



# SBÍRKA ZÁKONŮ

## ČESKÁ REPUBLIKA

---

Částka 155

Rozeslána dne 29. prosince 2011

Cena Kč 65,-

---

O B S A H:

453. Vyhláška, kterou se mění vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor
454. Vyhláška, kterou se mění vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.
-

## 453

## VYHLÁŠKA

ze dne 21. prosince 2011,

kteřou se mění vyhláška č. 523/2005 Sb.,

**o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení  
nakládajících s utajovanými informacemi a o certifikaci stínicích komor**

Národní bezpečnostní úřad stanoví podle § 33 písm. e), § 34 odst. 6, § 35 odst. 6, § 36 odst. 4 a § 53 písm. a), b), c), d), g), h), i) a j) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění zákona č. 255/2011 Sb.:

## Čl. I

Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, se mění takto:

1. V § 1 se slova „kopírovacím zařízení, zobrazovacím zařízení a psacím stroji s pamětí“ nahrazují slovy „elektronické podobě v zařízeních, která nejsou součástí informačního nebo komunikačního systému“.

2. V § 1, § 2 písm. x), § 30 odst. 2 a 3, § 31 odst. 1, 2 a 4, § 32, § 38 odst. 1 písm. d), § 38 odst. 2 a v příloze č. 2 se slovo „elektromagnetickým“ zrušuje.

3. V § 2 se na konci písmene x) tečka nahrazuje čárkou a doplňují se písmena y) a z), která znějí:

„y) nepopíratelností schopnost prokázat zpětě jednání či událost tak, aby dané jednání či událost nemohly být následně popřeny,

z) pravostí informací záruka, že informace jsou autentické a z důvěryhodných zdrojů.“

4. V § 3 odst. 1 písm. c) se slovo „elektromagnetického“ zrušuje.

5. V § 5 odst. 1 se za slova „utajované informace“ vkládají slova „ , dostupnost služeb informačního systému“ a poslední věta zní: „Pokud to funkce informačního systému vyžaduje, stanoví se rovněž způsob zaístění pravostí informací a nepopíratelnost.“

6. V § 5 se za odstavec 1 vkládá nový odstavec 2, který zní:

„(2) Zásady bezpečnostní politiky jsou rozpracovány v návrhu bezpečnosti informačního systému

a v provozní bezpečnostní dokumentaci informačního systému.“

Dosavadní odstavec 2 se označuje jako odstavec 3.

7. V § 8 odst. 1 se na konci písmene b) slovo „nebo“ zrušuje a za písmeno b) se vkládá nové písmeno c), které zní:

„c) bezpečnostní provozní mód s nejvyšší úrovní s formálním řízením přístupu k informacím, nebo“.

Dosavadní písmeno c) se označuje jako písmeno d).

8. V § 8 se za odstavec 3 vkládá nový odstavec 4, který zní:

„(4) Bezpečnostní provozní mód s nejvyšší úrovní s formálním řízením přístupu k informacím je takové prostředí, které odpovídá bezpečnostnímu provoznímu módu s nejvyšší úrovní, kde však formální řízení přístupu navíc předpokládá formální centrální správu kontroly přístupu.“

Dosavadní odstavce 4 až 8 se označují jako odstavce 5 až 9.

9. V § 9 odstavec 4 zní:

„(4) Přenos utajované informace komunikačním kanálem vedeným v rámci zabezpečené oblasti nebo objektu může být, na základě analýzy rizik, zabezpečen pouze s využitím opatření fyzické bezpečnosti všech komponentů komunikačního kanálu, přičemž přenášená utajovaná informace není chráněna kryptografickou ochranou nebo je chráněna kryptografickou ochranou na nižší úrovni, nežli je vyžadována pro stupeň utajení přenášené utajované informace. Takto zabezpečený přenos utajované informace Úřad schvaluje v rámci certifikace informačního systému.“

10. V § 9 odstavec 6 zní:

„(6) Přenos utajované informace komunikačním kanálem vedeným mimo objekt musí být zabezpečen certifikovaným kryptografickým prostředkem, který je certifikován nejměně pro stejný stupeň utajení jako přenášená utajovaná informace.“

11. V § 9 se doplňuje odstavec 7, který zní:

„(7) Během certifikace informačního systému může Úřad, na základě předložené analýzy rizik, přijatých specifických bezpečnostních opatření pro detekci narušení bezpečnosti komunikačního kanálu a opatření pro snížení důsledků útoku, schválit odlišný systém zabezpečení informačního systému, než je uveden v odstavcích 4 a 6.“

12. Za § 9 se vkládá nový § 9a, který včetně nadpisu zní:

„§ 9a

**Bezpečné propojení informačních systémů**

(1) Propojením informačních systémů se pro účely této vyhlášky rozumí přímé propojení dvou nebo více informačních systémů nebo informačního systému a informačního systému pro nakládání s neutajovanými informacemi za účelem jednosměrného či vícesměrného sdílení údajů a dalších informačních zdrojů. Propojení informačního systému s jiným informačním systémem nebo s informačním systémem pro nakládání s neutajovanými informacemi lze realizovat pouze v případě nezbytné provozní potřeby.

(2) Certifikovaný informační systém lze propojit s jiným certifikovaným informačním systémem, pokud to bylo na základě analýzy rizik schváleno v rámci certifikace těchto informačních systémů, je mezi nimi realizováno bezpečnostní rozhraní a jsou certifikovány pro nakládání s utajovanými informacemi

- a) stejného stupně utajení, nebo
- b) odlišného stupně utajení, za předpokladu, že se uplatní opatření podle odstavce 3.

(3) Propojení informačních systémů certifikovaných pro nakládání s utajovanou informací odlišného stupně utajení musí být realizováno tak, aby mezi nimi bylo zabráněno přenosu utajované informace vyššího stupně utajení, nežli je stupeň utajení, pro který je informační systém certifikován.

(4) Certifikovaný informační systém nesmí být propojen s veřejnou komunikační sítí, s výjimkou případů, kdy má instalované pro tento účel mezi sebou a veřejnou komunikační sítí vhodné bezpečnostní rozhraní, schválené na základě analýzy rizik v rámci jeho certifikace tak, aby bylo zamezeno průniku do certifikovaného informačního systému a byl umožněn pouze kontrolovaný přenos dat, který nenarušuje důvěrnost, integritu a dostupnost utajované informace a dostupnost služeb certifikovaného informačního systému.

(5) Certifikovaný informační systém, který nakládá s utajovanou informací stupně utajení Přísně tajné, nebo s utajovanou informací vyžadující zvláštní režim nakládání označené „ATOMAL“, nesmí být přímo ani postupně propojen s veřejnou komunikační sítí.

(6) Pokud je veřejná komunikační síť využívána výhradně k přenosu dat mezi informačními systémy nebo lokalitami informačního systému a přenášené informace jsou chráněny certifikovaným kryptografickým prostředkem, nepovažuje se takové spojení za propojení. Mezi informačním systémem a veřejnou komunikační sítí musí být realizováno vhodné bezpečnostní rozhraní tak, aby bylo zamezeno průniku do informačního systému. Připojení je předmětem analýzy rizik a musí být schváleno v rámci certifikace informačního systému.“

13. V § 11 se na konci textu odstavce 5 doplňují slova „a určují se zbytková rizika a jejich úroveň, přičemž se dbá na to, aby byly implementovány pouze funkce, zařízení a služby, které jsou nezbytné pro splnění účelu, pro který je informační systém zřizován“.

14. § 14 včetně nadpisu zní:

„§ 14

**Požadavky ochrany proti kompromitujícímu vyzářování**

(1) Komponenty informačního systému, které nakládají s utajovanými informacemi stupně utajení Důvěrné nebo vyššího a zabezpečená oblast nebo objekt, ve kterém se v informačním systému zpracovávají utajované informace stupně utajení Důvěrné nebo vyššího, musí být zabezpečeny takovým způsobem, aby kompromitující vyzářování nezpůsobilo únik utajované informace.

(2) Požadavky na zabezpečení proti kompromitujícímu vyzářování jsou závislé na stupni utajení utajované informace, se kterou informační systém nakládá, a jsou stanoveny v bezpečnostním standardu.

(3) Instalace informačního systému, který nakládá s utajovanou informací stupně utajení Důvěrné nebo vyššího, z hlediska jeho zabezpečení proti kompromitujícímu vyzářování musí být provedena v souladu s požadavky bezpečnostního standardu. Záznam o instalaci komponent informačního systému se vkládá do bezpečnostní dokumentace informačního systému. Obsah a forma záznamu jsou stanoveny v bezpečnostním standardu.“

15. V § 15 odst. 4 se slovo „života“ nahrazuje slovy „životního cyklu“.

16. V § 15 odstavce 5 a 6 znějí:

„(5) Stupeň utajení nosiče utajovaných informací stupně utajení Tajné může být snížen, stupně utajení Důvěrné může být snížen nebo zrušen, pouze v případě, že vymazání utajovaných informací z něj bylo provedeno způsobem uvedeným v odstavci 6 nebo je prokázáno, že na něm byly během jeho dosavadního životního cyklu uloženy pouze utajované informace nižšího stupně utajení nebo informace neutajované nebo je prokázáno, že stupeň utajení utajovaných informací uložených na něm během jeho dosavadního životního cyklu byl zrušen nebo snížen. Stupeň utajení nosiče utajovaných informací stupně utajení Vyhrazené může být zrušen pouze v případě, že vymazání utajovaných informací z něj bylo provedeno způsobem uvedeným v odstavci 6 nebo je prokázáno, že na něm byly během jeho dosavadního životního cyklu uloženy pouze informace neutajované nebo je prokázáno, že stupeň utajení utajovaných informací uložených na něm během jeho dosavadního životního cyklu byl zrušen.

(6) Vymazání utajované informace z nosiče utajovaných informací, které umožňuje snížení nebo zrušení jeho stupně utajení, musí být provedeno tak, aby utajovaná informace uložená na nosiči během jeho dosavadního životního cyklu byla obtížně zjistitelná i při použití laboratorních metod. Podmínky a postupy bezpečného vymazání stanoví Úřad v bezpečnostním standardu, postup musí být uveden v provozní bezpečnostní dokumentaci certifikovaného informačního systému a schválen v rámci jeho certifikace.“

17. V § 15 se doplňuje odstavec 8, který zní:

„(8) Při používání velkokapacitních vyměnitelných nosičů informací musí být v bezpečnostní politice stanoveno řízení přístupu uživatele ke vstupním a výstupním zařízením.“

18. V § 16 odst. 2 se slova „být držitelem osvědčení fyzické osoby“ nahrazují slovy „splňovat podmínky pro přístup fyzické osoby k utajované informaci“.

19. V § 16 se za odstavec 2 vkládají nové odstavce 3 až 5, které znějí:

„(3) Správce informačního systému, který vykonává funkci administrátora s právy úplného řízení systému, a bezpečnostní správce celého informačního systému, musí splňovat podmínky pro přístup fyzické osoby k utajované informaci stupně utajení o jeden stu-

peň vyššího, nežli je nejvyšší stupeň utajení utajovaných informací, se kterými může informační systém nakládat. To neplatí u informačního systému, který je určen pro zpracování utajované informace stupně utajení Přísně tajné. U správce informačního systému, který vykonává funkci administrátora s právy úplného řízení systému, a u bezpečnostního správce celého informačního systému malého rozsahu nebo s nízkým podílem zpracování utajovaných informací nejvyššího stupně utajení, pro jejichž zpracování je informační systém určen, nebo v nichž nedochází ke kumulaci utajovaných informací nebo v nichž se zpracovává pouze taktická utajovaná informace, může Úřad, se zvážením identifikovaných rizik, uznat jako dostačující splnění podmínek pro přístup fyzické osoby k utajované informaci na úrovni shodné s nejvyšším stupněm utajení utajovaných informací, se kterými může informační systém nakládat.

(4) Správce informačního systému, který vykonává funkci administrátora s omezenými právy řízení systému, zejména správu serverů, správu aplikace nebo lokální správu a bezpečnostní správce informačního systému zajišťující dílčí oblast bezpečnosti, zejména určitou bezpečnostní technologii nebo lokální správu, musí splňovat podmínky pro přístup fyzické osoby k utajované informaci stupně utajení shodného s nejvyšším stupněm utajení utajovaných informací, se kterými může informační systém nakládat.

(5) V případě, že odpovědná osoba nebo jí pověřená osoba schválí informační systém do provozu pro nakládání s utajovanou informací do stupně utajení nižšího, nežli je stupeň utajení utajovaných informací, se kterými může informační systém nakládat, je pro stanovení nutné úrovně podmínek pro přístup fyzické osoby k utajované informaci, určující stupeň utajení utajovaných informací, pro který je informační systém schválen do provozu.“

Dosavadní odstavce 3 a 4 se označují jako odstavce 6 a 7.

20. V § 17 se doplňuje odstavec 3, který včetně poznámky pod čarou č. 6 zní:

„(3) Vyžaduje-li to činnost, pro kterou je informační systém zřízen, je v informačním systému zajišťována nepopíratelnost stanovených jednání či událostí. V případě, že je v informačním systému požadována funkcionalita spisové služby v elektronické podobě<sup>6)</sup>, musí být software, kterým je realizována, hodnocen během certifikace informačního systému.

6) Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů.“.

21. V § 20 se doplňují odstavce 5 a 6, které znějí:

„(5) Minimální míra zabezpečení zabezpečené oblasti pro umístění části informačního systému, v níž mohou být ukládány utajované informace, se určuje v souladu s tabulkami bodových hodnot nejnižší míry zabezpečení fyzické bezpečnosti uvedenými v příloze č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

(6) Bodové ohodnocení fyzické bezpečnosti informačního systému je uvedeno v příloze č. 3 k této vyhlášce.“.

22. V § 23 se za odstavec 2 vkládá nový odstavec 3, který zní:

„(3) V provozovaném informačním systému je ověřována pravost informací, které vstupují do informačního systému.“.

Dosavadní odstavce 3 až 10 se označují jako odstavce 4 až 11.

23. V § 23 se za odstavec 8 vkládá nový odstavec 9, který zní:

„(9) V zabezpečené oblasti, v níž jsou umístěny komponenty informačního systému pro nakládání s utajovanou informací stupně utajení Tajné nebo Přísně tajné, se na žádost orgánu státu nebo podnikatele provádí kontrola ke zjištění nedovoleného použití technických prostředků určených k získávání informací. Tato kontrola se provede před prvním zpracováním utajované informace a dále opakovaně zpravidla v intervalu dvou let.“.

Dosavadní odstavce 9 až 11 se označují jako odstavce 10 až 12.

24. V § 24 odst. 1 písm. a) bodech 1 a 2 se za slova „identifikační číslo“ vkládají slova „, bylo-li přiděleno“.

25. V § 24 odst. 1 písm. a) bodě 2 se slova „trvalým pobytem“ nahrazují slovy „místem trvalého pobytu nebo u cizince místem obdobného pobytu“.

26. V § 24 odst. 1 se na konci textu písmene f) doplňují slova „nebo kopii platného prohlášení podnikatele“.

27. V § 27 se vkládá nový odstavec 1, který zní:

„(1) Projekt bezpečnosti komunikačního systému obsahuje tyto náležitosti

- a) bezpečnostní politiku komunikačního systému,
- b) organizační a provozní postupy provozování komunikačního systému,
- c) provozní směrnice pro bezpečnostní správu komunikačního systému a
- d) provozní směrnice uživatele komunikačního systému.“.

Dosavadní odstavce 1 až 4 se označují jako odstavce 2 až 5.

28. V § 28 odst. 2 písm. c), § 33 odst. 1 písm. c), § 37 písm. b) se slova „pro seznamování se s utajovanými informacemi“ nahrazují slovy „nebo kopii platného prohlášení podnikatele“.

29. V § 28 odst. 2 se na konci textu písmene f) doplňují slova „nebo kopii platného prohlášení podnikatele“.

30. V § 28 odst. 3 se slova „27 odst. 2“ nahrazují slovy „27 odst. 3“.

31. V § 29 odst. 1 se slova „27 odst. 2“ nahrazují slovy „27 odst. 3“, slova „27 odst. 3“ se nahrazují slovy „27 odst. 4“ a slova „27 odst. 4“ se nahrazují slovy „27 odst. 5“.

32. V nadpisu části čtvrté se slovo „ELEKTROMAGNETICKÉ“ zrušuje.

33. V části čtvrté se na začátek hlavy I vkládá nový § 29a, který zní:

#### „§ 29a

Kompromitující vyzařování je vyzařování elektrických a elektronických zařízení, které by mohlo způsobit únik utajované informace stupně utajení Přísně tajné, Tajné nebo Důvěrné.“.

34. V § 30 odst. 1 úvodní části ustanovení se za slovo „objektu“ vkládají slova „k ochraně před únikem informací kompromitujícím vyzařováním“.

35. V § 32 se vkládá nový odstavec 1, který zní:

„(1) Stínicí komorou je uzavřený stíněný prostor zabraňující šíření elektromagnetického, optického a akustického vyzařování mimo tento prostor.“.

Dosavadní text se označuje jako odstavec 2.

36. V § 38 odst. 1 se slova „provozování kopírovacího zařízení, zobrazovacího zařízení nebo psacího stroje s pamětí, které nejsou součástí informačního nebo komunikačního systému“ nahrazují slovy „zpracování utajovaných informací v elektronické podobě

v zařízení, které není součástí informačního nebo komunikačního systému, zejména v psacím stroji s pamětí a v zařízení umožňujícím kopírování, záznam nebo zobrazení utajované informace anebo její převod do jiného datového formátu“.

37. V § 38 odst. 2 se slova „Kopírovací zařízení, zobrazovací zařízení a psací stroj s pamětí, které se používají pro zpracování utajovaných informací stupně utajení Důvěrné nebo vyššího, musí být zabezpečeny“ nahrazují slovy „Zařízení podle odstavce 1, která se používají pro zpracování utajovaných informací stupně utajení Důvěrné nebo vyššího, musí být zabezpečena“.

38. V § 38 odst. 3 se slova „Kopírovací zařízení, zobrazovací zařízení a psací stroj s pamětí musí být umístěny“ nahrazují slovy „Zařízení podle odstavce 1 musí být umístěna“.

39. V § 38 odst. 4 se slova „Kopírovací zařízení, zobrazovací zařízení a psací stroje s pamětí musí být

fyzicky chráněny“ nahrazují slovy „Zařízení podle odstavce 1 musí být fyzicky chráněna“.

40. V § 38 odst. 5 se slova „kopírovacího zařízení, zobrazovacího zařízení a psacího stroje s pamětí“ nahrazují slovy „zařízení podle odstavce 1“.

41. V § 38 odst. 6 se slova „S kopírovacím zařízením a zobrazovacím zařízením“ nahrazují slovy „Se zařízením podle odstavce 1“ a slova „ , komponentách a pamětech“ se nahrazují slovy „a komponentách“.

42. V § 38 odst. 7 se slova „kopírovací zařízení, zobrazovací zařízení a psací stroje s pamětí“ nahrazují slovy „zařízení podle odstavce 1“, slovo „pamětí“ se nahrazuje slovy „komponent“ a na konci textu se doplňují slova „podle § 15, jinak nesmí být předmětem servisní činnosti“.

43. Doplňuje se příloha č. 3, která včetně nadpisu zní:

„Příloha č. 3 k vyhlášce č. 523/2005 Sb.

## FYZICKÁ BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ (IS)

### 1.1. ZPRACOVÁVÁNÍ DAT

**1.1.1. Danou částí informačního systému mohou být utajované informace pouze zobrazeny a zpracovávány nebo přenášeny:**

**SS1 = 4 body**

V případě, že je v zabezpečené oblasti umístěna jedna nebo více částí informačního systému, použije se nejnižší z hodnot parametru SS1 vztažených k jednotlivým částem informačního systému.

### 1.2. UKLÁDÁNÍ UTAJOVANÝCH INFORMACÍ NA POČÍTAČOVÝCH MÉDIÍCH (VEŠKERÁ NEVOLATILNÍ PAMĚŤOVÁ MÉDIA)

Prostory, v nichž jsou informační systémy používány pro ukládání utajovaných informací stupně utajení Vyhrazené a vyšší, musí být zřízeny jako zabezpečené oblasti.

**1.2.1. Uložená data jsou šifrována certifikovaným kryptografickým prostředkem**

**SS1 = 4 body**

Kromě parametru SS1, který se vztahuje na uložená zašifrovaná data, je nutné také pracovat s parametrem S1 kryptografického prostředku.

**1.2.2. Uložená data nejsou šifrována**

**SS1 = 1 bod**

**1.3.1. Identifikace jménem a autentizace předmětem s šifrovaným obsahem a přenosem:****SS2 = 4 body**

Kryptografické mechanismy předmětu používaného pro autentizaci musí být certifikované Úřadem.

Tento způsob autentizace tvoří bezpečnostní ekvivalent zámku úschovného objektu typu 4.

**1.3.2. Identifikace jménem a autentizace předmětem s šifrovaným obsahem:****SS2 = 3 body**

Kryptografické mechanismy předmětu používaného pro autentizaci musí být certifikované Úřadem.

Tento způsob autentizace tvoří bezpečnostní ekvivalent zámku úschovného objektu typu 3.

**1.3.3. Identifikace jménem a autentizace předmětem****SS2 = 2 body**

Předmět používaný pro autentizaci musí být schválen Úřadem v rámci certifikace informačního systému.

Tento způsob autentizace tvoří bezpečnostní ekvivalent zámku úschovného objektu typu 2.

**1.3.4. Identifikace jménem a autentizace heslem****SS2 = 1 bod**

Minimální délka a způsob vytváření hesla musí být schválen Úřadem v rámci certifikace informačního systému.

Tento způsob autentizace tvoří bezpečnostní ekvivalent zámku úschovného objektu typu 1.

Z bodových hodnot SS1 a SS2 získaných podle bodu 1.1. nebo 1.2. a bodu 1.3. této přílohy se vypočítá hodnota S1:

$$(S1) = SS1 \times SS2$$

Hodnotu SS1 a SS2 lze použít do tabulky bodových hodnot nejnižší míry zabezpečení zabezpečené oblasti nebo jednací oblasti.“.

Čl. II  
Účinnost

Tato vyhláška nabývá účinnosti dnem 1. ledna 2012.

Ředitel:

Ing. Navrátil v. r.

## 454

## VYHLÁŠKA

ze dne 21. prosince 2011,

kteřou se mění vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků,  
ve znění vyhlášky č. 19/2008 Sb.

Národní bezpečnostní úřad stanoví podle § 33 a § 53 písm. a), c), d), e), f) a j) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění zákona č. 255/2011 Sb.:

## Čl. I

Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb., se mění takto:

1. V § 2 písm. a) se za slova „ve kterém se“ vkládá slovo „zpravidla“.

2. V § 2 se písmeno f) včetně poznámky pod čarou č. 4 zrušuje.

Dosavadní písmena g) až m) se označují jako písmena f) až l).

3. V § 2 písm. i) se slova „ztěžuje nebo“ nahrazují slovem „ztěžuje“, za slovo „oznamuje“ se vkládají slova „nebo zaznamenává“ a za slovo „narušení“ se vkládá slovo „zabezpečení“.

4. V § 2 písm. j) se slova „ , uzamykatelná skříň“ zrušují a za slovo „jiná“ se vkládá slovo „uzamykatelná“.

5. V § 2 se na konci písmene k) čárka nahrazuje tečkou a písmeno l) se zrušuje.

6. § 3 včetně nadpisu a poznámky pod čarou č. 6 zní:

## „§ 3

**Zabezpečení objektu a zabezpečené oblasti**

(1) Hranici objektu nebo zabezpečené oblasti, zařazení objektu nebo zabezpečené oblasti do příslušné kategorie<sup>6)</sup> a zařazení zabezpečené oblasti do příslušné třídy stanoví odpovědná osoba nebo jí pověřená osoba.

(2) Zabezpečení objektu nebo zabezpečené oblasti je zajišťováno kombinací opatření fyzické bezpečnosti podle odstavců 3 až 10 a § 6 až 9.

(3) Objekt je zabezpečován v závislosti na katego-

rii objektu, s ohledem na charakter hranice objektu a v závislosti na vyhodnocení rizik těmito technickými prostředky

- a) pro kategorii Vyhrazené – mechanické zábranné prostředky,
- b) pro kategorii Důvěrné a Tajné – mechanické zábranné prostředky a zařízení elektrické zabezpečovací signalizace,
- c) pro kategorii Přísně tajné – mechanické zábranné prostředky, zařízení elektrické zabezpečovací signalizace a speciální televizní systémy. Speciální televizní systémy nesmí narušit ochranu utajovaných informací.

(4) Zabezpečená oblast je zabezpečována v závislosti na její kategorii, třídě a vyhodnocení rizik těmito technickými prostředky

- a) pro kategorii Vyhrazené – mechanické zábranné prostředky,
- b) pro kategorii Důvěrné – mechanické zábranné prostředky a zařízení elektrické zabezpečovací signalizace,
- c) pro kategorii Tajné a Přísně tajné – mechanické zábranné prostředky, systémy pro kontrolu vstupů, zařízení elektrické zabezpečovací signalizace, speciální televizní systémy, zařízení elektrické požární signalizace. Speciální televizní systémy lze nahradit tíšňovými systémy. Při použití speciálních televizních systémů nesmí být narušena ochrana utajovaných informací.

(5) Bodové hodnoty nejnižší míry zabezpečení zabezpečené oblasti jsou stanoveny v příloze č. 1 této vyhlášky.

(6) Objekty a zabezpečené oblasti kategorie Důvěrné a vyšší, v nichž je zajištěna trvalá přítomnost zde pracujících osob, se zabezpečují mechanickými zábrannými prostředky.

(7) K zabezpečení zabezpečených oblastí se používají certifikované nebo necertifikované technické prostředky. Necertifikované technické prostředky lze pou-



žit pouze za podmínek stanovených v příloze č. 1 této vyhlášky.

(8) Utajovaná informace se ukládá v zabezpečené oblasti příslušné kategorie nebo vyšší, popřípadě v úschovném objektu, je-li jeho bodová hodnota uplatněna v projektu fyzické bezpečnosti pro příslušnou zabezpečenou oblast.

(9) V objektu se umísťuje zařízení fyzického ničení nosičů informací podle přílohy č. 1 této vyhlášky.

(10) V případě, že hranice objektu je totožná s hranicí zabezpečené oblasti, je rozsah použití opatření fyzické bezpečnosti určen požadavky na kategorii zabezpečené oblasti.

<sup>6)</sup> § 25 odst. 1 zákona č. 412/2005 Sb., ve znění zákona č. 255/2011 Sb.“.

7. V § 4 odst. 1 se slova „a hranici objektu“ zrušují.

8. V 4 odst. 1 a v § 8 odst. 3 se slova „provozovatel objektu“ nahrazují slovy „odpovědná osoba nebo jí pověřená osoba“.

9. V § 4 odst. 2 se slova „a hranice objektu“ zrušují.

10. V § 4 odst. 2 se číslo „11“ nahrazuje číslem „8“ a číslo „10“ se nahrazuje číslem „9“.

11. V § 4 odst. 3 se slova „podle § 10 odst. 3“ zrušují.

12. V § 4 se na konci odstavce 5 doplňuje věta „Speciální televizní systémy nesmí narušit ochranu utajovaných informací.“.

13. V § 4 odst. 7 se za slova „přílohy č. 1“ vkládají slova „této vyhlášky“.

14. V § 4 odstavec 8 zní:

„(8) K zabezpečení jednacích oblastí se používají certifikované nebo necertifikované technické prostředky. Necertifikované technické prostředky lze použít pouze za podmínek stanovených v příloze č. 1 této vyhlášky.“.

15. V § 4 se odstavce 9 a 10 zrušují.

Dosavadní odstavec 11 se označuje jako odstavec 9.

16. § 5 včetně nadpisu zní:

„§ 5

### Zabezpečení technického zařízení

(1) Technické zařízení je zabezpečováno opatře-

nými fyzické bezpečnosti podle § 3, 6 až 10 nebo podle odstavců 2 až 4.

(2) Rozsah použití režimových opatření a technických prostředků k zabezpečení technického zařízení stanoví odpovědná osoba nebo jí pověřená osoba v závislosti na vyhodnocení rizik.

(3) Ostraha uloženého technického zařízení obsahujícího utajovanou informaci stupně utajení

a) Přísně tajné se zajišťuje typem 5 podle přílohy č. 1 této vyhlášky,

b) Tajné se zajišťuje minimálně typem 4 podle přílohy č. 1 této vyhlášky,

c) Důvěrné se zajišťuje minimálně typem 3 podle přílohy č. 1 této vyhlášky,

d) Vyhrazené se zajišťuje v rozsahu stanoveném odpovědnou osobou nebo jí pověřenou osobou.

(4) Rozsah použití opatření fyzické bezpečnosti k zabezpečení technického zařízení se stanoví v projektu fyzické bezpečnosti. Obsah a forma projektu fyzické bezpečnosti se použije přiměřeně.“.

17. V § 6 odst. 1 písm. d) se slovo „daty“ nahrazuje slovy „prostředky, zejména způsob jejich označování, přidělování, úschovy a evidence“.

18. V § 6 se na konci odstavce 1 tečka nahrazuje čárkou a doplňuje se písmeno f), které zní:

„f) režim pohybu utajovaných informací v objektu, zabezpečené oblasti a jednacích oblastí.“.

19. § 7 včetně nadpisu zní:

„§ 7

### Režim pohybu osob a dopravních prostředků

(1) Oprávnění ke vstupu do objektu, zabezpečené oblasti nebo jednacích oblastí vydává odpovědná osoba nebo jí pověřená osoba. Oprávnění ke vstupu do zabezpečené oblasti nebo jednacích oblastí stanovené kategorie lze vydat osobě, která je poučena a je držitelem oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené nebo osvědčení fyzické osoby pro odpovídající nebo vyšší stupeň utajení. Seznam osob s oprávněním ke vstupu do objektu kategorie Důvěrné, Tajné nebo Přísně tajné, do zabezpečené oblasti a do jednacích oblastí a dopravních prostředků oprávněných vjíždět do objektu kategorie Důvěrné, Tajné nebo Přísně tajné, do zabezpečené oblasti a do jednacích oblastí se ukládá u odpovědné osoby nebo jí pověřené osoby.

(2) Osoby bez oprávnění ke vstupu mohou do

objektu kategorie Důvěrné, Tajné nebo Přísně tajné, zabezpečené oblasti nebo jednacích oblastí vstupovat pouze za doprovodu osoby oprávněné ke vstupu do příslušného objektu, zabezpečené oblasti nebo jednacích oblastí za předpokladu, že vstup je nezbytný a nebude narušena ochrana utajovaných informací.

(3) Na vstupu do objektu kategorie Důvěrné, Tajné nebo Přísně tajné se provádí kontrola vstupu a u osob bez oprávnění ke vstupu do objektu je vedena evidence údajů a povinně se stanoví režim návštěv s doprovodem. Na vstupu do zabezpečené oblasti kategorie Vyhrazené, která je umístěna v objektu kategorie Vyhrazené, se provádí kontrola vstupu.

(4) Při vstupu osob bez oprávnění ke vstupu do objektu kategorie Přísně tajné se u nich provádí kontrola zařízením sloužícím k vyhledávání nebezpečných látek nebo předmětů.“.

20. V nadpisu § 8 se slovo „daty“ nahrazuje slovem „prostředky“.

21. V § 8 odst. 1, 3 a 4 se slovo „daty“ nahrazuje slovem „prostředky“.

22. V § 8 odst. 2 se slovo „data“ nahrazuje slovem „prostředky“ a slova „stupně utajení Vyhrazené, která vyžaduje zvláštní režim nakládání a utajovaná informace“ se zrušují.

23. V § 8 odst. 2 a 4 a v § 10 odst. 1 a 4 se slova

„provozovatel objektu“ nahrazují slovy „odpovědná osoba“.

24. V § 8 odst. 2, 4 a 5 a v § 10 odst. 1 a 4 se slovo „jím“ nahrazuje slovem „jí“.

25. V § 8 odst. 4 se slovo „utajeným“ nahrazuje slovem „utajovaným“, za slova „úschovných objektů“ se vkládá slovo „ , je“, slova „klíče a identifikační data“ se zrušují a slova „ , kde se zabezpečené nebo jednacích oblasti nacházejí“ se zrušují.

26. V § 8 odst. 5 se slovo „dat“ nahrazuje slovem „prostředků“ a slova „provozovateli objektu“ se nahrazují slovy „odpovědné osobě“.

27. V § 9 se za slovo „hodnoty“ vkládají slova „jednotlivých typů“.

28. V § 11 odst. 2 písm. c) se slova „nebo prohlášení o stejném složení a provedení technického prostředku, které obsahuje prohlášení výrobce, že technický prostředek bude vyráběn ve stejném složení a provedení, jak byl specifikován v posudku podle § 46 odst. 14 zákona“ nahrazují slovy „– pro jednotlivý technický prostředek není požadován“.

29. V § 12 se slovo „Doba“ nahrazuje slovem „Dobu“ a slova „je odvozena od doby“ se nahrazují slovy „stanoví Úřad, a to nejvýše na dobu“.

30. Příloha č. 1 zní:

## **1. ÚSCHOVNÉ OBJEKTY A JEJICH ZÁMKY**

### **1.1. ÚSCHOVNÉ OBJEKTY**

#### **1.1.1. Úschovný objekt typ 4:**

**SS1 = 4 body**

Úschovný objekt typu 4 je certifikovaný Národním bezpečnostním úřadem (dále jen „Úřad“) a splňuje požadavky bezpečnostní třídy II nebo vyšší podle ČSN EN 1143-1+A1 Bezpečnostní úschovné objekty – Požadavky, klasifikace a metody zkoušení odolnosti proti vloupání – Část 1: Skříňové trezory, trezorové dveře a komorové trezory.

V souladu s ČSN EN 1143-1+A1 musí být úschovný objekt typu 4 osazen zámkem minimálně třídy A podle ČSN EN 1300+A1 Bezpečnostní úschovné objekty – Klasifikace zámků s vysokou bezpečností vzhledem k jejich odolnosti proti nepovolenému otevření (zámek typu 2, bod 1.2.3. přílohy).

V případě, že je v úschovném objektu typu 4 uložen kryptografický materiál, musí být tento úschovný objekt vybaven kombinačním mechanickým zámkem, minimálně třípolohovým.

#### **1.1.2. Úschovný objekt typ 3:**

**SS1 = 3 body**

Úschovný objekt typu 3 je certifikovaný Úřadem a splňuje požadavky bezpečnostní třídy I podle ČSN EN 1143-1+A1.

V souladu s ČSN EN 1143-1+A1 musí být úschovný objekt typu 3 osazen zámkem minimálně třídy A podle ČSN EN 1300+A1 (zámek typu 2, bod 1.2.3. přílohy).

V případě, že je v úschovném objektu typu 3 uložen kryptografický materiál, musí být tento úschovný objekt vybaven kombinačním mechanickým zámkem, minimálně třípolohovým.

#### **1.1.3. Úschovný objekt typ 2:**

**SS1 = 2 body**

Úschovný objekt typu 2 je certifikovaný Úřadem a splňuje požadavky bezpečnostní třídy 0 podle ČSN EN 1143-1+A1.

V souladu s ČSN EN 1143-1+A1 musí být úschovný objekt typu 2 osazen zámkem minimálně třídy A podle ČSN EN 1300+A1 (zámek typu 2, bod 1.2.3. přílohy).

#### **1.1.4. Úschovný objekt typ 1:**

**S1 = 1 bod**

Úschovným objektem typu 1 je nerozebíratelná ocelová skříň pevné konstrukce, její dveřní uzávěr je opatřen třístranným rozvorovým mechanismem a uzamykán. Dveřní uzávěr je samosvorný v uzavřeném stavu.

Úschovný objekt typu 1 není certifikovaný Úřadem. Shodu vlastností těchto úschovných objektů s výše uvedenými požadavky posuzuje odpovědná osoba nebo jí pověřená osoba. Zápis o posouzení shody se stává součástí projektu fyzické bezpečnosti.

**1.1.5. Úschovný objekt typ 1A:****S1 = 1 bod**

Úschovný objekt typu 1A je certifikovaný Úřadem a splňuje, včetně uzamykacího systému, požadavky bezpečnostní třídy Z1 podle ČSN 91 6012 Bezpečnostní úschovné objekty – Požadavky, klasifikace a metody zkoušení odolnosti proti vloupání – Trezory se základní bezpečností.

**1.1.6. Úschovný objekt typ 1B:****S1 = 2 body**

Úschovný objekt typu 1B je certifikovaný Úřadem a splňuje, včetně uzamykacího systému, požadavky bezpečnostní třídy Z2 podle ČSN 91 6012.

**1.1.7. Úschovný objekt typ 1C:****S1 = 3 body**

Úschovný objekt typu 1C je certifikovaný Úřadem a splňuje, včetně uzamykacího systému, požadavky bezpečnostní třídy Z3 podle ČSN 91 6012.

**1.1.8. Úschovný objekt typ 0:****S1 =nehodnoceno (N)**

Úschovný objekt typu 0 je pevné konstrukce (např. schránka, kancelářský nábytek) a je opatřen zámek, který je uzamykán. Nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup. Úschovný objekt typu 0 není certifikovaný Úřadem.

Shodu vlastností těchto úschovných objektů s výše uvedenými požadavky odpovědná osoba nebo jí pověřená osoba v projektu fyzické bezpečnosti.

**1.2. ZÁMKY ÚSCHOVNÝCH OBJEKTŮ****1.2.1. Zámek typ 4:****SS2 = 4 body**

Zámek typu 4 je certifikovaný Úřadem v rámci certifikace úschovného objektu a splňuje požadavky bezpečnostní třídy C podle ČSN EN 1300+A1.

**1.2.2. Zámek typ 3:****SS2 = 3 body**

Zámek typu 3 je certifikovaný Úřadem v rámci certifikace úschovného objektu a splňuje požadavky bezpečnostní třídy B podle ČSN EN 1300+A1.

**1.2.3. Zámek typ 2:****SS2 = 2 body**

Zámek typu 2 je certifikovaný Úřadem v rámci certifikace úschovného objektu a splňuje požadavky bezpečnostní třídy A podle ČSN EN 1300+A1.

Poznámka k bodu 1.:

Převodní tabulka bodové hodnocení úschovného objektu

Typ úschovného objektu	Stupeň utajení pro který byla schválena způsobilost je vypsán slovy	Bodová hodnota SS1	Bodová hodnota SS2
	do 31.12. 1999		
Typ 4	PŘÍSNĚ TAJNÉ	4 body	2 body
Typ 3	TAJNÉ	3 body	2 body
Typ 2	DŮVĚRNÉ	2 body	2 body

## 2. ZABEZPEČENÉ OBLASTI A JEJICH UZAMYKACÍ SYSTÉMY

Mechanickými zábrannými prostředky se v této kapitole rozumí zejména zámky, dveře, mříže, folie, skla a další bezpečnostní konstrukční a stavební prvky s výjimkou úschovných objektů (bod 1. přílohy).

Mechanickými zábrannými prostředky se zabezpečují průlezná otvory, které dovolí průchod šablony o níže uvedených rozměrech:

Průlezný otvor	Rozměr
obdélník	400mm x 250mm
elipsa	400mm x 300mm
kruh	Průměr 350 mm

Pokud je průlezný otvor zabezpečen mechanickým zábranným prostředkem s jedním nebo více otvory (např. mříž), nesmí tyto otvory dovolit průchod šablony ve tvaru elipsy o rozměrech 250 mm x 150 mm a tloušťky 20 mm.

### 2.1. ZABEZPEČENÉ OBLASTI

Určení typu zabezpečené oblasti je dáno nejméně odolným prvkem její hranice.

#### 2.1.1. Zabezpečená oblast typ 4:

**SS3 = 4 body**

Stěny, podlahy a stropy musí mít následující stavební konstrukci:

- a) zděnou (cihelné nebo vápenocementové bloky, pórobetonové tvárnice) tloušťky větší než 300 mm, nebo
- b) z vyztuženého betonu tloušťky větší než 150 mm.

Bodové hodnocení ostatních mechanických zábranných prostředků musí splňovat hodnotu SS3 = 4. Mechanické zábranné prostředky nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup.

Okna, dveře a další uzávěry musí splňovat požadavky bezpečnostní třídy RC 4 nebo třídy RC 5 podle ČSN EN 1627 Okna, dveře, uzávěry - Odolnost proti násilnému vniknutí - Požadavky a klasifikace.

**2.1.2. Zabezpečená oblast typ 3:****SS3 = 3 body**

Stěny, podlahy a stropy musí mít následující stavební konstrukci:

- a) zděnou (cihelne nebo vápenocementové bloky, pórobetonové tvárnice) tloušťky větší než 150 mm, nebo
- b) z vyztuženého betonu tloušťky větší než 100 mm.

Bodové hodnocení ostatních mechanických zábranných prostředků musí splňovat minimálně hodnotu SS3 = 3. Mechanické zábranné prostředky nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup.

Okna, dveře a uzávěry musí splňovat požadavky bezpečnostní třídy RC 3 podle ČSN EN 1627.

**2.1.3. Zabezpečená oblast typ 2:****SS3 = 2 body**

Stěny, podlahy a stropy musí mít následující stavební konstrukci:

- a) zděnou (cihelne nebo vápenocementové bloky, pórobetonové tvárnice) tloušťky 100 až 150 mm, nebo
- b) z vyztuženého betonu tloušťky do 100 mm.

Podlahy a stropy mohou být i z jiného materiálu tloušťky větší než 150 mm (např. dřevěná sendvičová trámová konstrukce).

Bodové hodnocení ostatních mechanických zábranných prostředků musí splňovat minimálně hodnotu SS3 = 2.

Okna, dveře a uzávěry musí splňovat požadavky bezpečnostní třídy RC 2 podle ČSN EN 1627.

Průlezné otvory nemusí být zabezpečeny certifikovanými mechanickými zábrannými prostředky, pokud spodní okraj průlezného otvoru splňuje následující požadavky:

- a) nachází se alespoň 5,5 m nad terénem,
- b) nelze k němu jednoduše proniknout ze střechy nebo za pomoci hromosvodů, okapů, parapetů, jiných stavebních prvků, terénních nerovností, stromů či jiných staveb.

Mechanické zábranné prostředky nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup.

**2.1.4. Zabezpečená oblast typ 1:****SS3 = 1 bod**

Stěny, podlahy a stropy jsou lehké stavební konstrukce z materiálů jako například:

- sádkartónu,
- lehké zděné stavební konstrukce,
- dřeva, dřevotřískových desek,
- plastických tvrzených hmot,
- profilovaného nebo vlnitého plechu,
- skla.

Průlezné otvory musí být zabezpečeny mechanickými zábrannými prostředky, které poskytují stejný stupeň odolnosti jako zbývající části hranice zabezpečené oblasti typu 1, nebo jsou chráněny certifikovanými zařízeními elektrické zabezpečovací signalizace (EZS), jejichž instalace odpovídá minimálně hodnotě SS92 = 3.

Průlezné otvory nemusí být zabezpečeny těmito mechanickými zábrannými prostředky, pokud spodní okraj průlezného otvoru splňuje následující požadavky:

- a) nachází se alespoň 5,5 m nad terénem,
- b) nelze k němu jednoduše proniknout ze střechy nebo za pomoci hromosvodů, okapů, parapetů, jiných stavebních prvků, terénních nerovností, stromů či jiných staveb.

Mechanické zábranné prostředky musí být pevné konstrukce a nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup a shodu s těmito požadavky posuzuje odpovědná osoba nebo jí pověřená osoba.

Zápis o posouzení shody se stává součástí projektu fyzické bezpečnosti.

#### **2.1.5. Zabezpečená oblast typ 0:**

**SS3 = nehodnoceno (N)**

Zabezpečení průlezných otvorů musí umožňovat kontrolu pohybu osob a vozidel.

Mechanické zábranné prostředky nesmí vykazovat takové znaky poškození nebo opotřebení, které by znemožnily identifikovat pokusy o neoprávněný vstup.

Shodu s výše uvedenými požadavky potvrzuje odpovědná osoba nebo jí pověřená osoba v projektu fyzické bezpečnosti.

## **2.2. UZAMYKACÍ SYSTÉMY URČENÉ K UZAMYKÁNÍ ZABEZPEČENÝCH OBLASTÍ**

#### **2.2.1. Uzamykací systém typ 4:**

**SS4 = 4 body**

Uzamykací systém typu 4 je certifikovaný Úřadem.

Uzamykací systém a jeho komponenty musí splňovat požadavky bezpečnostní třídy RC 5 podle ČSN EN 1627.

#### **2.2.2. Uzamykací systém typ 3:**

**SS4 = 3 body**

Uzamykací systém typu 3 je certifikovaný Úřadem.

Uzamykací systém a jeho komponenty musí splňovat požadavky bezpečnostní třídy RC 4 podle ČSN EN 1627.

#### **2.2.3. Uzamykací systém typ 2:**

**SS4 = 2 body**

Uzamykací systém typu 2 je certifikovaný Úřadem.

Uzamykací systém a jeho komponenty musí splňovat požadavky bezpečnostní třídy RC 3 podle ČSN EN 1627.

#### **2.2.4. Uzamykací systém typ 1:**

**SS4 = 1 bod**

Uzamykací systém typu 1 je certifikovaný Úřadem.

Uzamykací systém a jeho komponenty musí splňovat požadavky bezpečnostní třídy RC 2 podle ČSN EN 1627.

**2.2.5. Uzamykací systém typ 0:****SS4 = nehodnoceno (N)**

Uzamykací systém typu 0 není certifikovaný Úřadem.

*Poznámka k bodu 2.:*

Pokud zabezpečenou oblast tvoří komorový trezor, nesmí být vstup do komorového trezoru v té části hranice zabezpečené oblasti, která je současně hranicí objektu. Bodové ohodnocení S2 je v tomto případě rovno 0.

**3. HRANICE OBJEKTU**

Při určení typu objektu je rozhodující ta část hranice objektu, která má nejnižší odolnost. V případě, že hranice objektu je v celé své délce shodná s hranicí zabezpečené oblasti, hodnotí se pouze zabezpečená oblast a bodové hodnocení objektu ( $S3 = 0$ ); režim návštěv v objektu se v tomto případě nehodnotí ( $SS7 = N$ ).

Zvláštním případem hranice objektu je perimetr (plot atd.) na jehož celé hranici a přístupových bodech je realizována ostrahou typu 5. V tomto případě lze hodnotu S3 nahradit součinem bodových hodnocení SS10 (fyzická bariéra typu 2 a výše) a SS11. Body z položek SS10 a SS11, které byly využity v hodnotě S3, se již nezapočítávají do výpočtu hodnoty S6, ale uvádí se v tabulce bodového ohodnocení pro informaci.

Zvláštním případem je hranice objektu vymezená hranicí perimetru (plot atd.). V tomto případě se jako hranice objektu posuzuje navíc i plášť budovy a započte se do hodnoty S3.

**3.1. Objekt typ 4:****S3 = 4 body**

Stěny, podlahy a stropy musí mít zvýšenou nebo zvláště pevnou stavební konstrukci (např. železobetonová konstrukce). Objekt typu 4 má minimální počet dveří, oken a ostatních průlezných otvorů, které musí být zabezpečeny mechanickými zábrannými prostředky a poskytují stejný stupeň odolnosti proti narušiteli jako ostatní části hranice objektu typu 4.

**3.2. Objekt typ 3:****S3 = 3 body**

Stěny, podlahy a stropy musí mít pevnou stavební konstrukci z cihel nebo tvárnic, případně je použita stavební technologie využívající prefabrikovaných a montovaných panelů apod. Průlezné otvory musí být zabezpečeny mechanickými zábrannými prostředky, které poskytují stejný stupeň odolnosti proti narušiteli jako ostatní části hranice objektu typu 3.

Průlezné otvory nemusí být zabezpečeny těmito mechanickými zábrannými prostředky, pokud spodní okraj průlezného otvoru splňuje následující požadavky:

- a) nachází se alespoň 5,5 m nad terénem,
- b) nelze k němu jednoduše proniknout ze střechy nebo za pomoci hromosvodů, okapů, parapetů, jiných stavebních prvků, terénních nerovností, stromů či jiných staveb.



**3.3. Objekt typ 2:****S3 = 2 body**

Objekt je lehké stavební konstrukce. Průlezné otvory musí být zabezpečeny mechanickými zábrannými prostředky nebo technickými prostředky EZS minimálně s instalací SS92=1. Tato podmínka neplatí, pokud spodní okraj průlezného otvoru splňuje následující požadavky:

- a) nachází se alespoň 5,5 m nad terénem,
- b) nelze k němu jednoduše proniknout ze střechy nebo za pomoci hromosvodů, okapů, parapetů, jiných stavebních prvků, terénních nerovností, stromů či jiných staveb.

**3.4. Objekt typ 1:****S3 = 1 bod**

Objekt je vylehčená prefabrikovaná konstrukce, která chrání osoby, materiál a zařízení před povětrnostními vlivy.

**3.5. Objekt typ 0:****S3 = nehodnoceno (N)**

Objekt má viditelně vymezenou hranici, v jejímž rámci existuje možnost kontroly jednotlivých osob a vozidel. Hranici objektu stanoví odpovědná osoba nebo jí pověřená osoba v projektu fyzické bezpečnosti.

**4. SYSTÉM KONTROLY VSTUPU DO ZABEZPEČENÉ OBLASTI NEBO OBJEKTU A REŽIM NÁVŠTĚV****4.1. SYSTÉM KONTROLY VSTUPU DO ZABEZPEČENÉ OBLASTI NEBO OBJEKTU**

Systém kontroly vstupu je hodnocen za předpokladu jeho realizace na všech vstupech do objektu nebo zabezpečené oblasti.

**4.1.1. Systém kontroly vstupu typ 4:****SS6 = 4 body**

Systém kontroly vstupu typu 4 musí být certifikovaný Úřadem a splňuje požadavky podle ČSN EN 50133-1 Poplachové systémy - Systémy kontroly vstupů pro použití v bezpečnostních aplikacích - Část 1: Systémové požadavky pro třídu přístupu B a třídu identifikace 3

- a) identifikační prvek a PIN,
- b) biometrie a PIN, nebo
- c) identifikační prvek a biometrie.

Systém kontroly vstupu typu 4 musí být doplněn přístupovou bariérou, znemožňující opakovaný přístup a zabezpečující režim „jedna transakce - jeden průchod“.

Kontrola vstupu je realizována na všech vstupech do objektu nebo zabezpečené oblasti.

Hlášení ze systému kontroly vstupu typu 4 musí být vyvedeno na stálé stanoviště ostrahy.

**4.1.2. Systém kontroly vstupu typ 3:****SS6 = 3 body**

Systém kontroly vstupu typu 3 musí být certifikovaný Úřadem a splňuje požadavky podle ČSN EN 50133-1. Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 1: Systémové požadavky pro třídu přístupu B a třídu identifikace 3

- a) identifikační prvek a PIN,
- b) biometrie a PIN, nebo
- c) identifikační prvek a biometrie.

Kontrola vstupu je realizována na všech vstupech do objektu nebo zabezpečené oblasti.

Hlášení ze systému kontroly vstupu typu 3 musí být vyvedeno na stálé stanoviště ostrahy.

**4.1.3. Systém kontroly vstupu typ 2:****SS6 = 2 body**

Systém kontroly vstupu typu 2 musí být certifikovaný Úřadem a splňuje požadavky podle ČSN EN 50133-1 Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 1: Systémové požadavky pro třídu přístupu B a třídu identifikace 2

- a) identifikační prvek,
- b) PIN, nebo
- c) biometrie.

Kontrola vstupu je realizována na všech vstupech do objektu nebo zabezpečené oblasti.

Hlášení ze systému kontroly vstupu typu 2 musí být vyvedeno na stálé stanoviště ostrahy.

Systém kontroly vstupu typu 2, lze nahradit kontrolou vstupu, kterou nepřetržitě provádí ostraha příslušníků ozbrojených sil nebo ozbrojených sborů, a to na všech vstupech do objektu nebo zabezpečené oblasti.

**4.1.4. Systém kontroly vstupu typ 1:****SS6 = 1 bod**

Systém kontroly vstupu typu 1 tvoří uzamykatelná mechanická zábrana na vstupu.

Kontrola vstupu je realizována na všech vstupech do objektu nebo na všech vstupech do zabezpečené oblasti.

*Poznámka k bodu 4.1.:*

Systém kontroly vstupu typu 1 lze použít pouze na vstupu do zabezpečené oblasti kategorie Důvěrné nebo Vyhrazené.

Při kontrole vstupu do objektu nebo zabezpečené oblasti kategorie Přísně tajné se používají zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů.

Systém kontroly vstupu, podle bodu 5.2.8 ČSN EN 50133-1 Poplachové systémy – Systémy kontroly vstupů pro použití v bezpečnostních aplikacích – Část 1: Systémové požadavky pro třídu přístupu B, musí hlásit neoprávněný pokus nebo samotné otevření místa

přístupu nebo uplynutí povolené doby po oprávněném otevření místa přístupu. Hlášení musí proběhnout do 10 sekund.

## 4.2. NAMÁTKOVÉ VSTUPNÍ A VÝSTUPNÍ PROHLÍDKY

### 4.2.1. Namátkové prohlídky

**SS12 = 1 bod**

Namátkové prohlídky zabezpečuje orgán státu, právnická nebo podnikající fyzická osoba a jsou prováděny náhodně při vstupu, vjezdu, výstupu a výjezdu z objektu. Namátkové prohlídky jsou určeny jako odstrašující prvek proti porušení ochrany utajovaných informací.

## 4.3. REŽIM NÁVŠTĚV V OBJEKTU

### 4.3.1. Návštěvy s doprovodem:

**SS7 = 3 body**

Návštěvy musí být doprovázeny po celou dobu pobytu v objektu.

Musí být vedena evidence údajů o návštěvách, která obsahuje osobní identifikační údaje návštěv, doprovázejících osob a časové údaje o tom, kdy byla návštěva vykonána.

### 4.3.2. Návštěvy bez doprovodu:

**SS7 = 1 bod**

Návštěvy, které mají povolen vstup bez doprovodu, musí být viditelně označeny. V tomto případě musí být viditelně označeni i všichni vlastní zaměstnanci.

Musí být vedena evidence údajů o návštěvách, která obsahuje osobní identifikační údaje návštěv a časové údaje o tom, kdy byla návštěva vykonána.

### 4.3.3. Návštěvy bez kontroly:

**SS7 = nehodnoceno (N)**

Návštěvy vstupují bez kontroly a doprovodu.

## 5. OSTRAHA A ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE (EZS)

### 5.1. OSTRAHA

#### 5.1.1. Ostraha typ 5:

**SS8 = 5 bodů**

Ostrahu typu 5 zabezpečují pouze příslušníci ozbrojených sil nebo ozbrojených sborů a je vykonávána způsobem nepravidelných obchůzek.

Ostraha provádí obchůzky po náhodně vybraných trasách v náhodných intervalech ne větších než 2 hodiny.

V průběhu výkonu ostrahy, včetně doby obchůzky, musí být na stanovišti stálé ostrahy neustále přítomna nejméně jedna osoba určená pro výkon ostrahy.

**5.1.2. Ostraha typ 4:****SS8 = 4 body**

Ostrahu typu 4 zabezpečují pouze příslušníci ozbrojených sil nebo ozbrojených sborů a je vykonávána způsobem nepravidelných obchůzek.

Ostraha provádí obchůzky v intervalu ne větším než 6 hodin.

V noci a v mimopracovní době se četnost obchůzek zvyšuje.

V průběhu výkonu ostrahy, včetně doby obchůzky, musí být na stanovišti stálé ostrahy neustále přítomna nejméně jedna osoba určená pro výkon ostrahy.

**5.1.3. Ostraha typ 3:****SS8 = 3 body**

Ostrahu typu 3 zabezpečují zaměstnanci orgánu státu, právnické osoby nebo podnikající fyzické osoby, o jejichž objekt jde, příslušníci ozbrojených sil nebo ozbrojených sborů anebo zaměstnanci bezpečnostní ochranné služby.

Intervaly obchůzek jsou závislé na vnitřním provozu a míře předpokládaného rizika.

V průběhu výkonu ostrahy, včetně doby obchůzky, musí být na stanovišti stálé ostrahy neustále přítomna nejméně jedna osoba určená pro výkon ostrahy.

**5.1.4. Ostraha typ 2:****SS8 = 2 body**

Ostrahu typu 2 zabezpečují zaměstnanci orgánu státu, právnické osoby nebo podnikající fyzické osoby, o jejichž objekt jde, příslušníci ozbrojených sil nebo ozbrojených sborů anebo zaměstnanci bezpečnostní ochranné služby.

U ostrahy typu 2 nejsou vyžadovány obchůzky.

**5.1.5. Ostraha typ 1:****SS8 = 1 bod**

Ostraha typu 1 odpovídá střežení objektu napojením na dohledové a poplachové přijímací centrum umožňující rychlý zásah.

*Poznámka k bodu 5.1.:*

Pravidla pro výkon ostrahy je nutné v případě objektu, ve kterém se nachází zabezpečená oblast kategorie Důvěrné, Tajné anebo Přísně tajné nebo jednacích oblast, stanovit v písemné formě.

Ostraha zabezpečených oblastí, ve kterých se ukládají utajované informace Evropské unie stupně utajení Důvěrné a vyšší, se zabezpečuje ostrahou typu 2 a vyšší, s tím že frekvence obchůzek musí být stanovena v intervalech ne větších než 2 hodiny. První obchůzka ostrahy se provede ihned po skončení pracovní doby.

Stanoviště stálé ostrahy je umístěno od zabezpečené oblasti kategorie Přísně tajné a Tajné nejdále 500 m nebo pokud je vzdálenost stanoviště stálé ostrahy větší než 500 m musí být zásah ostrahy proveden do 5 minut od přijetí poplašného nebo nouzového signálu z objektu, zabezpečené oblasti nebo jednacích oblastí.

Ostrahu typu 1 lze použít jen pro objekty kategorie Důvěrné nebo Vyhrazené.

Ostraha musí být vybavena při obchůzce prostředky umožňujícími spojení se stanovištěm pro stálý výkon ostrahy. Doba reakce ostrahy na poplašný nebo nouzový signál musí být ověřována odpovědnou osobou nebo jí pověřenou osobou.

## 5.2. ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE

### 5.2.1. Zařízení elektrické zabezpečovací signalizace typ 4:

SS91 = 4 body

Zařízení elektrické zabezpečovací signalizace typu 4 musí být certifikováno Úřadem a splňuje požadavky podle ČSN EN 50131-1 ed. 2 Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - pro stupeň zabezpečení 4 - vysoké riziko. Tísňový systém splňuje dále požadavky ČSN EN 50134 -1 Poplachové systémy - Systémy přivolání pomoci.

### 5.2.2. Zařízení elektrické zabezpečovací signalizace typ 3:

SS91 = 3 body

Zařízení elektrické zabezpečovací signalizace typu 3 musí být certifikováno Úřadem a splňuje požadavky podle ČSN EN 50131-1 ed. 2 pro stupeň zabezpečení 3 - střední až vysoké riziko. Tísňový systém splňuje dále požadavky ČSN EN 50134 - 1.

### 5.2.3. Zařízení elektrické zabezpečovací signalizace typ 2:

SS91 = 2 body

Zařízení elektrické zabezpečovací signalizace typu 2 musí být certifikováno Úřadem a splňuje požadavky podle ČSN EN 50131-1 ed. 2 pro stupeň zabezpečení 2 - nízké až střední riziko. Tísňový systém splňuje dále požadavky ČSN EN 50134-1.

### 5.2.4. Zařízení elektrické zabezpečovací signalizace typ 1:

SS91 = 1 bod

Zařízení elektrické zabezpečovací signalizace typu 1 nejsou certifikovaná Úřadem.

*Poznámka k bodu 5.2.:*

Předmětem certifikace zařízení elektrické zabezpečovací signalizace jsou:

- ústředny elektrické zabezpečovací signalizace,
- detektory elektrické zabezpečovací signalizace,
- perimetrické detekční systémy,
- tísňové systémy.

Tabulka přiřazení kategorií k typům technických prostředků EZS

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

**5.2.5. Instalace zařízení elektrické zabezpečovací signalizace typ 4:****SS92 = 4 body**

Instalace typu 4 je realizovaná v zabezpečené oblasti v rozsahu:

- a) prostorová ochrana,
- b) plášťová ochrana,
- c) tísňový systém,
- d) otřesové detektory nebo speciální televizní systém snímající nepřetržitě průlezná otvory zabezpečené oblasti.

**5.2.6. Instalace zařízení elektrické zabezpečovací signalizace typ 3****SS92 = 3 body**

Instalace typu 3 je realizovaná v zabezpečené oblasti v rozsahu:

- a) prostorová ochrana,
- b) plášťová ochrana,
- c) tísňový systém nebo speciální televizní systém snímající nepřetržitě průlezná otvory zabezpečené oblasti.

**5.2.7. Instalace zařízení elektrické zabezpečovací signalizace typ 2****SS92 = 2 body**

Instalace typu 2 je realizovaná v zabezpečené oblasti v rozsahu:

- a) prostorová ochrana,
- b) plášťová ochrana.

Průlezná otvory v hranici zabezpečené oblasti v případě instalace zařízení elektrické zabezpečovací signalizace typu 2 nemusí být chráněny prvky plášťové ochrany, pokud jejich spodní okraj splňuje následující podmínky:

- a) nachází se alespoň 5,5 m nad terénem,
- b) nelze k němu jednoduše proniknout ze střechy nebo za pomoci hromosvodů, okapů, parapetů, jiných stavebních prvků, terénních nerovností, stromů či jiných staveb.

**5.2.8. Instalace zařízení elektrické zabezpečovací signalizace typ 1****SS92 = 1 bod**

Instalace typu 1 je realizovaná v rozsahu prostorové ochrany zabezpečené oblasti.

*Poznámka k 5.2.5 až 5.2.8.:*

Instalace zařízení elektrické zabezpečovací signalizace musí splňovat požadavky podle norem řady ČSN EN (CLC/TS) 50131 – Poplachové zabezpečovací a tísňové systémy.

Výstupní hlášení zařízení elektrické zabezpečovací signalizace a speciálního televizního systému musí být vyvedena na stanoviště určené pro stálý výkon ostrahy.

Ovládání zařízení elektrické zabezpečovací signalizace v zabezpečené oblasti musí být nezávislé na ovládání zařízení elektrické zabezpečovací signalizace v ostatních zabezpečených oblastech nebo jiných prostorech.

Instalace zařízení elektrické zabezpečovací signalizace musí být ověřena funkční zkouškou podle TNI 334591-3. Rozsah funkčních zkoušek je stanoven nejméně každých 12 měsíců v tabulce A1 (stupeň 1). Funkční zkouška musí být zaznamenána v provozní knize nebo protokolem o zkoušce, který se ukládá u odpovědné osoby nebo jí pověřené osoby.

### 5.2.9. Výpočet SS9 podle bodového hodnocení SS91 a SS92

$$SS9 = (SS91 + SS92)/2 \times SS92/OBL$$

Hodnota SS9 se matematicky zaokrouhluje na celé číslo.  
Maximální hodnota SS9 může být 4.

**OBL** je bodová hodnota určená kategorií zabezpečené oblasti:

Kategorie zabezpečené oblasti	Bodová hodnota <b>OBL</b>
Přísně tajné	4 body
Tajné	3 body
Důvěrné	2 body
Vyhrazené	1 bod

Je-li v zabezpečené oblasti zajištěna trvalá přítomnost nejméně 1 osoby, není nutno instalovat zařízení elektrické zabezpečovací signalizace; v tomto případě je hodnota SS9 = 4.

Výsledné bodové ohodnocení úrovně zařízení elektrické zabezpečovací signalizace je dáno bodovým ohodnocením použitého technického prostředku nejnižšího typu.

## 5.3. SPECIÁLNÍ TELEVIZNÍ SYSTÉMY

Speciální televizní systémy slouží pro snímání, přenos a zobrazování pohybu osob a dopravních prostředků. Speciální televizní systémy nejsou certifikované Úřadem.

Instalace speciálních televizních systémů musí splňovat požadavky norem řady ČSN EN 50132 – Poplachové přenosové systémy a zařízení – CCTV sledovací systémy pro použití v bezpečnostních aplikacích.

## 6. OCHRANA PERIMETRU

Hranice perimetru je tvořena po celém obvodu fyzickou bariérou.

### 6.1. FYZICKÉ BARIÉRY

Fyzické bariéry jsou vyžadovány po celém obvodu hranice objektu tam, kde to umožňuje její charakter. Konstrukce přístupových bodů (vstupních bran) musí být na stejné bezpečnostní úrovni jako konstrukce fyzické bariéry (oplocení). Na všech přístupových bodech musí být zajištěn stejný standard kontroly vstupu.

#### 6.1.1. Fyzická bariéra typ 4:

**SS10 = 4 body**

Fyzická bariéra typu 4 umožňuje pozorování přilehlého terénu. Je-li to možné, musí být ponechán kolem chráněného objektu 25 metrový volný prostor. Minimální výška vertikální části bariéry je 2,15 metru. Musí být navržena a zkonstruována tak, aby poskytovala co největší překážku proti průniku průlomem. Horní část bariéry musí zajišťovat ochranu proti překonání lezením - oboustranné šikmé vzpěry vyčnívající ven i dovnitř pod úhlem 45° o minimální délce 40 cm, na nichž je po celé délce připevněn ostnatý drát. Fyzická bariéra typu 4 musí být doplněna perimetrickým detekčním systémem.

**6.1.2. Fyzická bariéra typ 3:****SS10 = 3 body**

Fyzická bariéra typu 3 umožňuje pozorování přilehlého terénu. Je-li to možné, musí být ponechán kolem chráněného objektu 25 metrový volný prostor. Minimální výška vertikální části bariéry je 2,15 metru. Musí být navržena a zkonstruována tak, aby poskytovala co největší překážku proti průniku průlomem. Horní část bariéry musí zajišťovat ochranu proti překonání lezením - jednostranné šikmé vzpěry vyčnívající ven pod úhlem 45° o minimální délce 40 cm, na nichž je po celé délce připevněn ostnatý drát.

**6.1.3. Fyzická bariéra typ 2:****SS10 = 2 body**

Fyzická bariéra typu 2 musí poskytovat překážku proti pokusu o překonání lezením a proti průniku průlomem. Minimální výška vertikální části bariéry je 2,15 metru.

**6.1.4. Fyzická bariéra typ 1:****SS10 = 1 bod**

Fyzické bariéry typu 1 odpovídá oplocení bez speciálních bezpečnostních požadavků. Účelem tohoto oplocení je vyznačit hranice a zajistit minimální úroveň odrazení nebo odolnosti. Fyzická bariéra typu 1 může být tvořena jakýmkoliv typem materiálu.

**6.2. Kontrola vstupu ve všech přístupových bodech perimetru****SS11 = 1 bod****6.3. Perimetrický detekční systém (PDS)****6.3.1. Perimetrický detekční systém (PDS) - certifikovaný:****SS13 = 2 body**

Perimetrický detekční systém je certifikovaný Úřadem a vztahují se na něj požadavky uvedené v bodě 5.2. přílohy.

**6.3.2. Perimetrický detekční systém (PDS) - necertifikovaný:****SS13 = 1 bod**

Perimetrický detekční systém není certifikovaný Úřadem a vztahují se na něj požadavky uvedené v bodě 5.2. přílohy.

**6.4. Bezpečnostní osvětlení perimetru:****SS14 = 2 body**

Požadavky na instalaci bezpečnostního osvětlení vyplývají například z požadavků speciálního televizního systému na perimetru.



**6.5. Speciální televizní systém na perimetru:****SS15 = 2 body**

Speciální televizní systém není certifikovaný Úřadem.

Instalace speciálního televizního systému musí splňovat požadavky norem řady ČSN EN 50132 – Poplachové přenosové systémy a zařízení – CCTV sledovací systémy pro použití v bezpečnostních aplikacích.

**7. ZAŘÍZENÍ ELEKTRICKÉ POŽÁRNÍ SIGNALIZACE**

Požární hlásiče musí být zapojeny do ústředny elektrické požární signalizace, nebo do ústředny elektrické zabezpečovací signalizace. V obou případech musí být signál poplachu vyveden na stanoviště určené pro stálý výkon ostrahy.

Zařízení elektrické požární signalizace musí splňovat požadavky norem řady ČSN EN 54 – Elektrická požární signalizace.

Zařízení elektrické požární signalizace nejsou certifikovaná Úřadem.

**8. ZAŘÍZENÍ SLOUŽÍCÍ K VYHLEDÁVÁNÍ NEBEZPEČNÝCH LÁTEK NEBO PŘEDMĚTŮ**

Zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů jsou používána na vstupu do objektu nebo do zabezpečené oblasti kategorie Přísně tajné anebo jednacích oblastí, ve které se pravidelně projednávají utajované informace stupně utajení Přísně tajné.

Zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů nejsou certifikovaná Úřadem. Použije se sestava v rozsahu:

1. Průchozí detektor kovových předmětů, případně doplněný ručním detektorem kovových předmětů.
2. Rentgenový přístroj pro kontrolu zavazadel, doložený kladným Rozhodnutím Státního úřadu pro jadernou bezpečnost o typovém schválení zdroje ionizujícího záření podle zákona č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

**9. ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT****9.1. Zařízení fyzického ničení nosičů informací nebo dat typ 4:****bez bodového ohodnocení**

Zařízení fyzického ničení nosičů informací nebo dat typu 4 jsou určena pro ničení utajovaných informací stupně utajení Přísně tajné nebo nižší. Zařízení fyzického ničení nosičů informací nebo dat je certifikováno Úřadem.

Nosič informací nebo dat	Velikost odpadních částic	
papír, film z polyesteru s uložením informace v originální velikosti, kov, umělá hmota, identifikační karty, magnetické pásky, pevné disky, diskety, kompaktní disky a obdobné nosiče;	šířka částic	≤ 0,8 mm
	délka částic	≤ 13,0 mm
film z polyesteru s uložením informace ve zmenšené velikosti jako mikrofilm, čipové karty, paměťové čipy a obdobné nosiče;	plocha částic	≤ 0,2 mm <sup>2</sup>

Zařízení fyzického ničení nosičů informací nebo dat typu 4 jsou určena také pro ničení utajovaných informací cizí moci stupně utajení Přísně tajné nebo nižší.

### 9.2. Zařízení fyzického ničení nosičů informací nebo dat typ 3: bez bodového ohodnocení

Zařízení fyzického ničení nosičů informací nebo dat typu 3 jsou určena pro ničení utajovaných informací stupně utajení Tajné nebo nižšího. Zařízení fyzického ničení nosičů informací nebo dat je certifikováno Úřadem.

Nosič informací nebo dat	Velikost odpadních částic	
papír, film z polyesteru s uložením informace v originální velikosti, kov, umělá hmota, identifikační karty, diskety, kompaktní disky a obdobné nosiče;	šířka částic	≤ 2,0 mm
	délka částic	≤ 15,0 mm
film z polyesteru s uložením informace ve zmenšené velikosti jako mikrofilm, čipové karty a obdobné nosiče	plocha částic	≤ 0,5 mm <sup>2</sup>

Zařízení fyzického ničení nosičů informací nebo dat typu 3 jsou určena také pro ničení utajovaných informací cizí moci stupně utajení Přísně tajné nebo nižší pouze tehdy, je-li šířka odpadních částic maximálně 1,5 mm.

### 9.3. Zařízení fyzického ničení nosičů informací nebo dat typ 2: bez bodového hodnocení

Zařízení fyzického ničení nosičů informací nebo dat typu 2 jsou určena pro ničení utajovaných informací stupně utajení Důvěrné nebo nižšího. Zařízení fyzického ničení nosičů informací nebo dat je certifikováno Úřadem.

Nosič informací nebo dat	Velikost odpadních částic		
papír, film z polyesteru s uložením informace v originální velikosti, kov, diskety, kompaktní disky a obdobné nosiče;	křížový řez	šířka částic	≤ 4,0 mm
		délka částic	≤ 80,0 mm
	přímý řez	šířka pruhu	≤ 2,0 mm
		délka pruhu	≤ 297,0 mm
		plocha částic*	≤ 320,0 mm <sup>2</sup>
umělá hmota, např. identifikační karty	šířka částic	≤ 4,0 mm	
	délka částic	≤ 80,0 mm	

film z polyesteru s uložením informace ve zmenšené velikosti jako mikrofilm, čipové karty a obdobné nosiče	plocha částic	$\leq 1,0 \text{ mm}^2$
--	---------------	-------------------------

*Poznámka:*

\* Platí pouze pro velkokapacitní zařízení s výkonem  $\geq 500 \text{ kg/h}$

Zařízení fyzického ničení nosičů informací nebo dat typu 2 jsou určena také pro ničení utajovaných informací cizí moci stupně utajení Důvěrné a nižší pouze tehdy, je-li šířka odpadních částic maximálně 3 mm a délka maximálně 25 mm. Plocha odpadních částic nesmí přesáhnout  $60 \text{ mm}^2$  s výjimkou nosičů informací nebo dat, kde je stanovena plocha částic  $\leq 1,0 \text{ mm}^2$ .

#### 9.4. Zařízení fyzického ničení nosičů informací nebo dat typ 1: bez bodového hodnocení

Zařízení fyzického ničení nosičů informací nebo dat typu 1 jsou určena pro ničení utajovaných informací stupně utajení Vyhrazené. Zařízení fyzického ničení nosičů informací nebo dat je certifikováno Úřadem.

Nosič informací nebo dat	Velikost odpadních částic		
papír, film z polyesteru s uložením informace v originální velikosti, kov, diskety, kompaktní disky a obdobné nosiče;	přímý řez	šířka pruhu	$\leq 6,0 \text{ mm}$
		délka pruhu	neomezena
		plocha částic*	$\leq 320,0 \text{ mm}^2$

*Poznámka:*

\* Platí pouze pro velkokapacitní zařízení s výkonem  $\geq 500 \text{ kg/h}$ .

#### 9.5. Zařízení fyzického ničení nosičů informací nebo dat typ 0: bez bodového hodnocení

Zařízení fyzického ničení nosičů informací nebo dat typu 0 jsou určena pro ničení utajovaných informací stupně utajení Přísně tajné nebo nižší. K ničení se používá spalení nebo roztavení, přičemž teplota, které budou vystaveny, a doba jejího působení musí vést k jejich úplnému zničení. Odpovědná osoba nebo jí pověřená osoba, která provádí vyřazování utajované informace, zajistí, že použitím metody spalení nebo roztavení, dojde k úplnému zničení nosiče a nemožnosti obnovení utajované informace.

## 10. ZAŘÍZENÍ PROTI PASIVNÍMU A AKTIVNÍMU ODPOSLECHU UTAJOVANÝCH INFORMACÍ

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

Požadavky na zajištění jednací oblasti proti pasivnímu a aktivnímu odposlechu:

- a) proti pasivnímu odposlechu musí být jednací oblast zajištěna dostatečně zvukotěsnými stěnami, dveřmi, podlahou a stropem,
- b) okna, větrací otvory nebo prostupy klimatizace musí být chráněny technickými prostředky certifikovanými Úřadem. Jednací oblast musí být chráněna proti odezírání z míst nacházejících se vně jednací oblasti,
- c) do jednací oblasti nesmí být umístěn jakýkoliv nábytek nebo jakékoliv zařízení, pokud neprošly kontrolou, zda v jednací oblasti nedochází k nedovolenému použití technických prostředků určených k získávání informací (dále jen „obránná prohlídka“). Nábytek a zařízení jednací oblasti musí být evidováno (včetně typu, případně sériového a inventárního čísla), včetně historie pohybu,
- d) umísťovat telefonní přístroje v jednací oblasti není žádoucí. Pokud je jejich instalace bezpodmínečně nutná, musí být vybaveny odpojovačem nebo odpojovány ručně před jednáním,
- e) do jednací oblasti nelze vnášet mobilní telefony, jakákoliv nahrávací zařízení, vysílací zařízení, jakákoliv testovací, měřicí a diagnostická zařízení a další elektronická zařízení (toto neplatí v případě, že jde o zařízení používané v rámci prováděné obranné prohlídky s vědomím odpovědné osoby nebo jí pověřené osoby),
- f) pro jednací oblast musí být zpracována pravidla pro evidenci a pohyb osob a zařízení.

Podle § 26 odst. 1 zákona je odpovědná osoba povinna požádat Úřad o provedení obranné prohlídky. Při obranné prohlídce bude ověřeno nasazení technických prostředků proti pasivnímu a aktivnímu odposlechu utajované informace.

Obranné prohlídky jednacích oblastí se provádějí ve lhůtách podle § 10 odst. 1 této vyhlášky a dále je nutno provádět obrannou prohlídku vždy po neautorizovaném vstupu či podezření na něj a po odchodu pracovníků provádějících údržbu nebo úpravy v jednací oblasti.

Žádost o provedení obranné prohlídky obsahuje:

- a) obchodní firmu, názvem popřípadě jménem a příjmením pokud je žadatel podnikatel nebo název orgánu státu včetně identifikačního čísla, pokud bylo přiděleno,
- b) adresu umístění jednací oblasti,
- c) výměru podlahové plochy a výška stropů,
- d) dobu předpokládaného provádění obranné prohlídky,
- e) důvod provádění obranné prohlídky (např. z důvodu doplnění nábytku nebo podezření na neautorizovaný vstup),
- f) jméno a příjmení kontaktního pracovníka a kontaktní spojení,
- g) podpis odpovědné osoby.

Požadavky na provádění obranných prohlídek:

- a) fyzická osoba provádějící obranné prohlídky musí být držitelem platného osvědčení fyzické osoby pro stupeň utajení Tajné nebo vyšší,
- b) o průběhu obranné prohlídky musí být vypracována zpráva obsahující:
  1. údaje o orgánu státu, který provádí obrannou prohlídku,
  2. název firmy pokud je žadatel podnikatel nebo název orgánu státu včetně identifikačního čísla, pokud bylo přiděleno, který využívá uvedenou jednací oblast,
  3. adresu umístění jednací oblasti,
  4. datum a čas provedení obranné prohlídky,

5. popis jednacích oblastí (kontrolovaného prostoru) včetně fotodokumentace,
6. provedené úkony,
7. použité kontrolní, měřicí a zkušební zařízení,
8. výsledky měření,
9. výsledek (hodnocení) obranné prohlídky.

Zpráva o průběhu obranné prohlídky musí být přiložena k projektu fyzické bezpečnosti.

## **11. PODMÍNKY POUŽÍVÁNÍ CERTIFIKOVANÝCH TECHNICKÝCH PROSTŘEDKŮ PO UPLYNUTÍ DOBY PLATNOSTI JEJICH CERTIFIKÁTŮ**

Technický prostředek pro ochranu utajovaných informací musí být nově pořízen v době platnosti jeho certifikátu.

Po uplynutí doby platnosti certifikátu může být technický prostředek pro ochranu utajovaných informací používán nebo nasazen za podmínky, že je plně funkční. Toto musí být ověřeno funkční zkouškou. Časové intervaly jsou stanoveny v § 10 této vyhlášky.

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

## **12. BODOVÉ HODNOTY NEJNIŽŠÍ MÍRY ZABEZPEČENÍ FYZICKÉ BEZPEČNOSTI**

### **12.1. TABULKA BODOVÝCH HODNOT NEJNIŽŠÍ MÍRY ZABEZPEČENÍ ZABEZPEČENÉ OBLASTI**

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

ZABEZPEČENÁ OBLAST KATEGORIE Tajné	Míra rizika		
	malá	střední	velká
Povinné : (S1) + (S2) + (S3)	8	9	10
Povinné : (S4) + (S5) **	4	5	5
Nepovinné : (S6)	4	5	5
<b>Celkový výsledek</b>	<b>16</b>	<b>19</b>	<b>20</b>

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
<b>Celkový výsledek</b>	<b>11</b>	<b>14</b>	<b>16</b>

ZABEZPEČENÁ OBLAST KATEGORIE Vyhrazené	
sloužící k ukládání utajované informace v komponentách informačního systému nebo kryptografickém prostředku nebo která vyžaduje zvláštní režim nakládání	
Povinné : (S1) + (S2) + (S3)	2
Nepovinné : (S4) + (S5) + (S6)	1
<b>Celkový výsledek</b>	<b>3</b>

*Poznámka:*

\* - Hodnota (S5) musí dosáhnout alespoň 5 bodů.

\*\* - Hodnota (S5) musí dosáhnout alespoň 4 bodů.

Pouze jedna z hodnot (S1), (S2) nebo (S3) může být rovna 0.

Stanovený objekt, zabezpečenou oblast může využívat k činnosti související s ochranou utajovaných informací pouze jeden orgán státu, právnická nebo podnikající fyzická osoba.

Tabulku bodových hodnot pro zabezpečenou oblast kategorie Vyhrazené, nesloužící k ukládání utajované informace v komponentách informačního systému nebo v kryptografickém prostředku nebo nevyžadující zvláštní režim nakládání, není nutno zpracovávat. V tomto případě pouze jedna z hodnot (S1), (S2) nebo (S3) nemusí být realizována.

U zabezpečené oblasti kategorie Vyhrazené, sloužící k ukládání utajovaných informací v komponentách informačního systému, je bodová hodnota nejnižší míry zabezpečení stanovena jako minimální. Bodové hodnocení může být navýšeno na základě certifikační zprávy informačního systému umístěného v této zabezpečené oblasti.

## 12.2. TABULKA BODOVÝCH HODNOT NEJNIŽŠÍ MÍRY ZABEZPEČENÍ JEDNACÍ OBLASTI

JEDNACÍ OBLAST pro pravidelné projednávání utajovaných informací stupňů utajení Přísně Tajné	Míra rizika		
	malá	střední	velká
Povinné : (S2) + (S3)	6	6	7
Povinné : (S4) + (S5) *	6	7	7
Nepovinné : (S6)	4	5	5
<b>Celkový výsledek</b>	<b>16</b>	<b>18</b>	<b>19</b>

JEDNACÍ OBLAST pro pravidelné projednávání utajovaných informací stupňů utajení <b>Tajné</b>	Míra rizika		
	malá	střední	velká
Povinné : (S2) + (S3)	5	5	6
Povinné : (S4) + (S5) **	4	5	5
Nepovinné : (S6)	4	5	5
<b>Celkový výsledek</b>	<b>13</b>	<b>15</b>	<b>16</b>

*Poznámka :*

\* - Hodnota (S5) musí dosáhnout alespoň 5 bodů.

\*\* - Hodnota (S5) musí dosáhnout alespoň 4 bodů.

Hodnota (S2) nesmí být rovna 0.

*Stanovenou jednací oblast může využívat k činnosti související s ochranou utajovaných informací pouze jeden orgán státu, právnická nebo podnikající fyzická osoba.*

### **13. FYZICKÁ BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ (IS)**

Pokud se v zabezpečené oblasti nebo objektu vyskytuje taková část informačního systému, která může obsahovat utajované informace, nahlíží se na tuto část informačního systému jako na bezpečnostní ekvivalent úschovného objektu (SS1). Identifikace spolu s autentizací uživatele tvoří bezpečnostní ekvivalent zámku úschovného objektu (SS2). Hodnoty SS1 a SS2 lze použít do tabulky bodových hodnot nejnižší míry zabezpečení zabezpečené a jednací oblasti (bod 12. přílohy). V odůvodněných případech, kdy nelze dosáhnout požadovaný minimální součet hodnot S1, S2 a S3, musí být komponenty informačního systému zabezpečeny certifikovanými zařízeními elektrické zabezpečovací signalizace, jejichž instalace odpovídá typu 4 v souladu s bodem 5.2.5.

Informační systémy používané pouze pro zobrazování, zpracovávání nebo přenos utajovaných informací do stupně utajení Tajné mohou být umístěny uvnitř objektu mimo zabezpečenou oblast nebo uvnitř objektu bez zabezpečené nebo jednací oblasti.

### **14. STRUKTURA PROJEKTU FYZICKÉ BEZPEČNOSTI OBJEKTU KATEGORIE DŮVĚRNÉ A VYŠŠÍ**

Obsahová náplň projektu fyzické bezpečnosti se stanovuje v závislosti na kategorii objektu nebo oblasti v rozsahu staveném v § 32 zákona v odst. 1, 3 nebo 4.

#### **14.1. VYHODNOCENÍ RIZIK**

Vyhodnocení rizik obsahuje:

- specifikace aktiv - předpokládané množství utajovaných informací podle stupňů utajení,
- stanovení jednotlivých hrozeb a zranitelnosti a jejich vyhodnocení,
- stanovení celkové míry rizika jako „malé“, „střední“ nebo „velké“.

## 14.2. URČENÍ KATEGORIÍ OBJEKTU, ZABEZPEČENÝCH OBLASTÍ A JEDNACÍCH OBLASTÍ VČETNĚ JEJICH HRANIC A URČENÍ TŘÍD ZABEZPEČENÝCH OBLASTÍ

1. Obecný úvod (adresa), popis areálu/budovy (popis hranice, počet budov/počet podlaží, vstupy, případně zabezpečení), okolí (především objekty, které by mohly mít vliv na bezpečnost), cizí subjekty v areálu/budově (počet, případně název a zaměření činnosti), schéma.
2. Stanovení objektu a jeho typu.
3. Stanovení hranic objektu (umístění v areálu/budově, síla zdí, vstupy, výška oken, stálé stanoviště ostrahy).
4. Popis zabezpečení objektu.
5. Hranici objektu zakreslit do výkresové části Technické dokumentace fyzické bezpečnosti (bod 14.3.2. přílohy).
6. Stanovení zabezpečených oblastí, které se v objektu nacházejí, jejich typ, kategorie a třídu. Je nutné rozlišit, jestli se jedná o úložny utajovaných informací, pracoviště s informačním systémem, oblasti s trvalou přítomností zde pracujících osob, jednacích místností nebo kombinace těchto typů.
7. Stanovení hranic zabezpečených a jednacích oblastí (umístění v objektu, síla zdí, podlah a stropů, vstupy, výška spodního okraje průlezných otvorů nad okolním terénem) a jejich zakreslení do výkresové části Technické dokumentace fyzické bezpečnosti (bod 14.3.2. přílohy).
8. Pro každou zabezpečenou a jednací oblast zpracovat Tabulku bodového ohodnocení opatření fyzické bezpečnosti.

## 14.3. ZPŮSOB POUŽITÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI

### 14.3.1. TABULKA BODOVÉHO OHODNOCENÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI V ZABEZPEČENÉ A JEDNACÍ OBLASTI

Záhlaví tabulky obsahuje tyto údaje:

- a) název zabezpečené (jednací) oblasti,
- b) kategorii a třídu zabezpečené oblasti,
- c) druh jednacích oblastí v závislosti na utajovaných informacích, které jsou v ní pravidelně projednávány,
- d) účel, k němuž má zabezpečená oblast sloužit.

BEZPEČNOSTNÍ OPATŘENÍ	TYP	BODOVÉ OHODNOCENÍ
Úschovné objekty	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body	SS1=
Zámky úschovných objektů	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body	SS2=
Úschovný objekt včetně uzamykacího systému,	<input type="checkbox"/> T. 1 – 1 bod <input type="checkbox"/> T. 1A – 1 bod <input type="checkbox"/> T. 1B – 2 body	S1=



	<input type="checkbox"/> T. 1C – 3 body	
Celkové hodnocení úschovného objektu a jeho zámku	$S1 = SS1 \times SS2$	<b>S1=</b>
Zabezpečené oblasti	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS3=
Uzamykací systém zabezpečené oblasti	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS4=
Celkové ohodnocení zabezpečené oblasti a jejího uzamykacího systému	$S2 = SS3 \times SS4$	<b>S2=</b>
Objekt	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	<b>S3=</b>
Systém kontroly vstupu	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS6=
Režim návštěv v objektu a) Návštěvy s doprovodem b) Návštěvy bez doprovodu c) Návštěvy bez kontroly	<input type="checkbox"/> ad a) – 3 bod <input type="checkbox"/> ad b) – 1 bod <input type="checkbox"/> ad c) – nehodnoceno	SS7=
Celkové hodnocení kontroly vstupu	$S4 = SS6 + SS7$	<b>S4=</b>
Ostraha	<input type="checkbox"/> T. 5 – 5bodů <input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS8=
Zařízení elektrické zabezpečovací signalizace	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS91=
Instalace zařízení elektrické zabezpečovací signalizace	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bod	SS92=
Mezivýsledek (SS 9)		SS9=
Celkové hodnocení ostrahy a systému EZS	$S5 = SS8 + SS9$	<b>S5=</b>
Fyzické bariéry	<input type="checkbox"/> T. 4 – 4 body <input type="checkbox"/> T. 3 – 3 body <input type="checkbox"/> T. 2 – 2 body <input type="checkbox"/> T. 1 – 1 bodů	SS10=

Kontrola vstupu v přístupových bodech perimetru a) Kontrola je realizována b) Kontrola není realizována	<input type="checkbox"/> ad a) – 1 bod <input type="checkbox"/> ad b) – 0 bodů	SS11=
Namátkové vstupní a výstupní prohlídky a) Prohlídky jsou prováděny b) Prohlídky nejsou prováděny	<input type="checkbox"/> ad a) – 1 bod <input type="checkbox"/> ad b) – 0 bodů	SS12=
Perimetrický detekční systém (PDS) - certifikovaný Úřadem - necertifikovaný Úřadem	2 body 1 bod	SS13=
Bezpečnostní osvětlení perimetru	2 body	SS14=
Speciální televizní systém na perimetru	2 body	SS15=
Celkové hodnocení ochrany perimetru	$S6 = (SS10 \times SS11) + SS12 + SS13 + SS14 + SS15$	<b>S6=</b>

Hodnoty proměnných S1 až S6 získané vyplněním tabulky bodového ohodnocení opatření fyzické bezpečnosti v zabezpečené oblasti je nutné porovnat s tabulkou bodových hodnot nejnižší míry zabezpečení zabezpečené a jednací oblasti podle bodu 12. přílohy

Na základě tohoto porovnání je nutné stanovit, zda přijatá opatření fyzické bezpečnosti jsou pro danou míru rizika a kategorii zabezpečené oblasti dostatečná.

Na základě tohoto porovnání je nutné stanovit, zda přijatá opatření fyzické bezpečnosti jsou pro danou míru rizika a dále na stupni utajovaných informací pravidelně projednávaných v jednací oblasti dostatečná.

Ověření, zda jednotlivá použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a právním předpisům v oblasti ochrany utajovaných informací, provádí odpovědná osoba nebo jí pověřená osoba.

Funkční zkoušky pro elektrické zabezpečovací systémy se provádí podle TNI 3345 91-3. Rozsah a časový interval funkčních zkoušek je stanoven v tabulce A1 (stupeň 1). Podmínky funkčních zkoušek u ostatních technických zařízení stanoví odpovědná osoba nebo jí pověřená osoba.

Zápis o provedení funkční zkoušky u technických prostředků uvedených v § 30 odst. 1 zákona se ukládají u odpovědné osoby nebo jí pověřené osoby.

### 14.3.2 TECHNICKÁ DOKUMENTACE FYZICKÉ BEZPEČNOSTI

Tato dokumentace se člení do těchto částí:

- a) Výkresová dokumentace, která obsahuje zejména vyznačení hranice objektu, hranic jednotlivých zabezpečených a jednacích oblastí a rozmístění technických prostředků určených k ochraně utajovaných informací v objektu a zabezpečených a jednacích oblastech,
- b) Dokumentace technických prostředků, která obsahuje zejména
  1. výčet (název, počet a v případě více typů jednoho druhu technického prostředku i umístění),
  2. kopie certifikátu a přílohy z doby instalace,

3. zápisy o posouzení shody z doby instalace (uvést specifikaci a způsob použití).

#### **14.4. PROVOZNÍ ŘÁD**

Provozní řád obsahuje:

1. pravidla pro režim pohybu osob (včetně návštěv) a dopravních prostředků v areálu /budově,
2. pravidla pro režim pohybu osob (včetně návštěv) a dopravních prostředků v objektu a zabezpečených oblastech,
3. pravidla pro režim pohybu utajovaných informací v objektu,
4. pravidla pro zacházení s provozní dokumentací k technickým prostředkům obsahující pokyny pro používání technických prostředků, datum instalace a stanovení pravidelných kontrol funkčnosti technických prostředků (např. provozní knihy, návody k obsluze EZS, speciální televizní systém, EKV, EPS a zařízení proti pasivnímu a aktivnímu odposlechu apod.),
5. pravidla pro manipulaci s klíči a identifikačními prostředky od vstupů do objektu a zabezpečených oblastí a s klíči od úschovných objektů. Tato pravidla musí řešit zejména systém a způsob označování, přidělování a odevzdávání těchto klíčů a identifikačních prostředků, jejich úschovu a evidenci, postup při ztrátě, uložení duplikátů a pravidla pro jejich použití. V případě, že odpovědná osoba nebo jí pověřená osoba rozhodla o uložení klíčů nebo identifikačních prostředků mimo objekt musí o této skutečnosti vést záznamy a dále musí zajistit kontrolu dodržování pravidel manipulace s klíči nebo identifikačními prostředky mimo objekt. Obdobná pravidla je třeba stanovit i pro zacházení s kombinacemi znaků, používaných jako hesla zjednávací přístup do objektů, zabezpečených oblastí nebo úschovných objektů,
6. popis režimových opatření pro ochranu jednacích oblastí,
7. pravidla pro výkon ostrahy stanovující počet členů ostrahy, způsob výkonu ostrahy, zejména způsob kontroly osob a dopravních prostředků při vstupu a výstupu, způsob provádění obchůzek a způsob reakce ostrahy na poplachové výstupní hlášení technických prostředků; v případě, že ostraha je vykonávána na základě smluvního vztahu, je nutné přiložit kopii smlouvy.

#### **14.5. PLÁN ZEBEZPEČENÍ OBJEKTU, ZABEZPEČENÝCH OBLASTÍ A JEDNACÍ OBLASTI V KRIZOVÝCH SITUACÍCH**

Popis opatření k minimalizaci hrozeb a zranitelností popsanych v kapitole vyhodnocení rizik.

Pokyny pro ochranu utajovaných informací v případě vzniku mimořádné situace.

### **15. STRUKTURA PROJEKTU FYZICKÉ BEZPEČNOSTI OBJEKTU KATEGORIE VYHRAZENÉ**

Obsahová náplň projektu fyzické bezpečnosti je stanovena v rozsahu uvedeném v § 32 odst. 2 a 4 zákona.

#### **15.1. URČENÍ OBJEKTU, ZABEZPEČENÝCH OBLASTÍ VČETNĚ JEJICH HRANIC A TŘÍD ZABEZPEČENÝCH OBLASTÍ**

1. Stanovení hranic objektu (umístění v areálu/budově, vstupy, výška oken, stálé stanoviště ostrahy).

2. Hranici objektu zakreslit do výkresové části Technické dokumentace fyzické bezpečnosti (bod 15.2.1. přílohy).
3. Stanovení zabezpečených oblastí, které se v objektu nacházejí a jejich třídu. Je nutné rozlišit, jestli se jedná o úložny utajovaných informací, pracoviště s informačním systémem, oblasti s trvalou přítomností zde pracujících osob nebo kombinace těchto typů.
4. Stanovení hranic zabezpečených oblastí (umístění v objektu, síla zdí, podlah a stropů, vstupy, výška spodního okraje průlezných otvorů nad okolním terénem) a jejich zakreslení do výkresové části Technické dokumentace fyzické bezpečnosti (bod 15.2.1. přílohy).

## 15.2. ZPŮSOB POUŽITÍ OPATŘENÍ FYZICKÉ BEZPEČNOSTI

Způsob použití opatření fyzické bezpečnosti popisuje:

- a) způsob výkonu ostrahy,
- b) přijatá režimová opatření fyzické bezpečnosti (zejména režim pohybu osob, režim pohybu utajovaných informací a pravidla pro manipulaci klíčů).

### 15.2.1 TECHNICKÁ DOKUMENTACE FYZICKÉ BEZPEČNOSTI

Tato dokumentace se člení do těchto částí:

- a) Výkresová dokumentace, která obsahuje zejména vyznačení hranice objektu, hranic jednotlivých zabezpečených oblastí a rozmístění technických prostředků určených k ochraně utajovaných informací v objektu a zabezpečených oblastech.
- b) Dokumentace technických prostředků, která obsahuje zejména
  1. výčet (název, počet a v případě více typů jednoho druhu technického prostředku i umístění),
  2. kopie certifikátu a přílohy z doby instalace,
  3. zápisy o posouzení shody z doby instalace (uvést specifikaci a způsob použití).

U zabezpečené oblasti, kde se ukládá utajovaná informace stupně utajení Vyhrazené v komponentách informačního systému nebo kryptografickém prostředku nebo která vyžaduje zvláštní režim nakládání, se dále zpracovává podle bodu 14.3.1. tabulka bodového ohodnocení opatření fyzické bezpečnosti zabezpečené oblasti.“.

#### Čl. II Účinnost

Tato vyhláška nabývá účinnosti dnem 1. ledna 2012.

Ředitel:

Ing. Navrátil v. r.









8591449 155014  
ISSN 1211-1244

**Vydává a tiskne:** Tiskárna Ministerstva vnitra, p. o., Bartůňkova 4, pošt. schr. 10, 149 01 Praha 415, telefon: 272 927 011, fax: 974 887 395 – **Redakce:** Ministerstvo vnitra, nám. Hrdinů 1634/3, pošt. schr. 155/SB, 140 21 Praha 4, telefon: 974 817 289, fax: 974 816 871 – **Administrace:** písemné objednávky předplatného, změny adres a počtu odebíraných výtisků – MORAVIAPRESS, a. s., U Póny 3061, 690 02 Břeclav, tel.: 516 205 175, e-mail: sbirky@moraviapress.cz. Objednávky ve Slovenské republice přijímá a titul distribuuje Magnet-Press Slovakia, s. r. o., Teslova 12, 821 02 Bratislava, tel.: 00421 2 44 45 46 28, fax: 00421 2 44 45 46 27. **Roční předplatné** se stanovuje za dodávku kompletního ročníku včetně rejstříku z předcházejícího roku a je od předplatitelů vybíráno formou záloh ve výši oznámené ve Sbírce zákonů. Závěrečné vyúčtování se provádí po dodání kompletního ročníku na základě počtu skutečně vydaných částek (první záloha na rok 2011 činí 8 000,- Kč) – Vychází podle potřeby – **Distribuce:** MORAVIAPRESS, a. s., U Póny 3061, 690 02 Břeclav, celoroční předplatné a objednávky jednotlivých částek (dobírky) – 516 205 175, objednávkovo-knihkupci – 516 205 177, e-mail – sbirky@moraviapress.cz, zelená linka – 800 100 314. **Internetová prodejna:** www.sbirkyzakonu.cz – **Drobný prodej** – **Benešov:** Oldřich HAAGER, Masarykovo nám. 231; **Brno:** Ing. Jiří Hrazdil, Vranovská 16, SEVT, a. s., Česká 14; **České Budějovice:** SEVT, a. s., Česká 3, tel.: 387 319 045; **Cheb:** EFREX, s. r. o., Karlova 31; **Chomutov:** DDD Knihkupectví – Antikvariát, Ruská 85; **Kadaň:** Knihařství – Příbíkova, J. Švermy 14; **Kladno:** eL VaN, Ke Stadionu 1953, tel.: 312 248 323; **Klatovy:** Krameriovo knihkupectví, nám. Míru 169; **Liberec:** Podještědské knihkupectví, Moskevská 28; **Litoměřice:** Jaroslav Tvrdík, Štursova 10, tel.: 416 732 135, fax: 416 734 875; **Olomouc:** Knihkupectví ANAG, Ostružnická 8, Zdeněk Chumchal – Knihkupectví Tycho, Ostružnická 3; **Ostrava:** LIBREX, Nádražní 14, SEVT, a. s., Denisova 1; **Otrokovice:** Ing. Kučeřík, Jungmannova 1165; **Pardubice:** LEJHANEK, s. r. o., třída Míru 65; **Plzeň:** Typos, tiskařské závody s. r. o., Úslavská 2, EDICUM, Bačická 15, Technické normy, Na Roudné 5, Vydavatelství a naklad. Aleš Čeněk, nám. Českých bratří 8; **Praha 1:** NEOLUXOR, Na Poříčí 25, LINDE Praha, a. s., Opletalova 35, NEOLUXOR s. r. o., Václavské nám. 41, Právnícké a ekonomické knihkupectví, Elišky Krásnohorské 14, tel.: 224 813 548; **Praha 6:** PPP – Staňková Isabela, Puškinovo nám. 17, PERIODIKA, Komornická 6; **Praha 9:** Abonentní tiskový servis – Ing. Urban, Jablonecká 362, po – pá 7 – 12 hod., tel.: 286 888 382, e-mail: tiskovy.servis@top-dodavatel.cz, DOVOZ TISKU SUWECO CZ, Klečáková 347; **Praha 10:** BMSS START, s. r. o., Vinohradská 190, MONITOR CZ, s. r. o., Třebohostická 5, tel.: 283 872 605; **Přerov:** Odborné knihkupectví, Bartošova 9, Jana Honková-YAHO-i-centrum, Komenského 38; **Sokolov:** KAMA, Kalousek Milan, K. H. Borovského 22, tel./fax: 352 605 959; **Tábor:** Milada Šimonová – EMU, Zavadilská 786; **Teplice:** Knihkupectví L & N, Kapelní 4; **Ústí nad Labem:** PNS Grosso s. r. o., Havířská 327, tel.: 475 259 032, fax: 475 259 029, Kartoon, s. r. o., Solvayova 1597/3, Vazby a doplňování Sbírky zákonů včetně dopravy zdarma, tel.+fax: 475 501 773, www.kartoon.cz, e-mail: kartoon@kartoon.cz; **Zábřeh:** Mgr. Ivana Patková, Žižkova 45; **Zátec:** Jindřich Procházka, Bezděkov 89 – Vazby Sbírek, tel.: 415 712 904. **Distribuční podmínky předplatného:** jednotlivé částky jsou expedovány neprodleně po dodání z tiskárny. Objednávky nového předplatného jsou vyřizovány do 15 dnů a pravidelné dodávky jsou zahajovány od nejbližší částky po ověření úhrady předplatného nebo jeho zálohy. Částky vyšlé v době od zaevidování předplatného do jeho úhrady jsou doposílány jednorázově. Změny adres a počtu odebíraných výtisků jsou prováděny do 15 dnů. **Reklamace:** informace na tel. čísle 516 205 175. V písemném styku vždy uvádějte IČO (právnícká osoba), rodné číslo (fyzická osoba). **Podávání novinových zásilek** povoleno Českou poštou, s. p., Odštěpný závod Jižní Morava Ředitelství v Brně č. j. P/2-4463/95 ze dne 8. 11. 1995.