpečená oblast je ohraničena ostěním místnosti č. 329. Jižní stěna je součástí opláštění budovy a má jedno okno vybavené žaluziemi. Jelikož je východní hranice zabezpečené oblasti lehké stavební konstrukce, je zabezpečená oblast typu 1. Bezpečnostní protipožární dveře typu PYROSAFE jsou pevné konstrukce. Dveře nevykazují žádné známky poškození, které by mohly bránit pokusům identifikovat neoprávněný vstup.

Dveře do zabezpečené oblasti jsou osazeny bezpečnostní cylindrickou vložkou 2502 BDN SGHK 4 (DYNAMIC PLUS). Uzamykací systém typu 3 je certifikován NBÚ a jeho komponenty splňují požadavky bezpečnostní třídy 4 podle ČSN P ENV 1627.

SS3 = 1 bod

SS4 = 3 body

(S2) = SS3 x SS4 = 3

3.5.3. Hranice objektu

Hranici zabezpečeného objektu tvoří místnost č. 329 a místnost č. 309b. Stropy a podlahy jsou pevné stavební konstrukce. Stěny jsou lehké stavební konstrukce.

Hranice zabezpečeného objektu splňuje podmínky, že spodní okraje průlezného otvoru jsou více jak 5,5 m nad trémem a nelze k nim jednoduše proniknout ze střechy, nebo za pomoci hromosvodů, okapů, parapetu, jiných stavebních prvků, terénních nerovností, stromů či jiných staveb.

(S3) = 2 body

3.5.4. Systém kontroly vstupu do zabezpečeného objektu a oblasti

Kontrola jediného možného vstupu do zabezpečeného objektu je typu 2. Jedná se o systém kontroly vstupu ACS – LINE certifikovaný pro způsobilost typu 2, bodové hodnocení SS6=2. Tato kontrola vstupu je ovládána bezkontaktní čtečkou karet, která je umístěna před vstupními dveřmi do zabezpečeného objektu. Pokud se tedy oprávněná osoba neidentifikuje kartou na čtečce, bude i přes autorizovanou deaktivaci EZS přenesena poplachová signalizace na stanoviště ostrahy. Dále je kontrola vstupu doplněna i mechanickou zábranou, tj. uzamykatelnými dveřmi.

Kontrola jediného možného vstupu do zabezpečenej oblasti je typu 2. Jedná se o systém kontroly vstupu ACS – LINE certifikovaný pro způsobilost typu 2, bodové hodnocení SS6=2. Tato kontrola vstupu je ovládána bezkontaktní čtečkou karet, která je umístěna před vstupními dveřmi do zabezpečenej oblasti. Pokud se tedy oprávněná osoba neidentifikuje kartou na čtečce, bude i přes autorizovanou deaktivaci EZS přenesena poplachová signalizace na stanoviště ostražky. Dále je kontrola vstupu doplněna i mechanickou zábranou, tj. uzamykatelnými dveřmi.

SS6 = 2 body

3.5.5. Režim návštěv v objektu

Návštěvy jsou doprovázeny po celou dobu pobytu v objektu. Pobyt návštěvy je veden v evidenci „Kniha návštěv“ se záznamem identifikačních údajů návštěvy, doprovázejících osob a časové údaje o tom, kdy návštěva byla vykonána.

SS7 = 3 body

(S4) = SS6 + SS7 = 5 bodů

3.5.6. Ostraha

Fyzická ostraha budovy B1 areálu UAI, a.s. se zajišťuje nepřetržitě. Ostrahu vykonává jeden pracovník na recepci. Na centrální stanoviště ostražky je vyveden výstup signalizace poplachu EZS zabezpečenej oblasti. Ostraha je určena ke kontrole vnějšího prostoru zabezpečenej oblasti. Provádí základní kontrolu perimetru. Nemá povolení ke kontrole uvnitř zabezpečenej oblasti a zabezpečenej oblasti a v případě potřeby kontaktuje osobu, která oprávnění vstupovat do oblasti má. Ostraha má povinnost v rámci kontrol budovy B1 ověřovat neporušenost a uzamčenost vstupních dveří zabezpečenej oblasti.

SS8 = 2 body

3.5.7. Zařízení elektrické zabezpečovací signalizace

V zabezpečenej oblasti a zabezpečenej oblasti je použito certifikované zařízení EZS, včetně jednotlivých komponentů, které splňují požadavky podle ČSN EN 50 134 - 1 pro stupeň zabezpečení 3 (střední až vysoké riziko).

Jedná se o tyto komponenty:

- ústředna EZS DIGIPLEX EVO192 PARADOX SECURITY SYSTEMS
- detektor pohybu PIR
- tísňová tlačítka ELM-PA-G3-W
- detektor otřesu SAFE PROTECTOR (950)
- detektor rozbití skla GLASS TREK (457)
- magnetické kontakty MAS 353
- hlásič požáru kouřový optický 2351E
- ovládací klávesnice PSD-CJ1000
- siréna instalovaná na chodbě před vstupem do zabezpečenej oblasti

Ústředna EZS je instalována uvnitř zabezpečenej oblasti (místnost 307). Vstup do zabezpečenej oblasti ovládán pomocí klávesnice umístěné uvnitř této oblasti. Podobně vstup do

zabezpečeného objektu je ovládán pomocí druhé klávesnice umístěné uvnitř objektu za dveřmi. Detektor rozbití skla zajišťuje kontrolu oken. Detektor otřesu je umístěn u skříňového trezoru. Detektor pohybu kontroluje narušení, vniknutí do prostoru. Tísňová tlačítka jsou používána pracovníky při pocitu osobního ohrožení.

$$SS91 = 2 \text{ body}$$

Instalace zařízení EZS - v zabezpečené oblasti je realizována prostorová i plášťová ochrana a tísňový systém. Výstupní hlášení technických prostředků EZS, stejně jako signalizace EPS, je vyvedeno na stanoviště určené pro stálý výkon fyzické ostrahy.

$$SS92 = 3 \text{ body}$$

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

$$(S5) = SS8 + SS9 = 4 \text{ bodů}$$

3.5.8. Ochrana perimetru

Fyzická bariéra odpovídá oplocení bez speciálních bezpečnostních požadavků. Účelem je vyznačit hranice a zajistit minimální úroveň odrazení, může být tvořena jakýmkoli materiálem.

$$SS10 = 1 \text{ bod}$$

$$(S6) = (SS10 \times SS11) + SS12 + SS13 + SS14 + SS15 = 0$$

3.5.9. Zařízení elektrické požární signalizace

Je realizováno kouřovým optickým detektorem umístěným na stropě v zabezpečené oblasti. Hlásič je certifikován NBÚ.

Bez bodového ohodnocení

4. Tabulka bodového ohodnocení opatření fyzické bezpečnosti v zabezpečené oblasti

<p>Název: Místnost 307 ve 3. NP, budova B1 v sídle společnosti UAI, a.s., Branišovská 31, České Budějovice</p> <p>Kategorie: Důvěrné</p> <p>Třída: Třída II</p> <p>Typ: Typ 2</p> <p>Účel zabezpečené oblasti: Místnost č. 307 slouží jako úložna UI SU Vyhrazené nebo Důvěrné a pro zpracování nebo vytváření UI SU Vyhrazené nebo Důvěrné.</p>		
BEZPEČNOSTNÍ OPATŘENÍ	TYP	BODOVÉ OHODNOCENÍ
Úschovné objekty	<input type="checkbox"/> T. 4 – 4 body <input checked="" type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS1= 3
Zámky úschovných objektů	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input checked="" type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS2= 2
Celkové hodnocení úschovného objektu a jeho zámku	$S1 = SS1 \times SS2$	S1= 6
Zabezpečené oblasti	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input checked="" type="checkbox"/> T. 1 – 1 bod	SS3= 1
Uzamykací systémy zabezpečené oblasti	<input type="checkbox"/> T. 4 – 4 body <input checked="" type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS4= 3
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	$S2 = SS3 \times SS4$	S2= 3

Objekt UI	<input type="checkbox"/> T. 4 – 5 bodů <input type="checkbox"/> T. 3 – 3 body <input checked="" type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS3= 2
Kontrola vstupu	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input checked="" type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS6= 2
Režim návštěv v objektu UI a) Návštěvy s doprovodem b) Návštěvy bez doprovodu c) Návštěvy bez kontroly	<input checked="" type="checkbox"/> ad a) – 3 bod <input type="checkbox"/> ad b) – 1 bod <input type="checkbox"/> ad c) – 0bodů	SS7 = 3
Celkové hodnocení kontroly vstupu	S4 = SS6 + SS7	S4= 5
Ostraha	<input type="checkbox"/> T. 5 – 5bodů <input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input checked="" type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS8= 2
Zařízení elektrické zabezpečovací signalizace	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input checked="" type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS91= 2
Instalace zařízení elektrické zabezpečovací signalizace	<input type="checkbox"/> T. 4 – 4 body <input checked="" type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS92= 3
Mezivýsledek (SS 9)		SS9= 2
Celkové hodnocení ostrahy a systému EZS	S5 = SS8 + SS9	S5= 4

Fyzické bariéry	<input type="checkbox"/> T. 7- 12 bodů <input type="checkbox"/> T. 6 – 9 bodů <input type="checkbox"/> T. 5 – 7 bodů <input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input checked="" type="checkbox"/> T. 1 –1 bodů	SS10= 1
Kontrola vstupu v přístupových bodech fyzické bariéry a) Kontrola je realizována b) Kontrola není realizována	<input type="checkbox"/> ad a) – 1 bod <input checked="" type="checkbox"/> ad b) – 0 bodů	SS11= 0
Namátkové vstupní a výstupní prohlídky a) Prohlídky jsou prováděny b) Prohlídky nejsou prováděny	<input type="checkbox"/> ad a) – 1 bod <input checked="" type="checkbox"/> ad b) – 0 bodů	SS12= 0
Perimetrický detekční systém (PDS)	2 body	SS13= 0
Bezpečnostní osvětlení perimetru	2 body	SS14= 0
Celkové hodnocení ochrany perimetru	$S6 = (SS10 \times SS11) + SS12 + SS13 + SS14 + SS15$	S6= 0

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

Zabezpečená oblast kategorie Důvěrné	Míra rizika
	střední
Povinné: (S1) + (S2) + (S3)	11
Povinné: (S4) + (S5)	9
Nepovinné: (S6)	0
Celkový výsledek	20

Přijatá opatření fyzické bezpečnosti jsou pro střední míru rizika a pro kategorii zabezpečené oblasti Důvěrné splňují dané požadavky. Odpovědná osoba ověřila, že jednotlivá použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a právním předpisům v oblasti OUI.

5. Technická dokumentace fyzické bezpečnosti

5.1. Výkresová dokumentace

Hranice objektu a hranice zabezpečené oblasti ve 3. NP objektu B1 a rozmístění technických prostředků určených k ochraně UI v zabezpečeném objektu a zabezpečené oblasti. Výkresová dokumentace je v Příloze A.

5.2. Dokumentace technických prostředků

Dokumentace obsahuje výčet (název, počet) jednotlivých technických prostředků a základní údaje:

- certifikované technické prostředky v zabezpečené oblasti (kopie certifikátu a přílohy z doby instalace)
- necertifikované technické prostředky (zápis o posouzení shody z doby instalace).

5.3. Specifikace certifikovaných prostředků

Název technického prostředku	Počet	Číslo certifikátu	Popis
Mechanické zábranné prostředky:			
Bezpečnostní protipožární dveří	2	T0082/2008	SS3=2, SS4=1
Skříňový trezor typ ASJ 1/I	1	T0054/2010	Ukládání UI do stupně „Důvěrné“, SS1=3, SS2=2
Zámková bezpečnostní cylindrická vložka DYNAMIC PLUS	2	T0124/2008	Vstupní dveře do zabezpečené objektu a oblasti, SS4 = 3
Systém kontroly vstupu:			
Řídící jednotka pro kontrolu vstupu	2	T3007/2008	Řídící jednotka pro kontrolu vstupu umístěná v zabezpečené oblasti, SS6 = 2

Bezdotyková čtečka	2	T3006/2009	Kontrola vstupu bezkontaktní čtečkou do zabezpečeného objektu a oblasti, SS6 = 2
Magnetický kontakt MAS 353	2	T1117/2009	Detektor otevření, SS91 = 3
EZS - komponenty:			
Ústředna EZS5230	1	T1175/2007	SS91 = 3
Ovládací klávesnice	2	T1175/2007	Po zadání číselného kódu deaktivuje/aktivuje magnetické kontakty a detektor pohybu, SS91=3
Detektor pohybu PIR	4	T1026/2009	SS91 = 2
Otřesový detektor SAFE PROTECTOR	1	T1048/2009	SS91 = 3
Detektor rozbití skla GlassTrek	5	T1049/2009	SS91 = 3
Hlásič konvenční kouřový optický	2	T4009/2009	Detektor požáru
Tísňové tlačítko ELM-PA-G3-W	2	T1036/2009	Skrytá tlačítka pro žádost o pomoc, SS91=3
Siréna	2	-	Před vstupem do objektu a na stanovišti ostrahy
Skartační stroj REXEL MERCURY RSM1130	1	T5033/2010	Bez bodového omezení

6. PODMÍNKY POUŽÍVÁNÍ TECHNICKÝCH PROSTŘEDKŮ PO UPLYNUTÍ DOBY PLATNOSTI JEJICH CERTIFIKÁTŮ

6.1. Po uplynutí doby platnosti certifikátu

Takový technický prostředek může být dále nasazován jen v případě, pokud je doloženo, že byl pořízen a nasazený v době platnosti certifikátu NBÚ. Jeho další nasazení je podmíněno provedením funkční zkoušky technického prostředku ke dni nasazení. Po uplynutí doby

platnosti certifikátu může být prostředek použit za podmínky, že je plně funkční. To musí být ověřeno funkční zkouškou.

6.2. Pravidla pro provádění funkčních zkoušek jednotlivých technických prostředků

Provádění funkčních zkoušek v průběhu platnosti certifikátu NBÚ k technickému prostředku zajistí odpovědná osoba. Kontrola funkčnosti všech prostředku instalovaných za účelem OUI se provádí každých 12 měsíců.

Provádění funkčních zkoušek po skončení platnosti certifikátu NBÚ se provádí každých 12 měsíců. Provádí se u mechanických zábranných prostředků, kontroluje se funkčnost, neporušenost a celistvost, aby se dalo identifikovat případné pokusy o násilné vniknutí. Funkční zkoušky u EZS a tísňového systému se provádí dle TNI 33 45 91 – 3.

7. Provozní řád

7.1. Pravidla pro režim vjezdu a pohybu dopravních prostředků do areálu

Režim vjezdu a výjezdu vozidel do zabezpečené oblasti není řešen, neboť zabezpečenou oblastí je jedna místnost, jejíž hranice po celé své délce odpovídá hranici objektu. Z těchto důvodů řeší provozní řád společnosti pouze výjezd a vjezd do garáží. Vjezd do garáže je povolen jen služebním vozidlům.

7.2. Pravidla pro režim vstupu a pohybu osob v budově B1

V budově B1 se mohou samostatně pohybovat pracovníci vybaveni osobní kartou. Ostatní osoby (návštěvy) se mohou pohybovat pouze v doprovodu. Jména osob zdržujících se v zabezpečeném objektu se zapisují do příslušného záznamu na recepci. Osoby mohou do budovy vstoupit pouze přes recepci budovy. Ve vstupní hale je umístěno pracoviště recepce, které zajišťuje ostrahu, kontrolu a prvotní jednání s návštěvami. Obecně je cizím osobám vstup do budovy umožněn za účelem služebních jednání, návštěv, provádění dodavatelských prací ze strany cizích firem (výstavba, opravy, havárie apod.).

7.3. Pravidla pro režim pohybu osob v objektu a v zabezpečené oblasti

Do zabezpečeného objektu a zabezpečené oblasti mají povolen vstup pouze poučení pracovníci oprávnění k přístupu k UI Vyhrazené a Důvěrné. Ti obdrží prostředky umožňující vstup do zabezpečeného objektu. Ostatní poučení a oprávnění zaměstnanci budou moci vstupovat do zabezpečeného objektu pouze v jejich přítomnosti. Zaměstnanec, který není oprávněn k přístupu k UI, případně návštěvník, se může pak zdržovat v zabezpečeném objektu, případně zabezpečené oblasti jen po dobu nezbytně nutnou k výkonu jeho činnosti. UI budou v takovém případě uloženy v úschovném objektu. Za umožnění takového vstupu je odpovědný oprávněný pracovník, který má povinnost nenechat návštěvníka v zabezpečeném objektu nebo oblasti za žádných okolností samotného. Tím je zajištěno, že do zabezpečeného objektu, nebo oblasti nebudou mít přístup žádné nepovolané osoby. Navštívený zaměstnanec zapisuje osobu do Knihy návštěv, kde uvede tyto údaje: jméno a příjmení, číslo dokladu totožnosti (občanského průkazu, pasu, případně služebního průkazu), firmu, důvod návštěvy, jméno zaměstnance, se kterým bude jednáno a časové údaje o tom, kdy byla návštěva vykonána. Po ukončení návštěvy odepíše návštěvu z Knihy návštěv (doba odchodu) a odvede ji zpět na recepci.

Příslušníkům Policie ČR, orgánům státního požárního dozoru a inspektorům bezpečnosti práce je vstup do zabezpečeného objektu, nebo oblasti umožněn po předložení

jejich služebního průkazu a zapsání do knihy návštěv pouze za doprovodu oprávněné a poučené osoby. Zaměstnancům zdravotní služby, plynárenské, vodárenské a kanalizační služby, hasičům bez předložení průkazu totožnosti, pokud účelem vstupu je poskytování první pomoci, odvoz nemocného zaměstnance nebo havárie plynu, vody nebo požár, vyžadující rychlý a nezbytný zásah. V ostatních případech je nutné předložit průkaz totožnosti.

Odpovědná osoba rozhodla, že jakýkoliv vstup do zabezpečené oblasti je zapisován do záznamu o vstupu, přičemž se zapisuje:

- odemčení místnosti spojené s vypnutím EZS – datum, čas, jméno, podpis, důvod
- uzamčení místnosti spojené se zapnutím EZS – datum, čas, jménem podpis
- jména všech dalších osob, kterým byl pobyt v místnosti umožněn – datum, čas příchodu a odchodu, důvod pobytu, podpis doprovázející osoby

7.4. Bezpečnostní a kontrolní opatření při vstupu do zabezpečeného objektu

Opatření provádí poučený zaměstnanec v souladu s těmito pravidly:

- před vstupem do místnosti má povinnost ověřit neporušenost vstupních dveří a rámu. V případě, že zjistí rozpor, povolat pracovníka ostrahy a zajistit provedení záznamu do dokumentace recepcce. O případu informovat bezpečnostního ředitele
- při odemčení místnosti musí použít identifikační kartu pro kontrolu vstupu, bezprostředně vypnout EZS, ověřit neporušenost okna, dveří, vybavení
- při umožnění vstupu jiné osoby musí ověřit totožnost osoby, důvod vstupu, je třeba provést zápis do knihy návštěv
- při ukončení činnosti v místnosti se kontroluje uzavření okna, aktivuje se EZS
-

7.5. Bezpečnostní a kontrolní opatření při vstupu do zabezpečené oblasti

Opatření provádí poučený zaměstnanec v souladu se těmito pravidly:

- před vstupem do místnosti má povinnost ověřit neporušenost vstupních dveří a rámu. V případě, že zjistí rozpor, povolat pracovníka ostrahy a zajistit provedení záznamu do dokumentace recepcce. O případu informovat bezpečnostního ředitele
- při odemčení místnosti musí použít identifikační kartu pro kontrolu vstupu, bezprostředně vypnout EZS, ověřit neporušenost okna, dveří, vybavení
- při umožnění vstupu jiné osoby musí ověřit totožnost osoby, důvod vstupu, je třeba provést zápis do knihy návštěv
- při ukončení činnosti v místnosti se kontroluje uzavření okna, aktivuje se EZS

7.6. Pravidla pro režim pohybu UI v zabezpečeném objektu

Pravidla tvoří systém opatření, jehož cílem je ochrana UI při jejich přijímání, evidenci, zpracovávání, přepravě, ukládání, vyřazování, skartaci a archivaci, případně i jiné manipulaci v souladu s platnou legislativou, zejména se ZOUI a prováděcí vyhláškou.

Zaměstnanci, kteří byli poučeni odpovědnou osobou, byli proškoleni, jakým způsobem a kdy evidovat UI do manipulační knihy, a jakým způsobem se UI přenáší a přepravují.

7.7. Provozní dokumentace k technickým prostředkům - pravidla pro jejich používání

Veškeré mechanické zábranné prostředky jsou používány poučenými osobami, které je obsluhují v rámci výkonu své činnosti. Tyto osoby jsou poučeny, jak s prostředky manipulovat, jak předejít jejich poškození nebo zničení, aby nedošlo ke snížení úrovně OUI. V případě zničení nebo poškození jsou tyto osoby povinny informovat odpovědnou osobu. Odpovědná osoba provádí pravidelné kontroly všech prostředků instalovaných v zabezpečené oblasti s ohledem na jejich poškození, korozi, funkčnost apod. V případě zjištění poruchy se zajistí odstranění škody.

Systém EZS a kontrolu vstupu smí využívat pouze poučené osoby. Poučená osoba je proškolená a má kód pro obsluhu EZS. Tyto osoby musí zabránit seznámení se s kódem nepovolaným osobám. V případě ztráty kódu nebo vyzrazení musí tyto skutečnosti nahlásit odpovědné osobě.

Všechny poučené osoby jsou proškoleny z obsluhy skartovacího zařízení. Poučené osoby jsou povinny skartovat dokumenty určené k likvidaci pouze na zařízení certifikovaném NBÚ.

Provozní dokumentaci k technickým prostředkům tvoří dokumentace úschovných objektů, dokumentace EZS, dokumentace skartačního zařízení a dokumentace (karta) bezpečnostního zámku dveří.

Provozní dokumentace je uložena v zabezpečené oblasti. Za její úplnost, dodržení termínů kontrol funkčnosti a revizí instalovaných technických prostředků odpovídá bezpečnostní ředitel.

Záznam o vstupu do zabezpečené oblasti je umístěn tak, aby každý oprávněný pracovník mohl provádět nařízené záznamy.

7.8. Pravidla pro manipulaci s klíči

Manipulaci s klíči a vstupními kódy zahrnuje:

- klíče od zabezpečeného objektu
- klíče od zabezpečené oblasti
- klíče a číselné kombinace od úschovného objektu
- kódy EZS a identifikační karty s rozlišením povolené zóny (objekt, oblast)
- klíče a číselné kombinace od přenosných schránek

Vstupní dveře do zabezpečeného objektu jsou opatřeny jedním zámkem. Existuje 5 klíčů od vstupních dveří, přičemž každý má přiděleno pořadové číslo 1 až 5 (č. 1 - pracovník pověřený vedením jednacního protokolu, č. 2 - bezpečnostní správce IS, č. 3 - odpovědná osoba, č. 4 - pomocný klíč uložený v trezoru, č. 5 nouzový duplikát v zapečetěné krabici v trezoru záložních klíčů správy).

Vstupní dveře do zabezpečené oblasti jsou opatřeny jedním zámkem. Existuje 5 klíčů od vstupních dveří, přičemž každý má přiděleno pořadové číslo 1 až 5 (č. 1 pracovník pověřený vedením jednacního protokolu, č. 2 - bezpečnostní správce IS, č. 3 - odpovědná osoba, č. 4 - pomocný klíč uložený v trezoru, č. 5 nouzový duplikát v zapečetěné krabici v trezoru záložních klíčů správy).

O předání a vrácení klíčů se vede záznam, který se ukládá v úschovném objektu. Klíče od zabezpečeného objektu a zabezpečené oblasti mohou vlastnit pouze zaměstnanci, kteří jsou oprávněni seznamovat se s UI SU Vyhrazené a Důvěrné.

Ztráta klíče nebo jeho duplikátu od zabezpečeného objektu nebo oblasti musí být neprodleně oznámena odpovědné osobě. Neprodleně musí být provedena kontrola neporušenosti a správnosti pečeti vstupních dveří, neporušenosti interiéru místnosti, úschovného objektu a jeho pečeti. Následně se provádí výměna zámku.

Ztráta klíčů od úschovného objektu musí být neprodleně oznámena odpovědné osobě, osobě pověřené a bezpečnostnímu správci IS. Obdobně se oznamuje poškození, nebo ztráta obálky s náhradním klíčem. Při ztrátě klíčů musí být neprodleně provedena kontrola pečetění úschovného objektu a urychleně se realizuje výměna zámku.

K ovládání EZS jsou používány dvě skupiny kódů:

- Master kód pro nastavování systému a definování oprávnění
- Uživatelské kódy zajišťující možnost odlišení jednotlivých pracovníků

Přenosné schránky pro přepravu utajovaných dokumentů jsou vybaveny mechanickými nebo kombinačními zámky. Duplikáty klíčků a záložní údaje číselné kombinace centrálně používaných schránek se ukládají v zalepené obálce v úschovném objektu.

Poučeným osobám je zakázáno půjčovat klíče jiným osobám, zamezit jejich poškození nebo ztrátě nebo vytvářet jejich duplikáty. V případě zjištění některého z těchto způsobů porušení klíčového režimu, je poučená osoba povinna hlásit tuto skutečnost bezpečnostnímu řediteli, který zajistí odstranění závady a stanoví náhradní způsob OUI.

Z výše uvedeného je zřejmé, že klíče (identifikační prvky) od oblasti, kde se bude nakládat s UI, podléhají přísnějšímu režimu než všechny ostatní klíče.

Poučeným osobám přiděluje bezpečnostní ředitel pro vstup do zabezpečené oblasti identifikační bezkontaktní karty. Pracovníci jsou při přidělení karty poučeni, jakým způsobem se s kartou zachází, a že nesmí kartu půjčovat jinému pracovníkovi nebo si karty vyměňovat. Pro karty platí obdobný režim jako pro klíče.

7.9. Pravidla pro výkon ostrahy

V areálu UAI, a.s. je zajištěna nonstop fyzická ostraha zabezpečené oblasti prostřednictvím ostrahy, která se nachází v přízemí budovy B1 na recepci. Pracovníci ostrahy jsou osobami, které mají oprávnění ke vstupu k UI. Do místnosti centrály je vedena signalizace poplachu EZS zabezpečeného objektu a oblasti.

Pracovník ostrahy vykonávající svoji službu má uloženy povinnosti, mezi které patří zejména:

- kontrola, zda jsou všechny vstupní a výstupní dveře v budově uzamčeny
- kontrola osob, které se pohybují v budově
- obsluha technických zařízení ostrahy budovy (kamerový systém CCTV, EZS, EPS, automatické ovládání garážových vrat)
- vedení odpovídajících záznamů, především knihy recepční a vrátné služby a přítomnosti osob po pracovní době,
- organizování a přiměřené poskytování pomoci v nouzi osobám pobývajících v budově
- hlášení případné havarijní události na havarijní dispečink dle rozpisu

Na stanoviště ostrahy v recepci budovy B1 je na pracovní pult vyvedena:

- elektronická požární signalizace budovy
- elektronická zabezpečovací signalizace budovy B1, chodeb a schodišť, jedno z čidel je umístěno v blízkosti vstupních dveří do zabezpečeného objektu
- monitor a ovládací panel pro sledování kamer průmyslové televize (CCTV) instalovaných vně zabezpečené oblasti a na některých bodech vnějšího pláště budovy

V případě zjištění zvýšeného rizika ohrožení UI (pokus o zcizení UI, nefunkčnost nebo omezení funkčnosti technických prostředků ochrany zabezpečené oblasti, změna bezpečnostní situace apod.) se vyhláší stav ohrožení UI. Tento stav vždy vyhláší odpovědná osoba společnosti. Pracovníci ostrahy uzavřou budovu, zamezí dalším návštěvám a začnou s prováděním důsledných prohlídek osob dle rozhodnutí odpovědné osoby. Zároveň je zajištěna trvalá přítomnost minimálně jedné poučené osoby v zabezpečené oblasti.

V případě nálezů UI v prostorech budovy mimo zabezpečenou oblast, je pracovník, který UI našel povinen okamžitě o této skutečnosti informovat odpovědnou osobu a zásadně se s UI neseznamovat. Zároveň musí zajistit, aby se s UI neseznamovaly ani jiné další osoby. Do okamžiku předání UI odpovědné osobě, je nálezce povinen chránit tuto nalezenou UI před ztrátou, odcizením, poškozením, případně seznámením nepovolanou osobou.

8. Další opatření v oblasti fyzické bezpečnosti

Odpovědná osoba vypracuje formou tabulky plán kontrol opatření fyzické bezpečnosti pro každý kalendářní rok, který bude mimo jiné obsahovat:

- kontrolu ukládání protokolů o ověření funkčnosti a revizi EZS a vedení záznamů v provozní knize (průběžně)
- kontrolu ukládání záznamů o ověření funkčnosti technických zařízení, jejichž platnost certifikátu vypršela a mechanických zábranných prostředků (např. dveře), které nebyly v době pořízení certifikovány NBÚ
- kontrolu vedení seznamu osob oprávněných vstupovat do zabezpečené oblasti (průběžně)
- kontrolu vedení záznamů o uložení klíčů od zabezpečené oblasti a úschovných objektů (průběžně)
- kontrolu dodržování pravidel manipulace s klíči (průběžně)
- kontrolu vstupu do zabezpečené oblasti a evidence údajů o návštěvách

Odpovědná osoba dále zajistí:

- ověření, zda jednotlivá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a právním předpisům v oblasti OUI nejméně každých 12 měsíců. Z ověření je proveden písemný Záznam o kontrole
- zkoušku funkčnosti technických prostředků instalovaných v zabezpečené oblasti, a to dle pravidel stanovených odpovědnou osobou v části 7 tohoto projektu
- aktualizaci projektu fyzické bezpečnosti při každé změně opatření fyzické bezpečnosti

Vzor záznamu o kontrole:

Z á z n a m o k o n t r o l e

z a b e z p e č e n á o b l a s t

Byla provedena kontrola zabezpečené oblasti s tímto výsledkem:

1. byl prostudován projekt fyzické bezpečnosti a odpovídá skutečnému stavu
2. celková míra rizik zůstává střední
3. byla provedena funkční zkouška:
 - a. EZS,
 - b. zámku a neporušenosti vstupních dveří do zabezpečené oblasti
 - c. zámky a těla úschovných objektů (trezorů)
 - d. funkční zkouška skartovacího stroje

Výsledek kontroly:

Datum:

Podpis odpovědné osoby (bezpečnostního ředitele):

9. Plán zabezpečení objektu a oblasti v krizových situacích

Mimořádnou situaci definuje vyhláška NBÚ č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků v § 2, písm. i), a to jako stav, kdy bezprostředně hrozí, že dojde k vyzrazení nebo zneužití UI.

Týká se:

- neoprávněné nakládání s UI poučenými osobami (úmyslně i neúmyslně)
- neoprávněné nakládání s UI nepovolanou osobou (vniknutím do zabezpečené oblasti, odcizení klíčů, úmyslné způsobení havárie)
- neoprávněné nakládání s UI při havárii (požár, toxické látky, průmyslová havárie, výbuch plynu, apod.)
- neoprávněné nakládání s UI při teroristickém útoku nebo vandalismu (telefonická pohružka, demonstrace, nepokoje, apod.)
- únik UI z IS, riziko zničení dat
- vyzrazení UI pasivním odposlechem, nasazením operativní techniky

Společnost se snaží riziko vzniku mimořádných situací minimalizovat:

- pečlivým výběrem zaměstnanců a jejich prověřením v rámci bezpečnostního řízení
- pravidelným školením
- umístěním zabezpečené oblasti v budově do místa, které není běžně dostupné
- důslednou pravidelnou kontrolní činností všech opatření personální, administrativní a fyzické bezpečnosti, včetně opatření bezpečnosti IS

- opatřeními fyzické bezpečnosti (technickými prostředky, režimovými opatřeními a ostrahou)

Pro řešení mimořádných situací a snížení škod v případě jejich vzniku je rozhodující:

- včasnost rozpoznání možného rizika ohrožení UI
- úroveň realizace opatření
- rychlost řešení
- rychlost informování subjektů
- schopnost obnovit standardní stav OUI na úroveň před vznikem takové situace

9.1. Zásady obecného postupu při řešení mimořádné situace

Pokyny a postup pro OUI v případě vzniku krizové situace:

- rychle analyzovat druh krizové situace
- vyhlásit stav ohrožení UI
- uzavřít úložný objekt
- zvolit optimální řešení s cílem ochrany lidských životů a docílení co nejmenší škody
- informovat odpovědnou osobu o vzniku krizové situace, paralelně informovat ostrahu
- realizovat opatření k odstranění následků krizové situace
- zabezpečit OUI do doby obnovy standardního stavu
- provést analýzu příčin vzniku krizové situace a navrhnout nápravná a preventivní bezpečnostní opatření
- neposkytovat informace o krizových situacích nepovolaným osobám s odvoláním na odpovědnou osobu

9.2. Povinnosti poučených zaměstnanců při řešení mimořádné situace

Všichni zaměstnanci poučení odpovědnou osobou jsou povinni:

- zamezit neoprávněné manipulaci s UI
- uzavřít úložný objekt
- zamezit neoprávněnému seznámení s UI nepovolaným osobám, ale brát v potaz prioritu lidského života
- ukončit manipulaci s UI
- minimalizovat dopad neoprávněné manipulace s UI
- okamžitě informovat odpovědnou osobu
- neposkytovat informace ostatním zaměstnancům, cizím osobám, případně médiím
- řídit se pokyny odpovědné osoby

9.3. Povinnosti bezpečnostního ředitele (odpovědné osoby)

Bezpečnostní ředitel je v případě vzniku krizové situace povinen:

- dostavit se neprodleně do budovy, kde je lokalizována zabezpečená oblast, pokud se nachází mimo tuto budovu
- vyhodnotit celou situaci, zvážit možné následky a přijmout přiměřená opatření k řešení celé situace
- koordinovat postup ostražky a ostatních přítomných poučených zaměstnanců
- informovat o krizové situaci odpovědnou osobu
- řídit a koordinovat vzniklou situaci v souladu s tímto plánem
- přijmout opatření k obnově původního stavu ochrany UI
- oznámit orgánům činným v trestném řízení případné spáchání trestného činu
- provést zápis o krizové situaci, do zprávy uvést případnou neoprávněnou manipulaci s UI, ve zprávě navrhnout soubor preventivních a nápravných opatření

9.4. Pokyny pro ochranu UI v případě vzniku mimořádné situace

Při havárii inženýrských sítí (voda, plyn, elektroinstalace) a při vzniku požáru (jiné živelné pohromy) má správce budovy povinnost ihned oznámit bezpečnostnímu řediteli (odpovědné osobě) vzniklou krizovou situaci. Tuto povinnost má i kterýkoliv pracovník, který takovou situaci zjistí. Pokud není v budově přítomen bezpečnostní ředitel (odpovědná osoba), bude řídit postup evakuace či likvidace v zabezpečené oblasti poučený zaměstnanec. Ten bude řídit zajištění ochrany UI (před zneužitím nebo vyzrazením) a jejich následnou obnovu.

Při vzniku požáru (jiné živelné pohromy) je potřeba ihned uvědomit také Policii ČR a podle rozsahu požáru a stupně nebezpečí ohrožení také plynárenskou, vodárenskou a energetickou společnost. Při teroristickém útoku nebo vyhlášení stavu ohrožení učiní první nezbytná opatření k odvrácení nebezpečí a přivolání pomoci poučený zaměstnanec, který se nachází v danou chvíli v zabezpečené oblasti a současně vyrozumí bezpečnostního ředitele (odpovědnou osobu) společnosti dle pokynů (telefonního spojení) uložených v zabezpečené oblasti a uvedených ve smlouvě s bezpečnostní agenturou. Další postup a případné zajištění UI před zneužitím nebo vyzrazením a jejich následnou obnovu řídí bezpečnostní ředitel společnosti nebo jím pověřená - poučená osoba v koordinaci s pracovníky ostražky a přivolanou pomocí.

Hlavním cílem je zamezení přístupu nebo v rámci likvidace katastrofy k přístupu nebo manipulaci s UI neoprávněnými osobami. Při zjištění neoprávněného nakládání nebo ztrátě UI je odpovědná osoba povinna tyto skutečnosti bez zbytečného odkladu oznámit písemně NBÚ, včetně opatření přijatých k nápravě. Veškerá tato zjištění neoprávněného nakládání nebo ztráty musí být odpovědnou osobou neprodleně evidována a vyhodnocována.

Základní podmínkou při jakékoli krizové situaci v zabezpečené oblasti je povinností vyrozumět odpovědnou osobu společnosti. O všech mimořádných situacích musí být sepsán protokol s podrobným popisem mimořádné události a s přijatými opatřeními k nápravě a osoba pověřená vedením jednacního protokolu provede evidenci dle ZOUI a prováděcích předpisů, dále pak odpovědná osoba (bezpečnostní ředitel) provede oznámení orgánu nebo organizaci, které mu UI poskytly a NBÚ. Za sepsání protokolu o mimořádné situaci a kontrolu zodpovídá odpovědná osoba.

9.5. Vyhlášení stavu ohrožení UI

Stav ohrožení vyhláší bezpečnostní ředitel nebo odpovědná osoba na základě zjištění zvýšeného rizika ohrožení UI.

Během stavu ohrožení se dodržují opatření:

- zákaz přenášení nebo přepravy UI nebo další manipulace s výjimkou případné evakuace nebo kontroly
- posílení výkonu ostrahy
- zpřísnění regulace režimu vstupu do budovy i do zabezpečené oblasti, zavedení prohlídek osob
- zpřísnění jiných zavedených režimů

9.6. Evakuace

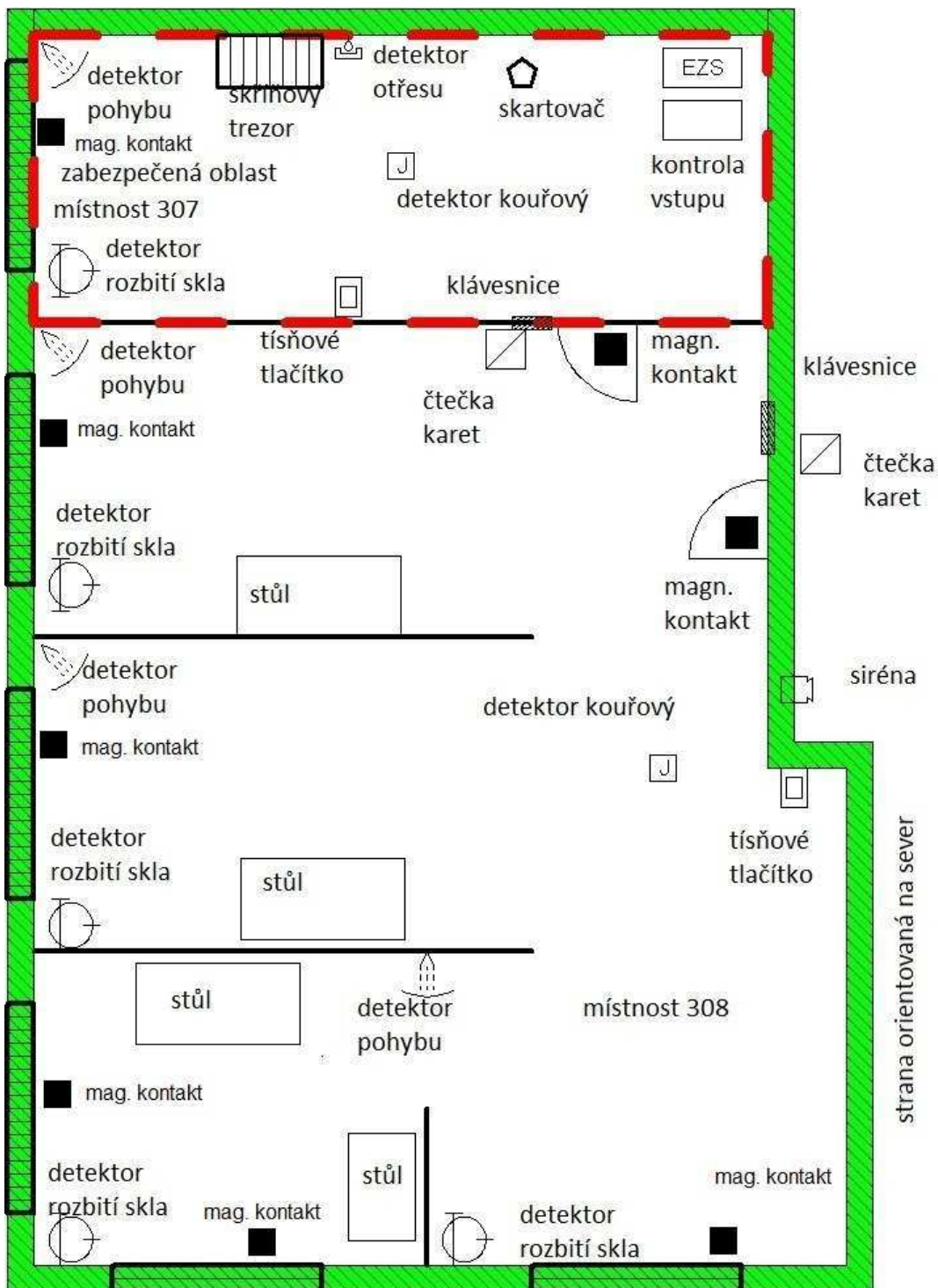
Poučené osoby přítomné v zabezpečené oblasti ukončí veškerou práci a na základě pokynů odpovědné osoby provedou přípravu UI k evakuaci. Poučené osoby uloží UI do přenosných schránek připravených v souladu s platnou legislativou a směrnicí zajišťující administrativní bezpečnost, a tyto přenosné schránky uloží do úschovného objektu, který řádně uzavřou a uzamknou. K UI uloženým do úschovných schránek se přiloží seznam obsažených UI. Zabezpečená oblast se uzamkne a aktivuje se EZS.

Bezpečnostní ředitel vyhlásí stav ohrožení UI, sepíše seznam UI ve dvou výtiscích, přičemž jeden přiloží k UI, jak bylo uvedeno výše. Druhý výtisk si ponechá u sebe. Poté zajistí podmínky pro evakuaci UI. Odpovědná osoba rozhodne, zda budou UI ponechány v zabezpečené oblasti nebo budou přepraveny na předem určené místo.

Následnou evakuaci ze zabezpečené oblasti nebo budovy řídí odpovědná osoba. V případě její nepřítomnosti řídí evakuaci jiná pověřená osoba.

Evakuační cesta vede schodištěm do vstupního vestibulu a zaměstnanci se shromáždí před budovou na ulici Branišovská. Pokud by šlo o evakuaci řízenou orgány ČR, bude evakuace shromážděných zaměstnanců probíhat dále podle pokynů sdělovacích prostředků.

Příloha A - Rozmístění technických prostředků v zabezpečeném objektu a zabezpečené oblasti



Legenda



- Detektor pohybu



- Detektor rozbití skla



- Skříňový trezor



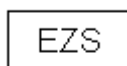
- Detektor otřesový



- Detektor kouřový



- Tísňové tlačítko



- Ústředna



- Kontrola vstupu



- Klávesnice



- Čtečka karet



- Magnetický kontakt

Příloha B - Certifikáty technických prostředků

Příloha č. 2 k vyhlášce č. .../2005 Sb.

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Pošt. příhr. 49

150 06 Praha 56

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

C E R T I F I K Á T **technického prostředku**

Evidenční číslo: ...

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

Výrobce:

Sídlo/trvalý pobyt/ místo podnikání/adresa:

IC/ rodné číslo:

Držitel:

Sídlo/trvalý pobytu/místo podnikání/adresa:

IC/ rodné číslo:

Tento certifikát potvrzuje ověření způsobilosti technického prostředku typu:

.....

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

.....

Platnost certifikátu do:

Datum vydání certifikátu:

Otisk úředního razítka

Podpis oprávněného zástupce

Přílohy:

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



PAVUS, a.s.
Autorizovaná osoba AO 216, Notifikovaná osoba 1391
Prosecká 412/74, 190 00 Praha 9 – Prosek
Rozhodnutí o autorizaci č. 46/2006 ze dne 22. listopadu 2006

CERTIFIKÁT VÝROBKU

č. 216/C5a/2008/0041
vydaný pro

výrobce:
CAG s.r.o., Kytín 19, 252 10 Mníšek pod Brdy, IČ: 25686925
místo výroby:
CAG s.r.o., Kytín 19, 252 10 Mníšek pod Brdy
stát původu výrobku:
Česká republika

V souladu s ustanovením § 5a odst. 1 nařízení vlády č. 163/2002 Sb., kterým se stanoví technické požadavky na vybrané stavební výrobky, ve znění nařízení vlády č. 312/2005 Sb. (dále jen „nařízení vlády č. 163/2002 Sb.“), Autorizovaná osoba AO 216 potvrzuje, že u stavebního výrobku:

Bezpečnostní protipožární dveře PYROSAFE SF

přezkoumala podklady předložené výrobcem, provedla počáteční zkoušku typu výrobku na vzorku a posoudila systém řízení výroby výrobků výrobcem a zjistila, že uvedený výrobek splňuje požadavky stanovené technickými předpisy, které souvisejí se základními požadavky uvedenými ve Stavebním technickém osvědčení č. S-216/C5a/2008/0041 ze dne 14. března 2008 (dále jen „STO“).

Autorizovaná osoba AO 216 zjistila, že systém řízení výroby výrobků výrobcem odpovídá příslušné technické dokumentaci a zabezpečuje, aby výrobky uváděné na trh, splňovaly požadavky stanovené ve shora uvedeném stavebním technickém osvědčení a odpovídaly technické dokumentaci podle § 4 odst. 3.

Nedílnou součástí tohoto certifikátu je Protokol o certifikaci č. P-216/C5a/2008/0041 ze dne 26. března 2008, který obsahuje závěry zjišťování, ověřování, výsledky zkoušek a základní popis certifikovaného výrobku, nezbytný pro jeho identifikaci.


Tento certifikát zůstává v platnosti po dobu, po kterou se požadavky stanovené ve stavebním technickém osvědčení, na které byl uveden odkaz, nebo výrobní podmínky v místě výroby a systém řízení výroby výrobků výrobcem, výrazně nezmění.

Autorizovaná osoba AO 216 provádí nejméně jedenkrát za 12 měsíců dohled nad řádným fungováním systému řízení výroby v místě výroby u výrobce podle § 5a nařízení vlády č. 163/2002 Sb.

Pokud Autorizovaná osoba AO 216 zjistí nedostatky, je oprávněna zrušit nebo změnit tento certifikát

V Praze dne 26. března 2008




Ing. Jaroslav Dufek
ředitel PAVUS, a.s. – AO 216

Posuzované vlastnosti certifikovaného výrobku jsou uvedeny na druhé straně tohoto certifikátu.

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Pošt. příhr. 49
150 06 Praha 56

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

CERTIFIKÁT

technického prostředku

Evidenční číslo: T1175/2007

Ústředna EZS

DIGIPLEX EVO192

(Název a typové označení technického prostředku)

Výrobce: PARADOX SECURITY SYSTEMS

Sídlo: Kanada

IČ:

-

Držitel: VARIANT plus, spol. s r.o.

Sídlo: U Obůrky 5

IČ:

674 01 Třebíč

46 96 71 68

Tento certifikát potvrzuje ověření způsobilosti technického prostředku typu:

3

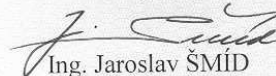
Bodové hodnocení technického prostředku podle přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků:

SS91=3

Platnost certifikátu do: 15.10.2010

Datum vydání certifikátu: 28.12.2007

Náměstek ředitele
Národního bezpečnostního úřadu


Ing. Jaroslav ŠMÍD



011431

Přílohy: 1/1

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

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD

Pošt. příhr. 49
150 06 Praha 56

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

PŘÍLOHU K CERTIFIKÁTU

Evidenční číslo: T1175/2007

Příloha číslo: 1

Omezující skutečnosti:

Ústředna EZS je certifikovaná s následujícími komponenty:

- klávesnice DGP2-648 LED, DGP2-640 ICON, EVO-641 LCD CZ, GRAFICA, DGP2-ANC1;
- expandéry DGP2-ZX1 BUS, APR3-ZX4 BUS, APR3-ZX8 BUS;
- moduly APR3-PGM4 BUS, APR3-HUB2 BUS, IP 100, VDMP3 CZ.

Při použití bezdrátové nadstavby a příslušenství splňuje ústředna požadavky typu 2 (SS91=2). Typ 2 je u bezdrátových systémů vázán na signalizaci demontáže z instalační plochy.

Platnost certifikátu do: 15.10.2010

Datum vydání certifikátu: 28.12.2007

Otisk úředního razítka



Náměstek ředitele

Národního bezpečnostního úřadu

J. Šmíd
Ing. Jaroslav ŠMÍD

Certifikát a přílohu lze reprodukovat pouze společně.