Sbírka zákonů a mezinárodních smluv

ČESKÁ REPUBLIKA

Zpřístupněna dne 19. prosince 2024

Vyhláška č. 430/2024 Sb.

Vyhláška o způsobilosti informačních a komunikačních systémů a samostatných elektronických zařízení, stínicích komor, zabezpečených oblastí a objektů k ochraně před únikem utajovaných informací kompromitujícím vyzařováním a o některých náležitostech žádosti o uzavření smlouvy o zajištění činnosti (vyhláška o kompromitujícím vyzařování)

430

VYHLÁŠKA

ze dne 18. prosince 2024

o způsobilosti informačních a komunikačních systémů a samostatných elektronických zařízení, stínicích komor, zabezpečených oblastí a objektů k ochraně před únikem utajovaných informací kompromitujícím vyzařováním a o některých náležitostech žádosti o uzavření smlouvy o zajištění činnosti (vyhláška o kompromitujícím vyzařování)

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 34 odst. 7 písm. a), § 35 odst. 6 písm. b), § 36 odst. 4 a § 53 písm. b) až f) zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění zákona č. 255/2011 Sb., 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 předpis Evropské unie[1)]

a) některé požadavky na informační systém spočívající v zabezpečení komponent informačního systému před únikem utajovaných informací stupně utajení Důvěrné nebo vyššího elektromagnetickým, akustickým nebo jiným fyzikálním vyzařováním, jehož nežádoucím zachycením a následným zpracováním je možné utajované informace získat (dále jen „kompromitující vyzařování“), a

b) některé náležitosti projektu bezpečnosti komunikačního systému spočívající v naplnění bezpečnostních požadavků na zabezpečení komponent komunikačních systémů před únikem utajovaných informací kompromitujícím vyzařováním.

(2) Tato vyhláška dále stanoví

a) podmínky bezpečného provozování elektrických nebo elektronických zařízení, která nejsou součástí informačního nebo komunikačního systému, zpracovávajících utajované informace stupně utajení Důvěrné nebo vyššího (dále jen „samostatné elektronické zařízení“) z hlediska zabezpečení před únikem utajovaných informací kompromitujícím vyzařováním,

b) náležitosti žádosti a opakované žádosti o certifikaci stínicí komory a dokumentaci nezbytnou k provedení certifikace stínicí komory,

c) způsob a podmínky provádění certifikace stínicí komory a jejich opakování a obsah certifikační zprávy podle § 46 odst. 13 zákona,

d) vzor certifikátu stínicí komory,

e) náležitosti žádosti o ověření způsobilosti elektrických nebo elektronických zařízení, které jsou součástí informačního nebo komunikačního systému zpracovávajícího utajované informace stupně utajení Důvěrné nebo vyšší (dále jen „komponenta informačního nebo komunikačního systému"), samostatného elektronického zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajovaných informací kompromitujícím vyzařováním (dále jen „způsobilost") a způsob hodnocení jejich způsobilosti a

f) náležitosti žádosti o uzavření smlouvy o zajištění činnosti podle § 52 zákona, jejímž předmětem je provádění měření možného úniku utajovaných informací podle § 45 odst. 4 zákona a provádění dílčích úloh při ověřování způsobilosti stínicí komory podle § 46 odst. 15 zákona.

§ 2

Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) zónovým měřením zjišťování útlumu kompromitujícího vyzařování v prostředí mezi umístěním komponent informačního nebo komunikačního systému nebo samostatným elektronickým zařízením a hranicí kontrolovaného prostoru a následným vyhodnocením a

b) technickou kontrolou ověření způsobilosti zabezpečených oblastí a objektů za účelem zjištění nedovoleného použití technických prostředků určených k získávání informací.

ČÁST DRUHÁ

KOMPROMITUJÍCÍ VYZAŘOVÁNÍ

HLAVA I

Informační a komunikační systém

§ 3

Bezpečnostní požadavky na ochranu před kompromitujícím vyzařováním

(1) Komponenty informačního nebo komunikačního systému musí být způsobilé k ochraně před kompromitujícím vyzařováním a musí být umístěny tak, aby bylo zamezeno nepovolané osobě odezírat, odposlouchávat nebo jinak získávat utajované informace.

(2) Komponenty informačního nebo komunikačního systému nesmí obsahovat funkční bezdrátové technologie, není-li v rámci ověřování způsobilosti stanoveno jinak.

§ 4

Žádost o ověření způsobilosti komponent informačního nebo komunikačního systému

(1) Žádost o ověření způsobilosti komponent informačního nebo komunikačního systému obsahuje

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

b) identifikaci komponent informačního nebo komunikačního systému, jejichž způsobilost má být ověřena,

c) údaj o stupni utajení utajovaných informací, které budou prostřednictvím komponent informačního nebo komunikačního systému zpracovávány, a

d) odůvodnění žádosti, které obsahuje účel využití komponent.

(2) Zpravodajská služba uvádí v žádosti podle odstavce 1 údaje podle písmen b) až d) pouze v rozsahu, který neohrozí plnění jejích úkolů podle jiného právního předpisu.

§ 5

Způsob hodnocení způsobilosti komponent informačního nebo komunikačního systému

(1) Hodnocení způsobilosti komponent informačního nebo komunikačního systému provádí Národní úřad pro kybernetickou a informační bezpečnost zpravidla měřením úrovní jejich kompromitujícího vyzařování a porovnáním naměřených hodnot s nejvýše přípustnými hodnotami.

(2) V rámci hodnocení způsobilosti posuzuje Národní úřad pro kybernetickou a informační bezpečnost zprávu o výsledku měření úrovní kompromitujícího vyzařování komponent informačního nebo komunikačního systému provedeného 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 § 16, bylo-li měření provedeno.

(3) Jsou-li v průběhu hodnocení způsobilosti komponent informačního nebo komunikačního systému zjištěny nedostatky v ochraně utajovaných informací před únikem kompromitujícím vyzařováním podle odstavce 1, vyzve Národní úřad pro kybernetickou a informační bezpečnost žadatele k jejich odstranění.

(4) Výsledek hodnocení způsobilosti je uveden v rozhodnutí o ověření způsobilosti komponent informačního nebo komunikačního systému.

HLAVA II

Samostatné elektronické zařízení

§ 6

(1) Podmínkou provozování samostatného elektronického zařízení je jeho způsobilost.

(2) Samostatné elektronické zařízení nesmí obsahovat funkční bezdrátové technologie, není-li v rámci ověřování způsobilosti stanoveno jinak.

(3) Samostatné elektronické zařízení musí být umístěno tak, aby bylo zamezeno nepovolané osobě odezírat, odposlouchávat nebo jinak získávat utajované informace.

(4) Při podání žádosti o ověření způsobilosti, při hodnocení způsobilosti a měření úrovní kompromitujícího vyzařování samostatného elektronického zařízení se použijí § 4 a 5 obdobně.

HLAVA III

Zabezpečená oblast a objekt

§ 7

Žádost o ověření způsobilosti zabezpečené oblasti nebo objektu

(1) Žádost o ověření způsobilosti zabezpečené oblasti nebo objektu 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 žadatelem podnikatel,

c) identifikaci zabezpečené oblasti nebo objektu, jejichž způsobilost má být ověřena,

d) údaj o stupni utajení utajovaných informací, které budou zpracovávány v zabezpečené oblasti nebo objektu, a

e) odůvodnění žádosti, které obsahuje účel využití zabezpečené oblasti nebo objektu.

(2) K žádosti žadatel přiloží zprávu o výsledku zónového měření zabezpečené oblasti nebo objektu provedeného 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 § 16, bylo-li měření provedeno.

(3) Zpravodajská služba uvádí v žádosti podle odstavce 1 údaje podle písmen c) až e) 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.

§ 8

Hodnocení způsobilosti zabezpečené oblasti nebo objektu

(1) Hodnocení způsobilosti zabezpečené oblasti nebo objektu provádí Národní úřad pro kybernetickou a informační bezpečnost zónovým měřením. V zabezpečené oblasti nebo objektu, kde jsou instalovány komponenty informačního nebo komunikačního systému nebo samostatné elektronické zařízení, které zpracovávají utajované informace stupně utajení Tajné nebo Přísně tajné, nebo v případě potřeby, se v rámci zónového měření provádí technická kontrola podle § 9.

(2) Jsou-li v průběhu hodnocení způsobilosti zabezpečené oblasti nebo objektu zjištěny nedo-

statky, vyzve Národní úřad pro kybernetickou a informační bezpečnost žadatele k jejich odstranění a stanoví k tomu přiměřenou lhůtu.

(3) Výsledek hodnocení způsobilosti je uveden v rozhodnutí o ověření způsobilosti zabezpečené oblasti nebo objektu.

(4) V případě, že zónové měření provádí orgán státu, právnická osoba podle § 60b zákona nebo podnikatel na základě smlouvy o zajištění činnosti podle § 52 zákona, vypracuje o zónovém měření zprávu a oznámí výsledek na vyžádání Národnímu úřadu pro kybernetickou a informační bezpečnost a žadateli.

§ 9

Technická kontrola

(1) Technickou kontrolu provádí Národní úřad pro kybernetickou a informační bezpečnost po dokončení instalace komponent informačního nebo komunikačního systému nebo samostatného elektronického zařízení.

(2) Opakovaná technická kontrola se provádí

a) při podezření na kompromitaci prostorů, kde již byla provedena technická kontrola, nebo

b) při změně, která by mohla mít vliv na ochranu utajovaných informací, zejména v důsledku stavebních úprav zabezpečené oblasti nebo objektu.

HLAVA IV

Instalace komponent informačního systému, komunikačního systému nebo samostatného elektronického zařízení

§ 10

Bezpečnostní požadavky na instalaci

(1) Komponenty informačního nebo komunikačního systému nebo samostatné elektronické zařízení musí být provozovatelem informačního nebo komunikačního systému instalovány tak, aby nedocházelo k úniku utajovaných informací kompromitujícím vyzařováním, a o této instalaci musí být Národním úřadem pro kybernetickou a informační bezpečnost vypracován instalační záznam.

(2) Správnost instalace komponent informačního nebo komunikačního systému je ověřována v rámci certifikace informačního systému nebo schvalování projektu bezpečnosti komunikačního systému. Správná instalace a instalační záznam jsou podmínkou bezpečného provozování samostatného elektronického zařízení.

(3) Jakákoliv změna v instalaci vyžaduje změnu instalačního záznamu.

(4) V případě informačního nebo komunikačního systému nebo samostatného elektronického zařízení provozovaného zpravodajskou službou vypracuje instalační záznam zpravodajská služba.

HLAVA V

Certifikace stínicí komory

§ 11

Stínicí komora

K ochraně utajovaných informací stupně utajení Důvěrné nebo vyššího před jejich únikem kompromitujícím elektromagnetickým vyzařováním lze použít stínicí komoru, která je uzavřeným elektromagneticky stíněným prostorem zabraňujícím šíření elektromagnetického vyzařování mimo tento prostor, certifikovanou Národním úřadem pro kybernetickou a informační bezpečnost.

§ 12

Žádost o certifikaci stínicí komory

(1) Žádost o certifikaci stínicí komory 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 žadatelem podnikatel,

c) označení a údaje o umístění stínicí komory a

d) identifikační údaje výrobce stínicí komory.

(2) K žádosti žadatel přiloží zprávu o výsledku provedení dílčích úloh v rámci hodnocení způsobilosti stínicí komory 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 § 16, byly-li tyto dílčí úlohy provedeny.

(3) 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.

§ 13

Způsob a podmínky provádění certifikace stínicí komory

(1) Certifikaci stínicí komory provádí Národní úřad pro kybernetickou a informační bezpečnost měřením útlumových vlastností stínicí komory a jejich porovnáním s nejvýše přípustnými hodnotami.

(2) Měření útlumových vlastností stínicí komory lze provádět za spoluúčasti žadatele a v případě potřeby i dodavatele stínicí komory.

(3) O průběhu a dílčích výsledcích certifikace stínicí komory vypracuje Národní úřad pro kybernetickou a informační bezpečnost zprávu, která je podkladem pro vydání certifikátu.

(4) Provádí-li dílčí úlohy v rámci hodnocení způsobilosti stínicí komory orgán státu, právnická osoba podle § 60b zákona nebo podnikatel, vypracuje o jejich výsledcích zprávu, která je součástí zprávy podle odstavce 3.

(5) Je-li postupem podle odstavce 1 ověřeno, že stínicí komora má způsobilost, Národní úřad pro kybernetickou a informační bezpečnost vydá certifikát.

(6) Vzor certifikátu stínicí komory je uveden v příloze k této vyhlášce.

§ 14

Certifikační zpráva stínicí komory

Certifikační zpráva stínicí komory obsahuje

a) orientační popis stínicí komory, jejího umístění a účel jejího používání,
b) údaj o stupni utajení zpracovávaných utajovaných informací a
c) zásady a podmínky používání stínicí komory.

§ 15

Opakovaná žádost o certifikaci stínicí komory a způsob jejího provedení

(1) Opakovaná žádost o certifikaci stínicí komory obsahuje

a) jméno a příjmení kontaktní osoby žadatele a kontaktní spojení na ni,
b) identifikaci vydaného certifikátu stínicí komory obsahující jeho držitele, evidenční číslo, datum vydání a dobu platnosti a
c) identifikaci certifikované stínicí komory obsahující její název, typové označení, variantní provedení a její umístění.

(2) K opakované žádosti o certifikaci žadatel přiloží zprávu o výsledku měření útlumových vlastností stínicí komory provedeného 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 § 16, bylo-li měření provedeno.

(3) Národní úřad pro kybernetickou a informační bezpečnost provede na základě opakované žádosti o certifikaci doplňující ověření způsobilosti stínicí komory v nezbytně nutném rozsahu, a ověří-li, že stínicí komora má způsobilost, vydá certifikát.

(4) Národní úřad pro kybernetickou a informační bezpečnost vydá certifikát, doloží-li žadatel, že v době od provedeného měření podle § 13 odst. 1 ke dni uplynutí doby platnosti dosavadního certifikátu stínicí komory nedošlo u stínicí komory ke změnám.

(5) Zpravodajská služba uvádí v žádosti podle odstavce 1 údaje podle písmen b) a c) 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.

ČÁST TŘETÍ

SMLOUVA O ZAJIŠTĚNÍ ČINNOSTI

§ 16

Náležitosti žádosti o uzavření smlouvy o zajištění činnosti podle § 52 zákona, jejímž předmětem je provádění měření možného úniku utajovaných informací podle § 45 odst. 4 zákona a provádění dílčích úloh při ověřování způsobilosti stínicí komory

(1) Žádost o uzavření smlouvy s Národním úřadem pro kybernetickou a informační bezpečnost o zajištění činnosti podle § 52 zákona (dále jen „smlouva o zajištění činnosti“) obsahuje

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

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

(2) Žádost podle odstavce 1, která se týká smlouvy o zajištění činnosti, jejímž předmětem je provádění měření možného úniku utajovaných informací podle § 45 odst. 4 zákona, obsahuje dále

a) identifikaci příslušného odborného pracoviště žadatele, zejména předmět činnosti a podrobnou specifikaci umístění pověřovaného pracoviště, jméno a příjmení kontaktní osoby žadatele a kontaktní spojení na ni,

b) údaje o personálních předpokladech pracoviště k provádění požadovaných činností, zejména jméno a příjmení vedoucího pracovníka odborného pracoviště, jména a příjmení ostatních odborných pracovníků pracoviště,

c) prohlášení odpovědné osoby nebo jí pověřené osoby nebo bezpečnostního ředitele o úrovni fyzické, personální a administrativní bezpečnosti, která je zajištěna pro odborné pracoviště,

d) údaj o stupni utajení utajovaných informací, se kterými je informační systém určen nakládat, a evidenční číslo certifikátu informačního systému, pokud je použití certifikovaného informačního systému potřebné pro provádění činností podle smlouvy o zajištění činnosti,

e) údaje o technickém vybavení odborného pracoviště, potřebném pro provádění činností podle smlouvy o zajištění činnosti, a

f) podmínku vypracování zprávy o průběhu a výsledcích měření a podmínku oznámení výsledku měření žadateli o provedení měření podle § 45 odst. 4 zákona a Národnímu úřadu pro kybernetickou a informační bezpečnost.

(3) Žádost podle odstavce 1, která se týká smlouvy o zajištění činnosti, jejímž předmětem je provádění dílčích úloh při ověřování způsobilosti stínicí komory, obsahuje dále

a) adresu umístění pracoviště provádějícího požadované činnosti,

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

c) údaje o rozsahu požadovaných činností,

d) údaje o personálním zabezpečení požadovaných činností a

e) údaje o technickém a organizačním zajištění požadovaných činností.

ČÁST ČTVRTÁ

PŘECHODNÁ A ZÁVĚREČNÁ USTANOVENÍ

§ 17

Přechodná ustanovení

Elektrická a elektronická zařízení, jejichž způsobilost byla ověřena podle vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb., se považují za způsobilá i podle tohoto právního předpisu podle své povahy jako

a) komponenty informačního nebo komunikačního systému podle § 3 odst. 1, nebo
b) samostatná elektronická zařízení podle § 6 odst. 1.

§ 18

Účinnost

Tato vyhláška nabývá účinnosti dnem 1. ledna 2025.

Ředitel:
Ing. Kintr v. r.

Příloha

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

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

Evidenční číslo certifikátu: .....

.....
(název, typové označení)

Držitel certifikátu: Adresa: IČO:

Výrobce stínicí komory: Adresa: IČO:

Tento certifikát potvrzuje způsobilost stínicí komory k ochraně před únikem utajovaných informací kompromitujícím vyzařováním do a včetně stupně utajení

.....

Platnost od:
Platnost do:

otisk úředního razítka

.....
podpis oprávněného zástupce

Datum vydání:
Přílohy:

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

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.