ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2004

Vyhlásené: 01.06.2004 Časová verzia predpisu účinná od: 01.06.2004

339

VYHLÁŠKA
Národného bezpečnostného úradu
z 10. mája 2004
o bezpečnosti technických prostriedkov

Národný bezpečnostný úrad (ďalej len „úrad“) podľa § 6 ods. 10, § 55 ods. 9, § 56 ods. 7 a § 58 ods. 4 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) ustanovuje:

§ 1
Predmet úpravy

Táto vyhláška ustanovuje podrobnosti o bezpečnosti technických prostriedkov, o schvaľovaní technických prostriedkov do prevádzky, o ich použití a podrobnosti o požiadavkách kladených na technické prostriedky, na ktorých sa vytvárajú, spracúvajú, prenášajú, ukladajú a archivujú utajované skutočnosti, podrobnosti o postupe pri certifikácii technických prostriedkov a podrobnosti o spracúvaní bezpečnostného projektu na technické prostriedky a o vydávaní a používaní bezpečnostných štandardov.

§ 2
Bezpečnosť technických prostriedkov

(1) Technické prostriedky sa zabezpečujú podľa osobitných predpisov[1]) tak, aby toto zabezpečenie zodpovedalo stupňu utajenia, pre ktorý je technický prostriedok schválený do prevádzky.

(2) Za bezpečnosť technických prostriedkov podľa odseku 1, ktoré pracujú s utajovanými skutočnosťami, zodpovedá vedúci.[2])

(3) Technické prostriedky určené na vytváranie, spracúvanie, prenos, ukladanie a ochranu utajovaných skutočností stupňa utajenia Vyhradené musia zabezpečovať najmenej jednoznačnú identifikáciu používateľa.

(4) Technické prostriedky určené na vytváranie, spracúvanie, prenos, ukladanie, ochranu a archivovanie utajovaných skutočností stupňov utajenia Prísne tajné, Tajné alebo Dôverné musia zabezpečovať najmenej tieto bezpečnostné funkcie:

a) jednoznačnú identifikáciu a autentizáciu používateľa, ktoré predchádzajú všetkým ďalším aktivitám používateľa pri práci s utajovanými skutočnosťami na technickom prostriedku,

b) voliteľné riadenie prístupu k objektom (súbor, adresár, periférne zariadenie, služba a pod.) 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 osoba poverená vykonávaním správy bezpečnosti informačných systémov (ďalej len „bezpečnostný správca“) v intervaloch uvedených v smernici o používaní technického prostriedku podľa § 4,

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

e) ochranu dát počas prenosu v nechránených sieťach zabezpečiť tak, aby utajovaná skutočnosť v procese prenosu medzi zdrojom a cieľom bola chránená podľa osobitného predpisu.[3])

(5) Technické prostriedky používané štátnym orgánom pri plnení úloh podľa osobitného predpisu,[4]) určené na vytváranie, spracúvanie, prenos, ukladanie, ochranu a archivovanie utajovaných skutočností stupňa utajenia Dôverné musia zaisťovať bezpečnostné funkcie podľa odseku 4 písm. a), b), d) a e).

(6) Stupeň utajenia nosiča utajovaných skutočností, ktorý bol označený stupňom utajenia Dôverné alebo stupňom utajenia Vyhradené, sa môže znížiť iba v prípade, ak sa odstránenie informácií tvoriacich utajované skutočnosti vykonalo takým spôsobom, aby ich spätné získanie nebolo možné alebo by bolo veľmi ťažké aj pri použití špeciálnych laboratórnych prostriedkov a metód.

(7) Stupeň utajenia nosiča utajovaných skutočností, ktorý bol označený stupňom utajenia Prísne tajné alebo stupňom utajenia Tajné, sa neznižuje.

(8) Nepoužiteľné nosiče utajovaných skutočností sa ničia fyzicky alebo špeciálnymi softvérovými a hardvérovými prostriedkami, a to komisionálnym spôsobom tak, aby žiadnym spôsobom nebolo možné informácie z nosiča spätne získať.

(9) Technické prostriedky sa zabezpečujú proti úniku utajovaných skutočností nežiaducim elektromagnetickým vyžarovaním podľa bezpečnostného štandardu na ochranu pred nežiaducim elektromagnetickým vyžarovaním.

(10) V prípade neprimeraných nákladov na zaistenie niektorej bezpečnostnej funkcie technického prostriedku možno vykonať jej náhradu použitím prostriedku alebo opatrenia podľa osobitných predpisov,[1]) prípadne ich vhodnou kombináciou za podmienky zachovania požadovanej úrovne bezpečnosti.

(11) Prenosné technické prostriedky (notebook, laptop), mobilné technické prostriedky a technické prostriedky umiestnené mimo chráneného priestoru majú charakter nosiča informácií. Utajované skutočnosti sa chránia podľa osobitných predpisov,[1]) prípadne ich vhodnou kombináciou za podmienky zachovania požadovanej úrovne bezpečnosti.

(12) Technický prostriedok schválený do prevádzky pre nižší stupeň utajenia, ako je stupeň utajovaných skutočností na ňom spracúvaných, možno vo výnimočných prípadoch používať so súhlasom úradu za podmienky zachovania požadovanej úrovne bezpečnosti pre stupeň utajenia spracúvaných utajovaných skutočností s využitím prostriedkov alebo opatrení podľa osobitného predpisu,[1]) prípadne ich vhodnou kombináciou za podmienky zachovania požadovanej úrovne bezpečnosti.

§ 3
Schvaľovanie technických prostriedkov do prevádzky

(1) Vedúci môže schváliť technický prostriedok do prevádzky, ak

a) technický prostriedok je certifikovaný,[5])

b) prevádzkové podmienky technických prostriedkov sú v súlade so schváleným bezpečnostným projektom[6]) a s podmienkami práce certifikovaného prostriedku.

(2) Vedúci pred uvedením technického prostriedku do prevádzky zabezpečí spracovanie

a) protokolu o schválení technického prostriedku do prevádzky, v ktorom určí obdobie povolenej prevádzky, podmienky a spôsob jeho používania,

b) smernice o používaní technického prostriedku.

§ 4
Smernica o používaní technického prostriedku

(1) Smernica o používaní technického prostriedku (ďalej len „smernica“) konkretizuje úlohy a opatrenia vyplývajúce z bezpečnostného projektu.

(2) Smernica 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; zoznamy osôb a rozsahy oprávnení môžu byť uvedené v samostatnej prílohe k smernici,

c) určenie bezpečnostného správcu, ktorý zodpovedá za správu bezpečnostných funkcií,

d) určenie správcu informačného systému, ktorý zodpovedá za výkon kontroly dodržiavania bezpečnostných zásad z hľadiska funkčnosti systému,

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

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

(3) Smernicu vypracúva žiadateľ osobitne pre bezpečnostného správcu, správcu informačného systému a pre jednotlivých používateľov, prípadne skupiny používateľov.

§ 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 na základe znalosti informácie dostupnej iba používateľovi, ktorou sa technickému prostriedku identifikuje, a autentizáciou používateľa. Autentizácia používateľa je overenie jeho totožnosti podľa požadovanej miery záruky na princípe porovnania prístupového identifikátora používateľa s hodnotou, ktorá je uložená v prístupovom prostriedku.

(2) Pre technický prostriedok určený na prácu s utajovanými skutočnosťami stupňa utajenia Vyhradené je identifikátorom používateľa

a) znalosť informácie dostupnej iba používateľovi,

b) prístupový prostriedok, ktorý jednoznačne identifikuje používateľa,

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

(3) Pre technický prostriedok určený na prácu s utajovanými skutočnosťami stupňov utajenia Prísne tajné, Tajné a Dôverné je identifikátorom používateľa

a) znalosť informácie dostupnej iba používateľovi, ktorou sa technickému prostriedku identifikuje, a súčasne prístupový prostriedok, ktorého prostredníctvom túto identitu potvrdzuje,

b) prístupový prostriedok, 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 chráni svoje identifikátory pred ich stratou, vyzradením alebo zneužitím.

(6) Každý technický prostriedok, na ktorom sa pracuje s utajovanou skutočnosťou, obsahuje kontrolný mechanizmus a blokovací mechanizmus, ktoré zabraňujú používateľovi pracovať s technickým prostriedkom v prípade, ak jeho identifikátor ho na túto prácu neoprávňuje.

(7) Utajovaná skutočnosť, ktorá je výstupom z technického prostriedku, musí byť označená príslušným stupňom utajenia tak, aby bola zaručená bezpečná manipulácia s ňou v súlade s podmienkami ustanovenými zákonom pre príslušný stupeň utajenia.

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

(9) Technické prostriedky sa umiestňujú v chránených priestoroch, v ktorých je zabezpečená ich ochrana pred neoprávneným prístupom nepovolaných osôb, pred poškodením, nežiaducim elektromagnetickým vyžarovaním alebo manipuláciou v súlade s bezpečnostným projektom. Spôsob ochrany technických prostriedkov musí zodpovedať požiadavkám na bezpečnosť technických prostriedkov spracúvajúcich utajované skutočnosti príslušného stupňa utajenia.

(10) Technický prostriedok sa umiestňuje tak, aby sa zamedzilo nepovolaným osobám oboznamovať sa s utajovanými skutočnosťami.

(11) Všetky nosiče utajovaných skutočností sa evidujú ako administratívne pomôcky,[7]) ak je to možné vzhľadom na charakter nosiča a účel použitia.

(12) Technické prostriedky na súčinnostné spojenie úradu a ústredných orgánov štátnej správy určuje úrad.

§ 6
Certifikácia technického prostriedku

(1) Druhy certifikácie technického prostriedku sú

a) certifikácia typu technického prostriedku (ďalej len „certifikácia typu“),

b) certifikácia jednotlivého technického prostriedku.

(2) Úrad alebo autorizovaná osoba uzná výsledky skúšok vydané zahraničnou certifikačnou autoritou, ak to vyplýva z medzinárodnej zmluvy alebo z inej dohody, ktorou je Slovenská republika viazaná.

§ 7
Certifikácia typu

(1) Certifikáciou typu sa overuje a osvedčuje zhoda vlastností typu technického prostriedku s požiadavkami bezpečnosti podľa § 2 a 5. Výsledkom certifikácie je certifikát podľa prílohy č. 2.

(2) Žiadosť o vykonanie certifikácie typu predkladá úradu alebo autorizovanej osobe písomne vedúci podľa prílohy č. 1.

§ 8
Certifikácia jednotlivého technického prostriedku

(1) Certifikáciou jednotlivého technického prostriedku sa overuje a osvedčuje zhoda jeho vlastností s požiadavkami bezpečnosti podľa § 2 a 5, ak úrad nevydal certifikát typu.

(2) Na certifikáciu jednotlivého technického prostriedku sa primerane vzťahujú ustanovenia § 7.

§ 9
Použitie systémových prostriedkov

(1) Na prácu s utajovanými skutočnosťami možno použiť len odporúčaný systémový prostriedok s odporúčaným bezpečnostným nastavením pre daný stupeň utajenia a za podmienok uvedených v certifikáte technického prostriedku. Zoznam odporúčaných systémových prostriedkov bude uverejňovaný na internetovej stránke úradu.

(2) Každý systémový prostriedok, ktorým sa spracúvajú utajované skutočnosti, obsahuje kontrolný mechanizmus a blokovací mechanizmus, ktoré zabraňujú používateľovi pracovať s daným systémovým prostriedkom v prípade, ak jeho identifikátor ho na túto prácu neoprávňuje.

(3) Systémové prostriedky pre súčinnostné spojenie úradu a ústredných orgánov štátnej správy určuje úrad.

§ 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 so smernicami. Informačným systémom sa rozumie jeden počítač alebo viac počítačov, ich programové vybavenie, periférne zariadenia, procesy alebo prostriedky, ktoré tvoria celok schopný vykonávať zber, tvorbu, spracovanie, ukladanie, zobrazenie a prenos utajovaných skutočností.

(2) Úloha bezpečnostného správcu obsahuje výkon správy bezpečnosti informačného systému, ktorý zahŕňa 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 preskúmania, ako aj stanovenia zodpovednosti konkrétneho používateľa za ním vykonané aktivity v informačnom systéme.

§ 11
Bezpečnostný projekt na technický prostriedok

(1) Bezpečnostný projekt na technický prostriedok obsahuje

a) základné údaje
   1. názov, druh, identifikáciu alebo špecifikáciu technického prostriedku,
   2. stupeň utajenia spracúvaných utajovaných skutočností,
   3. názov, adresu a IČO organizácie,
   4. meno spracovateľa (autora alebo kolektívu autorov),
   5. odtlačok pečiatky organizácie, dátum schválenia a podpis schvaľovateľa,

b) bezpečnostný zámer
   1. požiadavky na bezpečnosť technického prostriedku pre žiadaný stupeň utajenia,
   2. posúdenie súčasného stavu, špecifikáciu problémov a nedostatkov bezpečnosti technického prostriedku,
   3. vymedzenie kľúčových problémových miest,

c) opis technického prostriedku
   1. špecifikáciu prostredia, v ktorom je umiestnený technický prostriedok,
   2. špecifikáciu informačného prostredia (hardware, software),
   3. podmienky prevádzky technického prostriedku,

d) analýzu ochrany utajovaných skutočností
   1. klasifikovanie hlavných hrozieb pre utajované skutočnosti,
   2. klasifikovanie možných protiopatrení na jednotlivé hrozby,

e) špecifikáciu použitých bezpečnostných štandardov a určenie iných použitých metód a prostriedkov ochrany utajovaných skutočností, ktoré riešia problematiku zabezpečenia technického prostriedku pred stratou dôvernosti, integrity a dostupnosti utajovaných skutočností,

f) špecifikáciu hrozieb zabezpečených opatreniami na ochranu, ktorá obsahuje konkrétne hrozby, ktoré na aktíva reálne pôsobia, a realizované protiopatrenia,

g) špecifikáciu hrozieb nezabezpečených opatreniami na ochranu, ktorá obsahuje konkrétne hrozby, ktoré na aktíva reálne pôsobia a na ktoré nie sú primerané realizované protiopatrenia,

h) smernicu na havarijné plánovanie a obnovu činností technického prostriedku alebo systému, ktorá obsahuje
   1. organizačné opatrenia pri mimoriadnych udalostiach,
   2. spôsob kontroly týchto organizačných opatrení.

(2) Kontrola a aktualizácia bezpečnostného projektu sa vykonáva po každej zmene, ktorá by mohla mať vplyv na jeho obsah, a to formou dodatku. Bezpečnostný projekt a dodatok k nemu podliehajú schvaľovaciemu konaniu úradu.

§ 12
Používanie bezpečnostných štandardov

(1) Bezpečnostné štandardy predstavujú súbor noriem, ktoré určujú minimálne kritériá pre požadovanú úroveň ochrany technických prostriedkov.

(2) Zoznam noriem, podľa ktorých sa určuje bezpečnostný štandard, vydáva úrad; aktuálny zoznam úrad zverejňuje na svojej internetovej stránke.

(3) Bezpečnostný štandard technických prostriedkov sa určuje podľa technických noriem.[8])

§ 13
Účinnosť

Táto vyhláška nadobúda účinnosť 1. júna 2004.

Aurel Ugor v. r.

Príloha č. 1
vyhláške č. 339/2004 Z. z.

Ž I A D O S Ť

o vykonanie certifikácie typu/jednotlivého technického prostriedku
pre stupeň utajenia.....
podľa § 56 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností
a o zmene a doplnení niektorých zákonov

1. Žiadateľ

Názov:.....
Adresa:.....
IČO:.....
Tel.: ..... Fax: .....
Zodpovedný zamestnanec: .....Tel.: .....

2. Výrobca/dodávateľ

Názov:.....
Adresa:.....
IČO: .....
Tel.: ..... Fax: .....

3. Technický prostriedok

Typ: .....
Výrobné číslo (prípadne iný jednoznačne identifikujúci parameter):.....
.....
Identifikačný, autentifikačný prostriedok:
.....
Špecifikácia (matičná doska, BIOS a pod.): .....
.....
.....
.....

4. Sprievodná dokumentácia k žiadosti

Bezpečnostný projekt:	Príloha č. .....
Technická dokumentácia:	Príloha č. .....
Vydané certifikáty (aj zahraničné skúšobne):	Príloha č. .....
.....	Príloha č. .....
.....	Príloha č. .....
.....	Príloha č. .....

V .....dňa..... .....
(podpis a odtlačok pečiatky žiadateľa)

Príloha č. 2
vyhláške č. 339/2004 Z. z.

Národný bezpečnostný úrad podľa § 70 ods. 1 písm. a) bodu 8 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov vydáva

C E R T I F I K Á T
technického prostriedku

číslo: **C** ..... – stupeň utajenia/TP

Názov technického prostriedku: .....
(identifikačné vlastnosti)

Držiteľ certifikátu: .....

Sídlo: ..... IČO: .....

Výrobca/dodávateľ: .....

Sídlo: ..... IČO: .....

Týmto certifikátom sa osvedčuje spôsobilosť technického prostriedku na prácu s utajovanými skutočnosťami do stupňa utajenia (vrátane)

stupeň utajenia

Technický prostriedok sa môže používať na prácu s utajovanými skutočnosťami do stupňa utajenia .....(vrátane) len za dodržania podmienok uvedených v prílohe k tomuto certifikátu.

Dátum vydania certifikátu: .....

Platnosť certifikátu do: .....

V Bratislave dňa: .....

.....
(riaditeľ v. r.)

1) Vyhláška Národného bezpečnostného úradu č. 331/2004 Z. z. o personálnej bezpečnosti a o skúške bezpečnostného zamestnanca.
Vyhláška Národného bezpečnostného úradu č. 336/2004 Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti.
Vyhláška Národného bezpečnostného úradu č. 338/2004 Z. z. o administratívnej bezpečnosti.
Vyhláška Národného bezpečnostného úradu č. 340/2004 Z. z., ktorou sa ustanovujú podrobnosti o šifrovej ochrane informácií.

2) § 8 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.

3) Vyhláška Národného bezpečnostného úradu č. 340/2004 Z. z.

4) Zákon Národnej rady Slovenskej republiky č. 46/1993 Z. z. o Slovenskej informačnej službe v znení neskorších predpisov.

5) § 55 ods. 4 zákona č. 215/2004 Z. z.

6) § 58 zákona č. 215/2004 Z. z.

7) Vyhláška Národného bezpečnostného úradu č. 338/2004 Z. z.

8) STN ISO/IEC 17799 Informačné technológie. Kódex praxe manažérstva informačnej bezpečnosti, STN ISO/IEC TR 13335-1 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 1: Koncepcie a modely bezpečnosti IT, STN ISO/IEC TR 13335-2 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 2: Riadenie a plánovanie bezpečnosti IT, STN ISO/IEC TR 13335-3 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 3: Techniky pre manažment bezpečnosti IT, STN ISO/IEC TR 13335-4 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 4: Výber bezpečnostných opatrení, STN ISO 7498-2 Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). Základný referenčný model. Časť 2: Bezpečnostná architektúra, STN ISO/IEC 9796 Informačná technika. Bezpečnostné metódy. Metóda digitálneho podpisu s obnovou správy, STN ISO/IEC 9797 Informačné technológie. Bezpečnostné techniky. Mechanizmus na zachovanie integrity dát s kryptovacou kontrolnou funkciou pracujúcou s blokovým šifrovacím algoritmom, STN ISO/IEC 9798-1 Informačná technika. Bezpečnostné metódy. Mechanizmy autentifikácie entity. Časť 1: Všeobecný model, STN ISO/IEC 9798-2 Informačné technológie. Bezpečnostné techniky. Mechanizmus overovania entít. Časť 2: Mechanizmus so symetrickým šifrovacím algoritmom, STN ISO/IEC 9798-3 Informačné technológie. Bezpečnostné techniky. Mechanizmus overovania entít. Časť 3: Overovanie entít pomocou algoritmu verejného kľúča, ISO 8732, ISO 9564-1, ISO 9564-2, ISO/IEC 101664, TCSEC – Trusted Computer Evaluation Criteria, ITSEC – International Trusted Evaluation Criteria.

Vydavateľ Zbierky zákonov Slovenskej republiky a prevádzkovateľ právneho a informačného portálu Slov-Lex dostupného na webovom sídle www.slov-lex.sk je Ministerstvo spravodlivosti Slovenskej republiky, Župné námestie 13, 813 11 Bratislava, tel.: 02 571 01 000, e-mail: helpdesk@slov-lex.sk.