Ervín Šimko

**Legislatívny rámec k bezpečnosti informačných technológií**

**vo verejnej správe**

**Anotácia:** Autor sa v predkladanom príspevku zameral na bezpečnosť informačných technológií verejnej správy s dôrazom na jej legislatívne vymedzenie predovšetkým v zákone o informačných technológiách verejnej správy. Venoval sa tiež komparácií predchádzajúcej právnej úpravy a súčasného legislatívneho vymedzenia predmetnej problematiky, kde vyzdvihol pozitíva, ktoré so sebou nová právna úprava priniesla. V závere načrtol oblasti, ktoré si vyžadujú precíznejšiu úpravu zo strany zákonodarcu.

**Kľúčové slová:** informačné technológie, informačné systémy, kybernetická bezpečnosť, verejná správa, kybernetický priestor, analýza, rešerš, zhodnotenie

Prakticky všetky dôležité oblasti života spoločnosti v súčasnosti podstatne závisia od spoľahlivého fungovania systémov jej digitálneho priestoru, a preto zaistenie primeranej ochrany digitálneho priestoru je prioritným záujmom Slovenskej republiky. Keďže narušenie alebo zlyhanie jednej časti digitálneho priestoru môže ohroziť jeho inú podstatnú časť alebo aj celý digitálny priestor, zaistenie informačnej bezpečnosti digitálneho priestoru musí byť trvalé a komplexné, a to si vyžaduje systematický, koordinovaný a legislatívne podporený prístup všetkých zainteresovaných subjektov. Štát môže bezprostredne zaisťovať ochranu informačných systémov verejnej správy, z ktorých sú mnohé pre riadenia a chod štátu kľúčové. Preto je nevyhnutné, aby zákonodarca príslušnou legislatívou zabezpečil bezpečný priestor na využívanie a aplikáciu informačných technológií v celom IT priestore. Pri vhodnom nastavení a realizácii bezpečnostných opatrení v zmysle platnej legislatívy budú dostatočne chránené pred rôznymi hrozbami (či už z fyzického sveta alebo kybernetického priestoru).

V príspevku sme sa zamerali na legislatívny rámec informačných technológií v oblasti verejnej správy, kde často dochádza k výmene citlivých informácii. O to viac je preto potrebné danej problematike venovať dôslednú pozornosť. Spracovaniu príspevku budú aplikované viaceré vedecké metódy , pričom dominantnou bude analýza právnych predpisov, ako aj odbornej literatúry.

**Na úvod je potrebné definovať, čo je to kybernetická bezpečnosť. Je to** 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.[[1]](#footnote-1) O kybernetickej bezpečnosti hovoríme teda aj vtedy, ak máme na mysli bezpečnosť informačných technológií v oblasti verejnej správy. Slovenská legislatíva pre kybernetickú bezpečnosť je pomerne „mladá“. Na Národnú stratégiu pre informačnú bezpečnosť v SR z roku 2008 nadväzoval Akčný plán 2009 až 2013, v roku 2016 nasledovalo zriadenie národnej jednotky pre riešenie incidentov SK-CERT a koncepcia kybernetickej bezpečnosti 2015 – 2020 vytvorila inštitucionálny a právny rámec kybernetickej bezpečnosti. Slovenská republika pristúpila k povinnosti náležitej transpozície **smernice 2016/1148 o bezpečnosti sietí**

**a informačných systémov** (ďalej len „smernica NIS“)“ prostredníctvom**prijatia zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti**. Cieľom zákona je **zvýšiť bezpečnosť tých sietí**

**a informačných systémov,** na ktorých je postavené fungovanie hospodárskych, spoločenských a bezpečnostných záujmov Slovenskej republiky. V istom slova zmysle by sa dalo povedať, že podpornú funkciu k tomuto zákonu o kybernetickej bezpečnosti plní zákon o informačných systémoch verejnej správy, ktorý rozpracováva podrobnosti zo zákona o kybernetickej bezpečnosti vo svojich ustanoveniach s cieľom dosiahnuť vyššiu bezpečnosť sietí a informačných systémov. [[2]](#footnote-2)

Právna úprava ISVS a otázka ich bezpečnosti prešla v poslednom období výraznými zmenami. V minulosti kostru právnej úpravy pre informačné systémy verejnej správy tvorili zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších právnych predpisov spoločne s výnosom Ministerstva financií SR č. 55/2014 Z.z. o štandardoch pre informačné systémy verejnej správy. Zákon o informačných systémoch verejnej správy zaviedol štandardy, rozhrania a legálne definície pojmov v tejto oblasti, čo v jeho predchodcovi (v zákone o štátnom informačnom systéme) absentovalo. Dá sa povedať, že až od účinnosti zákona o informačných systémoch verejnej správy možno hovoriť o regulácii v oblasti IT technológii vôbec. Dovtedy bola regulácia nulová, respektíve veľmi nízka.

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. Dôvodom bola potreba zásadnej zmeny nielen z filozofického hľadiska, ale aj z hľadiska prístupu k regulácii. Zákon o ISVS dovtedy reguloval len primárne informačné systémy verejnej správy, ale nie aj ostatné súčasti informačných technológií verejnej správy (ITVS). Zákon o ISVS nepredstavoval komplexnú právnu úpravu informačných technológii vo verejnej správe; neboli v ňom jednotným spôsobom pokryté všetky oblasti vedenia a riadenia. Revízia ustanovení dovtedy platnej právnej úpravy bola potrebná aj s ohľadom na vývoj v oblasti informačných technológií, ako aj s ohľadom na zmeny vo vnímaní a v stave realizácie informatizácie verejnej správy na Slovensku.

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. Podľa § 24 zákona o ITVS sa štandardom rozumie súbor pravidiel spojených s vytváraním, rozvojom a využívaním informačných technológií verejnej správy, ktorých účelom je vytvorenie jednotného prostredia umožňujúceho výmenu a spoločné používanie údajov a spoločných modulov medzi jednotlivými informačnými systémami verejnej správy a na účel ich prístupnosti a poskytovania pre verejnosť a to v oblastiach ustanovenom v zákone o ITVS.[[3]](#footnote-3) Štandardy určujú podmienky, ktoré sa uplatňujú na informačné technológie verejnej správy a orgán riadenia (§ 5 ods. 2 zákon o ITVS) podľa nich postupuje pri riadení informačných technológií verejnej správy. Štandardy musia byť otvorené a technologicky neutrálne. Do 30. apríla 2020 boli štandardy upravené výnosom Ministerstva financií SR č. 55/2014 Z. z.  o štandardoch pre informačné systémy verejnej správy. S účinnosťou od 1. mája 2020 sú štandardy  pre ITVS upravené vyhláškou Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu  č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy (ďalej len „vyhláška o štandardoch pre ITVS“). S účinnosťou od 1. januára 2022 nadobudla účinnosť vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 546/2021 Z. z., ktorou sa mení a dopĺňa vyhláška úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy. Novela vyhlášky predstavuje kontinuitu k dnešným štandardom pre informačné technológie verejnej správy, ktoré precizuje a dopĺňa. Tieto zmeny a doplnenia vychádzajú z potrieb praxe. V súčasnosti ustanovenia štandardov  pre ITVS  bližšie upravuje  metodický pokyn k výnosu MF SR zo 4. marca 2014 č. 55/2014-173 Z. z. o štandardoch pre informačné systémy verejnej správy v znení dodatku č. 1. Metodický pokyn k výnosu o štandardoch ISVS  sa v súčasnosti aplikuje len v tom rozsahu, v akom je upravený právny rámec vo vyhláške o štandardoch pre ITVS. V ostatných častiach je tento metodický pokyn od 1. mája 2020 neplatný. Na účel doplnenia vyhlášky o štandardoch pre ITVS bude  Ministerstvom investícií, regionálneho rozvoja a informatizácie Slovenskej republiky vypracované nové metodické usmernenie. Cieľom metodického usmernenia bude doplniť rozdelenie, náležitosti a vysvetlenia štandardov, príklady správneho použitia štandardov, spôsob ich aktualizácie a oblasti ich uplatnenia pre informačné technológie verejnej správy, ako nástrojov výkonu informačných činností pri utváraní a prevádzkovaní informačných technológií verejnej správy alebo ich častí.

Bezpečnosť ISVS je takisto predmetom zákona o kybernetickej bezpečnosti (ďalej len „KB“), keďže za určitých okolností môže byť konkrétny informačný systém verejnej správy 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 informačný systém povinný plniť povinnosti v zmysle zákona o KB.

V súčasnosti platný zákon o informačných technológiách vo verejnej správe

v porovnaní so zrušeným zákonom o informačných systémoch verejnej správy 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 v tomto znení: *„informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby.“* [[4]](#footnote-4)

V prípade pojmu informačný systém došlo k zmene, keďže informačný systém v zmysle § 2 ods. 2 zákona o ITVS predstavuje *„funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov.“* V porovnaní s definíciou pojmu informačný systém v zmysle zrušeného zákona o ISVS nemusia byť technické prostriedky a programové prostriedky súčasťou informačného systému a tieto prostriedky takisto nemôžu poskytovať iný informačný systém.

Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe (ITVS)

a o zmene a doplnení niektorých zákonov komplexne upravuje organizáciu správy informačných technológií verejnej správy, práva a povinnosti v oblasti informačných technológií verejnej správy, na ktoré sa tento zákon vzťahuje a základné požiadavky kladené na informačné technológie verejnej správy a na ich správu.

Kým v minulom období sa dôraz z hľadiska právneho rámca kládol na technologický pohľad, teda na štandardy informačných systémov verejnej správy, v novej právnej úprave došlo k posunu do roviny procesnej. Nová úprava oproti pôvodnej právnej úprave priniesla systémovú zmenu, ktorá sa týka hlavne rozšírenia povinností pre jednotlivé inštitúcie verejnej správy v oblasti správy, t.j. vedenia a riadenia informačných technológií, a to od samotného plánovania, obstarania, implementáciu informačných technológií, až po monitoring a hodnotenie IT. Oproti predchádzajúcej právnej úprave zákon tiež posilnil pozíciu Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky, a to z koordinačnej do riadiacej. Zákon o ITVS na rozdiel od predchádzajúcej právnej úpravy upravuje aj výkon kontroly dodržiavania povinností ustanovených v zákone, ktorý má zabezpečiť nielen kontrolu plnenia povinností, ale aj spätnú väzbu o plnení povinností orgánov riadenia v správe informačných technológií.

V novej právnej úprave je vo zvýšenej miere pokrytá aj oblasť bezpečnosti. Zákon nadväzuje na [zákon o kybernetickej bezpečnosti](https://www.tuvsud.com/sk-sk/cinnosti/kyberneticka-bezpecnost/audit-kybernetickej-bezpecnosti) a upravuje činnosť vládnej jednotky CSIRT pri riešení a prevencii kybernetických hrozieb. Hlavným cieľom národného systému riadenia incidentov **kybernetickej bezpečnosti vo verejnej správe** je vytvorenie siete adekvátne odborne a technicky vybavených jednotiek pre riešenie **kybernetických bezpečnostných** incidentov (ďalej len „jednotky CSIRT“) na celonárodnej úrovni. Úlohou jednotiek CSIRT je vykonávanie preventívnych a reaktívnych opatrení v oblasti svojho pôsobenia a poskytovanie relevantných informácií o kybernetických incidentoch národnej jednotke CSIRT a vládnej jednotke CSIRT.

Zákon o ITVS v ustanoveniach § 18 až § 23 upravuje bezpečnosť ITVS, pričom sa však v ňom výslovne diferencuje a uvádza, že povinnosti správcu upravuje zákon o kybernetickej bezpečnosti a zákon o ITVS upravuje „len“ obsah bezpečnostných opatrení vo vzťahu k ITVS a spôsob a rozsah ich prijímania a realizácie v súlade so zákonom o kybernetickej bezpečnosti. V § 18 až § 23 zákona o ITVS v časti bezpečnosti v oblasti plánovania a organizácie sú nastavené najmä pravidlá pre zavedenie systému riadenia informačnej bezpečnosti v organizácií. K organizačne procesným podmienkam patria činnosti, ktoré majú vykonávať riadiace, výkonné a kontrolné zložky systému riadenia bezpečnosti. V ďalších častiach je regulácia koncipovaná predovšetkým s ohľadom na životný cyklus ITVS. Sú stanovené špecifické povinnosti pri plánovaní, vytváraní alebo nadobudnutí, ďalej pri zavedení, prevádzke a vyradení informačného systému verejnej správy. Na tieto ustanovenia nadväzuje vykonávací právny predpis vyhláška úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z.z. , ktorou sa stanovuje spôsob kategorizácie a obsah bezpečnostných opatrení ITVS účinný od 30. júna 2020. Vyhláška obsahuje podrobnosti o spôsobe zaraďovania do týchto kategórií s použitím klasifikácie informácií a kategorizácie sietí a informačných systémov podľa osobitného predpisu. Upravuje tiež podrobnosti o bezpečnosti ITVS rozpracované v zákone o ITVS

a v zákone o kybernetickej bezpečnosti, povinnosti správcu vo vzťahu k ITVS, pričom správca musí identifikovať a udržiavať svoj zoznam aktív a musí realizovať bezpečnostné opatrenia aspoň na úrovni minimálnych požadovaných bezpečnostných opatrení danej kategórie. Bezpečnostné opatrenia ITVS sú tvorené minimálnymi bezpečnostnými opatreniami troch úrovni.

Bezpečný informačný systém vo verejnej správe by mal spĺňať tieto požiadavky, a to v prvom rade dokázať zabezpečiť spoľahlivú prevádzku IS ako celku, zabezpečiť ochranu údajov a osôb, presnejšie zabezpečiť záujmy osôb využívajúcich služby IS. Skutočnosť, že hovoríme o troch aspektoch, by však nemala byť interpretovaná tak, že tieto sa navzájom vylučujú. Naopak, výsledkom snahy o bezpečný IS bude nejaká kombinácia týchto cieľov, pričom ich výber a ich „váha“ vo výslednej kombinácií bude závisieť od konkrétnej situácie a konkrétnych požiadaviek majiteľa, resp. prevádzkovateľa IS. Informačný systém sa zvyčajne nevybuduje len tak na uspokojenie kohosi rozmaru, ale s viac či menej presne definovaným úmyslom spracovávať informácie a poskytovať ich určenej skupine používateľov systému. Okrem toho vybudovanie čo len trochu väčšieho IS si vyžaduje nezanedbateľné investície, ktoré sú ekonomicky odôvodniteľné len v tom prípade, že systém bude v prevádzke, t.j. bude plniť účel, na ktorý bol vybudovaný. V novej právnej úprave je vo zvýšenej miere pokrytá oblasť bezpečnosti. Konkrétne sú to najmä § 18 až § 23 zákona o ITVS.

Od spoľahlivej prevádzky IS často závisí schopnosť jeho používateľov vykonávať svoju predpokladanú činnosť, plniť svoje záväzky, ktoré majú k ďalším subjektom či včas prijímať správne rozhodnutia. Hoci miera ich závislosti od funkčnosti IS závisí od konkrétnych okolností, prerušenie jeho prevádzky alebo iné odchýlky od jeho projektovanej či očakávanej činnosti (napríklad nesprávne spracovanie údajov) nesporne negatívne ovplyvnia výsledky ich práce. Hrozby pre IS môžu byť výsledkom nielen úmyselnej činnosti „útočníka“, ale aj nedbanlivosti osoby, ktorá participovala na návrhu, vývoji, implementácií, testovaní, inštalácií, údržbe alebo prevádzke systému – je jeho oprávneným používateľom. Z tohto dôvodu je preto nutné venovať dôslednú pozornosť plánovaniu, organizácii, obstarávaniu, implementácii, prevádzke, kontrole a hodnoteniu bezpečnosti informačných technológií.

Ako sme už predtým uviedli, oblasť bezpečnosti informačných technológií je upravená v úzkej súčinnosti s postupmi a opatreniami, ktoré sú stanovené návrhom zákona

o KB. Keďže predmetný zákon ustanovuje oblasť informačných systémov verejnej správy ako osobitný podsektor a zavádza nielen reguláciu systémov, ale aj ich prevádzkovateľov vrátane nahlasovania a riešenia bezpečnostných incidentov, vo veľkej miere dochádza k prekrývaniu s tým, čo sa v oblasti bezpečnosti informačných technológií reguluje v tomto zákone. Z toho dôvodu zákonodarca ponechal pri informačných technológiách podľa tohto zákona celý režim návrhu zákona o kybernetickej bezpečnosti s tým, že „len“ samotný obsah a rozsah bezpečnostných opatrení, ako aj povinnosť vypracúvať bezpečnostný projekt, sú stanovené týmto návrhom zákona. Táto oblasť je z dôvodu prehľadnosti pre špecifickú tému bezpečnosti uvedená v samostatných paragrafoch §18 až §23 a jednotlivé ustanovenia sú zosúladené s oblasťami riadenia v správe informačných technológií. V časti o bezpečnosti informačných technológii verejnej správy v oblasti plánovania a organizácie ide najmä o nastavenie pravidiel pre zavedenie systému riadenia informačnej bezpečnosti v organizácii.

K organizačne procesným podmienkam patria činnosti, ktoré majú vykonávať riadiace, výkonné a kontrolné zložky systému riadenia bezpečnosti. Správca je povinný vo svojej organizácii zaviesť a udržiavať systém riadenia informačnej bezpečnosti, ktorý okrem iného určí ciele, rozsah, podmienky, povinnosti osôb, ktoré vykonávajú činnosť pre správcu a organizačných zložiek správcu a prostriedky riadenia bezpečnosti vo forme bezpečnostnej dokumentácie schválených procesov riadenia bezpečnosti informačných technológií verejnej správy. Zriadi riadiacu, výkonnú a kontrolnú zložku systému riadenia bezpečnosti, ktoré sú navzájom personálne a kompetenčne oddelené, určí a zavedie bezpečnostné opatrenia na procesnej, organizačnej a na technickej úrovni, určí prostriedky kontroly uplatňovania bezpečnostných opatrení a postupy riešenia bezpečnostných incidentov. Ide len o demonštratívny výpočet povinnosti správcu informačného systému verejnej správy v oblasti bezpečnosti. Ich vyčerpávajúci výpočet je uvedený v už spomínaných ustanoveniach § 18 až § 23 zákona o ITVS. Okrem povinností je v týchto ustanoveniach regulácia koncipovaná predovšetkým s dôrazom na životný cyklus informačného systému verejnej správy. Stanovujú sa špecifické povinnosti v oblasti bezpečnosti informačných systémov verejnej správy pri plánovaní, vytváraní alebo nadobudnutí a takisto pri zavedení, prevádzke a vyradení informačného systému verejnej správy.

  Dôležitým nástrojom na komplexné posúdenie bezpečnostných potrieb, určenie bezpečnostných požiadaviek a návrh spôsobu ich efektívneho naplnenia je bezpečnostný projekt informačného systému. Inštitút bezpečnostného projektu je previazaný aj so životným cyklom informačného systému verejnej správy.  Špecifické vypracovávanie bezpečnostného projektu je previazané s riadením aktív v informačných technológiách verejnej správy uvedených v §15 ods. 8, pričom toto ustanovenie je východiskové pre plnenie viacerých povinností v § 18 až 23, v hoci nie je priamo uvedené v časti o bezpečnosti. Bezpečnostný projekt sa povinne vypracováva pre tie informačné systémy verejnej správy, ktoré sa

z hľadiska klasifikácie považujú za „najdôležitejšie“, resp. „najviac kritické“. Pre ostatné systémy je možné uložiť povinnosť vypracovať bezpečnostný projekt len z dôvodu výsledkov bezpečnostného auditu alebo penetračných testov, ktoré preukážu nedostatky v bezpečnosti takého charakteru, ktorý si vyžaduje vypracovanie bezpečnostného projektu.

Bezpečnostný projekt vymedzuje rozsah a spôsob technických, organizačných

a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti

a funkčnosti. Bezpečnostný projekt sa spracováva v súlade so základnými pravidlami bezpečnosti informačného systému vydanými bezpečnostnými štandardmi, právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná. Pri spracovaní bezpečnostného projektu informačného systému verejnej správy sa prihliada najmä na zložitosť informačného systému verejnej správy, komplexnosť agendy pokrytej informačným systémom verejnej správy a stanovenie bezpečnostných požiadaviek na informačný systém verejnej správy. Zohľadniť sa musí aj kategória, do ktorej je informačný systém verejnej správy zaradený. Bezpečnostný projekt informačného systému verejnej správy pozostáva z dvoch hlavných výstupov: *bezpečnostný zámer* (ide o prvý výstup bezpečnostného projektu informačného systému verejnej správy, ktorý určuje najmä kontext a zameranie bezpečnostného projektu, *analýza bezpečnosti* (súčasťou dokumentu *Analýza bezpečnosti* je analýza rizík. Rizikom sa v bezpečnostnom projekte chápe miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami). Jednotlivé výstupy vznikajú v určenom poradí a sú priebežne aktualizované počas celého projektu informačného systému verejnej správy realizovaného v súlade so zákonom č. 95/2019 Z.z. Obsah a štruktúru bezpečnostného projektu informačného systému verejnej správy upravuje príloha č. 3 vyhlášky č. 179/2020 Z.z.

Osobitnou úpravou je úprava vo vzťahu k nahlasovaniu, riešeniu a spolupráci pri riešení bezpečnostných incidentov, ktoré nie sú pokryté reguláciou nahlasovania a ukladania povinností riešiť incident podľa zákona o kybernetickej bezpečnosti. V zmysle § 23 ods. 3 zákona o ITVS sú orgán riadenia podľa § 5 ods. 2 písm. a) a b), 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 ktorý sa nevzťahuje povinnosť nahlasovania podľa osobitného predpisu (§ 24 ods. 1 zákona o KB),
* 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, v lehote do 30 dní odo dňa zriadenia

a uvedenia do prevádzky jednotného informačného systému kybernetickej bezpečnosti nahlasujú kybernetický bezpečnostný incident podľa § 23 ods. 3 písm. a) orgánu vedenia, ktorým je ÚPVII ním určeným spôsobom. Zákon o ITVS v § 23 ods. 4 zákona o ITVS ukladá plnenie povinností v zmysle § 23 ods. 3 písm. a) aj ostatným orgánom riadenia. Inými slovami, aj ostatné orgány riadenia, ak sú zaradené do registra PZS, sú prostredníctvom jednotného informačného systému kybernetickej bezpečnosti povinné nahlasovať aj kybernetický bezpečnostný incident, na ktorý sa nevzťahuje povinnosť nahlasovania podľa zákona o KB. Ostatné orgány riadenia sú povinné určiť jeden kontaktný bod na nahlasovanie kybernetických bezpečnostných incidentov.

Ide o svojho druhu nadstavbu k zákonu o kybernetickej bezpečnosti, ktorá v súlade s týmto zákonom rozširuje požiadavky na zabezpečenie sietí a informačných systémov v sektore informačných systémov verejnej správy s cieľom dosiahnuť vyššiu úroveň ich bezpečnosti.

Ani tie najprísnejšie bezpečnostné opatrenia nemôžu zabrániť tomu, aby nedošlo ku kybernetickému bezpečnostnému incidentu. V takýchto prípadoch je subjekt zasiahnutý v zmysle zákona o ITVS a zákona o KB povinný hlásiť konkrétny typ bezpečnostného incidentu konkrétnemu subjektu. Subjekt buď v postavení PZS podľa zákona o KB, alebo v postavení správcu v zmysle zákona o ITVS si pred samotným hlásením musí uvedomiť, aký typ bezpečnostného incidentu má hlásiť, akým spôsobom, akému subjektu a v akej lehote. Je preto 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. Na dosiahnutie tohto cieľa by bolo potrebné zosúladiť obsahové náležitosti formulárov, ktoré konkrétne subjekty využívajú pri hlásení konkrétnych typov bezpečnostných incidentov.[[5]](#footnote-5)

Nahlasovanie kybernetických incidentov je na jednej strane jednou z kľúčových povinností, ktoré vybraným organizáciám ukladá zákon, na druhej strane je kľúčové pri zabezpečení bezpečnosti informačných technológií vo verejnej správe, ako aj v kybernetickom priestore ako celku. [[6]](#footnote-6) Umožní nielen riešiť daný problém, ale aj predchádzať vzniku ďalších potenciálnych incidentov. Na tomto mieste chceme preto vyzdvihnúť a poukázať na novú právnu úpravu, v zmysle ktorej Národný bezpečnostný úrad môže po novom prevádzkovateľom základných služieb uložiť povinnosť vyhodnocovať a nahlasovať výskyt kybernetických bezpečnostných incidentov aj automatizovane. Nesplnenie tejto povinnosti sa považuje za správny delikt, za ktorý môže úrad prevádzkovateľovi základnej služby uložiť pokutu až do 30 000 eur. Schopnosť robiť rýchle a správne rozhodnutia na základe aktuálnych informácií o hrozbách a prispôsobovať proaktívne bezpečnostné upozornenia, výstrahy a odporúčania, je jedným z kľúčových predpokladov kvalitného zabezpečenia nášho kybernetického priestoru. Práve automatizácia, na ktorú aktuálna novela zákona o kybernetickej bezpečnosti upriamuje pozornosť, je toho základom. Prirodzene, legislatívne vymedzenie je len prvým, hoci nevyhnutným krokom. S cieľom zabezpečiť fungovanie ideálneho scenára, aby zodpovedné jednotky pre riešenie počítačových incidentov CSIRT vedeli automatizovane prijímať a spracúvať dáta o tom, čo sa v slovenskom kybernetickom priestore deje, treba pokračovať ďalej. Predovšetkým je potrebné technicky zabezpečiť, aby CSIRT vedel od dotknutých organizácií dáta automatizovane prijímať a zároveň, aby kvantá surových údajov dokázal aj analyzovať a vyhodnotiť – ideálne v reálnom čase a štandardizovaným spôsobom. Výsledkom automatizácie by bolo nielen odbremenenie prevádzkovateľov základných služieb, ktorí si dokážu jednoduchšie plniť zákonné povinnosti, ale predovšetkým lepší prehľad o dianí

a rizikách v slovenskom kybernetickom priestore.

**Záver**

Informatizácia verejnej správy je riadený proces, ktorý sa realizuje v rámci celej štruktúry verejnej správy. Je to proces vytvárania spoločenských, legislatívnych, metodických, technologických a organizačno-personálnych podmienok na efektívnu aplikáciu informačných technológií vo výkone verejnej správy, ako aj riadený proces vlastnej aplikácie IT, pričom pod IT sa rozumejú aj komunikačná infraštruktúra a komunikačné technológie, ktoré sú na prevádzku a používanie IT potrebné. Výsledkom tohto procesu by malo byť efektívne využívanie IT v procesoch verejnej správy pri súčasnom zachovaní bezpečnosti informácií, ktoré cez daný systém prechádzajú .Na dosiahnutie tohto cieľa je potrebná zodpovedajúca úprava procesov verejnej správy. Informatizácia by mala byť postavená v prvom rade na právnom rámci, ktorý predstavuje systém všeobecne záväzných právnych predpisov, ako aj metodických aktov, ktoré spolu vytvárajú záväzné podmienky budovania informatizácie spoločnosti. Z pohľadu bezpečnosti je kľúčovým zákon o informačných technológiách vo verejnej správe ako nástupca zákona o informačných systémoch verejnej správy, v ktorom sa vôbec prvýkrát precizovala oblasť bezpečnosti IT vo verejnej správe.

Je potrebné si uvedomiť, že súčasné legislatívne vymedzenie predstavuje „len“ minimálne bezpečnostné opatrenia informačných technológií verejnej správy, preto aj vzhľadom na stúpajúce množstvo kybernetických incidentov bude potrebné, aby zákonodarca pružnejšie reagoval na stále sa objavujúce nové hrozby, a tomu prispôsoboval legislatívu, vrátane dôrazu na jej lepšiu vynútiteľnosť.

**Literatúra**

ANDRAŠKO, J. a kol., 2018. *Zákon o kybernetickej bezpečnosti. Komentár*. Bratislava: Wolters Kluwer SR s.r.o. 544 s. ISBN 978-80-81689-05-5.

KOLOUCH, J., BAŠTA, P. a kol., 2019. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o, 556 s. ISBN 978-80-88168-34-8.

*Hlásenie kybernetických bezpečnostných incidentov*, 2019. [online]. [cit. 28. novembra 2022]. Dostupné na internete:< [Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe | NASES (gov.sk)](https://www.nases.gov.sk/projekty/narodny-system-riadenia-incidentov-kybernetickej-bezpecnosti-vo-verejnej-sprave/index.html)>.

*Jednotný informačný systém kybernetickej bezpečnosti*, 2018. [online]. [cit. 22. októbra 2022]. Dostupné na internete:< [Jednotný informačný systém kybernetickej bezpečnosti -NBU (gov.sk)](https://www.nbu.gov.sk/kyberneticka-bezpecnost/jednotny-informacny-system-kybernetickej-bezpecnosti/index.html)>.

*Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov.*

*Výnos Ministerstva financií SR č. 55/2014 Z.z. o štandardoch pre informačné systémy verejnej správy.*

*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.*

*Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.*

*Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.*

*Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z.z.*

**Keywords:** information technology, information systems, cyber security, public administration, cyber space, analysis, research, evaluation

**Summary**

Informatisation of public administration is a controlled process that is implemented within the entire structure of public administration. It is the process of creating social, legislative, methodological, technological, and organisational-personnel conditions for effective application of information technologies (IT) in the performance of public administration. It is also a controlled process of IT application itself, whereas IT also means the communication infrastructure and technologies that are necessary for the operation and use of IT. The result of this process should be the efficient use of IT in public administration processes while maintaining the security of the information passing through the system. To achieve this, a corresponding adjustment of public administration processes is required. The informatisation should be built primarily on a legal framework, which is a system of generally binding legal regulations, but also methodological acts that together create binding conditions for building the informatisation of society. From the security point of view, the law on information technologies in public administration is key as being the successor to the law on public administration information systems, in which the field of IT security in public administration was specified for the first time. It should be noted that the current legislative definition represents “only” minimal security measures of public administration information technology, therefore, even in view of the increasing number of cyber incidents, the legislator will need to respond more flexibly to the ever-emerging new threats and adapt the legislation to this, including an emphasis on its better enforceability.

*PhDr. JUDr. Mgr. Ervín Šimko, LL.M.*

*Katedra verejnej správy a krízového manažmentu*

*Akadémie PZ v Bratislave*

*e-mail:* [*ervin.simko@akademiapz.sk*](mailto:ervin.simko@akademiapz.sk)

Recenzenti: mjr. doc. PhDr. JUDr. Mgr. Jozef Medelský, PhD., pplk. Ing. Igor Pavlovič, PhD.

1. KOLOUCH, J., BAŠTA, P. a kol., 2019. *CyberSecurity*, s. 45-68 alebo BAYUK, L. a kol., 2012. *Cyber security policy guidebook*, s. 2-3. [↑](#footnote-ref-1)
2. ANDRAŠKO, J. a kol., 2018. *Zákon o kybernetickej bezpečnosti. Komentár,*  s. 544. [↑](#footnote-ref-2)
3. *§ 24 zákona č. 95/2019 Z.z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.* [↑](#footnote-ref-3)
4. *Zákon č. 275/2006 Z.z. Zákon o informačných systémoch verejnej správy* [↑](#footnote-ref-4)
5. *Jednotný informačný systém kybernetickej bezpečnosti, 2018.*  [online]. [cit. 12. októbra 2022]. Dostupné na internete: < [Jednotný informačný systém kybernetickej bezpečnosti -NBU (gov.sk)](https://www.nbu.gov.sk/kyberneticka-bezpecnost/jednotny-informacny-system-kybernetickej-bezpecnosti/index.html)>. [↑](#footnote-ref-5)
6. *Hlásenie kybernetických bezpečnostných incidentov*, 2019. [online] . [cit. 28. novembra 2022]. Dostupné na internete:< [Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe | NASES (gov.sk)](https://www.nases.gov.sk/projekty/narodny-system-riadenia-incidentov-kybernetickej-bezpecnosti-vo-verejnej-sprave/index.html)>. [↑](#footnote-ref-6)