453

VYHLÁŠKA

ze dne 21. prosince 2011,

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 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) 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.“.

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 zajištění pravosti informací a nepopiratelnost.“.

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 nejméně 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 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. 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 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.“.

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 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.

[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 x 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.