Vplyv školení užívateľov na bezpečnosť informačných a telekomunikačných systémov

The impact of user training on the security of information and telecommunication systems

Vincent Holubiczky[1]

Abstrakt: Vedecká štúdia je zameraná na prezentáciu parciálnych výsledkov čiastkovej úlohy „*Internet vecí – podstata, hrozby a riziká*“ z vedeckovýskumnej úlohy VÝSK. 245[2], ktorá je realizovaná na Akadémii Policajného zboru v Bratislave. Výskum bol realizovaný prostredníctvom dotazovania respondentov z prostredia Policajného zboru, iných štátnych inštitúcií a tiež súkromného sektora. Autor sa vo vedeckej štúdií venuje najmä vplyvu školení na vznik bezpečnostných incidentov pri využívaní telekomunikačných a informačných technológií.

Kľúčové slová: bezpečnosť, informačné systémy, školenie, bezpečnostné incidenty

Abstract: This paper was created within the solution of the partial task „Internet of Things“ of scientific research VÝSK. 245, registered at the Academy of the Police Force in Bratislava. This scientific paper focuses on the author's own research via questioning respondents from the environment of the Police Force, other state institutions as well as people from private sector. Additionally we focus mainly on the impact of user training on the security of information and telecommunication systems.

Key words: security, information systems, training, security incidents

Úvod

Žijeme v digitálnej dobe s extrémnym množstvom rôznych technológií, ktoré využívame v každodennom živote. Nie je tomu inak ani v týchto časoch, keď je takmer celý svet a mnohé krajiny paralyzované pandémiou koronavírusu - COVID19. Kvôli tejto hrozbe na naše zdravie a životy sa v mnohých prípadoch presunula práca do online priestoru.[3]

Informačná bezpečnosť sa stala okamžite stredobodom pozornosti. 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.[4]

Je dôležité si uvedomiť, že práve týmto spôsobom vykonávania pracovných povinností vznikajú určité riziká vzhľadom na únik a stratu citlivých informácií. Okrem toho v domácom prostredí často môže lákať užívateľov miešanie súkromných záležitostí s pracovnými povinnosťami. Takzvaný „internet vecí“ dnes ponúka nevídané možnosti online priestoru, ktoré by sme pred niekoľkými rokmi nečakali ani v najodvážnejších vedecko-fantastických filmoch.[5]

---

[1] mjr. Ing. Vincent Holubiczky, PhD., - odborný asistent, Katedra európskeho integrovaného riadenia hraníc, Akadémia Policajného zboru v Bratislave

[2] FELCAN, M. a kol. 2019. *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*. VVÚ VÝSK. 245. Akadémia Policajného zboru v Bratislave..

[3] HOLUBICZKY, V. 2020. *Moderné technológie a účel ich využívania.*

[4] HOLUBICZKY, V. 2020. *Frekvencia využívania moderných technológií Policajným zborom.*

[5] HOLUBICZKY, V. 2020. *Prítomnosť hrozieb a zraniteľností pri využívaní informačných technológií.*

Všade prítomné technológie a online prostredie v každodennom živote nás robia menej citlivými na potencionálne hrozby a zraniteľnosti.[6]
Rozhodli sme sa v tomto príspevku priblížiť čitateľom čiastkové výsledky nášho výskumu ohľadom bezpečnosti pri pomerne bežných činnostiach v rámci práce užívateľov s telekomunikačnými a informačnými technológiami používaných v súkromnom sektore aj príslušníkmi Policajného zboru. Výskum bol realizovaný v rámci dizertačnej práce autora a zároveň už v abstrakte uvedenej vedeckovýskumnej úlohy VÝSK. 245 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“. Výsledky nášho bádania budú využité konkrétne pri vyhodnocovaní čiastkovej úlohy č. 6 – „Internet vecí – podstata, hrozby a riziká“.
S touto problematikou súvisí mnoho pojmov, ako napríklad bezpečnosť, hrozba, riziko, online prostredie, informácie, údaje a iné.[7] Vzťah hrozieb a bezpečnosti popisuje mnoho autorov, medzi ktorými sa tejto téme intenzívne venuje Rak v spolupráci s Kopencovou a Kolitschovou. Bezpečnosť je mimoriadne komplexným a viacrozmerným fenoménom, ktorý zahŕňa veľké množstvo oblastí a oborov – spoločenskovedných, prírodovedných ale i technických, kde neodlučiteľne patrí aj informatika. Každý obor vníma bezpečnosť podľa svojej teórie, praxe, zamerania, znalostí a skúseností.[8] Hrozby môžeme deliť podľa rôznych kritérií[9], čo s týka ale našej problematiky, pri využívaní moderných technológií sú jednoznačne najčastejšie prítomné *„technogénne“* a *„sociogénne“* oblasti, ktorých zdrojom je človek. Tieto antropogénne hrozby môžu byť spôsobené úmyselne alebo neúmyselne[i], vždy je potrebné ale dbať na to, aby sme v čo najväčšej miere znížili riziko ich výskytu.[10]
Tento príspevok prezentuje iba čiastkové výsledky výskumu a nezaoberá sa tak hlbšou štatistickou analýzou údajov a verifikáciou predpokladov výskumu.[11]

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, 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 oslovení 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 ale vieme povedať, že odkaz bol doručený viac ako 2000 osobám a celkový počet vyplnených dotazníkov je 214. Znamená to približne 10%, pričom táto hodnota sa môže zdať nízka, je však podľa nášho názoru dostatočná na kvantitatívne aj kvalitatívne vyhodnotenie výskumu.[12]

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%)

[6] HOLUBICZKY, V. 2020. *Moderné technológie a účel ich využívania.*
[7] RAK, R., KOLITSCHOVÁ, P. 2019. *Bezpečnost a bezpečí – základní pojmy a jejich vnímání.*
[8] RAK, R., KOPENCOVÁ, D. 2019. *Bezpečnostní hrozby, vlastnosti a fáze*.
[9] KOPENCOVÁ, D., RAK, R. 2019. *Risk Analysis and Threats in Security Sciences*.
[10] HOLUBICZKY, V. 2018. *Vzdelaný policajt, garant bezpečnosti*.
[11] HOLUBICZKY, V. 2020. *Moderné technológie a účel ich využívania.*
[12] HOLUBICZKY, V. 2020. *Prítomnosť hrozieb a zraniteľností pri využívaní informačných technológií*.

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.

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.[13]

Na tomto mieste uvádzame vyhodnotenie výskumných otázok, zodpovedaním ktorých dostaneme komplexný obraz vnímania bezpečnosti výskumnej vzorky a cenné informácie o ich nebezpečných zvykoch, ktoré môžu viesť k bezpečnostným incidentom. Je dôležité si pripomenúť, že cieľom tejto vedeckej štúdie je poskytnúť čiastkové výsledky výskumu, nebudeme sa preto venovať vyhodnocovaniu jednotlivých otázok z dotazníka, ale zameriavame sa výlučne na hodnotenie vybraných výskumných otázok. Je možné pri tom, že sa odvoláme na výsledky z konkrétnych otázok dotazníka, tieto údaje však budú vždy prehľadne spracované v tabuľkách a vhodne graficky znázornené.

Na tomto mieste uvádzame výskumné otázky, ktoré sa budeme snažiť na nasledujúcich riadkoch zodpovedať a výsledky analyzovať. Pri stanovení **výskumných otázok** sme vychádzali z vedeckého problému a tiež z určeného hlavného cieľa výskumu a čiastkových cieľov. Pomocou týchto otázok, resp. ich zodpovedaním po vykonaní výskumu, sa budeme snažiť odhaliť niektoré hlbšie súvislosti premenných. Stanovili sme si tieto výskumné otázky:

- **Výskumná otázka č. 1:** Aký vplyv má školenie na dodržiavanie interných predpisov?
- **Výskumná otázka č. 2:** Aké zvyky majú užívatelia, ktoré používajú pracovné zariadenia na súkromné účely?
- **Výskumná otázka č. 3:** Ako vplýva dĺžka praxe na výskyt bezpečnostných incidentov?
- **Výskumná otázka č. 4:** Aké sú rozdiely v názoroch na školenia a podporu tých, ktorí už takéto školenie absolvovali a tých, ktorí nie?

Niektoré výskumné otázky nie je možné vyhodnotiť jednoducho, iba pomocou jednej otázky z dotazníka. Často je potrebné použiť celú sekciu otázok, prípadne kombináciu rôznych sekcií, aby sme názorne objasnili súvislosti. Ideálnym pomocníkom v tomto prípade je využitie kontingenčných tabuliek s uvedením početností odpovedí.

Aký vplyv má školenie na dodržiavanie interných predpisov?

V tejto otázke sa budeme venovať možnostiam povzbudenia užívateľov k dodržiavaniu predpisov, resp. chceme zistiť, aký vplyv na to má účasť na školení. Využili sme k tomu dve otázky zo sekcie otázok z dotazníka „školenia a podpora“ a výsledky sme zhrnuli v tabuľke nižšie. V tabuľke nižšie sú uvedené stupnice odpovedí, kde 0 znamená rozhodné odmietnutie tvrdenia (rozhodne nie), až číslo 5 označuje rozhodný súhlas respondenta. Takáto stupnica je použitá aj vo vyhodnotení zvyšných otázok.

Zo sumárnych početností je zrejmé, že väčšina respondentov uvádza, že predpisy dodržuje. Aký je stav vzhľadom na *„účasť na školení ohľadom informačnej bezpečnosti“* vidíme na grafe nižšie. Respondentov sme rozdelili do dvoch skupín.

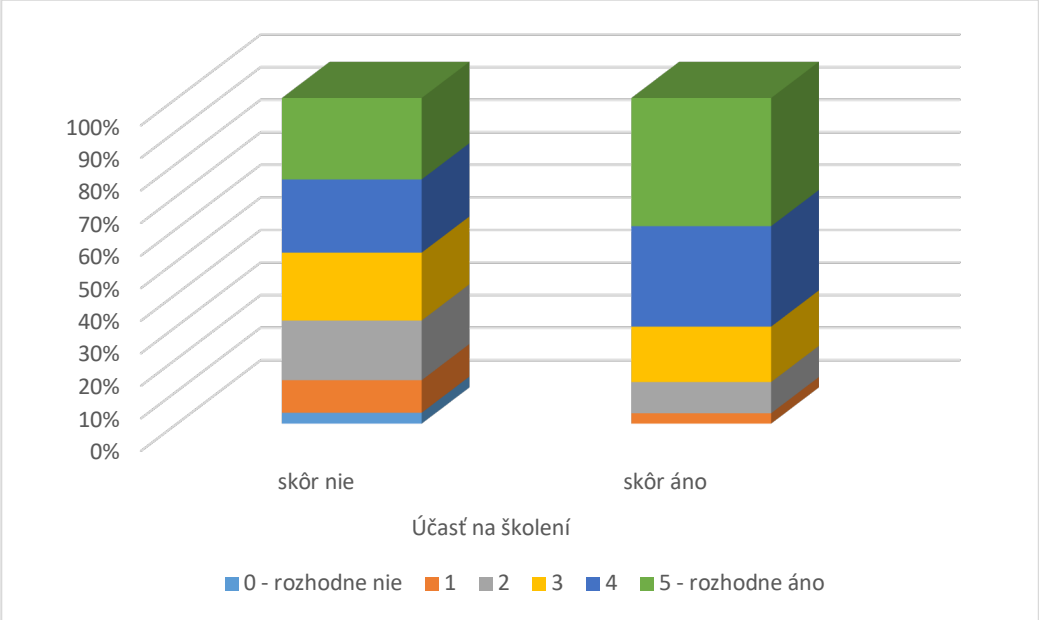
[13] HOLUBICZKY, V. 2020. *Prítomnosť hrozieb a zraniteľností pri využívaní informačných technológií.*

Tabuľka 1 Vplyv školenia na dodržiavanie interných predpisov

Kontingenčná tabuľka k VO5		Školenia a podpora (dodržiavanie predpisov)						
		0	1	2	3	4	5	Σ
Školenia a podpora (účasť na školení)	0	1	8	9	13	12	16	59
	1	2	2	4	4	12	7	31
	2	1	2	9	8	3	7	30
	3	0	2	3	3	5	7	20
	4	0	0	3	3	12	4	22
	5	0	1	3	10	12	26	52
	Σ	4	15	31	41	56	67	214

V prvom stĺpci je skupina, ktorá uviedla skôr negatívne odpovede na účasť na školeniach, druhý stĺpec grafu značí ostatných respondentov. Následne farebná škála značí ich postoj k dodržiavaniu predpisov. Môžeme vidieť, nie príliš veľký, ale badateľný rozdiel, ktorý značí pozitívny vplyv školení. Iba približne 13% školených respondentov uviedlo, že skôr nedodržiava predpisy, kým na strane neškolených, resp, menej školených dotazovaných je táto hodnota až na úrovni necelých 32%.

Graf 1 Vplyv školenia na dodržiavanie interných predpisov



(Zdroj: vlastné spracovanie)

Zastávame názor, že školenia sú účinným nástrojom v boji proti vzniku bezpečnostných incidentov a jednoznačne vnímame ich pridanú hodnotu aj v rámci informovanosti a bezpečnostného povedomia užívateľov.

Aké zvyky majú užívatelia, ktorí používajú pracovné zariadenia na súkromné účely?

Táto výskumná otázka vytvára priestor pre skúmanie prípadu, kedy užívatelia využívajú pracovné zariadenia a systémy na súkromné účely. Konkrétne sa zameriame na bezpečnostné zvyky týchto užívateľov, keďže nezodpovedným správaním by mohli ohroziť integritu, dôvernosť a dostupnosť technológií určených predovšetkým a výlučne na prácu.

Tabuľka 2 Zvyky užívateľov využívajúcich pracovné počítače na súkromné účely

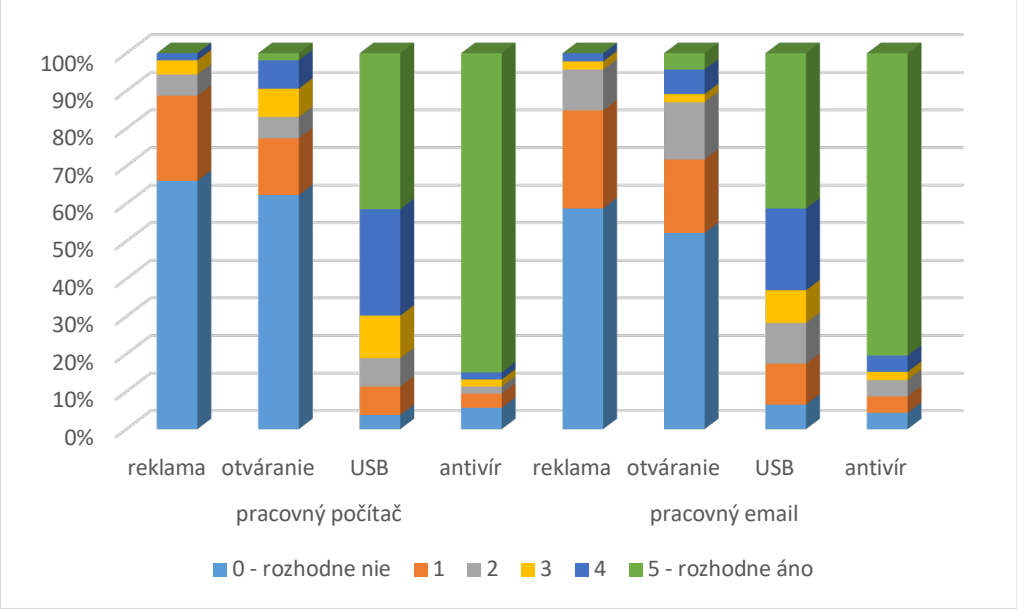
Kontingenčná tabuľka k VO7		Zvyky						
		0	1	2	3	4	5	Σ
Účel (pracovný počítač na súkromné účely)	reklama	35	12	3	2	1	0	53
	otváranie	33	8	3	4	4	1	53
	USB	2	4	4	6	15	22	53
	antivírus	3	2	1	1	1	45	53
	Σ	73	26	11	13	21	68	212

Tabuľka 3 Zvyky užívateľov využívajúcich pracovný email na súkromné účely

Kontingenčná tabuľka k VO7		Zvyky						
		0	1	2	3	4	5	Σ
Účel (pracovný email na súkromné účely)	reklama	35	12	3	2	1	0	53
	otváranie	33	8	3	4	4	1	53
	USB	2	4	4	6	15	22	53
	antivírus	3	2	1	1	1	45	53
	Σ	73	26	11	13	21	68	212

Okruh respondentov sme filtrovali na základe odpovedí na položky *„pracovný počítač“* a *„pracovný email“* zo sekcie otázok ohľadom účelu využívania technológií. Berieme do úvahy iba tých, ktorí svojou odpoveďou potvrdili, že využívajú pracovné zariadenia aj na súkromné účely. Následne sme zistili početnosti ich odpovedí na otázky zo sekcie *„Zvyky“*, konkrétne ohľadom *„reklamných ponúk v elektronickej pošte“*, *„otvárania správ od neznámych odosielateľov“*, *„používania USB na prenos údajov medzi počítačmi“* a *„prítomnosti antivírového programu“*. Údaje sú zobrazené v tabuľkách vyššie.

Graf 2 Zvyky užívateľov využívajúcich pracovné technológie na súkromné účely



(Zdroj: vlastné spracovanie)

Hodnoty sme následne prepočítali na percentuálne ukazovatele podľa riadkov a vytvorili graf nižšie, ktorý prehľadne prezentuje výsledky. V prípade reklám a otvárania správ od

neznámych odosielateľov sa naplnili naše očakávania, keďže jednotlivci výberovej skupiny k nim, v oboch prípadoch, prejavili rozhodné, odmietavé stanovisko na úrovni až 90%. Aj v prípade používania antivírových aplikácií sú odpovede respondentov na vynikajúcej úrovni, prítomnosť takéhoto softvéru potvrdilo približne 86% až 89% z nich. Pozitívne výsledky sa však v prípade používania USB na prenos údajov medzi počítačmi menia na znepokojujúce. Nekontrolované využívanie prenosových médií prináša so sebou veľkú pravdepodobnosť výskytu bezpečnostných incidentov. Napriek tomu až približne ¾ respondentov výberovej skupiny označilo, že ich skôr využíva ako nevyužíva.

Na základe vyššie uvedených, odpoveďou na výskumnú otázku môže byť, že užívatelia, ktorí využívajú pracovné počítače aj na súkromné účely majú prevažne dobré zvyky pri práci s technológiami a zmierňujú tak riziko vplyvu hrozieb a zraniteľností. Samozrejme, týmto vyjadrením v žiadnom prípade neschvaľujeme a nepodporujeme elementárnu skutočnosť, že vôbec využívajú pracovné zariadenia na súkromné účely. Tento názor zastávame osobitne aj v prípade využívania fyzických prenosových médií.

Ako vplýva dĺžka praxe na výskyt bezpečnostných incidentov?

Otázka ponúka možnosť hlbšieho prebádania otázok ohľadom výskytu bezpečnostných incidentov vzhľadom na dĺžku praxe respondentov. Respondenti odpovedali na stupnici 0 – nikdy až 5 často. Takáto škála odpovedí nám umožňuje rozdeliť odpovede do dvoch skupín, a to takých, kde prvú skupinu budú tvoriť respondenti, ktorí sa *„nikdy“* nestretli s výskytom incidentu a na druhej strane budú tí, ktorí *„už“* zaznamenali jeho výskyt, bez ohľadu na jeho frekvenciu. Vybrali sme štyri vzorové položky zo súboru incidentov, a to *„únik utajovaných skutočností“*, *„únik informácií“*, *„zneužitie oprávnenou osobou“* a *„poskytnutie prístupu neoprávnenej osobe“*. Výsledky sú zhrnuté v tabuľke nižšie.

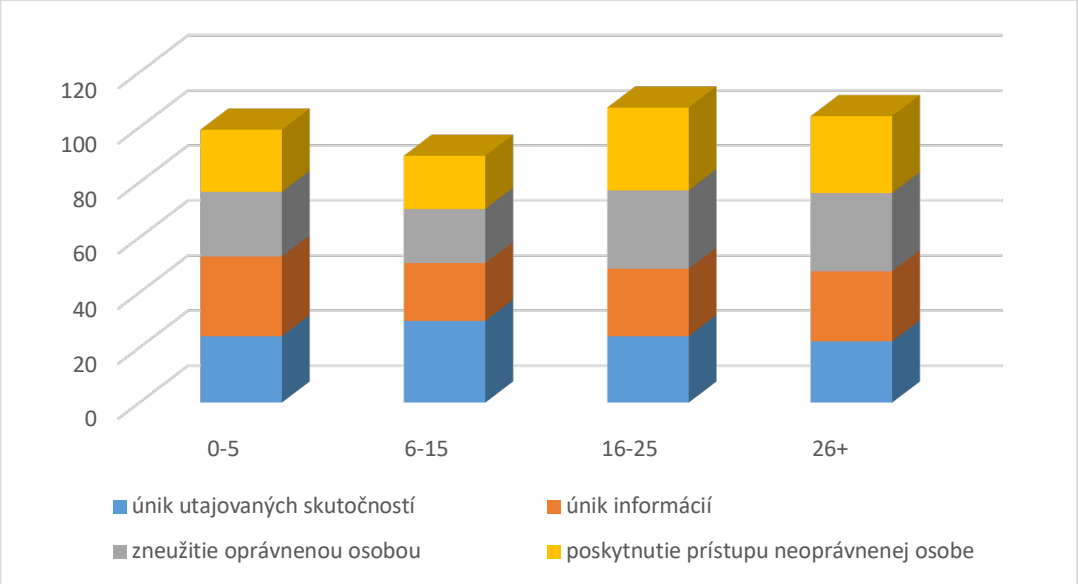
Tabuľka 4 Vplyv dĺžky praxe na výskyt incidentov

Kontingenčná tabuľka k VO8		Incidenty: únik utaj. skutočností		únik informácií		zneužitie opr. osobou		posk. prist. neopr. os.		Σ p. p.
		nik.	už	nik.	už	nik.	už	nik.	už	
Dĺžka praxe	0 – 5	43	13	23	33	32	24	35	21	56
	6 – 15	30	16	22	24	26	20	28	18	46
	16 – 25	43	13	28	28	27	29	28	28	56
	26+	44	12	27	29	27	29	30	26	56
	Σ	160	54	100	114	112	102	121	93	214

Nižšie sme graficky spracovali údaje o počte zachytených incidentov v závislosti od dĺžky praxe respondentov. Rozdiely sú veľmi malé, tak v rozložení incidentov podľa druhu, ako aj podľa dĺžky praxe. Je to určitý paradox, že napriek takýmto časovým rozpätiam sa výskyt incidentov nezvyšuje priamo úmerne. Predpokladali sme markantnejšie rozdiely vo výsledkoch v prospech dlhšej praxe, avšak rovnomerne rozložené hodnoty poukazujú na iné súvislosti.

Možným vysvetlením výsledkov môže byť, že incidenty takéhoto druhu sa vyskytujú pomerne krátke obdobie. Preto aj zamestnanci s dlhšou praxou registrovali iba také incidenty, ktoré už mohli evidovať aj respondenti s kratšou praxou. Znamenalo by to väčšiu hustotu výskytu incidentov za posledné obdobie, čo môže byť varovaním k prognóze blízkej budúcnosti.

Graf 3 Vplyv dĺžky praxe na výskyt incidentov



(Zdroj: vlastné spracovanie)

Aké sú rozdiely v názoroch na školenia a podporu tých, ktorí už takéto školenie absolvovali a tých, ktorí nie?

Poslednou výskumnou otázkou chceme zistiť, aký je rozdiel vo vnímaní školení tých, ktorí už školenia niekedy absolvovali a tých, ktorí sa školení zúčastňujú zriedka, resp. nikdy neabsolvovali. Respondentov sme rozdelili do týchto dvoch skupín na základe ich odpovedí na otázku *„Absolvovali ste niekedy školenie ohľadom informačnej bezpečnosti?“*. Pre jednoduchosť označenia sme pomenovali skupiny „*neabsolvoval*“, kde sú zahrnuté odpovede 0 až 2 zo stupnice, a „*absolvoval*“ s hodnotami 3 až 5. Následne v tabuľkách nižšie uvádzame početnosti odpovedí týchto skupín na otázky zo sekcie „*školenia a podpora*“, konkrétne ohľadom „*pozitívneho účinku školení*“, „*potreby zvyšovania kvalifikácie*“, „*vlastného pocitu potreby absolvovania školenia*“ a „*dostatočnosti ponúk školení*“.

Tabuľka 5 Pozitívny účinok školenia podľa účasti na školení

Kontingenčná tabuľka k VO9		Školenia a podpora (pozitívny účinok)						
		0	1	2	3	4	5	Σ
Školenia a podpora (účasť)	neabsolvoval	19	14	27	18	15	27	120
	absolvoval	1	2	12	18	23	38	94
	Σ	20	16	39	36	38	65	214

Tabuľka 6 Potreba zvyšovania kvalifikácie podľa účasti na školení

Kontingenčná tabuľka k VO9		Školenia a podpora (zvyšovanie kvalifikácie)						
		0	1	2	3	4	5	Σ
Školenia a podpora (účasť)	neabsolvoval	3	6	15	24	22	50	120
	absolvoval	0	0	4	15	23	52	94
	Σ	3	6	19	39	45	102	214

Tabuľka 7 Pocit potreby školenia podľa účasti na školení

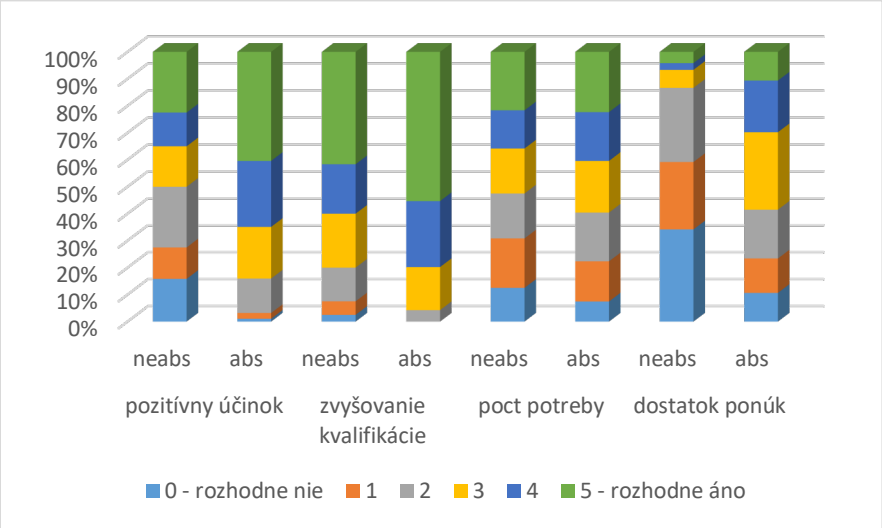
Kontingenčná tabuľka k VO9		Školenia a podpora (pocit potreby)						
		0	1	2	3	4	5	Σ
Školenia a podpora (účasť)	neabsolvoval	15	22	20	20	17	26	120
	absolvoval	7	14	17	18	17	21	94
	Σ	22	36	37	38	34	47	214

Tabuľka 8 Dostatočnosť ponúk podľa účasti na školení

Kontingenčná tabuľka k VO9		Školenia a podpora (dostatok ponúk)						
		0	1	2	3	4	5	Σ
Školenia a podpora (účasť)	neabsolvoval	19	14	27	18	15	27	120
	absolvoval	1	2	12	18	23	38	94
	Σ	20	16	39	36	38	65	214

Výsledky lepšie vynikajú na grafe nižšie. V prvom rade môžeme preskúmať vplyv účasti na školení na vnímanie jeho pozitívneho účinku. Ak aj z tohto pohľadu zoskupíme odpovede respondentov na *„súhlasné“* a *„nesúhlasné“* stanoviská[14], zistíme, že sú rozdelené v prípade „neabsolventov“ presne na polovicu, kým absolventi uznávajú pozitívny prínos až v 84% prípadov. Ďalšie dva stĺpce grafu znázorňujú názory na potrebu zvyšovania kvalifikácie. Aj keď v tomto prípade aj neabsolventi majú vo väčšej miere súhlasný názor na úrovni 80%, ich školení kolegovia jednotne odporúčajú zvyšovanie kvalifikácie s 95% súhlasného stanoviska. V ďalšej otázke sme s pýtali na subjektívny pocit vlastnej potreby respondenta absolvovať školenie ohľadom bezpečnosti informačných systémov. Odpovede oboch skupín sú prekvapivo na približne rovnakej úrovni a opytovaní sa mierne prikláňajú k názoru, že takéto školenie by potrebovali[15]. V poslednej hodnotenej otázke nachádzame najmarkantnejší rozdiel medzi odpoveďami jednotlivých skupín. Až viac ako 86% respondentov bez absolvovania školenia tvrdí, že ich je nedostatočné množstvo v ponuke, pričom predstavitelia druhej skupiny zastávajú takýto názor na úrovni 41%. Ani v tomto prípade však nemôžeme povedať, že takýto názor je upokojujúci.

Graf 4 Vplyv účasti na školení



Zdroj: *vlastné spracovanie)*

[14] súhlasné – 0 až 2; nesúhlasné – 3 až 5
[15] Približne 56%.

Z vyššie uvedených štatistických údajov, je podľa nášho názoru zrejmé, že školenia majú pozitívny vplyv na vnímanie bezpečnosti, ako komplexného systému a uvedomovanie si svojich vlastných nedostatkov, v tejto oblasti. Informovanosť je dôležitým kľúčom k pevným základom bezpečnosti a je účinnou zbraňou proti ľahostajnosti a dennej rutine užívateľov informačných a telekomunikačných systémov.

Diskusia a odporúčania

Po zodpovedaní výskumných otázok a ich vyhodnocovania sa rozhodnými krokmi dostávame k záverom našej vedeckej štúdie. V tejto časti zhrnieme dosiahnuté čiastkové výsledky a vytvoríme tak ucelený obraz našej práce. Oboznámime čitateľa aj s vybranými cieľmi našej práce, ktoré sme úspešne naplnili práve pomocou v tejto vedeckej štúdii uvedenými skutočnosťami. Všetky čiastkové ciele istým spôsobom spolu súvisia a nie je možné ich striktne od seba oddeliť. Na konci vyhodnotenia každého cieľa navrhneme a uvedieme aj naše odporúčania k riešeniu prípadných nedostatkov, pričom splnenie takejto úlohy je zároveň v súlade s ďalším čiastkovým cieľom výskumu.

Našou úlohu bolo zistiť stupeň dodržiavania interných a právnych predpisov o bezpečnosti používateľmi telekomunikačných a informačných systémov. Podľa odpovedí dotazovaných na otázku zo sekcie školenia, či dodržujú presne predpisy ohľadom informačnej bezpečnosti, by sme mohli prijať veľmi pozitívny záver, keďže až 76% z nich odpovedalo na ňu skôr kladne. Aj ohľadom oboznámenia sa internými predpismi sa stretávame vo veľkej miere so súhlasným stanoviskom. V súvislosti s tým sme poukázali aj na pozitívny vplyv školení na tomto úseku, keďže informovanosť povzbudzuje k dodržiavaniu základných bezpečnostných opatrení. Na základe vyššie uvedených zistení môžeme skonštatovať, že podľa vyjadrení respondentov je oboznámenie sa a dodržiavanie interných predpisov na vysokej úrovni. Zároveň však zdôrazňujeme aj odpovede zo sekcie zvyky, kde nachádzame určité nedostatky a tvrdíme, že je potrebné ešte viac upriamiť pozornosť užívateľov na tieto položky.

Preto odporúčame zabezpečiť lepší a priamejší prístup ku všetkým informáciám, odporúčaniam, interným predpisom, zákonom a medzinárodným právnym aktom o informačnej bezpečnosti na jednom mieste a vytvoriť tak priestor s komplexným prehľadom na všetkých úrovniach. Keďže tieto dokumenty sú navrhované expertmi a sú spracované na vysokej odbornej úrovni, je predpoklad, že nie každý užívateľ ich pochopí a následne aplikuje na potrebnej úrovni. Preto navrhujeme najdôležitejšie sekcie týchto aktov prispôsobiť znalostiam a úrovni informačnej gramotnosti užívateľov a priame a jednoduché fakty a pokyny im vhodným spôsobom prezentovať. Dobrým riešením by mohli byť rôzne vizuálne pomôcky, jednoduché infografiky alebo krátke a výstižné manuály k bezpečnému správaniu sa na pracovisku.

Je vhodné na tomto mieste uviesť aj názory expertov zo súkromného sektora aj policajného prostredia, ktoré sme doteraz v práci neprezentovali. Odpovedali na niekoľko otázok, medzi ktorými bola jedna aj v spojitosti s ich názormi na dodržiavanie zásad informačnej bezpečnosti. Pre vernú prezentáciu ich postoja doslovne a v nezmenenej podobe citujem niekoľko výstižných odpovedí:

- *„Myslím si, že jediný sektor, ktorý berie bezpečnosť vážne je bankový sektor. Štátny sektor sa ešte len zobúdza zo zimného spánku. Ľudia nemajú základné bezpečnostné povedomie, štát neinvestuje do vzdelania, nieto ešte do kontinuálneho vzdelávania. Bezpečnostný sektor je poddimenzovaný personálne, organizačne aj finančne.“*

- *„Nízka úroveň bezpečnostného povedomia, nedostatočne právne povedomie, neschopnosť identifikovať základne bezpečnostné riziká pri využívaní IKT a internetových technológií. Platí všeobecne nezávisle na sektore.“*

Aj z ostatných odpovedí je cítiť výrazne kritický názor expertov na postoj zamestnancov k dodržiavaniu zásad informačnej bezpečnosti a my sa s takýmto pohľadom bez dodatočných komentárov stotožňujeme.

Našim **ďalším cieľom pod bolo zistiť frekvenciu výskytu incidentov ohrozujúcich bezpečnosť informačných a telekomunikačných systémov v Policajnom zbore**. Tejto téme sme venovali všetky otázky sekcie incidenty. Z ich vyhodnotení je jasné, že respondenti sa veľmi zriedka stretli s výskytom hociktorého incidentu z vymenovaných možností. Nízke hodnoty výskytu môžu byť skreslené nevedomosťou respondentov o ich prítomnosti, keďže nie na každej úrovni musia byť bezpečnostné incidenty zverejnené. Najčastejší výskyt vykazuje všeobecne únik informácií, pričom viac ako 50% respondentov má o takejto udalosti znalosť. Pomerne vysoké hodnotenie dosiahli aj položky *„zneužitie prístupu oprávnenou osobou“* a *„nevedomá inštalácia škodlivého softvéru“*. Sú to nebezpečné oblasti, ktorých výskyt a zanedbanie môže napáchať rozsiahle škody. V rámci výskumnej otázky č. 3 sme bližšie skúmali vplyv dĺžky praxe na pohľad a vnímanie výskytu incidentov a zistili sme, že nie je badateľná súvislosť. Ako sme to už ale pri vyhodnocovaní tejto otázky napísali, značí to možnosť toho, že incidenty sa vyskytujú iba krátku dobu a ich intenzita sa časom rýchlo zvyšuje. Preto je potrebné, aj napriek relatívne upokojujúcim výsledkom, venovať sa tejto problematike aj v budúcnosti.

V rámci **našich odporúčaní** opäť nabádame na informovanosť. To, že užívatelia neregistrujú bezpečnostné incidenty informačných systémov neznamená, že sa nevyskytujú. Podľa nášho názoru je v prípade konfliktu potrebné o jeho výskyte v čo najväčšej miere informovať zainteresovaných a všetkých, ktorým hrozí vznik podobnej situácie. Po odstránení príčin neželaného stavu a po eliminácií jeho následkov je vhodné situáciu analyzovať a vyhodnotiť. Takéto reálne prípady z priameho prostredia užívateľov, resp. ponaučenia z nich, by sa mali ďalej aktívne využívať pri ďalšom vzdelávaní a príprave interných aktov riadenia.

Jedným z **najdôležitejších čiastkových cieľov našej práce je preskúmať aj vplyv školení a ďalšieho vzdelávania na bezpečnosť**. Podobne ako to bolo v prípade incidentov, aj tejto téme sa venuje celá sekcia otázok. Hneď na úvod je potrebné uviesť, že menej ako 45% respondentov vyjadrilo súhlasné stanovisko k absolvovaniu školenia ohľadom informačnej bezpečnosti. Je to podľa nášho názoru nízka úroveň účasti, pričom z výsledkov výskumnej otázky č. 4 je možné jednoznačne určiť pozitívny vplyv školení na vnímanie bezpečnosti, ako komplexného systému, a uvedomovanie si svojich vlastných nedostatkov v tejto oblasti. Domnievame sa, že existuje určitá súvislosť medzi vzdelaním a záujmom o školenia, avšak výsledky štatistickej analýzy náš predpoklad vyvrátili. Napriek malej účasti respondentov, vysoké percento z nich, so silným súhlasným stanoviskom uznáva pozitívne účinky školení, ich potrebnosť a potrebu zvyšovania kvalifikácie v oblasti bezpečnosti. Je to určitý paradox, ktorý môžeme vysvetliť názormi na ponuku školení. Viac ako $^2/_3$ účastníkov výskumu tvrdí, že množstvo ponúk školení je nedostatočné. Hájime názor, že informovanosť je kľúčovým riešením v boji proti počítačovej kriminalite a vzniku bezpečnostných incidentov.

Čísla hovoria za seba a my len môžeme dodať, že **našim odporúčaním** k tejto téme je jej maximálna miera propagácie na všetkých úrovniach. Informovanosť slúži ako preventívne opatrenie a zastávame názor, že sa skôr oplatí investovať prostriedky do prevencie a predísť tak nutným represívnym krokom a odstraňovaniu následkov. Je potrebné pripraviť a zabezpečiť adekvátne množstvo školení, pričom je žiaduce o týchto možnostiach užívateľov aj informovať.

V prvom kroku však odporúčame vyškoliť a zabezpečiť tak kvalitných školiteľov, pričom treba zvážiť prípadný prínos najlepších postupov a skúseností lektorov aj zo súkromného sektora.

V rámci výskumu sa vybraný experti vyjadrovali k téme školení, pričom bez bližšieho komentára uvádzame výber z odpovedí, korešpondujúci s názormi ostatných, na otázku *„Aké sú podľa Vášho názoru najefektívnejšie spôsoby na zvýšenie úrovne informačnej bezpečnosti?“*:

- *„Cyklické vzdelávacie procesy s úzko definovaným obsahom a meraným dosahom - podporené online dostupným obsahom.“*
- *„Osveta a pravidelné preškoľovanie, vrátane testovania v rozsahu minimálne jeden krát za rok a vždy, ak dôjde k zásadnej zmene, ktorá má vplyv na organizáciu alebo zamestnanca z pohľadu informačnej a kybernetickej bezpečnosti.“*

Ďalšia otázka sa venovala názorom na vplyv pravidelných školení zamestnancov na úroveň informačnej bezpečnosti, pričom sme zaznamenali odpovede v duchu *„Veľmi dobre, odhadujem zníženie rizika až do 50%, hlavne tam, kde sa zatiaľ nerobí nič.“*.

V závere uvádzame vybrané odpovede expertov k predpovedi budúceho vývoja hrozieb a zraniteľností a zároveň k prognóze úrovne informačnej bezpečnosti v období najbližších desaťročí. Predpovedať budúcnosť je veľmi náročná úloha a môžeme mať iba rôzne odhady. Experti sa k otázke „*Aké budú najvýraznejšie zmeny v otázkach informačnej bezpečnosti o 10 - 20 rokov oproti dnešnému stavu?“* vyjadrovali nasledovne:

- *„Nie je možné efektívne predpovedať vývoj na viac ako 5 rokov vopred. V horizonte 20 rokov je možné, že dôjde aj k zásadným objavom v technológii a fyzike, čím sa absolútne zmení spracovateľské prostredie. Na vývoj v oblasti kybernetickej bezpečnosti bude vplývať aj zmenené sociálne prostredie a nové typy motivácií ku generovaniu hrozieb. (Aktuálna majoritná motivácia je "zisk". Nové motivácie môžu byť a pravdepodobne budú viac sociálneho a politického charakteru).“*
- *„Možno predpokladať, že aj v nasledujúcom období budú najpočetnejšie incidenty spadajúce do kategórií nežiadúci obsah (rôzne formy malwaru), získavanie informácií (phishing, sociálne inžinierstvo) a zneprístupnenie služby (DoS, DDoS), nakoľko tieto formy útokov predstavujú často najefektívnejšiu cestu, ako môže útočník dosiahnuť svoj cieľ. Trend útokov typu APT (Advanced Persistent Threat) na konkrétne ciele – vládne ciele, finančná sféra, významné/kritické súkromné podniky a iné zaujímavé ciele – bude narastať nie len v globálnom meradle, ale možno predpokladať ich nárast aj v slovenskom kybernetickom priestore.“*
- *„Drvivý nedostatok špecialistov a nárast počtu pseudoodborníkov na SECURITY témy.“*

Prezentované názory odborníkov nie sú príliš optimistické a varujú pred nárastom počtu incidentov, výrazným zmenám podôb hrozieb a zraniteľností a celkovým vnímaním informačnej bezpečnosti. Sme presvedčení, že veľká väčšina čitateľov tejto práce si ešte pamätá svet bez dotykových obrazoviek mobilných telefónov, online úložných priestorov, desiatkom reklamných emailov denne a možno i bez počítača. Bolo to len pred niekoľkými rokmi a dnes sú už všetky tieto technológie bežnou, ba neoddeliteľnou súčasťou našich životov. Nemáme reálnu šancu odhadnúť, čo bude pre nás absolútnou samozrejmosťou o rok, o päť či desať rokov. Preto nemôže byť reálny ani odhad hrozieb a zraniteľností. Tvrdíme ale, že je potrebné byť pripravený, k čomu je najúčinnejším nástrojom informovanosť!

Záver

Predpokladali sme, že našim výskumom nájdeme určité medzery v bezpečnostnom systéme Policajného zboru, najmä v oblasti postoja personálu. Na určitej úrovni sa naše očakávania v tomto smere naplnili, pričom v žiadnom prípade nechceme a nemôžeme kriticky hodnotiť prácu a snahu pracovníkov zodpovedných za bezpečnosť telekomunikačných

a informačných systémov Policajného zboru. Zdôrazňujeme, že po osobných konzultáciách s kompetentnými vnímame túto problematiku ešte citlivejšie a uznávame jej komplexnosť. Nie je možné nájsť na niektoré zistené nedostatky generálne riešenie a ani manažéri bezpečnosti na najvyšších pozíciách nedokážu ovplyvniť slobodnú vôľu človeka. Chceme ale poukázať na to, že častejšími a pravidelnými školeniami v oblasti informačnej bezpečnosti, osobným prístupom k informovanosti a prípadne úpravou interných predpisov sú dosiahnuteľné dlhotrvajúce pozitívne výsledky.

Použitá literatúra

FELCAN, M. a kol. 2019. *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.* VVÚ VÝSK. 245. Akadémia Policajného zboru v Bratislave.

HOLUBICZKY, V. 2020. Frekvencia využívania moderných technológií Policajným zborom. In: *Moderné technológie v páchaní, odhaľovaní, dokumentovaní, dokazovaní a prevencii trestnej činnosti.* Bratislava: Akadémia Policajného zboru v Bratislave. s. 163-171. ISBN 978-80-8054-856-8.

HOLUBICZKY, V. 2020. Moderné technológie a účel ich využívania. In: *Projustice - vedecko-odborný recenzovaný časopis pre právo, spravodlivosť a bezpečnostné vedy.* Roč. 9 (2020) (Publikované 19.12.2020). ISSN 1339-1038.

HOLUBICZKY, V. 2020. Prítomnosť hrozieb a zraniteľností pri využívaní informačných technológií. In: *Policajná teória a prax*. Bratislava: Akadémia Policajného zboru v Bratislave. Roč. XXVIII., č. 2, s. 5-19. ISSN 1335-1370.

KOPENCOVÁ, D., RAK, R. 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.

RAK, R., KOLITSCHOVÁ, P. 2019. *Bezpečnost a bezpečí – základní pojmy a jejich vnímání.* In: Zborník z 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., KOPENCOVÁ, D. 2019. *Bezpečnostní hrozby, vlastnosti a fáze*. In: Zborník z 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.