Vincent Holubiczky

Prítomnosť hrozieb a zraniteľností pri využívaní informačných technológií

Anotácia: Štúdia je zameraná na prezentáciu čiastkových výsledkov výskumu realizovaného v rámci dizertačnej práce autora a zároveň čiastkovej úlohy „*Internet vecí – podstata, hrozby a riziká*“ z vedeckovýskumnej úlohy VÝSK. 245[1], ktorá je realizovaná na Akadémii Policajného zboru v Bratislave. Autor sa v úvode príspevku zameriava najmä na definíciu vybraných pojmov a popis a analýzu hrozieb a zraniteľností v oblasti informačnej bezpečnosti. Následne vyhodnocuje subjektívne vnímanie zraniteľností a hrozieb respondentmi a predkladá vlastné odporúčania pre prax.

Kľúčové slová: bezpečnosť, informačné technológie, hrozby, ľudský faktor.

Úvod

Povinnosťou každého štátu je zaručenie ochrany života, zdravia a majetku. V každom demokratickom štáte na prvom mieste zabezpečuje ochranu týchto základných životných hodnôt, vnútorný poriadok a bezpečnosť predovšetkým polícia, ktorá svojou pôsobnosťou a plnením špecifických úloh vytvára optimálne bezpečnostné podmienky.[2] Bezpečnosť je prvoradá vo všetkých smeroch. Stav neohrozenosti života, zdravia, životného prostredia, majetku a iných hmotných aj nehmotných subjektov jedinca má v komplexnom chápaní značný vplyv na zložitý systém spoločnosti a zaručuje jeho pokojný, efektívny a bezproblémový chod. Preto je stav a pocit bezpečnosti veľmi rozšírenou a obľúbenou témou mnohých vedeckých pracovníkov na Slovensku aj v zahraničí. Informačná bezpečnosť ako časť, smer tejto všeobecnej problematiky, je tiež stredobodom pozornosti najmä v uplynulom desaťročí. Tento fakt súvisí s rýchlym vývojom nových a moderných technológií umožňujúcich, pre jednoduchých i náročnejších užívateľov, využívať elektronické služby, spájať ich, a tak vytvárať zložité systémy, na ktoré potom kladú vysoké nároky v oblasti funkčnosti a efektivity. Takzvaný *internet vecí* dnes ponúka nevídané možnosti online priestoru, ktoré by sme pred niekoľkými rokmi nečakali ani v najodvážnejších vedecko-fantastických filmoch. Všade prítomné technológie a online prostredie v každodennom živote nás robia menej citlivými na potencionálne hrozby a zraniteľnosti. Takýto apatický postoj k pravdepodobnosti vzniku incidentov sa môže rozšíriť aj do pracovného prostredia, kde môže napáchať nemalé škody.

Základné pojmy

Bezpečnosť môžeme definovať, pre naše potreby ako stav, kedy sú všetky možné hrozby vhodnými opatreniami eliminované alebo úroveň ich vplyvu je znížená na subjektívne prijateľnú úroveň.[3] Existuje mnoho autorov, ktorí definujú bezpečnosť inými spôsobmi, často negatívne – neprítomnosťou nebezpečenstva alebo hrozby.[4] Je dôležité si uvedomiť to, že

[1] s názvom „*Moderné technológie v páchaní, odhaľovaní, dokumentovaní, dokazovaní a prevencii trestnej činnosti pri zabezpečení verejného poriadku, bezpečnosti a plynulosti cestnej dopravy : Aspekty technické, kriminalistické, kriminologické, penologické, právne, verejno-správne, sociálne, psychologické a bezpečnostné*“.
[2] IGENYES, L., HOLUBICZKY, V. 2017. *Úvaha o používaní zbraní súkromnými bezpečnostnými službami v prípade hromadného nasadenia na verejných kultúrnych a športových podujatiach*.
[3] HOLUBICZKY, V. 2019. *Bezpečnosť informačných systémov – ľudský faktor.*
[4] RAK, R., KOPENCOVÁ, D., FELCAN, M. 2019. *Objekty a systémy – základní analytické prvky bezpečnosti*.

tento pojem je výrazne subjektívny a úzko súvisí s vnímaním jednotlivca. Úroveň bezpečnosti je nemerateľná veličina, hoci mnohí označujú mieru rizika a pravdepodobnosť určitého neželaného stavu alebo hrozby za úroveň bezpečnosti. Každý vníma bezpečnosť inak, na základe subjektívnych vonkajších vplyvov, aktuálnych hrozieb a miery nebezpečenstva, rizika. Tieto pojmy sú veľmi úzko prepojené a nemôžu existovať a fungovať jednotlivo. Podľa Löfflera a Antala[5] predstavuje bezpečnosť veľmi zložitý multidimenzionálny sociálny fenomén, ktorý sa spája s rozmanitými formami ľudského správania a existencie, či už spoločenskej, materiálnej alebo duchovnej. Buzalka a Blažek[6] zadefinovali bezpečnosť vo všeobecnej rovine ako *„(...) relatívnu absenciu ohrozenia. Stav, kedy sú minimalizované riziká a z nich vyplývajúce možné ohrozenia, ktoré môžu vyústiť do kríz (krízových stavov)“,* bezpečnosť je podľa nich stav*, „(...) v ktorom sa daný subjekt necíti byť ohrozený z hľadiska svojej existencie, záujmov a hodnôt.“*[7]

Bezpečnosť má rôzne formy a delenia, ako napr. osobnú, národnú, medzinárodnú alebo, ako to vo svojom príspevku uvádza Medelský[8], vnútornú a vonkajšiu. Základný rozdiel vidí v tom, že v prípade vnútornej bezpečnosti smerujú všetky hrozby z vnútra štátu, v prípade bezpečnosti vonkajšej majú hrozby pôvod mimo štátu. Takto môžeme dospieť k deleniu na národnú a medzinárodnú bezpečnosť.[9] Medzi predikátory pojmu bezpečnosť, vývojom techniky, patria napríklad aj výrazy *„telekomunikačná“*, *„informačná“,* či *„kybernetická“* bezpečnosť. Ide o schopnosť systémov odolávať na určitom stupni konaniu, ktoré by mohlo ohroziť dostupnosť, dôvernosť, integritu a spoľahlivosť uchovávaných, prenášaných alebo spracovávaných dát.[10] **Informačná bezpečnosť**[11] je podľa medzinárodného štandardu ISO/IEC 270011 (prijatého Národnou stratégiou pre informačnú bezpečnosť) ochrana informácie pred širokým spektrom hrozieb, ktorej cieľom je zaistenie kontinuity obchodných procesov, minimalizácia strát a maximalizácia návratnosti investícií. Základné bezpečnostné požiadavky na ochranu informácií sú ich dostupnosť, dôvernosť, autentickosť a integrita.[12] Dáta sa stávajú informáciami, keď získajú zmysel a hodnotu. Hodnotu informácií určuje vždy ich vlastník, pre ktorého informácie majú význam a určitú hodnotu. **Bezpečnosť informačného systému** znamená schopnosť siete alebo informačného a komunikačného systému odolávať na určitom stupni spoľahlivosti náhodným udalostiam alebo úmyselnému konaniu, ktoré ohrozuje dostupnosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov[13] alebo súvisiacich služieb poskytovaných prostredníctvom tejto siete a informačného systému alebo prístupných prostredníctvom tejto siete a informačného systému.[14]

Podľa zákona o kybernetickej bezpečnosti informačným systémom je *„elektronická komunikačná sieť každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov.“*[15] Baričičová a Pajpachová tvrdia, že informačný systém predstavuje subsystém z množstva aplikovaných systémov v podmienkach

---

[5] LÖFFLER, B., ANTAL, M. 2017. *Vybrané aspekty ochrany verejného poriadku v Slovenskej republike.*
[6] BUZALKA, J., BLAŽEK, V. 2011. *Metodológia a metodika vypracovania analýzy vnútorného ohrozenia bezpečnosti SR a z nej vyplývajúcich ohrození a rizík*, s. 33 - 34
[7] HOLUBICZKY, V. 2018. *Vzdelaný policajt, garant bezpečnosti*.
[8] MEDELSKÝ, J. 2018. *Bezpečnostno strategické dokumenty,* s. 252 -253
[9] RAK, R., KOLITSCHOVÁ, P. 2019. *Bezpečnost a bezpečí – základní pojmy a jejich vnímání.*
[10] HOLUBICZKY, V. 2019. *Informačné systémy a ich bezpečnosť*.
[11] HOLUBICZKY, V. 2019. *Bezpečnosť informačných systémov – ľudský faktor*.
[12] KRESL, E. 2018. *Východiská legislatívnej prevencie počítačovej kriminality,* s. 76-78 alebo ISO/IEC 270011
[13] HOLUBICZKY, V. 2019. *Informačné systémy a ich bezpečnosť*.
[14] Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020, príloha 1, str. 22
[15] §3 ods. a) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti

policajnej organizácie. V podmienkach Policajného zboru sa prostredníctvom nich zabezpečuje realizácia riadiacich, výkonných aj podporných procesov, pričom ich elementárnou úlohou je poskytnúť dostatok relevantných, aktuálnych a presných informácií v potrebných termínoch a v požadovanej forme.[16]

Postupom času a vývojom techniky sa teda dostával postupne do povedomia pojem **informačná bezpečnosť**. Údaje a informácie sa neuchovávali už len vo fyzickej podobe v archívoch, ale postupne sa prešlo k elektronickej podobe úschovy.[17] Vo svete je nevyčísliteľné množstvo údajov. Základný rozdiel medzi týmito údajmi a informáciami je, že kým údaj obsahuje fakt, nejakú hodnotu, pre nás neutrálnu, informácia má pre danú osobu alebo inštitúciu určitú pridanú hodnotu (negatívnu alebo pozitívnu). Úschova informácií v elektronickej podobe je na prvý pohľad veľmi jednoduchou záležitosťou. Avšak opak je pravdou – je tu veľké riziko straty dát a existuje množstvo subjektov, ktoré v týchto systémoch môžu spôsobiť neočakávané negatívne javy, narušiť bezpečnosť, ohrozovať stabilitu a fungovanie systému, resp. môžu spôsobiť nebezpečenstvo.[18] Informačnú bezpečnosť môžeme definovať ako súhrn opatrení na zabezpečenie integrity, dôvernosti a dostupnosti informácií, sietí a informačných a komunikačných systémov. Kurilovská a Šišulák uvádzajú, že cieľom **informačnej bezpečnosti** je chrániť informácie a informačné systémy zabezpečením ich dostupnosti, integrity, dôvernosti, autentifikácie a nepopierateľnosti. Medzi základné vlastnosti, resp. úlohy informačnej bezpečnosti radia tiež schopnosť obnovy informačných systémov. Ďalej definujú pojem kybernetická bezpečnosť ako podmnožinu informačnej bezpečnosti. Vysvetľujú to tvrdením, že informačná bezpečnosť sa zaoberá ochranou informácií v akejkoľvek forme, kým kybernetická bezpečnosť zastrešuje ochranu výlučne digitálnych dát.[19]

Riziko (*bezpečnostné riziko*) je pojem na označenie skutočnosti, že existuje potenciálna možnosť narušenia bezpečnosti chráneného záujmu. Jav sociálneho charakteru, ktorý má potenciál poškodiť subjekt bezpečnosti, alebo môže mať negatívny dopad na záujmy iného subjektu. Vyjadruje sa ako kombinácia:[20]

- pravdepodobnosti (*početnosti, vierohodnosti*), že dôjde k ohrozeniu chráneného záujmu kriminálnym činom alebo jemu sa blížiacimi dôsledkami činnosti iných ľudí,
- veľkosti možných následkov takejto udalosti.

Riziká majú rôznu mieru pravdepodobnosti výskytu a rôzny čas, ktorý uplynie od aktivácie až po **ohrozenie.**[21] V interných predpisoch Ministerstva vnútra Slovenskej republiky je uvedené, že **hrozbou** môže byť čokoľvek, čo je schopné využiť zraniteľnosť a v čoho dôsledku dochádza k bezpečnostnému incidentu, pričom za hrozbu môžeme považovať aj akúkoľvek potencionálnu príčinu incidentu. **Zraniteľnosti**[22] sú definované ako vlastnosti komponentov v návrhu, vyhotovení alebo prevádzke informačného alebo telekomunikačného systému, prostredníctvom ktorej dochádza k prejaveniu sa konkrétnej hrozby. Je to v podstate nedostatok, ktorý robí komponenty citlivými na neoprávnený prístup,

---

[16] BARIČIČOVÁ, Ľ., PAJPACHOVÁ, M. 2014. *Hodnotenie interných faktorov úspechu policajnej organizácie ako východisko možných zmien v procese jej riadenia*.
[17] HOLUBICZKY, V. 2018. *Vzdelaný policajt, garant bezpečnosti*.
[18] ŠIMÁK, L. a kol. 2005. *Terminologický slovník krízového riadenia: aktualizované vydanie,* s. 24
[19] KURILOVSKÁ L., ŠIŠULÁK, S. 2017. *Použitie inštitútu agenta pri odhaľovaní a objasňovaní kriminality v kybernetickom prostredí. s. 134-135*
[20] IGENYES, L., HOLUBICZKY, V. 2018. *Ochrana určených osôb a objektov 1 – Mechanické zábranné prostriedky.*
[21] MIKOLAJ, J., HOFREITER, L., MACH, V., MIHÓK, J., SELINGER P. *Terminológia bezpečnostného manažmentu - Výkladový slovník*, s. 18
[22] RAK, R., KOPENCOVÁ, D. 2019. *Bezpečnostní hrozby, vlastnosti a fáze*.

zničenie alebo uvedenie do stavu nespôsobilosti prostredníctvom ohrozenia.[23] Takéto definície potvrdzujú aj autori Kopencová a Rak vo svojom príspevku.[24]

Výskum

Na nasledujúcich riadkoch sa budeme snažiť priblížiť čitateľom čiastkové výsledky súvisiaceho výskumu, ktorý sme realizovali v rámci dizertačnej práce autora a zároveň vedecko-výskumnej úlohy uvedenej v anotácií príspevku. V prvom rade však v krátkosti popíšeme metódy využité pri jeho spracovaní.

Metódy zberu dát

Venovali sme sa **kvantitatívnemu** výskumu, kde sa snažíme zistiť súčasný stav úrovne informačnej bezpečnosti a postoj užívateľov k dodržovaniu pravidiel a predpisov, ich návykov a postrehov. Na zber údajov z kvantitatívneho výskumu sme použili **dotazníkovú metódu.** Keďže cieľový súbor bol v tomto prípade pomerne rozsiahly (niekoľko tisíc osôb), museli sme vhodným spôsobom určiť aj výberový súbor. Rozhodli sme sa pre využitie **techniky elektronického, resp. online dotazovania** respondentov, pričom výskumným nástrojom bol elektronický dotazník vlastnej konštrukcie. Takáto forma zberu dát je najpoužívanejšia v kvantitatívnom výskume. Je to merací nástroj, ktorý je možné využiť v rôznych výskumných plánoch. Dotazník musí spĺňať kritérium reliability, objektivity, validity a štandardnosti. Náš dotazník obsahuje položky ponúkajúce jednu možnosť odpovede, čiže zatvorené otázky a taktiež otázky s možnosťou doplnenia vlastnej odpovede, ktoré sa nazývajú polootvorené otázky. Dotazník bol vypracovaný formou online dotazníka s automatickým ukladaním odpovedí prostredníctvom „Google Forms“ v rozhraní Google Drive, čo nám umožnilo efektívne a rýchle vyhodnocovanie dát. Dotazník obsahoval veľmi jednoduché otázky s veľmi jasnými obmedzeniami.

Charakteristika výskumnej vzorky

Cieľovou skupinou nášho výskumu boli najmä príslušníci Policajného zboru a štátni zamestnanci, ktorí pri svojej činnosti využívajú ľubovoľnú výpočtovú techniku, ako napríklad osobný počítač, notebook, mobilný telefón či iné zariadenia. Okrem tejto primárnej skupiny bol dotazník distribuovaný pre potreby komparácie výsledkov aj iným skupinám, a to zamestnancom v súkromnom sektore v oblasti informačných technológií a denným študentom Akadémie Policajného zboru v Bratislave. Dotazník, ako to už bolo vyššie spomenuté, bol vytvorený formou online formulára. Odkaz na tento formulár bol cielene rozposlaný všetkým vedúcim pracovníkom Policajného zboru na úrovni Prezídia Policajného zboru všetkých krajov a okresov Slovenskej republiky a boli oslovené aj ďalšie skupiny respondentov zo súkromného sektora. V prípade online dotazníka je veľmi náročné, až nemožné, určiť percentuálnu návratnosť vyplnených dotazníkov, keďže nie je známy presný počet osôb, ktoré sa k dotazníku dostali a rozhodli sa ho nevyplniť. Na tomto mieste však vieme povedať, že odkaz bol doručený viac ako 2000 osobám a celkový počet vyplnených dotazníkov je 214. Znamená to približne 10% úspešnosť. Táto hodnota sa môže zdať nízka, avšak podľa nášho názoru je dostatočná na kvantitatívne aj kvalitatívne vyhodnotenie výskumu.

[23] Nariadenie MV SR č. 35/2018 o bezpečnostnej politike pre oblasť informačných systémov, čl. 3
[24] KOPENCOVÁ, D., RAK, R. 2019. *Risk Analysis and Threats in Security Sciences*.

Príslušníkmi Policajného zboru je 137 opýtaných, čo tvorí najväčšiu časť, až 64,02% výskumnej vzorky. S podielom okolo 14% sú zastúpení študenti, 13% dosiahol súkromný sektor a občianski zamestnanci v štátnej sfére tvoria 7% všetkých respondentov. Štyria (1,87%) označili možnosť „iné“, keďže vyplnenie tejto otázky nebolo povinné. Takéto rozloženie respondentov je vyhovujúce, keďže výskum sa zameriava predovšetkým na činnosti Policajného zboru a štátnych zamestnancov, pričom tieto dve skupiny tvoria viac ako 71% všetkých opýtaných. Zisťovali sme aj pracovné zaradenie respondentov vo vertikálnej línii. Opýtaní sa jednoznačne museli vyjadriť, či pracujú na vedúcej pozícií alebo nie. Z celkového počtu 214 odpovedí až 99 osôb označilo možnosť, že v zamestnaní zastáva vedúcu pozíciu. Zvyšných 115 ľudí, samozrejme, vybralo druhú možnosť, čo znamená, že pri vykonávaní svojej činnosti sú podriadení. Značná prevaha vedúcich pracovníkov medzi príslušníkmi Policajného zboru je spôsobená tým, že počas distribúcie dotazníka boli oslovení najmä vedúci pracovníci Policajného zboru na všetkých úrovniach.

Dôvodom menšieho záujmu oslovených o vyplnenie dotazníka bola predovšetkým jeho vopred avizovaná časová náročnosť (v priemere 10 až 15 minút), ktorá mohla pracovne zaneprázdnených respondentov odradiť. K úplnému a kvalitnému vyhodnoteniu výskumu bolo potrebné zapracovať vyššie uvedené množstvo otázok v predloženej štruktúre.

Metódy vyhodnocovania dát

Údaje, získané dotazníkovou metódou sme spracovali v programe Microsoft Office Excel a vyhodnocovali pomocou štatistického softvéru PSPP, využitím deskriptívnej (opisnej) analýzy dát. **Softvér PSPP** je open–source, čiže voľne dostupný štatistický softvér zameraný na analýzu dát, ktorý je takmer identický so spoplatneným softvérom SPSS. Hanák[25] tvrdí, že na účel skúmania vzájomných vzťahov medzi premennými môžeme využiť viacero štatistických metód. Výber metódy závisí od charakteru premenných, ktoré sú v našom prípade prevažne **kvalitatívne – nominálne a ordinálne.** Vďaka programu PSPP máme možnosť vypočítať vzťahy medzi premennými použitím viacerých štatistických metód, medzi ktoré patria **kontingenčné tabuľky, test nezávislosti χ^2, Goodmanova – Kruskalova gamma, Kendallovo tau b/tau c, Somersove d** alebo **Spearmanovo rho.** Prehľadné zhrnutie niektorých z týchto štatistických metód, ktoré sme pri celkovom vyhodnocovaní výskumu použili, okrem iných autorov, uvádzajú vo svojom článku aj Šulovská a Holubiczká.[26] Autorky sa zamerali najmä na vyhodnocovanie nominálnych premenných, náš dotazník však obsahuje aj ordinálne premenné a v rámci verifikácie hypotéz bolo potrebné skúmať aj ich vzájomný vzťah. Okrem uvedených základných štatistických metód nám program PSPP ponúka širokú škálu možností vrátane faktorovej analýzy a reliability, ktoré sme využili na úplné vyhodnocovanie údajov a verifikáciu hypotéz.

Informácie uvedené vyššie však majú v našom prípade skôr informatívny charakter vzhľadom na fakt, že tento príspevok, ako sme to už zdôrazňovali vyššie, prezentuje iba čiastkové výsledky výskumu a nezaoberá sa tak hlbšou štatistickou analýzou údajov a verifikáciou predpokladov výskumu. Konečné grafické spracovanie sme vytvorili v Microsoft Office Excel a následne sme výsledky analyzovali a interpretovali. Prostredníctvom nich sme vytvorili odporúčania pre prax.

[25] HANÁK, R. 2016. *Dátová analýza pre sociálne vedy*.
[26] ŠULOVSKÁ, M., HOLUBICZKÁ, S. 2018. *Analýza potrieb učiteľov geografie špeciálnych základných škôl,* s. 314-316.

Ciele práce

V rámci našej výskumnej práce sme skúmali viaceré oblasti informačnej bezpečnosti. V prvom rade bolo dôležité zistiť a ohodnotiť stav technického zabezpečenia jednotlivých systémov využívaných Policajným zborom. Máme na mysli nielen softvérové a hardvérové zabezpečenie, ale aj fyzickú a objektovú bezpečnosť a ďalšie oblasti, ktoré môžu mať svoje slabé miesta. Skúmali sme ich kvalitu vzhľadom na dostupné prístroje, aktualitu, funkčnosť, efektívnosť a štruktúru. V ďalšej časti sme sa zamerali na zistenie a ohodnotenie stavu **informačnej gramotnosti, vzdelanosti a pripravenosti zamestnanco**v Ministerstva vnútra Slovenskej republiky, najmä príslušníkov Policajného zboru, ktorí sú v priamom kontakte s rôznymi systémami a databázami. Podľa nášho názoru je táto časť nosnou v našom výskume, keďže **ľudský faktor je dôležitým prvkom bezpečnosti**. Ak by bol aj technický stav na výbornej úrovni a bezpečnostná politika tiež bezchybná, nikdy nemôžeme mať istotu, že človek, zamestnanec, nepochybí. Preto bol náš výskum zameraný práve na tento fenomén.[27]

Hlavným cieľom nášho výskumu bolo zosumarizovať a analyzovať poznatky o stave bezpečnosti telekomunikačných a informačných technológií, využívaných pri činnostiach Policajného zboru, analýzou prostredia ich použitia (softvér), technických zariadení (hardvér) a **dodržiavania relevantných právnych predpisov a interných aktov obsluhujúcim personálom**. Takto sme dokázali zmapovať súčasný stav ich dodržiavania príslušnými orgánmi, zistiť problémové oblasti bezpečnosti s dôrazom na možné hrozby a zraniteľnosti.

Postupne sme si stanovili **výskumné otázky a všeobecné hypotézy**, pričom sme vychádzali z vopred určeného vedeckého problému, hlavného cieľa výskumu a čiastkových cieľov. Tieto časti nášho výskumu pre ich rozsiahlosť na tomto mieste neuvádzame, tvoria však súčasť dizertačnej práce autora a budú po úspešnej obhajobe zverejnené.

Na tomto mieste uvádzame vyhodnotenie otázok z dotazníka, konkrétne z oblasti hrozieb a zraniteľností zo sekcie „bezpečnosť“.

Bezpečnosť – hrozby a zraniteľnosti

V tejto sekcii otázok, kde skúmame možné hrozby a zraniteľnosti spojené s využívaním informačných a telekomunikačných systémov vychádzame predovšetkým zo subjektívnych názorov a postrehov respondentov. Zvlášť sme vyzývali respondentov, aby na otázky odpovedali čo najúprimnejšie, odpovede však kvôli neurčitému charakteru otázok môžu byť jemne rozptýlené.

Hrozby - vyhodnotenie

Popis otázky: *Kvalitatívna, ordinálna premenná. Povinná otázka. Odpovede použité najmä pri verifikácii pracovnej hypotézy H2. Touto otázkou sledujeme subjektívne vnímanie možných bezpečnostných hrozieb užívateľmi. Reliabilita meraná Cronbachovou alfou dosahuje* $\alpha = 0{,}92$ *na 9 položkách.*

Otázka v dotazníku znela: „*Považujete za reálnu hrozbu na bezpečnosť Vami používaných informačných a telekomunikačných systémov nasledujúce položky?“*, pričom sa odpovede mali určiť na stupnici od „*0 – rozhodne nie“* až po „*5 – rozhodne áno“*, kde neboli určené striktné hodnoty odpovedí. Následne bolo vymenovaných týchto 9 položiek:

- *zneužitie údajov oprávnenou osobou,*

[27] HOLUBICZKY, V. 2019. *Informačné systémy a ich bezpečnosť.*

- *prístup nepovolanej osoby k hardvéru,*
- *získanie prístupových hesiel nepovolanou osobou,*
- *nevyžiadaná pošta,*
- *odpočúvanie komunikácie,*
- *nespoľahlivosť systému,*
- *vandalizmus,*
- *terorizmus,*
- *prírodné katastrofy.*

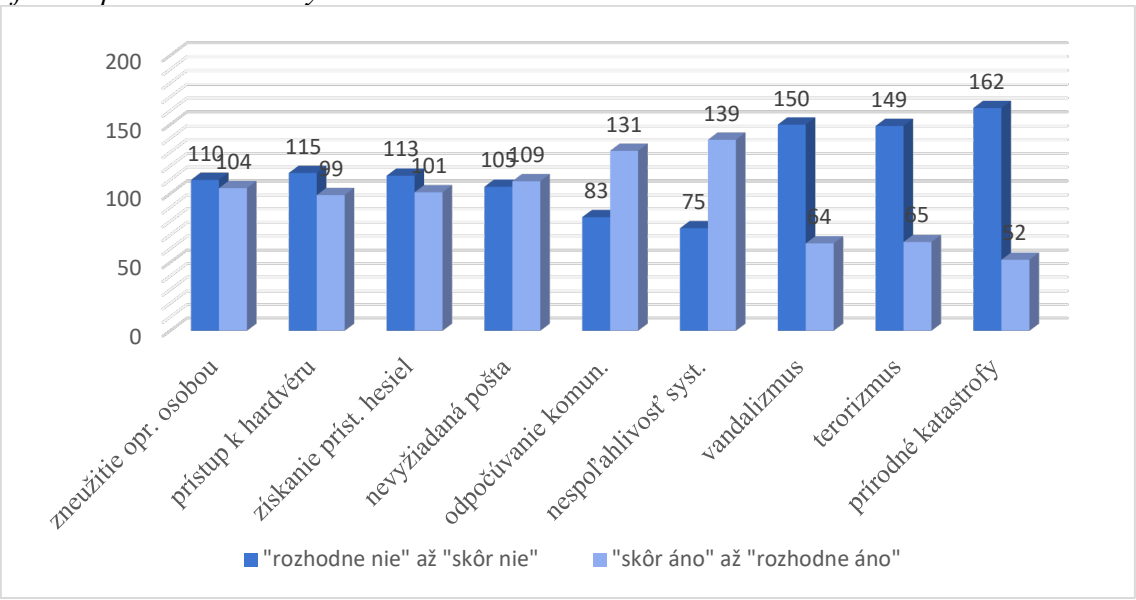
Výsledky sme zhrnuli do tabuľky nižšie, kde sme zelenou farbou vyznačili maximálne hodnoty v jednotlivých riadkoch. Už na prvý pohľad je zrejmá skutočnosť, ako sme na to upozornili už v úvode sekcie, že výsledky nie sú výrazne striktné a vykazujú iba jemné odchýlky.

Tabuľka 1 Bezpečnosť - hrozby

	Rozhodne nie - 0	**1**	**2**	**3**	**4**	**Rozhodne áno - 5**
Zneužitie opr. osobou	38	32	40	28	26	50
Prístup k hardvéru	40	39	36	20	22	57
Získanie prist. hesiel	43	41	29	23	22	56
Nevyžiadaná pošta	33	36	36	34	30	45
Odpočúvanie komun.	26	27	30	31	26	74
Nespoľahl. systému	14	22	39	48	37	54
Vandalizmus	71	44	35	19	14	31
Terorizmus	62	55	32	13	7	45
Prírodné katastrofy	71	62	29	17	11	24

Kategorizovali sme preto odpovede na „*súhlasné*“ a „*nesúhlasné*“ a vytvorili tak graf nižšie, ktorý prehľadne znázorňuje a vyzdvihuje aj menšie odchýlky. V prvom rade je evidentný záporný postoj respondentov v rozmedzí 70% až 75% v položkách vandalizmu, terorizmu a prírodných katastrof. Očakávali sme takýto výsledok a súhlasíme s ním. Výskyt týchto hrozieb je v našich podmienkach momentálne málo pravdepodobný, nemôžeme ale vylúčiť zmeny v budúcnosti.

Graf 1 Bezpečnosť – hrozby



(Zdroj: *vlastné spracovanie)*

Zreteľné sú výsledky aj v otázkach odpočúvania komunikácie a nespoľahlivosti systému, tentokrát ale prevažujú odpovede so súhlasným stanoviskom na hladine 61% až 65%. Môže to byť spôsobené subjektívnym pocitom odpovedajúcich, že tieto skutočnosti nemajú možnosť osobne výrazne ovplyvniť a je tu citeľná zodpovednosť tretích strán, ktoré by mali tieto hrozby v dostatočnej miere eliminovať. Okrem týchto otázok už iba v prípade nevyžiadanej pošty registrujeme neveľké prevýšenie súhlasných odpovedí nad nesúhlasnými v pomere 109:105. Takýto nerozhodný stav sa hodnotí ťažko, aj vo zvyšných prípadoch, kde negatívne odpovede majú veľmi nevýraznú prevahu nad pozitívnymi. Zaujímavým paradoxom je, že keby sme v týchto prípadoch hodnotili výlučne krajné odpovede uvedené v tabuľke, kladné odpovede by získali dominanciu nad krajne zápornými. Z týchto odpovedí nevieme a nemôžeme určiť predčasné závery.

Zraniteľnosti - vyhodnotenie

Popis otázky: *Kvalitatívna, ordinálna premenná. Povinná otázka. Odpovede boli použité pri zodpovedaní viacerých výskumných otázok a pri verifikácii pracovných hypotéz. Reliabilita meraná Cronbachovou alfou dosahuje α = 0,93 na 10 položkách.*

Po otázke o možných hrozbách nasledovala otázka ohľadom zraniteľností, ktorá znie nasledovne: *„Ktoré z nasledujúcich zraniteľností považujete za reálne vo Vami používaných informačných a telekomunikačných systémoch?“*. V prípade tejto otázky sme podobne, ako v predošlých prípadoch, dopredu určili položky, ktoré respondenti mali ohodnotiť súhlasným alebo odmietavým stanoviskom na vyššie popísanej stupnici od 0 po 5. Išlo o týchto 10 nasledovných položiek:

- *technický stav hardvéru,*
- *zastaranosť hardvéru,*
- *zastaranosť softvéru,*
- *neaktuálnosť softvéru,*
- *absencia aplikácií zvyšujúcich bezpečnosť,*
- *neinformovanosť užívateľov,*

- *zlé interné predpisy a smernice,*
- *nedostupnosť školení ohľadom bezpečnosti,*
- *ľahostajnosť užívateľov,*
- *každodenná rutina užívateľov.*

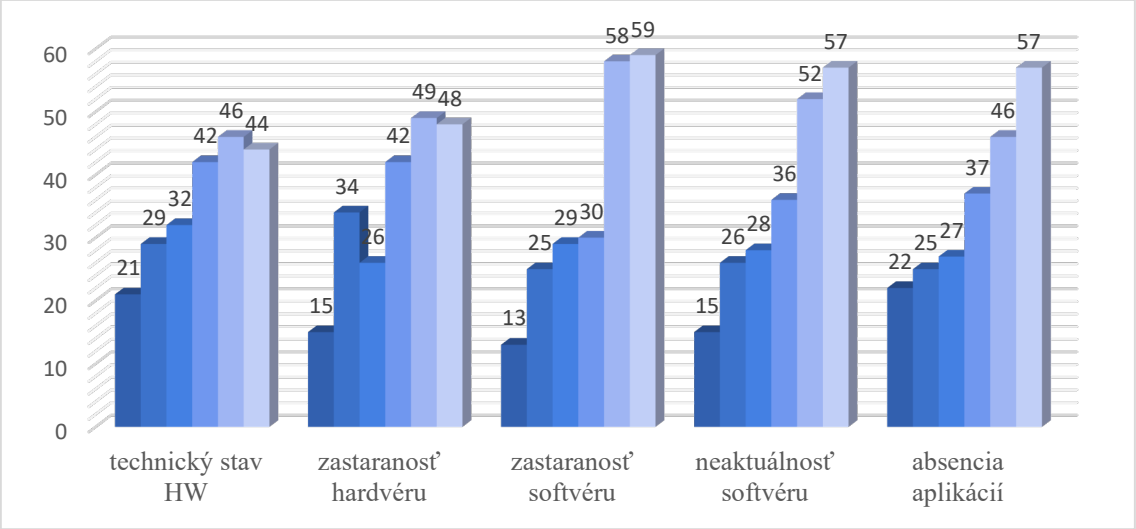
Tabuľka 2 Bezpečnosť - zraniteľnosti

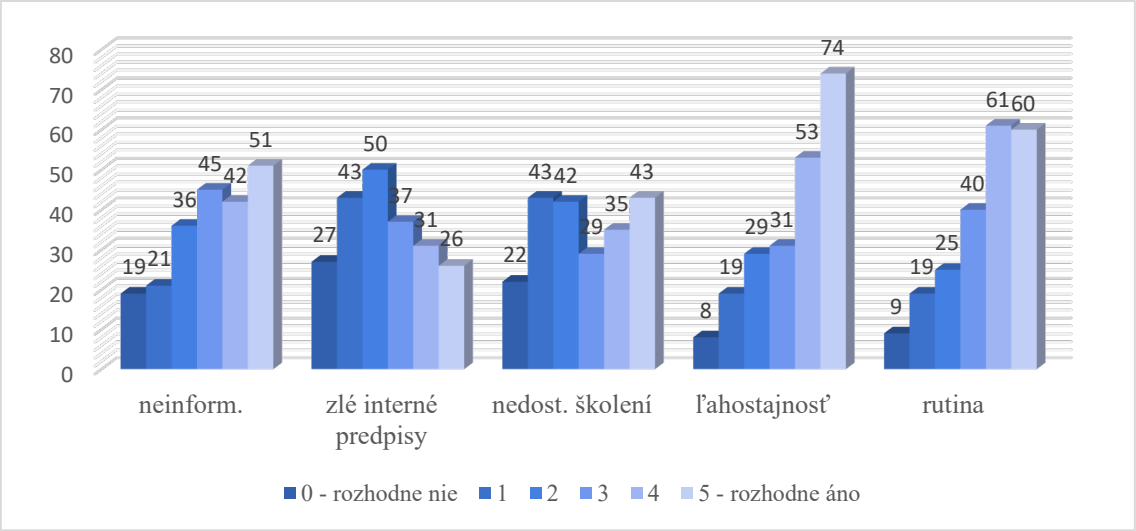
	Rozhodne nie - 0	1	2	3	4	Rozhodne áno - 5
Technický stav HW	21	29	32	42	46	44
Zastaranosť HW	15	34	26	42	49	48
Zastaranosť SW	13	25	29	30	58	59
Neaktuálnosť SW	15	26	28	36	52	57
Absencia aplikácií	22	25	27	37	46	57
Neinformovanosť	19	21	36	45	42	51
Zlé interné predpisy	27	43	50	37	31	26
Nedostupnosť školení	22	43	42	29	35	43
Ľahostajnosť	8	19	29	31	53	74
Rutina	9	19	25	40	61	60

Odpovede sme zhrnuli v tabuľke vyššie. Je vidieť, že odpovede sú aj v tomto prípade rozptýlené, v mnohých položkách sú maximálne početnosti odpovedí mimo krajných hodnôt 0 a 5, avšak prevládajú skôr pozitívne odpovede. Pre lepšiu predstavivosť sme zobrazili výsledky aj na grafe nižšie. Je vidieť takmer v každom prípade stúpajúcu tendenciu počtu odpovedí v smere od možnosti „*rozhodne nie*“ až po možnosť „*rozhodne áno*“. Najvýraznejší výsledok jednoznačne dosiahla zraniteľnosť „*ľahostajnosť užívateľov*“, kde krajné hodnoty majú medzi sebou najväčšiu medzeru.

Ak sa pozrieme aj na celkové výsledky tejto položky, ktoré sú uvedené aj v súhrnnej tabuľke nižšie, zistíme, že je na poprednom mieste s viac ako 73% súhlasných odpovedí. To znamená, že respondenti pokladajú takýto typ zraniteľnosti za reálny a je potrebné sa tým zaoberať. Ľahostajnosť predbehla iba jedna položka, veľmi podobná, a to každodenná rutina užívateľov, keďže dosiahla až viac ako 75% pomer súhlasných odpovedí.

Graf 2 Bezpečnosť – zraniteľnosti, 1. a 2. časť





(Zdroj: vlastné spracovanie)

Tieto dve zraniteľnosti majú spoločnú črtu v tom, že pravdepodobnosť ich výskytu je úzko spojená so samotnými užívateľmi. Iba oni o nich rozhoduje svojim správaním a nedajú sa účinne ovplyvniť treťou stranou. Je možné aplikovať rôzne technologické riešenia na vynútenie určitého správania[28], tiež spracovať a vydávať interné predpisy a smernice[29], ale podľa nášho názoru tieto opatrenia nemusia byť účinné a nedokážu v dostatočnej miere eliminovať ľudský faktor týchto zraniteľností.

Je na mieste vyhodnotiť aj položky týkajúce sa „*absencie aplikácií zvyšujúcich bezpečnosť*“ a „*zlých interných predpisov a smerníc*“. Viac ako 65% dotazovaných súhlasí s tým, že absencia aplikácií vnucujúcich bezpečné správanie užívateľom môže vytvárať reálnu zraniteľnosť systému. Takýto výsledok jednoznačne potvrdzuje ľahostajnosť užívateľov, keďže viditeľne majú určitú snahu zbaviť sa vlastnej zodpovednosti na úkor technológií. Ďalej môžeme povedať, že čiastočne potvrdzujú náš predpoklad prezentovaný vyššie ohľadom interných predpisov a smerníc aj odpovede rovnomennej položky. Tvrdenie, že zlá bezpečnostná politika by predstavovala reálnu zraniteľnosť svojimi odpoveďami vyvrátilo 56% respondentov. Je to značne nevýrazný výsledok a pohľadom na graf vyššie zistíme, že odpovede respondentov sú neisté a značne rozptýlené po celej škále. Môže to znamenať, podľa nášho názoru, práve ľahostajný vzťah respondentov k týmto predpisom.

Tabuľka 3 Bezpečnosť – zraniteľnosti, zhrnutie výsledkov

	Tech. stav HW	**Zastar. HW**	**Zastar. SW**	**Neakt. SW**	**Absencia aplikácií**	**Neinfo.**	**Interné predpisy**	**Nedost. školení**	**Ľahost.**	**Rutina**
Súhlas	132	139	147	145	140	138	94	107	158	161
Nesúhlas	82	75	67	69	74	76	120	107	56	53

Ešte väčšiu mieru zneistenia pozorujeme v prípade nedostupnosti školení ohľadom bezpečnosti. V súhrnnej tabuľke je počet súhlasných a nesúhlasných odpovedí rovnaký a nie je možné jednoznačne určiť názor respondentov. Tvrdíme však, že práve iba kvalitnými školeniami je možné zreteľným spôsobom ovplyvniť správanie a bezpečnostné povedomie

[28] Napr. kontrola sily hesla, blokácia prístupu k určitým internetovým lokalitám atď.
[29] Prihliadajúc na národné a medzinárodné predpisy.

ľudí. Je viac než žiadúce sa venovať problematike školení, čo potvrdzuje aj súhlasné stanovisko viac ako 64% respondentov v otázke neinformovanosti užívateľov. Interné predpisy a smernice síce ponúkajú dostatočné množstvo informácií v rozsahu, ktorý pokrýva všetky zraniteľnosti a hrozby, sú však písané vysoko odborným jazykom a neponúkajú bežným užívateľom zrozumiteľné a jasné pokyny k udržiavaniu vysokej úrovne bezpečnosti. Je dôležité o tejto téme diskutovať v rámci školení a komunikovať priamo s užívateľmi s uvedením praktických rád a príkladov. Zvyšné štyri položky riešili zastaranosť, technický stav a neaktuálnosť softvéru a hardvéru, ktoré sa používajú pri práci s informačnými a telekomunikačnými technológiami. Výsledky sú v rozmedzí 61% až 69% v rovine pozitívnych odpovedí, čo znamená, že podľa respondentov tieto položky môžu mať reálny vplyv na zraniteľnosť systémov.

Okrem priamych odpovedí sme v rámci výskumu pre respondentov vytvorili priestor pomocou doplňujúcich otázok aj na vyjadrenie svojich pocitov k danej téme. Neslúžili na konkrétne vyhodnocovanie výskumných otázok ani na verifikáciu pracovných hypotéz. Majú podporný charakter a pomáhajú pri vytváraní komplexného obrazu názorov respondentov. V tejto časti uvedieme niektoré relevantné a doslovné stanoviská respondentov, aby tak mal čitateľ priestor aj pre vlastné zhodnotenie situácie. Zdôrazňujeme, že tieto tvrdenia nepochádzajú od nás a sú jednoduchým konštatovaním respondentov. Jedna z doplňujúcich otázok znela nasledovne:

- *„Aké sú najčastejšie a najvýznamnejšie hrozby informačnej a telekomunikačnej bezpečnosti v súkromnom sektore / v štátnej sfére (Policajnom zbore)?“.*

Vo väčšine prípadov sa respondenti vyjadrovali stručne, skôr heslovito, kde uvádzali rôzne druhy hrozieb a zraniteľností, ako napr. *„ľudský faktor“, „hacknutie“, „únik informácií“, „prístup neoprávnených osôb“* a iné. Medzi významnejšie odpovede sme zaradili nasledovné:

- *„Najčastejšími hrozbami sú nedostatočná ochrana pridelených prístupových hesiel zo strany policajtov a osobné zlyhanie policajtov pri použití informácií získaných z informačných systémov na iné než služobné účely.“*
- *„Podľa môjho odhadu akákoľvek zmena na informačných a komunikačných systémoch v štátnej správe je zdĺhavá, mnohé systémy sú nepraktické, reakčný čas je dlhý a sú užívateľsky veľmi nepriateľské. Hlavne update systémov je pomalý.“*

Aj k ďalšej otázke ohľadom dodržiavania zásad informačnej bezpečnosti sa vyjadrovali respondenti skôr negatívne, väčšina jednoslovných odpovedí opisovala postoj užívateľov ako *„ľahostajný“*, *„laxný“* alebo jednoducho *„zlý“*. Našli sa aj pozitívne ladené odpovede, ich počet bol však veľmi malý.

Záver – súhrn výsledkov

Po pomerne dlhej analýze jednotlivých otázok dotazníka sa rozhodnými krokmi dostávame k čiastkovým záverom nášho výskumu. V tejto časti sa budeme snažiť zhrnúť všetky dosiahnuté výsledky, vyhodnotiť mieru naplnenia našich cieľov a vytvoriť tak ucelený obraz o našej práci.

Jedným z cieľov výskumu bolo **zmapovať súčasnú situáciu bezpečnostných hrozieb a zraniteľností, predpovedať ich budúci vývoj**. Obe oblasti, zraniteľnosti i hrozby, boli zahrnuté v samostatnej sekcii otázok a na prvom mieste sa budeme venovať bezpečnostným hrozbám respondentmi používaných informačných a telekomunikačných systémov. Už na prvý pohľad bolo z odpovedí jasné, že položky ako *„vandalizmus“, „terorizmus“* alebo

„prírodné katastrofy“ nepovažujú respondenti za relevantné. S takýmto názorom v určitej miere súhlasíme, keďže v Slovenskej republike nemáme takmer žiadne osobné skúsenosti s takýmito druhmi hrozieb, zatiaľ. Je zaujímavé, že na prvom mieste ako relevantná hrozba skončila, podľa počtu hlasov, *„nespoľahlivosť systému“*. Táto položka úzko súvisí s technickým stavom hardvéru i softvéru a môže viesť k nemalým komplikáciám a strate informácií. Druhú priečku obsadila hrozba *„odpočúvanie komunikácie“* a aj ostatné položky dosahovali približne 50% súhlasných stanovísk k reálnosti ich výskytu. Hodnotíme pozitívne, že užívatelia sú aspoň z časti oboznámení s hrozbami a dokážu ich identifikovať. Nie menej dôležité sú zraniteľnosti využívaných technológií, ktorých prítomnosť, na základe výsledkov z dotazníka, môžeme jednoznačne potvrdiť. Respondenti sa vyjadrovali kriticky najmä v položkách ohľadom technického stavu a zastaranosti hardvéru aj softvéru a vnímajú tieto zraniteľnosti ako reálne. Okrem toho sa umiestnili na popredných miestach aj tvrdenia ohľadom *„ľahostajnosti“* a *„každodennej rutiny“* užívateľov. Zastávame názor, že odstránenie potencionálnych zraniteľností alebo eliminácia pravdepodobnosti ich výskytu je prvoradou úlohou na ceste k budúcnosti bez incidentov.

Naše odporúčania smerujú, v prípade hrozieb a zraniteľností, k uvedomeniu si ich existencie. Je to prvý krok k tomu, aby sme pozitívne ovplyvnili riziko ich výskytu a potencionálne nebezpečenstvo. Mnohé druhy hrozieb a zraniteľností nedokážeme efektívne riadiť alebo eliminovať, ale myslíme si, že človek – užívateľ má obrovský potenciál, byť účinným nástrojom. Znovu tak prízvukujeme náš, už vyššie niekoľkokrát opakovaný názor, že najefektívnejším nástrojom k dosiahnutiu požadovaného stavu informačnej bezpečnosti sú popri správnom a kvalitnom technickom zabezpečení aj školenia a podanie informácií zrozumiteľným spôsobom na všetkých úrovniach pracovných pozícií.

Na záver uvádzame, bez komentára, vyjadrenia niekoľkých opýtaných expertov na otázku, v čom vidia najvýraznejšie a najzávažnejšie hrozby a zraniteľnosti informačných systémov:

- *„Sú viaceré, závisí to od organizácie, nastavených pravidiel a kontroly ich dodržiavania. Jednoznačne však naďalej prevláda ľudský faktor.“*
- *„Prienik sociálno-manipulačných techník do IKT najmä na úrovni technologických útokov.“*
- *„V rapídnom a permanentne narastajúcom počte čoraz sofistikovanejších útokov, rozvoj ľahko, prostredníctvom internetu, dostupných zdrojov útokov, ktoré dokáže útočník používať aj bez väčších odborných znalostí.“*

Literatúra

BARIČIČOVÁ, Ľ. a M. PAJPACHOVÁ, 2014. *Hodnotenie interných faktorov úspechu policajnej organizácie ako východisko možných zmien v procese jej riadenia*. In: Policajná teória a prax. Roč. 22, č. 4, s. 5-26. ISSN 1335-1370.

BUDÍKOVÁ, M., M. KRÁLOVÁ, B. MAROŠ, 2010. *Průvodce základními statistickými medotami*. Praha: Grada publishing, a.s. ISBN 978-80-247-3243-5.

BUZALKA, J. a V. BLAŽEK, 2011. *Metodológia a metodika vypracovania analýzy vnútorného ohrozenia bezpečnosti SR a z nej vyplývajúcich ohrození a rizík*. In: Metodológia a metodika analýzy zdrojov ohrozenia vnútornej bezpečnosti Slovenskej republiky. Bratislava: Akadémia Policajného zboru v Bratislave, s. 16-39. ISBN 978-80-8054-517-8.

HANÁK, R., 2016. *Dátová analýza pre sociálne vedy*. Bratislava: Vydavateľstvo Ekonóm, 151 s. ISBN 978-80-225-4345-3.

HOLUBICZKY, V., 2018. *Vzdelaný policajt, garant bezpečnosti*. In: Polícia ako garant bezpečnosti – zborník príspevkov z medzinárodnej vedeckej konferencie. Bratislava: Akadémia Policajného zboru v Bratislave, s. 105-113. ISBN 978-80-8054-751-6.

HOLUBICZKY, V., 2019. *Bezpečnosť informačných systémov – ľudský faktor*. In: Zborník zo 14. medzinárodného sympózia konaného dňa 14. 3. 2019 v rámci medzinárodného veľtrhu SECURITY BRATISLAVA 2019. Bratislava: Akadémia Policajného zboru v Bratislave, s. 177 – 187. ISBN 978-80-8054-795-0.

HOLUBICZKY, V., 2019. *Informačné systémy a ich bezpečnosť*. In: Vedecká konferencia doktorandov na APZ v Bratislave. Zborník príspevkov z 2. ročníka. Bratislava: Akadémia Policajného zboru v Bratislave, s. 93 – 99. ISBN 978-80-8054-824-7.

IGENYES, L., V. HOLUBICZKY, 2017. *Úvaha o používaní zbraní súkromnými bezpečnostnými službami v prípade hromadného nasadenia na verejných kultúrnych a športových podujatiach* In: Zborník z konferencie s medzinárodnou účasťou konanej dňa 15. novembra 2016 – Spoločenský boj proti diváckemu násiliu. Bratislava: Akadémia Policajného zboru v Bratislave, s. 56- 64. ISBN 978-80-8054-710-3

IGENYES, L., V. HOLUBICZKY, 2018. *Ochrana určených osôb a objektov 1 – Mechanické zábranné prostriedky*, Bratislava: Akadémia Policajného zboru v Bratislave, 180 s. ISBN 978-80-8054-786-8.

Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020.

KOPENCOVÁ, D., R. RAK, 2019. *Risk Analysis and Threats in Security Sciences*. In: Európska veda, vedecký časopis 3/2019. Podhájska: Európsky inštitút ďalšieho vzdelávania. s. 109-115. ISSN: 2585-7738.

KRESL, E., 2018. *Východiská legislatívnej prevencie počítačovej kriminality.* In: BARIČIČOVÁ, Ľ. (ed.) 2018. *Aktuálne výzvy prevencie počítačovej kriminality.* Bratislava: Akadémia Policajného zboru v Bratislave. ISBN 978-80-8054-773-8.

KURILOVSKÁ, L., S. ŠIŠULÁK, 2017. *Použitie inštitútu agenta pri odhaľovaní a objasňovaní kriminality v kybernetickom prostredí.* In: ZÁHORA, J.(ed.) 2017. *Teoretické a praktické problémy využívania informačno-technických prostriedkov v trestnom konaní.* Praha: Nakladatelství Leges, s. r. o., 284 s. ISBN 978-80-7502-206-6.

LÖFFLER, B., M. ANTAL, 2017. *Vybrané aspekty ochrany verejného poriadku v Slovenskej republike.* Bratislava: Akadémia Policajného zboru v Bratislave, 114 s. ISBN 978-80-8054-726-4.

MEDELSKÝ, J., 2018. *Bezpečnostno-strategické dokumenty.* In: Polícia ako garant bezpečnosti. Zborník príspevkov z vedeckej konferencie. Bratislava: Akadémia Policajného zboru v Bratislave, s. 252 -253. ISBN 978-80-8054-751-6.

MIKOLAJ, J., L. HOFREITER, V. MACH, J. MIHÓK, P. SELINGER, 2004. *Terminológia bezpečnostného manažmentu: Výkladový slovník.* Košice: Multiprint, 191 s. ISBN 80-969148-1-2.

Nariadenie MV SR č. 35/2018 o bezpečnostnej politike pre oblasť informačných systémov

RAK, R., P. KOLITSCHOVÁ, 2019. *Bezpečnost a bezpečí – základní pojmy a jejich vnímání.* In: Zborník zo 14. medzinárodného sympózia konaného dňa 14. 3. 2019 v rámci medzinárodného veľtrhu SECURITY BRATISLAVA 2019. Bratislava: Akadémia Policajného zboru v Bratislave. s. 28 – 40. ISBN 978-80-8054-795-0.

RAK, R., D. KOPENCOVÁ, 2019. *Bezpečnostní hrozby, vlastnosti a fáze*. In: Zborník zo 14. medzinárodného sympózia konaného dňa 14. 3. 2019 v rámci medzinárodného veľtrhu SECURITY BRATISLAVA 2019. Bratislava: Akadémia Policajného zboru v Bratislave. s. 72 – 85. ISBN 978-80-8054-795-0.

RAK, R., D. KOPENCOVÁ, M. FELCAN, 2019. *Objekty a systémy – základní analytické prvky bezpečnosti*. In: Zborník zo 14. medzinárodného sympózia konaného dňa 14. 3. 2019 v rámci medzinárodného veľtrhu SECURITY BRATISLAVA 2019. Bratislava: Akadémia Policajného zboru v Bratislave, s. 41 – 55. ISBN 978-80-8054-795-0.

ŠIMÁK, L. a kol., 2005. *Terminologický slovník krízového riadenia: Aktualizované vydanie v roku 2006.* Žilina: Žilinská univerzita v Žiline. 44 s. ISBN 80-88829-75-5.

ŠULOVSKÁ, M. a S. HOLUBICZKÁ, 2018. *Analýza potrieb učiteľov geografie špeciálnych základných škôl.* In: Pedagogica specialis XXXII. Bratislava: Univerzita Komenského v Bratislave, s. 312-327. ISBN 978-80-223-4610-8.

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predisov.

Keywords: security, information technologies, threats, human factor.

Summary

This paper describes the current state of security of telecommunication and information technologies used in the activities of the Police Force in comparison with other sectors. The main aim of this paper was to find out, describe and analyze information about the state of security of these systems. Its theoretical part focuses on the definition of basic terms, such as 'technology', 'security', 'data', 'information' and others. Besides that, it summarizes knowledge about information security and cybercrime and provides an introduction to the empirical part of the paper. It focuses on our own research via questioning respondents from the environment of the Police Force. Statistically based research results from 214 respondents including 137 members of the Police Force, it points to some inappropriate habits at work with technologies. We have identified some shortcomings in the interpretation of the results. Therefore; paper includes specific recommendations to eliminate vulnerability and to increase the level of security.

kpt. Ing. Vincent Holubiczky
Katedra európskeho integrovaného riadenia hraníc
Akadémia Policajného zboru v Bratislave
e-mail: vincent.holubiczky@minv.sk

Recenzenti: pplk. doc. RNDr. Tatiana Hajdúková, PhD.
mjr. JUDr. Matej Kostrec, PhD.