ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2002

Vyhlásené: 28. 02. 2002 Časová verzia predpisu účinná od: 1. 03. 2002 do: 30. 04. 2004

90

VYHLÁŠKA
Národného bezpečnostného úradu
z 30. januára 2002
o bezpečnosti technických prostriedkov

Národný bezpečnostný úrad (ďalej len „úrad“) podľa § 6 ods. 9, § 51 ods. 6 a § 52 ods. 7 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 bezpečnosti technických prostriedkov, o schvaľovaní technických prostriedkov do prevádzky, ich použití a podrobnosti o požiadavkách kladených na technické prostriedky, na ktorých sa spracúvajú utajované skutočnosti a podrobnosti o postupe pri certifikácii technických prostriedkov.

§ 2
Schvaľovanie technických prostriedkov do prevádzky

(1) Pri schvaľovaní technického prostriedku do prevádzky vedúci[1]) zisťuje, či

a) je technický prostriedok certifikovaný,[2])

b) sú prevádzkové podmienky technických prostriedkov v súlade so schváleným bezpečnostným projektom a podmienkami práce certifikovaného prostriedku,

c) je vypracovaná a schválená smernica o používaní technického prostriedku podľa § 3.

(2) Vedúci zabezpečí spracovanie protokolu o schválení technického prostriedku do prevádzky, v ktorom určí obdobie povolenej prevádzky, podmienky a spôsob použitia tohto technického prostriedku.

§ 3
Smernica o používaní technického prostriedku

(1) Na konkretizáciu úloh a opatrení pre jednotlivých používateľov technických a systémových prostriedkov vyplývajúcich z bezpečnostného projektu[3]) vydávajú štátny orgán, obec alebo iná právnická osoba smernicu o používaní technického prostriedku.

(2) Smernica o používaní technického prostriedku obsahuje

a) zoznam technických a systémových prostriedkov určených bezpečnostným projektom na prácu s utajovanými skutočnosťami s uvedením názvu a typu technického prostriedku, identifikátora

technického prostriedku, stupňa utajenia, pre ktorý možno technický prostriedok používať, a umiestnenie technického prostriedku,

b) zoznam osôb oprávnených používať technické a systémové prostriedky zostavený tak, aby bolo jednoznačne zrejmé, ktorá osoba bude na ktorom technickom prostriedku alebo na ktorých technických prostriedkoch pracovať, rozsah oprávnení, spôsob identifikácie a autentizácie konkrétnej osoby podľa § 5 pre každý priradený technický prostriedok, rozsah a spôsob používania systémových prostriedkov, služieb a aplikačného programového vybavenia,

c) určenie osoby poverenej vykonávaním správy bezpečnostných funkcií (ďalej len „bezpečnostný správca“),

d) určenie osoby poverenej výkonom kontroly dodržiavania bezpečnostných zásad (ďalej len „správca informačného systému“),

e) spôsob kontroly a najdlhšie časové limity medzi jednotlivými kontrolami,

f) spôsob zabezpečenia ochrany utajovaných skutočností pri haváriách a poruchách technického prostriedku,

g) ďalšie oprávnenia a opatrenia.

§ 4
Certifikát technického prostriedku

(1) Žiadosť o vykonanie certifikácie technického prostriedku (ďalej len „žiadosť“) predkladá úradu písomne vedúci štátneho orgánu, obec alebo iná právnická osoba (ďalej len „žiadateľ“).

(2) Žiadosť obsahuje

a) názov, identifikačné číslo organizácie, adresu žiadateľa,

b) stupeň utajenia, pre ktorý sa má certifikát technického prostriedku udeliť,

c) iné údaje a skutočnosti na bezpečnostné posúdenie technického prostriedku.

(3) K žiadosti sa prikladá

a) bezpečnostný projekt technického prostriedku, ktorého certifikácia sa požaduje,

b) technický prostriedok, ktorého certifikácia sa vyžaduje,

c) technická dokumentácia a prevádzková dokumentácia technického prostriedku,

d) zoznam noriem a štandardov, ktorým certifikovaný technický prostriedok vyhovuje, najvyšší bezpečnostný stupeň, ak bol takýto bezpečnostný stupeň technickému prostriedku pridelený,

e) kópia bezpečnostného certifikátu, ak bol pre technický prostriedok už skôr vydaný,

f) identifikačné údaje výrobcu a dodávateľa,

g) popis prevádzkového prostredia a režimov, v ktorých bude technický prostriedok prevádzkovaný.

(4) Ak žiadosť o vydanie certifikátu nespĺňa náležitosti podľa odsekov 2 a 3, úrad certifikát technického prostriedku nevydá a zaslanú žiadosť spolu s prílohami žiadateľovi vráti.

(5) Po splnení požiadaviek úrad vykoná posúdenie a zhodnotenie predmetného technického prostriedku a po kladnom posúdení schváli jeho spôsobilosť a vydá žiadateľovi certifikát.[4])

(6) Úrad vedie evidenciu vydaných certifikátov technických prostriedkov.

§ 5
Používanie technických prostriedkov

(1) Rozsah úkonov, ktoré môže oprávnená osoba vykonávať, určuje bezpečnostný správca. Rozsah úkonov je zakódovaný prostredníctvom identifikátora používateľa v priamej väzbe na technický prostriedok.

(2) Pre technický prostriedok, ktorým sa spracúvajú utajované skutočnosti stupňa utajenia Vyhradené, je identifikátorom používateľa

a) znalosť informácie dostupnej iba používateľovi,

b) pridelený predmet, ktorého obsah jednoznačne identifikuje používateľa,

c) kombinácia identifikátorov podľa písmen a) a b).

(3) Pre technický prostriedok, na ktorom sa spracúvajú utajované skutočnosti stupňov utajenia Dôverné, Tajné a Prísne tajné, je identifikátorom používateľa

a) znalosť informácie dostupnej iba používateľovi, ktorou sa technickému prostriedku identifikuje (identifikácia používateľa), a súčasne pridelený predmet, prostredníctvom ktorého túto identitu potvrdzuje (autentizácia používateľa),

b) pridelený predmet, ktorým sa technickému prostriedku identifikuje, a súčasné využitie technického prostriedku alebo jeho časti na nasnímanie niektorej z osobných charakteristických vlastností používateľa, ktorá jeho identitu jednoznačne potvrdzuje,

c) iná kombinácia spôsobov identifikácie a autentizácie podľa písmen a) a b), pričom identifikáciu a autentizáciu používateľa nemožno oddeľovať.

(4) Identifikátor používateľa môže obsahovať informácie určujúce rozsah oprávnení v rámci technického prostriedku.

(5) Používateľ je povinný zabezpečiť, aby nedošlo k strate, vyzradeniu alebo zneužitiu jeho identifikátora.

(6) Každý technický prostriedok, ktorým sa spracúvajú utajované skutočnosti, obsahuje kontrolný mechanizmus a blokovací mechanizmus, ktorý zabraňuje používateľovi pracovať s technickým prostriedkom v prípade, že jeho identifikátor ho na túto prácu neoprávňuje.

(7) Utajovaná skutočnosť, ktorá je výstupom z technického prostriedku, musí byť označená príslušným stupňom utajenia tak, aby pri akomkoľvek ďalšom použití či manipulácii bolo zaručené dodržanie podmienok ustanovených zákonom pre stupeň utajenia spojený s utajovanou skutočnosťou.

(8) Ustanovenie odseku 7 sa nevzťahuje na utajované dokumenty po zašifrovaní, ktoré sú určené na prenos štandardnými komunikačnými prostriedkami.

(9) Technické prostriedky sú umiestnené v chránených priestoroch, v ktorých je zaistená ich ochrana pred neoprávneným prístupom, poškodením alebo manipuláciou v súlade s bezpečnostným projektom. Spôsob ochrany technických prostriedkov zodpovedá požiadavkám na bezpečnosť technických prostriedkov spracúvajúcich utajované skutočnosti.

(10) Technický prostriedok sa umiestňuje tak, aby sa zamedzilo nepovolaným osobám nazerať na utajované skutočnosti.

(11) Všetky nosiče utajovaných skutočností sa evidujú ako administratívne pomôcky.[5])

§ 6
Požiadavky v oblasti bezpečnosti technických prostriedkov

(1) Kontrolné mechanizmy a blokovacie mechanizmy sa uplatňujú počas celej činnosti technických prostriedkov tak, aby tieto boli chránené pred narušením alebo neautorizovanými zmenami.

(2) Na technických prostriedkoch, ktoré pracujú iba s utajovanými skutočnosťami stupňa utajenia Vyhradené, zodpovedá používateľ za ich činnosť; prístup k utajovaným skutočnostiam sa umožňuje iba v rozsahu pracovnej náplne.

(3) Technické prostriedky, spracúvajúce utajované skutočnosti stupňov utajenia Dôverné, Tajné alebo Prísne tajné, musia zabezpečovať najmenej tieto bezpečnostné funkcie:

a) jednoznačnú identifikáciu a autentizáciu používateľa, ktorá predchádza všetkým ďalším aktivitám používateľa pri spracúvaní utajovaných skutočností na technickom prostriedku,

b) voliteľné riadenie prístupu k objektom na základe rozlišovania a správy prístupových práv používateľa, jeho identity alebo členstva v skupine používateľov,

c) nepretržité vedenie kontrolného záznamu technických prostriedkov o svojej činnosti s možnosťou sledovania, spätného preskúmavania technického prostriedku, ako aj stanovenia zodpovednosti konkrétneho používateľa za ním vykonané činnosti; záznam pravidelne kontroluje bezpečnostný správca,

d) odstránenie utajovaných skutočností z pamäťových prvkov po skončení práce na technickom prostriedku, ktoré nie sú potrebné na ďalšie spracovanie, archiváciu alebo manipuláciu (operačná pamäť, dočasné súbory a pracovné súbory) tak, aby sa znemožnilo zistenie ich predchádzajúceho obsahu alebo aby to bolo veľmi obtiažne aj za použitia špeciálnych laboratórnych prostriedkov a metód; takéto ošetrenie treba vykonať vždy pred pridelením týchto prostriedkov inému subjektu.

(4) Stupeň utajenia nosiča informácií, ktorý bol označený stupňom utajenia Dôverné alebo stupňom utajenia Vyhradené, sa znižuje iba v prípade, ak odstránenie informácií tvoriacich utajované skutočnosti sa vykonalo takým spôsobom, aby spätné získanie informácií nebolo možné, alebo bolo veľmi obtiažne v prípade použitia špeciálnych laboratórnych prostriedkov a metód.

(5) Stupeň utajenia nosiča informácií, ktorý bol označený stupňom utajenia Tajné alebo stupňom utajenia Prísne tajné, sa neznižuje.

(6) Nepoužiteľné nosiče informácií sa ničia fyzicky, a to komisionálnym spôsobom tak, aby žiadnym spôsobom nebolo možné informácie z nosiča spätne získať.

(7) Technické prostriedky, ktoré spracúvajú utajované skutočnosti stupňov utajenia Tajné alebo Prísne tajné, sa zabezpečujú proti nežiaducemu elektromagnetickému vyžarovaniu, ktoré by mohlo spôsobiť vyzradenie utajovaných skutočností. Spôsob zabezpečenia sa určí v súlade s inými prijatými bezpečnostnými opatreniami (najmä s opatreniami objektovej a personálnej bezpečnosti) a v súlade s ustanoveniami § 7 tak, aby ochrana bola dostatočne zabezpečená pre daný stupeň utajenia.

(8) V prípade neprimeraných nákladov na zaistenie niektorej bezpečnostnej funkcie technického prostriedku možno vykonať jej náhradu použitím prostriedku personálnej bezpečnosti, administratívnej bezpečnosti alebo fyzickej bezpečnosti, prípadne ich vhodnej kombinácie za podmienky zachovania úrovne bezpečnostnej funkcie podľa § 7.

(9) Technické prostriedky, ktoré spracúvajú utajované skutočnosti stupňov utajenia Tajné

a Prísne tajné, musia ukladať utajované skutočnosti na externom nosiči informácií (disk, disketa) v šifrovanom tvare.

§ 7
Spôsoby zabezpečenia technických prostriedkov

(1) Technické prostriedky sa zabezpečujú podľa osobitného predpisu[6]) tak, aby toto zabezpečenie zodpovedalo stupňu utajenia, pre ktorý bol technický prostriedok schválený do prevádzky.

(2) V odôvodnených prípadoch sa používa aj technický prostriedok schválený do prevádzky pre nižší stupeň utajenia, ako je stupeň utajovaných skutočností na ňom spracúvaných, ak je ochrana zabezpečená iným vhodným spôsobom, a to v súlade s bezpečnostným štandardom, ktorý vydá úrad.

§ 8
Použitie systémových prostriedkov

Pre prácu s utajovanými skutočnosťami stupňov utajenia Dôverné, Tajné alebo Prísne tajné možno použiť len systémový prostriedok certifikovaný úradom[7]) pre daný stupeň utajenia a za podmienok uvedených v certifikáte technického prostriedku.

§ 9
Certifikát systémového prostriedku

Pri certifikácii systémového prostriedku sa primerane použije § 4.

§ 10
Bezpečnosť informačných systémov

(1) Prevádzkovateľ informačného systému zabezpečuje jeho prevádzku prostredníctvom správcu informačného systému a bezpečnostného správcu a zodpovedá za bezpečnosť jeho prevádzky v súlade s bezpečnostným projektom a smernicou o používaní technického prostriedku.

(2) Úloha bezpečnostného správcu obsahuje výkon správy bezpečnosti informačného systému, ktorý obsahuje najmä prideľovanie prístupových práv, správu autentizačných funkcií a autorizačných funkcií, vyhodnocovanie kontrolných záznamov o činnosti informačného systému, vypracúvanie správ o neoprávnených manipuláciách informačného systému a úlohy vyplývajúce zo smernice o používaní technického prostriedku.

(3) Správca informačného systému vykonáva správu systému a jeho zdrojov.

(4) V informačnom systéme sa úloha bezpečnostného správcu zavádza oddelene od úlohy správcu informačného systému.

(5) V informačných systémoch, spracúvajúcich utajované skutočnosti stupňov utajenia Dôverné, Tajné a Prísne tajné, sa musí zabezpečiť nepretržité vedenie kontrolného záznamu o činnosti informačného systému a jeho zložiek s možnosťou jeho sledovania, spätného preskúmavania, ako aj stanovenia zodpovednosti konkrétneho používateľa za ním vykonané aktivity v informačnom systéme.

§ 11
Účinnosť

Táto vyhláška nadobúda účinnosť 1. marca 2002.

Ján Mojžiš v. r.

1) § 9 ods. 1 zákona č. 241/2001 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

2) § 51 ods. 4 zákona č. 241/2001 Z. z.

3) § 54 zákona č. 241/2001 Z. z.

4) § 52 ods. 5 zákona č. 241/2001 Z. z.

5) Vyhláška Národného bezpečnostného úradu č. 455/2001 Z. z. o administratívnej bezpečnosti.

6) Vyhláška Národného bezpečnostného úradu č. 88/2002 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti.

7) § 53 zákona č. 241/2001 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.