ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2018

Vyhlásené: 9. 3. 2018 Časová verzia predpisu účinná od: 1. 8.2021 do: 25. 2.2022

Obsah dokumentu je právne záväzný.

69

ZÁKON

z 30. januára 2018

o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

Čl. I

§ 1
Predmet zákona

Tento zákon upravuje

a) organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,

b) národnú stratégiu kybernetickej bezpečnosti,

c) jednotný informačný systém kybernetickej bezpečnosti,

d) organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“) a ich akreditáciu,

e) postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby,

f) bezpečnostné opatrenia,

g) systém zabezpečenia kybernetickej bezpečnosti,

h) kontrolu nad dodržiavaním tohto zákona a audit.

§ 2
Pôsobnosť zákona

(1) Tento zákon ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti.

(2) Tento zákon sa nevzťahuje na

a) požiadavky na zabezpečenie sietí a informačných systémov podľa všeobecného predpisu o ochrane utajovaných skutočností,

b) osobitné ustanovenia o úlohách a oprávneniach orgánu štátu pri ochrane kybernetického priestoru podľa osobitného predpisu,[1])

c) ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov,[2])

d) požiadavky na zabezpečenie sietí a informačných systémov v sektore bankovníctva, financií alebo finančného systému podľa osobitných predpisov,[3]) vrátane štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu,[4]) a ani na platobné systémy a na systémy

zúčtovania a vyrovnania cenných papierov a ich infraštruktúry dohliadané alebo prevádzkované Európskou centrálnou bankou alebo Eurosystémom podľa osobitných predpisov,[5])

e) požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu,[6]) ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona,

f) osobitné predpisy.[7])

§ 3
Vymedzenie základných pojmov

Na účely tohto zákona sa rozumie

a) sieťou elektronická komunikačná sieť podľa osobitného predpisu,[8])

b) informačným systémom funkčný celok, ktorý zabezpečuje získavanie, zhromažďovanie, automatické spracúvanie, udržiavanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archiváciu, likvidáciu a ochranu údajov prostredníctvom technických prostriedkov alebo programových prostriedkov,

c) kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,

d) kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,

e) dôvernosťou záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom,

f) dostupnosťou záruka, že údaj alebo informácia je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj a informácia potrebná a požadovaná,

g) integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,

h) kybernetickou bezpečnosťou stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,

i) rizikom miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,

j) hrozbou každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,

k) kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je

   1. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,
   2. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,
   3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo
   4. ohrozenie bezpečnosti informácií,

l) základnou službou služba, ktorá je zaradená v zozname základných služieb a

   1. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1, alebo

2. je prvkom kritickej infraštruktúry,[9])

m) prevádzkovateľom základnej služby orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena l),

n) digitálnou službou služba, ktorej druh je uvedený prílohe č. 2,

o) poskytovateľom digitálnej služby právnická osoba alebo fyzická osoba – podnikateľ, ktorá poskytuje digitálnu službu a zároveň zamestnáva aspoň 50 zamestnancov a má ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur,

p) riešením kybernetického bezpečnostného incidentu všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a s obmedzením jeho následkov.

§ 4
Pôsobnosť orgánov verejnej moci

Pôsobnosť v oblasti kybernetickej bezpečnosti vykonáva

a) Národný bezpečnostný úrad (ďalej len „úrad“),

b) Ministerstvo dopravy a výstavby Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Ministerstvo hospodárstva Slovenskej republiky, Ministerstvo obrany Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky, Ministerstvo zdravotníctva Slovenskej republiky, Ministerstvo životného prostredia Slovenskej republiky a Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „ústredný orgán“),

c) ministerstvá a ostatné ústredné orgány štátnej správy,[10]) ktoré nie sú ústredným orgánom, Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu sieťových odvetví a iné štátne orgány v rozsahu svojej pôsobnosti (ďalej len „iný orgán štátnej správy“).

§ 5
Úrad

(1) Úrad v oblasti kybernetickej bezpečnosti

a) riadi a koordinuje výkon štátnej správy,

b) určuje štandardy, operačné postupy, vydáva metodiku a politiku správania sa v kybernetickom priestore,

c) určuje zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia,

d) vypracúva národnú stratégiu kybernetickej bezpečnosti a ročnú správu o stave kybernetickej bezpečnosti v Slovenskej republike v spolupráci s príslušnými štátnymi orgánmi,

e) je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami členských štátov Európskej únie a Organizácie Severoatlantickej zmluvy,

f) plní notifikačné a nahlasovacie povinnosti voči príslušným orgánom Európskej únie a Organizácie Severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti,

g) zabezpečuje členstvo Slovenskej republiky v skupine pre spoluprácu a v sieti jednotiek CSIRT,

h) v spolupráci s Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky rozvíja medzinárodnú spoluprácu a sleduje vplyvy aktivít v oblasti kybernetickej bezpečnosti na zahraničnopolitické záujmy Slovenskej republiky a partnerov v rámci Európskej únie

a Organizácie Severoatlantickej zmluvy,

i) spolupracuje s ústrednými orgánmi, inými orgánmi štátnej správy a jednotkami CSIRT, prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb pri plnení úloh podľa tohto zákona,

j) spravuje a prevádzkuje jednotný informačný systém kybernetickej bezpečnosti,

k) na základe oznámenia ústredného orgánu, prevádzkovateľa základnej služby, poskytovateľa digitálnej služby alebo z vlastnej iniciatívy určuje

1. základnú službu a zaraďuje ju do zoznamu základných služieb,
2. digitálnu službu a zaraďuje ju do zoznamu digitálnych služieb,
3. poskytovateľa digitálnej služby a zaraďuje ho do registra poskytovateľov digitálnych služieb,
4. prevádzkovateľa základnej služby a zaraďuje ho do registra prevádzkovateľov základných služieb,

l) vedie a spravuje

1. zoznam základných služieb,
2. register prevádzkovateľov základných služieb,
3. zoznam digitálnych služieb,
4. register poskytovateľov digitálnych služieb,
5. zoznam akreditovaných jednotiek CSIRT,

m) systematicky získava, sústreďuje, analyzuje a vyhodnocuje informácie o stave kybernetickej bezpečnosti v Slovenskej republike,

n) akredituje jednotky CSIRT okrem Národnej jednotky CSIRT a vládnej jednotky CSIRT a zaraďuje ich do zoznamu akreditovaných jednotiek CSIRT,

o) plní úlohy príslušného orgánu pre digitálne služby,

p) zabezpečuje a zodpovedá za koordinované riešenie kybernetických bezpečnostných incidentov na národnej úrovni,

q) rieši kybernetické bezpečnostné incidenty, vyhlasuje výstrahu a varovania pred závažným kybernetickým bezpečnostným incidentom, ukladá povinnosť vykonať reaktívne opatrenie a schvaľuje ochranné opatrenie,

r) zasiela včasné varovania,

s) prijíma vnútroštátne hlásenia o kybernetických bezpečnostných incidentoch,

t) prijíma hlásenia o kybernetických bezpečnostných incidentoch zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom,

u) vykonáva kontrolu, vydáva rozhodnutia o uložení opatrení na nápravu a ukladá pokutu za priestupok alebo iný správny delikt,

v) vykonáva audit alebo požiada certifikovaného audítora kybernetickej bezpečnosti o vykonanie auditu u prevádzkovateľa základnej služby,

w) vydáva znalostné štandardy a zverejňuje ich na svojom webovom sídle, a v spolupráci s Ministerstvom školstva, vedy, výskumu a športu Slovenskej republiky vykonáva a zabezpečuje budovanie bezpečnostného povedomia,

x) koordinuje výskum a vývoj,

y) je vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti a orgánom posudzovania zhody podľa osobitného predpisu[10aa]),

z) plní úlohy kompetenčného a odvetvového centra podľa osobitného predpisu[10ab]),

aa) odníma certifikát kybernetickej bezpečnosti,

ab) v rámci systému certifikácie kybernetickej bezpečnosti vydáva bezpečnostné štandardy, certifikačné schémy a postupy,

ac) plní úlohy ústredného orgánu podľa prílohy č. 1,

ad) vedie a zverejňuje na svojom webovom sídle zoznam orgánov posudzovania zhody v systéme certifikácie kybernetickej bezpečnosti, zoznam certifikačných orgánov audítorov kybernetickej bezpečnosti a zoznam právnických osôb, prostredníctvom ktorých je možné realizovať audity kybernetickej bezpečnosti,

ae) posudzuje bezpečnostné riziká dodávateľa na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby (ďalej len „tretia strana“) pre kybernetickú bezpečnosť Slovenskej republiky a správu o tomto posúdení predkladá Bezpečnostnej rade Slovenskej republiky,

af) predkladá príslušnému osobitnému kontrolnému výboru Národnej rady Slovenskej republiky každoročne správu o dodržiavaní noriem týkajúcich sa ochrany telekomunikačného tajomstva a osobných údajov občanov Slovenskej republiky.

(2) Na účely zabezpečenia plnenia úloh podľa tohto zákona môže úrad na účel zabezpečenia kybernetickej bezpečnosti uzatvoriť písomnú dohodu o spolupráci a o výmene informácií a podkladov s orgánmi verejnej moci alebo s inou právnickou osobou.[10a]) Pri poskytnutí informácií je prijímajúci subjekt povinný zabezpečiť najmenej rovnakú úroveň dôvernosti ako subjekt, ktorý informácie poskytol.

(3) Na účely zabezpečenia plnenia úloh podľa tohto zákona môže úrad uzatvoriť písomnú dohodu o spolupráci s fyzickou osobou. Dohoda o spolupráci musí obsahovať konkrétnu formu a podmienky spolupráce a fyzická osoba musí byť oprávnená na oboznamovanie sa s utajovanými skutočnosťami príslušného stupňa utajenia, ak to plnenie úloh vyžaduje.

§ 5a

(1) Systémom certifikácie kybernetickej bezpečnosti je komplexný súbor pravidiel, technických požiadaviek, noriem a postupov, ktoré sa uplatňujú na certifikáciu alebo posudzovanie zhody konkrétnych produktov, služieb alebo procesov v oblasti sietí a informačných systémov, informačných a komunikačných technológií a kybernetickej bezpečnosti podľa osobitného predpisu.[10b])

(2) Úrad v rámci systému certifikácie kybernetickej bezpečnosti certifikuje produkty, služby a procesy[10c]) ako orgán posudzovania zhody podľa osobitného predpisu.[10d])

(3) Certifikačný orgán[10e]) orgánu posudzovania zhody podľa osobitného predpisu,[10f]) ktorý je verejným subjektom[10g]) a nie je vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti, certifikuje produkty, služby a procesy podľa osobitného predpisu[10g]) v rámci systému certifikácie kybernetickej bezpečnosti.

(4) Úrad odníme európske certifikáty kybernetickej bezpečnosti, ktoré vydal, alebo európske certifikáty kybernetickej bezpečnosti vydané podľa čl. 56 ods. 6 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (ďalej len „nariadenie (EÚ) 2019/881“) orgánmi posudzovania zhody, ktoré nie sú v súlade s nariadením (EÚ) 2019/881 alebo s európskym systémom certifikácie kybernetickej bezpečnosti.

(5) Úrad môže odňať vydaný európsky certifikát kybernetickej bezpečnosti aj držiteľovi certifikátu, ak tento

a) poruší povinnosť podľa čl. 56 ods. 8 nariadenia (EÚ) 2019/881,

b) neumožní úradu získať prístup do priestorov podľa čl. 58 ods. 8 písm. d) nariadenia (EÚ) 2019/881,

c) akýmkoľvek spôsobom znemožní vykonávať oprávnenie podľa čl. 58 ods. 8 písm. b) nariadenia (EÚ) 2019/881.

(6) Na účely tohto zákona sa rozumie

a) produktom produkt IKT podľa čl. 2 ods. 12 nariadenia (EÚ) 2019/881,

b) službou služba IKT podľa čl. 2 ods. 13 nariadenia (EÚ) 2019/881,

c) procesom proces IKT podľa čl. 2 ods. 14 nariadenia (EÚ) 2019/881.

§ 6
Národná jednotka CSIRT

(1) Úrad zriaďuje Národné centrum kybernetickej bezpečnosti ako svoju organizačnú zložku, ktorá má postavenie národnej jednotky CSIRT s pôsobnosťou pre Slovenskú republiku, ktorá musí spĺňať podmienky akreditácie podľa § 14 a plniť úlohy jednotky CSIRT podľa § 15 pre všetky sektory a podsektory uvedené v prílohe č. 1 a digitálne služby okrem tých sektorov a podsektorov, pre ktoré plní úlohy jednotky CSIRT ústredný orgán. Národná jednotka CSIRT je zaradená v zozname akreditovaných jednotiek CSIRT.

(2) Národná jednotka CSIRT plní úlohu ústredného orgánu v rozsahu podľa § 9 ods. 1 písm. a), ak ústredný orgán túto úlohu nezabezpečí spôsobom podľa § 9 ods. 2.

(3) Na činnosti národnej jednotky CSIRT sa vyslaním svojich zástupcov a ďalšími formami spolupráce môže podieľať aj iný orgán štátnej správy v rozsahu a spôsobom ustanovenými na základe uzatvorených zmlúv o spolupráci.

(4) Plnenie úloh úradu podľa odsekov 1 a 2 nezbavuje prevádzkovateľa základnej služby ani ústredný orgán zodpovednosti za plnenie povinností podľa tohto zákona a ani za plnenie povinností vo vzťahu k sieťam a informačným systémom podľa osobitných predpisov.

§ 7
Národná stratégia kybernetickej bezpečnosti

(1) Národná stratégia kybernetickej bezpečnosti je východiskový strategický dokument, ktorý komplexne určuje strategický prístup Slovenskej republiky k zabezpečeniu kybernetickej bezpečnosti. Súčasťou národnej stratégie kybernetickej bezpečnosti je akčný plán ako konkrétny plán čiastkových úloh a zdrojov.

(2) Národná stratégia kybernetickej bezpečnosti obsahuje najmä

a) ciele, priority a rámec riadenia na dosiahnutie týchto cieľov a priorít vrátane úloh a zodpovedností orgánov verejnej moci a ďalších relevantných subjektov,

b) identifikáciu opatrení týkajúcich sa pripravenosti, reakcie a obnovy vrátane spolupráce medzi verejným sektorom a súkromným sektorom,

c) popis bezpečnostného prostredia,

d) definíciu bezpečnostných hrozieb,

e) identifikáciu potrebných zdrojov,

f) určenie vzdelávacích programov, programov na budovanie bezpečnostného povedomia, zvyšovanie informovanosti a odbornej prípravy,

g) určenie plánov výskumu a vývoja,

h) plán posudzovania rizika na účely identifikácie rizík,

i) zoznam subjektov zapojených do vykonávania národnej stratégie kybernetickej bezpečnosti,

j) určenie hlavných zahraničnopolitických partnerov.

(3) Ústredný orgán a iný orgán štátnej správy spolupracujú s úradom na vypracovaní národnej stratégie kybernetickej bezpečnosti a na tento účel sú povinné poskytnúť mu informácie v potrebnom rozsahu.

(4) Národnú stratégiu kybernetickej bezpečnosti schvaľuje vláda Slovenskej republiky.

§ 8
Jednotný informačný systém kybernetickej bezpečnosti

(1) Jednotný informačný systém kybernetickej bezpečnosti je informačný systém, ktorého správcom a prevádzkovateľom je úrad a ktorý slúži na efektívne riadenie, koordináciu, evidenciu a kontrolu výkonu štátnej správy v oblasti kybernetickej bezpečnosti a jednotiek CSIRT. Jednotný informačný systém kybernetickej bezpečnosti je určený aj na spracovanie a vyhodnocovanie údajov a informácií o stave kybernetickej bezpečnosti a slúži pri krízovom plánovaní v čase mieru, riadení štátu v krízových situáciách mimo času vojny a vojnového stavu,[11]) ako aj na potrebné činnosti v čase vojny alebo vojnového stavu.

(2) Jednotný informačný systém kybernetickej bezpečnosti obsahuje komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania. Jednotný informačný systém pozostáva z verejnej časti a neverejnej časti a prístup k nemu je bezodplatný. Verejná časť jednotného informačného systému kybernetickej bezpečnosti obsahuje

a) register ústredných orgánov,

b) zoznam základných služieb,

c) register prevádzkovateľov základných služieb,

d) zoznam digitálnych služieb,

e) register poskytovateľov digitálnych služieb,

f) register kybernetických bezpečnostných incidentov,

g) zoznam akreditovaných jednotiek CSIRT,

h) metodiky, usmernenia, štandardy, politiky a oznamy,

i) informácie a údaje potrebné na používanie jednotného informačného systému kybernetickej bezpečnosti,

j) výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetického bezpečnostného incidentu.

(3) Komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov je komunikačný systém, ktorý zaisťuje systematické získavanie, sústreďovanie, analyzovanie a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch.

(4) Centrálny systém včasného varovania je informačný systém, ktorý zaisťuje včasnú výmenu

informácií o hrozbách, kybernetických bezpečnostných incidentoch a rizikách s nimi spojených medzi úradom a subjektmi podľa odseku 5.

(5) K neverejnej časti jednotného informačného systému kybernetickej bezpečnosti má priamy prístup v elektronickej forme v reálnom čase, v rozsahu určenom úradom alebo osobitným predpisom[12]) a na základe vecnej pôsobnosti

a) ústredný orgán,

b) jednotka CSIRT zaradená v zozname akreditovaných jednotiek CSIRT,

c) prevádzkovateľ základnej služby a poskytovateľ digitálnej služby,

d) Národná banka Slovenska,

e) Úrad na ochranu osobných údajov Slovenskej republiky,

f) Úrad pre reguláciu elektronických komunikácií a poštových služieb,

g) iný orgán verejnej moci rozhodnutím úradu.

(6) Ten, kto je povinný podľa tohto zákona poskytovať informácie, údaje a hlásenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti, je povinný ich poskytovať bezodplatne a bezodkladne po tom, ako sa dozvie o skutočnosti zakladajúcej túto povinnosť. Informácie, údaje a hlásenia sa poskytujú spôsobom určeným funkcionalitou jednotného informačného systému kybernetickej bezpečnosti.

§ 9
Ústredný orgán

(1) Ústredný orgán v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa prílohy č. 1, zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že

a) plní úlohy jednotky CSIRT spôsobom podľa odseku 2,

b) poskytuje úradu požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité na zabezpečenie kybernetickej bezpečnosti; informácie sa poskytujú len za podmienky, že ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy spravodajskej služby podľa osobitného predpisu[13]) alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb konajúcich v jej prospech alebo k ohrozeniu medzinárodnej spravodajskej spolupráce,

c) spolupracuje s ostatnými ústrednými orgánmi a prevádzkovateľmi základných služieb vo svojej pôsobnosti pri plnení úloh podľa tohto zákona,

d) buduje bezpečnostné povedomie, koordinovanú spoluprácu na všetkých stupňoch riadenia kybernetickej bezpečnosti a aplikuje bezpečnostné opatrenia a politiku správania sa v kybernetickom priestore,

e) v spolupráci s úradom určuje špecifické sektorové identifikačné kritériá podľa § 18 ods. 3,

f) identifikuje základnú službu a prevádzkovateľa základnej služby a ich aktuálny zoznam predkladá úradu na účely zaradenia do zoznamu základných služieb a registra prevádzkovateľov základných služieb,

g) spolupracuje so zahraničnou inštitúciou obdobného zamerania.

(2) Ústredný orgán na plnenie úloh podľa odseku 1 písm. a) v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa prílohy č. 1 využíva Národné centrum kybernetickej bezpečnosti alebo zriaďuje a prevádzkuje vlastnú akreditovanú jednotku CSIRT alebo využíva akreditovanú jednotku CSIRT v pôsobnosti ústredného orgánu, ak sa tak zmluvne dohodnú.

§ 10
Kybernetická bezpečnosť iného orgánu štátnej správy

Na účely zaistenia kontinuity a riadenia rizík súvisiacich so zabezpečením sietí a informačných systémov, ktoré nie sú základnou službou a procesu riešenia kybernetických bezpečnostných incidentov, iný orgán štátnej správy a ústredný orgán v rozsahu svojej pôsobnosti zodpovedá za zabezpečenie kybernetickej bezpečnosti tým, že prijíma a dodržiava vhodné a primerané bezpečnostné opatrenia podľa § 20.

§ 10a
Súčinnosť

(1) Orgán verejnej moci, prevádzkovateľ základnej služby a právnická osoba v sektore podľa prílohy č. 1 sú povinní poskytnúť úradu na plnenie jeho úloh pri riešení kybernetického bezpečnostného incidentu podľa tohto zákona požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité na zabezpečenie kybernetickej bezpečnosti a riešenie kybernetického bezpečnostného incidentu; informácie sa poskytujú len za podmienky, že sú nevyhnutné pre riešenie kybernetického bezpečnostného incidentu a ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu[13a]) alebo spravodajskej služby podľa osobitného predpisu[13]) alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb, ktoré konajú v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce.

(2) Žiadosť o súčinnosť musí byť riadne odôvodnená a musí obsahovať konkrétny rozsah požadovanej súčinnosti podľa tohto zákona.

§ 11
Vládna jednotka CSIRT

Zriaďuje sa vládna jednotka CSIRT v pôsobnosti Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky pre podsektor informačné systémy verejnej správy. Vládna jednotka CSIRT musí spĺňať podmienky akreditácie podľa § 14 a plniť úlohy podľa § 15. Vládna jednotka CSIRT sa zaraďuje do zoznamu akreditovaných jednotiek CSIRT.

§ 12
Mlčanlivosť a ochrana osobných údajov

(1) Kto plní alebo plnil úlohy na základe tohto zákona alebo v súvislosti s ním, je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa v súvislosti s plnením úloh podľa tohto zákona dozvedel a ktoré nie sú verejne známe. Povinnosť zachovávať mlčanlivosť trvá aj po skončení dohody o spolupráci podľa § 5 ods. 3, pracovnoprávneho vzťahu alebo obdobného pracovného vzťahu vrátane služobného pomeru.[14]) Ustanoveniami o povinnosti zachovávať mlčanlivosť podľa tohto zákona nie je dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.[15])

(2) O zbavení povinnosti mlčanlivosti osoby podľa odseku 1 rozhodne v pôsobnosti

a) úradu riaditeľ úradu,

b) iného subjektu štatutárny orgán.

(3) Na účely konania pred orgánom verejnej moci, na účely trestného konania, oznamovania skutočnosti nasvedčujúcej tomu, že bol spáchaný trestný čin, alebo oznamovania kriminality alebo inej protispoločenskej činnosti[16]) sa povinnosť zachovávať mlčanlivosť podľa odseku 1 nevzťahuje na prevádzkovateľa základnej služby a poskytovateľa digitálnej služby a jeho zamestnancov.

(4) Oznamovanie kybernetických bezpečnostných incidentov v rozsahu podľa tohto zákona, informovanie o hlásenom kybernetickom bezpečnostnom incidente, úkony súvisiace s riešením kybernetických bezpečnostných incidentov, vyhlásenie výstrahy a varovania spôsobom podľa tohto zákona nie je porušením povinnosti zachovávať mlčanlivosť podľa tohto zákona a podľa osobitných predpisov.[15])

(5) Za škodu spôsobenú prevádzkovateľom základnej služby, poskytovateľom digitálnej služby, ich zamestnancom alebo osobe oznamujúcej kybernetický bezpečnostný incident, ktorá vznikla oznámením podľa odseku 4, zodpovedá úrad.

(6) Na účely riešenia kybernetického bezpečnostného incidentu v rozsahu potrebnom na jeho identifikáciu a zabezpečenia kybernetickej bezpečnosti úrad v záujme národnej bezpečnosti spracováva v jednotnom informačnom systéme kybernetickej bezpečnosti na čas nevyhnutne potrebný osobné údaje spôsobom podľa osobitného predpisu.[17])

(7) Úrad zabezpečí nepretržitú ochranu osobných údajov a informácií spracúvaných podľa tohto zákona pred nezákonným vyzradením, zneužitím, poškodením, neoprávneným zničením, odcudzením a stratou spôsobom podľa osobitného predpisu.[18])

(8) Informácie a osobné údaje získané na základe tohto zákona alebo v súvislosti s ním môže úrad použiť len na plnenie úloh podľa tohto zákona.

§ 13
Akreditácia jednotky CSIRT

(1) Zhodu jednotky CSIRT s podmienkami akreditácie jednotky CSIRT posudzuje úrad na základe žiadosti.

(2) Žiadosť podľa odseku 1 predkladá úradu v elektronickej podobe orgán verejnej moci, ktorý k žiadosti prikladá dokumentáciu preukazujúcu splnenie podmienok akreditácie jednotky CSIRT.

(3) Konanie podľa odseku 1 sa začína dňom doručenia žiadosti úradu podľa odseku 2. Ak žiadosť nie je úplná, úrad vyzve žiadateľa na jej doplnenie v určenej lehote, ktorá nesmie byť kratšia ako desať dní. Ak žiadateľ žiadosť v stanovenej lehote nedoplní požadovaným spôsobom, úrad na žiadosť ďalej neprihliada.

(4) Úrad o akreditácii rozhodne do 90 dní odo dňa doručenia úplnej žiadosti, a ak posúdi splnenie zhody jednotky CSIRT s podmienkami akreditácie jednotky CSIRT, vydá rozhodnutie o akreditácii. Rozhodnutie o akreditácii sa vydáva na dobu určitú, najviac na päť rokov.

(5) Úrad môže na základe žiadosti opakovane predĺžiť platné rozhodnutie o akreditácii, ak nenastala zmena podmienok, na základe ktorých bolo rozhodnutie o akreditácii vydané. Žiadosť podľa predchádzajúcej vety sa predkladá úradu najmenej šesť mesiacov pred uplynutím doby platnosti rozhodnutia o akreditácii, ktoré sa má predĺžiť. Na konanie a na podanie žiadosti sa primerane vzťahujú odseky 2 až 4. Ak úrad predĺženie akreditácie uzná, vydá o tom rozhodnutie podľa odseku 4 s doložkou „predĺženie“.

(6) Úrad na základe žiadosti uzná aj akreditáciu jednotky CSIRT, ktorá bola akreditovaná podľa predpisov iného štátu alebo medzinárodnej organizácie, ak je preukázateľne zabezpečené splnenie podmienok akreditácie jednotky CSIRT; podmienka podľa § 14 písm. a) sa nepreukazuje. Na konanie a na podanie žiadosti sa primerane vzťahujú odseky 2 až 4. Úrad o akreditácii vydá rozhodnutie podľa odseku 4 s doložkou „uznanie“ najviac na dobu platnosti, na ktorú bola jednotka CSIRT akreditovaná podľa predpisov iného štátu alebo medzinárodnej organizácie.

(7) Úrad jednotku CSIRT akreditovanú spôsobom podľa tohto zákona zaradí do zoznamu

akreditovaných jednotiek CSIRT.

§ 14
Podmienky akreditácie jednotky CSIRT

Žiadateľ o akreditáciu jednotky CSIRT podľa § 13 dokumentáciou preukazuje, že jednotka CSIRT

a) má požadované technické, technologické a personálne vybavenie podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad,

b) má vytvorené podmienky umožňujúce chránený prenos a spracovanie údajov spôsobom podľa osobitného predpisu,[19])

c) chráni informácie a údaje, ktoré v súvislosti s plnením povinností podľa tohto zákona získava a spracováva ich tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita,[20])

d) má umiestnenú dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie v zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.[20])

§ 15
Úlohy jednotky CSIRT

(1) Ten, kto plní úlohy jednotky CSIRT v rozsahu svojej pôsobnosti určenej podľa prílohy č. 1, zodpovedá za riešenie kybernetických bezpečnostných incidentov a vykonáva preventívne služby a reaktívne služby.

(2) Preventívne služby sa zameriavajú na prevenciu kybernetických bezpečnostných incidentov

a) vytváraním bezpečnostného povedomia,

b) výcvikom,

c) spoluprácou s ostatnými jednotkami CSIRT,

d) monitorovaním a evidenciou kybernetických bezpečnostných incidentov,

e) pripojením na jednotný informačný systém kybernetickej bezpečnosti,

f) poskytovaním informácií a údajov do jednotného informačného systému kybernetickej bezpečnosti,

g) prijímaním a zasielaním včasného varovania pred kybernetickými bezpečnostnými incidentmi prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.

(3) Reaktívne služby sa zameriavajú na riešenie kybernetických bezpečnostných incidentov a sú nimi najmä

a) výstraha a varovanie,

b) detekcia kybernetických bezpečnostných incidentov,

c) analýza kybernetických bezpečnostných incidentov,

d) odozva, ohraničenie, riešenie a náprava následkov kybernetických bezpečnostných incidentov,

e) asistencia pri riešení kybernetického bezpečnostného incidentu na mieste,

f) reakcia na kybernetický bezpečnostný incident,

g) podpora reakcií na kybernetické bezpečnostné incidenty,

h) koordinácia reakcií na kybernetické bezpečnostné incidenty,

i) návrh opatrení na zabránenie ďalšiemu pokračovaniu, šíreniu a opakovanému výskytu kybernetických bezpečnostných incidentov.

(4) Reaktívne služby vykonáva jednotka CSIRT za účasti prevádzkovateľa základnej služby alebo poskytovateľa digitálnej služby.

§ 16
Povinnosti toho, kto plní úlohy jednotky CSIRT

(1) Ten, kto plní úlohy jednotky CSIRT,

a) musí zabezpečiť, aby jednotka CSIRT v jeho pôsobnosti, ktorá je zaradená v zozname akreditovaných jednotiek CSIRT, nepretržite počas celej doby svojej prevádzky spĺňala podmienky akreditácie jednotky CSIRT podľa § 14 a zároveň plnila všetky úlohy podľa § 15,

b) oznamuje úradu všetky zmeny, ktoré majú vplyv na akreditáciu jednotky CSIRT bezodkladne po tom, ako nastali,

c) si vyžiada vyjadrenie Národnej banky Slovenska alebo Európskej centrálnej banky k postupu ústredného orgánu pri plnení úloh podľa tohto zákona, ak prevádzkovateľom základnej služby je dohliadaný subjekt finančného trhu,[21]) nad ktorým vykonáva dohľad Národná banka Slovenska podľa osobitných predpisov[22]) alebo nad ktorým vykonáva dohľad Európska centrálna banka podľa osobitného predpisu.[22a])

(2) Ak akreditovaná jednotka CSIRT prestane spĺňať podmienky podľa § 14 alebo ak neplní úlohy podľa § 15, ten, kto plní úlohy jednotky CSIRT, to bezodkladne oznámi úradu; úrad na základe oznámenia podľa predchádzajúcej vety zruší rozhodnutie o akreditácii a jednotku CSIRT vyradí zo zoznamu akreditovaných jednotiek CSIRT.

(3) Úrad môže na základe vlastného zistenia oboznámiť toho, kto plní úlohy jednotky CSIRT o nedostatkoch v plnení podmienok podľa § 14 alebo úloh podľa § 15 s uvedením lehoty na ich odstránenie. Ak nedostatky podľa prechádzajúcej vety na základe oznámenia úradu neodstráni v určenej lehote, úrad zruší rozhodnutie o akreditácii a jednotku CSIRT vyradí zo zoznamu akreditovaných jednotiek CSIRT.

§ 17
Základná služba, prevádzkovateľ základnej služby a zaradenie do zoznamu základných služieb

(1) Ak prevádzkovateľ služby v sektore podľa prílohy č. 1 zistí, že došlo k prekročeniu identifikačných kritérií prevádzkovanej služby podľa § 18, je povinný to oznámiť úradu do 30 dní odo dňa, keď prekročenie zistil, najneskôr však do 60 dní, odkedy k prekročeniu došlo.

(2) Úrad zaradí základnú službu podľa § 3 písm. l) prvého bodu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb

a) na základe oznámenia prevádzkovateľom tejto služby podľa odseku 1,

b) na základe podnetu ústredného orgánu, ak došlo k prekročeniu identifikačných kritérií prevádzkovanej služby podľa § 18,

c) z vlastnej iniciatívy, ak sa úrad dozvedel o prekročení identifikačných kritérií prevádzkovanej služby podľa § 18 a nedošlo k postupu podľa písmena a) alebo písmena b).

(3) Úrad zaradí základnú službu podľa § 3 písm. l) druhého bodu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb zo zákona.

(4) Oznámenie podľa odseku 1 musí obsahovať

a) názov a sídlo,

b) kontaktné údaje,

c) zoznam služieb, ktorých sa prekročenie identifikačných kritérií týka,

d) informáciu o možnom alebo existujúcom cezhraničnom presahu služby,

e) percentuálny podiel služby na trhu,

f) geografické rozšírenie služby,

g) informáciu o alternatívnych možnostiach zachovania kontinuity služby v prípade kybernetického bezpečnostného incidentu.

(5) Zaradenie služby do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb oznámi úrad prevádzkovateľovi tejto služby prostredníctvom informačného systému kybernetickej bezpečnosti.

§ 18
Identifikačné kritériá prevádzkovanej služby

(1) Identifikačné kritériá prevádzkovanej služby sú dopadové kritériá a špecifické sektorové kritériá.

(2) Dopadové kritériá sú určené všeobecne záväzným právnym predpisom, ktorý vydá úrad, a zohľadňujú najmä

a) počet používateľov využívajúcich základnú službu,

b) závislosť ostatných sektorov podľa prílohy č. 1 od základnej služby,

c) vplyv, ktorý by mohli mať kybernetické bezpečnostné incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti a záujmy štátu alebo na bezpečnosť štátu,

d) trhový podiel prevádzkovateľa služby,

e) geografické rozšírenie z hľadiska oblasti, ktorú by kybernetický bezpečnostný incident mohol postihnúť,

f) význam prevádzkovateľa základnej služby z hľadiska zachovania kontinuity poskytovania služby.

(3) Špecifické sektorové kritériá zohľadňujú kritériá určené všeobecne záväzným právnym predpisom, ktorý vydá úrad.

(4) Ak prevádzkovateľ služby podľa prílohy č. 1 zistí, že došlo k prekročeniu špecifických sektorových kritérií, oznámi to úradu do 30 dní odo dňa, keď prekročenie zistil v rozsahu podľa § 17 ods. 4 aj v prípade, ak neprekročí dopadové kritériá.

§ 19
Povinnosti prevádzkovateľa základnej služby

(1) Prevádzkovateľ základnej služby je povinný do 12 mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté.

(2) Prevádzkovateľ základnej služby je povinný pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby výkonu tejto činnosti; pri uzatvorení zmluvy sa vykonáva analýza rizík.

(3) Povinnosť uzatvoriť zmluvu podľa odseku 2 neplatí, ak je tretia strana prevádzkovateľom základnej služby alebo poskytovateľom digitálnej služby, alebo ak je riziko vo vzťahu k činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany nízke.

(4) Prevádzkovateľ základnej služby je povinný informovať v nevyhnutnom rozsahu tretiu stranu o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie zmluvy podľa odseku 2 stalo nemožným, ak úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

(5) Ak prevádzkovateľ základnej služby túto službu poskytuje aj v inom členskom štáte Európskej únie, úrad v súčinnosti s príslušným orgánom tohto členského štátu rozhodne o tom, podľa kritérií ktorého členského štátu bude prevádzkovateľ základnej služby identifikovaný tak, aby bol jednoznačne identifikovaný ako prevádzkovateľ základnej služby aspoň v jednom z týchto členských štátov.

(6) Prevádzkovateľ základnej služby je ďalej povinný

a) riešiť kybernetický bezpečnostný incident,

b) bezodkladne hlásiť závažný kybernetický bezpečnostný incident,

c) spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,

d) v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,

e) oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie.

(7) Prevádzkovateľ základnej služby je povinný hlásiť zmeny v údajoch podľa § 17 ods. 4 do 30 dní odo dňa ich vzniku prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.

(8) Prevádzkovateľ základnej služby nezodpovedá za škodu, ktorá vznikne inému subjektu obmedzením kontinuity základnej služby pri riešení kybernetického bezpečnostného incidentu spôsobom a postupom podľa § 27. Za škodu spôsobenú obmedzením kontinuity základnej služby kybernetickým bezpečnostným incidentom plnením povinnosti spôsobom podľa predchádzajúcej vety zodpovedá úrad.

§ 20
Bezpečnostné opatrenia

(1) Bezpečnostnými opatreniami na účely tohto zákona sú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Bezpečnostné opatrenia realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti sa prijímajú s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na bezpečnosť prevádzkovania služby. Bezpečnostné opatrenia sú všeobecné, realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti pre všetky siete a informačné systémy a sektorové, ktoré sa realizujú na základe špecifík kategorizácie sietí

a informačných systémov ústredného orgánu v rozsahu svojej pôsobnosti podľa prílohy č. 1 a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti.

(2) Klasifikácia informácií a kategorizácia sietí a informačných systémov podľa odseku 1 sa vykonáva na základe významnosti, funkcie a účelu informácií a informačných systémov s ohľadom na dôvernosť, integritu, dostupnosť, kvalitu služby a kontrolnú činnosť.

(3) Bezpečnostné opatrenia sa prijímajú a realizujú najmä pre oblasť

a) organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,

b) riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,

c) personálnej bezpečnosti,

d) riadenia prístupov,

e) riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,

f) bezpečnosti pri prevádzke informačných systémov a sietí,

g) hodnotenia zraniteľností a bezpečnostných aktualizácií,

h) ochrany proti škodlivému kódu,

i) sieťovej a komunikačnej bezpečnosti,

j) akvizície, vývoja a údržby informačných sietí a informačných systémov,

k) zaznamenávania udalostí a monitorovania,

l) fyzickej bezpečnosti a bezpečnosti prostredia,

m) riešenia kybernetických bezpečnostných incidentov,

n) kryptografických opatrení,

o) kontinuity prevádzky,

p) auditu, riadenia súladu a kontrolných činností.

(4) Bezpečnostné opatrenia musia zahŕňať najmenej

a) určenie manažéra kybernetickej bezpečnosti, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,

b) detekciu kybernetických bezpečnostných incidentov,

c) evidenciu kybernetických bezpečnostných incidentov,

d) postupy riešenia a riešenie kybernetických bezpečnostných incidentov,

e) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,

f) pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania.

(5) Bezpečnostné opatrenia sa prijímajú a realizujú na základe analýzy rizík kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti. Súčasťou analýzy rizík je aj analýza politického rizika tretej strany, pričom politické riziko sa posudzuje najmä vzhľadom na

a) plnenie záväzkov z medzinárodných zmlúv, ktorými je Slovenská republika viazaná, a na jej členstvo v medzinárodných organizáciách,

b) možnosť ovplyvňovania a zasahovania do činnosti tretej strany štátom, ktorý nie je členským štátom Európskej únie a Organizácie Severoatlantickej zmluvy (ďalej len „cudzí štát“),

c) analýzu vlastníckej štruktúry a riadiacej štruktúry tretej strany vrátane vlastníckeho podielu cudzieho štátu a priamych zahraničných investícií do tretej strany,

d) analýzu právnych predpisov a medzinárodných záväzkov cudzieho štátu v oblasti ochrany základných ľudských práv a slobôd, kybernetickej bezpečnosti, boja proti počítačovej kriminalite, ochrany osobných údajov a ochrany informácií,

e) informácie špecifické pre cudzí štát a informácie spravodajskej služby o možných hrozbách pre záujmy Slovenskej republiky.

Politické riziká schvaľuje vláda Slovenskej republiky na základe stanoviska úradu. Stanovisko úradu sa predkladá Bezpečnostnej rade Slovenskej republiky. Politické riziká úrad zverejňuje v jednotnom informačnom systéme kybernetickej bezpečnosti. Úrad v analýze politického rizika zohľadní vyjadrenie Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky, Ministerstva hospodárstva Slovenskej republiky, Ministerstva vnútra Slovenskej republiky, Slovenskej informačnej služby a Ministerstva obrany Slovenskej republiky z oblasti ich pôsobnosti.

(6) Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

(7) Povinnosť dodržiavať všeobecné bezpečnostné opatrenia a sektorové bezpečnostné opatrenia v rozsahu podľa tohto zákona a všeobecne záväzných právnych predpisov vydaných na jeho vykonanie sa vzťahuje aj na právne vzťahy, o ktorých tak ustanoví osobitný predpis.

§ 21
Digitálna služba a poskytovateľ digitálnej služby

(1) Poskytovateľ digitálnej služby je povinný do 30 dní odo dňa začatia poskytovania digitálnej služby oznámiť úradu

a) názov a sídlo,

b) kontaktné údaje,

c) poskytovanú službu,

d) názov, sídlo a kontaktné údaje zástupcu podľa § 23.

(2) Na základe oznámenia podľa odseku 1 úrad zaradí službu do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb.

(3) Úrad zaradí službu do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb aj na základe vlastného zistenia.

(4) Zaradenie služby do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb oznámi úrad poskytovateľovi tejto služby.

(5) Poskytovateľ digitálnej služby je povinný hlásiť zmeny v údajoch podľa odseku 1 do 30 dní odo dňa ich vzniku.

§ 22
Povinnosti poskytovateľa digitálnej služby

(1) Poskytovateľ digitálnej služby je povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra poskytovateľov digitálnych služieb prijať a dodržiavať vhodné a primerané bezpečnostné opatrenia podľa osobitného predpisu[24]) na účely riadenia rizík súvisiacich s ohrozením kontinuity digitálnej služby a procesu riešenia kybernetických bezpečnostných incidentov. Na tento účel je poskytovateľ digitálnej služby povinný vyčleniť dostatočné personálne, materiálno-technické,

časové a finančné zdroje s cieľom zabezpečenia kontinuity digitálnej služby.

(2) Poskytovateľ digitálnej služby na účely splnenia povinnosti podľa odseku 1 posudzuje najmä

a) bezpečnosť sietí a informačného systému a jeho schopnosť predchádzať a riešiť kybernetický bezpečnostný incident,

b) spôsob zachovania kontinuity digitálnej služby v prípade kybernetického bezpečnostného incidentu,

c) súlad sietí a informačného systému s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti.

(3) Poskytovateľ digitálnej služby je povinný

a) hlásiť každý kybernetický bezpečnostný incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento kybernetický bezpečnostný incident podstatný vplyv podľa osobitného predpisu,[24]) a to bezodkladne po jeho zistení,

b) riešiť hlásený kybernetický bezpečnostný incident,

c) spolupracovať s úradom pri riešení hláseného kybernetického bezpečnostného incidentu.

(4) O hlásenom kybernetickom bezpečnostnom incidente v nevyhnutnom rozsahu informuje poskytovateľ digitálnej služby tretiu stranu, ak by sa plnenie zmluvy stalo nemožným, ak úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

§ 23
Zástupca poskytovateľa digitálnej služby

(1) Zástupcom poskytovateľa digitálnej služby je právnická osoba, ktorá má sídlo v Slovenskej republike, alebo fyzická osoba – podnikateľ, ktorá má miesto podnikania v Slovenskej republike, ak odsek 2 neustanovuje inak, a ktorá je poskytovateľom digitálnej služby písomne poverená konať v jeho mene a na jeho zodpovednosť vo vzťahu k povinnostiam podľa tohto zákona.

(2) Ak poskytovateľ digitálnej služby, ktorý poskytuje digitálnu službu v Slovenskej republike, nemá sídlo v Európskej únii a neustanovil si svojho zástupcu v inom členskom štáte Európskej únie, je povinný si ustanoviť svojho zástupcu v Slovenskej republike.

(3) Ak má poskytovateľ digitálnej služby sídlo v Slovenskej republike alebo tu má ustanoveného zástupcu, ale jeho siete a informačné systémy sa nachádzajú v inom členskom štáte Európskej únie, úrad pri výkone štátnej správy spolupracuje s príslušným orgánom členského štátu Európskej únie.

§ 24
Hlásenie kybernetických bezpečnostných incidentov prevádzkovateľom základnej služby

(1) Prevádzkovateľ základnej služby je povinný hlásiť každý závažný kybernetický bezpečnostný incident, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov.

(2) Závažný kybernetický bezpečnostný incident sa člení na kategóriu prvého (I) stupňa, druhého (II) stupňa a tretieho (III) stupňa v závislosti od

a) počtu používateľov základnej služby alebo digitálnej služby zasiahnutých kybernetickým bezpečnostným incidentom,

b) dĺžky trvania kybernetického bezpečnostného incidentu,

c) geografického rozšírenia kybernetického bezpečnostného incidentu,

d) stupňa narušenia fungovania základnej služby alebo digitálnej služby,

e) rozsahu vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu.

(3) Ak prevádzkovateľ základnej služby využíva na poskytovanie základnej služby poskytovateľa digitálnej služby, je poskytovateľ digitálnej služby povinný hlásiť každý závažný kybernetický bezpečnostný incident, ktorý postihol poskytovateľa digitálnej služby.

(4) Hlásenie kybernetických bezpečnostných incidentov sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.

(5) Ak do okamihu hlásenia kybernetického bezpečnostného incidentu nepominuli jeho účinky, prevádzkovateľ základnej služby je povinný odoslať neúplné hlásenie kybernetického bezpečnostného incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

(6) Na hlásenie kybernetických bezpečnostných incidentov alebo na zaistenie kybernetickej bezpečnosti môže úrad namiesto postupu podľa § 8 ods. 6 uzatvoriť písomnú zmluvu o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov s prevádzkovateľom základnej služby.

§ 24a
Automatizované poskytovanie informácií

(1) Ak je to vzhľadom na povahu alebo dôležitosť základnej služby potrebné a nedôjde k uzatvoreniu zmluvy podľa § 24 ods. 6, úrad môže rozhodnutím uložiť prevádzkovateľovi základnej služby povinnosť automatizovaným spôsobom vyhodnocovať výskyt kybernetického bezpečnostného incidentu a nahlasovať kybernetický bezpečnostný incident. Na tento účel zverejňuje úrad výstrahy, varovania a ďalšie informácie v jednotnom informačnom systéme kybernetickej bezpečnosti. Náklady spojené s technickým zabezpečením vyhodnocovania a nahlasovania kybernetického bezpečnostného incidentu znáša úrad.

(2) Povinnosť podľa odseku 1 nie je možné uložiť, ak ide o siete a informačné systémy, ktoré sa týkajú zabezpečenia obrany alebo bezpečnosti Slovenskej republiky.

(3) Úrad rozhodnutím podľa odseku 1 určí prevádzkovateľa základnej služby, ktorého sa povinnosť týka, spôsob poskytovania a rozsah informácií, ktoré sa týkajú automatizovaného spôsobu vyhodnocovania výskytu kybernetického bezpečnostného incidentu a nahlasovania kybernetického bezpečnostného incidentu a trvanie tejto povinnosti. Rozhodnutie sa môže týkať len takých informácií, ktoré sú nevyhnutné pre zabezpečenie kybernetickej bezpečnosti a riešenie kybernetického bezpečnostného incidentu, ak tento účel nemožno dosiahnuť inak.

(4) Obsah komunikácie a prenášaných správ a ochrana súkromia podľa osobitného predpisu[28a]) plnením povinností podľa odseku 1 nie sú dotknuté.

§ 25
Hlásenie kybernetických bezpečnostných incidentov poskytovateľom digitálnej služby

(1) Poskytovateľ digitálnej služby je povinný hlásiť kybernetický bezpečnostný incident podľa § 22 ods. 3 písm. a) spôsobom podľa § 24 ods. 4.

(2) Ak do okamihu hlásenia kybernetického bezpečnostného incidentu nepominuli jeho účinky, poskytovateľ digitálnej služby je povinný odoslať neúplné hlásenie kybernetického bezpečnostného incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

(3) Na účely hlásenia kybernetických bezpečnostných incidentov a zaistenia funkcionality jednotného informačného systému kybernetickej bezpečnosti môže úrad namiesto postupu uvedeného v § 8 ods. 6 uzatvoriť písomnú zmluvu o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov s poskytovateľom digitálnej služby.

§ 26
Dobrovoľné hlásenie kybernetických bezpečnostných incidentov

(1) Dobrovoľné hlásenie kybernetických bezpečnostných incidentov bez ohľadu na kategorizáciu kybernetického bezpečnostného incidentu sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.

(2) Úrad spracováva a analyzuje dobrovoľné hlásenia kybernetických bezpečnostných incidentov v rozsahu, v akom to úradu umožňujú technické podmienky a kapacity tak, aby nedošlo k neprimeranému zaťažovaniu subjektov a neobmedzovala sa medzinárodná spolupráca.

§ 27
Riešenie kybernetických bezpečnostných incidentov

(1) V prípade závažného kybernetického bezpečnostného incidentu alebo jeho hrozby môže úrad

a) vyhlásiť výstrahu a varovanie pred závažným kybernetickým bezpečnostným incidentom,

b) uložiť povinnosť riešiť kybernetický bezpečnostný incident,

c) uložiť povinnosť vykonať reaktívne opatrenie,

d) požadovať návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu (ďalej len „ochranné opatrenie“).

(2) Výstrahu a varovanie vyhlasuje úrad prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Ak ide o naliehavý verejný záujem, výstraha a varovanie sa vyhlási aj prostredníctvom hromadných oznamovacích prostriedkov[25]) a na ústrednom portáli verejnej správy.

(3) Povinnosť riešiť kybernetický bezpečnostný incident ukladá úrad rozhodnutím tomu, kto plní úlohy jednotky CSIRT, prevádzkovateľovi základnej služby a poskytovateľovi digitálnej služby.

(4) Reaktívne opatrenie je priama odpoveď na závažný kybernetický bezpečnostný incident a zabezpečuje sa službami podľa § 15 ods. 3 písm. b) až g).

(5) Povinnosť vykonať reaktívne opatrenie ukladá úrad rozhodnutím prevádzkovateľovi základnej služby alebo poskytovateľovi digitálnej služby, ktorí sú pri riešení závažného kybernetického bezpečnostného incidentu nečinní, alebo ak riešenie závažného kybernetického bezpečnostného incidentu je zjavne neúspešné. Poskytovateľovi digitálnej služby možno uložiť povinnosť vykonať reaktívne opatrenie iba počas krízovej situácie.[26])

(6) Prevádzkovateľ základnej služby alebo poskytovateľ digitálnej služby je povinný bezodkladne oznámiť a preukázať úradu prostredníctvom jednotného informačného systému kybernetickej bezpečnosti vykonanie reaktívneho opatrenia a jeho výsledok.

(7) Ochranné opatrenie prijíma prevádzkovateľ základnej služby na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.

(8) Prevádzkovateľ základnej služby je na výzvu úradu v určenej lehote povinný predložiť navrhované ochranné opatrenie na schválenie. Úrad rozhodnutím navrhované opatrenie schváli

a určí lehotu na jeho vykonanie. V prípade, ak prevádzkovateľ základnej služby nenavrhne ochranné opatrenie v určenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je prevádzkovateľ základnej služby povinný spolupracovať s úradom, ústredným orgánom a s tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.

(9) Ak úrad na účely zaistenia kybernetickej bezpečnosti vyčerpá všetky spôsoby riešenia závažného kybernetického bezpečnostného incidentu podľa tohto zákona, predloží predsedovi Bezpečnostnej rady Slovenskej republiky informáciu o predpokladaných vplyvoch kybernetického bezpečnostného incidentu na bezpečnosť štátu ako podklad na riešenie krízovej situácie.[27])

(10) Z dôvodu neodkladnosti a naliehavosti riešenia závažného kybernetického bezpečnostného incidentu úrad na účely kybernetickej obrany[28]) informuje Vojenské spravodajstvo, že závažný kybernetický bezpečnostný incident je kategórie tretieho (III) stupňa, alebo o skutočnostiach, ktoré nasvedčujú, že závažný kybernetický bezpečnostný incident môže byť kybernetickým terorizmom. Prevádzkovateľ základnej služby a poskytovateľ digitálnej služby, ktorí hlásia tento kybernetický bezpečnostný incident, sú na účely zabezpečenia kybernetickej obrany povinní poskytnúť Vojenskému spravodajstvu informácie v potrebnom rozsahu. O postupe podľa prvej vety informuje úrad predsedu Bezpečnostnej rady Slovenskej republiky.

§ 27a
Obmedzenie používania produktu, procesu, služby alebo tretej strany

(1) Úrad môže rozhodnutím zakázať alebo obmedziť používanie konkrétneho produktu, procesu, služby alebo tretej strany na poskytovanie základnej služby ak zistí, že takéto používanie

a) neumožňuje alebo zásadným spôsobom sťažuje udržanie kybernetickej bezpečnosti, a tým ohrozuje život alebo zdravie osôb, hospodárske fungovanie štátu, verejný poriadok, bezpečnosť alebo majetok osôb, alebo

b) ohrozuje bezpečnostné záujmy Slovenskej republiky.

(2) Konanie podľa odseku 1 úrad začne z vlastného podnetu alebo na základe odôvodneného podnetu iného orgánu verejnej moci Slovenskej republiky. Oznámenie o začatí konania úrad zverejní najmenej na 30 dní v jednotnom informačnom systéme kybernetickej bezpečnosti a na svojom webovom sídle a počas tejto doby nemôže vydať rozhodnutie.

(3) Úrad pred vydaním rozhodnutia podľa odseku 1 vždy vykoná vo vzťahu k produktu, procesu, službe alebo k tretej strane analýzu rizík podľa § 20 ods. 5 na základe vyjadrenia Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky, Ministerstva hospodárstva Slovenskej republiky, Ministerstva vnútra Slovenskej republiky, Slovenskej informačnej služby a Ministerstva obrany Slovenskej republiky z oblasti ich pôsobnosti. Návrh rozhodnutia predkladá Bezpečnostnej rade Slovenskej republiky a vláde Slovenskej republiky. Od stanoviska vlády Slovenskej republiky sa úrad nemôže odchýliť.

(4) Úrad vydá rozhodnutie podľa odseku 1 iba v prípade, ak prevádzkovateľ základnej služby alebo tretia strana nedostatky podľa odseku 1 neodstráni v primeranej lehote určenej úradom.

(5) Prevádzkovateľ základnej služby je povinný zdržať sa používania konkrétneho produktu, procesu, služby alebo tretej strany uvedenej v rozhodnutí podľa odseku 1 na poskytovanie základnej služby alebo ich používanie obmedziť.

(6) Rozhodnutie podľa odseku 1 sa vyhlási zverejnením v Zbierke zákonov Slovenskej republiky[28b]) a účinky nadobúda dňom vyhlásenia. Ak je vyhlásené rozhodnutie podľa odseku 1 zmenené alebo zrušené, na právny akt, ktorým sa rozhodnutie podľa odseku 1 zmenilo alebo zrušilo, sa prvá veta použije rovnako.

(7) Ak úrad rozhodnutím podľa odseku 1 zakáže alebo obmedzí používanie konkrétneho produktu, procesu, služby alebo tretej strany na poskytovanie základnej služby, v rozhodnutí podľa odseku 1 zároveň určí primeranú dobu zákazu alebo obmedzenia používania konkrétneho produktu, procesu, služby alebo tretej strany, ktorá nemôže byť dlhšia ako dva roky. O zákaze alebo obmedzení podľa prvej vety môže úrad rozhodnúť aj opakovane.

(8) Ak ide o produkt, proces, službu alebo tretiu stranu, ktorú prevádzkovateľ základnej služby začal používať pred zverejnením rozhodnutia podľa odseku 1, je prevádzkovateľ základnej služby povinný zdržať sa používania alebo obmedziť používanie produktu, procesu, služby alebo tretej strany uvedenej v rozhodnutí podľa odseku 1 v primeranej lehote určenej v rozhodnutí, ktorá nie je kratšia ako dva roky a dlhšia ako päť rokov. Zároveň je prevádzkovateľ základnej služby povinný najneskôr do šiestich mesiacov od zverejnenia rozhodnutia podľa odseku 1 vykonať primerané bezpečnostné opatrenia na riadenie rizík podľa odseku 3.

§ 28
Kontrola

(1) Pri výkone kontroly nad dodržiavaním ustanovení tohto zákona a jeho vykonávacích predpisov postupuje úrad ako pri výkone kontroly v štátnej správe podľa osobitného predpisu.[29])

(2) Na účely výkonu kontroly má prevádzkovateľ základnej služby a poskytovateľ digitálnej služby práva a povinnosti kontrolovaného subjektu podľa osobitného predpisu.[30])

(3) Úrad vykoná kontrolu u poskytovateľa digitálnej služby, ak je dôvodné podozrenie, že poskytovateľ digitálnej služby nespĺňa požiadavky ustanovené týmto zákonom.

§ 29
Audit

(1) Auditom kybernetickej bezpečnosti sa rozumie overenie plnenia povinností podľa tohto zákona, posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami podľa tohto zákona a osobitných predpisov, ktoré sa vzťahujú na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy základnej služby a pre prostriedky, ktoré podporujú základné služby. Cieľom auditu kybernetickej bezpečnosti je zabezpečiť požadovanú úroveň kybernetickej bezpečnosti, predchádzať kybernetickým bezpečnostným incidentom a identifikovať nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby na navrhnutie a prijatie opatrení na ich odstránenie, nápravu existujúceho stavu a na predchádzanie kybernetickým bezpečnostným incidentom. Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek ustanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základných služieb.

(2) Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad, a to v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale.

(3) Audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti,[31]) ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby. Certifikáciu audítora kybernetickej bezpečnosti vykonáva osoba akreditovaná podľa osobitného

predpisu[31a]) ako orgán certifikujúci osoby[31b]) (ďalej len „orgán certifikujúci osoby“) v oblasti kybernetickej bezpečnosti.

(4) Právnická osoba zabezpečuje audit kybernetickej bezpečnosti prostredníctvom certifikovaného audítora kybernetickej bezpečnosti alebo certifikovaných audítorov kybernetickej bezpečnosti. Zabezpečovanie auditu kybernetickej bezpečnosti právnickou osobou je podnikaním podľa osobitného predpisu.[31c]) Ak právnická osoba zabezpečuje audit prostredníctvom certifikovaného audítora kybernetickej bezpečnosti, zodpovedá za škodu spôsobenú pri výkone auditu kybernetickej bezpečnosti táto právnická osoba.

(5) Prevádzkovateľ základnej služby je povinný predložiť záverečnú správu o výsledkoch auditu úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.

(6) Úrad môže kedykoľvek vykonať audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby alebo požiadať certifikovaného audítora kybernetickej bezpečnosti, aby vykonal takýto audit u prevádzkovateľa základnej služby s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom.

(7) Náklady na audit kybernetickej bezpečnosti podľa odseku 1 znáša prevádzkovateľ základnej služby a náklady na audit kybernetickej bezpečnosti podľa odseku 6 znáša úrad.

§ 30
Priestupky

(1) Priestupku sa dopustí fyzická osoba, ktorá

a) poruší povinnosť uvedenú v § 12 ods. 1,

b) poskytla nepravdivé údaje v oznámení podľa § 17 ods. 4,

c) poruší niektorú z povinností podľa § 19 ods. 1 až 4, 6 alebo ods. 7,

d) neprijme bezpečnostnú dokumentáciu podľa § 20 ods. 6 alebo

e) nepostupovala v súlade s technickými, organizačnými alebo personálnymi opatreniami prijatými prevádzkovateľom základnej služby.

(2) Za priestupok môže úrad uložiť pokutu od 100 eur do 5 000 eur.

(3) Na priestupky a ich prejednávanie sa vzťahuje všeobecný predpis o priestupkoch.[32])

(4) Priestupky prejednáva úrad a pokuty ukladá úrad.

(5) Pokuty za priestupky sú príjmom štátneho rozpočtu.

§ 31
Správne delikty

(1) Úrad uloží pokutu od 300 eur do 30 000 eur prevádzkovateľovi základnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť

a) podľa § 19 ods. 2 až 4 alebo ods. 7, alebo

b) udržiavať bezpečnostnú dokumentáciu aktuálnu a zodpovedajúcu reálnemu stavu podľa § 20 ods. 6.

(2) Úrad uloží pokutu od 300 eur až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok, najviac však 300 000 eur, prevádzkovateľovi základnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť

a) podľa § 17 ods. 1,

b) podľa § 19 ods. 1 alebo ods. 6,

c) prijať bezpečnostnú dokumentáciu podľa § 20 ods. 6,

d) nahlásiť závažný kybernetický bezpečnostný incident podľa § 24 ods. 1, odoslať neúplné hlásenie podľa § 24 ods. 5 alebo zasielať automatizovaným spôsobom určené systémové informácie podľa § 24a ods. 1,

e) riešiť kybernetický bezpečnostný incident na základe rozhodnutia úradu podľa § 27 ods. 3, vykonať reaktívne opatrenie na základe rozhodnutia úradu podľa § 27 ods. 5 alebo oznámiť a preukázať vykonanie reaktívneho opatrenia a jeho výsledok podľa § 27 ods. 6,

f) predložiť ochranné opatrenie na schválenie alebo vykonať schválené ochranné opatrenie podľa § 27 ods. 8,

g) podľa § 29 ods. 1, 2 alebo ods. 5, alebo

h) vykonať opatrenie na nápravu v lehote podľa záverečnej správy o výsledkoch auditu podľa § 29.

(3) Úrad uloží pokutu od 300 eur do 30 000 eur poskytovateľovi digitálnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť podľa § 21 ods. 5 alebo § 23 ods. 2.

(4) Úrad uloží pokutu od 300 eur až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok, najviac však 300 000 eur, poskytovateľovi digitálnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť podľa § 21 ods. 1, § 22 ods. 3, § 24 ods. 3, § 25 ods. 1 alebo ods. 2 alebo povinnosť vykonať reaktívne opatrenie na základe rozhodnutia úradu podľa § 27 ods. 5.

(5) Úrad uloží pokutu od 300 eur do 100 000 eur tomu, kto

a) na výzvu úradu neposkytne informácie podľa § 7 ods. 3,

b) neposkytne úradu požadovanú súčinnosť alebo informácie podľa § 10a ods. 1,

c) používa konkrétny produkt, službu alebo proces v rozpore s § 27a ods. 5.

(6) Úrad uloží pokutu od 300 eur do 100 000 eur výrobcovi alebo poskytovateľovi produktov, služieb alebo procesov, ktorý sa dopustí správneho deliktu tým, že podľa čl. 53 nariadenia (EÚ) 2019/881 vydá EÚ vyhlásenie o zhode, ktoré je v rozpore s požiadavkami ustanovenými v Európskom systéme certifikácie kybernetickej bezpečnosti.

(7) Úrad uloží pokutu od 300 eur do 100 000 eur výrobcovi alebo poskytovateľovi certifikovaných produktov, služieb alebo procesov alebo výrobcovi alebo poskytovateľovi produktov, služieb a procesov, pre ktoré je vydané EÚ vyhlásenie o zhode, ktorý sa dopustí správneho deliktu tým, že nezverejní v elektronickej podobe alebo neaktualizuje doplňujúce informácie o kybernetickej bezpečnosti podľa čl. 55 ods. 1 písm. a) až d) nariadenia (EÚ) 2019/881.

(8) Úrad uloží pokutu od 300 eur do 100 000 eur orgánu posudzovania zhody, držiteľovi európskeho certifikátu kybernetickej bezpečnosti alebo vydavateľovi EÚ vyhlásení o zhode, ktorý sa dopustí správneho deliktu tým, že

a) neposkytne vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti informácie potrebné na plnenie svojich úloh podľa čl. 58 ods. 8 písm. a) nariadenia (EÚ) 2019/881,

b) znemožní vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti viesť vyšetrovanie v podobe auditu podľa čl. 58 ods. 8 písm. b) nariadenia (EÚ) 2019/881.

(9) Úrad uloží pokutu od 300 eur do 100 000 eur orgánu posudzovania zhody alebo držiteľovi európskeho certifikátu kybernetickej bezpečnosti, ktorý sa dopustí správneho deliktu tým, že neumožní vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti prístup do priestorov

podľa čl. 58 ods. 8 písm. d) nariadenia (EÚ) 2019/881.

(10) Pri ukladaní pokuty za správny delikt úrad prihliadne na závažnosť správneho deliktu, najmä na spôsob jeho spáchania, trvanie, následky a na okolnosti, za ktorých bol spáchaný.

(11) Ak do jedného roka odo dňa nadobudnutia právoplatnosti rozhodnutia o uložení pokuty dôjde k opätovnému porušeniu povinností, za ktoré bola pokuta uložená, úrad uloží pokutu až do dvojnásobku výšky súm uvedených alebo vypočítaných podľa odsekov 1 až 10.

(12) Celkovým ročným obratom podľa odsekov 2 a 4 sa na účely tohto zákona rozumie súčet všetkých tržieb, výnosov alebo príjmov z predaja tovaru alebo služieb bez nepriamych daní, ku ktorému sa pripočíta poskytnutá finančná pomoc. Obrat vyjadrený v cudzej mene sa prepočíta na eurá, pričom na prepočet cudzej meny na eurá sa použije priemer referenčných výmenných kurzov určených a vyhlásených Európskou centrálnou bankou alebo Národnou bankou Slovenska, ktoré sú platné pre príslušné účtovné obdobie.[33])

(13) Predchádzajúcim účtovným obdobím na účely tohto zákona je účtovné obdobie, za ktoré bola zostavená posledná účtovná závierka.

(14) Pokutu za správny delikt možno uložiť do dvoch rokov odo dňa zistenia porušenia povinnosti, najneskôr však do štyroch rokov odo dňa, keď k porušeniu povinnosti došlo.

(15) Pokuta za správny delikt je splatná do 30 dní odo dňa nadobudnutia právoplatnosti rozhodnutia o jej uložení.

(16) Pokuty za správny delikt sú príjmom štátneho rozpočtu.

§ 32
Splnomocňovacie ustanovenia

(1) Úrad ustanoví všeobecne záväzným právnym predpisom

a) podrobnosti o technickom, technologickom a personálnom vybavení jednotky CSIRT [§ 14 písm. a)],

b) identifikačné kritériá prevádzkovanej služby (§ 18),

c) obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (§ 20 ods. 1 a 6),

d) bezpečnostné štandardy a znalostné štandardy v oblasti kybernetickej bezpečnosti (§ 5 ods. 1 písm. w), § 20 ods. 1),

e) identifikačné kritériá pre jednotlivé kategórie kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov (§ 24 ods. 1 a 4),

f) pravidlá auditu kybernetickej bezpečnosti, časový rozsah a periodicitu vykonávania auditu kybernetickej bezpečnosti, podrobnosti o akreditácii certifikačných orgánov certifikujúcich audítorov kybernetickej bezpečnosti, certifikačnú schému a postupy pri certifikácii audítora kybernetickej bezpečnosti, podrobnosti o certifikáte audítora kybernetickej bezpečnosti a podrobnosti o formáte a obsahu záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti (§ 29 ods. 1 až 5),

g) certifikačné schémy a postupy v systéme certifikácie kybernetickej bezpečnosti,

h) bezpečnostné opatrenia, ak si to vyžadujú právne záväzné akty a odporúčania Európskej únie pre oblasť kybernetickej bezpečnosti.

(2) Ústredný orgán sa v spolupráci s úradom splnomocňuje na vydanie všeobecne záväzného právneho predpisu, ktorým ustanovia sektorové bezpečnostné opatrenia v rozsahu svojej

pôsobnosti podľa prílohy č. 1 a v súlade s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti.

§ 33
Spoločné ustanovenia

(1) Na konanie úradu podľa § 13 ods. 7, § 16 ods. 2 a 3, § 17, § 21 a § 27 sa nevzťahuje správny poriadok.

(2) Informácie, údaje a hlásenia podľa tohto zákona sa predkladajú úradu v elektronickej podobe prostredníctvom elektronického formulára, ktorého vzor zverejní úrad prostredníctvom jednotného informačného systému kybernetickej bezpečnosti a na ústrednom portáli verejnej správy v module elektronických formulárov.

(3) Ak služba spĺňa podmienky základnej služby a zároveň aj digitálnej služby, považuje sa za základnú službu a zaraďuje sa len do zoznamu základných služieb a jej prevádzkovateľ do registra prevádzkovateľov základných služieb.

(4) Ak základná služba spadá do viacerých sektorov alebo podsektorov podľa prílohy č. 1, pôsobnosť podľa tohto zákona vykonáva ústredný orgán určený úradom.

(5) Ústredný orgán, ktorým je Ministerstvo obrany Slovenskej republiky, plní úlohy, ktoré mu vyplývajú z tohto zákona, prostredníctvom Vojenského spravodajstva.[34])

Prechodné a záverečné ustanovenia

§ 34

(1) Úrad sprístupní jednotný informačný systém kybernetickej bezpečnosti spôsobom podľa § 8 do 18 mesiacov odo dňa účinnosti toho zákona.

(2) Osoba existujúca ku dňu účinnosti tohto zákona je povinná odo dňa prekročenia identifikačných kritérií podľa § 18 ods. 1, najneskôr však do šiestich mesiacov odo dňa účinnosti tohto zákona, podať úradu oznámenie podľa § 18 ods. 1.

(3) Osoba existujúca ku dňu účinnosti tohto zákona je povinná do šiestich mesiacov odo dňa účinnosti tohto zákona oznámiť úradu informácie podľa § 21 ods. 1.

(4) Ústredný orgán je povinný do 30 dní odo dňa zistenia prekročenia identifikačných kritérií podľa § 18 ods. 1 prevádzkovateľom služby existujúcim ku dňu účinnosti tohto zákona, najneskôr však do šiestich mesiacov odo dňa účinnosti tohto zákona, doručiť úradu zoznam podľa § 9 ods. 1 písm. e).

(5) Úrad do 9. novembra 2018 zaradí službu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb, ak ešte nie sú zaradení; na digitálnu službu a jej poskytovateľa sa to vzťahuje rovnako.

(6) Prevádzkovateľ základnej služby zaradený do registra prevádzkovateľov základných služieb podľa odseku 5 je povinný do dvoch rokov odo dňa účinnosti tohto zákona prijať bezpečnostné opatrenia podľa § 20.

(7) Poskytovateľ digitálnej služby zaradený do registra poskytovateľov digitálnych služieb podľa odseku 5 je povinný do dvoch rokov odo dňa účinnosti tohto zákona prijať bezpečnostné opatrenia podľa § 22 ods. 1.

(8) Zmluvy uzatvorené na výkon činností podľa § 19 ods. 2 musí prevádzkovateľ základnej služby

zosúladiť s týmto zákonom najneskôr do dvoch rokov od účinnosti tohto zákona.

(9) Prevádzkovateľ základnej služby je povinný podrobiť sa auditu kybernetickej bezpečnosti a predložiť záverečnú správu o výsledkoch auditu úradu najneskôr do troch rokov od uplynutia lehoty podľa odseku 5.

(10) V súvislosti so zriadením vládnej jednotky CSIRT podľa § 11 prechádzajú odo dňa účinnosti tohto zákona práva a povinnosti vyplývajúce zo štátnozamestnaneckých vzťahov, z pracovnoprávnych vzťahov a iných právnych vzťahov zamestnancov zabezpečujúcich výkon činností jednotky CSIRT v rozpočtovej organizácii DataCentrum zriadenej Ministerstvom financií Slovenskej republiky (ďalej len „DataCentrum“), ako aj práva a povinnosti z iných právnych vzťahov s touto činnosťou súvisiacich, z DataCentra a Ministerstva financií Slovenskej republiky na Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu. Majetok štátu, ktorý bol do 31. marca 2018 v správe DataCentra alebo Ministerstva financií Slovenskej republiky a ktorý slúži na zabezpečenie výkonu činností jednotky CSIRT v DataCentre, prechádza odo dňa účinnosti tohto zákona do správy Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu. Podrobnosti o prechode týchto práv a povinností a o prechode správy majetku štátu sa upravia dohodou medzi Ministerstvom financií Slovenskej republiky, DataCentrom a Úradom podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, v ktorej sa vymedzí najmä druh a rozsah preberaného majetku, práv a povinností.

§ 34a
Prechodné ustanovenia k úpravám účinným od 1. augusta 2021

(1) Prevádzkovateľ základnej služby je povinný zosúladiť bezpečnostné opatrenia platné do 31. júla 2021 s opatreniami podľa § 20 ods. 3 v znení účinnom od 1. augusta 2021 najneskôr do 31. decembra 2021.

(2) Prevádzkovateľ základnej služby môže v období od 1. augusta 2021 do 31. decembra 2023 pre I. a II. kategóriu sietí a informačných systémov podľa osobitného predpisu[35]) zabezpečiť plnenie povinnosti podľa § 29 v znení účinnom od 1. augusta 2021 vykonaním preverenia účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených týmto zákonom v znení účinnom do 31. júla 2021, prostredníctvom manažéra kybernetickej bezpečnosti podľa § 20 ods. 4 písm. a) v znení účinnom od 1. augusta 2021 funkcionalitou jednotného informačného systému kybernetickej bezpečnosti.

(3) Zmluvy uzatvorené podľa § 9 ods. 3 v znení účinnom do 31. júla 2021 sa považujú za zmluvy uzatvorené v súlade s § 9 ods. 2 v znení účinnom od 1. augusta 2021 do konca obdobia, na ktoré sú uzatvorené.

§ 35

Týmto zákonom sa preberajú právne záväzné akty Európskej únie uvedené v prílohe č. 3.

Čl. II

Zákon Národnej rady Slovenskej republiky č. 198/1994 Z. z. o Vojenskom spravodajstve v znení zákona č. 166/2003 Z. z., zákona č. 178/2004 Z. z., zákona č. 319/2012 Z. z., zákona č. 281/2015 Z. z. a zákona č. 444/2015 Z. z. sa dopĺňa takto:

1. V § 2 ods. 1 sa za písmeno g) vkladá nové písmeno h), ktoré znie:

„h) aktivity a ohrozenia v kybernetickom priestore,[1ba])“.

Doterajšie písmená h) až j) sa označujú ako písmená i) až k).

Poznámka pod čiarou k odkazu 1ba znie:

„[1ba]) § 3 písm. b) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“.

2. V § 2 sa za odsek 1 vkladá nový odsek 2, ktorý znie:

„(2) Ak je to potrebné na zabránenie aktivitám a ohrozeniam podľa odseku 1, Vojenské spravodajstvo vykonáva primerané bezpečnostné opatrenia.“.

Doterajšie odseky 2 až 6 sa označujú ako odseky 3 až 7.

3. Za § 4 sa vkladá § 4a, ktorý vrátane nadpisu znie:

„§ 4a
Centrum pre kybernetickú obranu Slovenskej republiky

(1) Vojenské spravodajstvo plní úlohy na úseku obrany štátu v kybernetickom priestore[2a]) (ďalej len „kybernetická obrana“) a kybernetickej bezpečnosti v rozsahu ustanovenom osobitným predpisom[2b]) prostredníctvom Centra pre kybernetickú obranu Slovenskej republiky (ďalej len „centrum“), ktoré je osobitnou organizačnou zložkou Vojenského spravodajstva.

(2) Centrum získava, sústreďuje, analyzuje a vyhodnocuje informácie dôležité na zabezpečenie kybernetickej obrany, informuje dotknuté subjekty a navrhuje vhodné opatrenia.

(3) Centrum je oprávnené požadovať od vlastníka alebo prevádzkovateľa objektov osobitnej dôležitosti, ďalších dôležitých objektov[2c]) a prvkov kritickej infraštruktúry[2d]) súčinnosť a informácie v rozsahu potrebnom na účely zabezpečenia kybernetickej obrany.

(4) Na účely zabezpečenia plnenia úloh podľa tohto zákona má centrum priamy prístup v elektronickej podobe, v reálnom čase a v plnom rozsahu k jednotnému informačnému systému kybernetickej bezpečnosti.[2e])“.

Poznámky pod čiarou k odkazom 2a až 2e znejú:

„[2a]) § 2 ods. 2 zákona č. 319/2002 Z. z. o obrane Slovenskej republiky v znení zákona č. 69/2018 Z. z.

[2b]) Zákon č. 69/2018 Z. z.

[2c]) § 27 ods. 5 zákona č. 319/2002 Z. z. v znení zákona č. 330/2003 Z. z.

[2d]) § 2 písm. a) zákona č. 45/2011 Z. z. o kritickej infraštruktúre.

[2e]) § 8 zákona č. 69/2018 Z. z.“.

4. Za § 14a sa vkladá § 14b, ktorý znie:

„§ 14b

Ak to nie je v rozpore s osobitným predpisom,[4]) na zabránenie aktivitám a ohrozeniam podľa § 2 ods. 1 je Vojenské spravodajstvo oprávnené získavať, sústreďovať a vyhodnocovať informácie odvodené zo signálov v elektromagnetickom spektre. Vojenské spravodajstvo pri plnení týchto úloh vystupuje ako národná autorita k domácim a zahraničným orgánom obdobného zamerania a pôsobnosti.“.

Čl. III

Zákon č. 73/1998 Z. z. o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení zákona č. 58/1999 Z. z., zákona č. 181/1999 Z. z., zákona č. 356/1999 Z. z., zákona č. 224/2000 Z. z., zákona č. 464/2000 Z. z., zákona č. 241/2001 Z. z., zákona č. 98/2002 Z. z., zákona č. 328/2002 Z. z., zákona č. 422/2002 Z. z., zákona č. 659/2002 Z. z., zákona č. 212/2003 Z. z., zákona č. 201/2004 Z. z., zákona č. 178/2004 Z. z, zákona č. 365/2004 Z. z., zákona č. 382/2004 Z. z., zákona č. 201/2004 Z. z., zákona č. 732/2004 Z. z., zákona č. 201/2004 Z. z., zákona č. 727/2004 Z. z., zákona č. 69/2005 Z. z., zákona č. 69/2005 Z. z., zákona č. 623/2005

Z. z., zákona č. 342/2007 Z. z., zákona č. 513/2007 Z. z., zákona č. 61/2008 Z. z., zákona č. 278/2008 Z. z., zákona č. 491/2008 Z. z., zákona č. 445/2008 Z. z., zákona č. 70/2009 Z. z., zákona č. 60/2010 Z. z., zákona č. 151/2010 Z. z., zákona č. 543/2010 Z. z., zákona č. 547/2010 Z. z., zákona č. 48/2011 Z. z., zákona č. 79/2012 Z. z., zákona č. 361/2012 Z. z., zákona č. 345/2012 Z. z., zákona č. 80/2013 Z. z., zákona č. 462/2013 Z. z., zákona č. 307/2014 Z. z., zákona č. 406/2015 Z. z. a zákona č. 125/2016 Z. z. sa dopĺňa takto:

1. V § 84 sa odsek 2 dopĺňa písmenom t), ktoré znie:

„t) príplatok za výkon činnosti v oblasti kybernetickej bezpečnosti.“.

2. Za § 102b sa vkladá § 102c, ktorý vrátane nadpisu znie:

„§ 102c
Príplatok za výkon činnosti v oblasti kybernetickej bezpečnosti

(1) Policajtovi, ktorý vykonáva osobitne významné úlohy alebo mimoriadne náročné činnosti v oblasti kybernetickej bezpečnosti, možno priznať príplatok až do výšky 90 % súčtu funkčného platu a hornej hranice prídavku za výsluhu rokov.

(2) Príplatok podľa odseku 1 určuje minister v závislosti od náročnosti, zodpovednosti a rozsahu činností v oblasti kybernetickej bezpečnosti.

(3) Príplatok podľa odseku 1 sa zaokrúhľuje na 50 eurocentov nahor.“.

Čl. IV

Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení zákona č. 430/2002 Z. z., zákona č. 510/2002 Z. z., zákona č. 165/2003 Z. z., zákona č. 603/2003 Z. z., zákona č. 215/2004 Z. z., zákona č. 554/2004 Z. z., zákona č. 747/2004 Z. z., zákona č. 69/2005 Z. z., zákona č. 340/2005 Z. z., zákona č. 341/2005 Z. z., zákona č. 214/2006 Z. z., zákona č. 644/2006 Z. z., zákona č. 209/2007 Z. z., zákona č. 659/2007 Z. z., zákona č. 297/2008 Z. z., zákona č. 552/2008 Z. z., zákona č. 66/2009 Z. z., zákona č. 186/2009 Z. z., zákona č. 276/2009 Z. z., zákona č. 492/2009 Z. z., zákona č. 129/2010 Z. z., zákona č. 46/2011 Z. z., zákona č. 130/2011 Z. z., zákona č. 314/2011 Z. z., zákona č. 394/2011 Z. z., zákona č. 520/2011 Z. z., zákona č. 547/2011 Z. z., zákona č. 234/2012 Z. z., zákona č. 352/2012 Z. z., zákona č. 132/2013 Z. z., zákona č. 352/2013 Z. z., zákona č. 213/2014 Z. z., zákona č. 371/2014 Z. z., zákona č. 374/2014 Z. z., zákona č. 35/2015 Z. z., zákona č. 252/2015 Z. z., zákona č. 359/2015 Z. z., zákona č. 392/2015 Z. z., zákona č. 405/2015 Z. z., zákona č. 437/2015 Z. z., zákona č. 90/2016 Z. z., zákona č. 91/2016 Z. z., zákona č. 125/2016 Z. z., zákona č. 292/2016 Z. z., zákona č. 298/2016 Z. z., zákona č. 299/2016 Z. z., zákona č. 315/2016 Z. z., zákona č. 386/2016 Z. z., zákona č. 2/2017 Z. z., zákona č. 264/2017 Z. z., zákona č. 279/2017 Z. z. a zákona č. 18/2018 Z. z. sa dopĺňa takto:

§ 91 sa dopĺňa odsekom 13, ktorý znie:

„(13) Za porušenie bankového tajomstva sa nepovažuje plnenie oznamovacej povinnosti banky, zahraničnej banky a pobočky zahraničnej banky voči Národnému bezpečnostnému úradu na účely plnenia ich povinnosti v oblasti kybernetickej bezpečnosti podľa osobitného predpisu.[86j])“.

Poznámka pod čiarou k odkazu 86j znie:

„[86j]) Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“.

Čl. V

Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky v znení zákona č. 330/2003 Z. z., zákona č. 545/2003 Z. z., zákona č. 570/2005 Z. z., zákona č. 333/2007 Z. z., zákona

č. 452/2008 Z. z., zákona č. 473/2009 Z. z. a zákona č. 345/2012 Z. z. sa mení a dopĺňa takto:

1. V § 2 sa za odsek 1 vkladá nový odsek 2, ktorý znie:

„(2) Obrana štátu sa zabezpečuje aj v kybernetickom priestore[1a]) prostredníctvom opatrení zameraných na riešenie závažných kybernetických bezpečnostných incidentov podľa osobitného predpisu[1b]) a obranu objektov osobitnej dôležitosti, ďalších dôležitých objektov a prvkov kritickej infraštruktúry[1c]) pred kybernetickým napadnutím, ktoré v tejto oblasti vykonáva Vojenské spravodajstvo.[1d])“.

Doterajšie odseky 2 až 5 sa označujú ako odseky 3 až 6.

Poznámky pod čiarou k odkazom 1a až 1c znejú:

„[1a]) § 3 písm. b) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

[1b]) § 27 ods. 10 zákona č. 69/2018 Z. z.

[1c]) § 2 písm. a) zákona č. 45/2011 Z. z. o kritickej infraštruktúre.

[1d]) § 4a zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z. o Vojenskom spravodajstve v znení zákona č. 69/2018 Z. z.“.

2. V § 6 písm. f) sa na konci čiarka nahrádza bodkočiarkou a pripájajú tieto slová: „na obranu objektov osobitnej dôležitosti a ďalších dôležitých objektov v kybernetickom priestore sa vzťahuje § 2 ods. 2,“.

3. V § 18 sa za odsek 1 vkladá nový odsek 2, ktorý znie:

„(2) Osoby oprávnené na podnikanie sú na úseku obrany štátu v kybernetickom priestore povinné poskytnúť Vojenským spravodajstvom požadovanú súčinnosť a informácie dôležité na zabezpečenie obrany štátu v kybernetickom priestore.[15d])“.

Doterajší odsek 2 sa označuje ako odsek 3.

Poznámka pod čiarou k odkazu 15d znie:

„[15d]) § 4a ods. 3 zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z. v znení zákona č. 69/2018 Z. z.“.

Čl. VI

Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení zákona č. 638/2005 Z. z., zákona č. 255/2006 Z. z., zákona č. 330/2007 Z. z., zákona č. 668/2007 Z. z., zákona č. 290/2009 Z. z., zákona č. 400/2009 Z. z., zákona č. 192/2011 Z. z., zákona č. 122/2013 Z. z., zákona č. 195/2014 Z. z., zákona č. 261/2014 Z. z., zákona č. 362/2014 Z. z., zákona č. 247/2015 Z. z., zákona č. 338/2015 Z. z., zákona č. 91/2016 Z. z., zákona č. 125/2016 Z. z., zákona č. 301/2016 Z. z., zákona č. 340/2016 Z. z., zákona č. 51/2017 Z. z., zákona č. 152/2017 Z. z. a zákona č. 334/2017 Z. z. sa mení a dopĺňa takto:

1. V § 24 ods. 2 písm. d) sa na konci slovo „alebo“ nahrádza čiarkou.

2. V § 24 ods. 2 písm. e) sa na konci vypúšťa bodka a pripája sa slovo „alebo“.

3. V § 24 sa odsek 2 dopĺňa písmenom f), ktoré znie:

„f) sa navrhovaná osoba na výzvu úradu nedostaví na bezpečnostný pohovor; na výzvu úradu sa primerane vzťahuje § 27 ods. 4.“.

4. V § 35 ods. 2 sa za slová „osoba konajúca v prospech orgánov podľa osobitných predpisov“ vkladá čiarka a slová „osoba na základe dohody podľa osobitného predpisu[18a])“.

Poznámka pod čiarou k odkazu 18a znie:

„[18a]) § 5 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“.

5. § 60 sa dopĺňa odsekom 9, ktorý znie:

„(9) Na poskytovanie utajovaných skutočností medzi ozbrojenými silami Slovenskej republiky

a ozbrojenými silami iného štátu, aliančného a koaličného partnera alebo partnera vo vojenskej operácii v rámci bilaterálnej spolupráce uskutočňovanej podľa osobitného predpisu[23a]) sa nevzťahujú odseky 3 až 6; o poskytnutí utajovaných skutočností podľa predchádzajúcej vety rozhoduje minister obrany, o čom vedie evidenciu.“.

Poznámka pod čiarou k odkazu 23a znie:

„[23a]) § 11 ods. 1 zákona č. 321/2002 Z. z. o ozbrojených silách Slovenskej republiky v znení neskorších predpisov.“.

6. V § 64 sa vypúšťajú odseky 2 a 3.

Doterajší odsek 4 sa označuje ako odsek 2.

7. V § 64 ods. 2 sa slovo „Žiadateľ“ nahrádza slovami „Podnikateľ podľa odseku 1“.

Čl. VII

Zákon č. 45/2011 Z. z. o kritickej infraštruktúre sa mení takto:

1. V § 1 sa vypúšťa odsek 2 vrátane poznámky pod čiarou k odkazu 1.
Súčasne sa zrušuje označenie odseku 1.
2. V § 3 písm. c) sa slová „Ministerstvo financií Slovenskej republiky, Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky“ nahrádzajú slovami „Úrad podpredsedu vlády pre investície a informatizáciu a Ministerstvo dopravy a výstavby Slovenskej republiky“.
3. V § 9 sa vypúšťa odsek 4.
4. V § 10 ods. 2 sa slová „bezpečnostné prvky informačných systémov“ nahrádzajú slovami „bezpečnostné opatrenia podľa osobitného predpisu[4a])“.

Poznámka pod čiarou k odkazu 4a znie:

„[4a]) § 20 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“.

5. Príloha č. 3 vrátane nadpisu znie:

„Príloha č. 3
k zákonu č. 45/2011 Z. z.

SEKTORY V PÔSOBNOSTI ÚSTREDNÝCH ORGÁNOV

Sektor	Podsektor	Ústredný orgán
1. Doprava	Cestná doprava Letecká doprava Vodná doprava Železničná doprava	Ministerstvo dopravy a výstavby Slovenskej republiky
2. Elektronické komunikácie	Satelitná komunikácia Siete a služby pevných elektronických komunikácií a mobilných elektronických komunikácií	Ministerstvo dopravy a výstavby Slovenskej republiky
3. Energetika	Baníctvo Elektroenergetika Plynárenstvo Ropa a ropné produkty	Ministerstvo hospodárstva Slovenskej republiky
4. Pošta	Poskytovanie poštových	Ministerstvo

	služieb, poštový platobný styk a obstarávateľská činnosť	dopravy a výstavby Slovenskej republiky
5. Priemysel	Farmaceutický priemysel Hutnícky priemysel Chemický priemysel	Ministerstvo hospodárstva Slovenskej republiky
6. Informačné a komunikačné technológie	Informačné systémy a siete	Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu
7. Voda a atmosféra	Meteorologická služba Vodné stavby Zabezpečovanie pitnej vody	Ministerstvo životného prostredia Slovenskej republiky
8. Zdravotníctvo		Ministerstvo zdravotníctva Slovenskej republiky

“.

Čl. VIII

Zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení zákona č. 241/2012 Z. z., zákona č. 547/2011 Z. z., zákona č. 352/2013 Z. z., zákona č. 402/2013 Z. z., zákona č. 128/2014 Z. z., zákona č. 402/2013 Z. z., zákona č. 139/2015 Z. z., zákona č. 247/2015 Z. z., zákona č. 269/2015 Z. z., zákona č. 97/2015 Z. z., zákona č. 444/2015 Z. z., zákona č. 391/2015 Z. z., zákona č. 247/2015 Z. z., zákona č. 125/2016 Z. z., zákona č. 353/2016 Z. z., zákona č. 386/2016 Z. z., zákona č. 238/2017 Z. z., zákona č. 243/2017 Z. z., zákona č. 319/2017 Z. z. a zákona č. 56/2018 Z. z. sa dopĺňa takto:

1. § 8 sa dopĺňa odsekom 3, ktorý znie:

„(3) Pri uplatňovaní pôsobnosti úradu vymedzenej týmto zákonom a pôsobnosti Národného bezpečnostného úradu ustanovenej osobitným predpisom[15a]) si tieto úrady vymieňajú informácie a podklady dôležité na zabezpečenie kybernetickej bezpečnosti v rozsahu a spôsobom ustanoveným na základe uzatvorených dohôd o spolupráci. V prípade výmeny informácií prijímajúci úrad zabezpečí rovnakú úroveň dôvernosti ako úrad, ktorý informáciu poskytne.“.

Poznámka pod čiarou k odkazu 15a znie:

„[15a]) Zákon č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“.

2. § 63 sa dopĺňa odsekom 17, ktorý znie:

„(17) Údaje, ktoré sú predmetom telekomunikačného tajomstva podľa odseku 1 písm. b) až d), možno sprístupniť Národnému bezpečnostnému úradu v záujme bezpečnosti štátu na účely riešenia kybernetického bezpečnostného incidentu, na účel ich zberu, spracovávania a uchovávania v rozsahu potrebnom na identifikáciu kybernetického bezpečnostného incidentu a zabezpečenia kybernetickej bezpečnosti podľa všeobecného predpisu o kybernetickej bezpečnosti.[15a])“.

Čl. IX

Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení zákona č. 214/2014

Z. z., zákona č. 29/2015 Z. z., zákona č. 130/2015 Z. z., zákona č. 273/2015 Z. z., zákona č. 272/2016 Z. z., zákona č. 374/2016 Z. z. a zákona č. 238/2017 Z. z. sa mení takto:

V § 60b ods. 3 sa slová „1. mája 2018“ nahrádzajú slovami „1. februára 2019“ a slová „30. apríla 2018“ sa nahrádzajú slovami „31. januára 2019“.

Čl. X

Zákon č. 281/2015 Z. z. o štátnej službe profesionálnych vojakov a o zmene a doplnení niektorých zákonov v znení zákona č. 378/2015 Z. z. a zákona č. 125/2016 Z. z. sa mení a dopĺňa takto:

1. V § 156 ods. 1 sa za písmeno h) vkladá nové písmeno i), ktoré znie:
„i) príplatok za výkon špecializovanej činnosti,“.

   Doterajšie písmená i) až k) sa označujú ako písmená j) až l).

2. V § 156 od. 2 sa slová „písm. a) až i)“ nahrádzajú slovami „písm. a) až j)“.

3. Za § 164 sa vkladá § 164a, ktorý vrátane nadpisu znie:

„§ 164a
Príplatok za výkon špecializovanej činnosti

(1) Profesionálnemu vojakovi, ktorý vykonáva činnosť, ktorá vyžaduje vykonávanie osobitne významných úloh alebo mimoriadne náročných úloh v oblasti kybernetickej bezpečnosti, možno priznať príplatok za výkon špecializovanej činnosti až do výšky 90 % jeho hodnostného platu.

(2) Funkcie a výšku príplatku podľa odseku 1 ustanoví služobný predpis.

(3) Príplatok podľa odseku 1 sa zaokrúhľuje na 50 eurocentov nahor.“.

Čl. XI

Tento zákon nadobúda účinnosť 1. apríla 2018 okrem čl. I § 12 ods. 6, ktorý nadobúda účinnosť 25. mája 2018.

Andrej Kiska v. r.

Andrej Danko v. r.

Robert Fico v. r.

1) § 2 ods. 1 písm. g), ods. 3 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z. o Slovenskej informačnej službe v znení zákona č. 151/2010 Z. z.
§ 2 ods. 1 písm. c) a h), ods. 2 a § 4a zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z. o Vojenskom spravodajstve v znení neskorších predpisov.
Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky neskorších predpisov.

2) Napríklad zákon č. 398/2015 Z. z. o európskom ochrannom príkaze v trestných veciach a o zmene a doplnení niektorých zákonov, zákon č. 91/2016 Z. z. o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

3) Napríklad § 28c, § 28d, § 45 ods. 8 a § 64 ods. 4 zákona č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov, nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27. 7. 2012) v platnom znení, čl. 45 nariadenia Európskeho parlamentu a Rady (EÚ) č. 909/2014 z 23. júla 2014 o zlepšení vyrovnania transakcií s cennými papiermi v Európskej únii, centrálnych depozitároch cenných papierov a o zmene smerníc 98/26/ES a 2014/65/EÚ a nariadenia (EÚ) č. 236/2012 (Ú. v. EÚ L 257, 28. 8. 2014) v platnom znení, § 14 zákona č. 429/2002 Z. z. o burze cenných papierov v znení neskorších predpisov, delegované nariadenie Komisie (EÚ) 2017/584 zo 14. júla 2016, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2014/65/EÚ, pokiaľ ide o regulačné technické predpisy bližšie určujúce organizačné požiadavky na obchodné miesta (Ú. v. EÚ L 87, 31. 3. 2017).

4) Napríklad čl. 127 ods. 2 Zmluvy o fungovaní Európskej únie v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016), čl. 12 ods. 12.1, čl. 22 Protokolu (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016), § 2 zákona Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska v znení neskorších predpisov, § 2 ods. 9 zákona č. 747/2004 Z. z. o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení zákona č. 132/2013 Z. z., nariadenie Rady (EÚ) č. 1024/2013 z 15. októbra 2013, ktorým sa Európska centrálna banka poveruje osobitnými úlohami, pokiaľ ide o politiky týkajúce sa prudenciálneho dohľadu nad úverovými inštitúciami (Ú. v. EÚ L 287, 29. 10. 2013).

5) Napríklad čl. 3 ods. 3.1, čl. 22 Protokolu (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016), nariadenie Európskej centrálnej banky (EÚ) č. 795/2014 z 3. júla 2014 o požiadavkách v oblasti dohľadu nad systémovo dôležitými platobnými systémami (Ú. v. EÚ L 217, 23. 7. 2014).

6) Zákon č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

7) Napríklad nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L257, 28. 8. 2014), zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov.

8) § 2 ods. 1 zákona č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.

9) § 2 písm. a) zákona č. 45/2011 Z. z.

10) § 3 a 21 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov.

10a) Napríklad § 6 ods. 2 písm. k) zákona Národnej rady Slovenskej republiky č. 566/1992 Zb. v znení neskorších predpisov.

10aa) Čl. 58 a 60 ods. 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7. 6. 2019).

10ab) Čl. 7 nariadenia Európskeho parlamentu a Rady (EÚ) 2021/887, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier (Ú. v. EÚ L 202, 8. 6. 2021).

10b) Čl. 2 ods. 10 nariadenia (EÚ) 2019/881.

10c) Napríklad STN EN ISO/IEC 17065 Posudzovanie zhody. Požiadavky na orgány vykonávajúce certifikáciu výrobkov, procesov a služieb (ISO/IEC 17065) (01 5256).

10d) Čl. 52 ods. 5 až 7 nariadenia (EÚ) 2019/881.

10e) Čl. 60 ods. 2 a príloha nariadenia (EÚ) 2019/881.

10f) Čl. 56 ods. 5 písm. b) nariadenia (EÚ) 2019/881.

10g) Čl. 52 ods. 5 a 6 nariadenia (EÚ) 2019/881.

11) Napríklad zákon č. 319/2002 Z. z. v znení neskorších predpisov, zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení neskorších predpisov, zákon č. 179/2011 Z. z. o hospodárskej mobilizácii a o zmene a doplnení zákona č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu v znení neskorších predpisov.

12) Napríklad nariadenie Európskeho parlamentu a Rady (EÚ) č. 1092/2010 z 24. novembra 2010 o makroprudenciálnom dohľade Európskej únie nad finančným systémom a o zriadení Európskeho výboru pre systémové riziká (Ú. v. EÚ L 331, 15. 12. 2010), nariadenie Európskej centrálnej banky (EÚ) č. 468/2014 zo 16. apríla 2014 o rámci pre spoluprácu v rámci jednotného mechanizmu dohľadu medzi Európskou centrálnou bankou, príslušnými vnútroštátnymi orgánmi a určenými vnútroštátnymi orgánmi (nariadenie o rámci JMD) (Ú. v. EÚ L 141, 14. 5. 2014), zákon Národnej rady Slovenskej republiky č. 566/1992 Zb. v znení neskorších predpisov, § 15 ods. 2 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z. v znení zákona č. 444/2015 Z. z.

13) Zákon Národnej rady Slovenskej republiky č. 46/1993 Z. z. v znení neskorších predpisov.
Zákon Národnej rady Slovenskej republiky č. 198/1994 Z. z. v znení neskorších predpisov.

13a) Napríklad zákon č. 747/2004 Z. z. v znení neskorších predpisov.

14) Zákon č. 73/1998 Z. z. o služobnom pomere príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície v znení neskorších predpisov.
Zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov.
Zákon č. 552/2003 Z. z. o výkone práce vo verejnom záujme v znení neskorších predpisov.
Zákon č. 281/2015 Z. z. o štátnej službe profesionálnych vojakov v znení neskorších predpisov.
Zákon č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov.

15) Napríklad čl. 37 ods. 37.1 Protokolu (č. 4) o Štatúte Európskeho systému centrálnych bánk a Európskej centrálnej banky v platnom znení (Ú. v. EÚ C 202, 7. 6. 2016), § 17 až 20 zákona č. 513/1991 Zb. Obchodný zákonník, § 39 zákona Slovenskej národnej rady č. 323/1992 Zb. o notároch a notárskej činnosti (Notársky poriadok) v znení neskorších predpisov, § 23 zákona Národnej rady Slovenskej republiky č. 46/1993 Z. z., § 20 zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z. v znení zákona č. 319/2012 Z. z., zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 23 zákona č. 586/2003 Z. z. o advokácii a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov v znení zákona č. 297/2008 Z. z., zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 24 a 25 zákona č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 11 zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 63 zákona č. 352/2011 Z. z. v znení neskorších predpisov, § 10 zákona č. 324/2011 Z. z. o poštových službách a o zmene a doplnení niektorých zákonov.

16) Zákon č. 583/2008 Z. z. o prevencii kriminality a inej protispoločenskej činnosti a o zmene a doplnení niektorých zákonov.
Zákon č. 307/2014 Z. z. o niektorých opatreniach súvisiacich s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov.

17) Čl. 23 nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L

119/89, 4. 5. 2016).

18) Čl. 5 nariadenia (EÚ) č. 2016/679.

19) Zákon č. 215/2004 Z. z. v znení neskorších predpisov.
§ 6 ods. 10, § 55 ods. 9, § 56 ods. 7, § 58 ods. 4 a § 69 zákona č. 215/2004 Z. z.

20) Napríklad STN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti (ISO/IEC 27002:2013).

21) § 1 ods. 3 písm. a) zákona č. 747/2004 Z. z. v znení neskorších predpisov.

22) Napríklad zákon č. 483/2001 Z. z. v znení neskorších predpisov, zákon č. 566/2001 Z. z. o cenných papieroch a investičných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 429/2002 Z. z. v znení neskorších predpisov, zákon č. 747/2004 Z. z. v znení neskorších predpisov, zákon č. 492/2009 Z. z. v znení neskorších predpisov.

22a) Napríklad nariadenie (EÚ) č. 1024/2013.

23) § 5 ods. 1 zákona č. 351/2011 Z. z. v znení zákona č. 247/2015 Z. z.

24) Vykonávacie nariadenie Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov, a parametrov na posudzovanie tohto, či má incident závažný vplyv (Ú. v. EÚ L 26, 31. 1. 2018).

25) Napríklad § 16 ods. 3 písm. j) zákona č. 308/2000 Z. z. o vysielaní a retransmisii a o zmene zákona č. 195/2000 Z. z. o telekomunikáciách v znení neskorších predpisov, § 6 ods. 1 zákona č. 167/2008 Z. z. o periodickej tlači a agentúrnom spravodajstve a o zmene a doplnení niektorých zákonov (tlačový zákon).

26) Zákon č. 387/2002 Z. z. v znení neskorších predpisov.

27) Napríklad čl. 1 ods. 4 ústavného zákona č. 227/2002 Z. z. o bezpečnosti štátu v čase vojny, vojnového stavu, výnimočného stavu a núdzového stavu, § 2 písm. a) zákona č. 387/2002 Z. z.

28) § 2 ods. 2 zákona č. 319/2002 Z. z. v znení zákona č. 69/2018 Z. z.

28a) Zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním) v znení neskorších predpisov.

28b) § 13 písm. f) zákona č. 400/2015 Z. z. o tvorbe právnych predpisov a o Zbierke zákonov Slovenskej republiky a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

29) Zákon Národnej rady Slovenskej republiky č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov.

30) § 12 zákona Národnej rady Slovenskej republiky č. 10/1996 Z. z. v znení neskorších predpisov.

31) Vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

31a) Zákon č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

31b) Napríklad STN EN ISO/IEC 17024 (015258) Posudzovanie zhody. Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb Vestník Úradu pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky č. 3/13.

31c) § 2 ods. 2 písm. c) zákona č. 513/1991 Zb.

32) Zákon Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov.

33) Čl. 219 ods. 1 až 3 Zmluvy o fungovaní Európskej únie v platnom znení (Ú. v. EÚ C 326, 26. 10. 2012).
§ 28 ods. 2 zákona Národnej rady Slovenskej republiky č. 566/1992 Zb. v znení neskorších predpisov.

34) § 4a zákona Národnej rady Slovenskej republiky č. 198/1994 Z. z. o Vojenskom spravodajstve

v znení zákona č. 69/2018 Z. z.

35) Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Príloha č. 1
k zákonu č. 69/2018 Z. z.

Sektor	Podsektor	Prevádzkovateľ služieb	Ústredný orgán
1. Bankovníctvo		**úverové inštitúcie,** ktorých predmetom činnosti je prijímanie vkladov alebo iných návratných peňažných prostriedkov od verejnosti a poskytovanie úverov na vlastný účet	Ministerstvo financií Slovenskej republiky
		správcovia, prevádzkovatelia a osoby zabezpečujúce činnosti Štátnej pokladnice podľa zákona č. 291/2002 Z. z. o Štátnej pokladnici a o zmene a doplnení niektorých zákonov v znení neskorších predpisov	
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov alebo sú k nemu priamo pripojené; tým nie sú dotknuté vylúčenia podľa § 2 ods. 2 písm. d) tohto zákona č. 69/2018 Z. z.	
2. Doprava	Cestná doprava	**cestné orgány zodpovedné za kontrolu riadenia cestnej premávky –** akýkoľvek verejný orgán zodpovedný za plánovanie, kontrolu alebo riadenie ciest, ktoré spadajú do jeho územnej pôsobnosti	Ministerstvo dopravy a výstavby Slovenskej republiky
		prevádzkovatelia inteligentných dopravných systémov, v ktorých sa uplatňujú informačné a komunikačné technológie v oblasti cestnej dopravy vrátane infraštruktúry, vozidiel a užívateľov a v oblasti riadenia dopravy a riadenia mobility, rovnako ako aj pre rozhrania s inými druhmi dopravy	
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
	Letecká doprava	**leteckí dopravcovia** - letecký dopravný podnik s platnou prevádzkovou licenciou alebo jej ekvivalentom	
		prevádzkovateľ letiska - subjekt, ktorý má v spojení s inými činnosťami alebo bez nich, podľa situácie, podľa vnútroštátnych zákonov, iných právnych predpisov alebo zmlúv za cieľ správu a riadenie infraštruktúry letiska alebo siete letísk a koordináciu a kontrolu činností jednotlivých prevádzkovateľov na príslušných letiskách alebo v príslušných sieťach letísk,	

		letiská vrátane hlavných letísk a subjekty prevádzkujúce pomocné zariadenia nachádzajúce sa na letiskách	
		prevádzkovatelia poskytujúci služby riadenia letovej prevádzky (ATC) ako služby poskytovanej na účely: a) zabránenia zrážke: - medzi lietadlami a - v prevádzkovom priestore medzi lietadlom a prekážkami; a b) urýchlenia a zachovania riadneho toku letovej prevádzky	
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
	Vodná doprava	**spoločnosti prevádzkujúce vnútrozemskú, námornú a pobrežnú osobnú a nákladnú vodnú dopravu**	
		riadiace orgány prístavu - ako akejkoľvek určenej časti pevniny a vody s hranicami vymedzenými členským štátom, kde sa nachádza prístav, vrátane závodov a zariadení určených na uľahčenie prevádzky komerčnej námornej dopravy; vrátane ich prístavných zariadení, kde dochádza k vzájomnému kontaktu lode a prístavu; patria sem oblasti ako napríklad kotviská, služobné kotviská a prístupy z mora, ako je to vhodné, a subjekty prevádzkujúce činnosti a zariadenia v rámci prístavu	
		prevádzkovatelia plavebno-prevádzkových služieb ako služba určená na zvýšenie bezpečnosti a efektívnosti lodnej dopravy a na ochranu životného prostredia, ktorá je schopná interakcie s dopravou a môže reagovať na dopravné situácie vznikajúce v oblasti plavebno-prevádzkových služieb	
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
	Železničná doprava	**prevádzkovateľ infraštruktúry** - každý orgán alebo podnik zodpovedný najmä za zriadenie, správu a údržbu železničnej infraštruktúry vrátane riadenia dopravy,	

		zabezpečenia a návestenia. Funkciou manažéra infraštruktúry na sieti alebo časti siete môžu byť poverené rôzne orgány alebo podniky	
		železničné podniky - každý verejnoprávny alebo súkromný podnik, ktorého hlavným predmetom činnosti je poskytovanie služieb s cieľom zabezpečenia železničnej prepravy tovaru alebo osôb, pričom tento podnik zabezpečuje trakciu; zahŕňa to aj podniky, ktoré zabezpečujú len trakciu, to neplatí pre podniky, ktoré zabezpečujú trakciu pre trolejbusovú a električkovú dráhu, vrátane prevádzkovateľov servisných zariadení - každý verejný alebo súkromný subjekt zodpovedný za správu jedného alebo viacerých servisných zariadení alebo za poskytovanie jednej alebo viacerých kľúčových služieb železničným podnikom	
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
3. Digitálna infraštruktúra		**poskytovateľ služby výmenného uzla internetu** na účel prepájania sietí, ktoré sú z technického a organizačného pohľadu oddelené	Národný bezpečnostný úrad
		poskytovateľ služieb systému doménových mien na internete	
		subjekt spravujúci alebo prevádzkujúci register internetových domén najvyššej úrovne	
		poskytovateľ služieb webhostingu, DNS hostingu alebo mailhostingu	
4. Elektronické komunikácie	Satelitná komunikácia	**správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry** podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre	Ministerstvo dopravy a výstavby Slovenskej republiky
	Siete a služby pevných a mobilných elektronických komunikácií	**správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry** podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre	
		služby prístupu do internetu pevnej a mobilnej siete	
5. Energetika	Baníctvo	**správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry** podľa zákona	Ministerstvo hospodárstva

		č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	Slovenskej republiky
	Elektroenergetika	**elektroenergetické podniky** - každá osoba, ktorá vykonáva aspoň jednu z týchto činností: výroba, prenos, distribúcia, dodávka alebo nákup elektriny a ktorá je v súvislosti s týmito činnosťami zodpovedná za obchodné a technické úlohy a/alebo údržbu; nezahŕňa však koncových odberateľov, ktorí vykonávajú predaj elektriny odberateľom vrátane jej ďalšieho predaja	
		prevádzkovatelia distribučnej sústavy – každá osoba zodpovedná za prevádzku, zabezpečovanie údržby a v prípade potreby rozvoj distribučnej sústavy v danej oblasti a prípadne aj rozvoj jej prepojení s inými sústavami a za zabezpečovanie dlhodobej schopnosti sústavy uspokojovať primeraný dopyt po distribúcii elektriny	
		prevádzkovatelia prenosovej sústavy - každá osoba zodpovedná za prevádzku, zabezpečovanie údržby a rozvoj prenosovej sústavy v danej oblasti a prípadne aj rozvoj jej prepojení s inými sústavami a za zabezpečovanie dlhodobej schopnosti sústavy uspokojovať primeraný dopyt po prenose elektriny	
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
	Plynárenstvo	**dodávateľské podniky** - každá osoba, ktorá vykonáva predaj vrátane ďalšieho predaja zemného plynu vrátane LNG odberateľom	
		prevádzkovatelia distribučnej siete - každá osoba, ktorá vykonáva distribúciu a je zodpovedná za prevádzku, zabezpečenie údržby a v prípade potreby rozvoj distribučnej siete v danej oblasti, prípadne jej prepojenie s inými sieťami a za zabezpečenie dlhodobej schopnosti siete uspokojovať primeraný dopyt po distribúcii zemného plynu	
		prevádzkovatelia prepravnej siete - každá osoba, ktorá vykonáva prepravu a je zodpovedná za prevádzku, zabezpečenie údržby a v prípade potreby rozvoj prepravnej siete v danej oblasti, prípadne jej prepojenie	

		s inými sieťami a za zabezpečenie dlhodobej schopnosti siete uspokojovať primeraný dopyt po preprave zemného plynu	
		prevádzkovatelia zásobníkov - každá osoba, ktorá vykonáva uskladňovanie a je zodpovedná za prevádzku zásobníka	
		prevádzkovatelia zariadení LNG - každá osoba, ktorá vykonáva skvapalňovanie zemného plynu alebo dovoz, vykládku a spätné splyňovanie LNG a je zodpovedná za prevádzku zariadenia LNG	
		plynárenské podniky - každá osoba vykonávajúca aspoň jednu z týchto činností: ťažba, preprava, distribúcia, dodávka, nákup alebo uskladňovanie zemného plynu vrátane LNG, ktorá je zodpovedná za obchodné úlohy, technické úlohy a/alebo údržbu v súvislosti s týmito činnosťami, nezahŕňa však koncových odberateľov	
		prevádzkovatelia zariadení na rafinovanie a spracovanie zemného plynu	
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
	Ropa a ropné produkty	**prevádzkovatelia ropovodov**	
		prevádzkovatelia zariadení na ťažbu, rafinovanie a spracovanie ropy, jej skladovanie a prepravu	
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
	Tepelná energetika	**výrobcovia a dodávatelia tepla** podľa zákona č. 657/2004 Z. z. o tepelnej energetike	
6. Infraštruktúra finančných trhov		**prevádzkovatelia obchodných miest** podľa zákona č. 429/2002 Z. z. o burze cenných papierov v znení neskorších predpisov	Ministerstvo financií Slovenskej republiky
		centrálne protistrany - právnická osoba, ktorá vstupuje medzi protistrany zmlúv obchodovaných na jednom alebo viacerých finančných trhoch a stáva sa kupujúcim voči všetkým predávajúcim a predávajúcim voči všetkým kupujúcim	

7. Pošta	Poskytovanie poštových služieb, poštový platobný styk a obstarávateľská činnosť	**poštový podnik**, ktorý poskytuje jednu alebo viacero poštových služieb alebo poštový platobný styk podľa zákona o poštových službách	Ministerstvo dopravy a výstavby Slovenskej republiky
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
8. Priemysel	Farmaceutický priemysel	**výrobca liekov** podľa zákona č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach a o zmene a doplnení niektorých zákonov v znení neskorších predpisov	Ministerstvo hospodárstva Slovenskej republiky
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
	Hutnícky priemysel	**správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry** podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
	Chemický priemysel	**dodávatelia, výrobcovia, dovozcovia a následní užívatelia látok a zmesí** podľa zákona č. 67/2010 Z. z. o podmienkach uvedenia chemických látok a chemických zmesí na trh a o zmene a doplnení niektorých zákonov (chemický zákon) v znení neskorších predpisov	
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
	Inteligentný priemysel	**subjekt zapojený do inteligentného priemyslu**	
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov alebo sú k nemu priamo pripojené	

9. Voda a atmosféra	Meteorologická služba	**správcovia a prevádzkovatelia štátnej hydrologickej siete**	Ministerstvo životného prostredia Slovenskej republiky
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
		správcovia a prevádzkovatelia štátnej meteorologickej siete	
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
	Vodné stavby	**správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry** podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
	Zabezpečovanie pitnej vody	**dodávatelia a distribútori vody** na pitie, varenie, prípravu potravín alebo iné domáce účely, bez ohľadu na jej pôvod a na to, či bola dodaná z distribučnej siete, cisterny alebo vo fľašiach či nádobách; s výnimkou distribútorov, u ktorých je distribúcia vody iba časťou ich celkovej činnosti v oblasti distribúcie iných komodít a tovaru, ktorá sa nepovažuje za základnú službu	
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	
10. Verejná správa	Bezpečnosť	**správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sa týkajú bezpečnosti Slovenskej republiky**	Ministerstvo vnútra Slovenskej republiky
	Informačné systémy verejnej správy	**správcovia a prevádzkovatelia sietí a informačných systémov verejnej správy** v pôsobnosti povinnej osoby podľa zákona č. 275/2006 Z. z. podporujúci služby verejnej správy, služby vo verejnom záujme a verejné služby	Úrad podpredsedu vlády pre investície a informatizáciu
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené	

	Obrana	**správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sa týkajú zabezpečenia obrany Slovenskej republiky**	Ministerstvo obrany Slovenskej republiky
	Utajované skutočnosti	**správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sa týkajú utajovaných skutočností** _____ **správca a prevádzkovateľ informačného systému Úradu pre verejnú regulovanú službu**	Národný bezpečnostný úrad
11. Zdravotníctvo	Zdravotnícke zariadenia (vrátane nemocníc a súkromných kliník)	**poskytovatelia zdravotnej starostlivosti** - akákoľvek osoba alebo akýkoľvek iný subjekt, ktorý legálne poskytuje zdravotnú starostlivosť na území členského štátu	Ministerstvo zdravotníctva Slovenskej republiky
		správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené _____ **orgány verejného zdravotníctva, správca a prevádzkovateľ národných zdravotných registrov, národných zdravotných administratívnych registrov a národného zdravotníckeho informačného systému**	

Príloha č. 2
k zákonu č. 69/2018 Z. z.

Druhy digitálnej služby

(1) Online trhovisko
(2) Internetový vyhľadávač
(3) Cloud computing

Vysvetlivky:

Online trhovisko – digitálna služba, ktorá umožňuje spotrebiteľom alebo podnikateľom uzatvárať online kúpne zmluvy alebo zmluvy o službách s podnikateľmi buď na webovom sídle online trhoviska, alebo na webovom sídle podnikateľa, ktoré využíva počítačové služby poskytované online trhoviskom.
Internetový vyhľadávač – digitálna služba, ktorá umožňuje používateľom vyhľadávať v zásade na všetkých webových sídlach alebo na webových sídlach v konkrétnom jazyku informácie o akejkoľvek téme na základe kľúčového slova, vety alebo iných zadaných údajov, pričom jeho výsledkom sú linky, prostredníctvom ktorých možno nájsť informácie súvisiace s požadovaným obsahom,
Služba v oblasti cloud computingu – digitálna služba, ktorá umožňuje prístup ku škálovateľnému a pružnému súboru počítačových zdrojov, ktoré možno zdieľať.

Príloha č. 3
k zákonu č. 69/2018 Z. z.

Zoznam preberaných právne záväzných aktov Európskej únie

Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. (Ú. v. EÚ L 194, 19. 7. 2016).

Vydavateľ Zbierky zákonov Slovenskej republiky, správca obsahu a prevádzkovateľ právneho a informačného portálu Slov-Lex dostupného na webovom sídle www.slov-lex.sk je
Ministerstvo spravodlivosti Slovenskej republiky, Račianska 71, 813 11 Bratislava,
tel.: +421 2 888 91 864, +421 2 888 91 865, e-mail: helpdesk@slov-lex.sk.