1. **Osobitná časť**

K čl. I

**K § 1**

V nadväznosti na smernicu NIS sa upravuje predmet zákona, ktorý zodpovedá požiadavkám transpozície a predstavuje nevyhnutý súbor nástrojov zabezpečenia kybernetickej bezpečnosti. Zákon upravuje práva a povinnosti osôb ako aj právomoc a pôsobnosť orgánov verejnej moci.

**K § 2**

Ustanovenie upravuje pôsobnosť zákona vo vzťahu k smernici NIS a národnej úprave zabezpečenia sietí a informačných systémov.

V odseku 1 sa vymedzuje cieľ zákona, ktorým je najmä stanoviť minimálne požiadavky na štandardné zabezpečenie významných informačných systémov v Slovenskej republike. V členských štátoch je totiž rôzna úroveň pripravenosti na zabezpečenie kybernetickej bezpečnosti, čo vedie k fragmentácii prístupov v Európskej únii. To má za následok rozdielnu úroveň ochrany spotrebiteľov a podnikov a narúša celkovú úroveň bezpečnosti sietí a informačných systémov v rámci Únie. Neexistencia spoločných požiadaviek na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb zase znemožňuje, aby sa na úrovni Únie vytvoril globálny a účinný mechanizmus spolupráce. Minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti v tomto zákone nebránia prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb uplatňovať prísnejšie bezpečnostné opatrenia.

V odseku 2 sa vymedzuje negatívnym spôsobom vecná pôsobnosť. Špecifické obmedzenia pôsobnosti sa vzťahujú na siete a informačné systémy, ktoré spracúvajú utajované skutočnosti. Dôvodom je, že tieto systémy sú regulované osobitným predpisom, ktorým je zákon č. 215/2004  Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Negatívne vymedzenie ďalej definuje, že ak osobitný právny predpis obsahuje ustanovenia na zabezpečenie sietí a informačných systémov, ktoré vychádzajú z rovnakých základov ako požiadavky na zabezpečenie kybernetickej bezpečnosti upravené v tomto zákone, použijú sa na zabezpečenie kybernetickej bezpečnosti osobitné predpisy. Ide napríklad o príslušné ustanovenia zákona č. 492/2009  Z. z. o platobných službách, zákon č. 541/2004  Z. z. o mierovom využívaní jadrovej energie, zákon č. 275/2006  Z. z. o informačných systémoch verejnej správy. Zákon o kybernetickej bezpečnosti sa ďalej nevzťahuje na zákon č. 351/2011  Z. z. o elektronických komunikáciách v znení neskorších predpisov, nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 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 Národnej rady Slovenskej republiky č. 46/1993  Z. z. o Slovenskej informačnej službe v znení neskorších predpisov, zákon Národnej rady Slovenskej republiky č. 198/1994  Z. z. o Vojenskom spravodajstve v znení neskorších predpisov.

Ustanovenia tohto zákona sa z povahy jeho predmetu úpravy nevzťahujú na činnosti Slovenskej informačnej služby a Ministerstva obrany Slovenskej republiky pri aktivitách a ohrozeniach v kybernetickom priestore, ak ohrozujú bezpečnosť štátu (kybernetická obrana).

Smernicou NIS nie sú dotknuté opatrenia prijímané členskými štátmi na zabezpečenie ich základných štátnych funkcií, najmä na zabezpečenie národnej bezpečnosti vrátane opatrení na ochranu informácií, ktorých sprístupnenie členské štáty považujú za odporujúce základným záujmom ich bezpečnosti, a na udržanie verejného poriadku, najmä na účely umožnenia vyšetrovania, odhaľovania a stíhania trestných činov.

**K § 3**

Definujú sa pojmy používané v tomto zákone.

Slovenská republika ešte nemá formálne ustálenú terminológiu v oblasti kybernetickej bezpečnosti a preto návrh na účely zákona tieto pojmy zavádza. Pojem „kybernetický“ sa nevyskytuje v žiadnom všeobecne záväznom právnom predpise a preto úrad pristúpil k  výkladu základných pojmov v súlade so smernicou NIS.

Pod pojmom kybernetická bezpečnosť môžeme rozumieť súhrn prostriedkov, ktorých cieľom je zaistenie ochrany kybernetického priestoru. Tieto prostriedky môžu byť prirodzene rôzneho charakteru, avšak na účely zákona o kybernetickej bezpečnosti je potrebné pojem „kybernetická bezpečnosť“ chápať ako súbor právnych nástrojov zabezpečujúcich ochranu kybernetického priestoru. Hlavným cieľom zákona je teda ochrana a funkčnosť kybernetického priestoru.

Kybernetický priestor je ohraničený používaním elektronických zariadení a elektronického spektra na vytvorenie, uloženie, modifikovanie, výmenu a využívanie dát prostredníctvom vzájomne závislých a prepojených sietí. Kybernetická bezpečnosť tak predstavuje systém, ktorého úlohou je poskytnúť prostrediu spoločensko-ekonomickej štruktúry štátu bezpečný, chránený a v primeranom rozsahu otvorený kybernetický priestor, teda garanciu bezpečnosti v tomto priestore sa nachádzajúcich elektronických, informačných, komunikačných a riadiacich systémov, v týchto systémoch uchovávaných, spracovávaných a prenášaných dát, ako aj týmito systémami poskytovaných služieb.

Regulácia sa vzťahuje na PZS a PDS, ktorí poskytujú svoje služby v určených regulovaných odvetviach hospodárstva, ktoré sú v zákone špecifikované a v záujme zaistenia konzistentného prístupu v celej Európskej únii vychádza vymedzenie PZS a PDS z kritérií určených NIS.

Úrad pri definovaní pojmov používaných na účely tohto zákona primerane vychádzal z pojmológie smernice NIS, podľa ktorej:

* „sieť a informačný systém“ je:
* elektronická komunikačná sieť v zmysle článku 2 písm. a) smernice 2002/21/ES;
* každé zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú na základe programu automatické spracúvanie digitálnych údajov, alebo
* digitálne údaje, ktoré sa ukladajú, spracúvajú, získavajú alebo prenášajú prostredníctvom prvkov uvedených v písmenách a) a b) na účely ich prevádzkovania, používania, ochrany a udržiavania;
* „bezpečnosť sietí a informačných systémov“ je schopnosť sietí a informačných systémov 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;
* „národná stratégia v oblasti bezpečnosti sietí a informačných systémov“ je rámec, v ktorom sa stanovujú strategické ciele a priority v oblasti bezpečnosti sietí a informačných systémov na vnútroštátnej úrovni;
* „prevádzkovateľ základných služieb“ je verejný alebo súkromný subjekt, ktorého typ sa uvádza v prílohe II, spĺňajúci kritériá stanovené v článku 5 ods. 2;
* „digitálna služba“ je služba v zmysle článku 1 ods. 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535 (1), ktorej druh sa uvádza v prílohe III;
* „poskytovateľ digitálnych služieb“ je každá právnická osoba, ktorá poskytuje digitálnu službu;
* „incident“ je každá udalosť, ktorá má skutočne nepriaznivý vplyv na bezpečnosť sietí a informačných systémov;
* „riešenie incidentov“ sú všetky postupy na podporu odhaľovania, analýzy a obmedzenia následkov incidentu a reakcie naň;
* „riziko“ je každá primerane rozpoznateľná okolnosť alebo udalosť, ktorá môže mať nepriaznivý vplyv na bezpečnosť sietí a informačných systémov.

Zákon o kybernetickej bezpečnosti je založený na plnení bezpečnostných požiadaviek a na oznamovaní bezpečnostných incidentov.

Keďže plnenie týchto povinností je vylúčené priamo v smernici NIS pre podniky, ktoré sú kategorizované ako malé a mikro, ani zákon o kybernetickej bezpečnosti tieto podniky nezahŕňa do regulácie, čo je deklarované definíciou jedného z povinných subjektov - poskytovateľa digitálnej služby, ktorým je v súlade s vyššie uvedeným právnická osoba alebo fyzická osoba - podnikateľ, ktorá poskytuje digitálnu službu a zároveň zamestnáva 50 a viac zamestnancov a má ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur.

**K § 4**

Ustanovenie vymedzuje osoby a orgány, ktorým je zákonom o kybernetickej bezpečnosti ukladaná povinnosť. Identifikujú sa orgány verejnej moci, v pôsobnosti ktorých je oblasť zabezpečenia kybernetickej bezpečnosti. Okrem úradu, ako ústredného orgánu štátnej správy pre oblasť kybernetickej bezpečnosti, sú to ústredné orgány explicitne vymenované v zákone (ďalej len „ÚO“) a iné orgány štátnej správy (ďalej len „IO“).

Ustanovenie transponuje v tomto smere smernicu NIS, podľa ktorej každý členský štát určí jeden alebo viaceré vnútroštátne príslušné orgány pre bezpečnosť sietí a informačných systémov (podľa zákona ÚO), ktoré sa zaoberajú prinajmenšom odvetviami uvedenými v prílohe II a službami uvedenými v prílohe III. Členské štáty môžu touto úlohou poveriť existujúci orgán alebo orgány.

ÚO je prirodzený regulátor v oblasti svojej pôsobnosti (napríklad pre sektor „Doprava“ Ministerstvo dopravy a výstavby SR, pre sektor „bankovníctvo“ Ministerstvo financií SR, atď.), ďalej je to aj subjekt, ktorého úlohy v oblasti kybernetickej bezpečnosti vyplývajú priamo z právnych predpisov upravujúcich jeho pôsobnosť napríklad Slovenská informačná služba, Vojenské spravodajstvo. Na druhej strane existujú aj ďalšie subjekty (ako napr. Ministerstvo zahraničných vecí a európskych záležitostí SR) s osobitným postavením na úseku kybernetickej bezpečnosti, ktoré majú povinnosť aplikovať primerané bezpečnostné opatrenia na zabezpečenie sietí a informačných systémov podľa tohto zákona. IO však na rozdiel od ÚO nemajú povinnosť zabezpečiť plnenie jednotky CSIRT vo svojej pôsobnosti.

**K § 5**

V súlade so smernicou NIS každý členský štát určí národné jednotné kontaktné miesto pre bezpečnosť sietí a informačných systémov. Jednotné kontaktné miesto vykonáva styčnú úlohu, aby zabezpečilo cezhraničnú spoluprácu príslušných orgánov v iných členských štátoch so skupinou pre spoluprácu a sieťou jednotiek CSIRT.

Úrad je v zmysle smernice NIS príslušným orgánom pre kybernetickú bezpečnosť a národné jednotné kontaktné miesto, ktoré zabezpečuje cezhraničnú spoluprácu. Úrad ako ústredný orgán štátnej správy v oblasti kybernetickej bezpečnosti riadi a koordinuje výkon štátnej správy.

Odsek 1 teda v nadväznosti na uvedené definuje jednotlivé úlohy úradu aj v spolupráci s Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky pri rozvíjaní medzinárodnej spolupráce alebo Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky pri zabezpečovaní budovania bezpečnostného povedomia.

Odsek 2 následne na vymedzené úlohy umožňuje úradu uzavrieť dohodu o spolupráci s fyzickou osobou na výkon činnosti podľa tohto zákona v záujme zabezpečenia kybernetickej bezpečnosti. Ide o možnosť uzatvoriť dohody o spolupráci pri riešení úloh so všeobecne uznávanými odborníkmi v oblasti bezpečnosti sietí a informačných systémov, ktorých štát z dôvodu limitovaných miezd nedokáže zamestnať, a to napríklad v prípade vzniku významných situácií alebo v rámci predchádzania ich vzniku. Ide o taký druh dohody týkajúci sa práv a povinností z pracovnoprávnych alebo iných pracovných vzťahov, pri ktorých výkone práce je zmluvný pracovník povinný dodržiavať príkazy a plniť úlohy úradu.

**K § 6**

V zmysle smernice NIS si každý členský štát určí jednu alebo viac jednotiek CSIRT, ktoré spĺňajú požiadavky stanovené v bode 1 prílohy I, pokrývajú aspoň odvetvia uvedené v prílohe II a služby uvedené v prílohe III a ktoré zodpovedajú za riešenie rizík a incidentov podľa presne stanoveného postupu. Jednotku CSIRT možno zriadiť v rámci príslušného orgánu.

Podľa odseku 1 v zmysle ustanovenia smernice NIS má úrad na úseku kybernetickej bezpečnosti pôsobnosť ako ústredný orgán štátnej správy, ako ÚO pre oblasť podľa prílohy č. 1 a zabezpečuje úlohy ako národná jednotka CSIRT pre sektory, v ktorých nie je určený žiadny ÚO. Rovnako národná jednotka CSIRT plní úlohy pre digitálne služby podľa prílohy č. 2. Národná jednotka CSIRT musí spĺňať všetky podmienky a úlohy v zmysle smernice NIS, ktoré boli transponované do zákona o kybernetickej bezpečnosti v § 13 až 15.

V zmysle smernice NIS jednotky CSIRT zabezpečujú vysokú úroveň dostupnosti svojich komunikačných služieb, a to tak, že predchádzajú tomu, že zlyhajú ako celok, ak zlyhá ich ľubovoľný jediný bod, a majú k dispozícii niekoľko spôsobov, ktorými ich možno kontaktovať a ktorými môžu oni kedykoľvek kontaktovať iných. Okrem toho sú komunikačné kanály jasne vymedzené a zainteresované strany a spolupracujúci partneri sú o nich dobre informovaní. Pracoviská jednotiek CSIRT a podporné informačné systémy sú umiestnené na zabezpečených miestach. Ďalej jednotky CSIRT majú zavedený vhodný systém riadenia a zasielania žiadostí v záujme ich jednoduchšieho odovzdávania, sú primerane personálne vybavené, aby sa zabezpečila stála dostupnosť ich služieb. Jednotky CSIRT využívajú infraštruktúru, ktorej kontinuita je zabezpečená. Na tento účel sú k dispozícii záložné systémy a záložný pracovný priestor.

Podľa odseku 2 národná jednotka CSIRT zabezpečuje úlohy jednotky CSIRT v pôsobnosti ÚO v prípade, ak ÚO túto úlohu nedokáže zabezpečiť spôsobom podľa tohto zákona, a to teda priamo vo svojej pôsobnosti alebo prostredníctvom inej jednotky CSIRT v pôsobnosti iného ÚO.

Podľa odseku 3 sa na plnení úloh národnej jednotky CSIRT môžu podieľať vyslaní zástupcovia orgánov verejnej moci. Ide najmä o vzájomnú kooperáciu pri riešení kybernetických bezpečnostných incidentov, ale aj výmenu praktických poznatkov.

Odsek 4 uvádza, že ÚO ani PZS sa nemôže zbaviť svojej povinnosti zabezpečiť bezpečnosť sietí a informačných systémov vo svojej pôsobnosti podľa tohto zákona alebo osobitných predpisov v prípade, ak úlohy jednotky CSIRT plní úrad.

**K § 7**

V zmysle smernice NIS každý členský štát prijme národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov, v ktorej sa vymedzia strategické ciele a vhodné politické a regulačné opatrenia na dosiahnutie a udržanie vysokej úrovne bezpečnosti sietí a informačných systémov a ktorá sa vzťahuje aspoň na odvetvia uvedené v prílohe II a služby uvedené v prílohe III. Národná stratégia v oblasti bezpečnosti sietí a informačných systémov sa venuje najmä týmto otázkam:

* ciele a priority národnej stratégie v oblasti bezpečnosti sietí a informačných systémov;
* rámec riadenia na dosiahnutie cieľov a priorít národnej stratégie v oblasti bezpečnosti sietí a informačných systémov vrátane úloh a zodpovedností vládnych orgánov a ďalších relevantných aktérov;
* identifikácia opatrení týkajúcich sa pripravenosti, reakcie a obnovy vrátane spolupráce medzi verejným a súkromným sektorom;
* určenie vzdelávacích programov, programov na zvyšovanie informovanosti a  programov odbornej prípravy súvisiacich s národnou stratégiou v oblasti bezpečnosti sietí a informačných systémov;
* určenie plánov výskumu a vývoja súvisiacich s národnou stratégiou v oblasti bezpečnosti sietí a informačných systémov;
* plán posudzovania rizika na účely identifikácie rizík;
* zoznam rôznych aktérov zapojených do vykonávania národnej stratégie v oblasti bezpečnosti sietí a informačných systémov.

Členské štáty môžu pri vypracúvaní národných stratégií v oblasti bezpečnosti sietí a informačných systémov požiadať o pomoc agentúru ENISA.

Podľa odseku 1 má úrad povinnosť prijať národnú stratégiu v oblasti kybernetickej bezpečnosti, v ktorej sa vymedzia strategické ciele a vhodné politické a regulačné opatrenia na dosiahnutie a udržanie vysokej úrovne kybernetickej bezpečnosti. Súčasťou národnej stratégie kybernetickej bezpečnosti je akčný plán.

Obsah národnej stratégie kybernetickej bezpečnosti je vymedzený v odseku 2 tak, aby korešpondoval s obsahovým vymedzením v smernici NIS.

Podľa odseku 3 národnú stratégiu kybernetickej bezpečnosti vypracováva úrad v spolupráci s ÚO a IO. Tieto subjekty majú povinnosť poskytovať úradu informácie potrebné na vypracovanie národnej stratégie kybernetickej bezpečnosti.

Podľa odseku 4 národnú stratégiu schvaľuje vláda Slovenskej republiky.

**K § 8**

V záujme účinnej podpory výmeny informácií a najlepších postupov má zásadný význam vytvorenie primeraného a bezpečného informačného systému, ktorý je založený na dôvere zúčastnených strán.

Podľa odseku 1 úrad vytvára a spravuje jednotný informačný systém kybernetickej bezpečnosti (ďalej len „JISKB“), ktorý bude dostupný nepretržitým a automatizovaným spôsobom prostredníctvom vlastného webového sídla aj prostredníctvom portálu slovensko.sk a bude slúžiť na efektívne riadenie, koordináciu, evidenciu a kontrolu výkonu štátnej správy v oblasti kybernetickej bezpečnosti a jednotiek CSIRT a na zbieranie, spracovanie a vyhodnocovanie informácií. JISKB má okrem toho poskytovať dôveryhodné informácie nie len v čase mieru v rámci krízového plánovania, ale aj v krízových situáciách.

JISKB poskytuje prioritne tri základné okruhy služieb:

* komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov,
* centrálny systém včasného varovania,
* verejné oznámenia o incidentoch, registre, zoznamy a metodiky.

Na účely identifikácie prevádzkovateľov by členské štáty mali vytvoriť zoznam služieb, ktoré sa považujú za základné. Vedenie zoznamov je v súlade so znením smernice NIS základným predpokladom identifikácie povinných subjektov, pretože pri posudzovaní toho, či subjekt poskytuje služby, ktoré sú pre zachovanie rozhodujúcich spoločenských alebo hospodárskych činností zásadné, stačí preskúmať, či uvedený subjekt poskytuje službu, ktorá je zahrnutá do zoznamu základných služieb. Na základe uvedeného je potom potrebné vytvoriť aj zoznam identifikovaných prevádzkovateľov základných služieb. Podľa smernice NIS potom členské štáty pravidelne a aspoň každé dva roky od 9. mája 2018 preskúmavajú a v prípade potreby aktualizujú zoznam identifikovaných prevádzkovateľov základných služieb. Vedenie týchto zoznamov má konštitutívne účinky vzhľadom na identifikovanie subjektov, ktorým vyplývajú povinnosti z tohto zákona.

Komunikácia s verejnosťou v čase akútneho ohrozenia kybernetickej bezpečnosti je kľúčovou pre zvládnutie situácie a môže predchádzať vzniku nezvratných škodlivých účinkov kybernetického bezpečnostného incidentu.

Rovnako tak smernica NIS uvádza, že informácie o incidentoch majú pre širokú verejnosť a podniky, najmä malé a stredné podniky, čoraz väčšiu hodnotu. V niektorých prípadoch sa tieto informácie už poskytujú prostredníctvom webových sídiel na vnútroštátnej úrovni, v jazyku danej krajiny a so zameraním najmä na incidenty a udalosti, ktoré majú vnútroštátny rozmer. Vzhľadom na to, že podniky čoraz väčšmi vykonávajú cezhraničnú činnosť a občania využívajú online služby, informácie o incidentoch by sa mali poskytovať v súhrnnej podobe aj na úrovni Únie. Jednotky CSIRT, ktoré sú súčasťou siete jednotiek CSIRT, sa nabádajú, aby dobrovoľne poskytovali informácie, ktoré by sa na webovom sídle mali uverejňovať, pričom by to nemalo zahŕňať dôverné ani citlivé informácie.

Úrad teda prostredníctvom JISKB poskytuje verejnosti nevyhnutné informácie vo vzťahu k stavu kybernetickej bezpečnosti, informuje o možných hrozbách a aktivitách národnej jednotky CSIRT, buduje bezpečnostné povedomie, zverejňuje oznamy, metodiky a poskytuje služby informačnej podpory.

Podľa odseku 3 je komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov komunikačný systém, ktorý zaisťuje systematický zber kybernetických bezpečnostných incidentov a ich analýzu. Do komunikačného systému je napojená každá jednotka CSIRT a PZS a prostredníctvom komunikačného systému sa oznamujú v štruktúrovanej podobe kybernetické bezpečnostné incidenty. Rovnakým spôsobom sa oznamujú dobrovoľné hlásenia kybernetických bezpečnostných incidentov. Tento systém napomôže efektívnej komunikácii medzi relevantnými aktérmi pre koordinované riešenie vzniknutého kybernetického bezpečnostného incidentu a to v reálnom čase trvania incidentu.

Podľa odseku 4 centrálny systém včasného varovania zaisťuje včasnú výmenu informácií o kybernetických bezpečnostných incidentoch a rizikách s nimi spojených medzi úradom a vymedzenými subjektmi, ktoré majú prístup k neverejnej časti JISKB.

V zmysle odseku 5 JISKB predstavuje online dostupné miesto, kde sa nachádzajú všetky informácie týkajúce sa kybernetickej bezpečnosti a miesto vzájomnej výmeny informácií medzi úradom a subjektami určenými zákonom. Z tohto dôvodu JISKB pozostáva z verejnej zóny a neverejnej zóny, ktorá bude prioritne slúžiť na zdieľanie citlivých informácií medzi určenými subjektami. Subjekty vymenované v zákone sú z dôvodu svojho osobitného postavenia vo vzťahu k zabezpečovaniu kybernetickej bezpečnosti vymenované v zákone, pričom zákon umožňuje do budúcnosti bez potreby legislatívnej zmeny zaradiť medzi takéto subjekty aj iné orgány verejnej moci na základe odôvodnenej potreby schválenej úradom. Tieto subjekty majú priamy bezplatný a automatizovaný prístup k JISKB v rozsahu určenom úradom, resp. v rozsahu, v akom je prístup k informáciám nevyhnutný na základe legálnej požiadavky konkrétneho právneho predpisu upravujúceho pôsobnosť subjektu vymenovaného v zákone. Osobitné predpisy sú príkladom uvedené v poznámke pod čiarou. Neverejná časť JISKB bude obsahovať napríklad auditné správy, súhrnné informácie a analýzy.

V odseku 6 je vyjadrená všeobecná povinnosť poskytovať úradu informácie v zmysle tohto zákona a to bezodplatne po tom, ako sa o nich povinný subjekt dozvedel.

**K § 9**

Podľa odseku 1 ÚO zodpovedá vo svojej pôsobnosti za vykonávanie a zabezpečovanie úloh súvisiace s kybernetickou bezpečnosťou a to prostredníctvom svojej zriadenej akreditovanej jednotky CSIRT. ÚO vyplývajú okrem tejto úlohy aj ďalšie povinnosti, a to najmä notifikačné a kooperatívne činnosti s úradom a inými ÚO ako aj zahraničnými partnermi.

Podľa odseku 2 zabezpečenie úloh na úseku kybernetickej bezpečnosti prostredníctvom jednotky CSIRT ÚO sa vykonáva jedným z týchto spôsobov:

* zriadením a prevádzkovaním vlastnej jednotky CSIRT, ktorá musí byť akreditovaná v zmysle tohto zákona, vo svojej vlastnej pôsobnosti,
* využitím akreditovanej jednotky CSIRT, ktorú zriaďuje a prevádzkuje iný ÚO, a to na základe zmluvy, okrem vládnej jednotky CSIRT,
* prostredníctvom národnej jednotky CSIRT, ak postup podľa bodu 1 a 2 nie je možný.

**K § 10**

Podľa smernice NIS by sa nemalo členským štátom brániť v tom, aby ukladali bezpečnostné a oznamovacie požiadavky subjektom, ktoré nie sú poskytovateľmi digitálnych služieb patriacimi do rozsahu pôsobnosti tejto smernice, bez toho, aby boli dotknuté povinnosti členských štátov podľa práva Únie.

Ustanovenie upravuje povinnosti vo vzťahu k sieťam a informačným systémom, ktoré nie sú kategorizované ako základná služba. Na tieto siete a informačné systémy je z dôvodu potreby komplexnej úpravy celého systému kybernetickej bezpečnosti aplikovať primerané bezpečnostné opatrenia definované v tomto zákone. Ustanovením sa teda apeluje na dodržiavanie spoločných bezpečnostných požiadaviek na zabezpečenie sietí a informačných systémov. Vytvorenie spoločnej platformy, bezpečnostnej základne, naprieč celým spektrom sietí a informačných systémov umožňuje, aby sa na úrovni nielen Slovenskej republiky ale aj celej Európskej únie vytvoril účinný mechanizmus spolupráce a reakcie na incidenty. Ide teda o prijímanie bezpečnostných opatrení, ktoré ÚO a IO považujú za vhodné na riadenie rizík v oblasti bezpečnosti ich sietí a informačných systémov.

Okrem uvedeného IO vykonávajú úkony súvisiace s informačnými a notifikačnými činnosťami na úseku kybernetickej bezpečnosti, spolupracujú s úradom a budujú bezpečnostné povedomie.

**K § 11**

Z dôvodu zabezpečenia právnej istoty a budovania vzájomnej dôvery sa týmto zákonom zriaďuje vládna jednotka CSIRT. Táto jednotka je určená výlučne pre podsektor informačné systémy verejnej správy a je zriadená v pôsobnosti Úradu vlády Slovenskej republiky, keďže strategickou činnosťou vlády je v plnom rozsahu vybudovať e-government, čo predstavuje komplexnú a efektívnu digitalizáciu administratívnych, správnych, rozhodovacích a riadiacich procesov, ako aj normotvorby v rámci všetkých odvetví a foriem správy. Úrad vlády Slovenskej republiky za účelom plnenia odborných úloh v oblasti informatizácie spoločnosti vyplývajúcich zo zákona č. 275/2006  Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, správy a prevádzkovania elektronických komunikačných sietí a služieb, a aj pre ostatné orgány štátnej správy, právnické osoby a fyzické osoby, ktoré požadujú informácie, údaje z informačných systémov, databáz a registrov verejnej správy zriadil príspevkovú organizáciu Národná agentúra pre sieťové a elektronické služby, ktorá má vzhľadom na svoje zameranie najvhodnejšie spôsobilosti vykonávať úlohy jednotky CSIRT pre uvedený podsektor.

Vládna jednotka CSIRT z dôvodu značného rozsahu poľa pôsobnosti, ako aj v rámci rešpektovania citlivých a dôverných informácií nachádzajúcich sa v týchto informačných systémov nevykonáva úlohy jednotky CSIRT pre iné podsektory.

**K § 12**

Smernica NIS sa nedotýka možnosti každého členského štátu prijať potrebné opatrenia na zaručenie ochrany základných záujmov vlastnej bezpečnosti, chrániť verejný poriadok a verejnú bezpečnosť a umožniť vyšetrovanie a odhaľovanie trestných činov, ako aj stíhanie ich páchateľov. V súlade s článkom 346 Zmluvy o fungovaní Európskej únie nie je žiadny členský štát povinný poskytovať informácie, ktorých sprístupnenie podľa neho odporuje základným záujmom jeho bezpečnosti.

Pri uverejňovaní incidentov oznámených príslušným orgánom by sa mala náležitým spôsobom udržiavať rovnováha medzi záujmom verejnosti disponovať informáciami o hrozbách a možným poškodením dobrej povesti a obchodných záujmov PZS a PDS, ktorí incidenty oznámia.

V odseku 1 sa upravuje individuálna povinnosť mlčanlivosti pre každého, kto vykonáva úlohy podľa tohto zákona v rámci rôznych druhov pracovnoprávnych vzťahov a zmlúv. Ide najmä o osoby tvoriace personálne vybavenie jednotiek CSIRT, vyčlenených zamestnancov PZS a PDS na úseku zabezpečenia činnosti súvisiacich s plnením povinností podľa tohto zákona a pod. Tak, ako je tvorená konštrukcia povinnosti zachovávať mlčanlivosť v iných právnych predpisoch, aj návrh zákona predpokladá zachovávanie tejto mlčanlivosti aj po skončení pracovnoprávneho alebo obdobného pracovného vzťahu vrátane služobného pomeru. Ochrana tajomstva alebo povinnosti zachovávať mlčanlivosť podľa iných predpisov zostáva zachovaná.

V odseku 2 sa upravuje možnosť a spôsob zbavenia povinnosti zachovávať mlčanlivosť podľa tohto zákona a v odseku 3 sa ustanovuje konkrétna výnimka z povinnosti mlčanlivosti na účely konania pred orgánom verejnej moci, oznamovania trestného činu alebo inej protispoločenskej činnosti pre zamestnancov PZS a PDS. Tieto subjekty sa ako prvé, pri riešení kybernetického bezpečnostného incidentu, dostanú k informácii, ktorej obsah môže nasvedčovať, že ide o protiprávne konanie. Z tohto dôvodu zákon o kybernetickej bezpečnosti netvorí prekážku pri oznamovaní kriminálnej činnosti alebo pri spolupráci napríklad s orgánom činným v trestnom konaní. Aj smernica NIS uvádza, že incidenty môžu byť výsledkom trestnej činnosti, ktorej prevenciu, vyšetrovanie a stíhanie podporuje koordinácia a spolupráca medzi PZS, PDS, príslušnými orgánmi a orgánmi presadzovania práva. Ak existuje podozrenie, že incident súvisí so závažnou trestnou činnosťou podľa práva Únie alebo vnútroštátneho práva, členské štáty by mali nabádať PZS a PDS, aby príslušným orgánom presadzovania práva oznamovali podozrenie o ich súvise incidentu so závažnou trestnou činnosťou.

Odsek 4 tvorí ďalšiu výnimku z povinnosti zachovávať mlčanlivosť a tajomstvo konštruovanú nie v závislosti od plnenia úloh podľa osobitných predpisov, ale pri úloh na úseku kybernetickej bezpečnosti. Ide najmä o oznamovanie kybernetických bezpečnostných incidentov a o úkony súvisiace so zabezpečovaním kybernetickej bezpečnosti v rozsahu a spôsobom podľa tohto zákona. Oznámenie kybernetického bezpečnostného incidentu a zabezpečovanie kybernetickej bezpečnosti spôsobom podľa tohto zákona teda nemôže byť nikomu na ujmu.

Odsek 5 upravuje zodpovednosť štátu za škodu, ktorá vznikla oznamovateľom kybernetického bezpečnostného incidentu v súvislosti s plnením si oznamovacej povinnosti alebo oprávnenia.

Podľa smernice NIS zdieľanie informácií o rizikách a incidentoch v rámci skupiny pre spoluprácu a siete jednotiek CSIRT a dodržiavanie požiadaviek oznamovať incidenty vnútroštátnym príslušným orgánom alebo jednotkám CSIRT, by si mohlo vyžadovať spracúvanie osobných údajov. V dôsledku incidentov je v mnohých prípadoch porušená ochrana osobných údajov. V tejto súvislosti by príslušné orgány a orgány na ochranu údajov mali navzájom spolupracovať a vymieňať si informácie o všetkých súvisiacich otázkach s cieľom riešiť akékoľvek prípady porušenia ochrany osobných údajov v dôsledku incidentov.

Odsek 6 a 7 upravuje ochranu osobných údajov v zmysle smernice NIS a 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) (ďalej len „GDPR“). V zmysle GDPR každé spracúvanie osobných údajov by malo byť zákonné a spravodlivé. Pre fyzické osoby by malo byť transparentné, že sa získavajú, používajú, konzultujú alebo inak spracúvajú osobné údaje, ktoré sa ich týkajú, ako aj to, v akom rozsahu sa tieto osobné údaje spracúvajú alebo budú spracúvať. Zásada transparentnosti si vyžaduje, aby všetky informácie a komunikácia súvisiace so spracúvaním týchto osobných údajov boli ľahko prístupné a ľahko pochopiteľné a formulované jasne a jednoducho. Uvedená zásada sa týka najmä informácií pre dotknuté osoby o identite prevádzkovateľa a účeloch spracúvania, a ďalších informácií na zabezpečenie spravodlivého a transparentného spracúvania, pokiaľ ide o dotknuté fyzické osoby a ich právo získať potvrdenie a oznámenie spracúvaných osobných údajov, ktoré sa ich týkajú. Fyzické osoby by mali byť upozornené na riziká, pravidlá, záruky a práva pri spracúvaní osobných údajov, ako aj na to, ako uplatňovať svoje práva pri takomto spracúvaní. Najmä konkrétne účely, na ktoré sa osobné údaje spracúvajú, by mali byť výslovne uvedené a legitímne a stanovené v čase získavania osobných údajov. Osobné údaje by mali byť primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú. To si vyžaduje najmä zabezpečenie toho, aby obdobie, počas ktorého sa tieto osobné údaje uchovávajú, bolo obmedzené na nevyhnutný rozsah. Osobné údaje by sa mali spracúvať len vtedy, ak účel spracúvania nebolo možné za primeraných podmienok dosiahnuť inými prostriedkami. S cieľom zabezpečiť, aby sa osobné údaje neuchovávali dlhšie, než je to nevyhnutné, by mal prevádzkovateľ stanoviť lehoty na vymazanie alebo pravidelné preskúmanie. Mali by sa prijať všetky primerané opatrenia, aby sa zabezpečila oprava alebo vymazanie nesprávnych údajov. Osobné údaje by sa mali spracúvať tak, aby sa zabezpečila primeraná bezpečnosť a dôvernosť osobných údajov vrátane predchádzania neoprávnenému prístupu k osobným údajom a zariadeniu používanému na spracúvanie, alebo neoprávnenému využitiu týchto údajov a zariadení.

Právom Únie alebo právom členského štátu sa môžu uložiť obmedzenia týkajúce sa osobitných zásad a práv na informovanie, prístup a opravu alebo vymazanie osobných údajov, práva na prenosnosť údajov, práva namietať, rozhodnutí založených na profilovaní, ako aj informovania dotknutej osoby o porušení ochrany osobných údajov a o určitých súvisiacich povinnostiach prevádzkovateľov, pokiaľ je to v demokratickej spoločnosti potrebné a primerané na zaistenie verejnej bezpečnosti vrátane ochrany ľudského života, najmä v reakcii na prírodné katastrofy alebo katastrofy spôsobené ľudskou činnosťou, predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií, vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu, alebo vyšetrovania porušovaniu etiky v regulovaných profesiách, ich vyšetrovania a stíhania, alebo iných dôležitých cieľov všeobecného verejného záujmu Únie alebo členského štátu, najmä ak ide o dôležitý hospodársky alebo finančný záujem Únie alebo členského štátu, vedenia verejných registrov vedených vo všeobecnom verejnom záujme, ďalšieho spracúvania archivovaných osobných údajov na účely poskytnutia konkrétnych informácií o politickom správaní počas bývalého totalitného štátneho režimu, alebo ochrany dotknutej osoby alebo práv a slobôd iných vrátane sociálnej ochrany, verejného zdravia a humanitárnych účelov. Uvedené obmedzenia by mali byť v súlade s požiadavkami stanovenými v Charte a v Európskom dohovore o ochrane ľudských práv a základných slobôd.

Podľa čl. 23 nariadenia GDPR v práve Únie alebo práve členského štátu, ktorému prevádzkovateľ alebo sprostredkovateľ podliehajú, sa prostredníctvom legislatívneho opatrenia môže obmedziť rozsah povinností a práv ustanovených v článkoch 12 až 22 a v článku 34, ako aj v článku 5, pokiaľ jeho ustanovenia zodpovedajú právam a povinnostiam ustanoveným v článkoch 12 až 22, ak takéto obmedzenie rešpektuje podstatu základných práv a slobôd a je nevyhnutným a primeraným opatrením v demokratickej spoločnosti s cieľom zaistiť národnú bezpečnosť, obranu, verejnú bezpečnosť a ďalšie.

Ochrana osobných údajov je v teda v zákone zabezpečená jednak špeciálnou úpravou, a to najmä s prihliadnutím na špecifickú oblasť bezpečnosti, kedy úrad spracováva osobné údaje v JISKB a zabezpečí ich ochranu pred akýmkoľvek zneužitím a vyzradením a zároveň je ochrana osobných údajov zabezpečená v zmysle čl. 2 smernice NIS, podľa ktorej spracúvanie osobných údajov podľa tejto smernice sa vykonáva v súlade so smernicou 95/46/ES a v nadväznosti na to sa práva a povinnosti PZS a PDS súvisiace s ochranou osobných údajov, ktoré nie sú upravené v tomto zákone, spravujú ustanoveniami všeobecného predpisu o ochrane osobných údajov.

Podľa odseku 8 sa limituje zaobchádzanie s osobnými údajmi a informáciami získanými v súvislosti s plnením činností na zabezpečenie kybernetickej bezpečnosti len na plnenie úloh podľa tohto zákona.

**K § 13**

Podľa smernice NIS každý členský štát určí jednu alebo viac jednotiek CSIRT, ktoré spĺňajú požiadavky stanovené v bode 1 prílohy I, pokrývajú aspoň odvetvia uvedené v prílohe II a služby uvedené v prílohe III a ktoré zodpovedajú za riešenie rizík a incidentov podľa presne stanoveného postupu. Jednotku CSIRT možno zriadiť v rámci príslušného orgánu.

Na účely zabezpečenia kybernetickej bezpečnosti a účinného reagovania na kybernetické bezpečnostné incidenty je nevyhnutné zabezpečiť, aby v štáte existovali dobre fungujúce jednotky CSIRT, ktoré budú dodržiavať základné požiadavky s cieľom zaručiť účinné a zlučiteľné spôsobilosti na riešenie incidentov a rizík a zabezpečiť účinnú spoluprácu na úrovni Európskej únie.

Predkladaný návrh zákona teda prichádza s legálnou definíciou jednotky CSIRT a to hlavne vymedzením požiadaviek, ktoré sú na ňu kladené. Nie je podstatné, či funguje ako samostatný útvar alebo ako organizačná zložka jej prevádzkovateľa, dôležité je, že spĺňa kritériá nevyhnutné pre plnenie jej funkcie. Overovateľom splnenia týchto požiadaviek bude úrad, ktorý splnenie požiadaviek preverí v rámci akreditácie. Po splnení požiadaviek úrad jednotku CSIRT zaradí na zoznam jednotiek CSIRT, čím jej status legálne deklaruje. Vďaka tomuto statusu získa jednotka CSIRT prístup k informáciám z JISKB a môže zdieľať informácie so všetkými zainteresovanými subjektami na úseku kybernetickej bezpečnosti. Okrem toho týmto statusom získa možnosť zúčastňovať sa stretnutí európskej siete jednotiek CSIRT.

Uvedeným postupom sa zabezpečí plnenie úloh podľa tohto zákona pre všetky kľúčové sektory a služby jednotkami CSIRT, ktoré sú schopné tieto úlohy plniť na požadovanej kvalitatívnej úrovni.

V súčasnosti v Slovenskej republike pôsobí viacero jednotiek CSIRT, ktoré majú potenciál splniť požiadavky zákona kladené na jednotku CSIRT. Vzhľadom na neexistenciu ich zákonného statusu však nie je možné ich fungovanie akokoľvek regulovať, koordinovať, či vyžadovať ich spoluprácu v záujmu dosiahnutia spoločného cieľa – kybernetickej bezpečnosti Slovenskej republiky. Predkladaným návrhom zákona sa toto právne vákuum odstraňuje.

Odsek 1 až 3 upravuje podanie žiadosti osoby, ktorá má plniť úlohy jednotky CSIRT a lehotu na začatie a ukončenie konania.

Podľa odseku 4 úrad vydá rozhodnutie s platnosťou najviac päť rokov, avšak podľa odseku 5, ak sú splnené podmienky akreditácie jednotky CSIRT, môže úrad toto rozhodnutie predĺžiť opäť na dobu maximálne 5 rokov.

Odsek 6 upravuje inštitút uznania akreditácie jednotky CSIRT, ktorá získala medzinárodnú akreditáciu. V tejto súvislosti nie je prirodzene možné, aby táto jednotka CSIRT mohla príslušnou dokumentáciu preukázať splnenie tých podmienok, ktoré sú určené všeobecne záväzným právnym predpisom, ktorý vydá úrad a konkretizuje technické, technologické a personálne vybavenie jednotky CSIRT. Tieto podmienky jednotka CSIRT akreditovaná v zmysle medzinárodnej organizácie spĺňa podľa odlišnej technickej normy kybernetickej bezpečnosti.

Podľa odseku 7 akreditovanú jednotku CSIRT úrad zaradí do zoznamu jednotiek CSIRT. Do zoznamu akreditovaných jednotiek CSIRT sa automaticky zapisuje národná jednotka CSIRT a vládna jednotka CSIRT, ktoré sú akreditované zo zákona. Navrhovaná úprava tak počíta so vzájomnou spoluprácou vládnej jednotky CSIRT, národnej jednotky CSIRT a ostatných akreditovaných jednotiek CSIRT prostredníctvom JISKB a to najmä formou výmeny informácií o riešených kybernetických bezpečnostných incidentoch.

**K § 14**

Ustanovenie upravuje podmienky akreditácie jednotky CSIRT.

Základné požiadavky na jednotky CSIRT v zmysle smernice NIS:

* Jednotky CSIRT zabezpečujú vysokú úroveň dostupnosti svojich komunikačných služieb, a to tak, že predchádzajú tomu, že zlyhajú ako celok, ak zlyhá ich ľubovoľný jediný bod, a majú k dispozícii niekoľko spôsobov, ktorými ich možno kontaktovať a ktorými môžu oni kedykoľvek kontaktovať iných. Okrem toho sú komunikačné kanály jasne vymedzené a zainteresované strany a spolupracujúci partneri sú o nich dobre informovaní.
* Pracoviská jednotiek CSIRT a podporné informačné systémy sú umiestnené na zabezpečených miestach.
* Jednotky CSIRT majú zavedený vhodný systém riadenia a zasielania žiadostí v záujme jednoduchšieho odovzdávania.
* Jednotky CSIRT sú primerane personálne vybavené, aby sa zabezpečila stála dostupnosť ich služieb.
* Jednotky CSIRT využívajú infraštruktúru, ktorej kontinuita je zabezpečená. Na tento účel sú k dispozícii záložné systémy a záložný pracovný priestor.
* Jednotky CSIRT musia mať možnosť zapojiť sa do sietí medzinárodnej spolupráce, pokiaľ majú v úmysle byť ich súčasťou.

V ustanovení sa teda konkrétne uvádzajú podmienky akreditácie jednotky CSIRT, čím dochádza k vytvoreniu hodnoverných rovnakých podmienok pre všetky jednotky CSIRT, čo je kľúčové pre účinné fungovanie jednotiek CSIRT.

Úrad vydá všeobecne záväzný právny predpis, ktorým určí konkrétne požiadavky na technické, technologické a personálne vybavenie jednotky CSIRT.

Zabezpečenie dostupnosti, dôvernosti, autenticity a integrity informácií a údajov je možné dosiahnuť napríklad splnení požiadaviek stanovených v § 2 vyhlášky Národného bezpečnostného úradu č. 339/2004  Z. z. o bezpečnosti technických prostriedkov alebo v STN ISO/IEC 27002.

Zabezpečenie priestoru v zmysle požiadaviek kladených na jednotku CSIRT je zasa možné dosiahnuť napríklad spôsobom uvedeným v § 5 vyhlášky Národného bezpečnostného úradu č. 336/2004  Z. z. o fyzickej bezpečnosti a objektovej bezpečnosti v znení vyhlášky č. 315/2006  Z. z. alebo v ISO/IEC 27002.

**K § 15**

Podľa smernice NIS členské štáty by mali mať primerané vybavenie, pokiaľ ide o technické a organizačné spôsobilosti, aby mohli predchádzať incidentom a rizikám v oblasti sietí a informačných systémov, odhaľovať ich, reagovať na ne a zmierňovať ich. Členské štáty by preto mali zabezpečiť, aby mali dobre fungujúce jednotky CSIRT, ktoré budú dodržiavať základné požiadavky s cieľom zaručiť účinné a zlučiteľné spôsobilosti na riešenie incidentov a rizík a zabezpečiť účinnú spoluprácu na úrovni Únie. Aby mohli mať z takýchto spôsobilostí a spolupráce úžitok všetky typy prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb, členské štáty by mali zabezpečiť, aby určená jednotka CSIRT pokrývala všetky tieto typy.

Podľa smernice NIS úlohy jednotiek CSIRT zahŕňajú prinajmenšom:

* monitorovanie incidentov na vnútroštátnej úrovni;
* vydávanie včasného varovania, upozornení, oznamovanie a šírenie informácií o rizikách a incidentoch príslušným zainteresovaným stranám;
* reagovanie na incidenty;
* zabezpečovanie dynamickej analýzy rizík a incidentov a získavanie informácií o situácii;
* účasť na činnosti siete jednotiek CSIRT.

Pod pojmom CSIRT rozumieme tím expertov, ktorý odhaľuje bezpečnostné incidenty, koordinuje a kooperuje pri ich riešení, a pôsobí preventívne proti vzniku ďalších hrozieb. CSIRT je expertný orgán, ktorý poskytuje svoje služby určitej zložke alebo skupine zložiek, na ktorých ochranu je zameraný. Pod zložkou sa v tomto prípade rozumie klient, resp. skupina klientov, pre ktorého je určená služba, ktorú poskytuje CSIRT a ktorý vytvára svoje služby na základe požiadaviek jednotlivých zložiek. Zložka je bazálnou časťou kybernetického prostredia, v ktorom CSIRT pôsobí a na základe vytvorených vzťahov medzi zložkami sa určuje úloha CSIRT v tomto systéme. Vo všeobecnosti platí, že CSIRT pre zložky plní úlohu monitorovacieho orgánu a pri vzniku incidentu koordinuje činnosť jednotlivých zložiek a navrhuje riešenia pre elimináciu kybernetických incidentov, pričom však samotné kroky na odstránenie rizika (samotné riešenie kybernetického incidentu) vykonáva sám klient, teda zložka kybernetického prostredia, v ktorom CSIRT pôsobí. Následne môže CSIRT vydať záväzné či odporúčacie stanovisko pre zabránenie opakovaného vzniku kybernetického incidentu, resp. pôsobiť preventívne. Nemožno však generalizovať činnosť CSIRT ako výsostne monitorovaciu či sledovaciu, keďže v korelácii s veľkosťou a zložitosťou prostredia, v ktorom pôsobí, môže vykonávať aj úlohy, súvisiace s priamym riešením kybernetických incidentov, s forenznou analýzou, výskumom a vývojom bezpečnostných technológií a pod.

Odsek 1 až 3 teda definuje služby, ktoré jednotka CSIRT plní. Uvedené úlohy-služby sú v rámci zákona kategorizované do dvoch hlavných okruhov služieb, a to preventívne služby a reaktívne služby. Preventívne služby poskytované jednotnou CSIRT sa zameriavajú na prevenciu, predchádzanie vzniku kybernetickým bezpečnostným incidentom. Reaktívne služby priamo reagujú na vzniknutú alebo na hroziacu bezpečnostnú situáciu.

Odsek 4 uvádza, že reaktívne služby sú vykonávane v kooperácii s PZS alebo PDS.

**K § 16**

Ustanovenie odseku 1 upravuje povinnosti toho, kto prevádzkuje jednotku CSIRT. Tento musí zabezpečiť, aby jeho akreditovaná jednotka CSIRT spĺňala podmienky akreditácie podľa tohto zákona nepretržite počas celej doby svojej prevádzky a plnila úlohy, ktoré sú v zákone vymedzené. V opačnom prípade úrad jednotku CSIRT vyradí zo zoznamu akreditovaných jednotiek CSIRT, a to buď na základe oznamovacej povinnosti toho, kto jednotku CSIRT prevádzkuje, alebo v zmysle odseku 3 aj na základe vlastného zistenia, keď nedôjde k náprave nedostatkov v lehote určenej úradom.

Podľa odseku 4 sa na vyradenie zo zoznamu akreditovaných jednotiek CSIRT nevzťahuje všeobecný predpis o správnom konaní s cieľom predísť prieťahom a akýmkoľvek nepokrytým priepastiam v nastavenom bezpečnostnom systéme.

**K § 17**

V zmysle smernice NIS by členské štáty mali byť zodpovedné za určenie subjektov, ktoré spĺňajú kritériá vymedzenia pojmu „prevádzkovateľ základných služieb“. V záujme zaistenia konzistentného prístupu by sa vymedzenie pojmu „prevádzkovateľ základných služieb“ malo jednotne uplatňovať vo všetkých členských štátoch. Na tento účel sa v smernici stanovuje posúdenie subjektov pôsobiacich v konkrétnych odvetviach a pododvetviach, vytvorenie zoznamu základných služieb, zohľadnenie spoločného zoznamu medziodvetvových faktorov na určenie toho, či by potenciálny incident mal závažný rušivý vplyv, konzultačný proces medzi príslušnými členskými štátmi v prípade subjektov poskytujúcich služby vo viac ako jednom členskom štáte a podporu skupiny pre spoluprácu pri procese identifikácie. S cieľom zabezpečiť, aby boli prípadné zmeny na trhu presne zaznamenané, by členské štáty mali pravidelne kontrolovať a v prípade potreby aktualizovať zoznam identifikovaných prevádzkovateľov. Napokon by členské štáty mali Komisii predložiť informácie potrebné na posúdenie miery, do akej táto spoločná metodika umožnila konzistentné uplatňovanie vymedzenia pojmu zo strany členských štátov.

V rámci procesu identifikácie prevádzkovateľov základných služieb by členské štáty mali posudzovať, aspoň pre každé pododvetvie uvedené v tejto smernici, ktoré služby sa musia považovať za základné pre zachovanie rozhodujúcich spoločenských a hospodárskych činností a či subjekty, ktoré sú uvedené v odvetviach a pododvetviach uvedených v tejto smernici a ktoré poskytujú tieto služby, spĺňajú kritériá na identifikáciu prevádzkovateľov. Pri posudzovaní toho, či subjekt poskytuje služby, ktoré sú pre zachovanie rozhodujúcich spoločenských alebo hospodárskych činností zásadné, stačí preskúmať, či uvedený subjekt poskytuje službu, ktorá je zahrnutá do zoznamu základných služieb. Okrem toho by sa malo preukázať, že poskytovanie základnej služby závisí od sietí a informačných systémov. Napokon by členské štáty pri posudzovaní toho, či by incident mal závažný rušivý vplyv na poskytovanie služby, mali zohľadniť viacero medziodvetvových faktorov a podľa potreby aj faktory špecifické pre určité odvetvie.

Je pravdepodobné, že subjekty pôsobiace v odvetviach a pododvetviach uvedených v tejto smernici poskytujú základné aj druhotné služby. Napríklad v odvetví leteckej dopravy letiská poskytujú služby, ktoré by členské štáty mohli považovať za základné, ako napríklad riadenie vzletových a pristávacích dráh, ale aj viaceré služby, ktoré by bolo možné považovať za druhotné, ako napríklad poskytovanie nákupných zón. Prevádzkovatelia základných služieb by mali podliehať osobitným bezpečnostným požiadavkám iba vo vzťahu k tým službám, ktoré sa považujú za základné. Na účely identifikácie prevádzkovateľov by preto členské štáty mali vytvoriť zoznam služieb, ktoré sa považujú za základné.

Zoznam služieb by mal obsahovať všetky služby poskytované na území daného členského štátu, ktoré spĺňajú požiadavky tejto smernice. Členské štáty by mali mať možnosť doplniť existujúci zoznam zahrnutím nových služieb. Zoznam služieb by mal pre členské štáty slúžiť ako referenčný bod umožňujúci identifikáciu prevádzkovateľov základných služieb. Jeho účelom je určiť typy základných služieb v ktoromkoľvek danom odvetví uvedenom v tejto smernici, čím sa odlíšia od druhotných činnosti, za ktoré by subjekt pôsobiaci v ktoromkoľvek z daných odvetví mohol byť zodpovedný. Zoznam služieb, ktorý zavedie každý členský štát, by slúžil ako ďalší vstup pri posudzovaní regulačnej praxe každého členského štátu s cieľom zabezpečiť celkovú jednotnosť procesu identifikácie medzi členskými štátmi.

Ustanovenie na základe aj vyššie uvedeného určuje spôsob definície základnej služby a PZS.

Odsek 1 až 4 definuje, aká služba je v zmysle zákona o kybernetickej bezpečnosti základnou službou a ako úrad zaradí túto službu do záväzného zoznamu základných služieb.

Zákon identifikuje tri druhy základnej služby:

1. Základná služba v zmysle transpozície smernice NIS - služba, ktorá je uvedená v prílohe č. 1 zákona a ktorá spĺňa identifikačné kritériá podľa tohto zákona.
2. Základná služba ako informačný systém verejnej správy – identifikuje sa na základe dohody s ÚO, do pôsobnosti ktorého sektor informačných systémov verejnej správy spadá (Úrad podpredsedu vlády SR pre investície a informatizáciu).
3. Základná služba ako prvok kritickej infraštruktúry.

Úrad zaradí službu do zoznamu základných služieb a jej prevádzkovateľa do zoznamu PZS.

Odsek 5 upravuje obsahové náležitosti oznámenia prevádzkovateľa služby, ktorá má byť zaradená do zoznamu základných služieb.

Podľa odseku 6 úrad oznámi PZS, že jeho služba bola zaradená do zoznamu základných služieb prostredníctvom JISKB. Uvedené v praxi znamená, že PZS a základná služba budú uvedení v príslušnom zozname a oznámenie o tom bude zaslané aj v zmysle zákona o eGovernmente (elektronicky, dátovou schránkou). Zaradenie do zoznamu/registra má pre PZS konštitutívne účinky, keďže okrem iného do šiestich mesiacov od doručenia tohto oznámenia musí PZS prijať a plniť bezpečnostné opatrenia na úseku kybernetickej bezpečnosti. Uvedený postup je aplikovaný aj pre PDS.

**K § 18**

V nadväznosti na predchádzajúce ustanovenie uvedené bližšie špecifikuje identifikačné kritériá poskytovanej služby.

Podľa odseku 2 a 3 sa tieto kritériá členia na dopadové a špecifické sektorové. Ich určenie bude upravené vo všeobecne záväznom predpise, ktorý vydá úrad.

Podľa odseku 4 má prevádzkovateľ služby povinnosť oznámiť úradu prekročenie špecifických kritérií, ktoré sú príznačné a svojské pre jednotlivé odvetvia aj v prípade, ak neprekročil určené dopadové kritériá. Prevádzkovateľ služby má teda povinnosť vždy skúmať všetky kritériá svojej poskytovanej služby.

**K § 19**

Podľa odseku 1 je PZS povinný do šiestich mesiacov od oznámenia o zaradení do zoznamu PZS prijať a dodržiavať bezpečnostné opatrenia v spravovaných a prevádzkovaných sieťach a informačných systémoch a viesť o tom príslušnú dokumentáciu. Účelom zavedenia bezpečnostných opatrení je zaistenie určitej miery úrovne bezpečnosti sietí a informačných systémov. Ide o zavedenie štandardov, ktoré majú najmä preventívny význam, keďže sieť a informačný systém, v ktorom majú byť tieto bezpečnostné opatrenia aplikované, by mali vykazovať určitú mieru odolnosti systému voči kybernetickým bezpečnostným incidentom a súčasne by mal byť systém schopný efektívne riešiť kybernetický bezpečnostný incident.

Odsek 2 až 4 upravuje povinnosť pre PZS od dodávateľa služieb požadovať dodatočné bezpečnostné opatrenia v súlade s požiadavkami tohto zákona. Mali by mať možnosť urobiť tak prostredníctvom zmluvných záväzkov, dohôd o zabezpečení plnenia povinností podľa tohto zákona. Ustanovujú sa náležitosti takejto dohody aj pre podniky na poskytovanie elektronických komunikačných služieb alebo sietí pre PZS. PZS, ak tomu nebránia dôvody zmarenia riešenia kybernetického bezpečnostného incidentu, informuje dodávateľa o hlásenom kybernetickom bezpečnostnom incidente. Informovanie sa realizuje takým spôsobom, aby nedošlo k porušeniu povinnosti mlčanlivosti alebo k vyzradeniu tajomstva.

Podľa odseku 5 sa určuje postup pri medzištátnom presahu základnej služby.

Odsek 6 následne definuje ďalšie povinnosti PZS na zaistenie kybernetickej bezpečnosti, ktorými je najmä hlásenie a riešenie kybernetického bezpečnostného incidentu.

Odsek 7 ukladá PZS povinnosť informovať úrad o zmenách v identifikačných údajoch a o základnej službe a odsek 9 formuluje zodpovednosť štátu za škodu, ktorá vznikne kybernetickým bezpečnostným incidentom obmedzením základnej služby pri plnení povinností PZS podľa § 27 zákona.

**K § 20**

V zmysle smernice NIS zodpovednosť za zaistenie bezpečnosti sietí a informačných systémov nesú vo veľkej miere PZS. Kultúra riadenia rizika vrátane hodnotenia rizika a vykonávania bezpečnostných opatrení, ktoré sú primerané existujúcim rizikám, by sa mala podporovať a rozvíjať prostredníctvom vhodných regulačných požiadaviek a dobrovoľných postupov v danom odvetví.

Je teda nutné zabezpečiť, aby PZS prijali technické a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré využívajú vo svojej prevádzke. S ohľadom na najnovší technický vývoj tieto opatrenia zabezpečujú takú úroveň kybernetickej bezpečnosti, ktorá zodpovedá miere daného rizika. PZS musia prijať opatrenia na zabránenie a minimalizovanie vplyvu incidentov, ktoré ovplyvňujú bezpečnosť sietí a informačných systémov používaných na poskytovanie týchto základných služieb, s cieľom zabezpečiť ich kontinuitu.

Podľa smernice NIS existujúce spôsobilosti nie sú na zaručenie vysokej úrovne bezpečnosti sietí a informačných systémov v Únii postačujúce. V členských štátoch je rôzna úroveň pripravenosti, čo vedie k fragmentácii prístupov v Únii. To má za následok rozdielnu úroveň ochrany spotrebiteľov a podnikov, ktorá narúša celkovú úroveň bezpečnosti sietí a informačných systémov v rámci Únie. Neexistencia spoločných požiadaviek na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb zase znemožňuje, aby sa na úrovni Únie vytvoril globálny a účinný mechanizmus spolupráce. Účinné reagovanie na výzvy, pokiaľ ide o bezpečnosť sietí a informačných systémov, si preto vyžaduje komplexný prístup na úrovni Únie, ktorý by sa vzťahoval na spoločné minimálne požiadavky na budovanie kapacít a plánovanie, výmenu informácií, spoluprácu a spoločné bezpečnostné požiadavky pre prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb.

Ustanovenie o bezpečnostných opatreniach tak reaguje na požiadavku smernice NIS a zavádza minimálne bezpečnostné „štandardy“ vo vzťahu k zabezpečeniu sietí a informačných systémov. Pri tejto konštrukcii úrad vychádza zo všeobecne uznávaných a dostupných bezpečnostných štandardov na úseku kybernetickej bezpečnosti.

PZS a PDS sa však nebráni uplatňovať prísnejšie bezpečnostné opatrenia, než sú opatrenia stanovené v tomto zákone.

Ustanovenie odseku 1 definuje bezpečnostné opatrenia nevyhnutné na zabezpečenie kybernetickej bezpečnosti prostredníctvom PZS a definuje ich ako úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti.

Bezpečnostné opatrenia sa podľa odseku 2 realizujú v závislosti od kategorizácie sietí a informačných systémov v pôsobnosti PZS.

Odsek 3 a 4 upravuje oblasti, pre ktoré sa bezpečnostné opatrenia prijímajú. Bezpečnostné opatrenia sú vymedzené všeobecne a ich splnenie je možné dosiahnuť rôznymi technologickými prostriedkami. Subjekty, ktoré majú povinnosť aplikovať tieto bezpečnostné opatrenia si môžu zvoliť vlastný konkrétny spôsob realizácie týchto bezpečnostných opatrení. Táto premisa zodpovedá princípu technickej neutrality zákona o kybernetickej bezpečnosti.

Podľa odseku 5 sa bezpečnostné opatrenia prijímajú v dokumente -  bezpečnostnej dokumentácii, ktorá musí byť aktuálna a vypracovaná v súlade s reálnym stavom.

**K § 21**

V zmysle smernice NIS a vzhľadom na fundamentálne rozdiely medzi PZS, najmä na ich priame prepojenie s fyzickou infraštruktúrou, a PDS, najmä na ich cezhraničný charakter, sa zaujal diferencovaný prístup, pokiaľ ide o úroveň harmonizácie vo vzťahu k týmto dvom skupinám subjektov.

Ustanovenie odseku 1 určuje PDS s cieľom vytvoriť a zabezpečiť efektívny a účinný systém zabezpečenia kybernetickej bezpečnosti.

Podľa odseku 2 až 4 úrad zaradí digitálnu službu a PDS do príslušného zoznamu. Zaradenie do zoznamu úrad notifikuje príslušnému PDS.

V zmysle odseku 5 PDS vyplýva notifikačná povinnosť voči úradu.

**K § 22**

Aj v zmysle smernice NIS je potrebné zabezpečiť, aby PDS identifikovali riziká súvisiace s bezpečnosťou sietí a informačných systémov, ktoré používajú v kontexte poskytovania digitálnych služieb a aby prijali vhodné a primerané technické a organizačné opatrenia na riadenie týchto rizík. S ohľadom na najnovší technický vývoj musia tieto opatrenia zabezpečiť takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika, a zohľadniť tieto prvky:

* bezpečnosť systémov a zariadení;
* riešenie incidentov;
* riadenie kontinuity činnosti;
* monitorovanie, audit a skúšanie;
* súlad s medzinárodnými normami.

Ďalej je potrebné zabezpečiť, aby PDS prijali opatrenia na zabránenie a minimalizovanie vplyvu incidentov ovplyvňujúcich bezpečnosť ich sietí a informačných systémov na digitálne služby, ktoré sa poskytujú.

Ustanovenie odseku 1 teda určuje bezpečnostné povinnosti PDS s cieľom vytvoriť a zabezpečiť efektívny a účinný systém zabezpečenia kybernetickej bezpečnosti. Bezpečnostné opatrenia, ktoré na účely zabezpečenia kybernetickej bezpečnosti vo svojich podmienkach musí PDS prijať, vychádzajú z bezpečnostných opatrení uvedených vo všeobecne záväznom predpise EÚ a PDS ich implementuje vhodným a primeraným spôsobom tak, aby opatrenia smerovali k zabezpečeniu stavu kybernetickej bezpečnosti a zodpovedali existujúcemu riziku. Na tieto účely je povinný prijať zodpovedajúce technické a organizačné opatrenia.

Ustanovenie odseku 3 predstavuje najmä transpozíciu čl. 16 ods. 3 a 4 smernice NIS, podľa ktorého PDS bezodkladne oznamujú príslušnému orgánu alebo jednotke CSIRT každý incident, ktorý má závažný vplyv na poskytovanie služby, ak má k dispozícii informácie, ktoré sú potrebné na posúdenie, že kybernetický bezpečnostný incident má podstatný dopad v zmysle všeobecne záväzného právneho predpisu EÚ.

Odsek 4 a 5 upravuje nevyhnutné povinnosti PDS vo vzťahu k tretím stranám.

**K § 23**

Podľa ustanovenia odseku 1 a 2 PDS, ktorý poskytuje služby na území Slovenskej republiky je povinný ustanoviť si svojho zástupcu v Slovenskej republike a to aj v prípade, ak nemá sídlo v Európskej únii.

Odsek 3 upravuje výkon štátnej správy u PDS v prípade, ak sa siete a informačné systémy nachádzajú v inom členskom štáte európskej únie.

Zákonná úprava vychádza priamo z požiadaviek smernice NIS a nepredstavuje tak zvýšenú reguláciu na PDS ako upravuje samotná smernica NIS.

**K § 24**

Ustanovenie odseku 1 upravuje povinnosť hlásenia kybernetických bezpečnostných incidentov PZS a ustanovenie odseku 2 kategorizuje kybernetické bezpečnostné incidenty na základe presiahnutia prahových hodnôt uvedených vo vykonávacom predpise vydanom úradom. Rozlišuje sa kybernetický bezpečnostný incident prvého, druhého a tretieho stupňa.

Pri určovaní kategórií kybernetického bezpečnostného incidentu sa vychádza z čl. 6 smernice NIS. Pri určovaní závažnosti sa zohľadňujú aspoň tieto medziodvetvové faktory:

* počet používateľov využívajúcich službu, ktorú poskytuje daný subjekt,
* závislosť ostatných odvetví od služby, ktorú poskytuje daný subjekt,
* vplyv, ktorý by mohli mať incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti alebo verejnú bezpečnosť,
* trhový podiel daného subjektu,
* geografické rozšírenie z hľadiska oblasti, ktorú by incident mohol postihnúť,
* význam subjektu z hľadiska zachovania dostatočnej úrovne služby, berúc do úvahy dostupnosť alternatívnych spôsobov poskytovania danej služby.

V zmysle odseku 3 ak PZS využíva tretiu stranu, ktorou je PDS, na poskytovanie služby, ktorá je základná, uvedený PZS oznamuje každý závažný kybernetický incident, ktorý postihol PDS. Ide napríklad o prípady využívania napríklad PDS. PZS s PDS uzatvára dohodu podľa § 19 ods. 2 o zabezpečení plnení bezpečnostných a notifikačných povinností, ktoré vyplývajú PZS z tohto zákona.

Odsek 4 až 6 upravuje spôsob hlásenia kybernetického bezpečnostného incidentu. Hlásenie sa vykonáva v JISKB. Oznámenia, ktoré sú formulované na základe funkcionality JISKB obsahujú informácie umožňujúce ÚO alebo jednotke CSIRT určiť prípadný cezhraničný vplyv incidentu. Oznámenie nemá pre oznamujúcu stranu za následok vyššiu zodpovednosť.

Povinné osoby majú teda povinnosť detegovať kybernetické bezpečnostné incidenty a hlásiť ich. Úrad, ako správca JISKB, zaznamená všetky hlásené incidenty do registra kybernetických bezpečnostných incidentov. Tieto informácie sprístupní oprávneným subjektom. Takto nastavený mechanizmus je potrebný pre plnenie úlohy úradu prostredníctvom Národnej jednotky CSIRT, a to koordinovať riešenie incidentov. Zavedením JISKB sa zriadi zabezpečený kanál na prenos všetkých relevantných informácií, nevyhnutných pre rýchle, efektívne a hlavne koordinované riešenie zistených kybernetických bezpečnostných incidentov.

**K § 25**

Ustanovenie upravuje hlásenie kybernetických bezpečnostných incidentov PDS. Povinnosť oznámiť incident sa uplatňuje len v prípade, ak má PDS prístup k informáciám, ktoré sú potrebné na posúdenie dosahu spôsobeného kybernetického bezpečnostného incidentu. Hlásenie sa vykonáva prostredníctvom JISKB.

**K § 26**

Ustanovenie umožňuje hlásiť kybernetický bezpečnostný incident fyzickými a právnickými osobami prostredníctvom JISKB. Vo vzťahu k dobrovoľnému hláseniu kybernetických bezpečnostných incidentov je irelevantné, či kybernetický bezpečnostný incident presahuje prahové kritériá určené na jednotlivé kategórie kybernetických bezpečnostných incidentov.

V zmysle smernice NIS subjekty, ktoré nepatria do rozsahu jej pôsobnosti, môžu byť vystavené incidentom, ktoré majú významný vplyv na služby, ktoré poskytujú. Ak sa tieto subjekty domnievajú, že je vo verejnom záujme oznámiť, že k takýmto incidentom došlo, mali by mať možnosť dobrovoľne ich oznamovať. Takéto oznámenia by mal príslušný orgán alebo jednotka CSIRT spracovať, ak to nepredstavuje neprimerané ani nenáležité zaťaženie dotknutých členských štátov.

**K § 27**

Ustanovenie upravuje riešenie kybernetických bezpečnostných incidentov úradom, ak reakcia na hroziaci alebo prebiehajúci závažný kybernetický bezpečnostný incident nie je dostatočná alebo nie je realizovaná vôbec.

Riešenie kybernetických bezpečnostných incidentov predstavuje všetky postupy na podporu odhaľovania, analýzy a obmedzenia následkov kybernetického bezpečnostného incidentu a reakcie naň.

Podľa odseku 1 riešením kybernetických bezpečnostných incidentov podľa uvedeného ustanovenia predstavujú postupy spočívajúce:

* vo vyhlasovaní výstrahy a varovania, ktoré sa vyhlasujú v JISKB alebo masovokomunikačnými prostriedkami, ak je to v naliehavom záujme spoločnosti a štátu. Ide o opatrenie pred vznikom kybernetického bezpečnostného incidentu za účelom zabránenia jeho vzniku alebo v čase incidentu na účely jeho riešenia a zamedzenia alebo zníženia škodlivých následkov,
* v ukladaní povinnosti riešiť kybernetický bezpečnostný incident. Povinnosť riešiť kybernetický bezpečnostný incident sa ukladá rozhodnutím úradu tomu, kto prevádzkuje jednotku CSIRT, PDS a PZS,
* v povinnosti vykonať reaktívne opatrenie, ako konkrétna cielená reakcia na kybernetický bezpečnostný incident. Povinnosť vykonať reaktívne opatrenie ukladá úrad rozhodnutím PDS v čase krízovej situácie a PZS,
* v povinnosti navrhnúť a vykonať ochranné opatrenie. Ochranné opatrenie má povinnosť navrhnúť a vykonať PZS.

Odsek 2 upravuje vyhlásenie výstrahy a varovania ako oficiálne publikovanie informácie o bezpečnostnej hrozbe. Ide teda o preventívne informovanie osôb a štátu.

Odsekom 3 sa ukladá rozhodnutím úradu povinnosť riešiť kybernetický bezpečnostný incident.

Podľa odseku 4 až 6 sa reaktívne opatrenie vykonáva jedným spôsobom určeným ako reaktívna služba jednotky CSIRT. PDS a PZS, ktorému bola povinnosť vykonať toto opatrenie je povinný dokázateľným spôsobom vykonané reaktívne opatrenie preukázať ako potreba spätnej väzby pre úrad pre vyhodnotenie efektívnosti opatrenia. Účelom reaktívneho opatrenia je okamžitá reakcia na výskyt kybernetického bezpečnostného incidentu. Charakter kybernetických bezpečnostných incidentov vyžaduje k úspešnosti reaktívneho opatrenia reakciu čo v najkratšom čase.

Odsek 7 a 8 upravuje bližšie ochranné opatrenie. Úrad vyzve PZS, aby vzhľadom na analýzu kybernetických bezpečnostných incidentov, ktoré postihli jeho siete a informačné systémy navrhol ochranné opatrenie, ktorého cieľom je zaistenie bezpečnosti jeho sietí a informačných systémov pred ďalšími možnými incidentmi. Ide teda o nutnosť bezprostredne reagovať na vyriešený kybernetický bezpečnostný incident a na základe získaných skúseností PZS všeobecne zvýšiť kvalitu ochrany jeho sietí a informačných systémov. Okruh adresátov môže byť konkrétny aj všeobecný v závislosti od toho, aký rozsah sietí a informačných systémov je potrebné ochranných opatrením zaistiť. Ochranné opatrenie je realizované bezprostredne po riešení incidentu, kedy z dôvodu časovej nedostatočnosti nie je možné legislatívne a technicky realizovať všeobecné požiadavky na zvýšenie štandardu bezpečnostných opatrení.

Odsek 9 a 10 upravuje úkony úradu smerujúce k informovaniu vlády SR a Vojenského spravodajstva v osobitných prípadoch.

Podľa odseku 11 sa na rozhodnutia úradu vykonať opatrenia nevzťahuje všeobecný predpis o správnom konaní. Rozhodnutie úradu je teda prvým úkonom v riešení incidentu a akýkoľvek ďalší časový priestor určený napríklad na odvolanie alebo rozklad by už v niekoľkých hodinách mohol znamenať exponenciálny rozvoj kybernetického bezpečnostného incidentu.

**K § 28**

Upravuje sa spôsob vykonávania kontroly. Pri vykonávaní kontroly úrad postupuje podľa základných pravidiel kontrolnej činnosti podľa všeobecného predpisu o kontrole v štátnej správe. V súlade so smernicou NIS úrad vykoná kontrolu u PDS len v odôvodnených prípadoch ex post.

**K § 29**

Ustanovenie upravuje požiadavky podrobiť sa auditu pre PZS a predložiť úradu auditnú správu. Povinnosť auditu sa nevťahuje na PDS, keďže v súlade so smernicou NIS nie je možné PDS ukladať povinnosti nad rámec tejto smernice.

Odsek 1 a 2 uvádza povinnosť PZS preveriť prijaté bezpečnostné opatrenia do 24 mesiacov odo dňa zápisu do registra PZS a ďalej po každej zmene, ktorá má zásadný vplyv na prijaté bezpečnostné opatrenia a v časovom intervale, ktorý vo všeobecnom vykonávacom predpise určí úrad v závislosti od kategorizácie sietí a informačných systémov a informácií v nich.

Podľa odseku 3 audit môže vykonať len akreditovaný orgán.

Podľa odseku 5 úrad môže vykonať u PZS audit, resp. nariadiť jeho vykonanie určeným akreditovaným audítorom. Náklady na tento audit znáša úrad.

**K § 30 a 31**

Ustanovenie identifikuje konania, ktoré predstavujú porušenie tohto zákona a pri jednotlivých skutkoch sa uvádza najvyššia sadzba pokuty.

Sadzba je určená buď ako rozpätie sumy alebo ako výpočet sumy prostredníctvom percentuálneho podielu na celkovom obrate za predchádzajúci kalendárny rok, v závislosti od konkrétnej skutkovej podstaty.

Ustanovenie upravuje spôsob výpočtu sankcie, jej splatnosť a náležitosti konania. Priestupky a správne delikty prejednáva úrad a príjmy z nich sú príjmom štátneho rozpočtu.

**K § 32**

Splnomocňovacie ustanovenie podľa odseku 1 splnomocňuje úrad na vydanie vykonávacieho predpisu v určených oblastiach.

Splnomocňovacie ustanovenie podľa odseku 2 splnomocňuje ÚO, aby v spolupráci s úradom vydal všeobecne záväzný právny predpis, ktorým v závislosti od špecifických požiadaviek konkrétneho sektoru určí špecifické sektorové bezpečnostné opatrenia na účely zabezpečenia bezpečnosti sietí a informačných systémov v sektore jeho pôsobnosti.

**K § 33**

Upravujú sa spoločné ustanovenia.

**K § 34**

Prechodné a záverečné ustanovenia definujú lehoty určené pre úrad, PZS, PDS a ÚO na splnenie povinností podľa tohto zákona.

**K § 35**

Ustanovením sa preberajú právne záväzné akty Európskej únie.

**K č. II**

Novelizuje sa zákon o Vojenskom spravodajstve.

K bodu 1

Legislatívno-technická úprava v súvislosti s precizovaním pojmológie.

K bodu 2

V súvislosti so zákonom o kybernetickej bezpečnosti sa legislatívne upravuje pôsobnosť Vojenského spravodajstva v súvislosti so zabezpečením obrany v kybernetickom priestore.

K bodu 3

Upravuje a precizuje sa výkon štátnej správy na úseku zabezpečenia kybernetickej obrany, zriaďuje sa Centrum pre kybernetickú obranu Slovenskej republiky a vymedzujú sa jeho úlohy a postavenie.

**K čl. III**

Novelizuje sa zákon o správnych poplatkoch v znení neskorších predpisov a dopĺňa sa nová položka „Akreditácia jednotky CSIRT“.

**K čl. IV**

Z dôvodu zabezpečenia mzdovej motivácie vo verejnom sektore a personálnych kapacít na výkon špecializovaných činností v oblasti kybernetickej bezpečnosti sa novelizuje zákon o štátnej službe príslušníkov Policajného zboru, Slovenskej informačnej služby, Zboru väzenskej a justičnej stráže Slovenskej republiky a Železničnej polície a zavádza sa nový príplatok za výkon činnosti v oblasti kybernetickej bezpečnosti.

**K čl. V**

Novelizuje sa zákon o bankách, v ktorom sa precizuje, že nejde o porušenie bankového tajomstva ak ide o plnenie povinnosti v oblasti kybernetickej bezpečnosti.

**K čl. VI**

Novelizuje sa zákon o obrane.

K bodu 1

V súvislosti so zákonom o kybernetickej bezpečnosti sa legislatívne upravuje pojmológia obrany štátu v súvislosti so zabezpečením obrany v kybernetickom priestore.

K bodu 2 a 3

Legislatívno-technická úprava v nadväznosti na novelu zákona o Vojenskom spravodajstve a pôsobnosti Centra pre kybernetickú obranu Slovenskej republiky.

**K čl. VII**

Novelizuje sa zákon o ochrane utajovaných skutočností.

K bodu 1

Precizuje sa ustanovenie o zastavení vykonávania bezpečnostnej previerky osoby na základe potrieb vyplývajúcich z aplikačnej praxe.

K bodu 2

V súvislosti s potrebou zabezpečiť úlohy Národného bezpečnostného úradu v zákone o kybernetickej bezpečnosti sa upravuje § 35 ods. 2 zákona č. 215/2004  Z. z. o ochrane utajovaných skutočností.

K bodu 3

Na základe požiadavky Ministerstva obrany Slovenskej republiky sa dopĺňa úprava medzinárodnej bilaterálnej výmeny medzi ozbrojenými silami SR a iného štátu.

K bodu 4 a 5

Legislatívno-technická úprava leteckého snímkovania, vypúšťajú sa odseky, ktorých predmet je obsahom osobitnej právnej úpravy, z dôvodu ktorej dochádzalo k aplikačným a výkladovým problémom.

K bodu 6 až 10

Dochádza k systémovej legislatívnej úprave postavenia riaditeľa Národného bezpečnostného úradu vo veciach služobného pomeru.

**K čl. VIII**

V nadväznosti na úpravu kybernetickej bezpečnosti v návrhu zákona sa novelizuje zákon č. 45/2011  Z. z. o kritickej infraštruktúre.

K bodu 1

Legislatívno-technická úprava.

K bodu 2

V zmysle zabezpečenia riadnej aplikácie zákona v súvislosti s novým prvkom kritickej infraštruktúry je potrebné doplniť ustanovenie, ktorým sa definuje prevádzkovateľ na účely zákona o kritickej infraštruktúre.

K bodu 3

V zmysle nových kompetenčných pôsobností dochádza k úprave kompetencií ústredných orgánov.

K bodu 4

Legislatívno-technická úprava vyplývajúca z aplikačnej praxe.

K bodu 5

V § 10 sa v rámci bezpečnostných opatrení dopĺňajú opatrenia na zaistenie kybernetickej bezpečnosti s odkazom na príslušné ustanovenie zákona o kybernetickej bezpečnosti.

K bodu 6

V zmysle kompetenčného zákona a návrhu zákona o kybernetickej bezpečnosti je potrebné formálne upraviť existujúcu prílohu č. 3.

**K čl. IX**

Na zaistenie účelnej úpravy kybernetickej bezpečnosti v navrhovanom zákone je nevyhnutné upraviť zákon č. 351/2011  Z. z. o elektronických komunikáciách v znení neskorších predpisov.

K bodu 1

Dopĺňa sa ustanovenie o vzájomnej spolupráci a výmene informácií potrebných na zabezpečenie kybernetickej bezpečnosti.

K bodu 2

Uvedenou úpravou, ktorá umožní sprístupniť Národnému bezpečnostnému úradu telekomunikačné tajomstvo, sa zaistí systematický zber a následné vyhodnocovanie incidentov, ktoré majú vplyv na kybernetickú bezpečnosť.

**K čl. X**

Novelizuje sa zákon o štátnej službe. V súlade s navrhovanou úpravou v rámci právnej úpravy odmeňovania, kedy je zamestnávateľom štát, sa ustanovením umožňuje priznať príplatok za vykonávanie špecializovaných činností na úseku kybernetickej bezpečnosti zamestnancovi až do výšky 90 % platovej tarify, čím zamestnávateľ, ktorým je štát, dostáva možnosť zamestnať špecializovaných odborníkov a konkurovať tak súkromným zamestnávateľom.

**K č. XI**

Navrhuje sa účinnosť zákona.