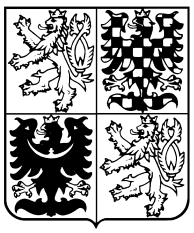

Sbírka zákonů a mezinárodních smluv

ČESKÁ REPUBLIKA

Zpřístupněna dne 27. prosince 2024

Vyhláška č. 479/2024 Sb.

Vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o některých náležitostech žádosti o uzavření smlouvy o zajištění činnosti (vyhláška o informační bezpečnosti)

479

VYHLÁŠKA

ze dne 19. prosince 2024

o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o některých náležitostech žádosti o uzavření smlouvy o zajištění činnosti (vyhláška o informační bezpečnosti)

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 34 odst. 7, § 35 odst. 6, § 36 odst. 4 a § 53 písm. b) až d) a f) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění zákona č. 255/2011, zákona č. 205/2017 Sb. a zákona č. 267/2024 Sb., (dále jen „zákon“):

ČÁST PRVNÍ

ÚVODNÍ USTANOVENÍ

§ 1

Předmět úpravy

(1) Tato vyhláška upravuje v návaznosti na předpisy Evropské unie[1])

a) požadavky na informační systém nakládající s utajovanými informacemi (dále jen „informační systém“) a podmínky jeho bezpečného provozování v závislosti na stupni utajení utajovaných informací, s nimiž nakládá, a na bezpečnostním provozním módu,

b) obsah bezpečnostní dokumentace informačního systému,

c) náležitosti oznámení provozovatele certifikovaného informačního systému o zavedení dalších nutných bezpečnostních funkcí nebo opatření podle § 34 odst. 7 písm. c) zákona,

d) obsah žádosti o schválení projektu bezpečnosti komunikačního systému nakládajícího s utajovanými informacemi (dále jen „komunikační systém“),

e) náležitosti projektu bezpečnosti komunikačního systému (dále jen „projekt bezpečnosti“) a způsob a podmínky jeho schvalování podle § 35 odst. 6 zákona,

f) způsob a podmínky provádění akreditace informačního systému cizí moci nakládajícího s utajovanými informacemi a provozovaného na území České republiky,

g) náležitosti žádosti a opakované žádosti o certifikaci informačního systému a dokumentaci nezbytnou k provedení certifikace informačního systému,

h) způsob a podmínky provádění certifikace nebo akreditace informačního systému, jejich opakování a obsah certifikační zprávy podle § 46 odst. 13 a

i) vzor certifikátu informačního systému.

(2) Tato vyhláška dále stanoví podmínky bezpečného provozování zařízení, které není součástí informačního nebo komunikačního systému (dále jen „samostatné elektronické zařízení"), a rozsah požadovaných informací podle § 36 odst. 2 písm. b) zákona.

(3) Tato vyhláška dále stanoví náležitosti žádosti o uzavření smlouvy o zajištění činnosti podle § 52 zákona, jejímž předmětem je provádění dílčích úloh při ověřování způsobilosti informačního systému k nakládání s utajovanými informacemi.

§ 2

Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) objektem informačního systému, komunikačního systému nebo samostatného elektronického zařízení (dále jen „systém") pasivní prvek, který obsahuje nebo přijímá informaci,

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

c) aktivem systému na základě analýzy rizik definované hardwarové a softwarové vybavení, dokumentace a informace, které jsou v systému uloženy,

d) auditním záznamem záznam systému poskytující bližší informace o události nebo stavu systému nebo o činnosti subjektu systému,

e) autentizací subjektu systému proces ověření předložených identifikačních znaků poskytující záruky, že prohlašovaná identita subjektu systému je pravá,

f) autorizací subjektu systému proces udělení oprávnění subjektu systému k provádění určených operací s určenými objekty systému,

g) informační bezpečností soubor, uspořádání a řízení bezpečnostních opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost aktiv systému, a odpovědnost subjektů systému za jejich činnost v systému,

h) komunikační bezpečností bezpečnostní opatření použitá k zajištění bezpečnosti informací v systému při přenosu komunikačním kanálem,

i) komunikačním kanálem prostředí sloužící k přenosu informací mezi objekty systému, případně subjekty systému v rámci jednoho nebo několika propojených systémů,

j) bezpečnostní událostí událost, která může způsobit bezpečnostní incident,

k) bezpečnostním incidentem narušení informační bezpečnosti,

l) uživatelem fyzická osoba jako subjekt systému v určité roli,

m) rolí souhrn určených činností a potřebných oprávnění,

n) nosičem informací zařízení s energeticky nezávislou pamětí, které je určeno výhradně pro použití v provozu systému jako jeho součást, a které není určeno k evidenci nebo doručení adresátovi jako utajovaný dokument v nelistinné podobě podle právního předpisu upravujícího administrativní bezpečnost,

o) řízením přístupu prostředky pro omezení přístupu subjektů systému k objektům systému, zajišťující, že přístup k nim získá jen oprávněný subjekt systému,

p) volitelným řízením přístupu řízení přístupu založené na kontrole přístupových práv subjektu systému k objektu systému, přičemž subjekt systému vybavený určitými přístupovými právy pro přístup k objektu systému může zvolit, které další subjekty systému autorizuje k přístupu k tomuto objektu systému, a může tak ovlivňovat tok informací mezi objekty systému, a

q) povinným řízením přístupu řízení přístupu založené na porovnání stupně utajení utajované informace obsažené v objektu systému a úrovně oprávnění subjektu systému pro přístup k utajované informaci a zajišťující správný tok informací mezi objekty systému s různými stupni utajení nezávisle na volbě učiněné uživatelem.

ČÁST DRUHÁ

INFORMAČNÍ BEZPEČNOST

§ 3

Bezpečnostní požadavky

(1) Bezpečnostní požadavky jsou požadavky na systém, jeho řízení, správu a provoz a na objekty, subjekty a aktiva systému, jejichž cílem je zajištění informační bezpečnosti v oblastech

a) počítačové a komunikační bezpečnosti,

b) kryptografické ochrany,

c) ochrany před únikem utajovaných informací kompromitujícím vyzařováním,

d) administrativní bezpečnosti a organizačních opatření,

e) personální bezpečnosti a

f) fyzické bezpečnosti.

(2) Bezpečnostní požadavky naplňuje provozovatel systému prostřednictvím souboru bezpečnostních opatření specifikovaného v příslušné bezpečnostní dokumentaci, která musí být autorizována odpovědnou osobou, jí pověřenou osobou nebo bezpečnostním ředitelem.

(3) Bezpečnostní opatření musí provozovatel systému nastavit tak, aby rizika, kterým je utajovaná informace v elektronické podobě v systému vystavena, byla snížena na přijatelnou úroveň.

(4) Bezpečnostní opatření realizuje provozovatel systému přednostně zaváděním a prováděním programově technických mechanismů systému (dále jen „bezpečnostní funkce“).

(5) Přijatý soubor bezpečnostních opatření musí být provozovatelem systému řízen tak, aby bylo zajištěno provádění jeho návrhu, implementace, provozování, monitorování, přezkoumávání, udržování a jeho zlepšování.

(6) Bezpečnostní opatření přijatá k zajištění informační bezpečnosti systému musí splňovat alespoň

a) bezpečnostní požadavky uvedené v této vyhlášce,

b) bezpečnostní požadavky uvedené v právním předpise upravujícím ochranu před únikem utajovaných informací kompromitujícím vyzařováním,

c) pravidla pro ochranu utajovaných informací uvedená v právním předpise upravujícím kryptografickou ochranu a

d) výsledky analýzy rizik podle § 38.

Bezpečnostní požadavky v oblasti počítačové bezpečnosti

§ 4

(1) Systémem musí být zajištěny bezpečnostní funkce

a) identifikace a autentizace subjektu systému, které musí předcházet všem jeho dalším činnostem, a musí být zajištěna ochrana důvěrnosti a integrity autentizační informace, nestanoví-li analýza rizik a popis bezpečnosti systému jinak,

b) volitelného řízení přístupu k objektům systému na základě rozlišování a správy přístupových práv subjektu systému a jeho identity nebo členství ve skupině subjektů se shodným oprávněním,

c) nepřetržitého zaznamenávání událostí, které mohou ovlivnit bezpečnost informací nebo systému, do auditních záznamů a zabezpečení auditních záznamů před neautorizovaným přístupem, změnou nebo zničením; zaznamenává se zejména použití identifikačních a autentizačních informací, pokus o změnu přístupových práv, vytváření nebo rušení objektů systému nebo činnost oprávněných subjektů systému ovlivňující bezpečnost informací nebo systému,

d) schopnosti zkoumání auditních záznamů a stanovení odpovědnosti každého subjektu systému,

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

f) ochrany důvěrnosti a integrity dat během přenosu mezi jejich zdrojem a cílem a

g) ochrany před škodlivým kódem.

(2) Bezpečnostní funkce uvedené v odstavci 1 se realizují pomocí identifikovatelných prostředků počítačové bezpečnosti. Úroveň popisu jejich provedení a nastavení uvedené v popisu bezpečnosti systému musí umožnit jejich nezávislé prověření a zhodnocení jejich dostatečnosti.

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

(4) Provozovatel systému musí zajistit, aby pro nepřetržité zaznamenávání událostí a jejich vyhodnocování bylo nastaveno aktuální datum a čas po celou dobu provozu systému.

(5) Na základě analýzy rizik se u rozsáhlých informačních nebo komunikačních systémů musí využívat technické nástroje pro zaznamenávání událostí, které umožňují i nepřetržité vyhodnocování událostí s cílem identifikace bezpečnostních incidentů včetně včasného varování určených rolí. Rozsáhlým informačním nebo komunikačním systémem se rozumí systém mající nejméně 200 uživatelů.

§ 5

(1) Bezpečnostní opatření spočívající v zavedení některých bezpečnostních funkcí počítačové bezpečnosti podle § 4 lze v odůvodněných případech nahradit použitím jiných bezpečnostních opatření personální, administrativní a fyzické bezpečnosti anebo použitím vhodných organizačních bezpečnostních opatření.

(2) Při nahrazení bezpečnostních opatření spočívajících v zavedení bezpečnostních funkcí počítačové bezpečnosti náhradním bezpečnostním opatřením podle odstavce 1 musí být zachován účel bezpečnostní funkce a kvalita a úroveň bezpečnosti poskytované nahrazovaným bezpečnostním opatřením.

(3) Nahrazení bezpečnostních opatření spočívajících v zavedení bezpečnostních funkcí počítačové bezpečnosti náhradním bezpečnostním opatřením podle odstavce 1 musí být popsáno a zdůvodněno v analýze rizik nebo popisu bezpečnosti systému.

Systémově závislé bezpečnostní požadavky na informační systém odvozené z bezpečnostního provozního módu

§ 6

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

a) bezpečnostní provozní mód dedikovaný,

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 dedikovaný je takové prostředí, které umožňuje zpracování utajovaných informací různého stupně utajení, přičemž všechny subjekty informačního systému musí splňovat podmínky pro přístup k utajovaným informacím nejvyššího stupně utajení, se kterými je informační systém určen nakládat, a zároveň musí být oprávněny pracovat se všemi obsaženými utajovanými informacemi. V bezpečnostním provozním módu dedikovaném není zajištěna bezpečnostní funkce podle § 4 odst. 1 písm. b) a e).

(3) Bezpečnostní provozní mód s nejvyšší úrovní je takové prostředí, které umožňuje současné zpracování utajovaných informací různého stupně utajení, ve kterém všechny subjekty informačního systému musí splňovat podmínky pro přístup k utajovaným informacím nejvyššího stupně utajení, přičemž všechny subjekty informačního systému nemusí být oprávněny pracovat se všemi obsaženými utajovanými informacemi.

(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 současné zpracování utajovaných informací různého stupně utajení, kde všechny subjekty informačního systému nemusí splňovat podmínky přístupu k utajovaným informacím nejvyššího stupně utajení a nemusí být oprávněny pracovat se všemi utajovanými informacemi. Při provozu v bezpečnostním provozním módu víceúrovňovém musí být zajištěna bezpečnostní funkce povinného řízení přístupu subjektu informačního systému k objektům informačního systému.

§ 7

(1) Bezpečnostní funkce povinného řízení přístupu subjektů informačního systému k objektům informačního systému musí zabezpečit

a) trvalé spojení každého subjektu a objektu informačního systému s bezpečnostními příznaky, které pro subjekt informačního systému vyjadřují úrovně oprávnění přístupu subjektu informačního systému k objektům informačního systému a pro objekt informačního systému stupeň utajení utajované informace, kterou objekt informačního systému obsahuje nebo přijímá,

b) ochranu integrity bezpečnostního příznaku,

c) výlučné oprávnění bezpečnostního správce k provádění změn bezpečnostních příznaků subjektů i objektů informačního systému a

d) přidělení předem definovaných hodnot bezpečnostních příznaků pro nově vytvořené objekty informačního systému a zachování bezpečnostního příznaku při kopírování objektu informačního systému.

(2) Při uplatňování bezpečnostní funkce povinného řízení přístupu subjektů informačního systému k objektům informačního systému může subjekt informačního systému

a) číst informace v objektu informačního systému pouze tehdy, je-li jeho bezpečnostní příznak stejný nebo vyšší než bezpečnostní příznak objektu informačního systému, a

b) zapisovat informace do objektu informačního systému pouze tehdy, je-li jeho bezpečnostní příznak stejný nebo nižší než bezpečnostní příznak objektu informačního systému.

(3) Subjekt informačního systému může přistupovat k informaci obsažené v objektu informačního systému, jestliže jej povolují jak pravidla povinného řízení přístupu, tak pravidla volitelného řízení přístupu.

(4) Při provozu informačního systému v bezpečnostním provozním módu víceúrovňovém musí být utajovaná informace vystupující z informačního systému přesně označena stupněm utajení a utajované informaci vstupující do informačního systému přiřazen stupeň utajení.

(5) Při provozu informačního systému v bezpečnostním provozním módu víceúrovňovém, ve kterém se nakládá s utajovanou informací stupně utajení Přísně tajné, musí být prověřeno, zda nedochází k nežádoucí výměně informací mezi informačním systémem a okolím způsobem, který není pro komunikaci přímo určen a ani předpokládán, a při kterém dochází k obcházení bezpečnostních mechanismů informačního systému.

§ 8

Bezpečnostní požadavky v oblasti komunikační bezpečnosti

(1) Při přenosu utajované informace komunikačním kanálem musí být zajištěna ochrana důvěrnosti a integrity této utajované informace prostřednictvím kryptografické ochrany nebo jiných vhodných bezpečnostních opatření tak, aby nebyla ohrožena informační bezpečnost.

(2) U komunikačních kanálů, které jsou vedeny v rámci zabezpečených oblastí nebo objektů, lze přenášené utajované informace chránit kryptografickou ochranou na nižší úrovni, než je pro daný stupeň utajení přenášené utajované informace vyžadováno, nebo lze kryptografickou ochranu utajovaných informací nahradit použitím vhodných bezpečnostních opatření fyzické bezpečnosti.

(3) V závislosti na komunikačním prostředí musí být zajištěna spolehlivá identifikace a autentizace komunikujících subjektů systému, včetně ochrany identifikačních a autentizačních dat. Tato identifikace a autentizace předchází přenosu utajované informace.

(4) Přenos utajované informace komunikačním kanálem vedený mimo zabezpečenou oblast nebo objekt musí být chráněn pomocí kryptografického prostředku certifikovaného alespoň pro stupeň utajení přenášené utajované informace.

(5) Při uplatnění specifických bezpečnostních opatření pro detekci narušení bezpečnosti komunikačního kanálu a bezpečnostních opatření pro zmírnění následků bezpečnostní události přijatých na základě analýzy rizik může Národní úřad pro kybernetickou a informační bezpečnost v rámci certifikace informačního systému nebo schvalování projektu bezpečnosti schválit i odlišný způsob zabezpečení, než je uveden v odstavcích 2 a 4.

(6) Úroveň použité ochrany komunikačních kanálů podle odstavce 1 musí odpovídat úrovni ochrany požadované pro nejvyšší stupeň utajení utajovaných informací, které budou komunikačním kanálem přenášeny.

Bezpečnostní požadavky na bezpečné propojení informačních nebo komunikačních systémů

§ 9

(1) Komunikační kanál mezi informačními nebo komunikačními systémy, které jsou určeny k nakládání s utajovanými informacemi stejných nebo různých stupňů utajení, případně je-li některý z nich určen pouze k nakládání s neutajovanými informacemi, lze zřídit pouze v případě nezbytné provozní potřeby a jestliže je stanoven způsob jeho ochrany prostřednictvím bezpečnostního rozhraní nebo jiným vhodným bezpečnostním opatřením.

(2) Popis propojení a bezpečnostního rozhraní je součástí popisu bezpečnosti každého propojovaného informačního nebo komunikačního systému.

(3) Propojení informačních nebo komunikačních systémů určených k nakládání s utajovanou informací odlišného stupně utajení musí být provedeno tak, aby mezi nimi bylo zabráněno přenosu utajované informace vyššího stupně utajení, než je stupeň utajení utajované informace, pro který je informační nebo komunikační systém určen.

(4) Mezi propojenými informačními nebo komunikačními systémy musí být komponenty bezpečnostního rozhraní umístěny v zabezpečené oblasti alespoň takové kategorie, jakou je nejvyšší stupeň utajení utajované informace, se kterým je možno nakládat v některém z propojovaných informačních nebo komunikačních systémů.

(5) Správa bezpečnostního rozhraní je zajišťována subjekty toho propojeného informačního nebo komunikačního systému, který je určen k nakládání s vyšším stupněm utajení utajovaných informací. Jsou-li propojené informační nebo komunikační systémy určeny k nakládání s utajovanými informacemi stejného stupně utajení, subjekty propojeného informačního nebo komunikačního systému zajišťující správu bezpečnostního rozhraní stanoví popis bezpečnosti systému.

§ 10

(1) Informační nebo komunikační systém nesmí být propojen s veřejnou komunikační sítí podle právního předpisu upravujícího elektronické komunikace, ledaže má pro tento účel instalované vhodné bezpečnostní rozhraní.

(2) Bezpečnostní rozhraní podle odstavce 1 musí zamezit průniku do informačního nebo komunikačního systému a musí umožnit pouze kontrolovaný přenos informací, který nenarušuje důvěrnost, integritu a dostupnost informací a služeb tohoto sytému.

(3) Informační nebo komunikační systém určený k nakládání s utajovanou informací stupně utajení Přísně tajné, nebo s utajovanou informací vyžadující zvláštní režim nakládání označenou textem „ATOMAL“, „SIOP“, „CRYPTO“, „BOHEMIA“ nebo „KRYPTO“, nesmí být přímo ani nepřímo propojen s veřejnou komunikační sítí.

(4) Pokud je veřejná komunikační síť využívána výhradně k přenosu informací a přenášené utajované informace jsou chráněny příslušným certifikovaným kryptografickým prostředkem, nepovažuje se takové propojení za propojovací komunikační kanál.

§ 11

Bezpečnostní požadavky na řízení kapacit a kontinuity

(1) Systém musí zajistit, že požadovaná utajovaná informace je přístupná na stanoveném místě, v požadované formě a v určeném časovém rozmezí.

(2) V rámci zajištění bezpečného provozu popis bezpečnosti systému vymezuje komponenty, které lze nahradit bez omezení kontinuity jeho provozu, a dále rozsah požadované základní funkčnosti a komponenty, při jejichž selhání musí být základní funkčnost zaručena.

(3) Provozovatel systému plánuje kapacity aktiv systému a sleduje kapacitní požadavky tak, aby nedocházelo k chybám způsobeným nedostatkem volných kapacit.

(4) Popis bezpečnosti systému obsahuje plán na obnovení činnosti systému po havárii. V případě havárie může být opětovné uvedení do známého zabezpečeného stavu provedeno automaticky, nebo manuálně provozním správcem. Všechny činnosti, které byly provedeny pro obnovení činnosti, jsou zaznamenány do auditních záznamů chráněných před neoprávněnou modifikací nebo zničením. Pokud činnosti podle věty třetí nelze zaznamenat do auditních záznamů, zaznamenají se do provozního deníku.

§ 12

Bezpečnostní požadavky na ochranu rozmístitelných nebo mobilních zařízení

(1) Pro rozmístitelné zařízení se v analýze rizik posuzují i rizika, která jsou spojena s prostředím, ve kterém se předpokládá použití tohoto zařízení.

(2) Pro mobilní zařízení se v analýze rizik posuzují i rizika, která jsou spojena s dopravou na místo, kde bude zařízení používáno.

(3) Rozmístitelné nebo mobilní zařízení obsahující utajovaný nosič informací se pro účely bezpečnostních opatření považuje za nosič informací utajovaný podle § 13 odst. 2.

Bezpečnostní požadavky na bezpečnost nosičů informací

§ 13

(1) Je-li nosič informací utajovaný, musí jeho stupeň utajení odpovídat nejvyššímu stupni utajení utajované informace, kterou lze na nosiči informací uchovávat.

(2) Na nosiči informací musí být uvedeno evidenční označení podle § 42 odst. 4 písm. c) a identifikace provozovatele systému. Informace se na nosič informací vyznačují přímo, pomocí štítku, visačky nebo jiným vhodným způsobem.

(3) V analýze rizik je identifikován nosič informací podle způsobu jeho zapojení do zařízení jako

a) vyjímatelný, pokud jej lze ze zařízení vyjmout i bez nutnosti použití nástroje, aniž by došlo k nevratnému poškození zařízení nebo k poškození ochranného prvku zařízení,

b) vyměnitelný, pokud jej lze ze zařízení vyjmout pouze s použitím nástroje, aniž by došlo k nevratnému poškození zařízení, nebo

c) zabudovaný, pokud jej lze ze zařízení vyjmout pouze způsobem, při němž dojde k nevratnému poškození zařízení.

(4) V případech odůvodněných v popisu bezpečnosti systému lze evidovat a označit stupněm utajení nosič informací umístěný v zařízení nejpozději po prvním otevření zařízení. Zařízení s neevidovaným nosičem informací podle věty první musí splňovat bezpečnostní požadavky podle § 22.

§ 14

(1) Stupeň utajení nosiče informací stupně utajení Přísně tajné, Tajné nebo se zvláštním režimem nakládání nesmí být zrušen.

(2) Stupeň utajení nosiče informací stupně utajení Přísně tajné, Tajné nebo se zvláštním režimem nakládání může být snížen, pouze pokud je prokázáno, že na něm byly během jeho dosavadního životního cyklu uloženy pouze utajované informace nižšího stupně utajení nevyžadující zvláštní režim nakládání nebo informace neutajované.

(3) Stupeň utajení nosiče informací stupně utajení Důvěrné může být snížen nebo zrušen, pouze pokud

a) vymazání utajovaných informací z něj bylo provedeno způsobem uvedeným v § 15 odst. 1,

b) je prokázáno, že na něm byly během jeho dosavadního životního cyklu uloženy pouze utajované informace nižšího stupně utajení nebo informace neutajované, nebo

c) je prokázáno, že stupeň utajení utajovaných informací uložených na něm během jeho dosavadního životního cyklu byl snížen nebo zrušen.

(4) Stupeň utajení nosiče informací stupně utajení Vyhrazené může být zrušen, pouze pokud

a) vymazání utajovaných informací z něj bylo provedeno způsobem uvedeným v § 15 odst. 1,

b) je prokázáno, že na něm byly během jeho dosavadního životního cyklu uloženy pouze informace neutajované, nebo

c) je prokázáno, že stupeň utajení utajovaných informací uložených na něm během jeho dosavadního životního cyklu byl zrušen.

(5) Stupeň utajení nosiče informací obsahujícího zálohy informací se určuje podle nejvyššího stupně utajení utajovaných informací, se kterými může systém nakládat.

§ 15

(1) Vymazání utajované informace z nosiče informací, které umožňuje snížení nebo zrušení jeho stupně utajení, musí být provedeno tak, aby znemožnilo z nosiče informací opětovně získat, byť laboratorními metodami, utajovanou informaci na něm uchovanou během jeho dosavadního životního cyklu.

(2) Postup podle odstavce 1 musí být uveden v popisu bezpečnosti systému.

(3) Ničení nosiče informací musí být provedeno v souladu s postupy ničení nosičů informací nebo dat podle právního předpisu upravujícího fyzickou bezpečnost tak, aby znemožnilo z něho opětovně získat, byť laboratorními metodami, utajovanou informaci na něm uchovanou během jeho dosavadního životního cyklu.

(4) Popis bezpečnosti systému stanoví řízení přístupu uživatelů k vyjímatelným nosičům informací a ke vstupně výstupním portům, přes které jsou tyto nosiče informací k zařízení připojovány.

(5) Popis bezpečnosti systému stanoví podmínky přidělování nosiče informací jinému subjektu systému a postupy znemožňující zjistit jejich předchozí obsah.

Bezpečnostní požadavky na přístup uživatele k utajované informaci v systému

§ 16

(1) Uživatel musí být autorizován postupem stanoveným v popisu bezpečnosti systému.

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

(3) Privilegovaným uživatelem se rozumí role uživatele s oprávněními, která mu kromě základního přístupu k poskytovaným službám umožňují i provádění provozní nebo bezpečnostní správy, zejména role pracovníka provozní nebo bezpečnostní správy.

(4) Koncovým uživatelem se rozumí role uživatele s oprávněními, která mu umožňují základní přístup k poskytovaným službám a nakládání s utajovanými informacemi.

(5) Privilegovaný uživatel musí činnost, která není bezpečnostní nebo provozní správou, provádět jako koncový uživatel.

§ 17

(1) Uživatel v dané roli má vždy oprávnění k činnostem v systému pouze v rozsahu nezbytném pro jejich provádění.

(2) Uživatel systému, který je určen k nakládání s utajovanými informacemi stupně utajení Vyhrazené, Důvěrné nebo Tajné, v roli

a) pracovníka provozní správy s oprávněním administrátora a s oprávněním úplného řízení, nebo

b) pracovníka bezpečnostní správy celého systému

musí splňovat podmínky pro přístup fyzické osoby k utajované informaci stupně utajení o jeden stupeň vyšší, nežli je nejvyšší stupeň utajení utajovaných informací, se kterými může systém nakládat.

(3) Uživatel systému, který je určen k nakládání s utajovanými informacemi stupně utajení Přísně tajné, v roli

a) pracovníka provozní správy s oprávněním administrátora a s oprávněním úplného řízení, nebo

b) pracovníka bezpečnostní správy celého systému

musí splňovat podmínky pro přístup fyzické osoby k utajované informaci stupně utajení Přísně tajné.

(4) Splnění požadavku podle odstavce 2 se nevyžaduje u systému

a) malého rozsahu, kterým se rozumí systém mající nejvýše 30 uživatelů, nebo

b) zpracovávajícího pouze taktické utajované informace,

jestliže systém nenakládá s utajovanou informací cizí moci Organizace Severoatlantické smlouvy a se zvážením identifikovaných rizik je v analýze rizik nebo popisu bezpečnosti systému uvedeno jako dostačující splnění podmínek pro přístup fyzické osoby k utajované informaci stupně utajení shodného s nejvyšším stupněm utajení utajovaných informací, se kterými může systém nakládat.

(5) Uživatel v roli

a) pracovníka provozní správy systému s oprávněním administrátora a s omezeným oprávněním řízení systému, zejména správy serverů, správy aplikace nebo lokální správy, nebo

b) pracovníka bezpečnostní správy systému zajišťujícího 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 systém nakládat.

(6) Roli uživatele systému je na základě autorizace přidělen jedinečný identifikátor. Roli s jedinečným identifikátorem podle věty první může využívat několik uživatelů, je-li to nezbytné pro zajištění nepřetržité dostupnosti systému nebo správy systému a je-li zaveden postup umožňující určit, který uživatel v dané době tuto roli využívá; to musí být popsáno a zdůvodněno v popisu bezpečnosti systému.

§ 18

Bezpečnostní požadavky na bezpečnostní a provozní správu

(1) Popis bezpečnosti systému stanoví vhodnou strukturu bezpečnostní a provozní správy. V rámci struktury bezpečnostní správy zavede provozovatel systému roli bezpečnostního správce odděleně od jiných rolí správy, pokud není dále stanoveno jinak. V rámci struktury provozní správy zavede provozovatel systému roli provozního správce.

(2) Bezpečnostní správce je uživatel v roli pracovníka správy s oprávněními, která mu kromě základního přístupu k poskytovaným službám umožňují i provádění činností k zajištění bezpečnosti systému.

(3) Provozní správce je uživatel v roli pracovníka správy s oprávněními, která mu kromě základního přístupu k poskytovaným službám umožňují i provádění činností k zajištění požadované funkčnosti systému a řízení jeho provozu.

(4) V případě potřeby zajistit stanovený rozsah činností k zajištění bezpečnosti nebo provozuschopnosti systému zavede provozovatel systému organizační strukturu bezpečnostních nebo provozních správců nebo další role v bezpečnostní nebo provozní správě.

(5) Výkon bezpečnostní správy spočívá v

a) přidělování přístupových práv,
b) správě autentizačních a autorizačních informací,
c) správě konfigurace systému,
d) správě a vyhodnocování auditních záznamů,
e) aktualizaci bezpečnostní dokumentace,
f) vedení příslušných evidencí,
g) řešení bezpečnostních incidentů a krizových situací a vypracování zpráv o nich,
h) zajištění školení uživatelů v oblasti bezpečnosti,
i) kontrole dodržování bezpečnostních opatření a
j) dalších činnostech stanovených v bezpečnostní dokumentaci.

(6) Výkon provozní správy spočívá v provádění činností k zajištění provozuschopnosti systému a v dalších činnostech stanovených v bezpečnostní dokumentaci.

(7) V odůvodněných případech lze v popisu bezpečnosti systému sloučit některé role bezpečnostní a provozní správy.

§ 19

Bezpečnostní požadavky personální bezpečnosti při provozu systému

(1) Uživatel může vykonávat pouze takovou roli, kterou byl pověřen.

(2) Pověření podle odstavce 1 může provádět pouze odpovědná osoba provozovatele systému nebo jí pověřená osoba postupem stanoveným v popisu bezpečnosti systému.

(3) Odpovědná osoba nebo jí pověřená osoba zruší uživateli pověření

a) v případě změny jeho role,
b) v případě ukončení pracovněprávního nebo obdobného vztahu s provozovatelem systému, nebo
c) pokud přestal splňovat podmínky přístupu k utajované informaci podle zákona.

(4) Uživatel může vykonávat určenou roli, pouze pokud byl proškolen ve správném užívání systému a v dodržování bezpečnostních opatření. Školení se vyžaduje dále při podstatných změnách bezpečnostních opatření bez zbytečného odkladu, jinak nejméně jednou ročně.

(5) Přehled provedených školení, jejich obsah a seznam uživatelů, kteří školení absolvovali, včetně záznamů o prokazatelném absolvování školení, je součástí provozní bezpečnostní dokumentace. Přehled podle věty první může být veden i mimo provozní bezpečnostní dokumentaci. Způsob vedení přehledu podle věty druhé stanoví provozní bezpečnostní dokumentace.

§ 20

Bezpečnostní požadavky na činnost subjektu systému

(1) Činnost subjektu systému lze provádět pouze postupy popsanými v provozní bezpečnostní směrnici.

(2) Informace o činnosti subjektu systému se v auditním záznamu zaznamenává tak, aby bylo možno identifikovat narušení bezpečnosti systému nebo pokusy o ně.

Bezpečnostní požadavky na fyzickou bezpečnost

§ 21

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

(2) Aktiva systému musí být umístěna do prostoru, ve kterém je zajištěna fyzická ochrana před neoprávněným přístupem a poškozením a ovlivněním aktiv systému. Na základě analýzy rizik se stanovuje, která aktiva systému musí být umístěna v zabezpečené oblasti nebo objektu a požadovaná kategorie zabezpečené oblasti nebo objektu.

(3) Způsob umístění aktiv systému stanoví popis bezpečnosti systému.

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

§ 22

(1) Nejnižší možná míra zabezpečení zabezpečené oblasti pro umístění zařízení, v němž mohou být ukládány utajované informace, se určuje v souladu s tabulkami bodových hodnot nejnižší míry zabezpečení fyzické bezpečnosti uvedenými v právním předpise upravujícím fyzickou bezpečnost.

(2) Bodové ohodnocení fyzické bezpečnosti zařízení, v němž mohou být ukládány utajované informace, je závislé na způsobu zajištění důvěrnosti

a) informací uložených v zařízení a

b) autentizačních údajů uložených v autentizačních předmětech.

(3) Bodové ohodnocení fyzické bezpečnosti podle odstavce 2 je uvedeno v příloze č. 1 k této vyhlášce.

(4) Zařízení, v nichž mohou být ukládány utajované informace a jejich hardwarové komponenty, jsou označeny a opatřeny ochrannými prvky způsobem uvedeným v popisu bezpečnosti systému.

(5) Ochranný prvek se umísťuje tak, aby při pokusu o rozebrání zařízení, v němž mohou být ukládány utajované informace nebo jeho hardwarové komponenty, došlo k jeho poškození.

(6) Popis bezpečnosti systému stanoví způsob zajišťování důvěrnosti podle odstavce 2 a dále pravidla k zajištění bezpečnosti při

a) změně umístění zařízení a jeho hardwarových komponent,
b) údržbě zařízení a jeho hardwarových komponent,
c) provozování zařízení nebo jeho hardwarových komponent mimo prostory provozovatele systému a
d) bezpečné likvidaci nebo opakovaném použití zařízení nebo jeho hardwarových komponent.

§ 23

Bezpečnostní požadavky na administrativní bezpečnost v informačním systému

(1) Utajovanou informaci lze prostřednictvím informačního systému odeslat evidenčnímu místu adresáta, pouze pokud jsou na ní vyznačeny

a) stupeň utajení,
b) evidenční označení podle právního předpisu upravujícího administrativní bezpečnost,
c) identifikace odesílatele a
d) datum vzniku.

(2) Utajovaná informace doručená evidenčnímu místu adresáta prostřednictvím informačního systému musí být bez zbytečného odkladu zaevidována v elektronickém systému spisové služby sloužícím k evidenci utajovaných informací nebo v jednacím protokolu v listinné nebo elektronické podobě. Ustanovení právního předpisu upravujícího administrativní bezpečnost se použijí obdobně.

(3) V odůvodněných případech může odpovědná osoba, jí pověřená osoba nebo bezpečnostní ředitel stanovit výjimky, kdy se postupy podle odstavců 1 a 2 nepoužijí. Pravidla pro stanovování výjimek podle věty první stanoví popis bezpečnosti systému.

§ 24

Bezpečnostní požadavky na informační systém s distribuční službou

(1) Informační systém určený k doručování utajovaných informací mezi různými evidenčními místy musí mít

a) zřízen pro každé evidenční místo v rámci tohoto informačního systému doručovací adresu, kterou je adresa elektronické pošty nebo obdobný identifikátor distribuční služby, a
b) veden seznam doručovacích adres všech evidenčních míst v rámci tohoto informačního

systému dostupný všem uživatelům informačního systému, kteří jej nezbytně potřebují k výkonu své funkce, pracovní nebo jiné činnosti.

(2) Způsob a podmínky doručování utajovaných informací podle odstavce 1 musí být stanoveny v popisu bezpečnosti informačního systému.

§ 25

Bezpečnostní požadavky na testování a prověřování

(1) Soulad bezpečnostních opatření s bezpečnostní dokumentací ověřuje provozovatel systému testováním. K provedení testování nelze používat utajované informace.

(2) Soulad bezpečnostních opatření s právními předpisy, vnitřními předpisy a dotčenými smluvními závazky a dodržování bezpečnostních opatření provozovatel systému průběžně prověřuje, u informačního systému nejpozději bezprostředně před podáním opakované žádosti o certifikaci podle § 48.

(3) Podmínky provádění testování, podmínky prověřování podle odstavce 2 a jejich výsledky jsou součástí dokumentace k bezpečnostním testům.

§ 26

Bezpečnostní požadavky na bezpečnost vývoje a instalace

(1) Ve vývojovém prostředí systému musí být zajištěna bezpečnost, ochrana používaných testovacích dat a prováděno bezpečnostní testování změn systému před jejich zavedením do provozu.

(2) Postup instalace aktiv systému musí provozovatel systému organizovat tak, aby nebyla ohrožena informační bezpečnost a oslabeny bezpečnostní funkce.

(3) V popisu bezpečnosti systému musí být stanovena zařízení nebo komponenty, které zajišťují bezpečnostní funkce nebo jsou zranitelné ve fázi instalace.

(4) Zařízení nebo komponenty podle odstavce 3 musí být instalovány osobami splňujícími podmínky pro přístup fyzické osoby k utajované informaci nejvyššího stupně utajení utajované informace, s níž je systém určen nakládat. Ostatní zařízení nebo komponenty mohou být instalovány i osobami nesplňujícími podmínky pro přístup k utajované informaci podle věty první, pokud jsou tyto osoby pod neustálým osobním dohledem příslušného pracovníka správy a jestliže byly schváleny odpovědnou osobou provozovatele systému, jí pověřenou osobou nebo bezpečnostním ředitelem.

Bezpečnostní požadavky na bezpečnost provozu

§ 27

(1) Pro bezpečný provoz systému jsou v popisu bezpečnosti systému stanovena

a) práva a povinnosti uživatelů v jednotlivých rolích a

b) provozní pravidla a postupy

1. pro uvedení systému do provozu, ukončení provozu a obnovení provozu po selhání, chybě nebo mimořádné události,

2. pro sledování a vyhodnocování auditních záznamů a pro ochranu přístupu k těmto auditním záznamům,
3. pro řešení a vyhodnocování detekovaných bezpečnostních událostí a
4. řízení a schvalování provozních změn.

(2) Popis bezpečnosti systému obsahuje pravidla pro průběžné prověřování a vyhodnocování bezpečnosti provozu.

(3) Provozovatel systému je povinen řídit veškeré změny v rámci provozu systému. V popisu bezpečnosti systému musí být uvedeny postupy a mechanismy, které příslušné změny umožňují.

§ 28

(1) Integrita softwarového vybavení a informací musí být chráněna před působením škodlivého kódu.

(2) Softwarové a hardwarové vybavení systému musí být uvedeno v evidenci aktiv a smí být používáno pouze v souladu s podmínkami v uvedenými popisu bezpečnosti systému a provozní bezpečnostní směrnici.

(3) Analýza rizik a popis bezpečnosti systému stanoví požadavky na provádění zálohování softwarového vybavení a uložených informací. Záloha musí být uložena tak, aby nemohlo dojít k jejímu poškození, zničení nebo zneužití.

(4) Popis bezpečnosti systému stanoví postup odstranění utajovaných informací z hardwarového vybavení před jeho vyřazením z používání, případně před jeho zničením.

§ 29

(1) Servisní činnost musí provozovatel systému organizovat tak, aby nebyla ohrožena bezpečnost a nedošlo k porušení povinností ochrany utajovaných informací.

(2) V případech, kdy hrozí možnost neoprávněného seznámení s utajovanou informací, musí být z nosičů informací přístupných při servisní činnosti bezpečně vymazány utajované informace a dálková diagnostika musí být zabezpečena před zneužitím.

(3) Servis zařízení nebo komponent zajišťujících bezpečnostní funkce musí zajišťovat osoby splňující podmínky pro přístup fyzické osoby k utajované informaci nejvyššího stupně utajení, s níž je systém určen nakládat. Údržba ostatních zařízení nebo komponent může být prováděna i osobami nesplňujícími podmínky pro přístup k utajované informaci podle věty první, pokud jsou tyto osoby pod neustálým osobním dohledem příslušného pracovníka správy a jestliže byly schváleny odpovědnou osobou provozovatele systému, jí pověřenou osobou nebo bezpečnostním ředitelem.

§ 30

(1) V rámci provozu systému musí provozovatel systému provádět hodnocení auditních záznamů v termínech stanovených v popisu bezpečnosti systému a při vzniku krizové situace bez zbytečného odkladu.

(2) Auditní záznamy musí být chráněny před změnou nebo zničením a uchovávány po dobu stanovenou v popisu bezpečnosti systému, nejméně však po dobu 5 let od vzniku.

(3) V popisu bezpečnosti systému musí být uvedena základní klasifikace krizových situací a pro každou z nich musí být specifikována činnost

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

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

(4) Pro řešení krizových situací musí být v popisu bezpečnosti systému stanovena bezpečnostní opatření zaměřená na uvedení systému do stavu odpovídajícího bezpečnostní dokumentaci.

(5) Při zvládání bezpečnostních událostí a bezpečnostních incidentů musí být

a) přijata nezbytná bezpečnostní opatření pro zajištění oznamování bezpečnostních událostí ze strany uživatelů a zajištění vedení záznamů o těchto oznámeních,

b) zajištěno prostředí pro provádění vyhodnocování oznámených bezpečnostních událostí a bezpečnostních událostí detekovaných technickými nástroji a pro identifikaci případných bezpečnostních incidentů,

c) provedena klasifikace bezpečnostních incidentů a přijata vhodná bezpečnostní opatření pro odvrácení a zmírnění dopadu bezpečnostních incidentů,

d) prošetřeny a určeny příčiny bezpečnostního incidentu, vyhodnocena účinnost řešení bezpečnostního incidentu a na základě vyhodnocení stanovena nutná bezpečnostní opatření k zamezení opakování daného bezpečnostního incidentu a

e) dokumentováno zvládání bezpečnostních incidentů.

(6) Pro případ havárie softwarového nebo hardwarového vybavení systému musí být uveden v popisu bezpečnosti systému způsob

a) zálohování a uložení záložních nosičů informací,

b) zajištění servisní činnosti,

c) zajištění nouzového provozu s vyjmenováním základních funkcí systému, které musí být zachovány, a

d) obnovy funkčnosti systému a uvedení do bezpečného stavu uvedeného v bezpečnostní dokumentaci.

§ 31

Pokud se na provozu, rozvoji nebo zajištění informační bezpečnosti podílí dodavatel, analýza rizik stanoví

a) zásady hodnocení rizik dodavatele,

b) náležitosti smlouvy s dodavatelem, kterými jsou smluvní ujednání o úrovni dodávaných služeb, o realizaci bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti, a

c) pravidla pro ověření bezpečnostních opatření zavedených dodavatelem.

§ 32

Popis bezpečnosti systému stanoví bezpečnostní opatření zaváděná za účelem ochrany utajovaných informací po ukončení provozu systému, zejména způsob naložení s nosiči informací a uložení kryptografických prostředků, jsou-li použity.

§ 33

Bezpečnostní požadavky na softwarové vybavení

(1) Popis bezpečnosti systému stanoví bezpečnostní funkce pro zajištění ochrany utajovaných informací zpracovávaných použitým softwarovým vybavením.

(2) Je-li v rámci provozu použito virtualizační prostředí, musí splňovat stejné bezpečnostní požadavky jako systémy provozované na jeho platformě.

§ 34

Zvláštní bezpečnostní požadavky na softwarové vybavení informačního systému

(1) Vyžaduje-li to činnost, pro kterou je informační systém zřízen, je v systému zajišťována nepopiratelnost provozovatelem informačního systému stanovených jednání či událostí, kterou se rozumí zajištění toho, že lze subjektu systému přičíst jím provedené předání informace nebo provedená změna stavu systému.

(2) Má-li být součástí informačního systému elektronický systém spisové služby sloužící k evidenci utajovaných informací, musí být hodnocení bezpečnosti softwarového vybavení, kterým je realizován, součástí procesu certifikace informačního systému.

§ 35

Bezpečnostní požadavky při nově identifikovaných hrozbách a zvýšení rizik

(1) Součástí analýzy rizik a popisu bezpečnosti informačního systému je i rozhodnutí Národního úřadu pro kybernetickou a informační bezpečnost o stanovení dalších nutných bezpečnostních funkcí nebo opatření podle § 34 odst. 4 zákona, bylo-li vydáno.

(2) Náležitosti oznámení provozovatele certifikovaného informačního systému o zavedení dalších nutných bezpečnostních funkcí nebo opatření podle § 34 odst. 4 zákona jsou

a) identifikační údaje provozovatele certifikovaného informačního systému,
b) jednoznačný identifikátor rozhodnutí podle § 34 odst. 4 zákona a
c) podrobnosti o zavedení bezpečnostní funkce nebo opatření, kterými jsou
    1. datum a čas zavedení,
    2. výsledek zavedení bezpečnostní funkce nebo opatření a
    3. popis problémů nebo negativních dopadů při zavádění bezpečnostní funkce nebo opatření.

ČÁST TŘETÍ

OBSAH DOKUMENTACE

§ 36

(1) Bezpečnostní dokumentaci systému tvoří
   a) projektová bezpečnostní dokumentace a
   b) provozní bezpečnostní dokumentace.

(2) Projektová bezpečnostní dokumentace obsahuje
   a) bezpečnostní politiku,
   b) analýzu rizik,
   c) popis bezpečnosti systému a
   d) dokumentaci k bezpečnostním testům.

(3) Provozní bezpečnostní dokumentace obsahuje
   a) provozní bezpečnostní směrnice pro každou zavedenou roli,
   b) evidence aktiv systému, zejména nosičů informací,
   c) evidenci uživatelů,
   d) provozní deníky a
   e) další provozní bezpečnostní dokumentaci definovanou v projektové bezpečnostní dokumentaci.

§ 37

Bezpečnostní politika

(1) Bezpečnostní politika
   a) je tvořena souborem obecných pravidel a postupů, který vymezuje způsob, jakým má být zajištěna informační bezpečnost a odpovědnost uživatele za jeho činnost v systému, který je konkretizován jako bezpečnostní opatření v popisu bezpečnosti systému,
   b) obsahuje prohlášení odpovědné osoby nebo bezpečnostního ředitele o naplnění požadavků právních předpisů z oblasti ochrany utajovaných informací a
   c) stanoví způsob zajištění pravosti a nepopiratelnosti informací, je-li to nutné.

(2) U informačního systému musí být bezpečnostní politika průběžně přezkoumávána, vyhodnocována a aktualizována, nejpozději však bezprostředně před podáním opakované žádosti o certifikaci podle § 48.

§ 38

Analýza rizik

(1) Pro účely analýzy rizik se rozumí
   a) hrozbou potenciální příčina bezpečnostního incidentu,
   b) zranitelností slabé místo aktiva systému, které může být využito hrozbou,
   c) rizikem kombinace pravděpodobnosti události a jejího následku jako souhrnu možností, že hrozba využije zranitelnost a způsobí škodu.

(2) Analýza rizik vychází z bezpečnostní politiky a u informačního systému i ze stanoveného bezpečnostního provozního módu.

(3) Analýza rizik obsahuje

a) provozovatelem systému stanovenou metodiku pro identifikaci a hodnocení aktiv systému a pro identifikaci a hodnocení rizik včetně stanovených kritérií pro přijatelnost rizik,

b) identifikaci a hodnocení aktiv systému z hlediska hrozeb, zranitelností a dopadů,

c) kvantifikaci rizik, která zohledňuje hrozby, zranitelnosti a dopady,

d) určenou a akceptovatelnou míru rizika a

e) přehled navržených bezpečnostních opatření.

(4) U informačního systému musí být analýza rizik přezkoumávána, vyhodnocována a aktualizována, nejpozději však bezprostředně před podáním opakované žádosti o certifikaci podle § 48.

§ 39

Popis bezpečnosti systému

(1) Popis bezpečnosti systému popisuje aplikaci bezpečnostních opatření navržených v analýze rizik pro splnění požadavků definovaných v bezpečnostní politice, včetně řešení kryptografické ochrany, pokud je aplikována. Popis bezpečnosti systému musí být konkrétní a přesný.

(2) U rozsáhlých systémů lze popis bezpečnosti systému rozdělit do několika samostatných dokumentů, které popisují konkrétní řešení jednotlivých částí systému, zpravidla na úrovni poskytovaných služeb.

§ 40

Dokumentace k bezpečnostním testům

Dokumentace k bezpečnostním testům obsahuje souhrn bezpečnostních testů a jejich výsledků z oblasti plnění bezpečnostních opatření navržených v analýze rizik a popsaných v popisu bezpečnosti systému.

§ 41

Provozní bezpečnostní směrnice

(1) Pro každou definovanou roli v systému musí být zpracována provozní bezpečnostní směrnice.

(2) Provozní bezpečnostní směrnice pro každou roli stanoví

a) práva uživatele v roli,

b) povinnosti uživatele v roli,

c) zakázané činnosti uživatele v roli a

d) postupy spojené s povinnostmi, právy a zakázanými činnostmi podle písmen a) až c).

(3) Provozní bezpečnostní směrnice pro roli koncového uživatele obsahuje také

a) stručný a zjednodušený popis systému včetně jeho rozsahu a případného umístění,

b) definici a klasifikaci krizových situací včetně základního popisu toho, jak se koncový uživatel podílí na jejich řešení,

c) definici a klasifikaci bezpečnostních událostí a incidentů včetně základního popisu toho, jak se koncový uživatel podílí na jejich řešení,
d) definici kompromitace utajované informace při použití kryptografického prostředku včetně základního popisu toho, jak se uživatel podílí na řešení,
e) způsob manipulace s nosiči informací a způsob jejich používání,
f) pravidla provádění tisku a
g) způsob používání specifického softwarového vybavení.

§ 42

Evidence aktiv

(1) Veškerá aktiva systému musí být evidována v evidenci aktiv.

(2) Záznam v evidenci aktiv musí obsahovat přesný název, typ, sériové nebo výrobní číslo aktiva a další informace, které umožní jednoznačnou identifikaci evidovaného aktiva.

(3) Evidovaná hmotná aktiva musí být, kromě výjimek uvedených v bezpečnostní dokumentaci, označena tak, aby byla jednoznačně určena jejich příslušnost k systému.

(4) Evidence nosičů informací obsahuje položky:
a) pořadové číslo,
b) stupeň utajení nebo informaci o tom, že nosič informací je neutajovaný,
c) evidenční označení, které tvoří zkratka stupně utajení, je-li nosič informací utajovaný, nebo zkratka informace o tom, že nosič informací je neutajovaný, pořadové číslo, rok zavedení do evidence a identifikaci provozovatele systému,
d) datum zavedení do evidence,
e) typ nosiče informací,
f) jednoznačný identifikátor nosiče informací, kterým je zpravidla sériové číslo, a
g) jméno, příjmení a podpis uživatele, kterému byl nosič informací přidělen, datum převzetí, datum vrácení nosiče informací a jméno, příjmení a podpis uživatele, kterému byl nosič informací vrácen.

(5) Evidence nosičů informací může být vedena i samostatně mimo provozní bezpečnostní dokumentaci. Způsob vedení evidence nosičů informací podle věty první je uveden v bezpečnostní dokumentaci.

§ 43

Evidence uživatelů

(1) Každý uživatel musí být evidován v evidenci uživatelů.

(2) Evidence uživatelů obsahuje
a) jméno a příjmení uživatele,
b) údaje o oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené, zejména datum jeho vydání; to neplatí, má-li uživatel přístup k utajované informaci stupně utajení Vyhrazené podle § 58a zákona,
c) údaje o osvědčení fyzické osoby, bylo-li uživateli vydáno, kterými se rozumí číslo

osvědčení, datum vydání, doba platnosti osvědčení a nejvyšší stupeň utajení utajovaných informací, ke kterým osvědčení umožňuje přístup,

d) údaje o osvědčení fyzické osoby pro cizí moc, bylo-li uživateli vydáno, kterými se rozumí číslo osvědčení, datum vydání, doba platnosti osvědčení a nejvyšší stupeň utajení utajovaných informací, ke kterým osvědčení umožňuje přístup, a

e) údaje o roli, kterou byl uživatel pověřen, zejména o rozsahu jeho oprávnění, datu pověření a datu zrušení pověření a datu proškolení podle § 19 odst. 5.

(3) V případě, že má uživatel přístup k utajované informaci podle § 58 zákona, nebo k utajované informaci stupně utajení Vyhrazené podle § 58a zákona, jsou tyto údaje uvedeny v evidenci uživatelů.

§ 44

Provozní deník

(1) Provozní deník slouží k řízení změn v systému a jejich zadokumentování. Do provozního deníku se zaznamenávají zejména změny prováděné v systému pracovníky správy.

(2) Provozní deník lze vést i v elektronické podobě, je-li zabezpečen proti neoprávněnému přístupu nebo zásahu a prokazatelným způsobem zaznamenává všechny v něm prováděné změny.

ČÁST ČTVRTÁ

CERTIFIKACE A AKREDITACE INFORMAČNÍHO SYSTÉMU A SCHVALOVÁNÍ PROJEKTU BEZPEČNOSTI

HLAVA I

Informační systém

Díl 1

Certifikace informačního systému

§ 45

Žádost o certifikaci informačního systému

(1) Žádost o certifikaci informačního systému obsahuje

a) číslo osvědčení podnikatele s uvedením příslušného stupně utajení nebo kopii platného prohlášení podnikatele, je-li žadatelem podnikatel,

b) jméno a příjmení kontaktní osoby žadatele a kontaktní spojení, kterým se rozumí alespoň její telefonní číslo a adresa elektronické pošty,

c) popis účelu a rozsahu informačního systému,

d) údaj o stupni utajení utajovaných informací, se kterými bude informační systém nakládat,

e) údaj o stanovení bezpečnostního provozního módu informačního systému a

f) identifikační údaje dodavatele informačního systému nebo jeho komponent ovlivňujících bezpečnost informačního systému a číslo osvědčení podnikatele s uvedením příslušného stupně utajení nebo kopii platného prohlášení podnikatele, je-li dodavatel podnikatelem.

(2) K provedení certifikace informačního systému žadatel předloží

a) žádost o certifikaci informačního systému podle odstavce 1,

b) projektovou bezpečnostní dokumentaci podle § 36 odst. 2,

c) provozní bezpečnostní dokumentaci v rozsahu § 36 odst. 3 písm. a),

d) popis bezpečnosti vývojového prostředí a

e) další podklady obsahující informace, které by mohly mít vliv na posuzování bezpečnosti informačního systému nebo jeho provoz.

(3) K provedení certifikace informačního systému nakládajícího s utajovanými informacemi stupně utajení Důvěrné nebo vyššího žadatel předloží podklady nezbytné k ověření způsobilosti elektrických nebo elektronických zařízení, které jsou součástí informačního systému, k ochraně před únikem utajovaných informací kompromitujícím vyzařováním.

(4) K žádosti žadatel přiloží výsledky dílčích úloh v rámci ověřování způsobilosti informačního systému k nakládání s utajovanými informacemi, provedených orgánem státu, právnickou osobou podle § 60b zákona nebo podnikatelem na základě smlouvy o zajištění činnosti uzavřené s Národním úřadem pro kybernetickou a informační bezpečnost podle § 52 zákona, byly-li tyto dílčí úlohy provedeny.

(5) Zpravodajská služba uvádí v žádosti podle odstavce 1 údaje podle písmen c) až f) pouze v rozsahu, který neohrozí plnění jejích úkolů podle jiného právního předpisu. Zpravodajská služba předkládá podklady podle odstavce 2 pouze v rozsahu, který neohrozí plnění jejích úkolů podle jiného právního předpisu.

§ 46

Způsob a podmínky provádění certifikace informačního systému

(1) V rámci certifikace informačního systému posuzuje Národní úřad pro kybernetickou a informační bezpečnost

a) vhodnost navrženého souboru bezpečnostních opatření pro dosažení informační bezpečnosti informačního systému podle § 3,

b) správnost a úplnost bezpečnostní dokumentace a

c) správnost realizace navrženého souboru bezpečnostních opatření v daném informačním systému a její soulad s bezpečnostní dokumentací.

(2) Certifikace informačního systému se provádí na základě předložených podkladů a provedených bezpečnostních testů. Bezpečnostní testy provádí žadatel o certifikaci informačního systému v provozním prostředí hodnoceného informačního systému za spoluúčasti Národního úřadu pro kybernetickou a informační bezpečnost, případně i dodavatele. Provádí-li bezpečnostní testy podle věty druhé zpravodajská služba, spoluúčast Národního úřadu pro kybernetickou a informační bezpečnosti se nevyžaduje.

(3) Certifikaci informačního systému lze provádět průběžně po ukončení jednotlivých fází výstavby informačního systému nebo až po jejím dokončení, uvede-li to žadatel v žádosti o certifikaci informačního systému podle § 45.

(4) Dojde-li v informačním systému, který byl certifikován a schválen do provozu, ke změnám uvedeným v § 51 odst. 2, provádí se pouze doplňující posouzení informačního systému v rozsahu provedených změn. Při provádění doplňujícího posouzení informačního systému se postupuje podle odstavce 1 v nezbytném rozsahu. Výsledek doplňujícího posouzení je součástí certifikační zprávy.

(5) Vzor certifikátu informačního systému je uveden v příloze č. 2 k této vyhlášce.

§ 47

Certifikační zpráva

Národní úřad pro kybernetickou a informační bezpečnost vydává k certifikátu informačního systému certifikační zprávu, která obsahuje

a) identifikaci informačního systému obsahující jeho název, označení verze a stupeň utajení utajovaných informací, pro který byla způsobilost informačního systému ověřena,
b) popis informačního systému,
c) zásady a podmínky provozování informačního systému, včetně typů změn informačního systému, které vyžadují provedení doplňujícího posouzení informačního systému, a podmínek ukončení jeho provozu,
d) identifikaci přijatelných rizik souvisejících s provozem informačního systému a
e) typy kryptografických prostředků, jsou-li použity, a způsob, jakým bude zajištěn výkon kryptografické ochrany v souladu s certifikační zprávou kryptografického prostředku.

§ 48

Opakovaná žádost o certifikaci informačního systému

(1) Opakovaná žádost o certifikaci informačního systému obsahuje

a) číslo osvědčení podnikatele s uvedením příslušného stupně utajení nebo kopii platného prohlášení podnikatele, je-li provozovatelem informačního systému podnikatel,
b) identifikaci vydaného certifikátu informačního systému obsahující identifikaci 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 způsobilost informačního systému ověřena, a
d) jméno a příjmení kontaktní osoby provozovatele informačního systému a kontaktní spojení na ni.

(2) Opakovaná žádost o certifikaci informačního systému dále obsahuje návrh změny bezpečnostní dokumentace, pokud ji ke dni ukončení platnosti dosavadního certifikátu provozovatel informačního systému navrhuje.

(3) Pokud v opakované žádosti provozovatel informačního systému doloží, že ke dni ukončení platnosti dosavadního certifikátu informačního systému bude informační systém provozován za podmínek stanovených v certifikační zprávě a v jeho provozování nenastaly změny, je rozsah posuzování podle § 46 odst. 1 omezen pouze na písmeno c).

(4) Pokud v opakované žádosti provozovatel informačního systému navrhuje změnu bezpečnostní dokumentace, je rozsah posuzování podle § 46 odst. 1 písm. a) a b) omezen na tyto navrhované změny.

(5) Pokud navrhované změny bezpečnostní dokumentace informačního systému jsou podstatné pro celkovou bezpečnost informačního systému, bude Národní úřad pro kybernetickou a informační bezpečnost postupovat jako v případě nové certifikace.

(6) Zpravodajská služba uvádí v žádosti podle odstavce 1 údaje podle písmen c) a d) pouze v rozsahu, který neohrozí plnění jejích úkolů podle jiného právního předpisu. Zpravodajská služba předkládá podklady podle odstavce 2 pouze v rozsahu, který neohrozí plnění jejích úkolů podle jiného právního předpisu.

Díl 2
Smlouva o zajištění činnosti

§ 49

(1) Žádost o uzavření smlouvy s Národním úřadem pro kybernetickou a informační bezpečnost o zajištění činnosti podle § 52 zákona, jejímž předmětem je provádění dílčích úloh při ověřování způsobilosti informačního systému k nakládání s utajovanými informacemi (dále jen „smlouva o zajištění činnosti“), obsahuje

a) číslo osvědčení podnikatele s uvedením příslušného stupně utajení, je-li žadatelem podnikatel,

b) jméno a příjmení kontaktní osoby žadatele a kontaktní spojení na ni a

c) specifikace činností, které mají být prováděny podle smlouvy o zajištění činnosti.

(2) Žádost dle odstavce 1 obsahuje dále

a) adresu umístění pracoviště provádějícího požadované činnosti,

b) prohlášení odpovědné osoby nebo jí pověřené osoby o splnění požadavků na fyzickou a personální bezpečnost pracoviště,

c) rozsah požadovaných činností,

d) údaje o personálním zabezpečení požadovaných činností a

e) údaje o technickém a organizačním zajištění požadovaných činností.

Díl 3
Akreditace informačního systému

§ 50

(1) Akreditaci informačního systému cizí moci provádí Národní úřad pro kybernetickou a informační bezpečnost na žádost, která obsahuje prohlášení o naplnění bezpečnostních požadavků vyžadovaných bezpečnostní akreditační autoritou cizí moci podle příslušného předpisu Evropské unie[2]) a podle mezinárodní smlouvy[3]).

(2) Pokud Národní úřad pro kybernetickou a informační bezpečnost ověří naplnění bezpečnostních požadavků vyžadovaných bezpečnostní akreditační autoritou cizí moci, předá prohlášení podle odstavce 1 bezpečnostní akreditační autoritě cizí moci.

(3) Na základě rozhodnutí bezpečnostní akreditační autority cizí moci o akreditaci informačního systému cizí moci Národní úřad pro kybernetickou a informační bezpečnost informační systém cizí moci akredituje.

(4) Pokud má být informační systém cizí moci používán i bezprostředně po uplynutí doby platnosti jeho akreditace, požádá jeho provozovatel o opakovanou akreditaci informačního systému podle odstavce 1 obdobně nejpozději 6 měsíců před koncem platnosti akreditace informačního systému cizí moci.

Díl 4
Podmínky bezpečného provozování informačního systému

§ 51

(1) Podmínky bezpečného provozování informačního systému spočívají v

a) dodržování bezpečnostních opatření,

b) dodržování podmínek provozování informačního systému stanovených v certifikační zprávě a

c) informování Národního úřadu pro kybernetickou a informační bezpečnost o významné změně týkající se provozu informačního systému, která by mohla mít vliv na informační bezpečnost.

(2) Pokud v rámci provozu informačního systému dojde ke změně podle odstavce 1 písmene c) nebo ke změně podle § 47 písm. c), musí být taková změna bez zbytečného odkladu zohledněna v bezpečnostní dokumentaci, zejména v analýze rizik.

HLAVA II
Komunikační systém

§ 52

Náležitosti projektu bezpečnosti

(1) Projekt bezpečnosti obsahuje bezpečnostní dokumentaci, a to alespoň v rozsahu § 36 odst. 2 písm. a) až c) a odst. 3 písm. a).

(2) Popis bezpečnosti podle § 39 obsahuje pro komunikační systém popis

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

b) bezpečnostní správy kryptografické ochrany v souladu s certifikační zprávou kryptografického prostředku a

c) bezpečnostních opatření a zásad provozních postupů, jejichž naplňováním bude zajištěna informační bezpečnost.

(3) Bezpečnostní směrnice jednotlivých rolí obsahují pro komunikační systém

a) požadavky uvedené v § 41 a

b) popis konkrétních provozních postupů pro zajištění bezpečnostní správy komunikačního systému a výkonu kryptografické ochrany.

(4) Popis bezpečnosti komunikačního systému, který pro zajištění komunikace a řízení používá prvky výpočetní techniky, musí obsahovat popis komunikační infrastruktury a popis informační infrastruktury.

§ 53

Žádost o schválení projektu bezpečnosti

(1) Žádost o schválení projektu bezpečnosti obsahuje

a) jméno a příjmení kontaktní osoby žadatele a kontaktní spojení na ni,

b) číslo osvědčení podnikatele s uvedením příslušného stupně utajení nebo kopii platného prohlášení podnikatele, je-li provozovatelem komunikačního systému podnikatel,

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

d) údaj o stupni utajení utajovaných informací, se kterými bude komunikační systém nakládat,

e) identifikační údaje dodavatele jednotlivých komponent komunikačního systému majících vliv na bezpečnost komunikačního systému a číslo osvědčení podnikatele s uvedením příslušného stupně utajení nebo kopii platného prohlášení podnikatele, je-li dodavatel podnikatelem, a

f) projekt bezpečnosti.

(2) Ke schválení projektu bezpečnosti komunikačního systému nakládajícího s utajovanými informacemi stupně utajení Důvěrné nebo vyššího žadatel předloží podklady nezbytné k ověření způsobilosti elektrických nebo elektronických zařízení, které jsou součástí komunikačního systému, k ochraně před únikem utajovaných informací kompromitujícím vyzařováním.

(3) Pokud žadatel poskytuje jednotlivé části projektu bezpečnosti v průběhu jeho schvalování postupně, musí je předkládat v pořadí podle § 36.

(4) Zpravodajská služba uvádí v žádosti podle odstavce 1 údaje podle písmen c) až f) pouze v rozsahu, který neohrozí plnění jejích úkolů podle jiného právního předpisu. Zpravodajská služba předkládá podklady podle odstavce 2 pouze v rozsahu, který neohrozí plnění jejích úkolů podle jiného právního předpisu.

§ 54

Způsob a podmínky schvalování projektu bezpečnosti

(1) V rámci schvalování projektu bezpečnosti posuzuje Národní úřad pro kybernetickou a informační bezpečnost

a) vhodnost navrženého souboru bezpečnostních opatření pro dosažení informační bezpečnosti komunikačního systému podle § 3,

b) správnost a úplnost bezpečnostní dokumentace a

c) správnost realizace navrženého souboru bezpečnostních opatření v daném komunikačním systému a její soulad s bezpečnostní dokumentací.

(2) Schvalování projektu bezpečnosti se provádí posouzením podkladů předložených provozovatelem komunikačního systému a posouzením správnosti realizace projektu bezpečnosti Národ-

ním úřadem pro kybernetickou a informační bezpečnost v provozním prostředí schvalovaného komunikačního systému.

(3) Schvalování projektu bezpečnosti lze provádět průběžně po ukončení jednotlivých fází výstavby komunikačního systému nebo až po jejím celkovém dokončení, podle požadavků žadatele, zažádá-li o to v žádosti o schválení projektu bezpečnosti podle § 53.

(4) Zjistí-li Národní úřad pro kybernetickou a informační bezpečnost při schvalování projektu bezpečnosti způsobilost hodnoceného komunikačního systému k nakládání s utajovanými informacemi, vydá rozhodnutí o schválení projektu bezpečnosti.

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

HLAVA III
Posuzování modulů

§ 55

(1) V rámci certifikace informačního systému nebo schvalování projektu bezpečnosti lze rozdělit existující informační nebo komunikační systém na moduly, které mohou být bez dalšího posuzování obdobně použity i v jiných informačních nebo komunikačních systémech podle § 46 nebo 54 při zachování stejné úrovně informační bezpečnosti.

(2) Modul je funkční celek tvořený

a) softwarovým vybavením, zejména elektronickým systémem spisové služby, sloužícím k evidenci utajovaných informací,

b) hardwarovým vybavením, zejména zástavbou kryptografického prostředku v systému, nebo

c) kombinací softwarového a hardwarového vybavení, zejména bezpečnostním oddělovacím blokem,

jestliže má jasně definované hranice určující způsob jeho začlenění do systému.

(3) Národní úřad pro kybernetickou a informační bezpečnost při posuzování jiného systému podle § 46 odst. 3 a § 54 odst. 1 a 2 nehodnotí modul, jestliže modul

a) byl posouzen a použit v již existujícím systému podle § 46 nebo 54 a

b) má být obdobně použit v jiném systému ve stejné konfiguraci a za stejných podmínek jako v jiném již existujícím systému podle písmene a).

ČÁST PÁTÁ

SAMOSTATNÁ ELEKTRONICKÁ ZAŘÍZENÍ

§ 56

Podmínky bezpečného provozování samostatného elektronického zařízení

(1) Podmínkou bezpečného provozování samostatného elektronického zařízení podle § 36 odst. 4 zákona je zpracování bezpečnostní provozní směrnice obsahující bezpečnostní dokumentaci alespoň v rozsahu § 36 odst. 2 písm. c) a odst. 3 písm. a).

(2) Popis bezpečnosti systému podle § 36 odst. 2 písm. c) stanoví způsob bezpečného provozování s ohledem na funkci samostatného elektronického zařízení a způsob ukládání zpracovávané utajované informace a identifikuje samostatné elektronické zařízení podle funkce jako

a) zobrazovací, které zobrazuje utajované informace,

b) zaznamenávací, které zaznamenává utajované informace v různých formátech, zejména psací stroj s pamětí, fotoaparát, kamera nebo záznamník,

c) kopírovací a převodní, které kopíruje nebo převádí utajované informace z jednoho formátu do druhého, a

d) kombinované, které kombinuje funkce uvedené v písmenech a) až c).

(3) Obsahuje-li samostatné elektronické zařízení nosič informací, pak popis bezpečnosti systému obsahuje i jeho identifikaci podle způsobu zapojení do zařízení podle § 13 odst. 3.

(4) Pokud provozovatel samostatného elektronického zařízení provozuje více samostatných elektronických zařízení stejného typu podle funkce a způsobu integrace nosiče informací, pak může zpracovat jednu bezpečnostní provozní směrnici pro daný typ samostatného elektronického zařízení.

§ 57

Oznámení o provozovaném samostatném elektronickém zařízení podle § 36 odst. 2 písm. b) zákona obsahuje

a) identifikační údaje provozovatele samostatného elektronického zařízení a

b) seznam provozovaných samostatných elektronických zařízení obsahující pro každé provozované samostatné elektronické zařízení

1. typ samostatného elektronického zařízení podle § 56 odst. 2 a 3 a

2. stupeň utajení utajovaných informací, pro něž je určeno.

ČÁST ŠESTÁ

PŘECHODNÁ A ZÁVĚREČNÁ USTANOVENÍ

§ 58

Přechodná ustanovení

(1) Bezpečnostní požadavky na

a) informační systémy certifikované před účinností této vyhlášky a

b) komunikační systémy, jejichž projekt bezpečnosti byl schválen přede dnem nabytí účinnosti této vyhlášky,

se posuzují podle dosavadních právních předpisů.

(2) Požadavky na ochranu utajovaných informací v elektronické podobě v samostatných elektronických zařízeních, která byla uvedena do provozu přede dnem nabytí účinnosti této vyhlášky, se řídí dosavadními právními předpisy po dobu 1 roku ode dne nabytí účinnosti této vyhlášky.

(3) Uživatelé, kteří nesplňují podmínky pro přístup fyzické osoby k utajované informaci podle § 17 odst. 2, musí tuto podmínku splnit nejpozději do 12 měsíců ode dne nabytí účinnosti této vyhlášky.

§ 59

Zrušovací ustanovení

Zrušují se:

1. Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.
2. Vyhláška č. 453/2011 Sb., 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.

ČÁST SEDMÁ

ÚČINNOST

§ 60

Tato vyhláška nabývá účinnosti dnem 1. ledna 2025.

Ředitel:
Ing. Kintr v. r.

Příloha č. 1

Fyzická bezpečnost

Pro potřeby výpočtu bodových hodnot zabezpečených oblastí, v nichž se nachází části informačního systému, komunikačního systému nebo samostatného elektronického zařízení obsahující v sobě nosiče informací, které pro uchování informace nepotřebují trvalé připojení ke zdroji elektrické energie, se použijí následující hodnoty parametru S1.

S1

Tabulka č. 1: Bezpečnostní ekvivalent parametru S1

Hodnota S1	**Popis autentizace subjektu systému**
0	bez autentizace*
1	identifikace jménem a autentizace heslem a systém ani data nejsou šifrovaná
2	identifikace jménem a autentizace heslem zaslaným jiným kanálem a systém ani data nejsou šifrovaná
2	autentizace předmětem s osobním identifikačním číslem (PIN) a systém ani data nejsou šifrovaná
2	autentizace pomocí biometrických charakteristik a systém ani data nejsou šifrovaná
2	identifikace jménem a autentizace heslem a celý systém nebo data jsou šifrovaná**
3	identifikace jménem a autentizace heslem zaslaným jiným kanálem a celý systém nebo data jsou šifrovaná**
3	autentizace předmětem s osobním identifikačním číslem (PIN) a celý systém nebo data jsou šifrovaná**
3	autentizace pomocí biometrických charakteristik a celý systém nebo data jsou šifrovaná**
4	autentizace předmětem s šifrovaným*** obsahem s osobním identifikačním číslem (PIN) a systém ani data nejsou šifrovaná
4	autentizace předmětem s šifrovaným*** obsahem s osobním identifikačním číslem (PIN) a přenosem a systém ani data nejsou šifrovaná
5	autentizace předmětem s šifrovaným*** obsahem s osobním identifikačním číslem (PIN) a celý systém nebo data jsou šifrovaná**
5	autentizace předmětem s šifrovaným*** obsahem s osobním identifikačním číslem (PIN) a přenosem a celý systém nebo data jsou šifrovaná**

* pouze pro samostatná elektronická zařízení
** způsob a mechanismus šifrování dat vyplývá z projektové bezpečnostní dokumentace
*** kryptografické mechanismy pro šifrování předmětu vyplývají z projektové bezpečnostní dokumentace

Příloha č. 2

Vzor certifikátu

NÁRODNÍ ÚŘAD
PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

Národní úřad pro kybernetickou a informační bezpečnost příslušný podle § 137a písm. e) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

vydává

CERTIFIKÁT

informačního systému
podle § 46 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Evidenční číslo certifikátu: .....

.....
(název, verze)

Držitel certifikátu: Adresa: IČO:

Tento certifikát potvrzuje ověření a schválení způsobilosti informačního systému k nakládání s utajovanými informacemi do a včetně stupně utajení

.....

Platnost od:
Platnost do:

otisk úředního razítka

.....
podpis oprávněného zástupce

Datum vydání:
Přílohy:

[1]) Rozhodnutí Komise (EU, Euratom) 2021/259 ze dne 10. února 2021, kterým se stanoví prováděcí pravidla pro průmyslovou bezpečnost s ohledem na utajované granty.

Rozhodnutí Rady (EU) 2013/488/EU ze dne 23. září 2013 o bezpečnostních pravidlech na ochranu utajovaných informací EU, v platném znění.

[2]) Rozhodnutí Rady 2013/488/EU.

[3]) Dohoda mezi smluvními stranami Severoatlantické smlouvy o bezpečnosti informací, vyhlášená pod č. 75/2001 Sb. m. s.

ISSN 3029-5092

Vydavatel: Ministerstvo vnitra, Nad Štolou 3, poštovní schránka 21, 170 34 Praha 7 • **Redakce Sbírky zákonů a mezinárodních smluv**: Ministerstvo vnitra, nám. Hrdinů 1634/3, poštovní schránka 155/SB, 140 21, Praha 4, telefon: 974 817 289, e-mail: sbirka@mvcr.cz • Sazba: Tiskárna Ministerstva vnitra, Bartůňkova 1159/4, poštovní schránka 10, 149 00 Praha 11-Chodov • **Právně závazná elektronická verze Sbírky zákonů a mezinárodních smluv je k dispozici na www.e-sbirka.cz** • Tištěnou verzi částky Sbírky zákonů a mezinárodních smluv lze objednat u Tiskárny Ministerstva vnitra, telefon: 974 887 312, e-mail: info@tmv.cz, www.tmv.cz • Předplatné je od 1. 1. 2024 ukončeno.