1.1 Analýza návrhu zákona o kybernetickej bezpečnosti

Daniel Olejár

Text zákona	Pripomienky	Návrhy
763 **VLÁDNY NÁVRH** **Zákon** z ... 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,	1. špecifikácia predmetu zákona je veľmi všeobecná a bolo by ju potrebné upresniť oblasť pôsobnosti	

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.	• • • • • 1. tento zákon nehovorí o bezpečnostných opatreniach vo všeobecnosti, ale len o vybranej triede bezpečnostných opatrení, ktoré sa navyše vzťahujú len na zaistenie ochrany špecifických entít (systémov, informácií) • 1. zabezpečenie bezpečnosti? 2. audit čoho?	

§ 2 **Pôsobnosť zákona**		
(1) Tento zákon ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti.	1. kybernetickej bezpečnosti čoho? štátu, organizácie, systému?	
(1) 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 týkajúce sa bezpečnosti sietí a informačných systémov a oznamovania kybernetických bezpečnostných incidentov v sektore bankovníctva, financií alebo finančného systému podľa osobitného predpisu,[3]) vrátane štandardov		

[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 v znení neskorších predpisov.
Zákon č. 319/2002 Z. z. o obrane Slovenskej republiky v znení 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

a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu,[4]) ak ich účinok je aspoň rovnocenný s účinkom povinností podľa tohto zákona, a vrátane rozhodnutí, štandardov a zásad vydaných alebo prijatých Národnou bankou Slovenska, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona, ani na platobné systémy a na systémy zúčtovania cenných papierov 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		

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.

[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 (ECB/2014/28) (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.
Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov, f) osobitné predpisy.[7])		

[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, zákon č. 45/2011 Z. z. o kritickej infraštruktúre, zákon č. 351/2011 Z. z. o elektronických komunikáciách v znení neskorších predpisov.

§ 3 **Vymedzenie základných pojmov**		
Na účely tohto zákona sa rozumie a) sieťou a informačným systémom elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov, b) 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 týmito entitami, c) kontinuitou strategická a taktická schopnosť organizácie plánovať a reagovať na udalosti a incidenty s cieľom pokračovať vo výkone činností na prijateľnej, vopred stanovenej úrovni,	1. cyklická nelogická definícia umožňujúca aj takúto interpretáciu: sieťou sú ... údaje vytvárané prostredníctvom elektronickej komunikačnej siete na účely používania systémov, resp. informačný systém je informačný systém, sieťou je každé zariadenie 2. podľa definície do informačného systému nepatria aplikačné programy a údaje, ale len systémové programy a údaje • 1. okrem absurdností vyplývajúcich zo zmätočných definícií siete a informačného systému a. je človek prvkom kybernetického priestoru? b. čo používatelia, ktorí pracujú s aplikačným programovým vybavením; keďže toto nie je súčasťou kybernetického priestoru, potom používatelia nemôžu vykonávať aktivity v kybernetickom c. ľudia, ktorí sú prvkami kybernetického priestoru fungujú aj mimo neho, aké interakcie medzi ľuďmi patria potom do kybernetického priestoru? 2. kontinuita čoho? 3. čo má organizácia plánovať? 4. väčšina udalostí nemá negatívny dopad a organizácia sa nemusí explicitne zaoberať tým, čo bude robiť, ak nastanú,	

	5. nejde len o cieľ, ide o jeho naplnenie, organizácia môže plánovať reakcie na incidenty, reagovať na udalosti, ale to nemusí stačiť, kontinuita nie je len zámer, ale dosiahnutie toho, že dôležité činnosti bude organizácia vykonávať bez prerušenia	
	6. dôvernosť čoho? 7. dôvernosť nie je záruka, ale požiadavka	
d) dôvernosťou záruka, že informácia nie je prezradená neoprávneným subjektom alebo procesom,	8. čo znamená prezradiť?	
e) dostupnosťou záruka, že údaje alebo informácie sú pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je informácia potrebná a požadovaná,	9. dostupnosťou čoho? (nemusí ísť len o informácie a údaje, ale aj o iné zdroje a služby) 10. dostupnosť (údajov) nie je záruka, ale požiadavka 11. zdroje nemajú byť dostupné komukoľvek, ale len oprávneným subjektom 12. aký je vzťah medzi dátami a informáciami? 13. čo je to potrebnosť informácie? 14. kto požaduje informáciu? 15. takáto definícia dostupnosti predpokladá okamžitú dostupnosť, v praxi sú požiadavky miernejšie (% času, počas ktorého sú zdroje prístupné oprávneným subjektom, doba čakania na odozvu)	
f) integritou záruka, že bezchybnosť, úplnosť alebo správnosť informácie neboli narušené,	16. integrita (údajov) je zasa bezpečnostná požiadavka 17. integrita sa vzťahuje aj na zariadenia 18. bezchybnosť, úplnosť a správnosť informácie sú sémantické kategórie a opatrenia, ktoré sa používajú na zaistenie integrity údajov sa za-	

g) 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,	kladajú buď na riadení prístupu, alebo na syntaktickej kontrole 19. vzťahuje sa len na siete a informačné systémy – a čo ostatné prvky kybernetického priestoru? 20. čo je určitý stupeň spoľahlivosti – keď si ho definujem ako nulový, aká bude úroveň kybernetickej bezpečnosti? 21. akékoľvek konanie – výbuch atómovej bomby ohrozuje CIAA všetkých údajov aj existenciu systému, ktorého kybernetickú bezpečnosť chceme zaistiť, takže požiadavka na akékoľvek konanie je nerealistická 22. čo je pravosť údajov? 23. čo je pravosť služieb?	
h) rizikom miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,	24. kybernetická bezpečnosť by sa mala na niečo vzťahovať, napr. na systém sieť, organizáciu, priestor 25. existujú riziká, ktoré nevyplývajú z kybernetických hrozieb (zúženie významu pojmu) 26. riziko sa vzťahuje na nejakú hrozbu (a aktívum, alebo aspoň organizáciu)	
i) hrozbou každá primerane rozpoznateľná okolnosť alebo udalosť proti sieťam a informačným systémom, ktorá môže mať nepriaznivý vplyv na kybernetickú bezpečnosť,	27. toto je skôr nepresná definícia hodnoty rizika 28. rozpor so štandardnou definíciou hrozby. Tu je hrozba niečo, čo už nastalo (udalosť), štandardne to je potenciálna možnosť (výbuch sopky, záplava, krádež, útok hackera, chyba obsluhy, výpadok elektrickej energie) 29. udalosť proti sieťam? 30. stále (zbytočne) cyklická definícia : hrozba môže mať nepriaznivý vplyv na stav, v ktorom	

j) 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,	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, 31. čo je bezpečnosť siete, informačného systému? 32. čo je bezpečnostná politika subjektu? 33. akého subjektu a ako súvisí s bezpečnostných incidentom? 34. kybernetická bezpečnosť čoho? 35. integrita bola zavedená ako miera bezchybnosti, úplnosti a správnosti informácie, integrita systému nebola definovaná 36. dostupnosť bola zavedená len v súvislosti s údajmi a informáciami, 37. čo znamená odmietnutie dostupnosti (podľa definície záruky)? 38. pojmy základná služba a digitálna služba neboli definované 39. nie je špecifikovaný význam pojmu vysoká pravdepodobnosť, 40. čo znamená kompromitácia (strata dôveryhodnosti?) 41. čo znamená ohrozenie – je to naplnená, alebo nenaplnená hrozba? 42. čo okrem narušenia dostupnosti, dôvernosti, integrity, autentickosti spadá pod pojem (narušenia) bezpečnosti informácií • •	

b) 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, 2. je informačným systémom verejnej správy,[8]) alebo 3. je prvkom kritickej infraštruktúry,[9]) •	• 1. pojem základná služba bol definovaný pomocou nedefinovaného pojmu služba 2. pojem essential service je definovaný v čl. 5, ods. 2 Smernice NIS o stanovovaní operátorov podstatných/základných služieb: • • 2.The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows: • (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service. • 1. pojem služby (na ktorý sa odvoláva aj smernica NIS, bol definovaný v DIRECTIVE (EU) 2015/1535 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) čl. 1, ods. 2 • • 'service' means any Information • Society service, that is to say, any service	

[8]) § 2 ods. 1 písm. b) zákona č. 275/2006 Z. z. v znení zákona č. 570/2009 Z. z.
[9]) § 2 písm. a) zákona č. 45/2011 Z. z.

•	normally provided for remuneration, at a distance, by electronic means and at the individual • request of a recipient of services. For the purposes of this definition: • (i) 'at a distance' means that the service is provided without the parties being simultaneously present; • (ii) 'by electronic means' means • that the service is sent initially • and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; • (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual • request. An indicative list of services not covered by this definition is set out in Annex I; • 1. definícia základnej služby je v rozpore s definíciou essential service Direktívy NIS, zahŕňa do služby aj entity, ktoré nespĺňajú definíciu služby (informačný systém, prvok kritickej infraštruktúry) 2. podľa § 2, ods. (2), písm. f) sa tento zákon nevzťahuje na kritickú infraštruktúru, čo je v rozpore s §3, ods k), pretože tento zákon pod-	

• • • • • • • • • • • • b) prevádzkovateľom základnej služby orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena k), c) digitálnou službou služba, ktorej druh je uvedený prílohe č. 2, d) 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,	ľa § 1 upravuje postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby a základná služba je o.i. aj prvkom kritickej infraštruktúry 3. čo vlastne je služba- prvok (systém) alebo činnosť? • • 1. aká osoba – právnická, fyzická? • • • • • • • • Druhy digitálnej služby • (1) Online- trhovisko • (2) Internetový vyhľadávač • (3) Cloud computing • • 1. toto je nelogická definícia. Poskytovateľom digitálnej služby je každý, kto digitálnu službu poskytuje ako službu. Niektorí poskytovatelia sú významnejší, podliehajú registrácii a vzťahujú sa na nich požiadavky tohto zákona. • • 1. bezpečnostný incident by sa mal aj skutočne riešiť, t.j. mali by sa v jeho priebehu prijímať opatrenia na jeho ohraničenie a likvidáciu (hasenie požiaru)	

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

§ 4 **Pôsobnosť orgánov verejnej moci**		
Pôsobnosť v oblasti kybernetickej bezpečnosti vykonáva a) Národný bezpečnostný úrad (ďalej len „úrad“), b) úrad, 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, Slovenská informačná služba, Úrad podpredsedu vlády pre investície a informatizáciu a Vojenské spravodajstvo (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“).	2. opakuje sa	

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

§ 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 iných 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	59. čo znamená riadi výkon štátnej správy? 60. akou formou bude úrad určovať povinnosti? 61. NIS o NATO nič nehovorí, je táto kompetencia v poriadku? 62. členmi NATO sú aj krajiny, ktoré nie sú v EÚ, a teda nemusia mať kontaktné miesta pre kybernetickú bezpečnosť podľa NIS (?) , ako bude NBÚ zabezpečovať spoluprácu s USA, Tureckom a i.? 63. štylistika a podieľa sa vytváranie partnerstiev 64. partnerstiev medzi kým? 65. akých aktivít? kto tieto aktivity má vyvíjať? •	

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 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,	59. zo zaradenia do zoznamu základných/digitálnych služieb poskytovateľovi vyplývajú netriviálne povinnosti a s nimi spojené náklady. Nemalo by byť rozhodovanie o základnej/digitálnej službe nejako formálne zdôvodnené? 60. akreditácia NBÚ nemá medzinárodnú váhu, vyňatie národnej a vládnej jednotky spod akreditácie nie je fair voči ostatným CSIRTom, ktoré musia byť akreditované a umožňuje, aby najvyššie postavené CSIRTy v SR nemali požadovanú úroveň. Navyše to je konflikt záujmov, pretože NBÚ zároveň zodpovedá za niektoré základné služby ako ústredný orgán 61. pre akreditáciu jednotiek CSIRT existujú medzinárodné pravidlá a úrad nie je oprávnený podľa nich posudzovať CRIRT-y a udeľovať im akreditáciu. To znamená, že pôjde o akredi-	

n) akredituje jednotky CSIRT, okrem Národnej jednotky CSIRT a vládnej jednotky CSIRT a zaraďuje ich do zoznamu akreditovaných jednotiek CSIRT,	táciu, ktorá nebude medzinárodne uznaná. 62. na tieto úlohy úrad nemá kapacity 63. kybernetický bezpečnostný incident je definovaný ako udalosť, t.j. niečo, čo nastalo; je nelogické vystríhať pred udalosťou, ktorá nastala; tu sa miešajú pojmy hrozba, riziko a bezpečnostný incident 64. komu zasiela varovania? čo je to včasné varovanie? 65. toto sú úlohy CSIRTov	
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,	66. kontrolu koho alebo čoho a na základe akých podkladov? •	
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	59. na tieto úlohy úrad nemá odborné kapacity 60. kto je orgán posudzovateľa zhody (a aké má odborné kompetencie a kapacity na vykonávanie dostatočne kvalifikovaného auditu) • 59. ani na tieto úlohy úrad nemá odborné kapacity • • • 59. táto ambícia je nepodložená, koordinovať nejakú činnosť môže len ten, kto jej rozumie a nie-	

priestupok alebo iný správny delikt, v) vykonáva audit alebo požiada orgán posudzovania zhody o vykonanie auditu u prevádzkovateľa základnej služby, w) vydáva znalostné štandardy a v spolupráci s Ministerstvom školstva, vedy, výskumu a športu Slovenskej republiky vykonáva a zabezpečuje budovanie bezpečnostného povedomia, x) koordinuje výskum a vývoj.	kedy ju vykonával. Toto kritérium NBÚ nespĺňa.	
(2) 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.	60. je toto potrebné uvádzať v zákone? Ktoré úlohy môže Úrad delegovať zmluvou na fyzickú osobu? Aj zastupovanie SR v orgánoch ENISA a NATO?	

§ 6 **Národná jednotka CSIRT**		
(1) Úrad 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 plnia úlohy jednotky CSIRT ústredné orgány. Národná jednotka CSIRT je zaradená v zozname akreditovaných jednotiek CSIRT.	59. NBÚ má mať sektory Digitálna infraštruktúra internetové prepojovacie uzly (IXP) poskytovatelia služieb DNS registre domén najvyššej úrovne (TLD) Utajované skutočnosti 60. Kto bude kontrolovať, či Národná jednotka (Úrad) spĺňa podmienky akreditácie? 61. konflikt záujmov – Úrad bude kontrolovať sám seba, či plní (ako CSIRT zodpovedný za sektory) povinnosti zákona	
(1) 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.	59. tu je zmätočná formulácia, lebo Ústredný orgán §9 ods. (1) a) plní úlohy jednotky CSIRT spôsobom podľa odseku (2), (2) Ústredný orgán na účely plnenia úloh podľa odseku 1 písm. a), v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa prílohy č. 1, zriaďuje a prevádzkuje akreditovanú jednotku CSIRT alebo na tento účel využíva akreditovanú jednotku CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, okrem vládnej jednotky CSIRT, ak sa tak dohodnú. Využívanie akreditovanej jednotky CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, sa vykonáva na základe zmluvy. Úrad podpredsedu vlády Slovenskej republiky pre investície	ak si ústredný orgán na zabezpečenie sektora alebo podsektora, za ktorý zodpovedá (Príloha č. 1) nezriadi (akreditovanú) jednotku CSIRT, ani na tento účel nevyužíva akreditovanú jednotku CSIRT iného ústredného orgánu, úlohy ústredného orgánu podľa §9 ods. 1 písm. a) vykonáva Národná jednotka CSIRT

	a informatizáciu zabezpečuje úlohy podľa odseku 1 písm. a) prostredníctvom vládnej jednotky CSIRT. T.j. Národná jednotka CSIRT by mala konať podľa ods. 1) písm. a) a potom postupovať podľa ods. 2), t.j. zriadiť a prevádzkovať akreditovanú jednotku CSIRT, alebo sa dohodnúť s iným št. orgánom (a uzavrieť s ním zmluvu) o tom, že jeho CSIRT sa bude starať o bezprizorný sektor. Ak sa jej to nepodarí, dostáva sa do bludného kruhu, lebo zlyhala ako ústredný orgán a problém musí riešiť podľa § 6 ods. 2	
(1) Na činnosti národnej jednotky CSIRT sa vyslaním svojich zástupcov a ďalšími formami spolupráce môžu podieľať aj iné orgány verejnej moci v rozsahu a spôsobom ustanoveným na základe uzatvorených zmlúv o spolupráci.		
(2) 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.	59. keďže úrad plní aj úlohu ústredného orgánu, opäť tu je logický spor (ak úrad ako ústredný orgán neplní povinnosti, bude ich plniť ako úrad). Ale ak by povinnosti nebol schopný plniť na úrovni ústredného orgánu, sotva ich bude schopný plniť ako úrad (s tými istými zdrojmi).	

§ 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.	59. zbytočné, úloha stratégie vyplýva priamo z jej názvu 60. plán zdrojov?	
(1) 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,	59. je možné stanovovať úlohy a povinnosti orgánom verejnej moci inak ako zákonom? 60. Národná stratégia nie je analýza rizík, alebo bezpečnostný projekt organizácie 61. akých opatrení – existujúcich alebo tie, ktoré je potrebné prijať? 62. bezpečnostného prostredia ale čoho? 63. definícia bezpečnostných hrozieb – to je obsiahnuté napr. v štandardoch nemeckého BSI, resp. existujú rozsiahle katalógy hrozieb, obsahujúce aj ich popis; bude stratégia preberať tieto definície? a v akom rozsahu? 64. aj keby sa Stratégia obmedzila na relevantné hrozby voči slovenskému kybernetickému priestoru, bude ich toľko, že zaradenie ich definícií do stratégie spôsobí, že stratégia môže mať stovky až tisíce strán (BSI Grundschutzbuch má cez 5.000 strán) 65. zdrojov na čo?	tento odsek vychádza zo štandardov ISO/IEC 27001 a ISO/IEC27002 o zavádzaní systému manažmentu informačnej bezpečnosti v organizácii, ale na systém veľkosti štátu sa nehodí

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.	66. na úrovni stratégie sa dá takýto program nanajvýš pomenovať, ale to nestačí – pozri osud Koncepcie kybernetickej bezpečnosti a Akčného plánu, to sú dokumenty na úrovni stratégie (oba boli schválené vládou a neplnia sa) 67. na stanovovanie obsahu plánov výskumu a vývoja sú iné inštitúcie, ktoré majú svoje pravidlá 68. čo je plán posudzovania rizika? komu je určený? kto ho bude plniť, kto kontrolovať plnenie a čo sa bude na základe výsledkov robiť? 69. stratégia môže nanajvýš uviesť, s kým by sme chceli spolupracovať (alebo uviesť zoznam tých, s ktorými nejako spolupracujeme); na tomto mieste by skôr malo význam spomenúť, z čoho stratégia vychádza (dokumenty EÚ, NATO, normy,...) •	
(1) Ústredné orgány a iné orgány štátnej správy spolupracujú s úradom na vypracovaní národnej stratégie kybernetickej bezpečnosti a na tento účel sú povinné poskytnúť mu informácie v potrebnom rozsahu.		
(2) Národnú stratégiu kybernetickej bezpečnosti schvaľuje vláda Slovenskej republiky.	59. doba platnosti, kontrola plnenia úloh (na aký čas bude prijatý Akčný plán?) 60. čo revízie národnej stratégie?	

§ 8 **Jednotný informačný systém kybernetickej bezpečnosti**		

	59. pri analýze funkcionality Jednotného systému sa ukazuje, že jeho úlohy by dokázalo plniť webové sídlo s niekoľkými webovými stránkami, a jednoduchá databáza. Ak by bol Jednotný systém jediným komunikačným kanálom na nahlasovanie bezpečnostných incidentov, negatívne by to ovplyvnilo riešenie bezpečnostných incidentov (ako nahlasovať bezpečnostné incidenty, ak došlo k strate konektivity) Na automatizované testovanie zraniteľností, monitoring siete a forenznú analýzu existujú špecializované nástroje. Vytvorenie Jednotného systému môže byť zbytočne drahé a trvať príliš dlho na to, ako rýchlo je potrebné reálne riešiť bezpečnostné incidenty. • •	

[10]) 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.

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.		
	59. Ako bude Jednotný systém prepojený na informačné zdroje zo zahraničia, CSIRT-ov a iné relevantné systémy? 60. komunikačný systém bude sotva analyzovať bezpečnostné incidenty. Špecifikácia poslania	

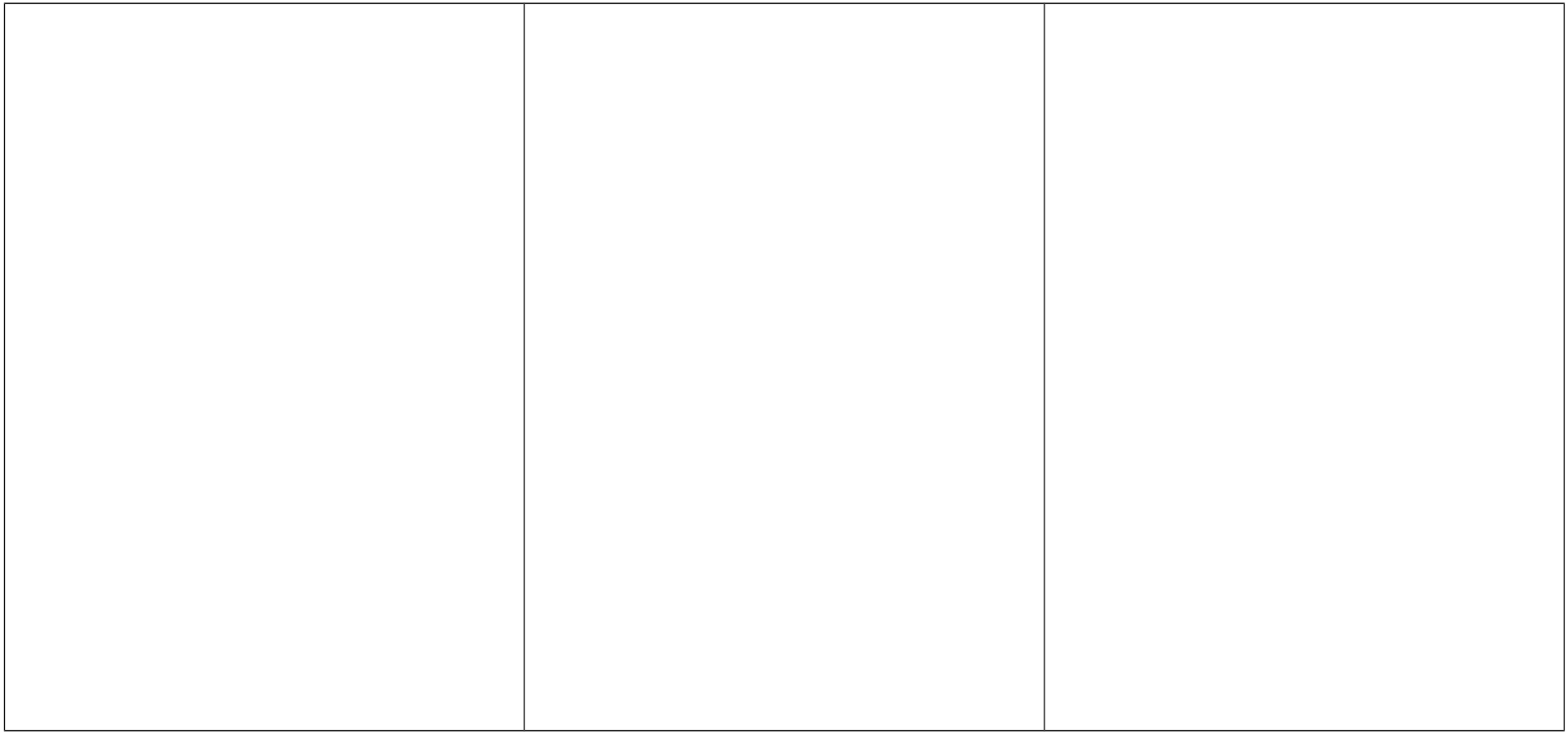
	tohto systému je nejasná. Môže ísť o systém, ktorý bude slúžiť ako komunikačný kanál fungujúci on-line (nahlasovanie bezpečnostných incidentov, resp. komunikácia s postihnutým subjektom). Zber, analýza a vyhodnocovanie informácií sa budú robiť off-line, lebo pri týchto činnostiach sa budú využívať aj informácie, ktoré získa CSIRT a iné orgány pri riešení a po doriešení bezpečnostného incidentu	

	59. na to stačí stránka s chráneným prístupom a upozornenia na to, že na nej je uverejnená nejaká nová informácia 60. kto bude zodpovedný za udržiavanie a aktualizáciu obsahu? •	

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) iný orgán verejnej moci rozhodnutím úradu.		

	59. obmedzenie na poskytovanie informácií len prostredníctvom jednotného informačného systému je v rozpore s účelom, ktorý má tento systém plniť. Jeho nedostupnosť bude znamenať, že postihnutý subjekt nebude môcť nahlásiť dôležitú informáciu (a požiadať o pomoc), hoci existujú ďalšie komunikačné kanály. Toto obmedzenie síce zjednodušuje spracovanie informácií (formuláre), ale vytvára z jednotného systému *single point of failure*	

[11]) 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 (ECB/2014/17) 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), v platnom znení, 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.



§ 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 pre zabezpečenie kybernetickej bezpečnosti; informácie sa poskytujú len za podmienky, že ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu[12]) 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 a politiku správania sa v kybernetic-	59. kto určí, ktoré informácie sú dôležité pre zabezpečenie kybernetickej bezpečnosti? 60. kybernetickej bezpečnosti čoho – vlastnej organizácie, štátu alebo niečoho iného? • 59. nasledujúce povinnosti sú nezrozumiteľné, alebo vágne: a. buduje koordinovanú spoluprácu? b. aplikuje bezpečnostné čo a na čo? c. aplikuje politiku správania sa v kybernetickom priestore – to je čo a ako sa to má robiť a ako sa to bude kontrolovať 60. aktuálny zoznam je zoznam obsahujúci všetkých prevádzkovateľov základnej služby	

[12]) 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.

kom 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.	v štáte, nestačilo by, aby ústredný orgán aktualizoval informácie o základných službách a ich poskytovateľoch zo svojej oblasti pôsobnosti? • 59. asi nie jednou, ale aspoň v rámci EÚ, možno aj s americkou, britskou, švajčiarskou, nórskou, izraelskou, kórejskou – budeme to špecifikovať? a spolupráca na základe čoho	
(2) Ústredný orgán na účely plnenia úloh podľa odseku 1 písm. a), v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa prílohy č. 1, zriaďuje a prevádzkuje akreditovanú jednotku CSIRT alebo na tento účel využíva akreditovanú jednotku CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, okrem vládnej jednotky CSIRT, ak sa tak dohodnú. Využívanie akreditovanej jednotky CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, sa vykonáva na základe zmluvy. Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu zabezpečuje úlohy podľa odseku 1 písm. a) prostredníctvom vládnej jednotky CSIRT.	59. je potrebné predpisovať, ako majú byť upravené vzťahy pri využívaní externej jednotky CSIRT?	

(2) Zmluva podľa odseku 2 musí obsahovať obdobie, počas ktorého sa akreditovaná jednotka CSIRT využíva, zoznam osôb v pôsobnosti ústredného orgánu, ktoré budú zodpovedné za poskytovanie údajov a informácií a ich rozsah, povinnosti o hlásení zmien ovplyvňujúcich riadne fungovanie akreditovanej jednotky CSIRT a vyčíslenie prevádzkových nákladov, ktoré je ústredný orgán povinný uhradiť.		

§ 10 **Úlohy iného orgánu štátnej správy**		
(1) 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.	59. tento odsek je nelogický a zmätočný: a. kontinuita čoho? b. riziko súvisiace so zabezpečením sietí a IS je napríklad to, že sieť nebude zabezpečená c. siete a informačné systémy, ktoré nie sú základnou službou? d. zaistenie kontinuity a riadenia procesu riešenia kybernetických bezpečnostných incidentov? e. iný orgán zodpovedá tým že prijíma a dodržiava vhodné a primerané bezpečnostné opatrenia podľa § 20.	Ústredný orgán a iný orgán štátnej správy zodpovedá za zaistenie kybernetickej bezpečnosti aj tých informačných systémov a sietí v rozsahu jeho pôsobnosti, ktoré sa nevyužívajú pri poskytovaní základných alebo digitálnych služieb.

(1) Iný orgán štátnej správy ďalej poskytuje úradu požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité pre zabezpečenie kybernetickej bezpečnosti; informácie sa poskytujú len za podmienky, že ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu[13] alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb konajúcich v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce.		
•	59. zmätočné číslovanie odkazov pod čiarou	

[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.

§ 11 **Vládna jednotka CSIRT**		
Zriaďuje sa vládna jednotka CSIRT v pôsobnosti Úradu vlády 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.	60. Prečo sa zriaďuje ďalší CSIRT a nevyužíva existujúci medzinárodne uznávaný CSIRT.SK? 61. prečo by mal byť vládny CSIRT organizačnou zložkou príspevkovej organizácie NASES a nie napr. Telekomunikačného úradu, MV SR alebo iného relevantného štátneho orgánu? 62. výnimka z akreditácie je nekorektná, akú autoritu bude mať CSIRT, ktorý neprejde ani len domácou akreditáciou?	Pre podsektor informačné systémy verejnej správy sa zriaďuje sa jednotka CSIRT v pôsobnosti Úradu podpredsedu vlády pre IIVS Slovenskej republiky. Kým táto jednotka CSIRT nezíska medzinárodnú akreditáciu organizácie FIRST, povinnosti vládnej jednotky bude vykonávať jednotka Ministerstva financií SR, CSIRT.SK.

§ 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. 2, 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])	•	

[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.

(1) O zbavení povinnosti mlčanlivosti osoby podľa odseku 1 rozhodne v pôsobnosti a) úradu riaditeľ úradu, b) iného subjektu štatutárny orgán.		
(1) Na účely konania pred orgánom verejnej moci, na účely trestného konania, oznamovania skutočnosti nasvedčujúce spáchaniu trestného činu 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.	•	
(1) 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)]	•	
(1) Za škodu spôsobenú prevádzkovateľom základnej služby, poskytovateľom digitálnej služby, ich		

[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

zamestnancom alebo osobe oznamujúcej kybernetický bezpečnostný incident, ktorá vznikla oznámením podľa odseku 4, zodpovedá úrad. •		
(1) 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 všeobecného nariadenia o ochrane údajov.[17])	59. keďže kybernetický incident môže súvisieť s trestnou činnosťou, na spracovanie osobných údajov sa vzťahuje aj • DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA 59. čo je rozsah potrebný na zabezpečenie kybernetickej bezpečnosti? kto určí, čo je v záujme národnej bezpečnosti? To je zmes prázdnych fráz, ale obsah chýba • •	
(1) Úrad zabezpečí nepretržitú ochranu osobných údajov a informácie spracúvané podľa tohto zákona pred nezákonným vyzradením, zneužitím, poškodením, neoprávneným zničením, odcudzením a stratou spôsobom podľa všeobecného	59. taktiež prázdna a zbytočne nabubrelá formulácia, gramaticky nesprávna a. čo je to zákonné vyzradenie? b. výpočet nezahŕňa dostupnosť, integritu (doplnenie, kombinovanie) 60. aj podľa vyššie uvedenej Smernice DIRECTI-	

[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).

nariadenia o ochrane údajov.[18])	VE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA	
(1) Informácie a osobné údaje získané na základe tohto zákona alebo v súvislosti s ním môže úrad použiť len na plnenie úloh podľa tohto zákona.		

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

§ 13 **Akreditácia jednotky CSIRT**		
(1) Zhodu jednotky CSIRT s podmienkami akreditácie jednotky CSIRT posudzuje úrad na základe žiadosti.	59. jednotka CSIRT sa nemôže zhodovať s podmienkami akreditácie, lebo CSIRT je organizácia a podmienky akreditácie sú nejaké myšlienky 60. CSIRT môže spĺňať nejaké požiadavky a akreditácie je potvrdenie o tom, že ich spĺňa 61. žiadosť o čo? o posúdenie jednotky CSIRT, alebo akreditáciu?	
(1) Žiadosť podľa odseku 1 predkladá úradu v elektronickej podobe žiadateľ, ktorý má plniť úlohy jednotky CSIRT; k žiadosti prikladá dokumentáciu preukazujúcu splnenie podmienok akreditácie jednotky CSIRT.	59. akreditácia je formálny akt, ktorým sa završuje skúmanie súladu nejakej skutočnosti oproti nejakým kritériám. Vydanie, udelenie alebo priznanie akreditácie = akreditácia, podmienky akreditácie = predloženie podkladov, zaplatenie poplatku a súlad deklarovaných skutočností s požiadavkami na CSIRT (napr. podľa dokumentov ENISA, alebo nejakých štandardov)	
(1) 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.		
(2) Úrad o akreditácii rozhodne do 90 dní odo dňa doručenia úplnej žiadosti a ak posúdi zhodu jednotky CSIRT s podmien-	59. uviesť presnú citáciu (aké podmienky)	Ak úrad zistil, že jednotka CSIRT spĺňa podmienky (citácia), vydá rozhodnutie o akreditácii danej

kami akreditácie jednotky CSIRT, vydá rozhodnutie o akreditácii. Rozhodnutie o akreditácii sa vydáva na dobu určitú, najviac na päť rokov.	60. posúdenie zhody znamená, že úrad preskúmal, či CSIRT spĺňa požiadavky podľa nejakého zoznamu. Výsledok posúdenia môže byť aj negatívny. V takom prípade by Úrad nemal akreditovať CSIRT 61. aká je minimálna doba a na základe čoho Úrad určí dobu platnosti akreditácie? •	jednotky.
(1) 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“.	59. čo ak dôjde k zmene podmienok po podaní žiadosti o akreditáciu, resp. reakreditáciu?	
(1) 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; § 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.	59. aj cudzí CSIRT bude musieť spĺňať podmienky vyhlášky o šifrovej ochrane informácií?	

(1) 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	59. tu sa spájajú 2 rôzne veci – podmienky na administratívny proces (akreditáciu) a požiadavky na to ako má CSIRT fungovať 60. podmienky na činnosť CSIRT sú uvedené len rámcovo a odvolávajú sa na neexistujúci alebo nedostupný predpis 61. požiadavka na šifrovú ochranu informácie v plnom rozsahu je neopodstatnená, je potrebné explicitne uviesť, aké informácie bude potrebné chrániť šifrovaním 62. bude Úrad kontrolovať aj situáciu na mieste, alebo len posudzovať dokumentáciu, ktorú mu CSIRT predloží? •	

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])		

[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).

§ 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.	59. kto plní úlohy jednotky CSIRT? Týmto pojmom sa vnáša neistota, pretože jednotka CSIRT (vlastná, alebo zastupujúca) je jednoznačne určená. To je Computer security incident response team s úlohami definovanými napr. https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process/at_download/fullReport 60. existuje iný subjekt, ako CSIRT, ktorý plní úlohy jednotky CSIRT? 61. pojem služba má presné určenie (aj v direktíve EU), ktoré nezodpovedá významu, v ktorom sa používa tu	
(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 systé-	62. upresniť – preventívna činnosť CSIRT • 59. výcvikom koho? 60. ako môže CSIRT vytvárať bezpečnostné povedomie? 61. činnosti uvedené v bodoch c – f výskyt bezpečnostných incidentov neovplyvnia 62. CSIRT-y budú mať aj iné kanály na šírenie potrebných informácií, najmä vlastné webové stránky, alebo dohodnutý spôsob komunikácie so svojimi klientmi. Používanie jednotného IS KB ako jediného kanála na včasné varovanie	

mu kybernetickej bezpečnosti.	bude znamenať a. oneskorenie varovania, ktoré by CSIRT inak posielal svojím klientom priamo b. zahltenie zbytočnými informáciami aj tých, ktorých sa netýkajú	
(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.	59. nebolo varovanie (ods 2, písm g) preventívnou činnosťou? 60. výpočet je trocha chaotický, viaceré činnosti sa opakujú, napr. f) zahŕňa aj body d, e, g), písm. i) je preventívna činnosť	
(4) Reaktívne služby vykonáva jednotka CSIRT za účasti prevádzkovateľa základnej služby	61. CSIRT bude riešiť len bezpečnostné incidenty súvisiace so základnými a digitálnymi služba-	

alebo poskytovateľa digitálnej služby.	mi? Nie je to priveľký luxus zriaďovať na to CSIRT? 62. a čo prípady podľa §10, ods. 1)? bude CSIRT pri zásahu v „obyčajnom“ systéme vyžadovať účasť nejakého 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 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])	59. kto to je – zriaďovateľ, alebo jednotka CSIRT? 60. podľa predchádzajúceho § 15 by tým, kto plní úlohy jednotky CSIRT (podľa charakteru úloh) mala byť jednotka CSIRT. V § 16 to je zriaďovateľ jednotky CSIRT. 61. presnejšia formulácia, zriaďovateľ oznamuje zmeny týkajúce sa ním zriadenej jednotky CSIRT 62. čo ak ústredný orgán využíva externú jednotku CSIRT a zistí, že nespĺňa podmienky akreditácie? Kto je povinný oznámiť túto skutočnosť Úradu?	
(2) Ak akreditovaná jednotka	59. čo ak vládna jednotka CSIRT, resp. CSIRT na	

[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.

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.	Úrade prestanú/nebudú spĺňať podmienky akreditácie, kto to bude oznamovať úradu? 60. vyradí Úrad sám seba (alebo vládny CSIRT) zo zoznamu akreditovaných CSIRTov?	
(2) 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 tento 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, kedy prekročenie zistil.		
(2) Úrad zaradí základnú službu podľa § 3 písm. k) 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 pre-		

kročení identifikačných kritérií prevádzkovanej služby podľa § 18 a nedošlo k postupu podľa písmena a) alebo písmena b).		
(3) Úrad v spolupráci s príslušným ústredným orgánom zaradí základnú službu podľa § 3 písm. k) druhého bodu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb.		
(4) Úrad zaradí základnú službu podľa § 3 písm. k) tretieho bodu do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb zo zákona.		
(5) 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.		
(6) Zaradenie služby do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb oznámi úrad prevádzkovateľovi tejto služby prostredníctvom informačného systému kybernetickej bezpečnosti.	59. tento odsek je úplne zbytočný, len umelo zdôrazňuje potrebu nejakého podivného systému. Poskytovateľ základnej služby sa môže obrátiť na úrad napríklad aj prostredníctvom elektronickej stránky úradu a požadovať odpoveď do svojej elektronickej schránky. Alebo pošle in-	

	formáciu úradu v papierovej forme.	

§ 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,	59. existuje taký predpis? 60. podľa definície základnej služby, základnou službou môže byť informačný systém VS. Ako je definovaný používateľ informačného systému VS? 61. ako tieto incidenty súvisia so základnou službou? 62. prevádzkovateľ môže poskytovať aj iné služby a mať vďaka tomu trhový podiel väčší alebo menší ako je hraničná hodnota, podiel sa musí vzťahovať na službu 63. geografické rozšírenie čoho? 64. čo to znamená?	

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.	65. vydal úrad taký predpis?	
(4) Ak prevádzkovateľ služby podľa prílohy č. 1 zistí, že došlo k prekročeniu špecifických sektorových kritérií, oznámi to úradu do 30 dní odo dňa, kedy prekročenie zistil v rozsahu podľa § 17 ods. 5 aj v prípade, ak neprekročí dopadové kritéria.		

§ 19 **Povinnosti prevádzkovateľa základnej služby**		
(1) Prevádzkovateľ základnej služby povinný je do šiestich 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 uzatvorení zmluvy s dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby (ďalej len „tretia strana“) uzatvoriť zmluvu o zabezpečení plnení bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby platnosti zmluvy.	59. zmluva by sa mala týkať len tých služieb a činností dodávateľa, ktoré sa týkajú systémov a sietí prostredníctvom ktorých prevádzkovateľ základnej služby poskytuje základnú službu, alebo ich bezpečnostného okolia (t.j. infraštruktúry a služieb, ktorých výpadok by mohol narušiť rozsah alebo kvalitu poskytovania základnej služby). Zmluva medzi prevádzkovateľom a dodávateľom by sa mala týkať úrovne poskytovaných služieb (SLA) a bezpečnosti. Takáto formulácia je príliš široká a všeobecná a vzťahuje sa na všetky služby, ktoré poskytuje dodávateľ, teda aj tie, ktoré sa netýkajú základnej služby	
(1) Prevádzkovateľ základnej služby je povinný dňom zaradenia do registra prevádzkovateľov základných služieb o tejto skutočnosti informovať podnik na poskytovanie elektronických komunikačných služieb alebo sietí podľa osobitného predpisu, [23]) ku ktorému je sieť alebo informačný systém základnej		

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

služby pripojená. Na základe informovania podľa predchádzajúcej vety uzatvára prevádzkovateľ základnej služby s podnikom zmluvu podľa odseku 2.		
(2) 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.	59. akú tretiu stranu? 60. bezpečnostný incident je potrebné bližšie špecifikovať, z tejto formulácie nevyplýva ani to, že k incidentu došlo u prevádzkovateľa základnej služby. Takisto súvislosť incidentu so zmluvou je nejasná. Tento odsek je potrebné preformulovať, lebo z neho nie je jasné, aké povinnosti má prevádzkovateľ základnej služby a voči komu 9dodávateľovi, klientovi?)	
(1) 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.		
(2) 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 bez-	59. komu a čo je závažný incident (vysvetlenie alebo odkaz) • • • •	

pečnostného 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.	• • • 59. túto povinnosť nemusí byť prevádzkovateľ základnej služby schopný splniť (z technických dôvodov), navyše existujú bezpečnostné incidenty (havárie, prírodné katastrofy), ktoré nespôsobil človek, resp. nemajú charakter trestného činu • 59. nie je náhodou povinnosťou človeka oznámiť trestný čin, ak sa o ňom dozvie z hodnoverného zdroja?	
(1) Prevádzkovateľ základnej služby je povinný hlásiť zmeny v údajoch podľa § 17 ods. 5 do 30 dní odo dňa ich vzniku prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.	59. väzba na jednotný informačný systém je zbytočná a komplikuje komunikáciu s úradom.	
(1) 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 bezpeč-	59. z čoho bude úrad platiť škody?	

	nostným 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	59. tento odsek odráža nepochopenie podstaty manažmentu rizík a úlohu bezpečnostných opatrení. a. výpočet v prvej vete nezahŕňa všetky oblasti informačnej/kybernetickej bezpečnosti uvedené v ISO/IEC 27002 b. nie roľa ale rola/roly c. opatrenie nie je technológia, technológia je podstatne širší pojem (napr. IKT) d. cieľ je len deklarácia, ktorá nemusí mať nič spoločné s realitou e. zabezpečenie kybernetickej bezpečnosti – nie je povedané čoho f. životný cyklus sietí a informačných systémov – ako to súvisí s opatreniami? Keď už, tak zaistenie bezpečnosti sietí a informačných systémov počas celého ich životného cyklu 60. klasifikácia informácií a kategorizácia systémov a sietí vypovedá o rozsahu a úrovni ochrany, ktoré si informácia, systém alebo sieť vyžadujú. Zodpovedná osoba vyberá a implementuje súbor opatrení, postačujúcich na dosiahnutie požadovanej úrovne ochrany 61. existuje jediný bezpečnostný štandard v kybernetickej bezpečnosti, ISO/IEC 27032, ostatné štandardy sú o informačnej bezpečnosti	Bezpečnostné opatrenia sú riešenia technického, organizačného, právneho, fyzického a iného charakteru, ktoré minimalizujú riziká vyplývajúce z hrozieb voči aktívam organizácie, informačného systému alebo siete

sa prijímajú s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu 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.	62. ciele bezpečnostných opatrení sú širšie ako kontinuita (dostupnosť) služby, lebo na systémy sú kladené požiadavky vyplývajúce z iných zákonov, ISO/IEC 27002 resp. podobné štandardy obsahuje opatrenia na zaistenie dôvernosti, dostupnosti, integrity a autentickosti	
(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.	63. toto je chaotické spojenie rôznych vecí: a. klasifikačných kritérií a b. úrovne bezpečnostných požiadaviek c. na druhej strane sa spája klasifikácia informácie a kategorizácia systémov, pričom kategorizácia systémov je odvodená od klasifikácie informácie, ktorá sa v nich spracováva 64. čo to je a. dôvernosť, integrita a kvalita služby b. funkcia informácie? 65. ako sa pri klasifikácii informácie má zohľa-	klasifikáciu informácií a kategorizáciu systémov popisujú americké štandardy FIPS 199 a FIPS 200. Na ne nadväzujú dokumenty popisujúce opatrenia, ktoré je potrebné implementovať, ak sa má dosiahnuť úroveň bezpečnosti zodpovedajúca jednotlivým kategóriám systémov

	dňovať kontrolná činnosť?	
(3) Bezpečnostné opatrenia sa prijímajú najmä pre oblasť a) organizácie informačnej bezpečnosti, b) riadenia aktív, hrozieb a rizík, c) personálnej bezpečnosti, d) riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov, e) technických zraniteľností systémov a zariadení, f) riadenia bezpečnosti sietí a informačných systémov, g) riadenia prevádzky, h) riadenia prístupov, i) kryptografických opatrení, j) riešenia kybernetických bezpečnostných incidentov, k) monitorovania, testovania bezpečnosti a bezpečnostných auditov, l) fyzickej bezpečnosti a bezpečnosti prostredia, m) riadenia kontinuity procesov.	59. toto je výpočet kapitol normy ISO/IEC 27002, chýba tam súlad s legislatívou a štandardami a jednotlivé oblasti neboli v zákone nejako definované. Keďže opatrenia by mali vychádzať z klasifikácie informácie a kategorizácie systémov a sietí úrad by mal udržiavať a aktualizovať súbory povinných opatrení. Tento článok je zbytočný, stačí odkaz na normu 60. čo je riadenie prístupov? kto a k čomu pristupuje? 61. prevádzky čoho? 62. bezpečnostné opatrenia sa prijímajú pre oblasť kryptografických opatrení? •	
(1) Bezpečnostné opatrenia musia zahŕňať najmenej a) detekciu kybernetických bezpečnostných incidentov, b) evidenciu kybernetických bezpečnostných incidentov, c) postupy riešenia a riešenie kybernetických bezpečnostných incidentov, d) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení, e) pripojenie do komunikačného systému pre hlá-	59. toto nie sú bezpečnostné opatrenia typu uvedeného v predchádzajúcom článku, ale a. na detekciu niektorých bezpečnostných incidentov sa dá použiť intrusion detection system b. evidencia bezpečnostných incidentov je administratívne opatrenie c. postupy riešenia bezpečnostných incidentov je dokument na úrovni špeciálnej bezpečnostnej politiky, alebo bezpečnostného štandardu organizácie	

senie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania.	d. riešenie bezpečnostných incidentov nie je opatrenie, ale činnosť e. určenie kontaktnej osoby je administratívno-organizačné opatrenie f. pripojenie do komunikačného systému je dobré len na prijímanie varovaní a hlásenie hrozieb 60. sumarizácia. Organizácia musí a. mať IDS b. evidovať bezpečnostné incidenty c. mať vypracované postupy na riešenie bezpečnostných incidentov d. riešiť bezpečnostné incidenty e. mať kontaktnú osobu (ale nemusí ju nahlásiť úradu) f. pripojiť sa na JISKB čo však na zaistenie informačnej/kybernetickej bezpečnosti zďaleka nestačí (o.i. chýba prevencia, budovanie bezpečnostného povedomia, kapacity na riešenie bezpečnostných incidentov, vnútorná legislatíva a i.)	
(5) Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.	61. kto tú dokumentáciu bude schvaľovať? 62. čo ak bude potrebné prijať akútne opatrenia na riešenie kritickej situácie – aj vtedy bude potrebné schvaľovanie? 63. aké oneskorenie na aktualizáciu dokumentácie je prípustné? (spracovanie bezpečnostného projektu na rozsiahly systém trvá značný čas)	

§ 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.	59. chýba bližšie určenie informácií, ktoré má poskytovateľ dig. služby nahlásiť Úradu – zrejme ide o **jeho názov a sídlo,** kontaktné údaje 60. má nahlásiť digitálnu službu a nie akúkoľvek službu, ktorú poskytuje; nemal by nahlasovať digitálnu službu, ktorú už v minulosti nahlásil, presnejšie má nahlásiť názov (a zrejme aj nejakú bližšiu špecifikáciu) digitálnej služby 61. tieto nepresnosti môžu spôsobiť zmätok, Úrad by mal presne špecifikovať, čo potrebuje vedieť 62. nie je ošetrený prípad, keď niekto poskytoval digitálnu službu ešte pred nadobudnutím platnosti zákona; potom nemôže stihnúť termín 30 dní stanovený zákonom	
(1) Na základe oznámenia podľa odseku 1 úrad zaradí službu do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb.	59. čo ak oznámenie nebude obsahovať potrebné údaje? 60. čo ak bude nepravdivé (niekto nahlási iný subjekt ako poskytovateľa digitálnej služby)? 61. Úrad by si mal overiť pravdivosť údajov, ktoré uviedol poskytovateľ digitálnej služby a až po overení by ho mal zaradiť do registra	
(1) Úrad zaradí službu do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb aj na základe vlastného zistenia.	59. čo to znamená? Okrem logického prípadu, ak poskytovateľ služby, ktorá spĺňa kritériá digitálnej služby, nenahlásil, že takú digitálnu službu poskytuje a Úrad to zistí, to môže znamenať duplicitu. Navyše, ako Úrad zistí údaje potrebné na registráciu?	ak Úrad zistí, že nejaký subjekt poskytuje službu, ktorú spĺňa špecifikáciu digitálnej služby a neoznámil to v stanovenej lehote Úradu, Úrad • by si od subjektu mal vyžiadať údaje potrebné na registráciu • začať správne konanie za nedodržanie zákonnej povinnosti

(1) Zaradenie služby do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb oznámi úrad poskytovateľovi tejto služby.	59. ako a do akého termínu?	
(1) Poskytovateľ digitálnej služby je povinný hlásiť zmeny v údajoch podľa odseku 1 do 30 dní odo dňa ich vzniku.	59. tu nejde o zmeny v údajoch, ale zmeny skutočností, ktoré sú zaznamenané v údajoch, ktoré poskytovateľ DS nahlásil úradu. Údaje o skutočnostiach, ktoré je poskytovateľ povinný nahlásiť, má Úrad, zmeny údajov robí Úrad a poskytovateľ o nich nemusí vedieť, a teda ich nemôže nahlásiť	

§ 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.	59. to je neskoro, takto môže subjekt minimálne 7 mesiacov poskytovať digitálnu službu bez patričných bezpečnostných opatrení 60. Tento článok sa nedá zosúladiť s chápaním bezpečnostných opatrení: *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*. a. Ako sa dajú *prijať a dodržiavať úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti* ? b. *vhodné a primerané úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti,* na *účely riadenia rizík súvisiacich s ohrozením kontinuity digitálnej služby* c. *vhodné a primerané úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, na účely procesu riešenia kybernetických bezpečnostných incidentov.* 61. čo sú časové zdroje? 62. zaistiť kontinuitu digitálnej služby nestačí,	

[24]) Vykonávacie nariadenie Komisie (EÚ) ... / ... ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148, pokiaľ ide o ďalšie špecifikácie prvkov, ktoré majú brať do úvahy poskytovatelia digitálnych služieb na riadenie rizík, ktoré predstavujú pre bezpečnosť sieťových a informačných systémov a parametre na určenie toho, či incident má podstatný vplyv.

	digitálnu službu je potrebné poskytovať v požadovanom rozsahu, kvalite a s primeranými (bezpečnostnými) zárukami	
(1) 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,	59. toto je nepresná formulácia, poskytovateľ DS môže niečo posúdiť, ale nemusí zistené problémy riešiť, 60. mal by posudzovať siete a informačné systémy, pomocou ktorých poskytuje digitálnu službu (a nie bližšie neurčené systémy) 61. štylisticky zlé: IS má schopnosť predchádzať kybernetický bezpečnostný incident 62. požiadavka na univerzálnu odolnosť systému voči kybernetickým bezpečnostným incidentom je nezmyselná, lebo a. existuje veľké množstvo hrozieb b. odolnosť systému voči konkrétnej hrozbe závisí od prijatých opatrení, ktoré nemusia byť implementované v systéme c. množstvo hrozieb zasahuje systém nepriamo, cez jeho okolie d. navyše navrhovaná formulácia nešpecifikuje, aké kybernetické bezpečnostné incidenty by mal byť systém schopný riešiť, či tie, ktoré sa vzťahujú na samotný systém, alebo akékoľvek (ktoré sa v organizácii vyskytnú) 63. ale podľa definície sú *riešením kybernetického bezpečnostného incidentu všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a jeho následky.* Informačný systém nie je (a nemôže byť schopný) riešiť kybernetické bezpečnostné incidenty v zmysle definície	

c) súlad sietí a informačného systému s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti.	64. táto povinnosť je definovaná nepresne: a. čo je to kontinuita digitálnej služby? je to zachovanie dostupnosti služby vo všeobecnosti, alebo zachovanie dostupnosti služby u daného poskytovateľa? b. aké kybernetické bezpečnostné incidenty treba zohľadniť? všetky? c. posúdenie spôsobu zachovania kontinuity DS ešte neznamená, že sa kontinuita DS zachová d. zachovanie kontinuity DS môže znamenať degradáciu jej úrovne 65. existuje jediný bezpečnostný štandard o kybernetickej bezpečnosti (ISO/IEC 27032), bežne sa používajú štandardy informačnej bezpečnosti, na ktoré sa ISO/IEC 27032 odvoláva 66. siete a informačné systémy (ktoré?) nemôžu byť v súlade so štandardami, ale s požiadavkami štandardov 67. keďže existuje veľké množstvo relevantných štandardov informačnej bezpečnosti, súlad s ktorými z nich vyžaduje zákon?	
(1) Poskytovateľ digitálnej služby je povinný a) hlásiť každý kybernetický bezpeč	59. poskytovateľ DS by mal nahlasovať len bezpečnostné incidenty, ktoré sa týkajú DS, ktorú poskytuje • 59. táto formulácia znamená, že ak je poskytovateľ schopný posudzovať vplyv kybernetických bezpečnostných incidentov (na čo?) tak by mal nahlasovať každý kybernetický bezpečnostný incident (nielen závažný a nielen taký, ktorý sa ho týka, ale napr. aj bezpečnostné incidenty u iných subjektov) •	

	nostný incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento	59. to by znamenalo, že poskytovateľ DS má riešiť každý kybernetický bezpečnostný incident, ktorý niekto nahlásil, alebo len tie, ktoré nahlásil on sám? 60. kybernetické bezpečnostné incidenty (menej významné) u poskytovateľa DS, ktoré nikto nenahlásil, poskytovateľ nemusí riešiť? 61. čo ak úrad nebude daný bezpečnostný incident riešiť?	

	ky- ber ne- tic- ký bez peč nos tný in- ci- den t pod stat ný vpl yv pod ľa oso bit- né- ho pre d- pi- su,[24]) a to bez od- kla dne po		

jeho zistení, b) riešiť hlásený kybernetický bezpečnostný incident, c) spolupracovať s úradom pri rieš		

ení hlá sen ého ky- ber ne- tic- ké- ho bez peč nos t- néh o in- ci- den tu.		
(1) Ak poskytovateľ digitálnej služby využíva na poskytovanie svojej digitálnej služby prevádzkovateľa základnej služby, je povinný uzatvoriť s prevádzkovateľom základnej služby zmluvu o zabezpečení plnení bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby, kedy poskytovateľ digitálnej služby využíva na poskytovanie svojej digitálnej služby prevádzkovateľa základnej služby.	59. nepresné – poskytovateľ DS nevyužíva prevádzkovateľa základnej služby, ale základnú službu; 60. štylistika: o zabezpečení plnenia 61. kto má plniť bezpečnostné opatrenia? 62. bezpečnostné opatrenia sú *sú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti,* a plnia sa nanajvýš úlohy, ostatné opatrenia sa implementujú, udržiavajú, dodržiavajú •	

(1) 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 nie je dotknutá.	59. akej zmluvy? 60. kto je tretia strana?	

§ 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.	61. čo ak sa rozhodne založiť si sídlo v inej krajine EÚ?	
(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.	62. nepresné, ide o siete a systémy, pomocou ktorých poskytuje digitálnu službu. 63. asi nie hociktorým, ale v tom štáte, kde má poskytovateľ inštalované svoje technické zariadenia, pomocou ktorých poskytuje dig. službu	

§ 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.	64. kybernetický bezpečnostný incident sa dá identifikovať na základe príznakov, potom sa rieši a až v tejto fáze sa dá posúdiť jeho dopad a následne ho porovnať s nejakými kritériami 65. keďže kybernetický bezpečnostný incident je definovaný veľmi všeobecne (a vecne nesprávne), poskytovateľ základnej služby má povinnosť hlásiť (komu – úradu?) aj bezpečnostné incidenty, ktoré sa netýkajú poskytovania základnej služby, dokonca aj tie, ktoré nenastali u neho(!)	
(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.	66. podľa definície je *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,* udalosť sa nemôže členiť na kategóriu, udalosti sa môžu zaraďovať do kategórií na základe nejakých kritérií 59. kritériá pre kategorizáciu kybernetických bezpečnostných incidentov sú definované veľmi všeobecne (musí bezpečnostný incident spĺňať všetky, alebo stačí jedno z kritérií, t.j. je v podmienke konjunkcia alebo disjunkcia?) 60. kategorizácia bezpečnostných incidentov sa nikde nevyužíva a teda je zbytočná	
(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 služieb.	61. nepresné, nie je jasné, či je poskytovateľ digitálnych služieb povinný hlásiť len bezpečnostné incidenty u seba, alebo aj u iných poskytovateľov digitálnych služieb	
(4) Hlásenie kybernetických bezpečnostných incidentov sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.	62. toto je dobré len na preukázanie potreby vytvorenia jednotného informačného systému kybernetickej bezpečnosti, ale nemá reálne opodstatnenie – ak dôjde k bezpečnostnému incidentu, ktorý vyradí počítačovú sieť, postihnutý subjekt sa nebude môcť pripojiť na JISKB ale ešte by mohol použiť iné komunikačné kanály a požiadať úrad o pomoc	
(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	63. postihnutý subjekt bude mať v priebehu bezpečnostného incidentu iné starosti, ako posielať úradu nejaké hlásenia	

toto hlásenie doplní.		
(6) 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 prevádzkovateľom základnej služby.	citácia (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.	

§ 25 **Hlásenie kybernetických bezpečnostných incidentov poskytovateľom digitálnej služby**	64. platia pripomienky k hláseniu bezpečnostných incidentov poskytovateľom základnej 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**	65. celý tento paragraf je zbytočný, lebo hovorí, že ľudia môžu úradu posielať hlásenia, ale úrad sa nimi nemusí zaoberať. Paragraf neukladá úradu žiadne povinnosti (napr. informovať toho, kto nahlásil bezpečnostný incident, čo sa s ním bude diať)	
(1) Dobrovoľné hlásenie kybernetických bezpečnostných incidentov, bez ohľadu na kategorizáciu kybernetického bezpečnostného incidentu, sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.	66. nie je jasné, kto by mal dobrovoľne nahlasovať bezpečnostné incidenty 67. keďže incidenty nie sú bližšie špecifikované, môže ísť o akékoľvek kybernetické bezpečnostné incidenty, ku ktorým došlo kedykoľvek a kdekoľvek na svete 68. ale ten, kto incidenty nahlasuje, musí byť pripojený na JISKB	
(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.	69. nezrozumiteľná a zmätočná formulácia: a. úrad môže nastavením JISKB zablokovať posielanie hlásení b. odvolaním sa na preťaženosť sa nemusí hláseniami vôbec zaoberať c. aké subjekty sa nemajú zaťažovať? d. aká 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 ich vykonanie určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu (ďalej len „ochranné opatrenie“).	59. nepochopenie vzťahu medzi hrozbou, naplnením hrozby, rizikom, hodnotou rizika, mierou pravdepodob	

	nosti naplnenia hrozby a do padom hrozby. Hrozba je objektívna skutočnosť (blesk, útok hackera), ktorá sa môže uplatniť	

	(naplniť) voči nejakému aktívu v prípade, ak toto aktívum má slabinu (výbuch sopky v oblasti, kde nie je aktívna sop-	

	ka asi ne-hroz í). To čo sa men í, je rizi-ko, lebo to závi sí aj od prav dep o-dob nos-ti na-pl-ne-nia hroz by aj do-pa-du hroz by	

	na aktívum. (napr. odborne zdatný hacker sa rozhodne zaútočiť na konkrétny systém) 60. formulácia je nepres	

	ná – bude úrad vydávať výstrahy ak niekde vo svete došlo k závažnému kybernetickému bezpečnostnému inci-	

	dentu, ktorý sa nás vôbec netýka? 61. aký je rozdiel medzi výstrahou a varovaním? 62. varovať možno pred hrozbou, alebo rizi-	

	kom, va-ro-vať pre uda-los-ťou, ktor á už na-stal a, je zby-toč-né. Va-ro-va-nie má zmy sel, ak sa za-brán i tom u, aby k po dob nej uda-	

	63.	lostined ošlonepresnáformulácia – komu môžeúradukladaťpovinnosťriešiťkybernetickýbezpečnostnýincident

	64. ? ako sa dá spl- niť po- vin- nosť rieši ť ky- ber- ne- tic- ký bez- peč- nost ný in- ci- dent , ak taký ešte ne- na- stal (V príp ade hroz by záv	

	ažného kybernetického bezpečnostného incidentu)	
(1) 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.		
(2) Povinnosť riešiť kybernetický bezpečnostný incident ukladá úrad rozhodnutím tomu, kto plní úlohy jednotky CSIRT, prevádzkovateľovi základnej služby a poskytovateľovi digitálnej služby.	59. nepresné. kybernetický bezpečnost	

[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).

	ný incident sa môže udiať u tretej strany, ktorá nemá s CSIRT-om, prevádzkovateľom základnej služby a poskyto-	

	va-te-ľom digi tál-nej služ by nič spol očné. Zm ysel by mal o to, keb y úrad ukla dal po-vin-nos-ti tým sub-jek-tom, ktor ých sa dan ý	

	ky-ber-ne-tic-ký bez-peč-nost-ný in-ci-dent re-álne týka (a môž u ho rieši ť)	
(1) Reaktívne opatrenie je priama odpoveď na závažný kybernetický bezpečnostný incident a zabezpečuje sa podľa § 15 ods. 3 písm. b) až g).	59. Citácia: *b)* *detekcia kyber-netic-kých bezpeč-nost-ných in-ciden-tov, c)*	

	analýza kybernetických bezpečnostných incidentov, *d)* *odozva, ohraničenie, riešenie a náprava následkov kybernetických bezpečnostných incidentov,* *e)* *asistencia pri riešení kybernetického bezpeč-*	

	nostného incidentu na mieste, f) *reakcia na kybernetický bezpečnostný incident, g)* *podpora reakcií na kybernetické bezpečnostné incidenty,* t.j. Reaktívne opatrenie je priama odpoveď na závažný	

	kybernetický bezpečnostný incident a zabezpečuje sa *reakciou na kybernetický bezpečnostný incident;* ale aj ďalšie navrhované riešenia sú pochybné	
(1) 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 povinnosť vykonať reaktívne opatrenie uložiť iba počas krízovej situácie.[26])	59. čo ak nie je v silách dotknutého	

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

	subjektu bezpečnostný incident vyriešiť? Tam mu žiadne povinnosti ukladané úradom nepomôžu	
(1) 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.	59. umelé a zby-	

	točné, nestačí zatelefonovať alebo poslať mail a neskôr analýzu? Bude sa úradne jako zapájať do riešenia nahlásené ho ky-	

	ber- ne- tic- ké- ho bez- peč- nost néh o in- ci- den- tu?	
(1) Ochranné opatrenie prijíma prevádzkovateľ základnej služby na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.	59.	toto je štan dard ný po- stup (IS O/I EC 270 05) správy ri- zík, ne- stač í sa od- vola

	ť na štan dar- dy • I	
(1) 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, s ústredným orgánom a tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.	59. Navrhované riešenie nehovorí nič o tom, že si úrad bude namieste overovať príčiny bezpečnostného in-	

	ci- den- tu a sta v bez- peč- nost nýc h opa- tren í sys- té- mu. Na zá- klad e čoh o bud e roz- ho- do- vať o pr i- me- ra- nos- ti na-	

	vrhovaného opatrenia? Aj na toto existuje štandardný nástroj, bezpečnostný audit a profesionáli (CISA), schopní ta-	

	kýto audit vy-kon ať. 60. na zá-klad e čoh o úrad roz-hod ne, že na-vrh ova-né opa-tren ie je zjav ne ne-ús-peš-né? 61. ne-pres né, mali by	

	62.	to byť subjekty, v ktorých pôsobnosti je prevádzkovateľ základnej služby povinnosť spolupracovať na návrhu (opa

	trenia) ešte nič nerieši, lebo spolu-práca ne-musí viesť ku konkrétnemu výsledku a toto opatrenie sa ešte ne-musí imple men	

	to-vať, resp. keď sa im-ple men tuje a uk áže sa, že je ne-pos-taču júce – čo sa bud e diať po-tom ?	
(1) 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 vply-voch kybernetického bezpečnostného incidentu na bezpečnosť štátu ako podklad na riešenie krízovej situácie.[27])	59. ne-pres né, nie je	toto by malo byť prefor-mulo-

[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.

	stanovená oblasť, v ktorej je potrebné zaistiť kybernetickú bezpečnosť 60. závažný bezpečnostný incident môže mať ob-	vané tak, že ak došlo k závažnému kybernetickému bezpečnostnému incidentu, ktorý má/môže mať závažný dopad na fungovanie štátu a úrad vyčerpal na riešenie daného kybernetického bezpeč-

	medzený dopad (4 kategórie), bude sa v každom prípade vyhlasovať stav núdze? •	nostného incidentu všetky možnosti dané týmto zákonom a napriek tomu sa mu tento incident nepodarilo vyriešiť, resp. zabrániť jeho opakovaniu v budúcnosti; úrad/riaditeľ úradu

		predloží predsedovi Bezpečnostnej rady Slovenskej republiky správu o danom kybernetickom bezpečnostnom incidente a jeho (predpokladaných) dopadoch a návrh na riešenie krízo-

		vej situácie.
(1) 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 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.		

§ 28 **Kontrola**		
(1)Pri výkone kontroly nad dodržiavaním ustanovení tohto zákona a jeho vykonávacích predpisov postupuje úrad podľa základných pravidiel kontrolnej činnosti ustanovených osobitným predpisom.[29])	59. Môže sa pri kontrole súkromných subjektov postupovať podľa zákona o kontrole v štátnej	

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

[29]) § 8 až 13 zákona Národnej rady Slovenskej republiky č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov.

	správe?	
(1)Na účely výkonu kontroly má prevádzkovateľ základnej služby a poskytovateľ digitálnej služby práva a povinnosti kontrolovaného subjektu podľa osobitného predpisu.[30])	59. detto	
(1)Úrad vykoná kontrolu u poskytovateľa digitálnej služby ak aj dôvodné podozrenia, že poskytovateľ digitálnej služby nespĺňa požiadavky stanovené týmto zákonom.	59. sú dôvodné podozrenia 60. čo sú dôvodné podozrenia a ako sa posudzuje, že ide o **dôvodné** podozrenie?	

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

§ 29 **Audit**		
(1) Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základných služieb.	59. pojem audit kybernetickej bezpečnosti nie je definovaný	
(1) 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.	59. nepresné formulácie – audit by sa mal vzťahovať len na systémy a siete, ktoré sa používajú pri poskytovaní základnej služby 60. zbytočne a na úkor zrozumiteľnosti sa spája niekoľko vecí a. klasifikácia informácie a systémov – to by mohlo ísť do predpisu, ak sa	

	klasifikácia informácie a systémov premieta do rozsahu a úrovne povinných opatrení b. dôvody pre vykonanie auditu (zmeny v organizácii (resp. jej systémoch)) c. pravidelný audit	
(1) Audit kybernetickej bezpečnosti vykonáva orgán posudzovania zhody podľa osobitného predpisu,[31]) ktorý je akreditovaný ako orgán príslušný na posudzovanie zhody v oblasti kybernetickej bezpečnosti.		

[31]) Čl. 2 bod 13 nariadenia Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13. 8. 2008).

(2) 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.		
(3) Bez toho, aby bol dotknutý odsek 1, môže úrad kedykoľvek vykonať audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby, alebo požiadať orgán posudzovania zhody, aby vykonal takýto audit u prevádzkovateľa základnej služby s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom.	59. je úrad akreditovaným audítorom podľa európskych predpisov?	
(1) Náklady na audit kybernetickej bezpečnosti podľa odseku 1 znáša prevádzkovateľ základnej služby a náklady na audit kybernetickej bezpečnosti podľa odseku 5 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. 5, c) poruší niektorú z povinností podľa § 19 ods. 1 až 4, 6 alebo ods. 7, d) neprijme bezpečnostnú dokumentáciu podľa § 20 ods. 5 alebo	59. Citácia §19, ods 6 *(6) Prevádzkovateľ základnej služby je ďalej povinný* a) *ri* b) *b* c) *sp* d) *v* e) *oz* toto sú povinnosti prevádzkovateľa, čiže právnickej osoby. Na ktorú fyzickú osobu (štatutára, operátora) sa budú tieto ustanovenia vzťahovať?	

	59. Citácia §19, ods 7	
e) nepostupovala v súlade s technickými, organizačnými alebo personálnymi opatreniami prijatými prevádzkovateľom základnej služby.	(7) Prevádzkovateľ základnej služby je povinný hlásiť zmeny v údajoch podľa § 17 ods. 5 do 30 dní odo dňa ich vzniku prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. je rovnako závažným priestupkom, ak sa pri nahlasovaní bezpečnostných incidentov nebude používať JISKB?	
	60. citácia §20, ods. 5 *Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.*	

	formulácia písm. d) je zmätočná, lebo ods. 5 §20 nehovorí o prijímaní bezpečnostnej dokumentácie, ale o prijímaní a implementácii (realizácii) bezpečnostných opatrení, ktoré majú byť zdokumentované. Fyzická osoba môže zodpovedať za to, že nerealizovala opatrenia, ktoré prevádzkovateľ prijal schválením bezpečnostnej dokumentácie (napr. bezpečnostnej politiky, bezpečnostných smerníc, štandardov), ale nemôže presadiť prijatie bezpečnostnej dokumentácie (to vydáva vedenie organizácie, alebo štatutár)	
(1) Za priestupok môže úrad uložiť pokutu od 100 eur do 5 000 eur.		

(2) Na priestupky a ich prejednávanie sa vzťahuje všeobecný predpis o priestupkoch.[32])	59. na aký orgán sa môže postihnutá osoba odvolať voči rozhodnutiu úradu?	
(1) Priestupky prejednáva úrad a pokuty ukladá úrad.		
(2) Pokuty za priestupky sú príjmom štátneho rozpočtu.		

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

§ 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	citácie (2) *Prevádzkovateľ základnej služby je povinný pri uzatvorení zmluvy s dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a infor-*	

b) udržiavať bezpečnostnú dokumentáciu aktuálnu a zodpovedajúcu reálnemu stavu podľa § 20 ods. 5.	*mač-ných systé-mov pre pre-vádz-kova-teľa zá-klad-nej služby (ďalej len „tretia strana“) uzat-voriť zmluvu o za-bezpe-čení pl není bez-peč-nost-ných opa-trení a noti-fikač-ných povin-*	

	ností podľa tohto zákona počas celej doby platnosti zmluvy. (3) *Prevádzkovateľ základnej služby je povinný dňom zaradenia do registra prevádzkovateľov základných služieb o tejto*	

	skutočnosti informovať podnika na poskytovanie elektronických komunikačných služieb alebo sietí podľa osobitného predpisu,[33]*) ku ktorému je sieť alebo informačný systém základnej služby*	

[33]) § 5 ods. 1 zákona č. 351/2011 Z. z. v znení zákona č. 247/2015 Z. z.

	pripojená. *Na základe informovania podľa predchádzajúcej vety uzatvára prevádzkovateľ základnej služby s podnikom zmluvu podľa odseku 2.* (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 ne-	

	mož-ným, ak úrad neroz-hodne inak. Povin-nosť zacho-vávať mlčan-livosť tým nie je dot-knutá. (7) *Pr* citácia §20 ods 5 *(5) Bez-peč-nost né opa-treni a sa prijí maj ú a rea-lizu-jú*	

	na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.	

(1) 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,	citácie §17 ods. 1	

c) prijať bezpečnostnú dokumentáciu podľa § 20 ods. 5, d) nahlásiť závažný kybernetický bezpečnostný incident podľa § 24 ods. 1 alebo odoslať neúplné hlásenie podľa § 24 ods. 5, 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,	§ 19 ods. 1 (2) *Prevádzkova-*	

f) predložiť ochranné opatrenie na schválenie alebo vykonať schválené ochranné opatrenie podľa § 27 ods. 8, g) podľa § 29 ods. 1, 2 alebo ods. 4, alebo h) vykonať opatrenie na nápravu v lehote podľa záverečnej správy o výsledkoch auditu podľa § 29.	*teľ základnej služby povinný je do šiestich 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. alebo ods. 6, (6) *Pr* a) *rie* b) *be* c) *sp*	

	d) *v č* e) *oz* § 24 ods. 1 *Prevádzkovateľ základnej služby je povinný hlásiť každý závažný kybernetický bezpečnost*	

	ný incident, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bez-	

	pečnostných incidentov. *§ 24 ods. 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 obnovení adnej prevádzky siete a informačného systému u toto hlás	

	enie do-plní § 27 ods. 3, *Po-vin-nosť rieši-ť ky-ber-ne-tický bez-peč-nost-ný inci-dent ukla-dá úrad roz-hod-nu-tím tom u, kto plní úlo-hy jedn*	

	otky CSI RT, pre-vádz kova teľo-vi zá-klad nej služ-by a po sky-to-va-teľo-vi digi-tál-nej služ-by. § 27 ods. 5 *Po-vin-nosť vy-kon ať reak tív-ne*	

	opatrenie ukladá úradrozhodnutím prevádzkovateľovi základnej služby alebo poskytovateľovi digitálnej služby, ktorí sú	

	pririešenízávažnéhokybernetickéhobezpečnostnéhoincidentunečinní,alebo akriešenie závažného kybernetického bezpeč-	

	nostného incidentu je zjavne neúspešné. Poskytovateľovi digitálnej služby možno povinnosť vykonať reaktívne opa-	

	treni e ulo-žiť iba po-čas kríz ovej situ-ácie .[34]) § 27 ods. 6, *Pre-vádz kova teľ zá-klad nej služ-by aleb o po sky-to-va-teľ digi-tál-nej služ-*	

[34]) Zákon č. 387/2002 Z. z. v znení neskorších predpisov.

	by je povinný bezodkladne oznámiť a preukázať úradu prostredníctvom jednotného informačného systému kyber-	

	ber- ne- tic- kej bez- peč- nos- ti vy- kon anie reak tív- ne- ho opa- treni a a jeho vý- sled ok. § 27 ods. 8, *pre- vádz kova teľ zá- klad nej služ- by je na vý-*	

	zvu úra- du v ur- čene j leho te po- vin- ný pred ložiť na- vrho vané ochr an- né opa- treni e na schv álen ie. Úra d roz- hod- nu- tím na- vrho vané opa-	

	trenie schváli a určí lehotu na jeho vykonanie. V prípade, ak prevádzkovateľ základnej služby nenavrhne ochranné opa-	

	trenie v určenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je prevádzkovateľ základnej služby	

	povinný spolupracovať s úradom, s ústredným orgánom a tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu. § 29		

	od s. 1, *Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bez-*	

	pe č- no st- ný ch op a- tre ní a pln e- nie po žia da vie k sta no ve- ný ch tý m- to zá- ko no m vy- ko na ní	

	m au di- tu ky- be r- ne- tic kej be z- pe č- no sti do dv oc h ro ko v od o dň a za- ra- de nia pr e- vá dz-	

	kovateľa základnej služby do registra prevádzkovateľov základných služieb.	

	§ 29 ods. 2 Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stan	

	ovenýchtýmtozákonomvykonaním auditukybernetickejbezpečnostiv rozsahustanovenompodľavšeobecnezáväzného	

	právneho predpisu, ktorý vydá úrad, a to v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov po kaž-	

	dej zme- ne maj úcej vý- zna mný vply v na rea- lizo- vané bez- peč- nost né opa- treni a a v ur- čeno m časo vom in- ter- vale. • *§*	
(1) 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, § 22 ods. 4 alebo § 23 ods. 2.		

(2) 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.	§ 21 ods. 1, (1) *Poskytovateľ digitálnej služby je povinný do 30 dní odo dňa začatia poskytovania digitálnej služby, oznámiť úradu* a) *n* b) *k* c) *p* d	

	n § 22 ods. 3, *Poskytovateľ digitálnej služby je povinný* a)	

	b) c) § 24 ods. 3, *Ak prevádzkovateľ základnej služby využíva na poskytovanie*		

	základnej služby poskytovateľa digitálnej služby, je poskytovateľ digitálnej služby povinný hlásiť každý závažný	

		ky-ber-ne-tický bez-peč-nost-ný inci-dent, ktor-ý pos-tihol po-sky-to-va-teľa digi-tál-nej služi-eb. § 25 ods. 1 alebo ods. 2 *Poskyto-va-teľ digi-tál-*	

	nej služby je povinný hlásiť kybernetický bezpečnostný incident podľa § 22 ods. 3 písm. a) spôsobom podľa § 24 ods. 4. *Ak do*	

	okamihu hlásenia kybernetického bezpečnostného incidentu nepominuli jeho účinky, poskytovateľ digitálnej služ-	

	by je povinný odoslať neúplné hlásenie kybernetického bezpečnostného incidentu, v ktorom vyznačí identifikátor neukon-	

	čené ho hlá- seni a a bez- od- klad ne po ob- nove riad nej pre- vádz ky siete a in- for- mač né- ho sys- té- mu toto hlá- seni e do- plní. § 27	

	ods. 5. *Povinnosť vykonať reaktívne opatrenie ukladá úrad rozhodnutím prevádzkovateľovi základnej služby alebo poskyto-*	

	va-teľo-vi digi-tál-nej služ-by, ktorí sú pri-rieš-ení záva-žné-ho ky-ber-ne-tic-kého bez-peč-nost-ném o in-ci-den-tu neči-nní, aleb o ak-rieš-enie	

	závažného kybernetického bezpečnostného incidentu je zjavne neúspešné. Poskytovateľovi digitálnej služby možno	

	povinnosť vykonať reaktívne opatrenie uložiť iba počas krízovej situácie.[35])	
(1) Úrad uloží pokutu od 300 eur do 100 000 eur tomu, kto na výzvu úradu neposkytne informácie podľa § 7 ods. 3.	*Ústredné orgány a iné orgá-*	

[35]) Zákon č. 387/2002 Z. z. v znení neskorších predpisov.

	ny štát-nej sprá vy spol u-pra-cujú s úr a-dom na vy-pra-co-vaní náro dnej strat égie ky-ber-ne-tic-kej bez-peč-nos-ti a na ten-to účel sú	

	povinné poskytnúť mu informácie v potrebnom rozsahu.	
(2) 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.		
(3) 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 6.		
(4) 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.[36)]		
(5) Predchádzajúcim účtovným obdobím na účely tohto zákona je účtovné obdobie, za ktoré bola zostavená posledná účtovná závierka.		

[36)] 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.

(6) 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.		
(7) Pokuta za správny delikt je splatná do 30 dní odo dňa nadobudnutia právoplatnosti rozhodnutia o jej uložení.		
(8) Pokuty za správny delikt sú príjmom štátneho rozpočtu.		

§ 32 **Splnomocňovacie ustanovenie**		
(1) Úrad ustanoví všeobecne záväzným právnym predpisom	a) b) c) citácia §20 ods. 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 kontinuitu 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.*	

	Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu. d) *vydáva znalostné štandardy a v spolupráci s Ministerstvom školstva, vedy, výskumu a športu Slovenskej republiky vykonáva a zabezpečuje budovanie bezpečnostného povedomia,* e) *Prevádzkovateľ základnej služby je povinný hlásiť každý závažný kybernetický bezpečnostný incident, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov.* f) *Hlásenie kybernetických bezpečnostných incidentov sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.* *Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základných služieb.* *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 závis-*	

	losti od klasifikácie informácií a kategorizácie sietí a informačných systémov po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale. *Audit kybernetickej bezpečnosti vykonáva orgán posudzovania zhody podľa osobitného predpisu,[37]) ktorý je akreditovaný ako orgán príslušný na posudzovanie zhody v oblasti kybernetickej bezpečnosti.* ● *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.*	
(1) 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 štandardami v oblasti kybernetickej bezpečnosti.		

[37]) Čl. 2 bod 13 nariadenia Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13. 8. 2008).

§ 33 **Spoločné ustanovenia**		
(1) Na konanie úradu podľa § 13 ods. 7, § 16 ods. 2 a 3, § 17 ods. 6, § 21 ods. 4 a § 27 sa nevzťahuje správny poriadok.	§ 13 ods. 7, *Úrad jednotku CSIRT akreditovanú spôsobom podľa tohto zákona zaradí do zoznamu akreditovaných jednotiek CSIRT.* § 16 ods. 2 a 3 (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 tento 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 ods. 6,	

	Zaradenie služby do zoznamu základných služieb a jej prevádzkovateľa do registra prevádzkovateľov základných služieb oznámi úrad prevádzkovateľovi tejto služby prostredníctvom informačného systému kybernetickej bezpečnosti. § 21 ods. 4 *Zaradenie služby do zoznamu digitálnych služieb a jej poskytovateľa do registra poskytovateľov digitálnych služieb oznámi úrad poskytovateľovi tejto služby.* ***§ 27 Riešenie kybernetických bezpečnostných incidentov***	
(1) 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.		
(2) 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.		
(3) Ak základná služba spadá do viacerých sektorov alebo podsektorov podľa prílohy č. 1, pôsobnosť podľa tohto zá-	59. úrad má právo určovať pôsobnosť ústredných orgánov?	

	kona vykonáva ústredný orgán určený úra-dom.		

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.	59. prevádzkovateľ základnej služby	
(1)Osoba existujúca ku dňu účinnosti tohto zákona je povinná do šiestich mesiacov odo dňa účinnosti tohto zákona oznámiť úradu informácie podľa § 21 ods. 1.	59. Poskytovateľ digitálnej služby	
(1)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).		
(2)Úrad do 9. novembra 2018 zapíše 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.		
(3)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.	59. dva roky bude fungovať bez bezpeč-	

	nost- ného projek- tu	
(1)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.		
(2)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.		
(3) Zmluvy uzatvorené na výkon činností podľa § 19 ods. 2 musí prevádzkovateľ základnej služby zosúladiť s týmto zákonom najne-skôr do dvoch rokov od účinnosti tohto zákona.		

§ 35		
Týmto zákonom sa preberajú právne záväzné akty Európskej únie uvedené v prílohe č. 3.	**Príloha č. 3 k zákonu č. .../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)	

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. 444/2015 Z. z. a zákona č. 281/2015 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. .../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 (ďalej len „kybernetická obrana“)[2d]) a kybernetickej bezpečnosti v rozsahu ustanovenom osobitným predpisom,[2e]) 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 pre 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[2f]) a prvkov kritickej infraštruktúry[2g]) súčinnosť a Zinformácie 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 v plnom rozsahu k jednotnému informačnému systému kybernetickej bezpečnosti.[2h])“. Poznámky pod čiarou k odkazom 2d až 2h znejú: „[2d]) § 2 ods. 2 zákona č. 319/2002 Z. z. o obrane Slovenskej republiky v znení zákona č. .../2018 Z. z. [2e]) Zákon č. .../2018 Z. z. [2f]) § 27 ods. 5 zákona č. 319/2002 Z. z. v znení zákona č. 330/2003 Z. z. [2g]) § 2 písm. a) zákona č. 45/2011 Z. z. o kritickej infraštruktúre. [2h]) § 8 zákona č. .../2018 Z. z.“.	59. chyba	

Čl. III		
Zákon Národnej rady Slovenskej republiky č. 145/1995 Z. z. o správnych poplatkoch v znení zákona Národnej rady Slovenskej republiky č. 123/1996 Z. z., zákona Národnej rady Slovenskej republiky č. 224/1996 Z. z., zákona č. 70/1997 Z. z., zákona č. 1/1998 Z. z., zákona č. 232/1999 Z. z., zákona č. 3/2000 Z. z., zákona č. 142/2000 Z. z., zákona č. 211/2000 Z. z., zákona č. 468/2000 Z. z., zákona č. 553/2001 Z. z., zákona č. 96/2002 Z. z., zákona č. 118/2002 Z. z., zákona č. 215/2002 Z. z., zákona č. 237/2002 Z. z., zákona č. 418/2002 Z. z., zákona č. 457/2002 Z. z., zákona č. 465/2002 Z. z., zákona č. 477/2002 Z. z., zákona č. 480/2002 Z. z., zákona č. 190/2003 Z. z., zákona č. 217/2003 Z. z., zákona č. 245/2003 Z. z., zákona č. 450/2003 Z. z., zákona č. 469/2003 Z. z., zákona č. 583/2003 Z. z., zákona č. 5/2004 Z. z., zákona č. 199/2004 Z. z., zákona č. 204/2004 Z. z., zákona č. 347/2004 Z. z., zákona č. 382/2004 Z. z., zákona č. 434/2004 Z. z., zákona č. 533/2004 Z. z., zákona č. 541/2004 Z. z., zákona č. 572/2004 Z. z., zákona č. 578/2004 Z. z., zákona č. 581/2004 Z. z., zákona č. 633/2004 Z. z., zákona č. 653/2004 Z. z., zákona č. 656/2004 Z. z., zákona č. 725/2004 Z. z., zákona č. 5/2005 Z. z., zákona č. 8/2005 Z. z., zákona č. 15/2005 Z. z., zákona č. 93/2005 Z. z., zákona č. 171/2005 Z. z., zákona č. 308/2005 Z. z., zákona č. 331/2005 Z. z., zákona č. 341/2005 Z. z., zákona č. 342/2005 Z. z., zákona č. 468/2005 Z. z, zákona č. 473/2005 Z. z., zákona č. 491/2005 Z. z., zákona č. 538/2005 Z. z., zákona č. 558/2005 Z. z., zákona č. 572/2005 Z. z., zákona č. 573/2005 Z. z., zákona č. 610/2005 Z. z., zákona		

č. 14/2006 Z. z., zákona č. 15/2006 Z. z., zákona č. 24/2006 Z. z., zákona č. 117/2006 Z. z., zákona č. 124/2006 Z. z., zákona č. 126/2006 Z. z., zákona č. 224/2006 Z. z., zákona č. 342/2006 Z. z., zákona č. 672/2006 Z. z., zákona č. 693/2006 Z. z., zákona č. 21/2007 Z. z., zákona č. 43/2007 Z. z., zákona č. 95/2007 Z. z., zákona č. 193/2007 Z. z., zákona č. 220/2007 Z. z., zákona č. 279/2007 Z. z., zákona č. 295/2007 Z. z., zákona č. 309/2007 Z. z., zákona č. 342/2007 Z. z., zákona č. 343/2007 Z. z., zákona č. 344/2007 Z. z., zákona č. 355/2007 Z. z., zákona č. 358/2007 Z. z., zákona č. 359/2007 Z. z., zákona č. 460/2007 Z. z., zákona č. 517/2007 Z. z., zákona č. 537/2007 Z. z., zákona č. 548/2007 Z. z., zákona č. 571/2007 Z. z., zákona č. 577/2007 Z. z., zákona č. 647/2007 Z. z., zákona č. 661/2007 Z. z., zákona č. 92/2008 Z. z., zákona č. 112/2008 Z. z., zákona č. 167/2008 Z. z., zákona č. 214/2008 Z. z., zákona č. 264/2008 Z. z., zákona č. 405/2008 Z. z., zákona č. 408/2008 Z. z., zákona č. 451/2008 Z. z., zákona č. 465/2008 Z. z., zákona č. 495/2008 Z. z., zákona č. 514/2008 Z. z., zákona č. 8/2009 Z. z., zákona č. 45/2009 Z. z., zákona č. 188/2009 Z. z., zákona č. 191/2009 Z. z., zákona č. 274/2009 Z. z., zákona č. 292/2009 Z. z., zákona č. 304/2009 Z. z., zákona č. 305/2009 Z. z., zákona č. 307/2009 Z. z., zákona č. 465/2009 Z. z., zákona č. 478/2009 Z. z., zákona č. 513/2009 Z. z., zákona č. 568/2009 Z. z., zákona č. 570/2009 Z. z., zákona č. 594/2009 Z. z., zákona č. 67/2010 Z. z., zákona č. 92/2010 Z. z., zákona č. 136/2010 Z. z., zákona č. 144/2010 Z. z., zákona č. 514/2010 Z. z., zákona č. 556/2010 Z. z., zákona č. 39/2011 Z. z., zákona č. 119/2011 Z. z., zákona č. 200/2011 Z. z., zákona č. 223/2011 Z. z., zákona č. 254/2011 Z. z., zákona č. 256/2011 Z. z., zákona		

č. 258/2011 Z. z., zákona č. 324/2011 Z. z., zákona č. 342/2011 Z. z., zákona č. 363/2011 Z. z., zákona č. 381/2011 Z. z., zákona č. 392/2011 Z. z., zákona č. 404/2011 Z. z., zákona č. 405/2011 Z. z., zákona č. 409/2011 Z. z., zákona č. 519/2011 Z. z., zákona č. 547/2011 Z. z., zákona č. 49/2012 Z. z., zákona č. 96/2012 Z. z., zákona č. 251/2012 Z. z., zákona č. 286/2012 Z. z., zákona č. 336/2012 Z. z., zákona č. 339/2012 Z. z., zákona č. 351/2012 Z. z., zákona č. 439/2012 Z. z., zákona č. 447/2012 Z. z., zákona č. 459/2012 Z. z., zákona č. 8/2013 Z. z., zákona č. 39/2013 Z. z., zákona č. 40/2013 Z. z., zákona č. 72/2013 Z. z., zákona č. 75/2013 Z. z., zákona č. 94/2013 Z. z., zákona č. 96/2013 Z. z., zákona č. 122/2013 Z. z., zákona č. 144/2013 Z. z., zákona č. 154/2013 Z. z., zákona č. 213/2013 Z. z., zákona č. 311/2013 Z. z., zákona č. 319/2013 Z. z., zákona č.347/2013 Z. z., zákona č. 387/2013 Z. z., zákona č. 388/2013 Z. z., zákona č. 474/2013 Z. z., zákona č. 506/2013 Z. z., zákona č. 35/2014 Z. z., zákona č. 58/2014 Z. z., zákona č. 84/2014 Z. z., zákona č. 152/2014 Z. z., zákona č. 162/2014 Z. z., zákona č. 182/2014 Z. z., zákona č. 204/2014 Z. z., zákona č. 262/2014 Z. z., zákona č. 293/2014 Z. z., zákona č. 335/2014 Z. z., zákona č. 399/2014 Z. z., zákona č. 40/2015 Z. z. zákona č. 79/2015 Z. z., zákona č. 120/2015 Z. z., zákona č. 128/2015 Z. z., zákona č. 129/2015 Z. z., zákona č. 247/2015 Z. z., zákona č. 253/2015 Z. z., zákona č. 259/2015 Z. z., zákona č. 262/2015 Z. z., zákona č. 273/2015 Z. z., zákona č. 387/2015 Z. z., zákona č. 403/2015 Z. z, zákona č. 125/2016 Z. z., zákona č. 272/2016 Z. z, zákona č. 342/2016 Z. z., zákona č. 386/2016 Z. z., zákona č. 51/2017 Z. z., zákona č. 238/2017 Z. z. a zákona č. 242/2017 Z. z. sa dopĺňa takto:		

1. V prílohe Prehľad sadzobníka správnych poplatkov sa na konci pripájajú tieto slová: „XXV. Kybernetická bezpečnosť ..... 276“.		
2. Sadzobník správnych poplatkov sa dopĺňa časťou XXV, ktorá vrátane nadpisu znie: „XXV. ČASŤ Kybernetická bezpečnosť Položka 276 Podanie žiadosti o akreditáciu jednotky CSIRT ..... 1 500 eur“.“.		

Čl. IV		
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 ods. 2 sa 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. V		
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. a zákona č. 2/2017 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...../2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“.		

Čl. VI		
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. .../2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. [1b]) § 27 ods. 10 zákona č. .../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. .../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 pre 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. ... /2018 Z. z.“.		

Čl. VII		

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. 340/2016 Z. z., zákona č. 301/2016 Z. z., zákona č. 51/2017 Z. z. a zákona č. 152/2017 Z. z. sa mení a dopĺňa takto:		
1. § 24 ods. 2 sa dopĺňa písmenom f), ktoré znie: „f) sa navrhovaná osoba na výzvu úradu nedostaví na bezpečnostný na pohovor; na výzvu úradu sa primerane vzťahuje § 27 ods. 4.“.		
2. 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. .../2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.“.		
3. V § 60 sa dopĺňa odsek 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.“.		
4. V § 64 sa vypúšťajú odseky 2 a 3. Doterajší odsek 4 sa označuje ako odsek 2.		
5. V § 64 ods. 2 sa slovo „Žiadateľ“ nahrádza slovami „Podnikateľ podľa odseku 1“.		
6. V § 71 ods. 2 sa na konci sa na konci pripája táto veta: „Vo veciach služobného pomeru riaditeľa úradu podľa osobitného predpisu[29]) koná a rozhoduje predseda vlády Slovenskej republiky.“.		
7. V § 71 sa vypúšťajú odseky 4, 9 a 12.		

Doterajšie odseky 5 až 8, 10 a 11 sa označujú ako odseky 4 až 9.		
8. V § 71 ods. 6 sa za slovom „vlády“ vypúšťa slovo „alebo“.		
9. V § 71a vrátane nadpisu znie: • • **„§ 71a** **Platové pomery a hmotné výhody riaditeľa úradu** (1) Riaditeľ úradu má počas vykonávania funkcie právo na bezplatné a) používanie služobného motorového vozidla s prideleným vodičom alebo bez neho na vykonávanie funkcie alebo v súvislosti s ňou, b) poskytnutie a používanie služobného mobilného telefónu na zabezpečenie dosiahnuteľnosti v čase vykonávania funkcie a mimo neho. (2) Riaditeľovi úradu patrí na pokrytie nevyhnutných výdavkov za služby a iných osobných výdavkov súvisiacich s vykonávaním funkcie paušálna náhrada mesačne v sume určenej osobitným predpisom.[30a])“. Poznámka pod čiarou k odkazu 30a znie: „[30a]) § 150 ods. 5 zákona č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov.“.		

Čl. VIII Zákon č. 45/2011 Z. z. o kritickej infraštruktúre sa mení takto:		
1.	(2) Súčasťou kritickej infraštruktúry je obranná infraštruktúra podľa osobitného predpisu.1) 1) § 26 a 27 zákona č. 319/2002 Z. z. o obrane Slovenskej republiky v znení zákona č. 330/2003 Z. z.	
2.	l) prevádzkovateľom právnická osoba, fyzická osoba	

	– podnikateľ alebo fyzická osoba, ktorá je vlastníkom prvku alebo z iného právneho dôvodu prevádzkuje prvok,	
3.	c) Ministerstvo hospodárstva Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky, Ministerstvo životného prostredia Slovenskej republiky a Ministerstvo zdravotníctva Slovenskej republiky (ďalej len „ústredný orgán“).	
4.	(4) Prevádzkovateľ má nárok na finančný príspevok na plnenie povinností súvisiacich s vykonaním bezpečnostných opatrení na ochranu prvku podľa § 10, a to voči ústrednému orgánu na úseku kritickej infraštruktúry, do sektora ktorého patrí prevádzkovateľ, ak mu to ústredný orgán určí a táto povinnosť mu nevyplýva z iného všeobecne záväzného právneho predpisu. Pravidlá poskytnutia finančného príspevku budú určené osobitným predpisom, ktorý vydá príslušný ústredný orgán.	
5.	(2) Bezpečnostné opatrenia na ochranu prvku sú najmä mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, bezpečnostné prvky informačných systémov, fyzická ochrana, organizačné opatrenia, kontrolné opatrenia a ich vzájomná kombinácia.	
Poznámka pod čiarou k odkazu 4a znie: „[4a]) § 20 zákona č. .../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.

upravený text

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 služieb, poštový platobný styk a obstarávateľská činnosť	Ministerstvo dopravy a výstavby Slovenskej republiky
5.	Priemysel	Farmaceutický priemysel Hutnícky priemysel Chemický priemysel	Ministerstvo hospodárstva Slovenskej republiky
6.	Verejná správa	Informačné systémy verejnej správy	Úrad podpredsedu vlády pre investície a informatizáciu
7.	Voda a atmo-	Meteorologická služba	Ministerstvo životného

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

pôvodný text

SEKTORY V PÔSOBNOSTI ÚSTREDNÝCH ORGÁNOV

	Sektor	Podsektor	Ústredný orgán
1.	Doprava	Cestná doprava Letecká doprava Vodná doprava Železničná doprava	Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky
2.	Elektronické komunikácie	Satelitná komunikácia Siete a služby pevných elektronických komunikácií a mobilných elektronických komunikácií	Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky
3.	Energetika	Baníctvo Elektroenergetika Plynárenstvo Ropa a ropné produkty	Ministerstvo hospodárstva Slovenskej republiky
4.	Informačné komunikačné technológie	Informačné systémy a siete Internet	Ministerstvo financií Slovenskej republiky
5.	Pošta	Poskytovanie poštových služieb, poštový platobný styk a obstarávateľská činnosť	Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky
6.	Priemysel	Farmaceutický priemysel Hutnícky priemysel Chemický priemysel	Ministerstvo hospodárstva Slovenskej republiky

	sféra	Vodné stavby Zabezpečovanie pitnej vody	prostredia Slovenskej republiky
8.	Zdravotníctvo		Ministerstvo zdravotníctva Slovenskej republiky

7.	Voda a atmosféra	Meteorologická služba Vodné stavby Zabezpečovanie pitnej vody	Ministerstvo životného prostredia Slovenskej republiky
8.	Zdravotníctvo		Ministerstvo zdravotníctva Slovenskej republiky

Čl. IX 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. a zákona č. 386/2016 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[46d]) si tieto úrady vymieňajú informácie a podklady dôležité pre 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 46d znie: „[46d]) Zákon č. .../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, za účelom ich zberu, spracovávania a uchovávania v rozsahu potrebnom na identifikáciu kybernetického bezpečnostného incidentu a zabezpečenia kybernetickej bezpečnosti podľa všeobecného predpisu o kybernetickej bezpečnosti.[46d])“.		

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. marca 2018 okrem ustanovenia čl. I § 12 ods. 6, ktoré nadobúda účinnosť 25. mája 2018.		

	Príloha č. 1 k zákonu č. .../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		59. NBS a ostatné banky nie sú prvkami kritickej infraštruktúry sektora bankovníctvo?
			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			
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			60. čo znamená riadenie ciest (cesta je horizontálna stavba, ktorá slúži na premávku vozidiel a možno chodcov)? 61. kontrola ciest označuje kontrolu stavy ciest?
			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			

				62. čo sú inteligentné dopravné systémy? 63. akej infraštruktúry? 64. čo je mobilita? 65. mobilita koho/čoho sa má na mysli: 66. čo sú rozhrania s inými druhmi dopravy? 67. prvkami kritickej infraštruktúry podľa zákona o KI je o.i. 14 informačných systémov v rezorte Ministerstva financií, tieto by mali spadať pod Ministerstvo dopravy?
	Letecká doprava	**letecký dopravcovia** - letecký dopravný podnik s platnou prevádzkovou licenciou alebo jej ekvivalentom		
		riadiace orgány 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 časť 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		68. opakujúca sa chyba, malo by sa to vzťahovať na prvky kritickej infraštruktúry, ktoré patria do daného sektora a nie formulovať všeobecne
		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, 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 uzlu internetu** za účelom prepájania sietí, ktoré sú z technického a organizačného pohľadu oddelené	Národný bezpečnostný úrad		69. môže sa slovenský zákon vzťahovať na prístavy, ktoré sú v inom štáte. (Slovensko nemá more)
			poskytovateľ služieb systému doménových mien na internete			
			subjekt spravujúci alebo prevádzkujúci register internetových domén najvyššej úrovne			
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 komu-	**správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sú prvkom kritickej infraštruktúry** podľa zákona č. 45/2011 Z. z. o kritickej			

		nikácií	infraštruktúre			
5.	Energetika	Baníctvo	**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	Ministerstvo hospodárstva Slovenskej republiky		70. obmedziť sa na informačné systémy v danom sektore
		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, ktoré 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		71. ide o kľúčové technické prvky Internetu, ktoré patria do počítačových sietí, teda pod Ministerstvo dopravy NBÚ doteraz nemalo nič s Internetom a správou domény, obmedziť sa na informačné systémy v danom sektore
		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		obmedziť sa na informačné systémy v danom sektore
			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		72. obmedziť sa na informačné systémy v danom sektore
			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 v znení neskorších predpisov			
			správcovia a prevádzkovatelia sietí a informač-			

			ných systémov, ktoré sú prvkom kritickej infraštruktúry podľa zákona č. 45/2011 Z. z. o kritickej infraštruktúre, alebo sú k nemu priamo pripojené			
9.	Voda a atmosféra	Meteorologická služba	**správcovia s 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 s 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			73. obmedziť sa na informačné systémy v danom sektore
			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	74. obmedziť sa na informačné systémy v danom sektore
	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 v znení neskorších predpisov	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	
	Spravodajské služby	**správcovia a prevádzkovatelia sietí a informačných systémov prevádzkovaných spravodajskou službou**	Slovenská informačná služba	
		správcovia a prevádzkovatelia sietí a informačných systémov prevádzkovaných spravodajskou službou	Vojenské spravodajstvo	
	Utajované skutočnosti	**správcovia a prevádzkovatelia sietí a informačných systémov, ktoré sa týkajú utajovaných skutočností**	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	75. obmedziť sa na informačné systémy v danom sektore
			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		
					76. obmedziť sa na informačné systémy v danom sektore
					77. obmedziť sa na informačné systémy v danom sektore

	78. obmedziť sa na informačné systémy v danom sektore 79. obmedziť sa na informačné systémy v danom sektore 80. obmedziť sa na informačné systémy v danom sektore 81. obmedziť sa na informačné systémy v danom sektore

	82. obmedziť sa na informačné systémy v danom sektore 83. bezpečnosti SR sa týkajú aj systémy, ktoré sú v pôsobnosti iných ústredných orgánov (obrana, zdravotníctvo, doprava,...) 84. obmedziť sa na informačné

	systémy v danom sektore 85. obmedziť sa na informačné systémy v danom sektore

	•

Príloha č. 2 k zákonu č. .../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. .../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)		