https://doi.org/10.5817/RPT2019-2-1

BEZPEČNOSŤ INFORMAČNÝCH SYSTÉMOV VEREJNEJ SPRÁVY VO SVETLE ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI A ZÁKONA O INFORMAČNÝCH TECHNOLÓGIÁCH VO VEREJNEJ SPRÁVE[1]

JOZEF ANDRAŠKO[2]

ABSTRAKT

Autor sa v predkladanom príspevku venuje otázke bezpečnosti informačných systémov verejnej správy v zmysle novej legislatívy, ktorá významným spôsobom pozmenila právnu úpravu bezpečnosti informačných systémov verejnej správy. Autor sa v prvom rade zameral na novoprijatý zákon o informačných technológiách verejnej správy, ktorý upravuje problematiku bezpečnosti informačných technológií verejnej správy. Autor príspevku v druhom rade upriamuje pozornosť na bezpečnosť informačných systémov verejnej správy v zmysle zákona o kybernetickej bezpečnosti, podľa ktorého sú informačné systémy verejnej správy zaradené medzi základné služby. V závere autor upriami pozornosť na prepojenie a rozdiely v otázkach bezpečnosti informačných systémov verejnej správy v zmysle zákona o kybernetickej bezpečnosti a zákona o informačných technológiách vo verejnej správe. Autor skúma danú problematiku z pohľadu právneho poriadku Slovenskej republiky.

[1] Tento príspevok vznikol v rámci projektu APVV-17-0403 Vplyv vzájomného uznávania prostriedkov elektronickej identifikácie na elektronické služby verejnej správy.

[2] JUDr. Jozef Andraško, PhD., odborný asistent, Ústav práva informačných technológií a práva duševného vlastníctva, Univerzita Komenského v Bratislave, Právnická fakulta, e-mail: jozef.andrasko@flaw.uniba.sk.

KLÍČOVÁ SLOVA

informačné systémy verejnej správy, informačné technológie, kybernetická bezpečnosť

ABSTRACT

The author deals with the issue of security of public administration information systems in accordance with the new legislation which significantly changed the legal regulation of security of public administration information systems. The author focuses primarily on the newly adopted Information Technologies of Public Administration Act which regulates the issue of security of information technologies of public administration. Secondly, the author focuses on the security of public administration information systems pursuant to the Cyber Security Act in which public administration information systems are considered as the essential services. In conclusion, the author will draw attention to the interconnection and differences in security issues of public administration information systems pursuant to the Cyber Security Act and the Information Technologies in Public Administration Act. The author deals with the issue in question from the perspective of the legal order of the Slovak Republic.

KEYWORDS

public administration information systems, information technologies, cyber security

1. ÚVOD

Bezpečnosť informačných systémov verejnej správy (ďalej len „ISVS“) zohráva významnú úlohu, a to hneď z niekoľkých dôvodov. Aby verejná správa mohla prostredníctvom svojich orgánov plniť svoje úlohy, musí sa spoliehať na svoje ISVS, resp. na informácie a údaje, ktoré sú v nich spracovávané. Bez dostatočnej úrovne bezpečnosti ISVS by nemohli orgány

verejnej správy vydávať individuálne správne akty alebo iné finálne formy činnosti verejnej správy.[3]

V kontexte bezpečnosti, resp. informačnej a kybernetickej bezpečnosti je potrebné nahliadať na informačné systémy verenej správy a na informácie, ktoré sa v nich spracúvajú ako na aktíva, ktoré je potrebné chrániť. Aby došlo k zabezpečeniu dostatočnej úrovne ochrany ISVS pred rôznymi hrozbami, je potrebné, aby konkrétne subjekty realizovali bezpečnostné opatrenia, ktoré môžu znižovať dopady bezpečnostných incidentov na tieto systémy. Roztrieštenosť právnej úpravy týkajúcej sa povinnosti realizovať bezpečnostné opatrenia môže spôsobiť, že subjekty v rôznych právnych postaveniach nebudú realizovať bezpečnostné opatrenia v dostatočnej miere resp. ich nebudú realizovať vôbec. V súvislosti s bezpečnostnými incidentmi je taktiež dôležité, aby príslušné právne predpisy jasne a zrozumiteľne upravovali, ktorý subjekt je povinný hlásiť bezpečnostné incidenty, ktorému subjektu sa takéto bezpečnostné incidenty nahlasujú a v akej lehote.

V tomto príspevku sa zameriavam na problematiku bezpečnosti ISVS, a to z pohľadu právneho poriadku Slovenskej republiky. V prvom rade považujem za potrebné ozrejmiť pojmy ako bezpečnosť, informačná bezpečnosť a kybernetická bezpečnosť, a to najmä z teoretického hľadiska. Následne sa budem venovať problematike bezpečnosti ISVS, a to z pohľadu novej právnej úpravy, ktorá sa týka informačných technológií verejnej

[3] V súčasnosti zohrávajú ISVS významnú úlohu aj v kontexte cezhraničnej autentifikácie osôb. Konkrétnym príkladom je ISVS, modul IAM (Identity Access Management), taktiež známy ako autentifikačný modul, ktorý plní dôležitú úlohu pri cezhraničnej autentifikácii osôb (občanov iných členských štátov Európskej únie). Pri prvom prihlásení osoby z iného členského štátu Európskej únie do online služby poskytovanou subjektom verejného sektora Slovenskej republiky sa zapíšu z eIDAS uzla do modulu IAM údaje o danej osobe a zároveň sa mu vytvorí elektronická schránka v zmysle zákona č. 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente). Bez toho aby sa orgány verejnej správy nemohli spoliehať na pravosť, dôveryhodnosť a dostupnosť informácií a údajov spracovávaných v ISVS, nemohli by vykonávať svoje úlohy, čo by znemožnilo riadny chod verejnej správy. Bližšie k problematike cezhraničnej autentifikácie pozri: ANDRAŠKO, J. a MESARČÍK, M. *Problematika GDPR v kontexte nariadenia eIDAS.* In Digitalizácia, zmeny vonkajšieho prostredia a spoločnosť budúcnosti. Bratislava, Univerzita Komenského v Bratislave, Právnická fakulta, s. 8- 22.

správy, ako aj z pohľadu právnej úpravy, ktorá sa týka kybernetickej bezpečnosti vo všeobecnosti. Prepojenosť týchto právnych úprav je najviac evidentná, najmä čo sa týka bezpečnosti ISVS. V ďalšej časti príspevku upriamim pozornosť na povinnosť konkrétnych subjektov v rôznych právnych postaveniach hlásiť bezpečnostné incidenty. V tejto súvislosti budem skúmať, aké bezpečnostné incidenty je potrebné hlásiť, ktoré subjekty, v akých právnych postaveniach sú povinné hlásiť bezpečnostné incidenty, v akých lehotách a voči ktorým subjektom si musia túto povinnosť plniť. V závere poukážem na najproblematickejšie časti skúmanej problematiky a dovolím si navrhnúť aj konkrétne riešenia.

2. BEZPEČNOSŤ

Vo všeobecnosti možno povedať, že bezpečnosť je založená na ochrane aktív pred rôznymi hrozbami pri určitej zraniteľnosti.[4] Za aktíva možno považovať všetko, čo má pre danú organizáciu[5] hodnotu. Môže ísť o hmotné aktíva (zariadenie, personál a pod.) alebo o nehmotné aktíva (napr. informácie, údaje, služby, dobré meno, know-how a pod.). Akákoľvek udalosť, skutočnosť, osoba, sila, ktorá môže spôsobiť, že sa aktíva organizácie dostanú do neželaného stavu (napr. nebudú fungovať počítače, zamestnanec ochorie a pod.), sa nazýva hrozba. Najčastejšími hrozbami, ktoré možno aplikovať na aktíva sú prírodné vplyvy (napr. zemetrasenie, búrka a pod.), technické poruchy (napr. výpadok siete, výpadok podpornej infraštruktúry a pod.), chyby v programovom vybavení, neúmyselné ľudské chyby, cieľavedomá ľudská činnosť (sabotáž, prieniky hackerov do systému) a pod.[6]

---

[4] VON SOLMS, R., VAN NIEKERK, J. *From information security to cyber security. In* Computers & Security, 2013, roč. 38, s. 100.

[5] V terminológii informačnej bezpečnosti je pojem organizácia definovaná ako skupina ľudí a zariadenie, so zodpovednosťou, právomocami a vzájomnými vzťahmi. Bližšie pozri bod 2.56 štandardu ISO/IEC 27000:2016 *Overview and vocabulary*. Pre účely tohto príspevku možno za organizáciu v zmysle informačnej bezpečnosti považovať verejnú správu ako takú, spravujúce subjekty verejnej správy, a teda aj orgány verejnej správy.

[6] OLEJÁR, D. a kol. *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015, s. 7. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

Je potrebné podotknúť, že hrozba sa môže, ale nemusí uplatniť. Aby sa hrozba vôbec naplnila, musí aktívum spĺňať nejaké predpoklady, ktoré nazývame zraniteľnosť. Každé aktívum je zraniteľné, nakoľko jeho hodnotu ohrozujú rôzne vplyvy. Pod zraniteľnosťou možno chápať chybu, nedostatok v podobe nedostatočne vyškoleného zamestnanca, ktorý sa svojou neodbornosťou a neskúsenosťou môže dopúšťať chýb. Takýto nedostatok môže byť zneužitý hrozbou v takom rozsahu, že hodnota aktíva môže byť poškodená alebo dokonca zničená.[7]

Aktívum môže byť objektom hrozby ale taktiež môže byť aj cieľom útoku. Útok predstavuje úmyselný pokus o naplnenie hrozby, ktorej nositeľom je človek (poškodenie údajov, prienik do systému) a výsledkom je škoda alebo strata aktív.[8]

V prípade, že bude hrozba voči aktívu naplnená a spôsobí narušenie požadovaného stavu aktíva, dochádza k vzniku bezpečnostného incidente. Bezpečnostný incident môže byť spôsobený aktivitou užívateľa (úmyselne, neúmyselne), alebo iným pôsobením (napr. havária, chyba systému a pod.). Dôsledkom bezpečnostného incidentu je ujma na aktívach organizácie (napr. nefunkčnosť aktíva, nemožnosť poskytovania služby, materiálne škody, finančné škody a pod.). Takáto ujma sa nazýva dopad, ktorý sa dá vyjadriť kvantitatívne (napr. finančne ako cena opravy alebo náhrady poškodeného počítača, obnova jeho programového vybavenia a údajov, a pod.) alebo kvalitatívne.[9]

---

[7] POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, s. 38.

[8] OLEJÁR, D. a kol. *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015, s. 8. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

[9] Pri ťažko merateľných dopadoch (napr. pri narušení reputácie) sa využíva kvalitatívne vyjadrenie dopadu bezpečnostného incidentu, a to označením nízky (ak nemá bezpečnostný incident vplyv na chod organizácie), alebo označením vysoký (organizácia nie je spôsobilá vykonávať svoje hlavné úlohy). Označenie dopadu bezpečnostného incidentu ako stredný predstavuje situáciu, kedy organizácia už pocítila dôsledky (dokáže plniť svoje primárne úlohy, ale nie v plnom rozsahu). Bližšie pozri OLEJÁR, D. a kol. *Manažment informačnej bezpečnosti* a *základy PKI*. Bratislava, 2015, s. 8-9. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

Organizácia počas plnenia svojich úloh čelí mnohým bezpečnostným incidentom či už tým vážnym alebo menej vážnym. Nie všetky hrozby sú pre danú organizáciu opodstatnené, a preto je potrebné vytvoriť kritéria, na základe ktorých bude organizácia rozlišovať hrozby na relevantné a tie menej relevantné. Takýmto kritériom je, napr. dopad hrozby, resp. bezpečnostného incidentu, pri ktorom došlo k naplneniu hrozby. Jedno kritérium by nebolo dostačujúce, a preto je potrebné stanoviť druhé kritérium, ktorým je pravdepodobnosť naplnenia hrozby. Tieto oba kritéria sú spojené v riziku. Vo všeobecnosti možno povedať, že riziko predstavuje možnosť (nie nutnosť), že konkrétna hrozba využije zraniteľnosť aktíva, čo spôsobí vznik ujmy vlastníkovi aktíva.[10]

Riziká vyplývajúce z hrozieb voči aktívam organizácie nepredstavujú rovnaký bezpečnostný problém, a preto je potrebné vykonať analýzu rizík, čo predstavuje stanovenie úrovne rizík. Následne sa riziká podľa závažnosti zoradia a rozhodne sa, ktorými rizikami sa bude organizácia zaoberať a ktorými nie. Hranica akceptovateľného rizika predstavuje pomyselnú čiaru v zozname rizík. Inými slovami možno povedať, že v prípade rizík, ktoré sa nachádzajú nad čiarou, musí organizácia prijať také riešenia, aby sa hodnoty daného rizika znížili. Takýmto riešením sú opatrenia, ktoré plnia niekoľko úloh. Na jednej strane znižujú dopady bezpečnostných incidentov na aktíva, a na strane druhej môžu odstraňovať zraniteľnosť aktív, čím v konečnom dôsledku znižujú pravdepodobnosť, že vôbec dôjde k bezpečnostnému incidentu. Takýmto opatrením môže byť, napr. spoľahlivá identifikácia a autentifikácia, šifrovanie citlivej informácie, zálohovanie údajov a pod.[11]

V dobe kedy sa informácie prenášajú a spracúvajú elektronicky a digitálne prostredníctvom informačných a komunikačných technológií (ďalej len „IKT“) sa problematika bezpečnosti spája najmä s pojmami informačná bezpečnosť a kybernetická bezpečnosť. V odbornej literatúre sa pojem informačná bezpečnosť častokrát zamieňa za pojem kybernetická

[10] OLEJÁR, D. a kol. *Manažment informačnej bezpečnosti* a *základy PKI*. Bratislava, 2015, s. 9. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

[11] Tamtiež, s. 9-10.

bezpečnosť a naopak. Nejasnosť v terminológii spomínaných pojmov vychádza najmä zo skutočnosti, že predmetné pojmy sú upravené v mnohých dokumentoch, národného, ako aj medzinárodného charakteru, avšak tieto dokumenty nemajú právnu záväznosť. Nejednotnosť týchto pojmov, ktoré sú používané najmä v rôznych stratégiách, ktoré upravujú bezpečnosť v kybernetickom priestore spôsobila roztrieštenosť pohľadov na skúmané pojmy.

Pojmy informačná a kybernetická bezpečnosť budem analyzovať najmä prostredníctvom medzinárodných štandardov, ktoré túto problematiku riešia už viac než 20 rokov. Hoci štandardy nie sú právne záväzné, častokrát sa na ne legislatíva odvoláva a dávajú presnejšie formulované odpovede na otázky, ktoré súvisia informačnou a kybernetickou bezpečnosťou.

Štandard možno z formálneho hľadiska definovať ako: *„dokument, ktorý vznikol na základe konsenzu a bol schválený uznaným orgánom, ktorý poskytuje pre všeobecné a opakované použitie pravidlá, smernice alebo charakteristiky činností alebo ich výsledkov zamerané na dosiahnutie optimálneho stupňa usporiadania v danom kontexte.*“[12]

Z hľadiska orgánu, ktorý prijíma konkrétny štandard, možno štandardy rozdeliť na formálne a neformálne. Zatiaľ čo formálne štandardy boli schválené národnými[13], európskymi[14] alebo medzinárodnými štandardizačnými orgánmi[15], neformálne štandardy boli publikované organizáciami pre rozvoj štandardov, ktoré však nie sú uznané za štandardizačné orgány.[16]

---

[12] ISO/IEC *Guide 2:2004 Standardization and related activities – General vocabulary,* s. 10.

[13] Zoznam národných štandardizačných orgánov dostupný z: https://standards.cen.eu/dyn/www/f?p=CENWEB:5. [citované 28.9.2019].

[14] Medzi európske štandardizačné orgány možno zaradiť *European Committee for Standardization* (CEN), *European Committee for Electrotechnical Standardization* (CENEL) a *European Telecommunications Standards Institute* (ETSI).

[15] Medzi medzinárodné štandardizačné orgány možno zaradiť *International Organization for Standardization* (ISO), *International Electrotechnical Commission* (IEC) a *International Telegraph Union* (ITU).

[16] Napr. *American Society for Testing Materials International, Society of Automotive Engineers, Internet Engineering Task Force* a i.

Problematike informačnej bezpečnosti sa venuje viacero medzinárodných štandardov. V ďalších častiach analýzy sa zameriam na medzinárodné ISO štandardy, ako aj na diela autorov, ktorí sú považovaní za odborníkov v oblasti informačnej a kybernetickej bezpečnosti.

2.1 INFORMAČNÁ BEZPEČNOSŤ - POJEM

Medzinárodný štandard ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary (ďalej len „ISO/IEC 27000:2016“) definuje informačnú bezpečnosť ako zachovanie dôvernosti, integrity a dostupnosti informácií.

Dôvernosť, integrita a dostupnosť predstavujú základné bezpečnostné požiadavky na ochranu informácií. Bezpečnostná požiadavka na zaistenie dôvernosti informácie znamená, že informácia je chránená pred prezradením neoprávneným osobám. Príkladom informácií, ktoré si vyžadujú ochranu pred neoprávneným prístupom sú, napr. osobné údaje, informácie týkajúce sa bezpečnosti štátu a pod.[17]

Bezpečnostná požiadavka na zaistenie integrity údajov znamená, že údaje[18] sú chránené pred náhodnou alebo úmyselnou modifikáciou, ktorá by mohla mať vplyv na platnosť údajov. Príkladom by mohla byť ochrana údajov v rámci transakcií, kde dochádza k platbe, kde by mohlo dôjsť k modifikácii sumy.[19]

---

[17] TODOROV, D. *Mechanics of Users Identification and Authentication. Fundamentals of Identity Management.* USA: Auerbach Publications, 2007, s. 2.

[18] V tomto prípade je potrebné rozlišovať medzi informáciou a údajom. Ako uvádza Olejár, informácie sú obsahom údajov a údaje sú len forma zápisu informácií. To znamená, že tú istú informáciu (napr. desať) možno zapísať v rôznej forme (napr. X, ten a pod.). Bližšie pozri OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti* a *základy PKI*. Bratislava, 2015, s. 11. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019]. K rozdielu medzi pojmom údaj a informácia taktiež pozri: POLČÁK, R. *Informace a data v právu.* In Revue pro právo a technologie 7, 2016, s. 67–91.

OLEJÁR, D. a kol.: *Manažment informačnej bezpečnosti* a *základy PKI*. Bratislava, 2015, s. 9-10.[on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

[19] TODOROV, D. *Mechanics of Users Identification and Authentication. Fundamentals of Identity Management.* USA: Auerbach Publications, 2007, s. 2.

Dostupnosť informácie ako bezpečnostná požiadavka znamená, že informácie a služby, ktoré poskytujú osobám a organizáciám, musia byť dostupné používateľovi kedykoľvek, keď o to požiada. Napr. webová stránka, prostredníctvom ktorej sa osoby identifikujú a autentifikujú pre využívanie elektronických služieb verejnej správy, musí byť dostupná kedykoľvek, ak o to daná osoba požiada. Nedostupnosť webovej stránky by narušila poskytovanie služieb.[20]

Popri vyššie uvedených bezpečnostných požiadavkách na ochranu informácií, existujú aj iné bezpečnostné požiadavky ako autentickosť, súkromnosť, anonymita, pseudonymita, nepopretie pôvodu, nepopretie doručenia, resp. v prípade ochrany systémov poznáme dosledovateľnosť.[21]

V zmysle predmetného štandardu sa za informácie považujú nielen informácie v digitálnej forme (údaje uložené na elektronických alebo optických médiách), ale aj v materiálnej forme (napr. papier). Medzi informácie môžeme taktiež zaradiť informácie ako vedomosti zamestnanca. Informácie môžu byť prenášané rôznymi spôsobmi, kuriérom, elektronickou alebo verbálnou komunikáciou. Bez ohľadu na formu informácií a spôsob jej prenosu platí, že si vyžadujú dostatočnú ochranu.[22]

Whitman a Mattord definujú informačnú bezpečnosť ako: *„ochranu informácií a ich kľúčových prvkov, vrátane systémov a hardvéru, ktoré používajú, uchovávajú a prenášajú túto informácie.“*[23] Kľúčovými prvkami sú v tomto prípade dôvernosť, integrita a dostupnosť informácie.[24]

Podľa Olejára sa pojem informačná bezpečnosť používa minimálne v troch významoch:[25]

---

[20] Tamtiež, s. 2.

[21] Pre tieto bezpečnostné požiadavky bližšie pozri OLEJÁR, D. a kol.: *Informačná bezpečnosť.* Bratislava, 2013. s. 12. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

[22] ISO/IEC 27000:2016, s. 15.

[23] WHITMAN, M.E. a MATTORD, H.J. *Principles of Information security*. Boston: Course Technology, 2012, s. 9.

[24] Dôvernosť, integrita a dostupnosť informácie sú v odbornej literatúre označené ako CIA trojuholník. Skratka CIA vychádza zo začiatočných písmen anglických názvov týchto základných bezpečnostných požiadaviek (*Confidentiality, Integrity, Availability*).

- je to ideálny stav systému alebo organizácie, ktorý sa dá charakterizovať tak, že všetko (IKT) funguje v súlade s požiadavkami (stanovenými napr. v bezpečnostnej politike) a v systéme/organizácii nedochádza k bezpečnostným incidentom,
- označuje činnosť smerujúcu k dosiahnutiu ideálneho stavu,
- medziodborová oblasť, ktorá skúma hrozby voči IKT a informácii a metódy eliminácie rizík, ktoré z nich vyplývajú.

2.2 KYBERNETICKÁ BEZPEČNOSŤ – POJEM

Pojem kybernetická bezpečnosť je v zmysle medzinárodného štandardu ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity (ďalej len „ISO/IEC 27032:2012“) definovaný ako zachovanie dôvernosti, integrity a dostupnosti informácií[26] v kybernetickom priestore.[27] V porovnaní s informačnou bezpečnosťou, pôjde teda len o informácie, ktoré sú prenášané a uložené v kybernetickom priestore. Kybernetická bezpečnosť sa vzťahuje na opatrenia, ktoré by zainteresované strany[28] mali stanoviť pre vytvorenie a zachovanie bezpečnosti v kybernetickom priestore.[29]

V zmysle vyššie uvedenej definície by sme mohli povedať, že kybernetická bezpečnosť je informačná bezpečnosť kybernetického

---

[25] OLEJÁR, D. a kol. *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015. s. 16. [on-line]. Dostupné z: https://www.csirt.gov.sk/bezpecnostna-studovna/mfsr-vzdelavanie-89f.html. [citované 28.9.2019].

[26] Podľa niektorých autorov je kybernetická bezpečnosť postavená na princípoch, ktoré sa nazývajú triády kybernetickej bezpečnosi. Konkrétne ide o:

1. CIA (*Confidentiality, Integrity, Availability*)
2. Prvky kybernetickej bezpečnosti (Ľudia, Technológie, Procesy)
3. Životný cyklus kybernetickej bezpečnosti (Prevencia, Detekcia, Reakcia).

Bližšie pozri KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o, 2019. s. 45-68 alebo BAYUK, L. a kol.: *Cyber security policy guidebook*. Wiley, 2012, s. 2-3.

[27] Predmetný medzinárodný štandard odkazuje na viacerých miestach na ISO štandardy, ktoré sa aplikujú v prípade informačnej bezpečnosti.

[28] Medzi zainteresované strany v kybernetickom priestore možno zaradiť užívateľov (jednotlivci, súkromné a verejné organizácie) a poskytovateľov (poskytovatelia Internetu a poskytovatelia aplikačných služieb).

[29] ISO/IEC 27032:2012, s. 17.

priestoru. Je viac ako potrebné ozrejmiť pojem kybernetický priestor *(cyberspace)*, nakoľko tento pojem určuje obsah pojmu kybernetická bezpečnosť.

Neexistuje jednoznačná, všeobecne akceptovaná definícia pojmu kybernetický priestor. Kybernetický priestor možno chápať ako systém systémov (SoS) zložený z rôznych digitálnych zariadení spojených počítačovými sieťami, pripojenými na Internet (vrátane programového vybavenia, údajov, aplikačných programov, technickej infraštruktúry) a ľudí, ktorí v tomto priestore pôsobia, činností, ktoré v ňom prebiehajú, pravidiel, ktoré upravujú činnosti a vzťahy v priestore. Iné definície chápu kybernetický priestor ako virtuálny systém informácií, vzťahov, činností, ktoré vznikajú pri spracovaní informácií prostredníctvom digitálnych IKT, ktorý však neexistuje v materiálnej forme.[30]

V zmysle medzinárodného štandardu ISO/IEC 27032:2012 predstavuje kybernetický priestor komplexné prostredie, ktoré vzniklo interakciou ľudí, softvéru a služieb na Internete prostredníctvom zariadení a sietí, technológií k nemu pripojených, ktoré neexistuje v žiadnej fyzickej podobe.[31]

Autori odbornej literatúry chápu kybernetický priestor ako geograficky neobmedzený, nefyzický priestor, v ktorom sa nezávisle od času, diaľky a miesta vykonávajú transakcie medzi ľuďmi, medzi počítačmi a medzi počítačmi a ľuďmi. Charakteristickým znakom kybernetického priestoru je nemožnosť určiť presné miesto a čas, kedy došlo k danej aktivite alebo kde došlo k presunu informácií.[32]

Hoci ISO/IEC 27032:2012 a niektorí autori odbornej literatúry chápu kybernetický priestor ako prostredie, ktoré neexistuje vo fyzickej podobe, nemožno ho chápať izolovane od jeho technologických komponentov, z ktorých je tvorený. Avšak, okrem technologickej úrovne má kybernetický

[30] Bližšie pozri: ANDRAŠKO, J. a kol.: *Zákon o kybernetickej bezpečnosti.* Komentár. Bratislava: Wolters Kluwer SR s.r.o. 2018, s. 96.

[31] ISO/IEC 27032:2012, s. 12.

[32] HAMELINK, C. J. *The ethics of cyberspace.* Sage, 2001, s. 9.

priestor aj sociálno-technickú úroveň, v rámci ktorej sa vykonávajú rôzne kybernetické aktivity.[33]

Legálnu definíciu pojmu kybernetický priestor možno nájsť v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o KB“). Kybernetický priestor je v zmysle § 3 písm. b) predmetného zákona definovaný ako: *„globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi.“* Predmetná definícia má viacero nedostatkov, nakoľko medzi prvky, ktoré patria do kybernetického priestoru zaradzuje len aktivované prvky, čím vylučuje prvky, ktoré nie sú aktivované. Ako príklad neaktivovaných prvkov možno uviesť siete, počítače a zariadenia, ktoré sa nemusia dočasne používať, avšak stále sú súčasťou technologickej infraštruktúry, ktorú je potrebné chrániť. V prípade ak by sme pripustili, že kybernetická bezpečnosť sa vzťahuje len na aktívne prvky kybernetického priestoru, potom by pasívne komponenty prestali byť prvkami kybernetického priestoru. Takéto úvahy sú namieste najmä z dôvodu, že nová právna úprava týkajúca sa ochrany informačných technológií verejnej správy sa netýka len ISVS, ale aj infraštruktúry, ktorá zabezpečujúce implementáciu a prevádzkovanie ISVS.[34]

Pre úplnosť je potrebné dodať, že kybernetická bezpečnosť sa v zmysle štandardu ISO/IEC 27032:2012 opiera o informačnú bezpečnosť *(information security)*, bezpečnosť aplikácií *(application security),* bezpečnosť siete *(network security)* a bezpečnosť Internetu *(Internet security)* ako o základné stavebné kamene. Kybernetická bezpečnosť je jednou z činností potrebných pre ochranu kritickej informačnej infraštruktúry *(critical information infrastructure protection)*. Primeraná ochrana služieb kritickej infraštruktúry súčasne prispieva k základným potrebám bezpečnosti

[33] VAN DEN BERG, J. a kol. *On (the Emergence of) Cyber Security Science and its Challenges for CyberSecurity Education.* NATO STO/IST-122 symposium, Tallinn, 13-14 október 2014, s. 12-2.

[34] Problematickým aspektom pojmu kybernetický priestor v zmysle zákona o KB je aj zaradenie ľudí medzi prvky kybernetického priestoru. Bližšie pozri ANDRAŠKO, J. a kol.: *Zákon o kybernetickej bezpečnosti.* Komentár. Bratislava: Wolters Kluwer SR s.r.o. 2018, s. 95.

(bezpečnosť, spoľahlivosť a dostupnosť kritickej infraštruktúry) za účelom dosiahnutia cieľov kybernetickej bezpečnosti.[35]

V odbornej literatúre možno nájsť rôzne definície pojmu kybernetická bezpečnosť.[36] Kolouch chápe kybernetickú bezpečnosť v dvoch rovinách. V prvej rovine definuje kybernetickú bezpečnosť ako: *„súhrn právnych, organizačných, technických a vzdelávacích prostriedkov, ktoré smerujú k zaisteniu ochrany počítačových systémov a ďalších prvkov IKT, aplikácií, údajov a užívateľov.“*[37]

V druhej rovine chápe kybernetickú bezpečnosť ako: „*schopnosť počítačových systémov a využívaných služieb reagovať na kybernetické hrozby či útoky a ich následky, ako aj plánovanie obnovy funkčnosti počítačových systémov a služieb s nimi spojených.“*

Pojem kybernetická bezpečnosť je definovaný zákone o KB. V zmysle § 3 písm. g) zákona o KB je kybernetická bezpečnosť[38] definovaná ako: „*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.“* Predmetná definícia vychádza z pojmu bezpečnosť sietí a informačných systémov v zmysle čl. 4 ods. 2 smernice 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 (ďalej len „smernica NIS“).[39]

---

[35] ISO/IEC 27032:2012, s. 17.

[36] K pojmu kybernetická bezpečnosť pozri: POLČÁK, R: *Kybernetická bezpečnost*. In Právo informačních technológií. Praha: Wolters Kluwer ČR, 2018, s. 587-593 alebo POLČÁK, R. *Kybernetická bezpečnost jako aktuální fenomén českého práva.* In Revue pro právo a technologie, 2015,č. 11, s. 95. [on-line]. Dostupné z: https://journals.muni.cz/revue/article/view/2980. [citované 29.9.2019].

[37] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o, 2019. s. 45-68 alebo BAYUK, L. a kol.: *Cyber security policy guidebook*. Wiley, 2012, s. 45.

[38] Bližšie k pojmu kybernetická bezpečnosť v zmysle zákona o KB pozri ANDRAŠKO, J. a kol. *Zákon o kybernetickej bezpečnosti.* Komentár. Bratislava: Wolters Kluwer SR s.r.o. 2018, s. 100-103.

2.3 ROZDIEL MEDZI INFORMAČNOU A KYBERNETICKOU BEZPEČNOSŤOU

V prvom rade si je potrebné uvedomiť, že v prípade skúmaných pojmov nejde o synonymá. Informačnú a kybernetickú bezpečnosť nemožno v zmysle skúmaných štandardov vnímať ako totožné pojmy a nie je ani vhodné ich rozlišovať na základe toho, ktorý pojem je širší alebo užší.

V prípade kybernetickej bezpečnosti je okrem iného taktiež cieľom ochrana informácií, ale len tých z prostredia kybernetického priestoru. V tejto súvislosti si je potrebné uvedomiť, že z pohľadu ochrany informácie ako aktíva, sú v prípade informačnej bezpečnosti chránené nie len informácie v elektronickej podobe, ale aj vo fyzickej podobe.

V druhom rade je potrebné podotknúť, že kybernetická bezpečnosť má z pohľadu štandardov za cieľ zabezpečiť zdieľanie a koordináciu medzi jednotlivými bezpečnostnými doménami. Možno povedať, že kybernetická bezpečnosť spravuje bezpečnostné problémy, ktoré nerieši žiadna z bezpečnostných domén alebo môže byť identifikovaná viacerými doménami. V druhom prípade je potrebné zdieľať a koordinovať informácií pre efektívne a komplexné riešenie bezpečnostného problému.[40]

Avšak v súčasnosti sa v právnom poriadku Slovenskej republiky nerozlišuje medzi informačnou bezpečnosťou a kybernetickou bezpečnosťou. Z právneho hľadiska, ako aj praktického hľadiska je rozlišovanie medzi informačnou bezpečnosťou a kybernetickou bezpečnosťou nepodstatné. Dôležitejšie je, aby právna úprava zabezpečila dostatočnú ochranu informačných systémov a informácií, ktoré sa v nich

[39] V zmysle smernice NIS sa bezpečnosť sietí a informačných systémov chápe ako: *„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.“* Smernica NIS chápe bezpečnosť sietí a informačných systémov ako vlastnosť sietí a informačných systémov, zatiaľ čo v zákone o KB je chápaná kybernetická bezpečnosť ako stav.

[40] V niektorých prípadoch je pojem kybernetickej bezpečností spájaný s ochranou kritickej informačnej infraštruktúry, čo však nie je pravdou. Súvislosť medzi kybernetickou bezpečnosťou a ochranou kritickej informačnej infraštruktúry je častokrát viac ako zrejmá, nakoľko napr. infraštruktúra telekomunikačných sietí zabezpečuje prístup do kybernetického priestoru.

spracúvajú, tak aby sa dalo spoľahnúť na ich dôvernosť, dostupnosť a integritu. Taktiež je potrebné, aby sa zabezpečila nielen ochrana informácií v materiálnej podobe, ale aj informácií, ktoré sú spracúvané v elektronickej alebo digitálnej forme.

3. BEZPEČNOSŤ ISVS V PRÁVNOM PORIADKU SLOVENSKEJ REPUBLIKY

Právna úprava ISVS a otázka ich bezpečnosti prešla v poslednom období výraznými zmenami. V prvom rade, zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ISVS“) bol zrušený zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS“), ktorý nadobudol účinnosť 5. mája 2019.

Problematika bezpečnosti ISVS je v súčasnosti stále upravená vo výnose Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy. Predmetný výnos obsahuje bezpečnostné štandardy.[41]

Bezpečnosť ISVS je taktiež predmetom zákona o KB, nakoľko za určitých okolností môže byť konkrétny ISVS zaradený medzi základné služby a jeho správca do registra prevádzkovateľov základných služieb (ďalej len „PZS“). V takejto situácii je správca v pôsobnosti ktorého je konkrétny ISVS povinný plniť povinnosti v zmysle zákona o KB.

V nasledujúcej časti príspevku dôjde k ozrejmeniu pojmu informačná technológia verejnej správy, ktorý v sebe zahŕňa aj pojem informačný systém verejnej správy. Taktiež upriamim pozornosť na ustanovenia zákona o ITVS, ktoré upravujú problematiku bezpečnosti informačných technológií verejnej správy. Následne poukážem na zákon o KB a jeho vzťah k zákonu o ITVS, a to najmä z pohľadu bezpečnostných opatrení resp. iných

[41] Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov zostáva platný a účinný do nadobudnutia účinnosti vykonávacieho právneho predpisu podľa § 31 zákona o ITVS, najneskôr však do 1. mája 2020.

povinností, ktoré musia konkrétne subjekty plniť, aby zabezpečili dostatočnú úroveň bezpečnosti informačných technológií verejnej správy, resp. ISVS.

3.1 BEZPEČNOSŤ ISVS V ZÁKONE O ITVS

Zákon o ITVS v porovnaní so zrušeným zákonom o ISVS definuje pojem informačné technológie verejnej správy (ďalej len „ITVS“) a rozširuje svoju pôsobnosť aj na bezpečnosť týchto technológií. V zmysle § 2 ods. 2 zákona ITVS sú ITVS definované ako: „*informačná technológia v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby*.“ Informačné technológie sú v zmysle § 2 ods. 1 zákona o ITVS chápané ako: „*prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe*.“ Zákon o ITVS uvádza príklady informačných technológií, konkrétne informačný systém, infraštruktúru, informačnú činnosť a elektronické služby. Definícia pojmu informačný systém verejnej správy zostala zachovaná v znení už zrušeného zákona o ISVS ako: „*informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby.“* V prípade pojmu informačný systém došlo k zmene, nakoľko informačný systém predstavuje v zmysle § 2 ods. 2 zákona o ITVS: „*funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov.*“[42] V porovnaní s definíciou pojmu informačný systém v zmysle zrušeného zákona o ISVS nemusia byť technické prostriedky a programové prostriedky súčasťou informačného systému a taktiež tieto prostriedky nemôžu poskytovať iný informačný systém.

Bezpečnosť ITVS je v zákone o ITVS upravená v § 18 až § 23. Predmetný zákon upravuje bezpečnosť ITVS v oblasti:

- plánovania a organizácie (§ 19),

[42] V zmysle § 2 ods. 1 písm. a) zákona o ISVS bol informačný systém definovaný ako: „*funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov, ktoré sú súčasťou informačného systému alebo ktoré informačnému systému poskytuje iný informačný systém.*“

- obstarávania a implementácie (§ 20),
- prevádzky, servisu a podpory (§ 21),
- monitoringu a hodnotenia (§ 22),

V § 18 zákona o ITVS sú základné ustanovenia týkajúce sa situácie kedy je správca aj PZS v zmysle zákona o KB. V § 23 predmetného zákona sú upravené osobitné opatrenia na úseku bezpečnosti ITVS (napr. bezpečnostný projekt).

Správcom ITVS je v zmysle § 2 ods. 5 zákona o ITVS ten orgán riadenia[43], ktorého za správcu ITVS ustanoví zákon alebo je ustanovený na základe zákona o ITVS. Povinnosť správcu zabezpečiť riadenie bezpečnosti je zakotvená v § 14 ods. 1 písm. i) zákona o ITVS. V súvislosti s bezpečnostnými opatreniami je správca povinný:

- identifikovať potrebné bezpečnostné opatrenia (§ 19 ods. 1 písm. e) zákona o ITVS),
- určiť prostriedky na zabezpečenie implementácie a riadneho fungovania bezpečnostných opatrení (§ 19 ods. 1 písm. h) zákona o ITVS),
- realizovať bezpečnostné opatrenia (§ 19 ods. 3 písm. c) zákona o ITVS).

Z pohľadu správcu ITVS bude dôležité, aké bezpečnostné opatrenia musí prijať a realizovať a taktiež, ktorý právny predpis má aplikovať pri prijímaní konkrétnych bezpečnostných opatrení. V zmysle § 18 ods. 1 zákona o ITVS je správca, ktorý je zároveň aj PZS povinný prijať a realizovať bezpečnostné opatrenia vo vzťahu k ISVS v jeho správe v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov v zmysle § 20 zákona o KB. Inými slovami, vo všeobecnosti platí, ak je správca aj PZS v zmysle zákona o KB, prijíma a realizuje bezpečnostné opatrenia v zmysle zákona o KB.

Povinnosti správcov ITVS v oblasti bezpečnosti ITVS budú detailne upravené vo vykonávacom právnom predpise, ktorý nahradí výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch

[43] Taxatívny zoznam orgánov riadenia je uvedený v § 5 ods. 2 zákona o ITVS.

pre informačné systémy verejnej správy. Obsah bezpečnostných opatrení v novej vyhláške by mal reflektovať už existujúce bezpečnostné opatrenia, ktoré sú správcovia povinní realizovať.

3.2 NOVÁ VYHLÁŠKA

Dôležitým aspektom, ktorý ovplyvní vytvorenie právneho rámca bezpečnosti ITVS, bude prijatie vykonávacieho právneho predpisu, konkrétne vyhlášky. Predmetná vyhláška bude v zmysle § 31 písm. a) a i) zákona o ITVS upravovať:

- jednotlivé kategórie ITVS a podrobnosti o spôsobe zaraďovania do týchto kategórií,
- podrobnosti o bezpečnosti ITVS podľa § 18 až 23, obsahu bezpečnostných opatrení, obsahu a štruktúre bezpečnostného projektu a rozsah bezpečnostných opatrení v závislosti od klasifikácie informácií a od kategorizácie sietí a informačných systémov.

Klasifikácia informácii je prejavom hodnoty a statusu informácie danej organizácie. S tým priamo súvisí aj určenie, kto je vlastníkom informácií.[44] Jednotlivé kategórie ITVS a podrobnosti o spôsobe zaraďovania do týchto kategórií sa vykoná v zmysle § 31 písm. a) zákon o ITVS s použitím klasifikácie informácií a kategorizácie sietí a informačných systémov v zmysle zákona o KB.[45]

V súvislosti s klasifikáciou informácií vznikajú správcovi v zmysle zákona o ITVS viacero povinností. Správca v zmysle § 19 ods. 1 písm. c) zákona o ITVS zavedie a udržiava systém riadenia informačnej bezpečnosti, ktorý zabezpečí identifikovanie aktív v ITVS. Navyše správca v zmysle § 15 ods. 8 písm. a) a c) zákona o ITVS identifikuje a udržiava zoznam svojich aktív a taktiež identifikuje časti aktív, ktorých nedostupnosť alebo znížená

[44] WONG, H. *Cyber Security: Law and Guidance.* Bloomsbury Professional, 2018, s. 456.

[45] Bližšie pozri: vyhláška č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

kvalita má zásadný vplyv na poskytovanie služieb verejnej správy, služieb vo verejnom záujme alebo verejných služieb.[46]

V súvislosti s kategorizáciou ISVS platí, že správca má v zmysle § 19 ods. 5 písm. a) zákona o ITVS povinnosť určiť kategóriu ISVS, do ktorej bude z hľadiska klasifikácie informácií a kategorizácie sietí a informačných systémov patriť už pri plánovaní vytvorenia alebo nadobudnutí ISVS.

V súvislosti s bezpečnostným projektom platí, že správca je povinný v zmysle § 23 ods. 2 zákona o ITVS vypracovať bezpečnostný projekt vždy pre ISVS, ktorý je z pohľadu klasifikácie informácií a kategorizácie sietí a informačných systémov v najvyššej kategórii z hľadiska jeho významnosti, funkcie a účelu použitia s ohľadom na potrebu zabezpečenia ochrany dôvernosti a integrity a zabezpečenia dostupnosti a úrovne činností vykonávaných s jeho použitím. Inými slovami, správca je povinný vypracovať bezpečnostný projekt pre ITVS v jeho pôsobnosti, ak je predmetná ITVS zaradená v najvyššej kategórii. Výnimkou z tohto pravidla je situácia, kedy bezpečnostný audit alebo hodnotenie zraniteľnosti vykonané orgánom vedenia zistí riziko alebo hrozbu pre ITVS. V takomto prípade je správca povinný v zmysle § 23 ods. 3 písm. d) zákona o ITVS vypracovať bezpečnostný projekt bez ohľadu na kategorizáciu ITVS.

3.3 BEZPEČNOSŤ ISVS V ZÁKONE O KB

Na bezpečnosť ISVS sa možno pozerať aj z pohľadu zákona o KB. Predmetný zákon stanovil, že medzi základné služby možno zaradiť aj ISVS. Národný bezpečnostný úrad (ďalej len „NBÚ“) zaraďuje základnú službu - ISVS, do zoznamu základných služieb a jej prevádzkovateľa do registra PZS v spolupráci s príslušným ústredným orgánom. Príslušným ústredným orgánom pre oblasť ISVS je Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (ďalej len „ÚPVII“), ktorý má v sektore verejná správa v pôsobnosti podsektor ISVS.

V praxi v súčasnosti zatiaľ nedochádza k zaraďovaniu všetkých ISVS do zoznamu základných služieb a ich správcov do registra PZS, čo odzrkadľuje

[46] Bližšie k pojmom služba verejnej správy, služba vo verejnom záujme a verejná služba pozri § 3 zákona o ITVS.

požiadavku smernice NIS na PZS, ktorý má poskytovať službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností.[47] Ak by došlo k zaradeniu všetkých ISVS do zoznamu základných služieb, nebola by spomínaná požiadavka naplnená, nakoľko mnoho ISVS neposkytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností.

Konkrétne bezpečnostné opatrenia, ktoré musí PZS splniť sú stanovené v § 20 zákona o KB a vyhláške NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

3.3.1 POSTAVENIE A POVINNOSTI PZS

V súvislosti s vyššie uvedeným je potrebné ozrejmiť, akým spôsobom môže byť správca ITVS zaradený do registra PZS a jeho ISVS do zoznamu základných služieb. V zmysle zákona o KB existuje niekoľko spôsobov ako dôjde k zaradeniu základnej služby do príslušného zoznamu a zaradeniu PZS do príslušného registra.[48]

V prípade základných služieb a ich prevádzkovateľov platí, že ak entita zistí, že došlo k prekročeniu identifikačných kritérií prevádzkovanej služby a takáto entita patrí do niektorého zo sektorov podľa prílohy č. 1 zákona o KB, je povinná urobiť oznámenie do 30 dní odo dňa, keď sa o prekročení identifikačných kritérií dozvedela. Takéto oznámenie obsahuje konkrétne informácie a je adresované NBÚ. Právny základ pre zaradenie základnej služby do zoznamu základných služieb a PZS do registra PZS závisí od jednotlivých druhov základných služieb.

Slovenský zákonodarca definuje tri druhy základných služieb. V zmysle § 3 písm. k) zákona o KB je základnou službou služba, ktorá je zaradená v zozname základných služieb a:

[47] Pozri čl. 5 ods. 2 smernice NIS.

[48] PZS je v zmysle § 19 ods. 1 zákona o KB povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra PZS prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté.

A. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohyč. 1 zákona o KB,
B. je informačným systémom verejnej správy[49], alebo
C. je prvkom kritickej infraštruktúry[50].

V prípade ak ide o zaradenie základnej služby typu A platí, že NBÚ zaradí túto službu do zoznamu základných služieb a jej prevádzkovateľa do registra PZS:

a) na základe oznámenia prevádzkovateľom tejto služby,
b) na základe podnetu ústredného orgánu, ak došlo k prekročeniu identifikačných kritérií prevádzkovanej služby podľa § 18 zákona o KB,
c) z vlastnej iniciatívy, ak sa NBÚ dozvedel o prekročení identifikačných kritérií prevádzkovanej služby podľa § 18 zákona o KB a nedošlo k postupu podľa písmena a) alebo písmena b).[51]

V prípade základných služieb typu B (služba ako ISVS) platí, že NBÚ v spolupráci s príslušným ústredným orgánom zaradí základnú službu do zoznamu základných služieb a jej prevádzkovateľa do registra PZS.[52]

V súvislosti so základnými službami typu C platí, že NBÚ zaradí takúto základnú službu do zoznamu základných služieb a jej prevádzkovateľa do registra PZS zo zákona.[53]

Zaradenie základnej služby do zoznamu základných služieb a jej prevádzkovateľa do registra PZS oznámi NBÚ prevádzkovateľovi tejto služby prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.[54]

---

[49] § 2 ods. 1 písm. b) zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov.

[50] § 2 písm. a) zákona č. 45/2011 Z. z. o kritickej infraštruktúre.

[51] § 17 ods. 2 zákona o KB.

[52] Tamtiež, § 17 ods. 3.

[53] Tamtiež, § 17 ods. 4.

[54] Tamtiež, § 17 ods. 5. Oznámenie nemá charakter individuálneho právneho aktu. Na zaradenie služby do zoznamu základných služieb a jej prevádzkovateľa do registra PZS sa nevzťahuje zákon č. 71/1967 Zb. o správnom konaní (správny poriadok), čo znamená, že zaradený subjekt nemôže použiť opravné prostriedky v zmysle správneho poriadku.

Aby došlo k zaradeniu základnej služby do zoznamu základných služieb a jej prevádzkovateľa do registra PZS, musí príslušná základná služba, ktorú poskytuje entita prekročiť identifikačné kritériá prevádzkovanej služby. V zmysle § 18 zákona o KB sa identifikačné kritéria prevádzkovanej služby delia na dopadové kritéria a špecifické sektorové kritériá.

Dopadové kritériá vychádzajú z článku 6 smernice NIS, ktorý upravuje faktory pre určenie závažnosti rušivého vplyvu. Podrobnosti o dopadových a špecifických sektorových kritériách pre základnú službu sú upravené vo vyhláške NBÚ č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby).[55] Na tomto mieste je potrebné podotknúť, že európsky zákonodarca určuje identifikačné kritéria PZS a nie pre základné služby. Avšak slovenský zákonodarca upravuje v zákone KB a predmetnej vyhláške identifikačné kritéria prevádzkovanej služby a ak entita tieto kritéria prekročí následne možno hovoriť o tom, že má postavenie PZS.

Z praktického hľadiska je však problematickejšia skutočnosť, že vyššie uvedená vyhláška určuje identifikačné kritériá len pre PZS typu A. Inými slovami, pri prevádzkovateľoch základnej služby typu B a C sa neskúmajú dopadové kritériá, ktoré vychádzajú z článku 6 smernice NIS. V tejto súvislosti je evidentný jasný rozpor s článkom 5 ods. 2 smernice NIS, v zmysle ktorého musí PZS kumulatívne spĺňať tieto kritériá:

- subjekt poskytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností;
- poskytovanie tejto služby je závislé od sietí a informačných systémov a
- incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby.

[55] V zmysle § 2 predmetnej vyhlášky platí, že: „*prevádzkovaná služba spĺňa identifikačné kritériá základnej služby, ak spĺňa aspoň jedno dopadové kritérium a aspoň jedno špecifické sektorové kritérium, ak je uvedené v prílohe č. 1.*“ Avšak, v zmysle § 18 ods. 4 zákona o KB platí, že: „*ak prevádzkovateľ služby podľa prílohy č. 1 zistí, že došlo k prekročeniu špecifických sektorových kritérií, oznámi to úradu do 30 dní odo dňa, keď prekročenie zistil v rozsahu podľa § 17 ods. 5 aj v prípade, ak neprekročí dopadové kritériá.*“ Neskoršie citované ustanovenie nevyžaduje naplnenie dopadového kritéria, čo je v rozpore so smernicou NIS.

V prípade ak sa neskúma posledné spomenuté kritérium, a teda závažný rušivý vplyv, nemožno hovoriť o PZS v zmysle smernice NIS.

Skutočnosť či správca ISVS bude zároveň aj v postavení PZS v zmysle zákona o KB, bude mať dopad najmä na to či tento subjekt bude pri realizácii bezpečnostných opatrení postupovať v zmysle zákona o ITVS alebo zákona o KB. Nejasnosť tejto situácie možno demonštrovať na prepojení zákona o ITVS a zákona o KB.

3.4 PREPOJENIE ZÁKONA O ITVS A ZÁKONA O KB

Ako už bolo spomenuté, ak je správca ITVS aj v postavení PZS v zmysle zákona o KB, prijíma a realizuje bezpečnostné opatrenia v zmysle zákona o KB. Avšak môže dôjsť k situácii, kedy správca v pozícii PZS nebude realizovať bezpečnostné opatrenia v zmysle zákona o KB ale v zmysle zákona o ITVS.

V zmysle § 18 ods. 2 zákona o ITVS platí, že: *„obsah bezpečnostných opatrení vo vzťahu k informačným systémom verejnej správy a spôsob a rozsah ich prijímania a realizácie v súlade s osobitným predpisom.“* Týmto osobitným predpisom je zákon o KB, konkrétne jeho *§ 2* ods. 2 písm. e), v zmysle ktorého sa zákon o KB nevzťahuje na: *„požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona.“* Predmetným osobitným predpisom je už zrušený zákon o ISVS.[56] Na základe vyššie uvedeného možno konštatovať, že v prípade ak zákon o ITVS stanoví pre správcu, ktorý je zároveň aj PZS, striktnejšie bezpečnostné opatrenia, bude musieť správca prijať a realizovať bezpečnostné opatrenia v zmysle zákona o ITVS. V praxi to bude pre správcu, ktorý je aj PZS znamenať, že bude musieť porovnávať bezpečnostné opatrenia v zmysle zákona o KB a zákona o ITVS.

V tejto súvislosti by bolo viac ako vhodné, aby ÚPVII ako orgán vedenia v zmysle zákona o ITVS prijal výkladové stanoviská v zmysle § 9 ods. 1 písm. a) zákona o ITVS alebo metodické usmernenia v zmysle § 8 ods. 1

[56] V zmysle § 33 ods. 1 zákona o ITVS: *„informačné systémy verejnej správy podľa doterajších predpisov sú informačnými systémami verejnej správy podľa tohto zákona.“*

písm. a) zákona o ITVS. Výkladové stanoviská alebo metodické usmernenia by mohli prispieť k tomu, aby správcovia vedeli identifikovať, prijať a realizovať konkrétne bezpečnostné opatrenia v zmysle príslušných právnych predpisov, čo by mohlo dopomôcť k právnej istote.

Ak správca nie je PZS, prijíma a realizuje bezpečnostné opatrenia v zmysle zákona o ITVS.

Možno konštatovať, že bezpečnostné opatrenia upravené v zákone o ITVS sa aplikujú na ISVS ktoré neboli zaradené do zoznamu základných služieb v zmysle zákona o KB a taktiež na tie, ktoré boli zaradené do zoznamu základných služieb v zmysle zákona o KB, ale bezpečnostné opatrenia stanovené v zákone o ITVS majú za cieľ dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako v zákone o KB.

4. HLÁSENIE BEZPEČNOSTNÝCH INCIDENTOV

Akokoľvek striktné bezpečnostné opatrenia nemôžu zabrániť tomu, že hrozba (napr. v podobe kybernetického útoku) zneužije zraniteľnosť ISVS a spôsobí narušenie požadovaného stavu aktíva, čím dôjde k bezpečnostnému incidentu. Takáto situácia znamená, že správca ITVS je povinný takýto bezpečnostný incident hlásiť konkrétnej entite. Správca je povinný hlásiť kybernetické bezpečnostné incidenty v zmysle zákona o ITVS a v prípade ak je aj PZS, tak aj kybernetické bezpečnostné incidenty v zmysle zákona o KB. Navyše, za určitých podmienok, môže kybernetický bezpečnostný incident spôsobiť aj porušenie ochrany osobných v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) 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“).

4.1 HLÁSENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV V ZMYSLE ZÁKONA O KB

PZS je v zmysle § 19 ods. 6 písm. b) zákona o KB povinný bezodkladne hlásiť závažný kybernetický bezpečnostný incident. Rovnakú povinnosť musí PZS splniť aj v zmysle § 24 ods.1 predmetného zákona. PZS

identifikuje závažný kybernetický bezpečnostný incident na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov. V zmysle § 24 ods. 2 zákona o KB sa závažné kybernetické bezpečnostné incidenty členia na kategórie prvého, druhého a tretieho stupňa. Stanovenie konkrétneho stupňa závisí od nasledujúcich faktorov:

- počtu používateľov základnej služby alebo digitálnej služby zasiahnutých kybernetickým bezpečnostným incidentom,
- dĺžky trvania kybernetického bezpečnostného incidentu,
- geografického rozšírenia kybernetického bezpečnostného incidentu,
- stupňa narušenia fungovania základnej služby alebo digitálnej služby,
- rozsahu vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu.[57]

Presná špecifikácia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov je predmetom vyhlášky NBÚ č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov. PZS má povinnosť hlásiť kybernetické bezpečnostné incidenty prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.[58]

Na tomto mieste je potrebné podotknúť, že v zmysle čl. 14 ods. 3 smernice NIS má PZS povinnosť bezodkladne hlásiť incidenty, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú. S cieľom určiť závažnosť vplyvu incidentu sa zohľadňujú konkrétne parametre osobitne pre základné služby a digitálne služby.

Parametre pre určenie závažnosti vplyvu incidentu na kontinuitu základných služieb, ktoré PZS poskytujú sú najmä: počet používateľov postihnutých narušením základnej služby; dĺžka trvania incidentu a geografické rozšírenie z hľadiska oblasti, ktorú incident postihol.[59]

---

[57] § 24 ods. 2 písm. a) - e) zákona o KB.

[58] § 24 ods. 4 a § 25 ods. 1 zákona o KB.

[59] Čl. 14 ods. 4 smernice NIS.

Pre určenie závažnosti vplyvu na poskytované digitálne služby sú najmä tieto parametre: počet používateľov postihnutých incidentom, najmä používateľov využívajúcich danú službu na účely poskytovania vlastných služieb; dĺžka trvania incidentu; geografické rozšírenie z hľadiska oblasti, ktorú incident postihol; stupeň narušenia fungovania služby; rozsah vplyvu na hospodárske a spoločenské činnosti.[60]

V zákone o KB boli parametre pre určenie závažnosti vplyvu incidentu na kontinuitu základných služieb a pre určenie závažnosti vplyvu na poskytované digitálne služby v zmysle smernice NIS spojené do jedného, a to pre účely stanovenia stupňa závažného kybernetického bezpečnostného incidentu.

4.1.1 JEDNOTNÝ INFORMAČNÝ SYSTÉM KYBERNETICKEJ BEZPEČNOSTI

Jednotný informačný systém kybernetickej bezpečnosti predstavuje základný komunikačný kanál medzi NBÚ a ostatnými entitami v oblasti kybernetickej bezpečnosti. NBÚ je správcom a prevádzkovateľom predmetného informačného systému. NBÚ sprístupní jednotný informačný systém kybernetickej bezpečnosti do 18 mesiacov od účinnosti predmetného zákona.[61]

Jednotný informačný systém kybernetickej bezpečnosti obsahuje komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania. V súvislosti s prístupom k jednotnému informačnému systému kybernetickej bezpečnosti má tento informačný systém verejnú časť a neverejnú časť. Verejná časť obsahuje príslušné registre PZS, poskytovateľov digitálnych služieb, ústredných orgánov, kybernetických bezpečnostných incidentov a zoznamy základných služieb, digitálnych služieb a akreditovaných jednotiek CSIRT.[62] Do neverejnej časti jednotného informačného systému kybernetickej bezpečnosti majú prístup v elektronickej forme, v reálnom čase a v rozsahu určenom NBÚ alebo

[60] Tamtiež, čl. 16 ods. 4.

[61] § 34 ods. 1 zákona o KB.

[62] Tamtiež § 8 ods. 2. [on-line] https://www.nbu.gov.sk/kyberneticka-bezpecnost/jednotny-informacny-system-kybernetickej-bezpecnosti/index.html [citované 30.9.2019]

osobitným predpisom na základe vecnej pôsobnosti ústredný orgán, jednotka CSIRT (zaradená v zozname akreditovaných jednotiek CSIRT), PZS, poskytovateľov digitálnych služieb, Národná banka Slovenska, Úrad na ochranu osobných údajov Slovenskej republiky a iný orgán verejnej moci rozhodnutím NBÚ.[63]

Z dikcie zákona o KB vyplýva, že jednotný informačný systém kybernetickej bezpečnosti je primárnym komunikačným kanálom. Avšak, je potrebné myslieť aj na situácie, kedy by jednotný informačný systém kybernetickej bezpečnosti nemohol plniť svoj účel, napr. z dôvodu incidentu, ktorý by ochromil alebo znefunkčnil jeho prevádzku. Predpokladám, že pre tieto prípady by sa mal aplikovať § 24 ods. 6 zákona o KB. V zmysle predmetného ustanovenia platí, že NBÚ môže uzatvoriť písomnú zmluvu o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov s PZS. Podobným spôsobom môže NBÚ uzavrieť zmluvu aj s poskytovateľom digitálnych služieb.[64]

4.2 HLÁSENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV V ZMYSLE ZÁKONA O ITVS

V zmysle § 23 ods. 3 zákona o ITVS sú orgán riadenia podľa § 5 ods. 2 písm. a) a b)[65] a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti povinní:

- ak sú zaradení do registra PZS podľa osobitného predpisu (ISVS ako základná služba podľa zákona o KB), nahlasovať spôsobom podľa osobitného predpisu (prostredníctvom jednotného informačného systému kybernetickej bezpečnosti) aj kybernetický bezpečnostný incident, na

[63] Tamtiež, § 8 ods. 5.

[64] Tamtiež, § 25 ods. 3.

[65] Orgán riadenia je podľa § 5 ods. 2 písm. a) a b) zákona o ITVS: ministerstvo a ostatný ústredný orgán štátnej správy, 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 elektronických komunikácií a poštových služieb, Dopravný úrad, Úrad pre reguláciu sieťových odvetví a iný štátny orgán.

ktorý sa nevzťahuje povinnosť nahlasovania podľa osobitného predpisu (§ 24 ods. 1 zákona o KB),

- ak nie sú zaradení do registra PZS, nahlasujú takýto kybernetický bezpečnostný incident ÚPVII ním určeným spôsobom,
- určiť jeden kontaktný bod na nahlasovanie kybernetických bezpečnostných incidentov.

V zmysle § 33 ods. 5 zákona o ITVS platí, že orgán riadenia podľa § 5 ods. 2 písm. a) a b) a rozpočtová organizácia a príspevková organizácia v jeho zriaďovateľskej pôsobnosti, ktorí sú zaradení do registra PZS podľa osobitného predpisu, nahlasujú do uplynutia 30 dní odo dňa zriadenia a uvedenia do prevádzky jednotného informačného systému kybernetickej bezpečnosti [66] kybernetický bezpečnostný incident podľa § 23 ods. 3 písm. a) orgánu vedenia, ktorým je ÚPVII, ním určeným spôsobom.

Zákon o ITVS ukladá v § 23 ods. 4 zákona o ITVS plniť povinnosti v zmysle § 23 ods. 3 písm. a) aj ostatným orgánom riadenia[67]. Inými slovami, aj ostatné orgány riadenia, ak sú zaradení do registra PZS, sú

---

[66] JISKB musí byť uvedený do prevádzky najneskôr 18.10.2019 v zmysle § 34 ods. 1 zákona o KB.

[67] Ostatné orgány riadenia možno chápať ako tie, ktoré neboli uvedené v § 23 ods. 3, a teda ide o orgány riadenia podľa § 5 ods. 2 písm. c) – h):

„c)obec a vyšší územný celok,

d)Kancelária Národnej rady Slovenskej republiky, Kancelária prezidenta Slovenskej republiky, Kancelária Ústavného súdu Slovenskej republiky, Kancelária Najvyššieho súdu Slovenskej republiky, Kancelária Súdnej rady Slovenskej republiky, Kancelária verejného ochrancu práv, Úrad komisára pre deti, Úrad komisára pre osoby so zdravotným postihnutím, Ústav pamäti národa, Sociálna poisťovňa, zdravotné poisťovne, Tlačová agentúra Slovenskej republiky, Rozhlas a televízia Slovenska, Rada pre vysielanie a retransmisiu,

e)právnická osoba v zriaďovateľskej pôsobnosti alebo zakladateľskej pôsobnosti orgánu riadenia uvedeného v písmenách a) až d),

f)komora regulovanej profesie a komora, na ktorú je prenesený výkon verejnej moci s povinným členstvom,

g)osoba neuvedená v písmenách a) až f) okrem Národnej banky Slovenska, na ktorú je prenesený výkon verejnej moci alebo ktorá plní úlohy na úseku preneseného výkonu štátnej správy podľa osobitných predpisov,

h)záujmové združenie právnických osôb DataCentrum elektronizácie územnej samosprávy Slovenska, ktorého jedinými členmi sú Ministerstvo financií Slovenskej republiky a Združenie miest a obcí Slovenska.“

povinné nahlasovať prostredníctvom jednotného informačného systému kybernetickej bezpečnosti aj kybernetický bezpečnostný incident, na ktorý sa nevzťahuje povinnosť nahlasovania podľa zákona o KB. Taktiež, ak nie sú zaradení do registra PZS, nahlasujú kybernetický bezpečnostný incident, ktorý nespĺňa kritériá podľa zákona o KB ÚPVII ním určeným spôsobom. A v neposlednom rade sú ostatné orgány riadenia povinné určiť jeden kontaktný bod na nahlasovanie kybernetických bezpečnostných incidentov.

V prípade ak správca nie je PZS v zmysle zákona o KB, má možnosť nahlasovať aj závažné kybernetické bezpečnostné incidenty podľa § 24 ods. 1 zákona o KB, resp. príslušnej vyhlášky, a to prostredníctvom inštitútu dobrovoľného hlásenia kybernetických bezpečnostných incidentov v zmysle § 26 ods. 1 zákona o KB. V recitáli 67 smernice NIS sa uvádza, že subjekty, ktoré neboli určené ako PZS a nie sú ani poskytovateľmi digitálnych služieb, majú možnosť dobrovoľne oznamovať incidenty, ktoré majú významný vplyv na služby, ktoré poskytujú, ak sa domnievajú, že je vo verejnom záujme oznámiť, že k takýmto incidentom došlo.

4.3 PORUŠENIE OCHRANY OSOBNÝCH ÚDAJOV V ZMYSLE GDPR

V praxi môže nastať situácia, kedy si ten istý subjekt bude plniť svoju oznamovaciu povinnosť v zmysle zákona o KB, resp. zákona o ITVS a zároveň si musí splniť oznamovaciu povinnosť v zmysle GDPR. Inými slovami, subjekt bude nahlasovať rovnakú skutočnosť rôznym inštitúciám. V podmienkach Slovenskej republiky by išlo o splnenie si oznamovacej povinnosti voči NBÚ, resp. ÚPVII a Úradu na ochranu osobných údajov.[68]

[68] Príkladom entity, ktorá môže byť správcom v zmysle zákona o ITVS a zároveň aj prevádzkovateľom základných služieb v zmysle zákona KB a prevádzkovateľom v zmysle GDPR je napr. Ministerstvo vnútra Slovenskej republiky vo vzťahu k informačnému systému s názvom Evidencia vozidiel.

GDPR ukladá prevádzkovateľovi[69] a sprostredkovateľovi[70] povinnosť oznamovať porušenie ochrany osobných údajov.[71] Za porušenie ochrany osobných údajov považuje: *„porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim“*.[72]

Je potrebné podotknúť, že k splneniu si oznamovacej povinnosti v zmysle GDPR dôjde len v prípadoch, keď došlo k porušeniu ochrany osobných údajov.

V nasledujúcej tabuľke uvádzam prehľad oznamovacích povinností jednotlivých subjektov v zmysle GDPR.

Povinnosť	Lehota	Výnimka
Prevádzkovateľ oznamuje dozornému orgánu (čl. 33 ods. 1 GDPR)	Bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o porušení ochrany osobných údajov dozvedel	Oznámenie sa nevyžaduje, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb.
Sprostredkovateľ oznamuje prevádzkovateľovi (čl. 33 ods. 2 GDPR)	Bez zbytočného odkladu po tom, čo sa o porušení ochrany osobných údajov dozvedel	Oznámenie sa nevyžaduje, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva

[69] Prevádzkovateľ je v zmysle čl. 4 bodu 7 GDPR definovaný ako: *„fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu.“*

[70] Sprostredkovateľom je v zmysle čl. 4 bodu 8 GDPR: *„fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.“*

[71] Bližšie k pojmom prevádzkovateľ a sprostredkovateľ pozri: MESARČÍK, M. *Základné pojmy Nariadenia*. In Všeobecné nariadenie o ochrane osobných údajov. Praha: C.H. Beck, 2018, s. 123-186.

[72] Čl. 4 ods. 12 GDPR.

		a slobody fyzických osôb.
Prevádzkovateľ oznamuje dotknutej osobe (čl. 34 ods. 1 GDPR)	Bez zbytočného odkladu	Oznámenie sa nevyžaduje ak: a) prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a tieto opatrenia uplatnil na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä tie opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup, ako je napríklad šifrovanie; b) prevádzkovateľ prijal následné opatrenia, ktorými sa zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb uvedené v odseku 1 pravdepodobne už nebude mať dôsledky; c) by to vyžadovalo neprimerané úsilie. V takom prípade dôjde namiesto toho k informovaniu verejnosti alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom.

Zdroj: vlastné spracovanie

K prelínaniu sa oznamovacej povinnosti v zmysle GDPR a zákona o KB, resp. zákona o ITVS, môže dôjsť v mnohých prípadoch. Ak berieme do úvahy koncept kybernetickej bezpečnosti v zmysle zákona o KB, kedy konanie, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, by mohlo zároveň spôsobiť porušenie ochrany osobných údajov v zmysle GDPR.

V teoretickej rovine možno povedať, že narušenie ochrany osobných údajov v zmysle GDPR sa spája najmä s narušením bezpečnostnej požiadavky súkromnosti, ktorá znamená, že k osobným údajom majú prístup len tie osoby, ktoré majú na to oprávnenie. Na druhej strane, zákon o KB upriamuje pozornosť na bezpečnostné požiadavky ako dôvernosť, integrita, dostupnosť a autentickosť. Napr. narušenie integrity služby, poskytovanej prostredníctvom sietí a informačných systémov a údajov, ktoré sú v rámci jej poskytovania spracované, môže znamenať aj porušenie ochrany osobných údajov v zmysle GDPR, nakoľko v mnohých prípadoch pôjde o narušenie integrity osobných údajov.

Ako už bolo vyššie uvedené, hlásený kybernetický bezpečnostný incident môže mať charakter porušenia ochrany osobných údajov. V praxi by bolo preto vhodné, aby si subjekty mohli plniť oznamovaciu povinnosť v zmysle zákona o KB, resp. zákona o ITVS a GDPR jedným oznámením. Na tieto účely by mohol slúžiť aj jednotný informačný systém kybernetickej bezpečnosti. Takéto riešenie v zásade potvrdzuje aj ust. § 8 ods. 5 písm. e) zákona o KB, v zmysle ktorého má Úrad na ochranu osobných údajov prístup k neverejnej časti jednotného informačného systému kybernetickej bezpečnosti. V tejto súvislosti je potrebné zabezpečiť, aby oznamovanie porušenia ochrany osobných údajov, ktoré sa bude vykonávať prostredníctvom oznámenia v zmysle zákona o KB, obsahovalo náležitosti oznámenia v zmysle GDPR. Preto je potrebné zabezpečiť, aby Úrad na ochranu osobných údajov bol adresátom a spracovateľom len tých údajov, ktoré sa týkajú porušenia ochrany osobných údajov.

Povinnosť hlásiť konkrétny typ kybernetických bezpečnostných incidentov, konkrétnym subjektom v zmysle zákona o ITVS, zákona o KB a GDPR uvádzam v nasledujúcej súhrnnej tabuľke.

	Zákon o ITVS I	**Zákon o ITVS II**	**Zákon o KB**	**GDPR**
Subjekt	Orgán riadenia (zároveň aj PZS)	Orgán riadenia (nie je PZS)[73]	PZS (zároveň aj správca ISVS)	Prevádzkovateľ
Druh bezpečnostného incidentu (BI)	Kybernetický BI	Kybernetický BI	Závažný kybernetický BI	Porušenie ochrany osobných údajov
Komu a akým spôsobom sa oznamuje bezpečnostný incident (BI)	NBÚ (JISKB)	Orgánu vedenie (ÚPVII), ním určeným spôsobom	NBÚ (JISKB)	Úradu na ochranu osobných údajov[74]
Lehota			Bezodkladne	Bez zbytočného odkladu/72 hodín

Zdroj: vlastné spracovanie

5. ZÁVER

Pri vhodnom nastavení a realizácii bezpečnostných opatrení v zmysle zákona o ITVS a zákona o KB budú ISVS dostatočne chránené pred rôznymi hrozbami (či už z fyzického sveta alebo z kybernetického priestoru). Avšak, pre dosiahnutie potrebnej úrovne bezpečnosti ISVS je potrebné zabezpečiť, aby správcovia tieto opatrenia vedeli identifikovať, prijať a realizovať.

[73] Orgán riadenia, ktorý nie je PZS môže hlásiť kybernetické bezpečnostné incidenty podľa zákona o KB prostredníctvom dobrovoľného hlásenia.

[74] Povinnosť hlásiť porušenie ochrany osobných údajov vznikne len za predpokladu, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb.

Prijatie novej legislatívy v oblasti bezpečnosti ISVS je nepochybne krokom vpred, avšak v otázke právnej istoty prináša nová legislatíva niekoľko problémov. V prvom rade, zaraďovanie všetkých ISVS do zoznamu základných služieb a ich správcov do registra PZS v zmysle zákona o KB odporuje smernici NIS, nakoľko nie všetky ISVS, resp. ich správcovia poskytujú službu, ktorá má zásadný význam z pohľadu zachovania hospodárskych alebo spoločenských činností. Navyše, ak sa pri zaraďovaní správcov ITVS do registra PZS neskúmajú dopadové kritériá, ktoré vychádzajú z článku 6 smernice NIS, dochádza k jasnému porušeniu smernice NIS.

Prepojenosť zákona o ITVS a zákona o KB môže významným spôsobom ovplyvniť dosiahnutie dostatočnej úrovne bezpečnosti ISVS. V praxi môžu nastať situácie, kedy budú subjekty v právnom postavení správcov ITVS alebo v právnom postavení PZS v istých momentoch porovnávať striktnosť bezpečnostných opatrení v zmysle zákona o ITVS a zákona o KB. V tejto súvislosti bude potrebné, aby ÚPVII prijal výkladové stanoviská alebo metodické usmernenia, ktoré by mohli prispieť k tomu, aby správcovia vedeli identifikovať, prijať a realizovať konkrétne bezpečnostné opatrenia v zmysle príslušných právnych predpisov, čo by mohlo dopomôcť k právnej istote.

K dosiahnutiu dostatočnej úrovne bezpečnosti ISVS by mohla dopomôcť aj kontrola realizácie bezpečnostných opatrení a následné sankcionovanie v prípade neplnenia si povinností v zmysle zákona o ITVS a zákona o KB. V tejto súvislosti je potrebné podotknúť, že cieľom zákona o ITVS a zákona o KB nie je represívne pôsobiť na správcov a PZS pri nesplnení si povinností, najmä v podobe nedostatočného realizovania bezpečnostných opatrení, resp. absencie realizovania bezpečnostných opatrení. V tejto súvislosti si dovolím tvrdiť, že zákon o ITVS a jeho vykonávací právny predpis bude upravovať len minimálne bezpečnostné opatrenia, ktoré je potrebné prijať a realizovať v závislosti od konkrétnej kategórie ITVS. Správcovia, ktorých ITVS budú zaradené do vyšších kategórií, budú povinní prijať striktnejšie bezpečnostné opatrenia v porovnaní s nižšími kategóriami ITVS. Taktiež je potrebné podotknúť, že už v súčasnosti sú správcovia

povinní plniť v zmysle výnosu Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy mnohé bezpečnostné opatrenia.

Predmetom spomínaného vykonávacie právneho predpisu bude taktiež pôsob zaradenia ITVS do konkrétnych kategórií a klasifikácia informácií. Vyhláška taktiež upraví obsah a rozsah bezpečnostných opatrení v závislosti od konkrétnej kategórie ITVS a obsah a štruktúru bezpečnostného projektu.

Ani tie najprísnejšie bezpečnostné opatrenia nemôžu zabrániť tomu, aby nedošlo ku kybernetickému bezpečnostnému incidentu. V takýchto prípadoch je zasiahnutý subjekt v zmysle zákona o ITVS, zákona o KB a GDPR povinný hlásiť konkrétny typ bezpečnostného incidentu, konkrétnemu subjektu. Subjekt či už v postavení PZS podľa zákona o KB, postavení správcu v zmysle zákona o ITVS alebo postavení prevádzkovateľa v zmysle GDPR si pred samotným hlásením musí uvedomiť, aký typ bezpečnostného incidentu má hlásiť, akým spôsobom, akému subjektu a v akej lehote. Bolo by viac ako vhodné, aby konkrétny subjekt mohol urobiť jedno hlásenie bezpečnostného incidentu, ktoré by bolo adresované zainteresovaným subjektom. V podmienkach Slovenskej republiky sa ako najvhodnejšie riešenie tejto situácie javí využitie jednotného informačného systému kybernetickej bezpečnosti, prostredníctvom ktorého by sa mohli hlásiť kybernetické bezpečnostné incidenty, ktoré nespĺňajú kritériá v zmysle zákona o KB, závažné kybernetické bezpečnostné incidenty podľa zákona o KB, ako aj oznámenia, ktoré majú charakter porušenia ochrany osobných údajov. Pre dosiahnutia tohto cieľa by bolo potrebné zosúladiť obsahové náležitosti formulárov, ktoré konkrétne subjekty využívajú pri hlásení konkrétnych typov bezpečnostných incidentov. K jednotnému informačnému systému kybernetickej bezpečnosti, resp. jeho neverejnej časti, kde by boli evidované jednotlivé hlásenia by mal prístup okrem NBÚ, Úradu na ochranu osobných údajov aj ÚPVII.

6. ZOZNAM LITERATÚRY

[1] ANDRAŠKO, J. a kol. *Zákon o kybernetickej bezpečnosti.* Komentár. Bratislava: Wolters Kluwer SR s.r.o. 2018, s. 544 s.

[2] ANDRAŠKO, J., MESARČÍK, M.: *Problematika GDPR v kontexte nariadenia eIDAS*. In Digitalizácia, zmeny vonkajšieho prostredia a spoločnosť budúcnosti. Bratislava, Právnická fakulta UK, 2018, s. 8-21.

[3] BAYUK, L. a kol.: *Cyber security policy guidebook*. Wiley, 2012, 270 s.

[4] BERTHOTY, Jakub a kol. : *Všeobecné nariadenie na ochranu údajov*. 1. vydanie. Praha : C.H. Beck, 2018.

[5] HAMELINK, C. J. *The ethics of cyberspace.* Sage, 2001, 224 s.

[6] KOLOUCH, J., BAŠTA, P. a kol. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o, 2019. 556 s.

[7] OLEJÁR, Daniel a kol.: *Manažment informačnej bezpečnosti a základy PKI*. Bratislava, 2015, 175 s.

[8] OLEJÁR, Daniel a kol.: *Informačná bezpečnosť.* Bratislava, 2013. 246 s.

[9] POLČÁK, R. *Informace a data v právu.* Revue pro právo a technologie 7, 2016, s. 67–91.

[10] POLČÁK, R. a kol. *Právo informačních technológií.* Praha: Wolters Kluwer ČR, 2018, s 656 s.

[11] POLČÁK, R. *Kybernetická bezpečnost jako aktuální fenomén českého práva.* Revue pro právo a technologie, 2015,č. 11, s. 95-149. [on-line]. Dostupné z: https://journals.muni.cz/revue/article/view/2980.

[12] POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s.

[13] TODOROV, D. *Mechanics of Users Identification and Authentication. Fundamentals of Identity Management.* USA: Auerbach Publications, 2007, 756 s. ISBN 978-1-4200-5219-0

[14] VAN DER HOF, Simone a kol.: *Framing Citizen's Identities: The construction of personal identities in new modes of government in the Netherlands.* Nijmegen: Wolf Legal Publishers, 2010, 258 s.

[15] VON SOLMS, R. a VAN NIEKERK, J. *From information security to cyber security. In* Computers & Security, 2013, roč. 38, s. 97-102

[16] WHITMAN, M, E. a MATTORD, H, J.: *Principles of Information security*. Boston: Course Technology, 2012, 617 s.

[17] WONG, H. *Cyber Security: Law and Guidance.* Bloomsbury Professional, 2018, 792 s.

[18] nariadenie Európskeho parlamentu a Rady (EÚ) 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)

[19] 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

[20] zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov

[21] zákon č. 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente)

[22] zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

[23] zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

[24] vyhláška NBÚ č. 164/2018 z. Z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby).

[25] vyhláška NBÚ č. 165/2018 Z. z. ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov

[26] vyhláška NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

[27] ISO/IEC 27001:2013 INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS

[28] ISO/IEC 27002:2013 INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- CODE OF PRACTICE FOR INFORMATION SECURITY CONTROLS

[29] ISO/IEC 27032:2012 *Information technology -- Security techniques -- Guidelines for cybersecurity*

[30] ISO/IEC 27000:2016 *Overview and vocabulary*