

412/2005 Sb.

ZÁKON

ze dne 21. září 2005

o ochraně utajovaných informací a o bezpečnostní způsobilosti

ve znění zákona č. 119/2007 Sb., zákona č. 177/2007 Sb., zákona č. 296/2007 Sb., zákona č. 32/2008 Sb., zákona č. 124/2008 Sb., zákona č. 126/2008 Sb.,

zákona č. 250/2008 Sb., zákona č. 41/2009 Sb., zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 255/2011 Sb., zákona č. 420/2011 Sb., zákona č. 458/2011 Sb.,

zákona č. 167/2012 Sb., zákona č. 303/2013 Sb., zákona č. 181/2014 Sb., zákona č. 250/2014 Sb., zákona č. 204/2015 Sb., zákona č. 375/2015 Sb., zákona č. 135/2016 Sb., zákona č. 298/2016 Sb.,

zákona č. 183/2017 Sb. a zákona č. 205/2017 Sb.

(zkráceno - text neobsahující změny byl vypuštěn)

HLAVA VI

BEZPEČNOST INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMŮ

§ 33a

Státní správu v oblasti ochrany utajovaných informací podle této hlavy vykonává Národní úřad pro kybernetickou a informační bezpečnost, pokud tento zákon nestanoví jinak.

§ 34

Informační systém

(1) Informačním systémem nakládajícím s utajovanými informacemi se pro účely tohoto zákona rozumí jeden nebo více počítačů, jejich programové vybavení, k tomu patřící periferní zařízení, správa tohoto informačního systému a k tomuto systému se vztahující procesy nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací (dále jen "informační systém").

(2) Informační systém musí být certifikován Národním úřadem pro kybernetickou a informační bezpečnost [§ 46 odst. 1 písm. b)] a písemně schválen do provozu odpovědnou osobou nebo jí pověřenou osobou.

(3) Informační systém podnikatele, který má přístup k utajovaným informacím stupně utajení Vyhrazené, může být schválen do provozu jen v době platnosti prohlášení podnikatele; zánikem platnosti prohlášení podnikatele zaniká též schválení informačního systému do provozu.

(4) Nakládat s utajovanou informací lze pouze v informačním systému splňujícím podmínky podle odstavce 2 nebo 3.

(5) Schválení informačního systému do provozu podle odstavce 2 musí odpovědná osoba nebo jí pověřená osoba písemně oznámit Národnímu úřadu pro kybernetickou a informační bezpečnost do 30 dnů od tohoto schválení.

(zkráceno - text neobsahující změny byl vypuštěn)

§ 35

Komunikační systém

(1) Komunikačním systémem nakládajícím s utajovanými informacemi (dále jen "komunikační systém") se pro účely tohoto zákona rozumí systém zajišťující přenos těchto informací mezi koncovými uživateli a zahrnující koncové komunikační zařízení, přenosové prostředí, kryptografické prostředky, obsluhu a provozní podmínky a postupy.

(2) Komunikační systém nelze provozovat bez projektu bezpečnosti komunikačního systému schváleného Národním úřadem pro kybernetickou a informační bezpečnost. O schválení projektu bezpečnosti komunikačního systému písemně žádá u Národního úřadu pro kybernetickou a informační bezpečnost orgán státu, právnická osoba nebo podnikající fyzická osoba, která jej bude provozovat.

(zkráceno - text neobsahující změny byl vypuštěn)

HLAVA VII OCHRANA UTAJOVANÝCH INFORMACÍ PŘI ZPRACOVÁNÍ V ELEKTRONICKÉ PODOBĚ V ZAŘÍZENÍ, KTERÉ NENÍ SOUČÁSTÍ INFORMAČNÍHO NEBO KOMUNIKAČNÍHO SYSTÉMU

§ 36a

Státní správu v oblasti ochrany utajovaných informací podle této hlavy vykonává Národní úřad pro kybernetickou a informační bezpečnost, pokud tento zákon nestanoví jinak.

§ 36

(zkráceno - text neobsahující změny byl vypuštěn)

HLAVA VIII KRYPTOGRAFICKÁ OCHRANA

§ 37

(1) Kryptografickým materiálem je kryptografický prostředek, materiál k zajištění jeho funkce nebo kryptografický dokument.

(2) Kryptografické prostředky používané pro kryptografickou ochranu utajovaných informací musí být certifikovány Národním úřadem pro kybernetickou a informační bezpečnost [§ 46 odst. 1 písm. c)].

(3) Kryptografickým pracovištěm je pracoviště určené k výrobě nebo testování materiálu k zajištění funkce kryptografického prostředku, ukládání kryptografického materiálu nebo k distribuci a evidenci kryptografického materiálu nebo k výrobě a testování kryptografických prostředků. Kryptografické pracoviště musí splňovat bezpečnostní standardy a musí být do provozu schváleno odpovědnou osobou nebo bezpečnostním ředitelem.

(4) Kryptografické pracoviště určené k výrobě nebo testování materiálu k zajištění funkce kryptografického prostředku nebo které je centrálním distribučním a evidenčním místem kryptografického materiálu k zajištění funkce kryptografického prostředku orgánu státu, právnické osoby nebo podnikající fyzické osoby, musí být před schválením do provozu odpovědnou osobou nebo bezpečnostním ředitelem certifikováno Národním úřadem pro kybernetickou a informační bezpečnost [§ 46 odst. 1 písm. d)].

(zkráceno - text neobsahující změny byl vypuštěn)

§ 37a

Kontrolovaná kryptografická položka

(1) Kontrolovanou kryptografickou položkou se rozumí neutajované zařízení nebo jeho součást, zařazené do seznamu podle odstavce 3, sloužící k ochraně informací při jejich zpracování nebo přenosu a využívající kryptografických metod.

(2) Kontrolovanou kryptografickou položku lze použít pouze v souladu s bezpečnostním standardem.

(3) Zařízení uvedené v odstavci 1 nebo jeho součást na základě písemné žádosti jeho výrobce, dovozce, distributora nebo uživatele Národní úřad pro kybernetickou a informační bezpečnost schválí a zařadí do jím vedeného seznamu kontrolovaných kryptografických položek v případě, že je to v souladu se záměry České republiky v oblasti zajišťování ochrany utajovaných informací.

§ 38

Výkon kryptografické ochrany

(1) Výkonem kryptografické ochrany se rozumí

- a) její bezpečnostní správa,
- b) speciální obsluha kryptografického prostředku, nebo
- c) výroba nebo servis kryptografického prostředku nebo materiálu k zajištění jeho funkce.

(zkráceno - text neobsahující změny byl vypuštěn)

§ 39

Zvláštní odborná způsobilost pracovníka kryptografické ochrany a zkouška zvláštní odborné způsobilosti

(1) Zvláštní odborná způsobilost pracovníka kryptografické ochrany (dále jen "zvláštní odborná způsobilost") zahrnuje znalost předpisů z oblasti kryptografické ochrany utajovaných informací, schopnost jejich aplikace a další schopnosti podle § 38 odst. 1. Tyto znalosti a schopnosti ověřuje Národní úřad pro kybernetickou a informační bezpečnost zkouškou zvláštní odborné způsobilosti (dále jen "odborná zkouška"). Odborná zkouška probíhá před zkušební komisí; to není podmínkou pro její část prováděnou podle odstavce 3 písm. b). Členy zkušební komise jmenuje odpovědná osoba nebo jí pověřená osoba Národního úřadu pro kybernetickou a informační bezpečnost nebo orgánu státu podle odstavce 3 písm. a). Tomu, kdo složil odbornou zkoušku, vydá Národní úřad pro kybernetickou a informační bezpečnost nebo orgán státu podle odstavce 3 písm. a) osvědčení o zvláštní odborné způsobilosti a vede o tom evidenci. Osvědčení o zvláštní odborné způsobilosti se vydává nejdéle na 5 let.

(2) Přihlášku k odborné zkoušce podává písemně odpovědná osoba orgánu státu nebo podnikatele u Národního úřadu pro kybernetickou a informační bezpečnost nebo u jím pověřeného orgánu státu. Odborná zkouška se musí konat do 6 měsíců od podání přihlášky. Národní úřad pro kybernetickou a informační bezpečnost nebo jím pověřený orgán státu písemně oznámí tomu, kdo o odbornou zkoušku požádal, termín a místo konání odborné zkoušky; oznámení musí být odesláno nejpozději 20 dnů předem dnem konání odborné zkoušky. Ten, kdo při odborné zkoušce nevyhověl, ji může vykonat opakovaně. Opakovaná zkouška může být vykonána nejdříve po uplynutí 5 pracovních dnů ode dne neúspěšně vykonané zkoušky.

(3) Národní úřad pro kybernetickou a informační bezpečnost může uzavřít s orgánem státu smlouvu o zajištění činnosti podle § 52, jejímž předmětem je provedení

- a) odborné zkoušky a vydání osvědčení o zvláštní odborné způsobilosti, nebo
- b) části odborné zkoušky, týkající se § 38 odst. 1 písm. b) nebo c) a příslušné návaznosti na § 38 odst. 1 písm. a).

Smlouvu podle písmene b) může Národní úřad pro kybernetickou a informační bezpečnost uzavřít též s podnikatelem.

(zkráceno - text neobsahující změny byl vypuštěn)

§ 42

Převážení kryptografického materiálu a vývoz kryptografického prostředku

(1) Převážení kryptografického materiálu provádí kurýr kryptografického materiálu. Kurýrem kryptografického materiálu je osoba, která

- a) byla k přepravě pověřena odpovědnou osobou nebo jí pověřenou osobou,
- b) je držitelem platného osvědčení fyzické osoby, nejméně pro stupeň utajení přepravovaného kryptografického materiálu,
- c) byla k přepravě zaškolená.

(2) Z území České republiky lze vyvážet certifikovaný kryptografický prostředek [§ 46 odst. 1 písm. c)] pouze na základě povolení Národního úřadu pro kybernetickou a informační bezpečnost. Za vývoz se nepovažuje používání certifikovaného kryptografického prostředku mimo území České republiky orgánem státu.

(3) Povolení podle odstavce 2 lze udělit na základě písemné žádosti. Povolení se vydává na vývoz konkrétního kryptografického prostředku a obsahuje též účel vývozu. Národní úřad pro kybernetickou a informační bezpečnost povolení nevydá, jestliže by vývozem byla ohrožena utajovaná informace České republiky nebo utajovaná informace, k jejíž ochraně se Česká republika zavázala; tuto skutečnost písemně oznámí žadateli o povolení. Na udělení povolení není právní nárok.

(4) Národní úřad pro kybernetickou a informační bezpečnost ~~(4) Úřad~~ vede evidenci povolení udělených podle odstavce 2.

§ 43

Kompromitace kryptografického materiálu

(1) Kompromitací kryptografického materiálu se rozumí nakládání s kryptografickým materiálem, které způsobilo nebo by mohlo způsobit porušení ochrany utajované informace.

(2) Kompromitaci kryptografického materiálu je orgán státu, právnická osoba nebo podnikající fyzická osoba povinná neprodleně oznámit Národnímu úřadu pro kybernetickou a informační bezpečnost ~~Úřadu~~.

§ 43a

(1) Distribuci a evidenci kryptografického materiálu České republiky, kryptografického materiálu Evropské unie a kryptografického materiálu distribuovaného na základě mezinárodní smlouvy, s výjimkou kryptografického materiálu pro vojenské účely, zajišťuje Národní úřad pro kybernetickou a informační bezpečnost ~~Úřad~~. Distribuci a evidenci kryptografického materiálu Organizace Severoatlantické smlouvy a kryptografického materiálu pro vojenské účely zajišťuje Ministerstvo obrany.

(2) Podmínky evidence, manipulace a kontroly kryptografického materiálu v České republice, zahrnující zejména možnost zřízení účtů pro kryptografický materiál v orgánech státu nebo u podnikatele, vedení evidencí, kontrolní funkce, povinnosti držitelů kryptografického materiálu vůči Národnímu úřadu pro kybernetickou a informační bezpečnost ~~Úřadu~~ nebo Ministerstvu obrany a zajištění kurýrní služby pro kryptografický materiál Evropské unie upraví bezpečnostní standard.

(zkráceno - text neobsahující změny byl vypuštěn)

Kompromitující vyzařování

§ 45

(1) Ochranou utajovaných informací stupně utajení Přísně tajné, Tajné nebo Důvěrné před jejich únikem kompromitujícím vyzařováním je zabezpečení elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu.

(2) Je-li ochrana utajované informace před únikem kompromitujícím vyzařováním zabezpečena stínicí komorou, musí být tato komora certifikována Národním úřadem pro kybernetickou a informační bezpečnost ~~Úřadem~~ [§ 46 odst. 1 písm. e)].

(3) Ověřování způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajované informace kompromitujícím vyzařováním zajišťuje Národní úřad pro kybernetickou a informační bezpečnost ~~Úřad~~ při certifikaci informačního systému nebo kryptografického prostředku, při schvalování projektu bezpečnosti komunikačního systému nebo na základě odůvodněné písemné žádosti orgánu státu nebo podnikatele v souvislosti s ochranou utajovaných informací.

(4) K provádění měření možného úniku utajovaných informací podle odstavce 3 může Národní úřad pro kybernetickou a informační bezpečnost ~~Úřad~~ uzavřít s orgánem státu nebo podnikatelem smlouvu podle § 52 o zajištění této činnosti.

(5) K provádění měření zařízení, zabezpečené oblasti nebo objektu podle odstavce 3, které jsou provozovány nebo užívány zpravodajskými službami, jsou oprávněny zpravodajské služby. V těchto případech není vyžadováno uzavření smlouvy podle § 52. Pro potřeby certifikace informačního systému nebo kryptografického prostředku, nebo při schválení projektu bezpečnosti komunikačního systému předají zpravodajské služby Národnímu úřadu pro kybernetickou a informační bezpečnost ~~Úřadu~~ zprávy o provedeném měření včetně jeho výsledku.

(6) Při provádění měření podle odstavce 5 jsou zpravodajské služby povinny dodržovat ustanovení tohoto zákona, prováděcích právních předpisů a bezpečnostních standardů Národního úřadu pro kybernetickou a informační bezpečnost ~~Úřadu~~.

Státní správu v oblasti ochrany utajovaných informací podle této hlavy vykonává Národní úřad pro kybernetickou a informační bezpečnost, pokud tento zákon nestanoví jinak.

§ 46

Společná ustanovení

(1) Certifikace je postup, jímž Úřad nebo Národní úřad pro kybernetickou a informační bezpečnost

- a) ověřuje způsobilost technického prostředku k ochraně utajovaných informací,
- b) ověřuje způsobilost informačního systému k nakládání s utajovanými informacemi,
- c) ověřuje způsobilost kryptografického prostředku k ochraně utajovaných informací,
- d) ověřuje způsobilost kryptografického pracoviště pro vykonávání činností podle § 37 odst. 4, nebo
- e) ověřuje způsobilost stínicí komory k ochraně utajovaných informací.

(2) Zjistí-li Úřad nebo Národní úřad pro kybernetickou a informační bezpečnost způsobilost podle odstavce 1, certifikát technického prostředku, certifikát informačního systému, certifikát kryptografického prostředku, certifikát kryptografického pracoviště nebo certifikát stínicí komory vydá.

(3) Certifikáty podle odstavce 2 jsou veřejnými listinami.

(4) Certifikát technického prostředku obsahuje

- a) evidenční číslo certifikátu,
- b) název a typové označení technického prostředku,
- c) identifikaci výrobce technického prostředku obchodní firmou (dále jen "firma") nebo názvem, identifikačním číslem osoby (dále jen "identifikační číslo") a sídlem, jde-li o právnickou osobu, nebo jménem, příjmením, rodným číslem a místem trvalého pobytu, jde-li o osobu fyzickou,
- d) identifikaci držitele certifikátu technického prostředku podle písmene c),
- e) hodnocení technického prostředku,
- f) datum vydání a dobu platnosti certifikátu a
- g) otisk úředního razítka a podpis oprávněného zástupce Úřadu; otisk úředního razítka se nevyžaduje, byl-li certifikát vydán v elektronické podobě.

(5) Certifikát informačního systému, certifikát kryptografického prostředku, certifikát kryptografického pracoviště a certifikát stínicí komory obsahuje

- a) evidenční číslo certifikátu,
- b) identifikaci držitele certifikátu podle odstavce 4 písm. c),
- c) datum vydání a dobu platnosti certifikátu a
- d) otisk úředního razítka Národního úřadu pro kybernetickou a informační bezpečnost ~~Úřadu~~ a podpis oprávněného zástupce Úřadu.

(6) Certifikát informačního systému vedle náležitostí podle odstavce 5 obsahuje identifikaci informačního systému a stupeň utajení utajovaných informací, pro který byla způsobilost informačního systému ověřena.

(7) Certifikát kryptografického prostředku vedle náležitostí podle odstavce 5 obsahuje

- a) identifikaci kryptografického prostředku,
- b) identifikaci výrobce kryptografického prostředku podle odstavce 4 písm. c) a
- c) stupeň utajení utajovaných informací, pro který byla způsobilost kryptografického prostředku schválena.

(8) Certifikát kryptografického pracoviště vedle náležitostí podle odstavce 5 obsahuje

- a) identifikaci kryptografického pracoviště
- b) rozsah způsobilosti kryptografického pracoviště a
- c) kategorii kryptografického pracoviště.

(9) Certifikát stínicí komory vedle náležitostí podle odstavce 5 obsahuje

- a) identifikaci stínicí komory, pro kterou je vydáván,
- b) identifikaci výrobce stínicí komory podle odstavce 4 písm. c) a
- c) stupeň utajení utajovaných informací, pro který byla způsobilost stínicí komory schválena.

(10) Není-li Úřadem nebo Národním úřadem pro kybernetickou a informační bezpečnost zjištěna způsobilost podle odstavce 1, rozhodne o nevydání certifikátu. Proti rozhodnutí o nevydání certifikátu podle odstavce 1 písm. b) a c) není odvolání přípustné.

(11) Úřad rozhoduje o zániku platnosti certifikátu v případech uvedených v § 47 odst. 4 písm. b). Národní úřad pro kybernetickou a informační bezpečnost rozhoduje o zániku platnosti certifikátu v případech uvedených v b), § 48 odst. 4 písm. d), § 49 odst. 5 písm. b), § 50 odst. 4 písm. d) a § 51 odst. 4 písm. d). Odvolání podané proti rozhodnutí Úřadu nebo Národního úřadu pro kybernetickou a informační bezpečnost o zániku platnosti certifikátu nemá odkladný účinek. Proti rozhodnutí Národního úřadu pro kybernetickou a informační bezpečnost Úřadu o zániku platnosti certifikátu informačního systému a certifikátu kryptografického prostředku není odvolání přípustné.

(12) Jestliže platnost certifikátu zanikla podle § 47 odst. 4 písm. b), § 48 odst. 4 písm. b) a d), § 49 odst. 5 písm. b), § 50 odst. 4 písm. b) a d) nebo § 51 odst. 4 písm. b) a d), je držitel certifikátu povinen do 5 dnů ode dne doručení oznámení Národního úřadu pro kybernetickou a informační bezpečnost odevzdat certifikát Národnímu úřadu pro kybernetickou a informační bezpečnost. Jestliže platnost certifikátu zanikla podle § 47 odst. 4 písm. b), je držitel certifikátu povinen do 5 dnů ode dne doručení oznámení Úřadu odevzdat certifikát Úřadu.

(13) Přílohou certifikátu informačního systému, kryptografického prostředku, kryptografického pracoviště nebo stínicí komory je certifikační zpráva, která obsahuje zásady a podmínky jejich provozování. V příloze certifikátu technického prostředku mohou být stanoveny podmínky jeho používání.

(14) Úřad ověřuje způsobilost technického prostředku podle odstavce 1 písm. a) na základě posudku vlastností technického prostředku (dále jen "posudek"). K vydávání posudku podle věty první může Úřad uzavřít s orgánem státu nebo podnikatelem smlouvu podle § 52 o zajištění činnosti.

(15) K vydávání posudku podle odstavce 14 a k provádění dílčích úloh při ověřování způsobilosti podle odstavce 1 písm. b) až e) může Národní úřad pro kybernetickou a informační bezpečnost Úřad uzavřít s orgánem státu nebo podnikatelem smlouvu podle § 52 o zajištění těchto činností; to neplatí, jde-li o ověřování způsobilosti informačního systému, kryptografického prostředku nebo pracoviště anebo stínicí komory, které mají být provozovány zpravodajskými službami.

(16) Seznam orgánů státu a podnikatelů, s nimiž Úřad uzavřel smlouvu podle § 52, zveřejňuje Úřad a Národní úřad pro kybernetickou a informační bezpečnost v příslušném věstníku ve Věstníku Úřadu.

(17) K provádění dílčích úloh při ověřování způsobilosti podle odstavce 1 písm. b) až e), které z důvodu utajení nelze provést Národním úřadem pro kybernetickou a informační bezpečnost Úřadem, jde-li o informační systém, kryptografický prostředek, kryptografické pracoviště nebo stínicí komoru, které mají být provozovány zpravodajskými službami, jsou oprávněny tyto zpravodajské služby. V těchto případech zpravodajské služby předají Národnímu úřadu pro kybernetickou a informační bezpečnost Úřadu protokoly o provedení dílčích úloh, včetně jejich výsledků.

(18) Při provádění dílčích úloh podle odstavce 17 jsou zpravodajské služby povinny dodržovat ustanovení tohoto zákona, prováděcích právních předpisů a bezpečnostních standardů Národního úřadu pro kybernetickou a informační bezpečnost Úřadu.

(zkráceno - text neobsahující změny byl vypuštěn)

§ 48

Žádost o certifikaci informačního systému a platnost certifikátu informačního systému

(1) O certifikaci informačního systému písemně žádá u Národního úřadu pro kybernetickou a informační bezpečnost Úřadu orgán státu nebo podnikatel, který bude informační systém provozovat.

(2) Ten, kdo o certifikaci informačního systému podle odstavce 1 požádal, předkládá v průběhu certifikace na žádost Národního úřadu pro kybernetickou a informační bezpečnost Úřadu dokumentaci nezbytnou pro provedení certifikace.

(3) Dobu platnosti certifikátu informačního systému stanoví Národní úřad pro kybernetickou a informační bezpečnost Úřad. Platnost certifikátu informačního systému je pro stupeň utajení

a) Přísně tajné a Tajné nejdéle 2 roky,

b) Důvěrné nejdéle 3 roky a

c) Vyhrazené nejdéle 5 let.

(4) Platnost certifikátu informačního systému zaniká

a) uplynutím doby jeho platnosti,

b) v případě informačního systému pro nakládání s utajovanými informacemi stupně utajení Důvěrné nebo vyššího zánikem platnosti osvědčení podnikatele,

c) zrušením orgánu státu,

d) rozhodnutím Národního úřadu pro kybernetickou a informační bezpečnost Úřadu o zániku platnosti certifikátu, přestal-li být informační systém způsobilý k nakládání s utajovanými informacemi nebo

e) oznámením orgánu státu nebo podnikatele, který je držitelem certifikátu, o zrušení informačního systému.

(5) Má-li být informační systém používán i bezprostředně po uplynutí doby platnosti jeho certifikátu, je žadatel podle odstavce 1 povinen požádat Národní úřad pro kybernetickou a informační bezpečnost Úřad o certifikaci informačního systému. Opakovaná žádost musí být Národnímu úřadu pro kybernetickou a informační bezpečnost Úřadu doručena nejméně 6 měsíců před uplynutím doby platnosti původního certifikátu informačního systému.

(6) Národní úřad pro kybernetickou a informační bezpečnost ~~(6) Úřad~~ je povinen rozhodnout o certifikaci informačního systému do 1 roku od zahájení řízení o certifikaci, ve zvlášť složitých případech do 2 let; nelze-li vzhledem k povaze věci rozhodnout v této lhůtě, může ji přiměřeně prodloužit ředitel Národního úřadu pro kybernetickou a informační bezpečnost Úřadu, nejvýše však o 6 měsíců.

§ 49

Žádost o certifikaci kryptografického prostředku a platnost certifikátu kryptografického prostředku

(1) O certifikaci kryptografického prostředku písemně žádá u Národního úřadu pro kybernetickou a informační bezpečnost Úřadu výrobce, dovozce, distributor nebo uživatel kryptografického prostředku. Žádá-li o certifikaci kryptografického prostředku podnikatel, musí být držitelem platného osvědčení podnikatele pro přístup k utajované informaci podle § 20 odst. 1 písm. a).

(2) Národní úřad pro kybernetickou a informační bezpečnost ~~(2) Úřad~~ žádost podle odstavce 1 rozhodnutím odmítne, není-li v souladu se záměry České republiky v oblasti zajišťování ochrany utajovaných informací kryptografickou ochranou. Proti rozhodnutí podle věty první není odvolání přípustné a nelze jej ani přezkoumat soudem.

(3) Ten, kdo o certifikaci kryptografického prostředku podle odstavce 1 požádal, předkládá v průběhu certifikace na žádost Národního úřadu pro kybernetickou a informační bezpečnost Úřadu kryptografický prostředek v potřebném počtu a dokumentaci nezbytnou pro provedení certifikace.

(4) Doby platnosti certifikátu kryptografického prostředku stanoví Národní úřad pro kybernetickou a informační bezpečnost Úřad na dobu nejdéle 5 let.

(5) Platnost certifikátu kryptografického prostředku zaniká

a) uplynutím doby jeho platnosti, nebo

b) rozhodnutím Národního úřadu pro kybernetickou a informační bezpečnost Úřadu o zániku platnosti certifikátu, přestal-li být kryptografický prostředek způsobilý k ochraně utajovaných informací.

(6) Má-li být kryptografický prostředek používán i bezprostředně po uplynutí doby platnosti jeho certifikátu, je žadatel podle odstavce 1 povinen požádat Národní úřad pro kybernetickou a informační bezpečnost Úřad o certifikaci kryptografického prostředku. Opakovaná žádost musí být Národnímu úřadu pro kybernetickou a informační bezpečnost Úřadu doručena nejméně 6 měsíců před uplynutím doby platnosti původního certifikátu kryptografického prostředku.

(7) Národní úřad pro kybernetickou a informační bezpečnost ~~(7) Úřad~~ může při certifikaci kryptografického prostředku přihlídnout k certifikátu nebo obdobnému dokumentu kryptografického prostředku vydanému oprávněným pracovištěm cizí moci.

(8) Řízení o certifikaci kryptografického prostředku lze též přerušit současně s odesláním žádosti adresované zahraničnímu subjektu o informaci nezbytnou pro spolehlivé zjištění stavu věci.

(9) Národní úřad pro kybernetickou a informační bezpečnost ~~(9) Úřad~~ může stanovit při certifikaci kryptografického prostředku jeho způsobilost k ochraně taktické informace.

(zkráceno - text neobsahující změny byl vypuštěn)

§ 50

Žádost o certifikaci kryptografického pracoviště a platnost certifikátu kryptografického pracoviště

(1) O certifikaci kryptografického pracoviště písemně žádá u Národního úřadu pro kybernetickou a informační bezpečnost Úřadu orgán státu nebo podnikatel, u kterého má být kryptografické pracoviště provozováno. Žádá-li o certifikaci kryptografického pracoviště podnikatel, musí být držitelem platného osvědčení podnikatele.

(2) Ten, kdo o certifikaci kryptografického pracoviště podle odstavce 1 požádal, předkládá v průběhu certifikace na žádost Národního úřadu pro kybernetickou a informační bezpečnost Úřadu dokumentaci nezbytnou pro provedení certifikace.

(3) Dobu platnosti certifikátu kryptografického pracoviště stanoví Národní úřad pro kybernetickou a informační bezpečnost Úřad na dobu nejdéle 3 let.

(4) Platnost certifikátu kryptografického pracoviště zaniká

- a) uplynutím doby jeho platnosti,
- b) zánikem platnosti osvědčení podnikatele,
- c) zrušením orgánu státu, ~~nebo~~
- d) rozhodnutím Národního úřadu pro kybernetickou a informační bezpečnost Úřadu o zániku platnosti certifikátu, přestalo-li být kryptografické pracoviště způsobilé pro vykonávání určených činností, ~~nebo-~~
- e) oznámením orgánu státu nebo podnikatele, který je držitelem certifikátu, o zrušení kryptografického pracoviště.

(5) Má-li být kryptografické pracoviště využíváno i bezprostředně po uplynutí doby platnosti jeho certifikátu, je žadatel podle odstavce 1 povinen požádat Národní úřad pro kybernetickou a informační bezpečnost Úřad o certifikaci kryptografického pracoviště. Opakovaná žádost musí být Národnímu úřadu pro kybernetickou a informační bezpečnost Úřadu doručena nejméně 6 měsíců před uplynutím doby platnosti původního certifikátu kryptografického pracoviště.

(6) Národní úřad pro kybernetickou a informační bezpečnost (6) Úřad je povinen rozhodnout o certifikaci kryptografického pracoviště do 6 měsíců od zahájení řízení o certifikaci, ve zvlášť složitých případech do 1 roku; nelze-li vzhledem k povaze věci rozhodnout v této lhůtě, může ji přiměřeně prodloužit ředitel Národního úřadu pro kybernetickou a informační bezpečnost Úřadu, nejvýše však o 3 měsíce.

§ 51

Žádost o certifikaci stínící komory a platnost certifikátu stínící komory

(1) O certifikaci stínící komory písemně žádá u Národního úřadu pro kybernetickou a informační bezpečnost Úřadu orgán státu nebo podnikatel, u kterého je stínící komora používána.

(2) Ten, kdo o certifikaci stínící komory podle odstavce 1 požádal, předkládá v průběhu certifikace na žádost Národního úřadu pro kybernetickou a informační bezpečnost Úřadu dokumentaci nezbytnou pro provedení certifikace.

(3) Dobu platnosti certifikátu stínící komory stanoví Národní úřad pro kybernetickou a informační bezpečnost Úřad na dobu nejdéle 5 let.

(4) Platnost certifikátu stínící komory zaniká

- a) uplynutím doby jeho platnosti,
- b) zánikem platnosti osvědčení podnikatele,
- c) zrušením orgánu státu, nebo
- d) rozhodnutím Národního úřadu pro kybernetickou a informační bezpečnost Úřadu o zániku platnosti certifikátu, přestala-li být stínící komora způsobilá k ochraně utajovaných informací.

(5) Má-li být stínící komora používána i bezprostředně po uplynutí doby platnosti jejího certifikátu, je žadatel podle odstavce 1 povinen požádat Národní úřad pro kybernetickou a informační bezpečnost Úřad o certifikaci stínící komory. Opakovaná žádost musí být Národnímu úřadu pro kybernetickou a informační bezpečnost Úřadu doručena nejméně 12 měsíců před uplynutím doby platnosti původního certifikátu stínící komory.

(zkráceno - text neobsahující změny byl vypuštěn)

§ 52

Smlouva o zajištění činnosti

(1) Smlouva o zajištění činnosti (dále jen "smlouva") uvedená v § 39 odst. 3, § 45 odst. 4 a § 46 odst. 14 a 15 se uzavírá na dobu určitou nebo neurčitou. Smlouva musí mít písemnou formu. Projev vůle účastníků smlouvy musí být na téže listině.

(2) Smlouvu lze uzavřít s orgánem státu nebo podnikatelem na základě jejich písemné žádosti, a to pouze tehdy, budou-li činnosti, jež jsou předmětem smlouvy,

- a) prováděny odborně způsobilými zaměstnanci státu nebo podnikatele,

b) zajištěny u orgánu státu nebo podnikatele organizačně, technicky a materiálně.

(3) Smlouvu s podnikatelem lze dále uzavřít pouze tehdy, je-li

a) jeho sídlo nebo místo podnikání na území České republiky,

b) držitelem platného osvědčení podnikatele příslušného stupně utajení; tato podmínka neplatí, má-li být uzavřena smlouva k vydávání posudku uvedená v § 46 odst. 14 a 15.

(4) Smlouva musí obsahovat

a) označení účastníků smlouvy,

b) vymezení předmětu smlouvy a jeho rozsahu,

c) práva a povinnosti účastníků smlouvy,

d) způsob kontroly prováděné Úřadem nebo Národním úřadem pro kybernetickou a informační bezpečnost podle odstavce 6,

e) způsob a podmínky odstoupení účastníků od smlouvy,

f) souhlas se zveřejněním technického prostředku na internetových stránkách Úřadu, jde-li o smlouvu k vydávání posudku uvedenou v § 46 odst. 14 a 15.

(5) V podmínkách podle odstavce 4 písm. e) musí být též stanoveno, že Úřad nebo Národní úřad pro kybernetickou a informační bezpečnost odstoupí od smlouvy v případě, že druhý účastník smlouvy poruší povinnost stanovenou tímto zákonem, prováděcími právními předpisy nebo uzavřenou smlouvou.

(6) Úřad nebo Národní úřad pro kybernetickou a informační bezpečnost ~~(6) Úřad~~ kontroluje, zda druhý účastník smlouvy dodržuje ustanovení tohoto zákona, prováděcích právních předpisů a uzavřené smlouvy.

(zkráceno - text neobsahující změny byl vypuštěn)

§ 53

Zmocňovací ustanovení

Prováděcí právní předpis stanoví

a) náležitosti žádosti o certifikaci technického prostředku, dokumentaci nezbytnou k provedení certifikace technického prostředku, pravidla pro stanovení doby platnosti certifikátu technického prostředku, pravidla a způsob používání technického prostředku po uplynutí doby platnosti jeho certifikátu a vzor certifikátu technického prostředku ~~certifikaci informačního systému, certifikaci kryptografického prostředku, certifikaci kryptografického pracoviště a certifikaci stínící komory,~~

b) náležitosti žádosti a opakované žádosti o certifikaci informačního systému, certifikaci kryptografického prostředku, certifikaci kryptografického pracoviště a certifikaci stínící komory, a dokumentaci nezbytnou k provedení certifikace informačního systému, certifikace kryptografického prostředku, certifikace kryptografického pracoviště a certifikace stínící ~~stínící~~ komory,

~~c) dokumentaci nezbytnou k provedení certifikace technického prostředku, certifikace informačního systému, certifikace kryptografického prostředku, certifikace kryptografického pracoviště a certifikace stínící komory,~~

~~d) vzory certifikátu technického prostředku, certifikátu informačního systému, certifikátu kryptografického prostředku, certifikátu kryptografického pracoviště a certifikátu stínící komory,~~

~~e) pravidla pro stanovení doby platnosti certifikátu technického prostředku,~~

~~f) pravidla a způsob používání technického prostředku po uplynutí doby platnosti jeho certifikátu,~~

g) způsob a podmínky provádění certifikace informačního systému, certifikace kryptografického prostředku, certifikace kryptografického pracoviště a certifikace stínící ~~stínící~~ komory a jejich opakování a obsah certifikační zprávy podle § 46 odst. 13,

d) vzory certifikátu informačního systému, certifikátu kryptografického prostředku, certifikátu kryptografického pracoviště a certifikátu stínící komory,

~~e) h) obsah certifikační zprávy podle § 46 odst. 13,~~

~~i) náležitosti žádosti o ověření způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajované informace kompromitujícím vyzařováním a způsob hodnocení jejich způsobilosti a~~

~~j) náležitosti žádosti orgánu státu nebo podnikatele o uzavření smlouvy podle § 52.~~

(zkráceno - text neobsahující změny byl vypuštěn)

§ 65

Obecné povinnosti

(1) Každý je povinen neprodleně odevzdat nalezenou utajovanou informaci nebo utajovanou informaci získanou v rozporu s tímto zákonem anebo osvědčení fyzické osoby, osvědčení podnikatele, osvědčení fyzické osoby pro cizí moc nebo osvědčení podnikatele pro cizí moc (dále jen "nalezená písemnost") Úřadu, policii nebo zastupitelskému úřadu České republiky.

(2) Každý, kdo měl nebo má přístup k utajované informaci, je povinen zachovávat o ní mlčenlivost a nesmí k ní umožnit přístup neoprávněné osobě.

(3) Každý je povinen při výkonu ~~státní~~ kontroly Úřadem plnit pokyny kontrolního pracovníka při provádění neodkladných opatření podle § 144 odst. 1.

(zkráceno - text neobsahující změny byl vypuštěn)

§ 67

Povinnosti odpovědné osoby

(1) Odpovědná osoba je povinna zajistit

- a) poučení fyzické osoby,
- b) jednou ročně provedení proškolení fyzických osob, které mají přístup k utajované informaci, z právních předpisů v oblasti ochrany utajovaných informací a vést o těchto proškoleních přehledy,
- c) ověřování splnění podmínek pro přístup fyzické osoby k utajované informaci stupně utajení Vyhrazené,
- d) schválení informačního systému do provozu a písemné oznámení této skutečnosti Národnímu úřadu pro kybernetickou a informační bezpečnost Úřadu,

(zkráceno - text neobsahující změny byl vypuštěn)

§ 69

**Povinnosti právnické osoby a podnikající fyzické osoby,
které mají přístup k utajované informaci, a orgánu státu**

(1) Právnická osoba a podnikající fyzická osoba, které mají přístup k utajované informaci, a orgán státu jsou povinni

- a) zajistit ochranu utajovaných informací podle tohoto zákona a mezinárodních smluv,
- b) zpracovávat a vést přehled míst nebo funkcí, na kterých je nezbytné mít přístup k utajovaným informacím včetně utajovaných informací Evropské unie, Organizace Severoatlantické smlouvy a utajovaných informací vyžadujících zvláštní režim nakládání, s uvedením stupně utajení, nebo které nelze vykonávat bez osvědčení o zvláštní odborné způsobilosti podle tohoto zákona (§ 39); tím nejsou dotčena ustanovení zvláštních právních předpisů na úseku odborné způsobilosti ²⁹⁾,
- c) neprodleně písemně oznámit Úřadu skutečnost, která může mít vliv na vydání nebo na platnost osvědčení fyzické osoby nebo osvědčení podnikatele,
- d) zajistit vytvoření podmínek pro označování, evidenci, zapůjčování, ukládání, přepravu, další manipulaci a vyřazování utajované informace a utajované informace se zvláštním režimem nakládání v souladu s prováděcím právním předpisem,
- e) provozovat jen informační systém, který je certifikován Národním úřadem pro kybernetickou a informační bezpečnost Úřadem a písemně schválen do provozu,
- f) zastavit provoz informačního systému, který nesplňuje podmínky stanovené v certifikační zprávě, a zajistit ochranu utajované informace v něm a o těchto skutečnostech informovat Národní úřad pro kybernetickou a informační bezpečnost Úřad,
- g) provozovat jen komunikační systém, jehož projekt bezpečnosti byl schválen Národním úřadem pro kybernetickou a informační bezpečnost Úřadem,

- h) zastavit provoz komunikačního systému, který nesplňuje podmínky stanovené v projektu bezpečnosti komunikačního systému, a o této skutečnosti informovat Národní úřad pro kybernetickou a informační bezpečnost Úřad,
- i) používat pro kryptografickou ochranu jen prostředek, který je certifikován Národním úřadem pro kybernetickou a informační bezpečnost Úřadem, a používat kryptografické pracoviště jen k účelu, ke kterému bylo certifikováno a schváleno do provozu,
- j) ~~vést evidenci fyzických osob, které mají přístup k utajované informaci, evidenci kryptografického materiálu, evidenci pracovníků kryptografické ochrany, evidenci provozní obsluhy kryptografického prostředku, evidenci kurýrů kryptografického materiálu a evidenci případů neoprávněného nakládání s utajovanou informací,~~
- k) hlásit porušení povinnosti při ochraně utajované informace nebo povinnosti uložené mezinárodní smlouvou v oblasti ochrany utajovaných informací a přijetí opatření k odstranění příčin a nepříznivých následků porušení Úřadu; tato povinnost se nevztahuje na zpravodajské služby v případech podle § 140 odst. 1 písm. a) a na Ministerstvo vnitra v případech podle § 141 odst. 1, s výjimkou případů porušení ochrany utajovaných informací Organizace Severoatlantické smlouvy nebo Evropské unie,
- l) zřídit registr poskytovaných utajovaných informací (§ 79) a hlásit změny v něm Úřadu v rozsahu stanoveném prováděcím právním předpisem,
- m) provést kontrolu utajovaných informací vedených v registru utajovaných informací k 31. prosinci kalendářního roku a zprávu o jejím výsledku zaslat Úřadu do 15. února následujícího kalendářního roku spolu s uvedením počtu utajovaných informací a jejich stupňů utajení; zpravodajské služby zasílají zprávu o utajovaných informacích poskytnutých ústředním registrem a registrem vedeným Ministerstvem zahraničních věcí podle § 78 odst. 1,
- n) předat utajovanou informaci poskytnutou cizí mocí nebo zahraničním partnerem právnické osoby nebo podnikající fyzické osoby k zaevidování Úřadu nebo Ministerstvu zahraničních věcí podle § 79 odst. 5,
- o) zasílat v případech stanovených tímto zákonem utajované informace cizí moci prostřednictvím ústředního registru (§ 79 odst. 2),
- p) zajistit písemné pověření fyzické osoby k přístupu k utajované informaci se zvláštním režimem nakládání označené "ATOMAL",
- q) jako poskytovatel vyhrazené informace neprodleně zaslat Úřadu kopii prohlášení podnikatele podle § 15a odst. 2,
- r) jako zadavatel, není-li zpravodajskou službou, neprodleně písemně oznámit a doložit Úřadu doklady ke
1. skutečnosti, že bude zadávat veřejnou zakázku mimo zadávací řízení z důvodu ochrany utajovaných informací ⁴⁹⁾,
 2. skutečnosti, že v zadávacím řízení stanoví opatření k zajištění ochrany utajované informace ⁵⁰⁾ stupně utajení Důvěrné nebo vyšší,
 3. stanovení požadavku na profesní způsobilost v zadávacím řízení ⁵¹⁾ spočívající v předložení dokladu prokazujícího schopnost dodavatele zabezpečit ochranu utajovaných informací stupně utajení Důvěrné nebo vyšší nebo oprávnění ke vstupu osob dodavatele do zabezpečené oblasti kategorie Důvěrné nebo vyšší anebo jednacích oblastí podle tohoto zákona, nebo
 4. stanovení podmínky na uzavření smlouvy v zadávacím řízení spočívající v předložení dokladu prokazujícího schopnost dodavatele zabezpečit ochranu utajovaných informací ⁵³⁾ stupně utajení Důvěrné nebo vyšší.
- s) kontrolovat dodržování dalších povinností stanovených tímto zákonem⁵²⁾.
- t) vést evidenci kryptografického materiálu, evidenci pracovníků kryptografické ochrany, evidenci provozní obsluhy kryptografického prostředku a evidenci kurýrů kryptografického materiálu.

(zkráceno - text neobsahující změny byl vypuštěn)

§ 75a

(1) Smlouva, při jejímž plnění je nutný přístup k utajované informaci cizí moci, obsahuje bezpečnostní instrukci upravující podmínky ochrany této informace a utajované informace, která při plnění smlouvy popřípadě vznikne.

(2) Bezpečnostní instrukce musí být před uzavřením smlouvy schválena

- a) Úřadem, pokud si to vyhradí, nebo pokud nedojde k dohodě podle písmene b) anebo nenáleží-li utajovaná informace do věcné působnosti jiného ústředního správního úřadu,
- b) jiným ústředním správním úřadem, do jehož působnosti utajovaná informace náleží, a náleží-li do působnosti více ústředních správních úřadů, jedním z nich na základě dohody mezi nimi.

Ústřední správní úřad, který bezpečnostní instrukci schválil, provádí kontrolu jejího dodržování, a to podle kontrolního řádu zákona upravujícího státní kontrolu ⁴⁶⁾.

(zkráceno - text neobsahující změny byl vypuštěn)

Úřad jako ústřední správní úřad

- a) rozhoduje o žádosti fyzické osoby, žádosti podnikatele a žádosti o doklad a o zrušení platnosti osvědčení fyzické osoby, osvědčení podnikatele a dokladu, s výjimkou případů stanovených tímto zákonem [§ 140 odst. 1 písm. a) a § 141 odst. 1], a vydává osvědčení fyzické osoby podle § 56a,
- b) vykonává kontrolu státní dozor v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti (§ 143) a metodickou činnost, s výjimkou případů stanovených tímto zákonem (§ 143 odst. 5),
- ~~c) zajišťuje zkoušky zvláštní odborné způsobilosti a vydává osvědčení o zvláštní odborné způsobilosti,~~
- d) plní úkoly v oblasti ochrany utajovaných informací v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, Organizaci Severoatlantické smlouvy a z mezinárodních smluv, jimiž je Česká republika vázána,
- ~~e) vede ústřední registr a schvaluje zřízení registrů v orgánech státu a u podnikatelů,~~
- ~~e) f) ve stanovených případech povoluje poskytování utajovaných informací v mezinárodním styku,~~
- ~~f) g) ke kurýrní přepravě utajovaných informací stupně utajení Přísně tajné, Tajné nebo Důvěrné poskytovaných v rámci mezinárodního styku, s výjimkou utajované informace poskytované podle § 78 odst. 1, vydává na základě písemné žádosti odpovědné osoby nebo bezpečnostního ředitele kurýrní listy a v odůvodněných případech zajišťuje jejich přepravu,~~
- g) provádí certifikace technického prostředku,
- h) vydává bezpečnostní standardy,
- i) ukládá správní tresty za nedodržení povinností stanovených tímto zákonem,
- j) rozhoduje v dalších věcech a plní další úkoly na úseku ochrany utajovaných informací a bezpečnostní způsobilosti stanovené tímto zákonem a
- k) vydává Věstník Úřadu, který zveřejňuje na svých internetových stránkách.

§ 137aNárodní úřad pro kybernetickou a informační bezpečnostNárodní úřad pro kybernetickou a informační bezpečnost v oblasti působnosti svěřené mu tímto zákonem

- a) zajišťuje zkoušky zvláštní odborné způsobilosti a vydává osvědčení o zvláštní odborné způsobilosti,
- b) plní úkoly v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, Organizaci Severoatlantické smlouvy a z mezinárodních smluv, jimiž je Česká republika vázána, ve vybraných oblastech ochrany utajovaných informací,
- c) vykonává metodickou činnost,
- ~~d) h) zajišťuje činnost Národního střediska komunikační bezpečnosti, Národního střediska pro distribuci kryptografického materiálu, Národního střediska pro měření kompromitujícího vyzařování a Národního střediska pro bezpečnost informačních systémů, které jsou jeho součástí,~~
- ~~e) i) provádí certifikace technického prostředku, informačního systému, kryptografického prostředku, kryptografického pracoviště a stínící stínicí komory a schvaluje projekt bezpečnosti komunikačního systému,~~
- ~~f) j) zajišťuje výzkum, vývoj a výrobu národních kryptografických prostředků,~~
- ~~g) k) vyvíjí a schvaluje národní šifrové algoritmy a vytváří národní politiku kryptografické ochrany,~~
- ~~h) l) zjišťuje kompromitující vyzařování tam, kde se vyskytnou nebo budou vyskytovat utajované informace,~~
- ~~i) m) zjišťuje v součinnosti se zpravodajskými službami a policií, zda v jednacích oblastech nedochází nedovoleným použitím technických prostředků určených k získávání informací k ohrožení nebo únikům utajovaných informací,~~
- ~~j) n) vydává bezpečnostní standardy,~~
- ~~k) o) ukládá správní tresty za nedodržení povinností stanovených tímto zákonem,~~
- ~~l) p) rozhoduje v dalších věcech a plní další úkoly na úseku ochrany utajovaných informací a bezpečnostní způsobilosti stanovené tímto zákonem a~~
- ~~q) vydává Věstník Úřadu, který zveřejňuje na svých internetových stránkách.~~

(1) Úřad je při plnění úkolů podle tohoto zákona oprávněn

- a) zpracovávat osobní údaje v rozsahu nezbytném pro plnění úkolů podle tohoto zákona,
- b) vést evidenci porušení ochrany utajovaných informací, evidenci bezpečnostních ředitelů, evidenci fyzických osob a podnikatelů, kteří mají přístup k utajovaným informacím, s výjimkou příslušníků a zaměstnanců zařazených do zpravodajských služeb a vybraných policistů, evidenci fyzických osob, které jsou držiteli dokladu, ~~evidenci pracovníků kryptografické ochrany, kurýrů kryptografického materiálu a evidenci fyzických osob, které jsou držiteli osvědčení o zvláštní odborné způsobilosti,~~
- ~~c) vést certifikační spis informačního systému, kryptografického prostředku, kryptografického pracoviště a stínící komory, vést seznam kontrolovaných kryptografických položek a vést dokumentaci pro provádění činností podle § 45,~~
- d) požadovat bezplatně poskytnutí informace u orgánu státu, právnické osoby nebo podnikající fyzické osoby a tyto informace využívat a evidovat,
- ~~e) pro účely řízení požadovat od policie a zpravodajských služeb informace získané postupy podle zvláštního právního předpisu ⁴³⁾,~~
- ~~e) f) vyžadovat opis z evidence Rejstříku trestů ¹¹⁾ a z evidence přestupků vedené Rejstříkem trestů; žádost o vydání opisu z evidence Rejstříku trestů a z evidence přestupků a opis z evidence Rejstříku trestů a z evidence přestupků se předávají v elektronické podobě, a to způsobem umožňujícím dálkový přístup,~~
- ~~f) g) nahlížet do trestních spisů, pořizovat si z nich výpisy a kopie,~~
- g) h) poskytovat v nezbytném rozsahu orgánu státu, právnické osobě nebo podnikající fyzické osobě potřebné osobní údaje vztahující se k vyžádané informaci,
- ~~h) i) uzavírat smlouvu s orgánem státu nebo podnikatelem k provádění dílčích úloh při certifikaci technických prostředků, informačních systémů, kryptografických prostředků, kryptografického pracoviště, stínících komor, k provádění školení zvláštní odborné způsobilosti pracovníků kryptografické ochrany a zjišťování možnosti výskytu kompromitujícího vyzařování tam, kde se utajované informace budou vyskytovat, a provádět výrobu kryptografických prostředků,~~
- i) j) uchovávat ve svých informačních systémech údaje získané v rámci plnění úkolů podle tohoto zákona,
- ~~j) k) při provádění bezpečnostního řízení spolupracovat s úřadem cizí moci, který má v působnosti ochranu utajovaných informací, zejména vyžadovat informace k účastníku řízení,~~
- ~~k) l) vyjadřovat se k oznámení podle § 69 odst. 1 písm. r) ve lhůtě 30 dnů ode dne jeho doručení a poskytovat přehled těchto oznámení a vyjádření k nim Úřadu pro ochranu hospodářské soutěže a~~
- ~~l) m) pro rozhodování Úřadu pro zahraniční styky a informace a Vojenského zpravodajství podle § 140 odst. 1, na základě jejich písemné žádosti, provádět úkony podle § 107 odst. 1.~~

(2) Úřad poskytuje zpravodajským službám a Ministerstvu vnitra jedenkrát měsíčně seznam

- a) vydaných osvědčení fyzických osob, osvědčení podnikatelů a dokladů,
- b) osob, u kterých rozhodl o nevydání veřejné listiny uvedené v písmenu a), nebo kterým byla platnost této listiny zrušena,
- c) podnikatelů, k nimž obdržel podle § 15a odst. 2 nebo 3 prohlášení podnikatele.

(3) Národní úřad pro kybernetickou a informační bezpečnost je při plnění úkolů podle tohoto zákona oprávněn k činnostem podle odstavce 1 písm. a), c), g) a i), a dále je oprávněn

- a) vést evidenci fyzických osob, které jsou držiteli osvědčení o zvláštní odborné způsobilosti, evidenci porušení ochrany utajovaných informací a evidenci pracovníků kryptografické ochrany a kurýrů kryptografického materiálu,
- b) uzavírat smlouvu s orgánem státu nebo podnikatelem k provádění dílčích úloh při certifikaci informačních systémů, kryptografických prostředků, kryptografického pracoviště, stínících komor, k provádění školení zvláštní odborné způsobilosti pracovníků kryptografické ochrany a zjišťování možnosti výskytu kompromitujícího vyzařování tam, kde se utajované informace budou vyskytovat, a provádět výrobu kryptografických prostředků a
- c) vést certifikační spis informačního systému, kryptografického prostředku, kryptografického pracoviště a stínící komory, vést seznam kontrolovaných kryptografických položek a vést dokumentaci pro provádění činností podle § 45.

(1) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona ze základního registru obyvatel referenční údaje, kterými jsou

- a) přijmení,

- b) jméno, popřípadě jména,
- c) adresa místa pobytu,
- d) datum, místo a okres narození; u subjektu údajů, který se narodil v cizině, datum, místo a stát, kde se narodil,
- e) datum, místo a okres úmrtí; jde-li o úmrtí subjektu údajů mimo území České republiky, datum úmrtí, místo a stát, na jehož území k úmrtí došlo,
- f) státní občanství, popřípadě více státních občanství.

g) záznam o zřízení datové schránky a identifikátor datové schránky, je-li tato datová schránka zpřístupněna.

(2) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona z agendového informačního systému evidence obyvatel o státních občanech České republiky údaje, kterými jsou

- a) jméno, popřípadě jména, příjmení, včetně předchozích příjmení, rodné příjmení,
- b) pohlaví,
- c) rodné číslo, pokud není přiděleno, datum narození,
- d) adresa místa trvalého pobytu, včetně předchozích adres místa trvalého pobytu, popřípadě adresa, na kterou mají být doručovány písemnosti podle jiného právního předpisu,
- e) počátek trvalého pobytu, popřípadě datum zrušení údaje o místě trvalého pobytu nebo datum ukončení trvalého pobytu na území České republiky,
- f) omezení svéprávnosti, jméno, popřípadě jména, příjmení a rodné číslo opatrovníka; nebylo-li opatrovníkovi rodné číslo přiděleno, datum, místo a okres narození; je-li opatrovníkem ustanoven orgán místní správy, název a adresa sídla,
- g) jméno, popřípadě jména, příjmení a rodné číslo otce, matky, popřípadě jiného zákonného zástupce; v případě, že jeden z rodičů nebo jiný zákonný zástupce nemá přiděleno rodné číslo, jméno, popřípadě jména, příjmení, datum narození; je-li jiným zákonným zástupcem dítěte právnická osoba, název a adresa sídla,
- h) rodinný stav, datum, místo a okres uzavření manželství, došlo-li k uzavření manželství mimo území České republiky, místo a stát, datum nabytí právní moci rozhodnutí soudu o prohlášení manželství za neplatné, datum nabytí právní moci rozhodnutí soudu o neexistenci manželství, datum zániku manželství smrtí jednoho z manželů, nebo datum nabytí právní moci rozhodnutí soudu o prohlášení jednoho z manželů za mrtvého a den, který byl v pravomocném rozhodnutí o prohlášení za mrtvého uveden jako den smrti, popřípadě jako den, který manžel prohlášený za mrtvého nepřežil, anebo datum nabytí právní moci rozhodnutí soudu o rozvodu manželství,
- i) datum a místo vzniku registrovaného partnerství, datum nabytí právní moci rozhodnutí soudu o neplatnosti nebo o neexistenci registrovaného partnerství, datum zániku registrovaného partnerství smrtí jednoho z registrovaných partnerů, nebo datum nabytí právní moci rozhodnutí soudu o prohlášení jednoho z registrovaných partnerů za mrtvého a den, který byl v pravomocném rozhodnutí soudu o prohlášení za mrtvého uveden jako den smrti, popřípadě jako den, který partner prohlášený za mrtvého nepřežil, anebo datum nabytí právní moci rozhodnutí soudu o zrušení registrovaného partnerství,
- j) jméno, popřípadě jména, příjmení, včetně předchozích příjmení, a rodné číslo manžela nebo registrovaného partnera; je-li manželem nebo registrovaným partnerem fyzická osoba, která nemá přiděleno rodné číslo, jméno, popřípadě jména, příjmení manžela nebo registrovaného partnera a datum jeho narození,
- k) jméno, popřípadě jména, příjmení a rodné číslo dítěte; je-li dítě cizinec, který nemá přiděleno rodné číslo, jméno, popřípadě jména, příjmení dítěte a datum jeho narození,
- l) o osvojeném dítěti údaje v rozsahu
 1. stupeň osvojení,
 2. původní a nové jméno, popřípadě jména, příjmení dítěte,
 3. původní a nové rodné číslo dítěte,
 4. datum, místo a okres narození,
 5. rodná čísla osvojitelů; v případě, že osvojiteli nebylo přiděleno rodné číslo, údaje o jménu, popřípadě jménech, příjmení a datu narození osvojitele,
 6. rodná čísla otce a matky; pokud jim nebylo přiděleno, jejich jméno, popřípadě jména, příjmení a datum narození,
 7. datum nabytí právní moci rozhodnutí o osvojení nebo rozhodnutí o zrušení osvojení dítěte,
- m) datum, místo a okres úmrtí; jde-li o úmrtí občana mimo území České republiky, datum úmrtí, místo a stát, na jehož území k úmrtí došlo,
- n) den, který byl v rozhodnutí soudu o prohlášení za mrtvého uveden jako den smrti, popřípadě jako den, který občan prohlášený za mrtvého nepřežil.

Údaje, které jsou vedeny jako referenční údaje v základním registru obyvatel, se využijí z agendového informačního systému evidence obyvatel, pouze pokud jsou ve tvaru předcházejícím současný stav.

(3) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona z informačního systému cizinců o cizincích údaje, kterými jsou

- a) jméno, popřípadě jména, příjmení, rodné příjmení,
- b) datum narození,
- c) pohlaví,
- d) místo a stát, kde se cizinec narodil; v případě, že se cizinec narodil na území České republiky, místo a okres narození,
- e) rodné číslo,
- f) státní občanství, popřípadě více státních občanství,
- g) druh a adresa místa pobytu,
- h) číslo a platnost oprávnění k pobytu,
- i) počátek pobytu, popřípadě datum ukončení pobytu,
- j) omezení svéprávnosti,
- k) správní vyhoštění a doba, po kterou není umožněn vstup na území České republiky,
- l) rodinný stav, datum a místo uzavření manželství, datum nabytí právní moci rozhodnutí soudu o prohlášení manželství za neplatné, datum nabytí právní moci rozhodnutí soudu o neexistenci manželství, datum zániku manželství smrtí jednoho z manželů, nebo datum nabytí právní moci rozhodnutí soudu o prohlášení jednoho z manželů za mrtvého a den, který byl v pravomocném rozhodnutí soudu o prohlášení za mrtvého uveden jako den smrti, popřípadě jako den, který manžel prohlášený za mrtvého nepřežil, anebo datum nabytí právní moci rozhodnutí soudu o rozvodu manželství,
- m) datum a místo vzniku registrovaného partnerství, datum nabytí právní moci rozhodnutí soudu o neplatnosti nebo o neexistenci registrovaného partnerství, datum zániku registrovaného partnerství smrtí jednoho z registrovaných partnerů, nebo datum nabytí právní moci rozhodnutí soudu o prohlášení jednoho z registrovaných partnerů za mrtvého a den, který byl v pravomocném rozhodnutí soudu o prohlášení za mrtvého uveden jako den smrti, popřípadě jako den, který partner prohlášený za mrtvého nepřežil, anebo datum nabytí právní moci rozhodnutí soudu o zrušení registrovaného partnerství,
- n) jméno, popřípadě jména, příjmení manžela nebo registrovaného partnera a jeho rodné číslo; je-li manžel nebo registrovaný partner cizinec, který nemá přiděleno rodné číslo, jméno, popřípadě jména, příjmení a datum narození,
- o) jméno, popřípadě jména, příjmení dítěte, pokud je cizincem podle jiného právního předpisu, a jeho rodné číslo; v případě, že dítěti nebylo rodné číslo přiděleno, jméno, popřípadě jména, příjmení a datum narození,
- p) jméno, popřípadě jména, příjmení otce, matky, popřípadě jiného zákonného zástupce, pokud jsou cizinci podle jiného právního předpisu, a jejich rodné číslo; v případě, že jeden z rodičů nebo jiný zákonný zástupce nemá přiděleno rodné číslo, jméno, popřípadě jména, příjmení a datum narození,
- q) o osvojeném dítěti, pokud je cizincem podle jiného právního předpisu,
 - 1. stupeň osvojení,
 - 2. původní a nové jméno, popřípadě jména, příjmení dítěte,
 - 3. původní a nové rodné číslo dítěte,
 - 4. datum a místo narození,
 - 5. rodná čísla osvojitelů; v případě, že osvojiteli nebylo přiděleno rodné číslo, údaje o jménu, popřípadě jménech, příjmení a datu narození osvojitele,
 - 6. rodná čísla otce a matky; pokud jim nebylo přiděleno, údaje o jejich jménu, popřípadě jménech, příjmení a datu narození; tyto údaje se neposkytují, pokud se jedná o dítě narozené ženě s trvalým pobytem v České republice, která porodila dítě a písemně požádala o utajení své osoby v souvislosti s porodem,
 - 7. datum nabytí právní moci rozhodnutí o osvojení nebo rozhodnutí o zrušení osvojení dítěte,
- r) vyhoštění a doba, po kterou není umožněn vstup na území České republiky,
- s) datum, místo a okres úmrtí; jde-li o úmrtí mimo území České republiky, stát, na jehož území k úmrtí došlo, popřípadě datum úmrtí,
- t) den, který byl v rozhodnutí soudu o prohlášení za mrtvého uveden jako den smrti, popřípadě jako den, který cizinec prohlášený za mrtvého nepřežil,
- u) jméno, popřípadě jména, příjmení
 - 1. zletilého nezaopatřeného dítěte cizince s povolením k pobytu na území České republiky,
 - 2. nezletilého cizince, který byl cizinci s povolením k pobytu na území České republiky nebo jeho manželů rozhodnutím příslušného orgánu svěřen do náhradní rodinné péče, nebo který byl cizincem s povolením k pobytu na území České republiky nebo jeho manželem osvojen anebo jehož poručníkem nebo manželem jeho poručníka je cizinec s povolením k pobytu na území České republiky,

3. osamělého cizince staršího 65 let nebo bez ohledu na věk cizince, který se o sebe nedokáže ze zdravotních důvodů sám postarat, jde-li o sloučení rodiny s rodičem nebo dítětem s povolením k pobytu na území České republiky,
4. cizince, který je nezaopatřeným přímým příbuzným ve vzestupné nebo sestupné linii nebo takovým příbuzným manžela občana Evropské unie,
5. rodiče nezletilého cizince, kterému byl udělen azyl podle zvláštního právního předpisu, a jeho rodné číslo; jde-li o cizince, kteří nemají přiděleno rodné číslo, jméno, popřípadě jména, příjmení a datum narození.

Údaje, které jsou vedeny jako referenční údaje v základním registru obyvatel, se využijí z informačního systému cizinců, pouze pokud jsou ve tvaru předcházejícím současný stav.

(4) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona z registru rodných čísel o fyzických osobách, kterým bylo přiděleno rodné číslo, avšak nejsou vedeny v agendovém informačním systému evidence obyvatel, údaje, kterými jsou

- a) jméno, popřípadě jména, příjmení, popřípadě rodné příjmení,
- b) rodné číslo,
- c) v případě změny rodného čísla původní rodné číslo,
- d) den, měsíc a rok narození,
- e) místo a okres narození; u fyzické osoby narozené v cizině stát, na jehož území se narodila.

(5) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona ze základního registru právnických osob, podnikajících fyzických osob a orgánů veřejné moci údaje, kterými jsou

- a) obchodní firma nebo název právnické osoby nebo jméno, popřípadě jména, a příjmení podnikající fyzické osoby,
- b) datum vzniku nebo datum zápisu do evidence podle zvláštních právních předpisů,
- c) datum zániku nebo datum výmazu z evidence podle zvláštních právních předpisů,
- d) právní forma,
- e) záznam o zřízení datové schránky a identifikátor datové schránky, je-li tato datová schránka zpřístupněna,
- f) statutární orgán vyjádřený referenční vazbou na registr obyvatel anebo na registr osob nebo údajem o jménu, popřípadě jménech, příjmení a bydlišti u zahraniční fyzické osoby,
- g) právní stav,
- h) adresa sídla právnické osoby nebo adresa místa podnikání fyzické osoby ve formě referenční vazby (kódu adresního místa) na referenční údaj o adrese v registru územní identifikace.

(6) K údajům podle odstavců 2 až 54 vedených v agendových informačních systémech jsou Úřadu poskytovány i jejich předchozí změny.

(7) Z poskytovaných údajů lze v konkrétním případě použít vždy jen takové údaje, které jsou nezbytné ke splnění daného úkolu.

(8) Národnímu úřadu pro kybernetickou a informační bezpečnost jsou poskytovány pro výkon jeho působnosti podle tohoto zákona údaje podle odstavce 1, odstavce 2 písm. a), c), d), f), m) a n), odstavce 3 písm. a), b), e) až g), j), k) a r) až t), odstavce 4 písm. a), b), d) a e) a odstavce 5.

§ 138b

Spolupráce Úřadu a Národního úřadu pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost předá bez zbytečného odkladu Úřadu oznámení, které obdržel podle § 34 odst. 5, § 43 odst. 2 nebo § 69 odst. 1 písm. f) a h).

(zkráceno - text neobsahující změny byl vypuštěn)

ČÁST ŠESTÁ KONTROLA STÁTNÍ DOZOR

(1) ~~Úřad Státním dozorem~~ v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti ~~kontroluje~~ ~~dozor nad tím, jak orgány státu, právnické osoby, podnikající fyzické osoby a fyzické osoby (dále jen "kontrolované osoby")~~ dodržují právní předpisy v této oblasti.

(2) Při výkonu ~~kontroly státního dozoru~~ se postupuje přiměřeně podle ~~kontrolního řádu, zákona upravujícího státní kontrolu~~⁴⁵⁾, nestanoví-li tento zákon jinak.

(3) Zaměstnanci Úřadu mají při výkonu ~~kontroly státního dozoru~~ (dále jen "kontrolní pracovníci") přístup k utajovaným informacím v rozsahu prováděné kontroly, prokáží-li se platným osvědčením fyzické osoby pro příslušný stupeň utajení.

(4) Úřad cizí moci, který má v působnosti ochranu utajovaných informací, je oprávněn účastnit se ~~kontroly státního dozoru~~ v oblasti ochrany utajovaných informací, které jsou jím poskytnuty České republice, vyplývá-li to ze závazku členství České republiky v Evropské unii, nebo stanoví-li tak mezinárodní smlouva, kterou je Česká republika vázána.

(5) ~~Kontrola Státnímu dozoru~~ podle tohoto zákona nepodléhá činnost zpravodajských služeb a činnost Ministerstva vnitra v případech podle § 141.

(6) V případě kontroly, která zasahuje do oblasti působnosti ochrany utajovaných informací, jejíž státní správu podle tohoto zákona vykonává Národní úřad pro kybernetickou a informační bezpečnost, bude ke kontrole přizván jeho zástupce.

§ 144

Opatření k nápravě

(1) Kromě oprávnění podle ~~kontrolního řádu, zákona upravujícího státní kontrolu~~⁴⁶⁾ jsou kontrolní pracovníci při zjištění porušení právních předpisů v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti u kontrolované osoby oprávněni přijmout neodkladná opatření k zajištění ochrany utajovaných informací, včetně odejmutí utajované informace, opatření ke zrušení nebo změně stupně utajení utajované informace nebo k označení utajované informace stupněm utajení. O odejmutí vydají kontrolované osobě potvrzení. Rovněž jsou oprávněni požadovat, aby ve stanovené lhůtě byly odstraněny zjištěné nedostatky.

(zkráceno - text neobsahující změny byl vypuštěn)

ČÁST SEDMÁ

KONTROLA ČINNOSTI ÚŘADU

§ 145

(1) Kontrolu činnosti Úřadu vykonává Poslanecká sněmovna, která k tomuto účelu zřizuje zvláštní kontrolní orgán (dále jen "kontrolní orgán").

(2) Kontrolní orgán se skládá ze 7 členů. Členem kontrolního orgánu může být pouze poslanec Poslanecké sněmovny.

(3) Pokud tento zákon nestanoví jinak, vztahuje se na jednání kontrolního orgánu a na práva a povinnosti jeho členů přiměřeně zvláštní právní předpis⁴⁶⁾.

(4) Členové kontrolního orgánu mohou vstupovat v doprovodu ředitele Úřadu nebo jím pověřeného zaměstnance do objektů Úřadu.

(5) Ředitel Úřadu předkládá kontrolnímu orgánu

a) zprávu o činnosti Úřadu,

b) zprávu o jednotlivých řízeních o žádosti fyzické osoby, žádosti podnikatele a žádosti o doklad a o zrušení platnosti osvědčení fyzické osoby, osvědčení podnikatele nebo dokladu [§ 137 písm. a)],

c) návrh rozpočtu Úřadu,

d) podklady potřebné ke kontrole plnění rozpočtu Úřadu,

e) vnitřní předpisy Úřadu,

~~f) na vyžádání zprávu o jednotlivých kybernetických bezpečnostních incidentech z kritické informační infrastruktury.~~

(zkráceno - text neobsahující změny byl vypuštěn)

(1) Má-li kontrolní orgán za to, že činnost Úřadu nezákonně omezuje nebo poškozuje práva a svobody občanů nebo že rozhodovací činnost Úřadu v rámci bezpečnostního řízení ~~nebo v rámci správního řízení o vydání opatření podle zákona o kybernetické bezpečnosti~~ je stížena vadami, je oprávněn požadovat od ředitele Úřadu potřebné vysvětlení.

(2) Každé porušení zákona zaměstnancem Úřadu při plnění povinností podle tohoto zákona ~~nebo podle zákona o kybernetické bezpečnosti~~, které kontrolní orgán zjistí při své činnosti, je povinen oznámit řediteli Úřadu a předsedovi vlády.

(zkráceno - text neobsahující změny byl vypuštěn)

ČÁST OSMÁ PŘESTUPKY

§ 148

(1) Fyzická osoba se dopustí přestupku tím, že

- a) jako účastník bezpečnostního řízení neoznámí změnu údaje uvedeného v žádosti fyzické osoby podle § 103 odst. 2 nebo údaje uvedeného v žádosti o doklad podle § 103 odst. 2,
- b) neodevzdá nalezenou písemnost podle § 65 odst. 1 nebo nalezený doklad podle § 87 odst. 2,
- c) poruší povinnost zachovávat mlčenlivost o utajované informaci,
- d) umožní přístup k utajované informaci neoprávněné osobě,
- e) vykonává funkci bezpečnostního ředitele v rozporu s § 71 odst. 5,
- f) provádí kryptografickou ochranu, aniž je pracovníkem kryptografické ochrany splňujícím požadavky stanovené v § 38 odst. 2,
- g) provádí provozní obsluhu kryptografického prostředku, aniž splňuje požadavky stanovené v § 40 odst. 2,
- h) přepravuje kryptografický materiál, aniž je kurýrem kryptografického materiálu splňujícím požadavky stanovené v § 42 odst. 1,
- i) zajistí si přístup k utajované informaci, aniž splňuje podmínky podle § 6 odst. 1 nebo § 11 odst. 1, nebo
- j) vyveze z území České republiky certifikovaný kryptografický prostředek bez povolení Národního úřadu pro kybernetickou a informační bezpečnost Úřadu.

(zkráceno - text neobsahující změny byl vypuštěn)

§ 153

(1) Právnícká osoba nebo podnikající fyzická osoba, které mají přístup k utajované informaci, nebo orgán státu se dopustí přestupku tím, že

- a) nezajistí podle § 28 odst. 2 nebo 4 ostrahu u objektu, ve kterém se nachází zabezpečená oblast kategorie Vyhrazené,
- b) v rozporu s § 36 odst. 2 nevydá bezpečnostní provozní směrnici,
- c) nezajistí písemné pověření fyzické osoby k přístupu k utajované informaci se zvláštním režimem nakládání označené "ATOMAL",
- d) nezřídí a neobsadí funkci bezpečnostního ředitele podle § 71 odst. 1,
- e) neoznámí podle § 71 odst. 2 jmenování bezpečnostního ředitele,
- f) nevyznačí na utajované informaci náležitosti podle § 21 odst. 2 až 4,
- g) jako původce vyznačí stupeň utajení na informaci, aniž je uvedena v seznamu utajovaných informací nebo aniž její vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné,
- h) jako původce neoznámí zrušení nebo změnu stupně utajení podle § 22 odst. 6,
- i) jako adresát utajované informace neoznámí změnu nebo zrušení stupně utajení podle § 22 odst. 6,

- j) nezajistí podle § 28 odst. 1, 3 nebo 4 nepřetržitou ostrahu u objektu, ve kterém se nachází zabezpečená oblast nebo jednacích oblast,
- k) nenahlásí porušení povinnosti při ochraně utajované informace,
- l) nezpracuje projekt fyzické bezpečnosti podle § 32,
- m) nevede některou z evidencí stanovených v § 69 odst. 1 písm. j),
- n) nepředá k zaevidování utajovanou informaci podle § 69 odst. 1 písm. n),
- o) nezajistí, aby použitá opatření fyzické bezpečnosti odpovídala projektu fyzické bezpečnosti a požadavkům stanoveným podle § 31,
- p) jako původce nevyznačí náležitosti podle § 21 odst. 1 a 4, ačkoli je informace uvedena v seznamu utajovaných informací a její vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné,
- q) jako původce nezruší nebo nezmění neprodleně stupeň utajení v případech, kdy pominul důvod pro utajení informace, důvody pro utajení neodpovídají stanovenému stupni utajení nebo byl-li stupeň utajení stanoven neoprávněně,
- r) nezajistí vytvoření podmínek stanovených na základě § 33 pro ukládání a § 23 odst. 2 pro evidenci, zapůjčování nebo přepravu utajovaných informací nebo utajovaných informací se zvláštním režimem nakládání nebo pro jinou manipulaci s nimi,
- s) provozuje informační systém, který není certifikován Národním úřadem pro kybernetickou a informační bezpečnost ~~Úřadem~~ nebo není písemně schválen do provozu odpovědnou osobou nebo jí pověřenou osobou,
- t) provozuje komunikační systém, jehož bezpečnostní projekt není schválen Národním úřadem pro kybernetickou a informační bezpečnost ~~Úřadem~~,
- u) nezastaví provoz informačního systému, který nesplňuje podmínky stanovené v certifikační zprávě, nebo nezastaví provoz komunikačního systému, který nesplňuje podmínky stanovené v projektu bezpečnosti komunikačního systému,
- v) používá pro kryptografickou ochranu prostředek, který není certifikován Národním úřadem pro kybernetickou a informační bezpečnost ~~Úřadem~~, nebo používá kryptografické pracoviště k jinému účelu, ke kterému bylo certifikováno a schváleno do provozu,
- w) nezajistí výkon kryptografické ochrany osobou, která splňuje požadavky stanovené v § 38 odst. 2,
- x) nezajistí obsluhu kryptografického prostředku osobou, která splňuje požadavky stanovené v § 40 odst. 2,
- y) nezajistí přepravu kryptografického materiálu osobou, která splňuje požadavky stanovené v § 42 odst. 1,
- z) neoznámí kompromitaci kryptografického materiálu podle § 43 odst. 2,
- aa) ~~—~~ nezřídí registr nebo nenahlásí Úřadu změny v registru podle § 79 odst. 8 písm. f),
- bb) ~~—~~ neprovádí kontrolu utajovaných informací podle § 69 odst. 1 písm. m) vedených v registru nebo neoznámí její výsledek Úřadu,
- cc) ~~—~~ odešle utajovanou informaci stupně utajení Přísně tajné, Tajné nebo Důvěrné v rozporu s § 77,
- dd) ~~—~~ umožní výkon citlivé činnosti fyzické osobě, která není držitelem platného dokladu nebo osvědčení fyzické osoby, ~~nebo~~
- ee) ~~—~~ neoznámí jako zadavatel veřejné zakázky Úřadu skutečnost podle § 69 odst. 1 písm. r) nebo
- ff) nevede některou z evidencí stanovených v § 69 odst. 1 písm. t).

(2) Za přestupek lze uložit pokutu do

- a) 300 000 Kč, jde-li o přestupek podle odstavce 1 písm. a), b), c), d), e), f) nebo g),
- b) 500 000 Kč, jde-li o přestupek podle odstavce 1 písm. h), i), j), k), l), m), n), o) nebo ~~ff)~~,

(zkráceno - text neobsahující změny byl vypuštěn)

§ 156

Společné ustanovení k přestupkům

Přestupky podle tohoto zákona projednává a pokuty vybírá Úřad, s výjimkou přestupků podle § 148 odst. 1 písm. f) až h) a j), § 149 odst. 1 písm. g) až k), § 153 odst. 1 písm. b), s) až z) a ff) a § 154 odst. 1 písm. e), které projednává a za něž pokuty vybírá Národní úřad pro kybernetickou a informační bezpečnost.

(zkráceno - text neobsahující změny byl vypuštěn)

Zmocňovací ustanovení

Úřad vydá vyhlášku k provedení § 7 odst. 3, § 9 odst. 8, § 15a odst. 7, § 23 odst. 2, § 33, § ~~34 odst. 6, § 35 odst. 6, § 36 odst. 4, § 44, 53 písm. a) a f), § 64, § 75a odst. 4, § 79 odst. 8, § 85 odst. 5 a § 135. Národní úřad pro kybernetickou a informační bezpečnost vydá vyhlášku k provedení § 34 odst. 6, § 35 odst. 6, § 36 odst. 4, § 44 a § 53 písm. b) až f).~~

(zkráceno - text neobsahující změny byl vypuštěn)

Zaorálek v. r.

Klaus v. r.

Paroubek v. r.

-
- 1) Například § 3 zákona č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích, § 2 odst. 7 zákona č. 238/2000 Sb., o Hasičském záchranném sboru České republiky a o změně některých zákonů, § 55b odst. 3 zákona č. 49/1997 Sb., o civilním letectví a o změně a doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, ve znění zákona č. 258/2002 Sb.
 - 2) Zákon č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů.
 - 3) Zákon č. 131/2000 Sb., o hlavním městě Praze, ve znění pozdějších předpisů.
 - 4) Zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů.
 - 5) Zákon č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů.
 - 6) Zákon č. 289/2005 Sb., o Vojenském zpravodajství.
 - 7) Zákon č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů.
 - 8) Obchodní zákoník.
 - 9) § 2 odst. 2 obchodního zákoníku.
 - 10) § 14 odst. 3 trestního zákoníku.
 - 11) Zákon č. 269/1994 Sb., o Rejstříku trestů, ve znění zákona č. 126/2003 Sb.
 - 12) § 68 odst. 1 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů.
 - 13) § 3 zákona č. 153/1994 Sb., o zpravodajských službách České republiky.
 - 15) Zákon č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.
 - 17) Zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů.
 - 18) § 7 a násl. zákona č. 499/2004 Sb.
 - 19) § 10 zákona č. 153/1994 Sb.
 - 20) Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.
 - 21) Například § 14 odst. 3 zákona č. 219/1999 Sb., o ozbrojených silách České republiky, § 50a odst. 1 zákona č. 283/1991 Sb., o Policii České republiky, ve znění zákona č. 26/1993 Sb.
 - 24) § 18 odst. 1 zákona č. 153/1994 Sb.
§ 15 odst. 2 zákona č. 154/1994 Sb.
 - 25) § 33f zákona č. 13/1993 Sb., celní zákon, ve znění zákona č. 1/2002 Sb. § 23f zákona č. 283/1991 Sb., ve znění zákona č. 265/2001 Sb.
 - 26) Zákon č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.
 - 27) Zákon č. 361/2003 Sb., o služebním poměru příslušníků bezpečnostních sborů, ve znění pozdějších předpisů.
 - 28) Trestní řád.
Občanský soudní řád.

Soudní řád správní.

- 28a) Zákon č. 125/2008 Sb., o přeměnách obchodních společností a družstev.
- 29) Například zákon č. 218/2002 Sb., o službě státních zaměstnanců ve správních úřadech a o odměňování těchto zaměstnanců a ostatních zaměstnanců ve správních úřadech (služební zákon), ve znění pozdějších předpisů, zákon č. 312/2002 Sb., o úřednících územních samosprávných celků a o změně některých zákonů, ve znění zákona č. 46/2004 Sb., vyhláška č. 50/1978 Sb., o odborné způsobilosti v elektrotechnice, ve znění vyhlášky č. 98/1982 Sb.
- 30) Například zákon č. 283/1991 Sb., ve znění pozdějších předpisů, zákon č. 137/2001 Sb.
- 31) Například § 47a odst. 6 zákona č. 283/1991 Sb., ve znění pozdějších předpisů, § 21 odst. 1 zákona č. 137/2001 Sb.
- 32) Například zákon č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálem a o doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, a zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů, ve znění pozdějších předpisů, zákon č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.
- 33) Zákon č. 273/2001 Sb., o právech příslušníků národnostních menšin a o změně některých zákonů, ve znění zákona č. 320/2002 Sb.
- 34) Zákon č. 41/1993 Sb., o ověřování shody opisů nebo kopie s listinou a o ověřování pravosti podpisu okresními a obecními úřady a o vydávání potvrzení orgány obcí a okresními úřady, ve znění pozdějších předpisů.
- 35) Zákon č. 167/1998 Sb., o návykových látkách a o změně některých dalších zákonů, ve znění pozdějších předpisů.
- 36) § 115 občanského zákoníku.
- 37) § 18 a § 19 odst. 1 zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
- 38) Zákon č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů.
- 39) § 116 občanského zákoníku.
- 40) Zákon č. 119/1992 Sb., o cestovních náhradách, ve znění pozdějších předpisů.
- 41) Zákon č. 36/1967 Sb., o znalcích a tlumočnících.
- 42) Soudní řád správní.
- 43) Zákon č. 153/1994 Sb., ve znění pozdějších předpisů.
Zákon č. 283/1991 Sb., ve znění pozdějších předpisů.
- 43a) Zákon č. 133/2000 Sb., o evidenci obyvatel a o rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů.
- 43b) § 1 zákona č. 133/2000 Sb., ve znění pozdějších předpisů.
- 43c) § 13b zákona č. 133/2000 Sb., ve znění zákona č. 53/2004 Sb. a zákona č. 342/2006 Sb.
- 43d) Zákon č. 40/1993 Sb., o nabytí a pozbytí státního občanství České republiky, ve znění pozdějších předpisů.
- 43e) § 4 písm. h) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
- 43f) § 57 zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů.
- 44) Zákon č. 153/1994 Sb., ve znění pozdějších předpisů.
Zákon č. 154/1994 Sb., ve znění pozdějších předpisů.
- ~~45) Zákon č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů.~~

(zkráceno - text neobsahující změny byl vypuštěn)