

## **Výklad k § 4 odst. 4 vyhlášky č. 366/2001 Sb.**

### **Bezpečnost informačního systému pro certifikační služby (ISCS) z hlediska požadavků objektové bezpečnosti**

*Dokument je určen všem poskytovatelům certifikačních služeb, kteří vydávají nebo uvažují o vydávání kvalifikovaných certifikátů. Je stručným náhledem na celou problematiku zabezpečení prostor pro činnost, která se v souladu s § 4 odst. 4 vyhlášky provádí v prostorách, které musí být zabezpečeny obdobně jako objekty kategorie „D“.*

## Obsah

Výklad k § 4 odst. 4 vyhlášky č. 366/2001 Sb.

### Bezpečnost informačního systému pro certifikační služby (ISCS) z hlediska požadavků objektové bezpečnosti

Obsah .....	2
1 Úvod do problematiky .....	3
2 Komentář a výklad .....	4
3 Dokumentace.....	4
3.1 Povinné dokumenty PCS.....	4
3.2 Doporučené dokumenty PCS.....	5
4 Ochrana objektu .....	6
4.1 Fyzická ostraha objektu.....	6
4.2 Technické prostředky k zabezpečení objektů kategorie „D“.....	6
4.3 Režimová opatření.....	7
4.4 Zacházení s klíči od úschovných objektů.....	7
4.5 Oprávnění ke vstupu do objektu .....	8
4.6 Vnější ochrana objektu.....	8
4.7 Vnitřní ochrana objektu.....	8
4.8 Vyhodnocení rizik.....	9
5 Použité zkratky.....	9
6 Literatura .....	10

# 1 Úvod do problematiky

Bezpečnost informačního systému pro certifikační služby obecně řeší prováděcí vyhláška [1] č. 366/2001 Sb. v § 4 odst. 4.

Příslušné citace z této vyhlášky:

## § 4

*(4) Prostory, kde dochází k činnosti podle odstavců 1 až 3 (§ 4) a podle § 5 odst. 1, musí být zabezpečeny obdobně jako objekty kategorie „D“ podle zvláštního právního předpisu.*

Tímto zvláštním právním předpisem je vyhláška [2] Národního bezpečnostního úřadu (dále **NBÚ**).

## § 4

*(1) Používaný informační systém pro certifikační služby se považuje za bezpečný, pokud u dat, která zpracovává, je zajištěna důvěrnost, integrita, dostupnost a prokazatelnost jejich původu a pokud odpovídá požadavkům technické normy upravující oblast informační bezpečnosti.*

Touto technickou normou je: ČSN ISO/IEC 15408 [3].

## § 4

*(2) Za účelem doložení bezpečnosti postupů podle § 6 odst. 1 písm. j) zákona o elektronickém podpisu poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajistí zaznamenávání událostí při:*

- a) vydání kvalifikovaných certifikátů,
- b) ukončení platnosti kvalifikovaných certifikátů,
- c) nakládání s daty pro vytváření elektronického podpisu a jim odpovídajícími daty pro ověřování elektronického podpisu poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty (dále jen „párová data poskytovatele“), a to během jejich celého životního cyklu, a
- d) nakládání s kvalifikovaným certifikátem poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty, a to během celého životního cyklu tohoto certifikátu.

## § 4

*(3) Záznamy o událostech podle odstavce 2 musí být pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, dostupnosti, integrity, časové autentičnosti a důvěrnosti těchto záznamů.*

## § 5

### **Bezpečnost postupu při nakládání s párovými daty poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty**

*(1) Při vytváření, používání a uchovávání párových dat poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty musí být jakákoliv manipulace s těmito daty prováděna:*

- a) výhradně fyzickými osobami, které jsou pro tuto činnost určeny poskytovatelem certifikačních služeb vydávajícím kvalifikované certifikáty,
- b) podle postupů stanovených certifikační prováděcí směrnici, a
- c) v souladu se systémovou bezpečnostní politikou.

## 2 Komentář a výklad

Prováděcí vyhláška [1] stanovuje, že poskytovatel certifikačních služeb (dále **PCS**) musí určitou činnost provádět v chráněných prostorách, které musí být zabezpečeny **obdobně jako objekty kategorie „D“** vyhlášky [2] NBÚ. Z tohoto předpisu byla využita z kategorizace objektů pouze kategorie „D“, neboť požadavky na zabezpečení prostor PCS, ve kterých bude docházet k činnosti podle § 4 odst. 1 až 3 a § 5 odst. 1 vyhlášky [1] (dále **zabezpečená činnost**), jsou z hlediska zabezpečení objektu obdobné. Podobně jsou kladeny nároky na oblast informační bezpečnosti v technických normách informační technologie.

**Zabezpečenou činností PCS** se zejména rozumí činnost spojená s:

- podepisováním kvalifikovaných certifikátů (dále **QC**) zaručeným elektronickým podpisem PCS;
- podepisováním seznamů QC, které byly zneplatněny;
- uvedením do provozu a změnami provozního režimu nástroje elektronického podpisu (dále **EP**);
- nakládáním s párovými daty PCS, a to během jejich celého životního cyklu;
- dalšími pracemi, které specifikuje PCS ve vlastní bezpečnostní dokumentaci, např. v certifikační prováděcí směrnici (dále **CPS**), v systémové bezpečnostní politice (dále **SBP**) aj.

**Zabezpečené prostory PCS**, které se zabezpečují obdobně jako **objekty kategorie „D“**, určuje PCS, který vydává kvalifikované certifikáty. Jsou to zejména prostory, kde se provádí:

- zabezpečená činnost PCS;
- další prostory, které jsou určeny v dokumentaci objektové bezpečnosti a v bezpečnostní dokumentaci PCS, např. v certifikační prováděcí směrnici, v systémové bezpečnostní politice aj.

Požadavky na vytvoření zabezpečených prostor u PCS, s obdobným zabezpečením jako objekty kategorie „D“ podle vyhlášky [2], byly určeny na základě obdobných požadavků k provádění zabezpečené činnosti PCS. Konkrétně stanovená opatření ochrany prostoru ve vyhlášce [2] jsou vhodná i pro prostory PCS.

Doporučuje se, aby PCS popsal v příslušné povinné a doporučené dokumentaci svého Informačního systému pro certifikační služby (dále **ISCS**) zabezpečení objektové bezpečnosti s rozsahem a požadovanými detaily podle typu příslušné dokumentace. Rovněž se doporučuje, aby PCS konkretizoval oddělení prostorů, ve kterých bude docházet k zabezpečené činnosti PCS, od ostatních prostorů. Důležité je, aby byl přesně vymezen ISCS a prostory, které mají být zabezpečeny obdobně jako objekty kategorie „D“ podle vyhlášky [2].

**Zabezpečené prostory PCS** budeme z důvodu ujednání terminologie s vyhláškou [2] a dalšími dokumenty NBÚ považovat za **objekty a zabezpečené oblasti kategorie „D“**.

## 3 Dokumentace

### 3.1 Povinné dokumenty PCS

Povinné dokumenty se v souladu s § 2 odst. 1 vyhlášky [1] předkládají při žádosti o akreditaci. Ve vztahu k bezpečnosti ISCS a z hlediska požadavků objektové bezpečnosti se doporučuje v jednotlivých dokumentech uvést:

- **certifikační politika** – zásady, podle kterých je realizována bezpečnost prostor, kde PCS zajišťuje služby spojené s elektronickými podpisy;
- **certifikační prováděcí směrnice** – informace o uplatňovaných postupech při zajišťování služeb spojených s elektronickými podpisy;
- **celková bezpečnostní politika** – způsob zajištění celkové bezpečnosti PCS;

- **systémová bezpečnostní politika** – konkrétní způsob zajištění bezpečnosti ISCS (způsoby ochrany dat, popis bezpečnostních opatření, vyhodnocení analýzy rizik, ...);
- **plán pro zvládání krizových situací** – postupy (včetně krizového plánu ochrany objektu), které jsou uplatněny v případě mimořádné události;
- **plán obnovy**, ve kterém jsou stanoveny postupy pro obnovu řádné funkce ISCS.

### 3.2 Doporučené dokumenty PCS

Doporučené dokumenty zpracovává PCS většinou na základě požadavků daných jinými normami, které přímo nejsou uvedeny v zákoně [4] nebo ve vyhlášce [1]. Skutečnosti týkající se problematiky objektové bezpečnosti z hlediska zajištění bezpečnosti ISCS se doporučuje uvést v následujících dokumentech:

#### A Směrnice a metodické pokyny PCS

V dokumentu se popisují např. další požadavky na osoby poskytovatele, dále způsob auditu, kontroly chování zaměstnanců PCS, dozor nad chováním zaměstnanců poskytovatele apod. V metodických pokynech může být např. rozbor bezpečnostního incidentu, který se stal a výklad správného a závazného chování osob v jednotlivých rolích zaměstnavatele tak, jak je upraven v předpisové základně poskytovatele.

#### B Dokumentace objektové (fyzické) bezpečnosti

(kap. 15 „Bezpečnostní standardy [5] NBÚ objektové (fyzické) bezpečnosti“)

##### 1. Vyhodnocení rizik

(§ 14 odst. 1 písm. a) vyhlášky [2]; kap. 15.1. Bezpečnostní standardy [5]

V dokumentu se specifikují aktiva, vyhodnocují jednotlivé hrozby a zranitelnost, stanovuje se míra rizika jako „malé“, „střední“ nebo „velké“ riziko.

##### 2. Bezpečnostní projekt ochrany objektu

(§ 14 odst. 1 písm. b) vyhlášky [2]; kap. 15.2. Bezpečnostní standardy [5]

Dokument obsahuje umístění zabezpečených oblastí v objektu a způsob použití bezpečnostních opatření při vnější a vnitřní ochraně objektu.

##### 3. Tabulka bodového ohodnocení bezpečnostních opatření v zabezpečené oblasti

(kap. 15.3. Bezpečnostní standardy [5])

Dokument podle standardu [5] obsahuje bodové ohodnocení jednotlivých konkrétních bezpečnostních opatření a výpočty pro možné porovnání s hodnotami v tabulce minimálních hodnot.

##### 4. Technická dokumentace objektové bezpečnosti

(§ 14 odst. 1 písm. c) vyhlášky [2]; kap. 15.4. Bezpečnostní standardy [5])

- **výkresová dokumentace**, která obsahuje zejména vyznačení hranice objektu, hranic jednotlivých zabezpečených oblastí a rozmístění technických prostředků určených k ochraně zabezpečených prostor PCS;
- **dokumentace technických prostředků**, která obsahuje zejména výčet (název, počet a v případě více typů jednoho druhu technického prostředku i umístění) a základní údaje:
  - a) Certifikované technické prostředky – kopie certifikátu a přílohy (pokud není příloha, vypsát typ a ohodnocení technického prostředku z dostupných zdrojů NBÚ);
  - b) Necertifikované technické prostředky – zápis (uvést specifikaci a způsob použití) o ověření shody s bezpečnostními standardy, který je podepsaný statutárním orgánem.

## 5. Provozní řád

(§ 14 odst. 1 písm. d) vyhlášky [2]; kap. 15.5. Bezpečnostní standardy [5]

- a) Pravidla pro režim pohybu osob;
- b) Provozní dokumentace k technickým prostředkům;
- c) Pravidla pro manipulaci s klíči od vstupů do objektu a zabezpečených oblastí a s klíči od úschovných objektů;
- d) Pravidla pro výkon fyzické ostrahy.

## 6. Krizový plán ochrany objektu

(§ 14 odst. 1 písm. e) vyhlášky [2]; kap. 15.6. Bezpečnostní standardy [5]

- a) Popis mimořádných situací, které vyplývají z procesu vyhodnocení rizik;
- b) Pokyny k ochraně zabezpečené činnosti a zabezpečených prostor PCS v případě vzniku mimořádné situace.

Údaje uvedené v doporučených dokumentech není třeba v povinných dokumentech „opakovat“. Lze se na doporučené dokumenty pouze odvolávat.

Dokumentace objektové bezpečnosti je uložena u statutárního orgánu PCS nebo jím pověřené osoby. Statutární orgán odpovídá za shodu dokumentace se skutečným stavem bezpečnostních opatření odpovídajících vyhodnoceným rizikům.

Kontrola shody skutečného stavu s dokumentací se provádí nejméně každých 12 měsíců. Při realizaci objektové bezpečnosti musí být dodržena zásada, že počet osob, které jsou určovány k seznamování s informacemi o technických prostředcích a bezpečnostních opatřeních k ochraně objektů, se musí omezit pouze na osoby, které se na procesu realizace objektové bezpečnosti nezbytně podílejí.

## 4 Ochrana objektu

Ochrana objektu se zabezpečuje kombinací bezpečnostních opatření, kterými jsou:

- a) fyzická ostraha objektu,
- b) technické prostředky,
- c) režimová opatření.

### 4.1 Fyzická ostraha objektu

U objektů kategorie „D“ se zajišťuje nepřetržitě. Fyzickou ostrahu objektu zajišťuje na stanovišti určeném pro stálý výkon ostrahy objektu nejméně 1 pracovník fyzické ostrahy objektu. Stanoviště určené pro stálý výkon fyzické ostrahy objektu může být umístěno mimo tento objekt za předpokladu, že kombinace bezpečnostních opatření (fyzická ostraha objektu, technické prostředky, režimová opatření) umožní náležitě rychlý zásah. Na stanoviště určené pro stálý výkon fyzické ostrahy objektu musí být vyveden výstup hlášení od zařízení elektrické zabezpečovací signalizace sloužící ke zjišťování a vyhodnocování neoprávněného vstupu. K fyzické ostraze objektu lze využít i strážní službu. Pravidla pro výkon strážní služby je nutno stanovit písemnou formou. Povinnosti osob, které strážní službu vykonávají, stejně jako intervaly obchůzek, se stanovují v závislosti na míře rizika a v závislosti na ostatních použitých bezpečnostních systémech.

### 4.2 Technické prostředky k zabezpečení objektů kategorie „D“

K ochraně hranic objektů kategorie „D“ se používají:

- mechanické zábranné prostředky, kterými jsou úschovné objekty, zámky, dveře, mříže, fólie, bezpečnostní rámy a skla,
- zařízení elektrické zabezpečovací signalizace sloužící ke zjišťování a vyhodnocování neoprávněného vstupu.

**K ochraně zabezpečené oblasti** kategorie „D“ se používají:

- mechanické zábranné prostředky, kterými jsou úschovné objekty, zámky, dveře, mříže, fólie, bezpečnostní rámy a skla,
- zařízení elektrické zabezpečovací signalizace sloužící ke zjišťování a vyhodnocování neoprávněného vstupu,
- zařízení fyzického ničení nosičů informací.

**K ochraně zabezpečené oblasti** kategorie „D“, v nichž je zajištěna trvalá přítomnost zde pracujících osob, se používají:

- mechanické zábranné prostředky, kterými jsou úschovné objekty, zámky, dveře, mříže, fólie, bezpečnostní rámy a skla,
- tísňové systémy, zejména tísňové hlásiče, které fungují jako součást elektrické zabezpečovací signalizace.

Technické prostředky splňující požadavky, které stanoví vyhláška [2], jsou většinou již certifikovány NBÚ jako způsobilé pro navrženou kategorii a jsou volně dostupné na trhu.

### **4.3 Režimová opatření**

Režimová opatření musí být konkrétně stanovena v dokumentaci poskytovatele certifikačních služeb.

**Režimovými opatřeními jsou:**

1. Režim vstupu a výstupu osob, který stanoví:
  - a) oprávnění osob pro vstup do objektu, výstup z objektu a způsob kontroly;
  - b) podmínky a způsob kontroly vynášení chráněných informací z objektu;
2. Definování bezpečnostních opatření a specifikace chráněných informací a všech chráněných skutečností, které podléhají bezpečnostní manipulaci v zabezpečené oblasti kategorie „D“.  
Rozsah, způsob a podmínky použití bezpečnostních opatření se určují na základě vyhodnocení rizik;
3. Režim pohybu osob a zabezpečení chráněných informací v objektu a v zabezpečených oblastech v pracovní a mimopracovní době;
4. Režim manipulace s klíči, identifikačními prostředky a médii, které se používají pro systémy zabezpečení vstupů (zejména se určuje systém a způsob označování, přidělování a odevzdávání klíčů, jejich úschovy a evidence, uložení duplikátů a způsob jejich použití);
5. Režim manipulace s technickými prostředky a jejich používání.

### **4.4 Zacházení s klíči od úschovných objektů**

Nastavení kombinace u kombinačního zámku úschovného objektu se musí osoby, které je potřebují znát, naučit nazpaměť. Náhradní klíče a písemný zápis každého nastavení kombinace pro případ použití v mimořádných situacích musí být uloženy v zapečetěné neprůhledné obálce u statutárního orgánu PCS nebo jím pověřené osoby. Pracovní a náhradní klíče od úschovných objektů musí být uloženy odděleně. Zápis každé kombinace musí být uložen ve zvláštní obálce. U klíčů, zápisů nastavení kombinací a obálek musí být zajištěna dostatečná ochrana.

Znalost nastavení kombinací u kombinačních zámků úschovných objektů musí být omezena na co nejmenší počet osob. Nastavení kombinací se musí měnit v následujících případech:

- při prvním převzetí úschovného objektu do užívání,
- vždy, když dojde ke změnám v okruhu osob, kterým byla tato kombinace známa,
- vždy, když dojde k neoprávněnému nakládání s chráněnými informacemi, nacházejícími se v úschovném objektu nebo existujícími podezření, že k němu došlo,
- v intervalech nepřekračujících 12 měsíců.

## 4.5 Oprávnění ke vstupu do objektu

Seznam osob (oprávněné osoby) oprávněných vstupovat do stanoveného objektu a seznam dopravních prostředků oprávněných vjíždět do objektu, včetně podmínek organizačního zajištění, se stanoví v provozním řádu k zabezpečení objektové bezpečnosti v souladu s Celkovou bezpečnostní politikou (dále **CBP**) a Certifikační prováděcí směrnicí PCS.

Oprávnění ke vstupu do objektu vydává statutární orgán PCS nebo jím pověřená osoba. Oprávněnost ke vstupu osob do objektu se prokazuje stanoveným způsobem popsaným ve výše uvedených dokumentech, který umožňuje jednoznačnou identifikaci osob.

V objektech kategorie „D“ je návštěvám dovolen pohyb jen v doprovodu oprávněné osoby. V uvedených dokumentech musí být stanovena opatření, která zabrání návštěvám, aby se neoprávněně seznámily s chráněnými informacemi. Za dodržování stanovených opatření odpovídá osoba, která návštěvu doprovází.

Kontrolu oprávněnosti vstupu osob a vjezdu dopravních prostředků do objektu provádí fyzická ostraha nebo osoba pověřená statutárním zástupcem PCS způsobem stanoveným v provozním řádu k zabezpečení objektové bezpečnosti v souladu s Celkovou bezpečnostní politikou a v souladu s Certifikační prováděcí směrnicí PCS.

## 4.6 Vnější ochrana objektu

Vnější ochrana objektu je zajišťována fyzickou ostrahou objektu, technickými prostředky a režimovými opatřeními.

V pracovní době mohou být vyřazena některá bezpečnostní opatření použitá pro ochranu hranice objektu. V mimopracovní době se celá hranice objektu nepřetržitě zabezpečuje bezpečnostními opatřeními stanovenými v souladu s Celkovou bezpečnostní politikou a s Certifikační prováděcí směrnicí PCS. Rozsah, způsob a podmínky použití bezpečnostních opatření se určují na základě vyhodnocení rizik a provedeného vyhodnocení stavu bezpečnostních opatření.

Vstupy do objektu kategorie „D“ se v době, kdy nejsou využívány, zabezpečují kombinací bezpečnostních opatření a technickými prostředky k zabezpečení objektů kategorie „D“.

Tam, kde to umožňuje charakter hranice objektu, jsou po celém jejím obvodu vyžadovány **fyzické bariéry**. Jejich efektivnost závisí na stupni úrovně zabezpečení přístupových bodů. Brány musí být konstruované ve stejném bezpečnostním provedení jako oplocení, musí být zajištěn stejný standard kontroly vstupu ve všech přístupových bodech.

## 4.7 Vnitřní ochrana objektu

Pro efektivní střežení hranice zabezpečené oblasti se doporučuje využívat **perimetrické bezpečnostní systémy**, k nimž se řadí perimetrické detekční systémy, bezpečnostní osvětlení, kamerové systémy. Perimetrické detekční systémy mohou být instalovány skrytě (obvykle z estetických důvodů) nebo zjevně jako odrazující prvek. Perimetrické detekční systémy jsou ze své podstaty náchylné k falešným poplachům, a proto by měly být doplněny o další kontrolní systém, jako jsou například kamerové systémy.

Zabezpečené oblasti, v nichž je zajištěna trvalá přítomnost zde pracujících osob, musí být vybaveny úschovnými objekty pouze v případě, že se v nich hromadně ukládají chráněné informace. Úschovný objekt musí být umístěn tak, aby byl zabezpečen trvalý přímý dohled přítomných osob.

V případě, kdy zabezpečené oblasti současně plní úlohu stanovišť určených pro stálý výkon fyzické ostrahy objektu, nemusí být vybaveny tísňovými systémy.

## 4.8 Vyhodnocení rizik

Základním předpokladem pro efektivní a ekonomické využití bezpečnostních opatření je vyhodnocení rizik, na jehož podkladě se stanovují příslušná opatření pro objektovou bezpečnost. Stanovuje se rozsah, způsob a podmínky použití bezpečnostních opatření.

**Na základě vyhodnocení rizik se provádí:**

- vyhodnocení stavu bezpečnostních opatření a posouzení, zda jejich realizace pro danou míru rizika odpovídá bezpečnostním standardům NBÚ pro zabezpečenou oblast kategorie „D“,
- další vhodná bezpečnostní opatření, pokud bylo při vyhodnocení stavu zjištěno, že stav bezpečnostních opatření je nedostatečný,
- zjištění rizik, která přetrvávají i po aplikaci bezpečnostních opatření.

Existující stav bezpečnostních opatření se hodnotí podle bezpečnostních standardů [5]. Tento standard je předpisem doplňující vyhlášku [2] a vyhlášku č. 244/1998 Sb. ve znění vyhlášky č. 338/1999 Sb.

Na základě hodnocení se přijímá konkrétní způsob řešení ochrany. Zpravidla se stanovuje soubor kombinací nutných bezpečnostních opatření pro nejmenší možnou úroveň zabezpečení chráněných informací, která ještě vyhovuje stanovenému bodovému ohodnocení. Není-li zabezpečení pro danou kategorie „D“ vzhledem k vyhodnocené míře rizika dostatečné, je nutné určit optimální způsob, jak zabezpečení zvýšit na požadovanou úroveň.

K tomuto dokumentu byla Odborem elektronického podpisu zpracována příloha, která zestručňuje „Bezpečnostní standardy [5] NBÚ objektové (fyzické) bezpečnosti“ pro výše uvedený cíl. Jsou v ní popsána především bezpečnostní opatření vztahující se k zabezpečení objektů kategorie „D“ a uvedeny příklady s výpočty bodového ohodnocení bezpečnostních opatření v zabezpečené oblasti.

**Příloha bude na vyžádání zaslána zájemcům elektronickou poštou. Žádosti lze uplatnit na adrese elektronické podatelny ministerstva informatiky: [posta@micr.cz](mailto:posta@micr.cz).**

**„Bezpečnostní standardy NBÚ objektové (fyzické) bezpečnosti“, schválené znění ze dne 21. 3. 2001, lze získat ve formátu RTF na webových stránkách NBÚ:**

**[http://www.nbu.cz/\\_mpokyn\\_index.html](http://www.nbu.cz/_mpokyn_index.html)**

## 5 Použité zkratky

<b>NBÚ</b>	Národní bezpečnostní úřad
<b>EP</b>	elektronický podpis
<b>QC</b>	kvalifikovaný certifikát
<b>PCS</b>	poskytovatel certifikačních služeb
<b>ISCS</b>	informační systém pro certifikační služby
<b>CPS</b>	certifikační prováděcí směrnice
<b>CBP</b>	celková bezpečnostní politika
<b>SBP</b>	systémová bezpečnostní politika
<b>zabezpečená činnost</b>	činnost podle § 4 odst. 1 až 3 a § 5 odst. 1 vyhlášky [1]
<b>zabezpečené prostory</b>	prostory PCS, které musí být zabezpečeny obdobně jako objekty kategorie „D“ podle vyhlášky [2] (objekty a zabezpečené oblasti kategorie „D“)

## 6 Literatura

- [1] Vyhláška č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu.
- [2] Vyhláška č. 339/1999 Sb., o objektové bezpečnosti.
- [3] ČSN ISO/IEC 15408 Informační technologie – Bezpečnostní techniky – kritéria pro hodnocení bezpečnosti informačních technologií, bezpečnostní profil odpovídající úrovni zaručitelnosti bezpečnosti 4.
- [4] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění zákona č. 226/2002 Sb.
- [5] Bezpečnostní standardy NBÚ objektové (fyzické) bezpečnosti, schválené znění ze dne 21. 3. 2001.
- [6] Vyhláška č. 244/1998 Sb., o podrobnostech stanovení a označení stupně utajení a o postupech při tvorbě, evidenci, přenášení, přepravě, zapůjčování, ukládání, jiné manipulaci a skartaci utajovaných písemností, ve znění vyhlášky č. 338/1999 Sb.
- [7] Bosáková, D., Vondruška, P.: Prezentace k vypořádání s připomínkami k návrhu prováděcí vyhlášky k zákonu o elektronickém podpisu, část objektová bezpečnost, 29.7.2001).
- [8] Bosáková, D., Kučerová, A., Peca, J., Vondruška, P.: Elektronický podpis – přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů, Nakladatelství ANAG, 2002.