**523/2005 Sb.**

# VYHLÁŠKA

ze dne 5. prosince 2005

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

Změna: 453/2011 Sb.

Národní bezpečnostní úřad stanoví podle § 34 odst. 5, § 35 odst. 5, § 36 odst. 5 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, (dále jen "zákon"):

## ČÁST PRVNÍ

## ÚVODNÍ USTANOVENÍ

§ 1

### Předmět úpravy

Touto vyhláškou se stanoví požadavky na informační systémy nakládající s utajovanými informacemi[1)] (dále jen "informační systém") a provádění jejich certifikace, na komunikační systémy nakládající s utajovanými informacemi[2)] (dále jen "komunikační systém") a schvalování jejich projektů bezpečnosti, ochranu utajovaných informací v elektronické podobě v zařízeních, která nejsou součástí informačního nebo komunikačního systému, ochranu utajovaných informací před jejich únikem kompromitujícím vyzařováním a provádění certifikace stínicích komor.

§ 2

### Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) aktivem informačního systému na základě analýzy rizik (§ 11) definovaný hardware, software, dokumentace informačního systému a utajované informace, které jsou v informačním systému uloženy,

b) objektem informačního systému pasivní prvek informačního systému, který obsahuje nebo přijímá informaci,

c) subjektem informačního systému aktivní prvek informačního systému, který způsobuje předání informace mezi objekty informačního systému nebo změnu stavu systému,

d) analýzou rizik proces, během něhož jsou zjišťována aktiva informačního systému, hrozby působící na aktiva informačního systému, jeho zranitelná místa, pravděpodobnost realizace

hrozeb a odhad jejich následků,

e) auditním záznamem záznam informačního systému o události, která může ovlivnit bezpečnost informačního systému,

f) identifikací subjektu informačního systému proces zjištění jeho identity v informačním systému,

g) autentizací subjektu informačního systému proces ověření jeho identity v informačním systému, splňující požadovanou míru záruky,

h) autorizací subjektu informačního systému udělení určitých práv pro vykonávání určených aktivit v informačním systému,

i) důvěrností utajované informace její vlastnost, která znemožňuje odhalení utajované informace neoprávněné osobě,

j) fyzickou bezpečností informačního systému nebo komunikačního systému opatření použitá k zajištění fyzické ochrany aktiv těchto systémů proti náhodným nebo úmyslným hrozbám,

k) integritou aktiva informačního systému nebo komunikačního systému vlastnost, která umožňuje provedení jeho změny určeným způsobem a pouze oprávněným subjektem informačního systému,

l) komunikační bezpečností opatření použitá k zajištění ochrany utajovaných informací při přenosu definovaným komunikačním prostředím,

m) počítačovou bezpečností bezpečnost informačního systému zajišťovaná jeho technickými a programovými prostředky,

n) povinným řízením přístupu prostředky pro omezení přístupu subjektů informačního systému k objektům informačního systému, založené na porovnání stupně utajení utajované informace obsažené v objektu informačního systému a úrovně oprávnění subjektu informačního systému pro přístup k utajované informaci a zajišťující správný tok informací mezi objekty informačního systému s různými stupni utajení, nezávisle na volbě učiněné uživatelem,

o) rizikem pro informační systém nebo komunikační systém pravděpodobnost, že určitá hrozba využije zranitelných míst některého z těchto systémů,

p) rolí souhrn určených činností a potřebných autorizací pro subjekt informačního systému působící v informačním systému nebo komunikačním systému,

q) bezpečnostním správcem informačního systému nebo komunikačního systému pracovník správy informačního systému nebo komunikačního systému v roli vytvořené pro řízení a kontrolu bezpečnosti informačního systému nebo komunikačního systému a provádění stanovených činností pro zajištění bezpečnosti informačního systému nebo komunikačního systému,

r) správcem informačního systému nebo komunikačního systému pracovník správy informačního systému nebo komunikačního systému v roli vytvořené zejména pro zajištění

požadované funkčnosti informačního systému nebo komunikačního systému a řízení provozu informačního systému nebo komunikačního systému,

s) uživatelem informačního systému nebo komunikačního systému fyzická osoba v roli vytvořené zejména pro nakládání s utajovanými informacemi v informačním systému nebo pro přenos utajovaných informací v komunikačním systému,

t) řízením přístupu prostředky pro omezení přístupu subjektů informačního systému k objektům informačního systému, zajišťující, že přístup k nim získá jen autorizovaný subjekt informačního systému,

u) volitelným řízením přístupu prostředky omezení přístupu subjektů informačního systému k objektům informačního systému, založené na kontrole přístupových práv subjektu informačního systému k objektu informačního systému, přičemž uživatel, správce nebo bezpečnostní správce informačního systému vybavený určitými přístupovými právy pro přístup k objektu informačního systému může zvolit, na které další subjekty informačního systému přenese přístupová práva k tomuto objektu informačního systému, a může tak ovlivňovat tok informace mezi objekty informačního systému,

v) bezpečnostním standardem utajovaný soubor pravidel, ve kterém se stanoví postupy, technická řešení, bezpečnostní parametry a organizační opatření pro zajištění nejmenší možné míry ochrany utajovaných informací,

w) bezpečnostním provozním módem prostředí, ve kterém informační systém pracuje, charakterizované stupněm utajení zpracovávané utajované informace a úrovněmi oprávnění uživatelů,

x) žadatelem orgán státu nebo podnikatel, který písemně požádal Národní bezpečnostní úřad (dále jen "Úřad") o certifikaci informačního systému, o certifikaci stínicí komory, o schválení projektu bezpečnosti komunikačního systému nebo o ověření způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajované informace kompromitujícím vyzařováním,

y) nepopiratelností schopnost prokázat zpětně 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.

## ČÁST DRUHÁ

## INFORMAČNÍ SYSTÉM

### HLAVA I

### POŽADAVKY NA BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ

§ 3

**Bezpečnost informačních systémů**

(1) Bezpečnosti informačního systému se dosahuje uplatněním souboru opatření z oblasti

a) počítačové a komunikační bezpečnosti,

b) kryptografické ochrany,

c) ochrany proti úniku kompromitujícího vyzařování,

d) administrativní bezpečnosti a organizačních opatření,

e) personální bezpečnosti a

f) fyzické bezpečnosti informačního systému.

(2) Opatření přijatá v procesu certifikace informačního systému zajišťují, aby rizika, kterým je informační systém vystaven, byla snížena na přijatelnou úroveň.

(3) Soubor opatření uvedený v odstavci 1 je specifikován v bezpečnostní dokumentaci informačního systému.

§ 4

**Bezpečnostní dokumentace informačního systému**

(1) Bezpečnostní dokumentaci informačního systému tvoří

a) projektová bezpečnostní dokumentace informačního systému a

b) provozní bezpečnostní dokumentace informačního systému.

(2) Projektová bezpečnostní dokumentace informačního systému obsahuje

a) bezpečnostní politiku informačního systému a výsledky analýzy rizik,

b) návrh bezpečnosti informačního systému zajišťující splnění bezpečnostní politiky informačního systému, přičemž podrobnost jeho popisu musí umožnit přímou realizaci navrhovaných opatření, a

c) dokumentaci k testům bezpečnosti informačního systému.

(3) Provozní bezpečnostní dokumentace informačního systému obsahuje

a) bezpečnostní směrnice informačního systému, které předepisují činnost bezpečnostních správců informačního systému v jednotlivých rolích zavedených v informačním systému pro zajištění bezpečnostní správy informačního systému,

b) bezpečnostní směrnice informačního systému, které předepisují činnost správců informačního systému v jednotlivých rolích zavedených v informačním systému pro správu informačního systému, pokud se týká zajištění bezpečnosti informačního systému, a

c) bezpečnostní směrnice informačního systému, které předepisují činnost uživatelů informačního systému, pokud se týká zajištění bezpečnosti informačního systému.

§ 5

**Bezpečnostní politika informačního systému**

(1) Pro každý informační systém musí být již v počáteční fázi jeho vývoje zpracována bezpečnostní politika informačního systému. Bezpečnostní politiku informačního systému tvoří soubor norem, pravidel a postupů, který vymezuje způsob, jakým má být zajištěna důvěrnost, integrita a dostupnost utajované informace, dostupnost služeb informačního systému a odpovědnost uživatele, bezpečnostního správce a správce informačního systému za jeho činnost v informačním systému. Pokud to funkce informačního systému vyžaduje, stanoví se rovněž způsob zajištění pravosti informací a nepopiratelnost.

(2) Zásady bezpečnostní politiky jsou rozpracovány v návrhu bezpečnosti informačního systému a v provozní bezpečnostní dokumentaci informačního systému.

(3) Při formulaci bezpečnostní politiky informačního systému a posuzování bezpečnostních vlastností komponentů informačního systému lze využít též mezinárodních standardizovaných bezpečnostních specifikací [3)].

§ 6

**Požadavky na formulaci bezpečnostní politiky informačního systému**

Bezpečnostní politika informačního systému se formuluje na základě

a) minimálních bezpečnostních požadavků v oblasti počítačové bezpečnosti,

b) systémově závislých bezpečnostních požadavků, požadavků uživatele a výsledků analýzy rizik a

c) bezpečnostních požadavků bezpečnostní politiky nadřízeného orgánu, pokud byla zpracována.

§ 7

**Minimální bezpečnostní požadavky v oblasti počítačové bezpečnosti**

(1) Informační systém nakládající s utajovanými informacemi stupně utajení Důvěrné nebo vyššího musí zajišťovat tyto bezpečnostní funkce

a) jednoznačnou identifikaci a autentizaci uživatele, bezpečnostního správce nebo správce informačního systému, které musí předcházet všem jejich dalším aktivitám v informačním systému a musí zajistit ochranu důvěrnosti a integrity autentizační informace,

b) volitelné řízení přístupu k objektům informačního systému na základě rozlišování a správy přístupových práv uživatele, bezpečnostního správce nebo správce informačního systému a

jejich identity nebo jejich členství ve skupině uživatelů, bezpečnostních správců nebo správců informačního systému,

c) nepřetržité zaznamenávání událostí, které mohou ovlivnit bezpečnost informačního systému do auditních záznamů a zabezpečení auditních záznamů před neautorizovaným přístupem, zejména modifikací nebo zničením. Zaznamenává se zejména použití identifikačních a autentizačních informací, pokusy o zkoumání přístupových práv, vytváření nebo rušení objektu informačního systému nebo činnost autorizovaných subjektů informačního systému ovlivňující bezpečnost informačního systému,

d) možnost zkoumání auditních záznamů a stanovení odpovědnosti jednotlivého uživatele, bezpečnostního správce nebo správce informačního systému,

e) ošetření paměťových objektů před jejich dalším použitím, zejména před přidělením jinému subjektu informačního systému, které znemožní zjistit jejich předchozí obsah, a

f) ochranu důvěrnosti dat během přenosu mezi zdrojem a cílem.

(2) K zajištění bezpečnostních funkcí uvedených v odstavci 1 se v informačním systému realizují identifikovatelné programově technické mechanismy. Dokumentace popisující jejich provedení a operační nastavení musí umožnit jejich nezávislé prověření a zhodnocení jejich dostatečnosti.

(3) Bezpečnostní mechanismy, jimiž se realizují bezpečnostní funkce uplatňující bezpečnostní politiku informačního systému, musí být v celém životním cyklu informačního systému chráněny před narušením nebo neautorizovanými změnami.

(4) V informačním systému, který nakládá s utajovanými informacemi nejvýše do stupně utajení Vyhrazené, se musí přiměřeně využívat bezpečnostní funkce uvedené v odstavci 1, a dále opatření z oblasti personální, administrativní a fyzické bezpečnosti informačních systémů.

§ 8

**Systémově závislé bezpečnostní požadavky odvozené z bezpečnostního provozního módu**

(1) Informační systémy se mohou provozovat pouze v některém z uvedených bezpečnostních provozních módů, jimiž jsou

a) bezpečnostní provozní mód vyhrazený,

b) bezpečnostní provozní mód s nejvyšší úrovní,

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

d) bezpečnostní provozní mód víceúrovňový.

(2) Bezpečnostní provozní mód vyhrazený je takové prostředí, které umožňuje zpracování utajovaných informací různého stupně utajení, přičemž všichni uživatelé musí

splňovat podmínky pro přístup k utajovaným informacím nejvyššího stupně utajení, které jsou v informačním systému obsaženy, a zároveň musí být oprávněni pracovat se všemi utajovanými informacemi, které jsou v informačním systému obsaženy. Bezpečnost informačního systému, který je provozován v bezpečnostním provozním módu vyhrazeném, se zabezpečuje splněním minimálních bezpečnostních požadavků v oblasti počítačové bezpečnosti uvedených v § 7 odst. 1 písm. a), c), d) a f) a dále opatřeními z oblasti administrativní a personální bezpečnosti a fyzické bezpečnosti informačních systémů. Úroveň použitých opatření z uvedených oblastí a opatření k zajištění důvěrnosti dat během přenosu musí odpovídat úrovni požadované pro nejvyšší stupeň utajení utajovaných informací, se kterými informační systém nakládá.

(3) Bezpečnostní provozní mód s nejvyšší úrovní je takové prostředí, které umožňuje současné zpracování utajovaných informací klasifikovaných různými stupni utajení, ve kterém všichni uživatelé musí splňovat podmínky pro přístup k utajovaným informacím nejvyššího stupně utajení, které jsou v informačním systému obsaženy, přičemž všichni uživatelé nemusí být oprávněni pracovat se všemi utajovanými informacemi. Bezpečnost informačního systému, který je provozován v bezpečnostním provozním módu s nejvyšší úrovní, se zabezpečuje splněním minimálních bezpečnostních požadavků v oblasti počítačové bezpečnosti uvedených v § 7 a dále opatřeními z oblasti administrativní a personální bezpečnosti a fyzické bezpečnosti informačních systémů. Úroveň použitých opatření z uvedených oblastí a opatření k zajištění důvěrnosti dat během přenosu musí odpovídat úrovni požadované pro nejvyšší stupeň utajení utajovaných informací, se kterými informační systém nakládá.

(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.

(5) Bezpečnostní provozní mód víceúrovňový je takové prostředí, které umožňuje v jednom informačním systému současné zpracování utajovaných informací klasifikovaných různými stupni utajení, ve kterém nemusí všichni uživatelé splňovat podmínky přístupu k utajovaným informacím nejvyššího stupně utajení, které jsou v informačním systému obsaženy, přičemž všichni uživatelé nemusí být oprávněni pracovat se všemi utajovanými informacemi. Bezpečnost informačního systému, který je provozován v bezpečnostním provozním módu víceúrovňovém, se zabezpečuje opatřeními uvedenými v odstavci 3 a bezpečnostní funkcí povinného řízení přístupu subjektů informačního systému k objektům informačního systému. Úroveň použitých opatření z oblasti administrativní a personální bezpečnosti, fyzické bezpečnosti informačních systémů a opatření k zajištění důvěrnosti dat během přenosu se stanoví na základě principu povinného řízení přístupu.

(6) Funkce povinného řízení přístupu subjektů informačního systému k objektům informačního systému musí zabezpečit

a) trvalé spojení každého subjektu informačního systému a objektu informačního systému s bezpečnostním atributem, který pro subjekt informačního systému vyjadřuje úroveň oprávnění subjektu informačního systému a pro objekt informačního systému jeho stupeň utajení,

b) ochranu integrity bezpečnostního atributu,

c) výlučné oprávnění bezpečnostního správce informačního systému k provádění změn

bezpečnostních atributů subjektů informačního systému i objektů informačního systému a

d) přidělení předem definovaných hodnot atributů pro nově vytvořené objekty informačního systému a zachování atributu při kopírování objektu informačního systému.

(7) Při uplatňování bezpečnostní funkce povinného řízení přístupu subjektů informačního systému k objektům informačního systému musí být zabezpečeny tyto zásady

a) subjekt informačního systému může číst informace v objektu informačního systému pouze tehdy, je-li úroveň jeho oprávnění stejná nebo vyšší než stupeň utajení objektu informačního systému,

b) subjekt informačního systému může zapisovat informaci do objektu informačního systému pouze tehdy, je-li úroveň jeho oprávnění stejná nebo nižší než stupeň utajení objektu informačního systému, a

c) přístup subjektu informačního systému k informaci obsažené v objektu informačního systému je možný, jestliže jej povolují jak pravidla povinného řízení přístupu, tak pravidla volitelného řízení přístupu.

(8) Informační systém, který je provozován v bezpečnostním provozním módu víceúrovňovém, musí být schopen přesně označit stupněm utajení utajované informace vystupující z informačního systému a umožnit přiřadit stupeň utajení utajované informaci vstupující do informačního systému.

(9) U informačního systému, který je provozován v bezpečnostním provozním módu víceúrovňovém a nakládá s utajovanou informací stupně utajení Přísně tajné, musí být provedena identifikace a analýza skrytých kanálů. Skrytým kanálem se rozumí nepřípustná komunikace, jíž se utajovaná informace může dostat k neoprávněnému subjektu informačního systému.

§ 9

**Systémově závislé bezpečnostní požadavky na bezpečnost v prostředí počítačových sítí**

(1) Při přenosu utajované informace komunikačním kanálem musí být zajištěna ochrana její důvěrnosti a integrity.

(2) Základním prostředkem pro zajištění důvěrnosti utajované informace při jejím přenosu komunikačním kanálem je kryptografická ochrana[4)].

(3) Základním prostředkem pro zajištění integrity utajované informace při jejím přenosu komunikačním kanálem je spolehlivá detekce záměrné i náhodné změny utajované informace.

(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.

(5) V závislosti na komunikačním prostředí se zajišťuje spolehlivá identifikace a autentizace komunikujících stran, včetně ochrany identifikační a autentizační informace. Tato identifikace a autentizace předchází přenosu utajované informace.

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

(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.

§ 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.

§ 10

**Požadavky na dostupnost utajované informace a služeb informačního systému**

(1) Informační systém musí zajistit, aby požadovaná utajovaná informace byla přístupná ve stanoveném místě, v požadované formě a v určeném časovém rozmezí.

(2) V zájmu zajištění bezpečného provozu informačního systému se v bezpečnostní politice informačního systému stanoví komponenty, které musí být nahraditelné bez přerušení činnosti informačního systému. Dále se definuje rozsah požadované minimální funkčnosti informačního systému a uvedou se komponenty, při jejichž selhání musí být minimální funkčnost informačního systému zaručena.

(3) Plánování kapacit aktiv informačního systému a sledování kapacitních požadavků se provádí tak, aby nedocházelo k chybám způsobeným nedostatkem volných kapacit.

(4) Informační systém musí mít zpracován plán na obnovení jeho činnosti po havárii. Opětovné uvedení informačního systému do známého zabezpečeného stavu může být provedeno manuálně správcem informačního systému nebo automaticky. Všechny činnosti, které byly provedeny pro obnovení činnosti informačního systému, se zpravidla zaznamenávají do auditních záznamů chráněných před neoprávněnou modifikací nebo zničením.

§ 11

**Systémově závislé bezpečnostní požadavky odvozené z analýzy rizik**

(1) Pro stanovení hrozeb, které ohrožují aktiva informačního systému, musí být provedena analýza rizik.

(2) V rámci provedení analýzy rizik se vymezují aktiva informačního systému a hrozby, které působí na jednotlivá aktiva informačního systému. Posuzují se zejména hrozby, které způsobují ztrátu funkčnosti nebo bezpečnosti informačního systému.

(3) Po stanovení hrozeb se vymezují zranitelná místa informačního systému tak, že ke každé hrozbě se najde zranitelné místo nebo místa, na která tato hrozba působí.

(4) Výsledkem provedené analýzy rizik je seznam hrozeb, které mohou ohrozit informační systém, s uvedením odpovídajícího rizika.

(5) Na základě provedené analýzy rizik se provádí výběr vhodných protiopatření 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.

§ 12

**Možnost nahrazení prostředků počítačové bezpečnosti**

Zajištění některých bezpečnostních funkcí informačního systému prostředky počítačové bezpečnosti lze v odůvodněných případech nahradit zvýšeným použitím prostředků personální nebo administrativní bezpečnosti, fyzické bezpečnosti informačních systémů anebo organizačních opatření. Při nahrazení prostředků počítačové bezpečnosti náhradním bezpečnostním mechanismem nebo skupinou mechanismů, které mají zajišťovat určitou bezpečnostní funkci, musí být plně realizována bezpečnostní funkce a zachována kvalita a úroveň bezpečnostní funkce.

§ 13

**Požadavky na ochranu mobilních a přenosných informačních systémů**

(1) Pro mobilní a přenosné informační systémy se v analýze rizik posuzují i rizika, která jsou u mobilních informačních systémů spojená s dopravním prostředkem, a u přenosných informačních systémů s prostředími, ve kterých budou tyto informační systémy používány.

(2) Systém opatření použitých pro celkovou ochranu mobilních a přenosných informačních systémů, obsahujících komponenty umožňující uchování utajovaných informací, musí vedle ostatních požadavků stanovených touto vyhláškou zahrnovat pojetí tohoto zařízení jako nosiče utajované informace klasifikovaného nejvyšším stupněm utajení utajované informace, se kterou nakládá.

§ 14

**Požadavky ochrany proti kompromitujícímu vyzařování**

(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 vyzařování nezpůsobilo únik utajované informace.

(2) Požadavky na zabezpečení proti kompromitujícímu vyzařování 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 vyzařování 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

**Požadavky na bezpečnost nosičů utajovaných informací**

(1) Všechny nosiče utajovaných informací používané v provozu informačního systému musí být evidovány. Stupeň utajení těchto nosičů informací musí odpovídat bezpečnostnímu provoznímu módu a nejvyššímu stupni utajení utajovaných informací na nosiči uložených.

(2) Pokud je vyměnitelný nosič utajovaných informací určen výhradně pro použití v provozu určitého informačního systému, vyznačuje se spolu se stupněm utajení i název daného informačního systému a evidenční číslo nosiče informací. Nosiče utajovaných informací určené pro předání nebo výdej informací z informačního systému se označují stupněm utajení a dalšími údaji podle zvláštního právního předpisu[5)].

(3) Nosiče utajovaných informací zabudované do zařízení a jiné komponenty umožňující uchování utajovaných informací musí být evidovány a označeny stupněm utajení nejpozději po jejich vyjmutí z daného zařízení. Zařízení se evidují v provozní bezpečnostní dokumentaci informačního systému.

(4) Stupeň utajení nosiče utajovaných informací stupně utajení Přísně tajné nesmí být snížen, vyjma případu, kdy je prokázáno, že na něm byly během jeho dosavadního životního cyklu uloženy pouze utajované informace nižšího stupně utajení nebo informace neutajované.

(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.

(7) Ničení nosiče utajovaných informací informačního systému musí být provedeno tak, aby se znemožnilo utajovanou informaci z něho opětovně získat.

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

§ 16

**Požadavky na přístup k utajované informaci v informačním systému**

(1) Uživatelem, bezpečnostním správcem nebo správcem informačního systému může být pouze osoba, která byla pro svou činnost v informačním systému autorizována postupem stanoveným v bezpečnostní dokumentaci informačního systému.

(2) Uživatel, bezpečnostní správce a správce informačního systému musí splňovat podmínky pro přístup fyzické osoby k utajované informaci stupně utajení, který se stanovuje v souladu s bezpečnostním provozním módem a v závislosti na nejvyšším stupni utajení utajovaných informací, se kterými může informační systém nakládat.

(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 stupeň 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.

(6) Uživateli, bezpečnostnímu správci a správci informačního systému se na základě autorizace přiděluje v rámci informačního systému jedinečný identifikátor. Pro zajištění nepřetržité dostupnosti utajovaných informací a služeb informačního systému, který je ve stálém provozu, může v odůvodněných případech Úřad v rámci jeho certifikace umožnit, aby určitý identifikátor byl využíván několika uživateli, bezpečnostními správci nebo správci informačního systému. Předpokladem je zavedení postupu umožňujícího určit, který uživatel, bezpečnostní správce nebo správce informačního systému v dané době daný identifikátor využíval.

(7) Uživateli, bezpečnostnímu správci nebo správci informačního systému se uděluje oprávnění pouze v rozsahu nezbytném pro provádění jemu určených aktivit v informačním

systému.

§ 17

**Požadavek odpovědnosti za činnost v informačním systému**

(1) Uživatel, bezpečnostní správce a správce informačního systému dodržuje předepsané postupy stanovené v bezpečnostní dokumentaci informačního systému, kterými je zajišťována bezpečnost informačního systému.

(2) Informace o činnosti subjektu informačního systému v informačním systému se zaznamenává tak, aby bylo možno identifikovat narušení bezpečnosti informačního systému nebo pokusy o ně. Záznamy o činnosti subjektu informačního systému v informačním systému se uchovávají pro zpětné zkoumání po dobu stanovenou v bezpečnostní politice informačního systému.

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

§ 18

**Bezpečnostní správa informačního systému**

(1) V informačním systému se zavádí vhodný systém bezpečnostní správy informačního systému. V rámci systému bezpečnostní správy informačního systému se zavádí role bezpečnostního správce informačního systému, odděleně od jiných rolí ve správě informačního systému, pokud není dále stanoveno jinak.

(2) V případě potřeby zajistit stanovený rozsah činnosti pro zajištění bezpečnosti informačního systému se zavádějí další role v bezpečnostní správě informačního systému, zejména organizační struktura bezpečnostních správců, bezpečnostní správci jednotlivých lokalit, bezpečnostní správce pro oblast komunikační bezpečnosti nebo bezpečnostní správce bezpečnostního rozhraní informačních systémů.

(3) Role bezpečnostního správce informačního systému obsahuje výkon správy bezpečnosti informačního systému spočívající zejména v přidělování přístupových práv, správě autentizačních a autorizačních informací, správě konfigurace informačního systému, správě a vyhodnocování auditních záznamů, aktualizaci bezpečnostních směrnic, řešení bezpečnostních incidentů a krizových situací a vypracování zpráv o nich, zajištění školení uživatelů v oblasti bezpečnosti informačního systému, kontroly dodržování bezpečnostních provozních směrnic, jakož i v dalších činnostech stanovených v bezpečnostní dokumentaci informačního systému.

(4) V informačním systému malého rozsahu může Úřad v rámci jeho certifikace umožnit spojení role bezpečnostního správce a některých dalších rolí ve správě informačního systému.

(5) Správce informačního systému mimo činnosti pro zajištění funkčnosti informačního systému a řízení jeho provozu plní stanovené činnosti pro zajištění počítačové a komunikační

bezpečnosti informačního systému.

§ 19

**Požadavky personální bezpečnosti při provozu informačního systému**

(1) Činnost uživatele, bezpečnostního správce a správce informačního systému v informačním systému se umožňuje na základě jeho autorizace pro tuto činnost, která musí být změněna při změně jeho role v rámci informačního systému nebo zrušena, pokud přestal splňovat podmínky přístupu k utajované informaci. Bezpečnostní správce vede seznam uživatelů informačního systému.

(2) Provozovatel informačního systému zajišťuje úvodní školení uživatelů, bezpečnostních správců a správců informačního systému v dodržování opatření stanovených v bezpečnostní dokumentaci informačního systému a správném užívání informačního systému. Další školení zajišťuje při podstatných změnách v informačním systému okamžitě, jinak nejméně jednou ročně.

§ 20

**Požadavky fyzické bezpečnosti informačních systémů**

(1) Aktiva informačního systému musí být umístěna do prostoru, ve kterém je zajištěna fyzická ochrana informačního systému před neoprávněným přístupem, poškozením a ovlivněním. V rámci certifikace informačního systému se stanovuje, které komponenty informačního systému musí být umístěny v zabezpečené oblasti nebo v objektu, a požadovaná kategorie zabezpečené oblasti.

(2) Aktiva informačního systému musí být chráněna před bezpečnostními hrozbami a riziky vyplývajícími z prostředí, ve kterém jsou umístěna.

(3) Umístění aktiv informačního systému musí být provedeno tak, aby zamezovalo nepovolané osobě odezírat utajované informace nebo informace sloužící k identifikaci a autentizaci uživatele.

(4) Komunikační infrastruktura přenášející data nebo podporující služby informačního systému musí být chráněna před možností zachycení přenášených utajovaných informací a před poškozením.

(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.

§ 21

**Požadavek testování bezpečnosti informačního systému**

(1) Bezpečnost informačního systému se musí před vydáním certifikátu ověřit nezávislým testováním. K provedení testování se nesmějí používat utajované informace.

(2) Výsledky testů musí prokázat, že bezpečnostní funkce jsou plně v souladu s bezpečnostní politikou informačního systému. Výsledky testů musí být zadokumentovány. Chyby nalezené během testování musí být odstraněny a jejich odstranění musí být ověřeno následnými testy.

§ 22

**Požadavky na bezpečnost při instalaci informačního systému**

Postup instalace informačního systému musí být organizován tak, aby nebyla ohrožena jeho bezpečnost a oslabeny jeho bezpečnostní funkce. V bezpečnostní politice informačního systému se stanoví komponenty informačního systému, které musí být instalovány osobami splňujícími podmínky zákona pro přístup k utajovaným informacím nejvyššího stupně utajení, pro jehož nakládání je informační systém určen. Jedná se o komponenty zajišťující bezpečnostní funkce informačního systému nebo komponenty vyhodnocené jako zranitelné ve fázi instalace. Ostatní komponenty informačního systému mohou být instalovány osobami splňujícími podmínky zákona pro přístup k utajované informaci nižšího stupně utajení nebo osobami nesplňujícími podmínky pro přístup k utajované informaci, schválenými bezpečnostním ředitelem provozovatele informačního systému, avšak pod neustálým dohledem pracovníka správy informačního systému, prověřeného pro přístup k utajovaným informacím nejvyššího stupně utajení, pro jehož nakládání je informační systém určen.

§ 23

**Požadavky na bezpečnost provozovaného informačního systému**

(1) Bezpečnost provozovaného informačního systému musí být průběžně, s ohledem na skutečný stav informačního systému, prověřována a vyhodnocována. Dílčí změnu v informačním systému je možno provést až po vyhodnocení vlivu této změny na bezpečnost informačního systému a po jejím schválení Úřadem, nestanoví-li certifikační zpráva jinak.

(2) Integrita programového vybavení i utajovaných informací musí být chráněna před působením škodlivého kódu.

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

(4) V provozovaném informačním systému může být používáno pouze softwarové a hardwarové vybavení odpovídající bezpečnostní dokumentaci informačního systému schválené Úřadem a podmínkám certifikační zprávy k certifikátu informačního systému.

(5) V provozovaném informačním systému musí být prováděno zálohování programového vybavení a utajovaných informací. Záloha programového vybavení a utajovaných informací musí být uložena tak, aby nemohlo dojít k jejímu poškození nebo ke zničení při ohrožení informačního systému anebo zneužití pro narušení důvěrnosti utajovaných

informací.

(6) Servisní činnost v provozovaném informačním systému se musí organizovat tak, aby nebyla ohrožena jeho bezpečnost. Z nosičů utajovaných informací informačního systému přístupných při servisní činnosti musí být vymazány utajované informace a dálková diagnostika musí být zabezpečena před zneužitím.

(7) Údržbu komponent informačního systému zajišťujících bezpečnostní funkce informačního systému nebo přímo ovlivňujících bezpečnost informačního systému musí zajišťovat osoby splňující podmínky zákona pro přístup k utajovaným informacím nejvyššího stupně utajení, pro jehož nakládání je informační systém určen. Takové komponenty musí být stanoveny v provozní bezpečnostní dokumentaci informačního systému. Údržba ostatních komponentů informačního systému může být prováděna osobami splňujícími podmínky zákona pro nižší stupeň utajení nebo osobami schválenými bezpečnostním ředitelem provozovatele informačního systému, avšak pod neustálým dohledem pracovníka správy informačního systému prověřeného pro přístup k utajovaným informacím nejvyššího stupně utajení, pro jehož nakládání je informační systém určen.

(8) V provozovaném informačním systému musí být v termínech stanovených v bezpečnostní dokumentaci informačního systému a při vzniku krizové situace neprodleně prováděno vyhodnocení auditních záznamů. Auditní záznamy musí být archivovány po dobu stanovenou v bezpečnostní dokumentaci informačního systému a chráněny před modifikací nebo zničením.

(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.

(10) Pro řešení krizové situace provozovaného informačního systému musí být v bezpečnostní dokumentaci informačního systému stanovena opatření zaměřená na jeho uvedení do stavu odpovídajícího bezpečnostní dokumentaci informačního systému. V bezpečnostní dokumentaci informačního systému musí být uvedeny základní typy krizových situací, které mohou podle analýzy rizik nastat, a pro každou z nich specifikována činnost následující

a) bezprostředně po vzniku krizové situace zaměřená na minimalizaci škod a zajištění informací potřebných pro zjištění příčin a mechanismu vzniku krizové situace a

b) po vzniku krizové situace zaměřená na likvidaci následků krizové situace včetně vymezení osobní odpovědnosti za jednotlivé úkoly.

(11) Pro případ havárie softwarového nebo hardwarového vybavení musí být uveden v bezpečnostní dokumentaci informačního systému způsob

a) zálohování informačního systému a uložení záložních médií,

b) zajišťování servisní činnosti,

c) zajištění nouzového provozu informačního systému s vyjmenováním minimálních funkcí,

které musí být zachovány, a

d) obnovy funkčnosti a uvedení informačního systému do známého bezpečného stavu.

(12) Před trvalým ukončením provozu informačního systému musí být provedeno vyjmutí nebo zničení nosičů utajovaných informací, se kterými informační systém nakládal.

## HLAVA II

## CERTIFIKACE INFORMAČNÍCH SYSTÉMŮ

### § 24

### Žádost o certifikaci informačního systému a způsob a podmínky jejího provedení

(1) Žádost o certifikaci informačního systému obsahuje

a) identifikaci žadatele
1. obchodní firmou, popřípadě názvem, sídlem a identifikačním číslem, bylo-li přiděleno, je-li žadatelem právnická osoba,
2. obchodní firmou, popřípadě jménem a příjmením, případně odlišujícím dodatkem, místem trvalého pobytu nebo u cizince místem obdobného pobytu a místem podnikání, liší-li se od trvalého pobytu, datem narození a identifikačním číslem, bylo-li přiděleno, je-li žadatelem fyzická osoba, která je podnikatelem, nebo
3. názvem, sídlem, identifikačním číslem a jménem a příjmením odpovědné osoby, jde-li o orgán státu,

b) jméno a příjmení kontaktního pracovníka žadatele a kontaktní spojení,

c) stručný popis účelu a rozsahu informačního systému,

d) stupeň utajení utajovaných informací, se kterými bude informační systém nakládat,

e) stanovení bezpečnostního provozního módu informačního systému a

f) identifikaci dodavatele informačního systému nebo jeho komponent ovlivňujících bezpečnost informačního systému, podle písmene a) bodu 1 nebo 2, a stupeň utajení, pro který bylo vydáno dodavateli osvědčení podnikatele nebo kopii platného prohlášení podnikatele.

(2) K provedení certifikace informačního systému žadatel předloží následující podklady

a) bezpečnostní politiku informačního systému a výsledky analýzy rizik,

b) návrh bezpečnosti informačního systému,

c) sadu testů bezpečnosti informačního systému, jejich popis a popis výsledků testování,

d) bezpečnostní provozní dokumentaci informačního systému,

e) popis bezpečnosti vývojového prostředí a

f) další podklady nezbytné k certifikaci informačního systému, vyplývající ze specifikace informačního systému.

(3) Žádá-li o provedení certifikace informačního systému zpravodajská služba, uvede v žádosti podle odstavce 1 a v podkladech podle odstavce 2 pouze nezbytné údaje, které umožní Úřadu provedení certifikace informačního systému.

(4) Jako podklad pro certifikaci informačního systému může žadatel předložit také výsledky dílčích úloh v hodnocení některých komponent informačního systému a v hodnocení jednotlivých oblastí bezpečnosti uvedených v § 3 odst. 1, provedených orgánem státu nebo podnikatelem na základě smlouvy o zajištění činnosti uzavřené s Úřadem.

(5) V rámci certifikace informačního systému se posuzuje vhodnost souboru opatření navržených pro dosažení bezpečnosti informačního systému podle § 3, správnost a úplnost bezpečnostní dokumentace informačního systému a správnost realizace navrženého souboru opatření v daném informačním systému.

(6) Certifikace informačního systému se provádí posouzením podkladů předložených žadatelem a provedením dodatečných testů. Dodatečné testy provádí Úřad v provozním prostředí hodnoceného informačního systému za spoluúčasti žadatele a v případě potřeby dodavatele.

(7) Certifikaci informačního systému lze provádět průběžně po ukončení jednotlivých fází výstavby informačního systému nebo až po jeho celkovém dokončení.

(8) Dojde-li v informačním systému, který byl certifikován a schválen do provozu, ke změnám uvedeným v § 25 písm. d), provádí se doplňující hodnocení informačního systému v rozsahu potřebném k posouzení provedených změn. V případě provádění doplňujícího hodnocení informačního systému se postupuje obdobně jako při provádění certifikace informačního systému.

(9) Vzor certifikátu informačního systému je uveden v příloze č. 1 této vyhlášky.

§ 25

**Certifikační zpráva informačního systému**

Certifikační zpráva obsahuje

a) orientační popis informačního systému,

b) podmínky provozu informačního systému,

c) identifikaci případných přijatelných rizik souvisejících s provozem informačního systému a

d) typy změn informačního systému, které vyžadují provedení doplňujícího hodnocení informačního systému.

§ 26

**Žádost o opakovanou certifikaci informačního systému a způsob jejího provedení**

(1) Žádost o opakovanou certifikaci informačního systému obsahuje

a) identifikaci žadatele podle § 24 odst. 1 písm. a),

b) úplnou identifikaci vydaného certifikátu informačního systému obsahující jeho držitele, evidenční číslo, datum vydání a dobu platnosti,

c) identifikaci informačního systému obsahující jeho název, označení verze a stupeň utajení utajovaných informací, pro který byla schválena jeho způsobilost, a

d) jméno a příjmení kontaktního pracovníka žadatele a kontaktní spojení.

(2) Pokud žadatel doloží, že ke dni ukončení platnosti dosavadního certifikátu bude informační systém provozován v rámci podmínek stanovených v certifikační zprávě, a žadatel ani Úřad neidentifikovali nová rizika pro informační systém, vydá Úřad certifikát na základě existující bezpečnostní dokumentace informačního systému a provedené kontroly bezpečnosti informačního systému.

(3) Pokud ke dni ukončení platnosti dosavadního certifikátu provozovatel navrhuje změnu bezpečnostní politiky informačního systému, případně byla identifikována nová rizika pro informační systém, vyžádá si Úřad doplnění nebo úpravu odpovídajících částí dokumentace a provede doplňující hodnocení informačního systému v rozsahu stanoveném Úřadem. Pokud informační systém vyhoví stanoveným bezpečnostním podmínkám, Úřad vydá certifikát.

(4) V případě, že navrhované změny bezpečnostní politiky informačního systému jsou podstatné pro celkovou bezpečnost informačního systému, bude Úřad postupovat jako v případě nové certifikace.

## ČÁST TŘETÍ

## KOMUNIKAČNÍ SYSTÉM

§ 27

**Náležitosti projektu bezpečnosti komunikačního systému**

(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.

(2) Bezpečnostní politika komunikačního systému vymezuje způsob, jakým má být

zajištěna důvěrnost, integrita a dostupnost utajované informace a odpovědnost uživatele za jeho činnost v daném komunikačním systému.

(3) Bezpečnostní politika komunikačního systému obsahuje souhrn zásad a požadavků v oblasti personální, administrativní, fyzické a komunikační bezpečnosti, stanovených v závislosti na stupni utajení přenášených utajovaných informací, na výsledcích analýzy rizik komunikačního systému a na zásadách a podmínkách provozování kryptografického prostředku uvedených v certifikační zprávě kryptografického prostředku.

(4) Organizační opatření a provozní postupy provozování komunikačního systému obsahují

a) způsob, jakým bude zajištěn výkon kryptografické ochrany v souladu s certifikační zprávou kryptografického prostředku,

b) požadovanou strukturu správy komunikačního systému a

c) organizační opatření a zásady provozních postupů, jejichž naplňováním bude zajištěna ochrana utajovaných informací přenášených v komunikačním systému.

(5) Na základě bezpečnostní politiky komunikačního systému a organizačních opatření a provozních postupů provozování komunikačního systému se zpracují odděleně provozní směrnice pro bezpečnostní správu komunikačního systému a provozní směrnice uživatele komunikačního systému. Tyto směrnice musí obsahovat konkrétní provozní postupy pro zajištění bezpečnostní správy komunikačního systému a výkonu kryptografické ochrany a musí stanovit odpovědnost pracovníků správy komunikačního systému, pracovníků kryptografické ochrany a uživatelů k zajištění ochrany utajovaných informací.

§ 28

**Žádost o schválení projektu bezpečnosti komunikačního systému**

(1) Žádost o schválení projektu bezpečnosti komunikačního systému předkládá orgán státu nebo podnikatel, který bude komunikační systém provozovat.

(2) Žádost podle odstavce 1 obsahuje

a) identifikaci žadatele podle § 24 odst. 1 písm. a),

b) jméno a příjmení kontaktního pracovníka a kontaktní spojení,

c) stupeň a číslo osvědčení podnikatele nebo kopii platného prohlášení podnikatele, je-li žadatelem podnikatel,

d) název a stručný popis účelu a rozsahu komunikačního systému včetně stanovení jeho běžných provozních funkcí,

e) stupeň utajení utajovaných informací, se kterými bude komunikační systém nakládat, a

f) identifikaci dodavatele jednotlivých komponent komunikačního systému majících vliv na

bezpečnost komunikačního systému, podle § 24 odst. 1 písm. a) bodu 1 nebo 2, a stupeň utajení, pro který bylo vydáno dodavateli osvědčení podnikatele nebo kopii platného prohlášení podnikatele.

(3) K žádosti podle odstavce 2 se v průběhu schvalování přikládají jednotlivé části projektu bezpečnosti komunikačního systému podle § 27 odst. 3.

(4) Žádá-li o schválení projektu bezpečnosti komunikačního systému zpravodajská služba, uvede v žádosti podle odstavce 2 a v podkladech podle odstavce 3 pouze nezbytné údaje, které umožní Úřadu schválení projektu bezpečnosti komunikačního systému.

§ 29

**Způsob a podmínky schvalování projektu bezpečnosti komunikačního systému**

(1) V rámci schvalování projektu bezpečnosti komunikačního systému se posuzuje vhodnost souhrnu zásad a požadavků v oblasti personální, administrativní, fyzické a komunikační bezpečnosti podle § 27 odst. 3 a organizačních opatření a provozních postupů provozování komunikačního systému podle § 27 odst. 4, navržených pro dosažení bezpečnosti komunikačního systému, a správnost a úplnost provozních směrnic podle § 27 odst. 5.

(2) Schvalování projektu bezpečnosti komunikačního systému se provádí posouzením podkladů předložených žadatelem a provedením kontroly realizace projektu bezpečnosti komunikačního systému Úřadem v provozním prostředí schvalovaného komunikačního systému.

(3) Schvalování projektu bezpečnosti komunikačního systému lze provádět průběžně po ukončení jednotlivých fází výstavby komunikačního systému nebo až po jeho celkovém dokončení, podle požadavků žadatele.

(4) Jestliže se při schvalování projektu bezpečnosti komunikačního systému zjistí způsobilost hodnoceného komunikačního systému pro nakládání s utajovanými informacemi, bude žadateli písemně zasláno schválení projektu bezpečnosti komunikačního systému.

(5) Dojde-li v komunikačním systému k závažným změnám, které mají vliv na celkovou bezpečnost tohoto komunikačního systému, provádí se doplňující hodnocení komunikačního systému v rozsahu potřebném k posouzení provedených změn. V případě provádění doplňujícího hodnocení komunikačního systému se postupuje obdobně jako při schvalování projektu bezpečnosti komunikačního systému.

# ČÁST ČTVRTÁ

# KOMPROMITUJÍCÍ VYZAŘOVÁNÍ

## HLAVA I

## ELEKTRICKÁ A ELEKTRONICKÁ ZAŘÍZENÍ, ZABEZPEČENÁ OBLAST NEBO OBJEKT

§ 29a

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

§ 30

**Žádost o ověření způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu**

(1) Žádost o ověření způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem informací kompromitujícím vyzařováním obsahuje

a) identifikaci žadatele podle § 24 odst. 1 písm. a),

b) jméno a příjmení kontaktního pracovníka a kontaktní spojení,

c) identifikaci elektrického nebo elektronického zařízení, zabezpečené oblasti nebo objektu, jehož způsobilost má být ověřena, a

d) stupeň utajení utajovaných informací, které budou v elektrickém nebo elektronickém zařízení, zabezpečené oblasti nebo objektu zpracovávány.

(2) K žádosti může být přiložena zpráva o výsledku hodnocení způsobilosti elektrického nebo elektronického zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajované informace kompromitujícím vyzařováním, provedeného orgánem státu nebo podnikatelem na základě smlouvy o zajištění činnosti uzavřené s Úřadem.

(3) Podmínky hodnocení a používání elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu k ochraně utajovaných informací před únikem utajované informace kompromitujícím vyzařováním stanoví Úřad v bezpečnostních standardech.

§ 31

**Způsob hodnocení způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu**

(1) Hodnocení způsobilosti elektrických a elektronických zařízení z hlediska úniku utajované informace kompromitujícím vyzařováním se provádí měřením úrovní vyzařovaného elektromagnetického pole a porovnáním naměřených hodnot s bezpečnostními standardy.

(2) Hodnocení způsobilosti zabezpečené oblasti nebo objektu k ochraně před únikem utajované informace kompromitujícím vyzařováním se provádí měřením jeho útlumových vlastností a porovnáním naměřených hodnot s bezpečnostními standardy.

(3) Jsou-li v průběhu hodnocení způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu zjištěny nedostatky, vyzve Úřad žadatele k jejich odstranění.

(4) O průběhu a výsledcích hodnocení způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajované informace kompromitujícím vyzařováním vypracuje Úřad zprávu a výsledek písemně oznámí žadateli.

## HLAVA II

## STÍNICÍ KOMORA

### § 32

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

(2) K ochraně utajovaných informací před jejich únikem kompromitujícím elektromagnetickým vyzařováním se používá stínicí komora certifikovaná Úřadem. Podmínky hodnocení stínicí komory k ochraně utajovaných informací stanoví Úřad v bezpečnostních standardech.

**Certifikace stínicí komory**

### § 33

**Žádost o certifikaci stínicí komory**

(1) Žádost o certifikaci stínicí komory obsahuje

a) identifikaci žadatele podle § 24 odst. 1 písm. a),

b) jméno a příjmení kontaktního pracovníka žadatele a kontaktní spojení,

c) stupeň a číslo osvědčení podnikatele nebo kopii platného prohlášení podnikatele, je-li žadatelem podnikatel,

d) označení a umístění stínicí komory a

e) identifikaci výrobce stínicí komory, podle § 24 odst. 1 písm. a) bodu 1 nebo 2.

(2) K žádosti může být přiložena zpráva o výsledku hodnocení stínicí komory, provedeného orgánem státu nebo podnikatelem na základě smlouvy o zajištění činnosti uzavřené s Úřadem. Ke dni podání žádosti o certifikaci stínicí komory nesmí být její výsledek hodnocení uvedený v přiložené zprávě starší 6 měsíců.

### § 34

**Způsob a podmínky provádění certifikace stínicí komory**

(1) Certifikace stínicí komory se provádí měřením útlumových vlastností stínicí komory a jejich porovnáním s bezpečnostními standardy. Měření stínicí komory se provádí za spoluúčasti žadatele a v případě potřeby i dodavatele stínicí komory.

(2) O průběhu a dílčích výsledcích certifikace stínicí komory vypracuje Úřad zprávu.

(3) Vzor certifikátu stínicí komory je uveden v příloze č. 2 této vyhlášky.

§ 35

**Certifikační zpráva stínicí komory**

Certifikační zpráva stínicí komory obsahuje

a) orientační popis stínicí komory, jejího umístění a účelu jejího používání,

b) podmínky provozu stínicí komory a

c) typy změn, které vyžadují provedení opakované certifikace stínicí komory.

§ 36

**Žádost o opakovanou certifikaci stínicí komory a způsob jejího provedení**

(1) Žádost o opakovanou certifikaci stínicí komory obsahuje

a) identifikaci žadatele podle § 24 odst. 1 písm. a),

b) úplnou identifikaci vydaného certifikátu stínicí komory obsahující jeho držitele, evidenční číslo, datum vydání a dobu platnosti,

c) identifikaci certifikované stínicí komory obsahující její název, typové označení, variantní provedení a umístění a

d) jméno a příjmení kontaktního pracovníka žadatele a kontaktní spojení.

(2) K žádosti může být přiložena zpráva o výsledku hodnocení stínicí komory, provedeného orgánem státu nebo podnikatelem na základě smlouvy o zajištění činnosti uzavřené s Úřadem, podle § 33 odst. 2.

(3) Pokud žadatel doloží, že ke dni ukončení platnosti dosavadního certifikátu stínicí komory nedochází ke změnám podmínek podmiňujících platnost vydaného certifikátu, Úřad vydá certifikát.

(4) Pokud ke dni ukončení platnosti certifikátu stínicí komory žadatel nemůže doložit skutečnosti uvedené v odstavci 3, Úřad provede doplňující hodnocení stínicí komory, a pokud ověří způsobilost stínicí komory k ochraně utajovaných informací, vydá certifikát. V případě podstatných změn podmínek provozu stínicí komory se postupuje jako při nové certifikaci.

## ČÁST PÁTÁ

## NÁLEŽITOSTI ŽÁDOSTI ORGÁNU STÁTU NEBO PODNIKATELE O UZAVŘENÍ SMLOUVY O ZAJIŠTĚNÍ ČINNOSTI

§ 37

Žádost o uzavření smlouvy o zajištění činnosti obsahuje

a) identifikaci žadatele podle § 24 odst. 1 písm. a),

b) stupeň a číslo osvědčení podnikatele nebo kopii platného prohlášení podnikatele, je-li žadatelem podnikatel,

c) jméno a příjmení kontaktního pracovníka žadatele a kontaktní spojení,

d) identifikaci příslušného odborného pracoviště žadatele (předmět činnosti a podrobná specifikace umístění pověřovaného pracoviště, jméno a příjmení kontaktního pracovníka a kontaktní spojení),

e) specifikace činností, které mají být prováděny podle smlouvy,

f) personální předpoklady pracoviště k provádění požadovaných činností (jméno, příjmení a kvalifikace vedoucího pracovníka odborného pracoviště, jména a příjmení ostatních odborných pracovníků pracoviště a jejich kvalifikace),

g) prohlášení odpovědné osoby o úrovni fyzické, personální a administrativní bezpečnosti, která je zajištěna pro odborné pracoviště,

h) stupeň a evidenční číslo certifikátu informačního systému, pokud je použití certifikovaného informačního systému potřebné pro provádění činností podle smlouvy, a

i) vybavenost odborného pracoviště technickým zařízením potřebným pro provádění činností podle smlouvy.

## ČÁST ŠESTÁ

## PODMÍNKY BEZPEČNÉHO PROVOZOVÁNÍ KOPÍROVACÍHO ZAŘÍZENÍ, ZOBRAZOVACÍHO ZAŘÍZENÍ NEBO PSACÍHO STROJE S PAMĚTÍ

§ 38

(1) Bezpečného 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, se v závislosti na stupni utajení utajovaných informací dosahuje uplatněním souboru opatření z oblasti

a) personální bezpečnosti,

b) fyzické bezpečnosti,

c) administrativní bezpečnosti a organizačních opatření a

d) ochrany utajované informace před jejím únikem kompromitujícím vyzařováním.

(2) Zařízení podle odstavce 1, která se používají pro zpracování utajovaných informací stupně utajení Důvěrné nebo vyššího, musí být zabezpečena proti úniku utajované informace

kompromitujícím vyzařováním. Při ověřování způsobilosti kopírovacího zařízení, zobrazovacího zařízení nebo psacího stroje s pamětí k ochraně utajované informace před jejím únikem kompromitujícím vyzařováním se postupuje podle § 31.

(3) Zařízení podle odstavce 1 musí být umístěna do prostoru, ve kterém je zajištěna jejich fyzická ochrana před neoprávněným přístupem, poškozením a ovlivněním. Tento prostor je vymezen definovanými prvky ochrany s vhodnými kontrolami vstupu a bezpečnostními bariérami. Podle charakteru zařízení se na základě analýzy rizik stanovuje, zda musí být umístěno v zabezpečené oblasti nebo v objektu, a požadovaná kategorie zabezpečené oblasti. Analýza rizik stanoví pro zranitelná místa zařízení pravděpodobnost realizace možných hrozeb a odhad jejich následků.

(4) Zařízení podle odstavce 1 musí být fyzicky chráněna před bezpečnostními hrozbami a riziky prostředí.

(5) Umístění zařízení podle odstavce 1 musí být provedeno tak, aby zamezovalo nepovolané osobě odezírat utajované informace.

(6) Se zařízením podle odstavce 1 obsahujícím zabudované nosiče utajovaných informací nebo jiné komponenty umožňující uchování utajovaných informací a s psacím strojem s pamětí musí být spojena informace o stupni utajení informací uchovávaných na těchto nosičích, komponentách a pamětech. Tato informace může být vyjádřena na štítku připevněném k zařízení, stanovena v bezpečnostní provozní směrnici nebo být vyjádřena jiným vhodným způsobem. Nosiče utajovaných informací zabudované do zařízení a jiné komponenty umožňující uchování utajovaných informací musí být evidovány a označeny stupněm utajení nejpozději po jejich vyjmutí z daného zařízení.

(7) Servisní činnost pro zařízení podle odstavce 1 se musí organizovat tak, aby nebyla ohrožena bezpečnost utajovaných informací. Z nosičů utajovaných informací a komponent přístupných při servisní činnosti musí být vymazány utajované informace podle § 15, jinak nesmí být předmětem servisní činnosti.

## ČÁST SEDMÁ

## ÚČINNOST

§ 39

Tato vyhláška nabývá účinnosti dnem 1. ledna 2006.

Ředitel:

**Mgr. Mareš v. r.**

1) § 34 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

2) § 35 zákona č. 412/2005 Sb.

3) Například ČSN ISO/IEC 15408 Kritéria pro hodnocení bezpečnosti IT.

4) Vyhláška č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací.

5) Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.

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