ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2002

Vyhlásené: 28. 02. 2002 Vyhlásená verzia v Zbierke zákonov Slovenskej republiky

Obsah tohto dokumentu má informatívny charakter.

91

VYHLÁŠKA
Národného bezpečnostného úradu
z 30. januára 2002,
ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií

Národný bezpečnostný úrad (ďalej len „úrad“) podľa § 65 zákona č. 241/2001 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) ustanovuje:

§ 1
Predmet úpravy

Táto vyhláška upravuje podrobnosti o

a) certifikácii a schvaľovaní systémov a prostriedkov šifrovej ochrany informácií (ďalej len „prostriedok“) do prevádzky, o ich použití, nasadení, preprave, evidencii a o používaní šifrových materiálov,

b) vedení evidencií zamestnancov na úseku šifrovej ochrany informácií a o overovaní ich odbornej spôsobilosti,

c) zriaďovaní rezortného šifrového orgánu alebo jemu na roveň postaveného šifrového orgánu (ďalej len „rezortný šifrový orgán“).

§ 2
Certifikácia a schvaľovanie prostriedkov do prevádzky

(1) Hodnotiace požiadavky na certifikáciu prostriedkov, kryptografické metódy a algoritmy použité v prostriedkoch ustanovuje úrad v zásadách šifrovej ochrany informácií.

(2) Úrad alebo rezortný šifrový orgán vydáva certifikát prostriedku spolu s návodom na obsluhu a pravidlami na používanie prostriedku.

(3) Rezortný šifrový orgán vedie evidenciu certifikátov prostriedkov vydaných vo svojej pôsobnosti. O vydaných certifikátoch informuje úrad.

(4) Úrad vedie evidenciu certifikátov prostriedkov vydaných vo svojej pôsobnosti a v pôsobnosti rezortných šifrových orgánov.

(5) Na požiadanie rezortného šifrového orgánu úrad informuje o certifikátoch vydaných v jeho pôsobnosti.

(6) Schvaľovať do prevádzky možno iba certifikované prostriedky.

§ 3
Postup a spôsob certifikácie prostriedkov

(1) Certifikácia prostriedku sa vykonáva na základe písomnej žiadosti.

(2) Žiadosť obsahuje

a) názov, identifikačné číslo organizácie, adresu žiadateľa,

b) vydané certifikáty iných autorizovaných osôb[1]) spolu s výsledkami meracích protokolov a zoznamom noriem, ktorým prostriedok vyhovel,

c) protokol o vykonaných prevádzkových skúškach prostriedku s uvedením dosiahnutých prevádzkových parametrov,

d) dokumentáciu prostriedku v štátnom jazyku[2]) v písomnej alebo elektronickej forme na bežných nosičoch elektronického spracovania.

(3) Pri inštalácií v podmienkach certifikačného pracoviska alebo úvodného zoznámenia sa s prostriedkom žiadateľ dodá potrebný počet kusov prostriedku podľa rozhodnutia certifikačného pracoviska.

(4) Úrad certifikuje prostriedky, o ktorých certifikáciu ho požiadal rezortný šifrový orgán alebo právnická osoba, ktorá spĺňa podmienky priemyselnej bezpečnosti podľa osobitného predpisu.[3])

(5) Rezortný šifrový orgán certifikuje prostriedky, o ktorých certifikáciu ho požiadala právnická osoba, ktorá spĺňa podmienky priemyselnej bezpečnosti podľa osobitného predpisu.[3])

(6) Dokumentácia prostriedku obsahuje tieto údaje podľa stupňa utajenia chránených utajovaných skutočností:

a) pre stupeň utajenia Vyhradené

1. určenie a vymedzenie spôsobu použitia prostriedkov,
2. typ užívateľského prostredia a systémové začlenenie prostriedku,
3. návod na obsluhu prostriedku,
4. pravidlá na používanie prostriedku,
5. základné kryptografické parametre, typ kryptografického algoritmu, matematický model všetkých použitých kryptografických metód v hodnotenom prostriedku,
6. verifikačné dáta a programy na overenie matematického modelu algoritmu prostriedku,
7. verifikačné dáta a programy na overenie a testovanie funkcie prostriedku,
8. popis kľúčového hospodárstva, veľkosť a štruktúru kľúčov prostriedku,
9. spôsob generovania šifrovacích kľúčov prostriedku,
10. blokovú schému a popis prostriedku s vyznačením súčinnostných väzieb jednotlivých častí,
11. blokovú schému a popis častí prostriedku,
12. kryptografický rozbor prostriedku,
13. bezpečnostný rozbor prostriedku,
14. dokumentáciu a výsledky vykonávaných bezpečnostných analýz prostriedku,
15. posúdenie možnosti zmeny kryptografického algoritmu z hľadiska modifikácie prostriedku a licenčnej politiky,
16. postup inštalácie prostriedku,

17. spôsob ochrany prostriedku proti kompromitácii utajovaných skutočností,
18. detekciu kryptografických chýb,

b) pre stupeň utajenia Dôverné údaje uvedené v písmene a) a

1. spôsob fyzickej realizácie prostriedku,
2. technickú dokumentáciu prostriedku a popis funkčných a technických parametrov,
3. spôsob spravovania kľúčového hospodárstva prostriedku,
4. spôsob generovania počiatočných nastavení prostriedku,
5. diagnostický systém prostriedku,
6. popis použitých metód autentizácie a identifikácie prostriedku,
7. postup deinštalácie prostriedku,

c) pre stupeň utajenia Tajné údaje uvedené v písmenách a) a b) a

1. spôsob fyzickej realizácie algoritmu, všetkých jeho používaných režimov činnosti vrátane kontrolných príkladov,
2. časový diagram hlavných funkčných stavov a čiastkových blokov a popis základných funkčných režimov prostriedku,
3. schému zapojenia prostriedku vrátane technického popisu, definičného obsahu programovateľných obvodov, mikroprogramov, pamätí a podobne,
4. komentované zdrojové texty celého programového vybavenia,
5. zdrojový text programového vybavenia prostriedku umožňujúci preklad do tvaru zhodného s certifikovaným prostriedkom a jeho kontrolu,
6. bezpečnostné vlastnosti a technické parametre nosiča kľúčov,
7. spôsob distribúcie kľúčov,
8. spôsob ochrany kľúčov a kryptografického algoritmu pred kompromitáciou,
9. spôsob likvidácie kryptografických stôp po deinštalácii,
10. popis použitých metód, vlastností a bezpečnostných úrovní auditných funkcií,
11. pravidlá na návrh topológie sietí prostriedkov,
12. odolnosť prostriedku proti modifikácii kryptografických častí,
13. odolnosť a spôsob ochrany programových častí prostriedku proti napadnutiu vírusom a inými škodlivými programami alebo proti ich čiastočnej modifikácii,
14. diagnostiku, priebeh a spôsoby testovania a inicializácie kryptografických častí pri certifikácii prostriedku,
15. diagnostiku, priebeh a spôsoby testovania a inicializácie kryptografických častí pri sériovej výrobe prostriedku,
16. spôsob ochrany prostriedku proti kompromitácii utajovaných skutočností parazitným elektromagnetickým vyžarovaním,
17. bezpečnostné opatrenia pri sériovej výrobe prostriedku,
18. spôsob vykonávania servisnej činnosti prostriedku u používateľa,

d) pre stupeň utajenia Prísne tajné údaje uvedené v písmenách a) až c) a

1. reakciu prostriedku na vonkajšie podnety rušenia,
2. reakcie prostriedku na náhodné, prípadne úmyselné zmeny pracovného prostredia,

3. reakcie prostriedku na výskyt vlastnej chyby,
4. odolnosť prostriedku proti chybe obsluhy,
5. bezpečnostné opatrenia pri výrobe šifrovacích kľúčov,
6. spôsob likvidácie chybných dielcov a komponentov pri sériovej výrobe a servise prostriedku,
7. spôsob likvidácie použitých, prípadne chybných nosičov kryptografických prvkov.

§ 4
Používanie, nasadenie a preprava prostriedkov

(1) Prostriedky možno používať a nasadzovať iba v súlade s návodom na obsluhu a pravidlami na ich používanie.

(2) Prostriedok použitý na ochranu informácií s rôznym stupňom utajenia musí byť certifikovaný na najvyšší stupeň utajenia chránených informácií.

(3) Za prenos utajovaných skutočností technickými prostriedkami[4]) sa nepovažuje prenos vnútri chráneného priestoru.[5])

(4) Používať a nasadzovať prostriedky v zahraničí s výnimkou zastupiteľského úradu Slovenskej republiky možno len na základe medzinárodnej zmluvy o vzájomnej ochrane utajovaných skutočností[6]) a v súlade s ňou.

(5) Prepravu prostriedkov uskutočňuje kuriér podľa osobitného predpisu.[7])

§ 5
Evidencia prostriedkov

(1) Rezortný šifrový orgán vedie evidenciu všetkých prostriedkov vo svojej správe.

(2) Evidencia prostriedkov sa vedie samostatne, oddelene od ostatných materiálových evidencií.

(3) Rezortný šifrový orgán raz ročne vykoná fyzickú inventarizáciu prostriedkov. O výsledku inventarizácie informuje úrad.

§ 6
Používanie šifrových materiálov

(1) Šifrové materiály ako súčasť prostriedku[8]) sú heslá, kľúče, premenné parametre kryptografických algoritmov označené podľa druhu prostriedku a stupňa ochrany utajovaných skutočností. Šifrové materiály možno používať len v súlade s pravidlami na používanie prostriedku.

(2) Šifrové materiály, ktoré sa použili, ktoré sú poškodené, podozrivé z neoprávnenej manipulácie a ktorým skončila platnosť je zakázané používať na šifrovú ochranu ďalších utajovaných informácií.

§ 7
Overovanie odbornej spôsobilosti zamestnanca na úseku šifrovej ochrany informácií

(1) Zamestnanec na úseku šifrovej ochrany informácií preukazuje odbornú spôsobilosť znalosťou právnych predpisov o ochrane utajovaných skutočností a v prípade práce s prostriedkom aj znalosťou návodu na jeho obsluhu, pravidiel na jeho používanie a praktickej obsluhy prostriedku.

(2) Odbornú spôsobilosť zamestnancov na úseku šifrovej ochrany informácií na stupeň utajenia Vyhradené, Dôverné a Tajné overuje rezortný šifrový orgán.

(3) Odbornú spôsobilosť zamestnancov na úseku šifrovej ochrany informácií na stupeň utajenia Prísne tajné overuje úrad alebo zamestnanci na úseku šifrovej ochrany informácii rezortného šifrového orgánu poverení úradom.

(4) Na základe overenia odbornej spôsobilosti zamestnanca na úseku šifrovej ochrany informácií podľa odsekov 2 a 3 vydáva vedúci ústredného orgánu štátnej správy (ďalej len „vedúci“) osvedčenie na prácu na určenom úseku šifrovej ochrany informácií podľa prílohy.

(5) Rezortný šifrový orgán vedie evidenciu vydaných osvedčení na prácu na určenom úseku šifrovej ochrany informácií.

§ 8
Vedenie evidencie zamestnancov na úseku šifrovej ochrany informácií

(1) Rezortný šifrový orgán vedie evidenciu zamestnancov na úseku šifrovej ochrany informácií vo svojej pôsobnosti. Úrad vedie evidenciu zamestnancov na úseku šifrovej ochrany informácií rezortných šifrových orgánov.

(2) O zmenách v evidencii zamestnancov na úseku šifrovej ochrany informácií rezortného šifrového orgánu informujú rezortné šifrové orgány úrad.

(3) Evidencia zamestnancov na úseku šifrovej ochrany informácií[9]) obsahuje tieto údaje:

a) meno a priezvisko (rodné priezvisko),

b) dátum a miesto narodenia,

c) rodné číslo,

d) osobné evidenčné číslo,

e) názov a adresu zamestnávateľa,

f) vykonávanú funkciu,

g) stupeň bezpečnostnej previerky, dátum a číslo vyjadrenia orgánu vykonávajúceho bezpečnostnú previerku navrhovanej osoby,

h) dátum podpisu záznamu o určení navrhovanej osoby oboznamovať sa s utajovanými skutočnosťami,

i) dátum podpisu vyhlásenia o mlčanlivosti,

j) evidenčné číslo a dátum vydania osvedčenia na prácu na určenom úseku šifrovej ochrany informácií,

k) dátum zaradenia do evidencie,

l) dátum odňatia osvedčenia na prácu na určenom úseku šifrovej ochrany informácií.

§ 9
Zriaďovanie rezortného šifrového orgánu

(1) Žiadosť vedúceho o súhlas ústredného šifrového orgánu na zriadenie rezortného šifrového orgánu má obsahovať

a) názov ústredného orgánu štátnej správy,

b) odôvodnenie zriadenia,

c) navrhovaný termín zriadenia,

d) začlenenie rezortného šifrového orgánu v organizačnej štruktúre ústredného orgánu štátnej správy.

(2) Zamestnancom na úseku šifrovej ochrany informácií rezortného šifrového orgánu môže byť iba osoba oprávnená oboznamovať sa s utajovanými skutočnosťami. Najmenej jeden zamestnanec na úseku šifrovej ochrany informácií rezortného šifrového orgánu musí byť oprávnenou osobou oboznamovať sa s utajovanými skutočnosťami stupňa utajenia Prísne tajné.

(3) Utajované písomnosti na úseku šifrovej ochrany informácií sa evidujú v samostatných protokoloch písomností. Na evidenciu a manipuláciu s utajovanými písomnosťami na úseku šifrovej ochrany informácií sa vzťahuje osobitný predpis.[10])

§ 10
Zrušenie rezortného šifrového orgánu

(1) Vedúci zruší rezortný šifrový orgán, ak

a) pominula potreba šifrovej ochrany informácií v ústrednom orgáne štátnej správy,

b) došlo k zániku alebo zrušeniu ústredného orgánu štátnej správy,

c) došlo k zlúčeniu ústredného orgánu štátnej správy s ústredným orgánom štátnej správy, ktorý má zriadený rezortný šifrový orgán.

(2) Zrušenie rezortného šifrového orgánu s uvedením dôvodu a dátumu zrušenia vedúci vopred oznámi úradu.

(3) Na zrušenie rezortného šifrového orgánu vedúci určí komisiu, ktorá preverí úplnosť prostriedkov a utajovaných skutočností rezortného šifrového orgánu a navrhne vedúcemu spôsob materiálového vysporiadania prostriedkov[11]) a odovzdania utajovaných skutočností podľa osobitného predpisu.[12])

§ 11
Účinnosť

Táto vyhláška nadobúda účinnosť 1. marca 2002.

Ján Mojžiš v. r.

Príloha
k vyhláške č. 91/2002 Z. z.

Príloha
k vyhláške č. 91/2002 Z. z.

_____
(Názov ústredného orgánu štátnej správy)

Evidenčné číslo:

O S V E D Č E N I E

NA PRÁCU NA URČENOM ÚSEKU ŠIFROVEJ OCHRANY INFORMÁCIÍ

Na základe overenia odbornej spôsobilosti vykonaného dňa: .....

protokol č. p.: .....

v y d á v a m

podľa § 64 ods. 2 zákona č. 241/2001 Z. z. o ochrane utajovaných skutočností
a o zmene a doplnení niektorých zákonov

.....
(meno, priezvisko, miesto narodenia, rodné číslo)

osvedčenie

.....
(Uviesť konkrétne určený úsek šifrovej ochrany informácií, napríklad na riadenie šifrového orgánu, na obsluhu prostriedku.)

Dátum vydania:

Vedúci ústredného orgánu štátnej správy
(podpis a odtlačok pečiatky)

1) Zákon č. 264/1999 Z. z. o technických požiadavkách na výrobky a o posudzovaní zhody a o zmene a doplnení niektorých zákonov v znení zákona č. 436/2001 Z. z.§ 7 zákona Národnej rady Slovenskej republiky č. 330/1996 Z. z. o bezpečnosti a ochrane zdravia pri práci v znení neskorších predpisov.

2) Zákon Národnej rady Slovenskej republiky č. 270/1995 Z. z. o štátnom jazyku Slovenskej republiky v znení neskorších predpisov.

3) Vyhláška Národného bezpečnostného úradu č. 28/2002 Z. z. o priemyselnej bezpečnosti.

4) § 6 ods. 3 zákona č. 241/2001 Z. z.

5) § 2 písm. b) vyhlášky Národného bezpečnostného úradu č. 88/2002 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti.

6) Napríklad Dohoda medzi vládou Slovenskej republiky a vládou Spolkovej republiky Nemecko o vzájomnej ochrane utajovaných skutočností (oznámenie č. 289/1998 Z. z.), Dohoda medzi vládou Slovenskej republiky a vládou Ukrajiny o vzájomnej ochrane utajovaných skutočností (oznámenie č. 374/1998 Z. z.), Dohoda medzi vládou Slovenskej republiky a vládou Českej republiky o vzájomnej ochrane utajovaných skutočností (oznámenie č. 72/2001 Z. z.).

7) § 17 a 20 vyhlášky Národného bezpečnostného úradu č. 455/2001 Z. z. o administratívnej bezpečnosti.

8) § 2 písm. p) zákona č. 241/2001 Z. z.

9) § 40 písm. c) zákona č. 52/1998 Z. z. o ochrane osobných údajov v informačných systémoch v znení neskorších predpisov.

10) Vyhláška Národného bezpečnostného úradu č. 455/2001 Z. z.

11) Zákon č. 278/1993 Z. z. o správe majetku štátu v znení neskorších predpisov.

12) § 22 vyhlášky Národného bezpečnostného úradu č. 455/2001 Z. z.

Vydavateľ Zbierky zákonov Slovenskej republiky, správca obsahu a prevádzkovateľ právneho a informačného portálu Slov-Lex dostupného na webovom sídle www.slov-lex.sk je
Úrad vlády Slovenskej republiky, Námestie slobody 1, 813 70 Bratislava,
tel.: 02 888 91 131, e-mail: helpdesk@slov-lex.sk.