Matej Kostrec

**Medzinárodná komparácia povedomia v oblasti ochrany informácií**

**Anotácia:** Autor vedeckej štúdie si stanovil za cieľ prostredníctvom medzinárodného výskumu overiť úroveň vedomostí študentov o ochrane informácií v informačných a komunikačných systémoch. Na výskume participovali respondenti z Akadémie Policajného zboru v Bratislave a z Francúzskej Policajnej akadémie (ENP) v Montbéliarde. Výskum v oboch krajinách potvrdil značné rezervy vo vedomostiach študentov zo skúmanej oblasti. Z toho dôvodu autor štúdie navrhuje metódy ochrany informácií na rôznych úrovniach (procesnej, technickej, mechanickej, režimovej, softvérovej, na úrovni prístupov a na úrovni vzdelávania a osvety). Autor sa v štúdii osobitne venoval návrhu metód ochrany na úrovni vzdelávania, a to konkrétne formou návrhov tematických plánov pre nové predmety „základy kybernetickej bezpečnosti“, „teória kybernetickej bezpečnosti I“. a „teória kybernetickej bezpečnosti II.“, ktoré odporúča implementovať do výučby na Akadémii Policajného zboru v Bratislave v študijných programoch bezpečnostnoprávna ochrana osôb a majetku a bezpečnostnoprávne služby vo verejnej správe.

**Kľúčové slová:** vedecký výskum, ochrana informácií, návrh metód ochrany, vyučovací proces, návrh opatrení

**Úvod**

Táto štúdia vznikla ako súčasť vedecko-výskumnej úlohy s názvom „Metódy spracovania policajne relevantných informácií“, ktorá bola vyhlásená na Akadémii Policajného zboru v Bratislave v roku 2011 pod č. 161/2011. Čiastková úloha tejto vedecko-výskumnej úlohy s názvom „Metódy ochrany policajne relevantných informácií“, ktorej hlavným riešiteľom je autor tohto príspevku, bola zameraná na vykovanie výskumu metód ochrany policajne relevantných informácií. Predmetný výskum,  jeho závery, ako aj príslušné odporúčania a návrhy opatrení a metód sú predmetom publikácie „Metódy ochrany policajne relevantných informácií“, ktorá bola dokončená v roku 2024 a bude vydaná v roku 2025. Predmetom tejto publikácie je aj vykonanie opätovného výskumu s rovnakou štruktúrou otázok v distribuovanom dotazníku a súčasne porovnanie výsledkov pôvodného výskumu s výsledkami výskumu vykonaného po ôsmich rokoch. Závery z predmetného porovnania sú, žiaľ, pomerne nepriaznivé, keďže povedomie respondentov výskumu o ochrane policajných informácií, ktorý sa uskutočnil po ôsmich rokoch, vykazuje takmer nezmenenú úroveň oproti predchádzajúcemu výskumu, pričom obe úrovne je nutné považovať za nedostatočné. Z konštatovanej skutočnosti vyplýva záver, že vzdelávanie v tejto oblasti by sa malo zlepšiť nielen kvalitatívne, ale najmä kvantitatívne.

Okrem toho vzhľadom na spoločenské zmeny, ktoré sa v posledných mesiacoch s narastajúcou intenzitou dejú na európskom kontinente a ktoré vyvolávajú obavy o pravdepodobné zvýšenie úrovne páchania všetkých druhov kriminality, vzniká potreba konsolidácie metód ochrany policajne relevantných informácií na medzinárodnej úrovni. Z uvedeného dôvodu považujeme výsledky a závery výskumu predkladanej čiastkovej vedecko-výskumnej úlohy za východiskovú bázu pre vyhlásenie potenciálnej budúcej vedecko-výskumnej úlohy s názvom „Medzinárodné metódy ochrany policajne relevantných informácií“, na ktorej by spolupracovali aj vedecko-výskumní pracovníci akadémií Policajného zboru iných členských štátov EÚ. Takáto spolupráca akademických pracovísk by prostredníctvom výskumov zrealizovaných v rôznych krajinách určite priniesla vhodné podklady pre prijatie konsolidovaných legislatívnych štandardov i konsolidovaných vzdelávacích cyklov z oblasti informačnej bezpečnosti.[[1]](#footnote-1)

S ohľadom na vyššie uvedené konštatovania sa autor tejto štúdie rozhodol v roku 2024 vykonať medzinárodný výskum, ktorého účastníkmi boli študenti z Akadémie Policajného zboru v Bratislave (ďalej len APZ) a študenti francúzskej Policajnej akadémie v Montbéliarde (ďalej len ENP)[[2]](#footnote-2)

**Metodológia a cieľ výskumu[[3]](#footnote-3)**

***Cieľom výskumu*** je potvrdiť, resp. vyvrátiť platnosť nasledujúcej hypotézy:

***„Existujú rezervy pri vzdelávaní aktérov pristupujúcich k dátam spracovávaným v informačných systémoch PZ o požadovanej úrovni ochrany týchto dát.“***

***Metódy použité pri výskume:***

##### **Teoretické metódy:**

##### **klasifikačnej, vzťahovej, systémovo-štruktúrnej a kauzálnej analýzy** pri determinácii dotazníkovej štruktúry výskumu a jeho vyhodnocovaní v súlade s cieľom výskumu,

##### **syntézy** pri určovaní reálnej úrovne ochrany policajne relevantných informácií v informačných systémoch PZ,

##### **komparácie** pri porovnávaní výsledkov výskumu s požadovanou úrovňou ochrany v zmysle klasifikácie stupňa citlivosti a utajenia spracovávaných informácií,

##### **indukcie a dedukcie** pri návrhu bezpečnostných opatrení a vzdelávacieho programu na zvýšenie úrovne ochrany policajne relevantných informácií v informačných systémoch PZ.

**Matematické a štatistické metódy** pri vyhodnocovaní výskumu.

1. **Výskum**

Výskum sa realizoval formou dotazníka, ktorého znenie bolo rovnaké (s výnimkou jazykovej mutácie) pre obe účastnícke strany a ktorý pozostával v úvodnej časti zo získania anonymizovaných identifikačných údajov zúčastnených respondentov. V ďalšej, nosnej časti výskumu, dotazník obsahoval 10 zatvorených otázok a jednu otvorenú otázku.

* 1. ***Identifikačné údaje respondentov výskumu***

Účasť respondentov bola dobrovoľná, preto sa zo slovenskej, ako aj z francúzskej strany ich výber obmedzil na počet 20 respondentov. Vzhľadom na skutočnosť, že výskum sa vykonal v študentskom prostredí, identifikácia sa obmedzila výlučne na pohlavie respondenta a interval, do ktorého spadá jeho vek. Poznamenávame, že výučby na francúzskej ENP sa môžu zúčastniť aj frekventanti staršieho veku (do 35 rokov), ktorí majú maturitné vzdelanie. Z tohto dôvodu musíme zaradiť medzi identifikačné údaje aj ďalší vekový interval, pretože na výskume sa mohli zúčastniť aj respondenti vyššej vekovej kategórie.

V nasledujúcich tabuľkách si bližšie predstavíme štruktúru respondentov podľa pohlavia a podľa vekovej kategórie.

|  |  |  |
| --- | --- | --- |
| **Pohlavie** | **Počet SR** | **Počet FR** |
| M | 10 | 13 |
| Ž | 10 | 7 |
| **Celkový počet** | **20** | **20** |

Tabuľka č. 1: Prehľad respondentov podľa pohlavia

Je dôležité poznamenať, že vo Francúzsku sa študenti ENP stávajú príslušníkmi polície až od začiatku štúdia na ENP. Pozície v praxi si vyberajú na konci štúdia, a to na základe svojich študijných výsledkov. Väčšina pozícií je však ponúkaných v Paríži, kde je práca policajtov veľmi náročná aj vzhľadom na skutočnosť, že je tu nielen veľmi vysoká trestná činnosť, ale sa tu organizujú aj mnohé štrajky a protesty. To je jeden z dôvodov, prečo je počet žien, ktoré sa hlásia k polícii, nižší. V podstate dosahuje asi jednu štvrtinu všetkých študentov na škole.

To sa prejavilo aj v našom výskume, v ktorom je počet respondentiek nižší ako na Slovensku.

|  |  |  |
| --- | --- | --- |
| **Vek** | **Počet SR** | **Počet FR** |
| 21-30 | 20 | 18 |
| 31-40 |  | 2 |
| **Celkový počet** | **20** | **20** |

Tabuľka č. 2: Prehľad respondentov podľa veku

Z tabuľky je zrejmé, že medzi francúzskymi respondentmi sú aj dvaja respondenti, ktorých vek spadá do vekového intervalu 31 – 40 rokov.

* 1. ***Výskum realizovaný pomocou zatvorených otázok***

Predmetom výskumu realizovaného formou dotazníka boli aj nasledujúce zatvorené otázky. Poznamenávame, že v zátvorkách za znením otázky sú uvedené alternatívy odpovedí, ktoré boli respondentom ponúkané ako možné odpovede.

1. Poznáte stupeň utajenia, resp. citlivosti dát uložených alebo spracúvaných v informačných systémoch Policajného zboru (ďalej len „PZ“)? (áno, čiastočne, nie).
2. Existujú na vašom pracovisku bezpečnostné manuály popisujúce spôsoby prístupu do informačných systémov a k jednotlivým kategóriám dát? (pod kategóriou rozumieme stupeň citlivosti dát) (áno, čiastočne, nie, neviem).
3. Sú podľa vášho názoru dáta v informačných systémoch PZ chránené dostatočne? (áno, čiastočne, nie, neviem sa vyjadriť).
4. Pracujete v priestoroch, kde majú prístup aj iné osoby, ktoré v tomto priestore bežne nepracujú? (áno, nie).
5. Sú vaše pracovné počítače (PC, notebooky) dostatočne chránené pred zneužitím inou osobou? (áno, čiastočne, nie, neviem).
6. Má podľa vášho názoru kategorizácia údajov spracovávaných v informačných systémoch PZ priamy vplyv na úroveň ich ochrany? (áno, čiastočne, nie, neviem sa vyjadriť).
7. Stretávate sa na vašom pracovisku aj s dátami pochádzajúcimi z informačných systémov PZ iných štátov, resp. bezpečnostných inštitúcií? (áno, nie).
8. Sú podľa vášho názoru dáta pochádzajúce z informačných systémov PZ iných štátov, resp. bezpečnostných inštitúcií, chránené lepšie ako dáta spracúvané v našich informačných systémoch PZ? (áno, čiastočne, nie, neviem sa vyjadriť).
9. Absolvovali ste školenie alebo výučbu o ochrane citlivých dát alebo utajovaných skutočností spracúvaných v informačných systémoch? (áno, nie).
10. Máte záujem vzdelávať sa v oblasti ochrany dát a bezpečnosti informačných systémov? (áno, nie).
    * 1. ***Vyhodnotenie odpovedí respondentov na zatvorené otázky dotazníkového výskumu***

Otázka č.1:

Poznáte stupeň utajenia, resp. citlivosti dát uložených alebo spracúvaných v informačných systémoch Policajného zboru (PZ)? (áno, čiastočne, nie).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Odpovede na otázku č.1** | | | |
| **áno** | **čiastočne** | **nie** | **Celkový súčet** |
| **Počet odpovedí FR** | **5** | **10** | **5** | **20** |
| **Počet odpovedí SR** | **8** | **9** | **3** | **20** |

Tabuľka č. 3 Prehľad odpovedí na otázku č. 1: Poznáte stupeň utajenia, resp. citlivosti dát uložených alebo spracúvaných v IS PZ?

Z vyššie uvedenej tabuľky vyplýva, že stav poznania stupňa utajenia dát v IS PZ je v podstate rovnaký u respondentov z oboch škôl. Žiaľ, polovica respondentov v oboch štátoch deklaruje, že pozná stupeň utajenia dát iba čiastočne.

Graf č. 1: Grafické znázornenie odpovedí na otázku č.1

Otázka č. 2:

Existujú na vašom pracovisku bezpečnostné manuály popisujúce spôsoby prístupu do informačných systémov a k jednotlivým kategóriám dát? (pod kategóriou rozumieme stupeň citlivosti dát) (áno, čiastočne, nie, neviem).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  | **Odpovede na otázku č. 2** | | | | |
| **áno** | **čiastočne** | **neviem** | **nie** | **Celkový súčet** |
| **Počet odpovedí FR** | **5** | **4** | **7** | **4** | **20** |
| **Počet odpovedí SR** | **5** | **6** | **3** | **6** | **20** |

Tabuľka č. 4 Prehľad odpovedí na otázku č. 2

Aj v tomto prípade respondenti vo FR, ako aj v SR, dali na vedomie, že polovica z nich buď nevie o existencii bezpečnostných manuálov na pracovisku, alebo deklaruje, že takéto manuály na ich pracovisku nie sú. O ich existencii vie v oboch krajinách len štvrtina respondentov.

Otázka č. 3:

Sú podľa vášho názoru dáta v informačných systémoch PZ chránené dostatočne? (áno, čiastočne, nie, neviem sa vyjadriť).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Odpovede na otázku č. 3** | | | | |
| **áno** | **čiastočne** | **neviem sa vyjadriť** | **nie** | **Celkový súčet** |
| **Počet odpovedí FR** | **5** | **6** | **4** | **5** | **20** |
| **Počet odpovedí SR** | **4** | **8** | **4** | **4** | **20** |

Tabuľka č. 5 Prehľad odpovedí na otázku č. 3

Odpovede na táto otázku sa v oboch krajinách v podstate zhodujú. Respondenti nie sú presvedčení o dostatočnej ochrane dát v informačných systémoch PZ. Iba štvrtina si myslí, že ochrana dát je dostatočná. Vzhľadom na posledné útoky hackerov v SR na databázy dôležitých štátnych inštitúcií (kataster, Všeobecná zdravotná poisťovňa), ku ktorým pristupujú pri svojej práci aj príslušníci PZ na Slovensku, si myslíme, že dôveryhodnosť u slovenských respondentov ešte klesne.

Otázka č. 4

Pracujete v priestoroch, kde majú prístup aj iné osoby, ktoré v tomto priestore bežne nepracujú? (áno, nie).

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Odpovede na otázku č. 4** | | |
| **áno** | **Nie** | **Celkový súčet** |
| **Počet odpovedí FR** | **20** | **0** | **20** |
| **Počet odpovedí SR** | **6** | **14** | **20** |

Tabuľka č. 6 Prehľad odpovedí na otázku č. 4

Táto otázka sa zdala francúzskym respondentom trochu zvláštna, pretože v ENP prebieha vzdelávanie štyroch až piatich študijných behov paralelne. Samozrejme, s určitým časovým posunom. Počítače teda v učebniach používa, a teda má prístup k nim, vo vzdelávacích cykloch spolu až 300 – 350 študentov. To nie je prípad slovenských respondentov, ktorí sú okrem študijných povinností na APZ, už zaradení na konkrétne posty v praxi.

Otázka č. 5

Sú vaše pracovné počítače (PC, notebooky) dostatočne chránené pred zneužitím inou osobou? (áno, čiastočne, nie, neviem).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Odpovede na otázku č. 5** | | | | |
| **áno** | **čiastočne** | **neviem** | **nie** | **Celkový súčet** |
| **Počet odpovedí FR** | **5** | **4** | **8** | **3** | **20** |
| **Počet odpovedí SR** | **8** | **7** | **1** | **4** | **20** |

Tabuľka č. 7 Prehľad odpovedí na otázku č. 5

Respondenti zo SR sú vo väčšej miere ako ich francúzski kolegovia presvedčení, že sú ich počítače dostatočne, resp. čiastočne, chránené pred zneužitím inou osobou. Študenti ENP vo Francúzsku nevedia celkom posúdiť ochranu ich pracovných počítačov. Jedným z dôvodov je aj vyššie uvedená skutočnosť, že pri každom počítači sa denne aj viackrát menia ich používatelia.

Otázka č. 6

Má podľa vášho názoru kategorizácia údajov spracovávaných v informačných systémoch PZ priamy vplyv na úroveň ich ochrany? (áno, čiastočne, nie, neviem sa vyjadriť).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Odpovede na otázku č. 6** | | | | |
| **áno** | **čiastočne** | **neviem sa vyjadriť** | **nie** | **Celkový súčet** |
| **Počet odpovedí FR** | **8** | **5** | **5** | **2** | **20** |
| **Počet odpovedí SR** | **4** | **11** | **5** | **0** | **20** |

Tabuľka č. 8 Prehľad odpovedí na otázku č. 6

Z odpovedí respondentov z oboch štátov je zrejmé, že kategorizácia údajov nie je pre nich rozhodujúcim faktorom pre posúdenie a následné zvýšenie úrovne ochrany predmetných údajov. Okrem toho na strane slovenských respondentov vplyvu kategorizácie na úroveň ochrany dát verí iba 5 % respondentov, čo pravdepodobne svedčí o celkovej neznalosti kategórií dát zo strany väčšiny respondentov.

Otázka č. 7

Stretávate sa na vašom pracovisku aj s dátami pochádzajúcimi z informačných systémov PZ iných štátov, resp. bezpečnostných inštitúcií? (áno, nie).

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Odpovede na otázku č. 7** | | |
| **áno** | **nie** | **Celkový súčet** |
| **Počet odpovedí FR** | **10** | **10** | **20** |
| **Počet odpovedí SR** | **3** | **17** | **20** |

Tabuľka č. 9 Prehľad odpovedí na otázku č. 7

Vo Francúzsku až polovica respondentov priznáva, že sa stretáva aj s dátami z IS PZ iných štátov. Naopak, takmer všetci slovenskí respondenti deklarujú, že s týmto typom dát sa počas výskumu nestretávali. Je však veľmi dôležité uviesť, že respondenti sú študentmi policajných škôl, kde študenti oboch škôl majú prístup len do školiacich prostredí informačných systémov vrátane niektorých vybraných IS aj z iných štátov EÚ. Do prevádzkových prostredí IS PZ nemajú študenti ani v jednej škole žiadny povolený prístup.

Otázka č. 8

Sú podľa vášho názoru dáta pochádzajúce z informačných systémov PZ iných štátov, resp. bezpečnostných inštitúcií, chránené lepšie ako dáta spracúvané v našich informačných systémoch PZ? (áno, čiastočne, nie, neviem sa vyjadriť).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Odpovede na otázku č. 8** | | | |
| **áno** | **neviem sa vyjadriť** | **nie** | **Celkový súčet** |
| **Počet odpovedí FR** | **2** | **12** | **6** | **20** |
| **Počet odpovedí SR** | **3** | **17** | **0** | **20** |

Tabuľka č. 10 Prehľad odpovedí na otázku č. 8

Je len prirodzené, že respondenti z oboch krajín sa k tejto otázke postavili skoro zhodne, a to odpoveďou, že sa k tejto problematike nevedia vyjadriť. Sú to zatiaľ len študenti a určite ešte nemajú reálne skúsenosti z medzinárodnej policajnej spolupráce. Zaujímavý je ale názor skoro tretiny francúzskych respondentov, ktorí sú presvedčení, že dáta v policajných IS sú vo Francúzsku chránené lepšie ako v iných krajinách.

Otázka č. 9

Absolvovali ste školenie alebo výučbu o ochrane citlivých dát alebo utajovaných skutočností spracúvaných v informačných systémoch? (áno, nie).

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Odpovede na otázku č. 9** | | |
| **áno** | **nie** | **Celkový súčet** |
| **Počet odpovedí FR** | **2** | **18** | **20** |
| **Počet odpovedí SR** | **7** | **13** | **20** |

Tabuľka č. 11 Prehľad odpovedí na otázku č. 9

Z tabuľky č. 11 je vzhľadom na vysoký počet záporných odpovedí, zrejmé, že respondenti oboch krajín sa pravdepodobne vyjadrovali len k možnostiam absolvovania školení, resp. výučby, ktoré predchádzali ich súčasnému štúdiu na škole.

Otázka č. 10

Máte záujem vzdelávať sa v oblasti ochrany dát a bezpečnosti informačných systémov? (áno, nie).

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Odpovede na otázku č. 10** | | |
| **áno** | **nie** | **Celkový súčet** |
| **Počet odpovedí FR** | **20** | **0** | **20** |
| **Počet odpovedí SR** | **12** | **8** | **20** |

Tabuľka č. 12 Prehľad odpovedí na otázku č. 10

Na rozdiel od francúzskych respondentov, ktorí úplne všetci majú záujem o vzdelávanie sa v oblasti ochrany dát a bezpečnosti IS, respondenti zo Slovenska nie sú až tak orientovaní na tento typ vzdelávania. Skoro polovica z nich totiž oň neprejavila záujem.

* 1. ***Výskum realizovaný pomocou otvorenej otázky***

Pre potreby vedeckej štúdie bol zaujímavý aj osobný názor respondentov na ochranné mechanizmy, ktorými sú chránené dáta v informačných systémoch Policajných zborov v jednotlivých štátoch. Preto súčasťou výskumu bola aj nasledujúca otvorená otázka:

Otázka č.1

Uveďte ochranné mechanizmy, ktorými sú chránené dáta, s ktorými pracujete v informačných systémoch PZ (príklady ochranných mechanizmov: zamknutá kancelária, keď v nej nie sú osoby, ktoré v nej pracujú; prístupové heslo do informačného systému; ochrana biometrickými prvkami; šifrované dáta; ochrana pred kopírovaním a pod.)

V nižšie uvedenej tabuľke je prehľad ochranných mechanizmov, ktoré respondenti z oboch krajín uviedli do dotazníkov. Je potrebné poznamenať, že pre kompaktnosť výstupu neboli do tabuľky zaradené ochranné mechanizmy, ktoré figurovali v dotazníku výhradne jedného respondenta bez ohľadu na krajinu jeho pôsobenia.

|  |  |  |
| --- | --- | --- |
| Názov mechanizmu | Počet respondentov | |
| FR | SR |
| Alarm pri nepovolanom vstupe do priestoru | 5 | 3 |
| Biometria pre vstup do priestorov | 2 | 1 |
| Blokovanie PC |  | 3 |
| Blokovanie súborov | 6 | 4 |
| Elektronické kódovanie dverí | 15 | 16 |
| Mechanické zamykanie | 12 | 14 |
| Obmedzenie pripojenia do verejných sietí | 15 | 7 |
| Ochrana pred kopírovaním | 6 | 8 |
| Ochrana prístupovými heslami | 20 | 20 |
| Pohybové senzory |  | 3 |
| Šifrovanie | 15 | 7 |
| Trezor na uloženie notebookov |  | 4 |
| Vypnutie PC pri odchode z miesta | 20 | 11 |
| Zamedzenie fyzického prístupu nepovolaným osobám | 12 | 10 |
| Zamknutá kancelária | 15 | 12 |

Tabuľka č. 13 Prehľad ochranných mechanizmov uvedených respondentmi výskumu

Z prehľadu ochranných mechanizmov pre zabezpečenie ochrany dát v informačných systémoch PZ, ktoré uviedli respondenti, vyplýva, že veľká väčšina mechanizmov spadá pod fyzickú a mechanickú ochranu. Ďalšiu skupinu tvoria mechanizmy založené na softvérmi spravovaných prístupoch k počítačom i externým počítačovým sieťam a šifrovanie údajov. Pre rozšírenie povedomia o iných formách a typoch ochranných mechanizmov budú v nižšie uvedenej kapitole opísané metódy ochrany informácií.

* 1. ***Vyhodnotenie výskumu vzhľadom na cieľ výskumu***

Cieľom výskumu bolo vyhodnotenie platnosti hypotézy, že „Existujú rezervy pri vzdelávaní aktérov pristupujúcich k dátam spracovávaným v informačných systémoch PZ o požadovanej úrovni ochrany týchto dát“.

Z vyhodnotenia jednotlivých zatvorených otázok dotazníka, ktorý bol výkonným nástrojom prezentovaného medzinárodného výskumu, ako aj z vyhodnotenia otvorenej otázky je nutné konštatovať, že bola overená platnosť vyššie uvedenej hypotézy a  v oboch krajinách, vo Francúzsku aj na Slovensku, existujú rezervy pri vzdelávaní aktérov pristupujúcich k dátam spracovávaným v IS Policajných zborov.

Z tohto dôvodu pristúpime v nasledujúcej kapitole k návrhu metód na ochranu informácií.

1. **Návrh metód na ochranu informácií**

S cieľom zvýšiť ochranu citlivých, dôverných, osobných a ďalších kategórií policajne relevantných informácií spracúvaných v informačných systémoch je potrebné aplikovať niektoré z nižšie uvedených metód.

* 1. ***Metódy ochrany informácií na procesnej úrovni***

Metódy ochrany informácií na procesnej úrovni sú založené na transpozícii európskych smerníc a prijatí národných legislatívnych štandardov, princípov a opatrení[[4]](#footnote-4), ktorým sa v tejto štúdii detailnejšie venovať nebudeme, pretože legislatívne štandardy sú v každej krajine participujúcej na výskume v niektorých oblastiach rozdielne a ich porovnávanie by si vyžadovalo samostatnú štúdiu. Ako príklad môžeme uviesť rozdiel pri stanovení úrovní klasifikácie údajov, pričom vo Francúzsku okrem štyroch úrovní spoločných so Slovenskom (prísne tajné, tajné, dôverné, neklasifikované) majú aj úroveň s názvom „obmedzené“ informácie, ktorá sa v SR nepoužíva. Pre zaujímavosť uvedieme aj znenie opisu tejto úrovne: „Vyzradenie alebo zverejnenie informácií stupňa „obmedzené“ by mohlo spôsobiť neželané dopady na príjmoch a reputácii spoločnosti.“[[5]](#footnote-5)

* 1. ***Metódy ochrany informácií na technickej úrovni***

Metódy ochrany informácií na technickej ochrany sú založené na ochrane hardvérových komponentov informačno-komunikačných systémov.[[6]](#footnote-6) Táto metóda bola respondentmi výskumu ovládaná na celkom obstojnej úrovni, preto sa ani tejto metóde nebudeme v tejto štúdii podrobnejšie venovať.

* 1. ***Metódy ochrany informácií na mechanickej úrovni a na úrovni režimových opatrení***

Tento typ metód ochrany bol respondentmi dotazníka v otvorenej otázke v oboch krajinách vyhodnotený ako najlepšie poznaný zo všetkých ostatných typov metód ochrany informácií v IS PZ. To je opäť dôvod, pre ktorý sa mu v tejto štúdii detailnejšie venovať nebudeme.

* 1. ***Metódy ochrany informácií na softvérovej úrovni***

Metódy ochrany informácií na softvérovej úrovni sú založené na implementácii bezpečnostných mechanizmov na báze programových produktov, ktorých cieľom je zvýšiť úroveň ochrany dát spracúvaných v IS.[[7]](#footnote-7) Ani tomuto typu metódy sa v predkladanej štúdii nebudeme venovať podrobnejšie, pretože rozsah spracovania by bol značný.

* 1. ***Metódy ochrany informácií na úrovni riadenia prístupov***

Metódy ochrany informácií na úrovni riadenia prístupov sú založené na bezpečnostných mechanizmoch, ktoré môžeme diferencovať na základe niektorého z nasledujúcich typov prístupov:

* prístup do priestorov, kde sú umiestnené zariadenia informačno-komunikačných technológií,
* prístup k používaniu zariadení informačno-komunikačných technológií,
* prístup do informačného systému/do softvérovej aplikácie,
* prístup k údajom.

Pre všetky vyššie uvedené typy prístupov sa používajú autentizačné metódy ochrany informácií. Metóda autentizácie (autentifikácie) spočíva v identifikácii a overení identity subjektu, ktorý žiada o prístup. Metódy autentizácie sú založené na preukázaní identity, pričom existujú približne tieto základné spôsoby autentizácie:

* autentizácia podľa toho, ***čo subjekt má*** (identifikačná karta, čipová karta, token, identifikačný žetón, USB ​​kľúč, smartfón, atď.),
* autentizácia podľa toho, ***čo subjekt pozná*** (užívateľské meno, PIN, heslo, prístupové frázy, atď.),
* autentizácia podľa toho, ***čím subjekt je*** (rôzne biometrické údaje, ako odtlačok prsta, dlane, sietnica oka, atď.),
* autentizácia podľa toho, ***čo subjekt robí alebo vie robiť***(ručný podpis, výpočet, ktorý ovláda iba subjekt, modulácia hlasu, správanie sa subjektu, atď.),
* autentizácia podľa toho, ***kde sa subjekt nachádza*** (geografické údaje stanovené subjektom za možné pôsobiská overované systémom GPS)[[8]](#footnote-8).
  1. ***Metódy ochrany informácií na úrovni vzdelávania a osvety***

Metódy ochrany informácií na úrovni vzdelávania a osvety je možné na základe výsledkov výskumu považovať za najmenej rozpracované a aplikované na oboch školách, ktoré sa zúčastnili medzinárodného výskumu.

Francúzski kolegovia z ENP sa vzhľadom na výsledky výskumu, ktoré vyplynuli z odpovedí ich respondentov, rozhodli, že ich učebné osnovy v rámci informaticky zameraných predmetov rozšíria o detailnejšiu výuku týchto oblastí:

* Riadiace dokumenty dátovej bezpečnosti.
* Klasifikácia aktív (priestorov, zariadení, dát) a organizácia a riadenie ich ochrany.
* Fyzická, režimová a personálna bezpečnosť.
* Riadenie prístupov k informatickým aktívam, vrátane prístupov k informáciám spracúvaným v IS.

Pre pedagógov APZ odporúčame rozšírenie v súčasnosti poskytovaného vzdelávania v oblasti kybernetickej bezpečnosti (aktuálne predmet informačná bezpečnosť) o predmety základy kybernetickej bezpečnosti, teória kybernetickej bezpečnosti I. a teória kybernetickej bezpečnosti II., pre ktoré je **v nasledujúcich tabuľkách** **rozpracovaný návrh tematických plánov a ktoré je možné využiť pre oba študijné programy: bezpečnostnoprávna ochrana osôb a majetku a bezpečnostnoprávne služby vo verejnej správe.** Odporúčame aj doplniť vyučovacie hodiny o riešenie praktických situácií v rámci odborne zameraných seminárov, ktoré momentálne nie sú implementované v učebných osnovách.

**Tematický plán predmetu: Základy kybernetickej bezpečnosti**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **P. č.** | **Názov témy** | **P** | **S** | **C** | **Spolu** |
| 1. | Systém informačnej a kybernetickej bezpečnosti, základy technickej normalizácie | 2 |  |  | 2 |
| 2. | Bezpečnostné politiky a bezpečnostná dokumentácia | 2 |  | 2 | 4 |
| 3. | Organizácia bezpečnosti a kľúčové roly v informačnej bezpečnosti | 2 |  |  | 2 |
| 4. | Klasifikácia informácií a riadenie aktív | 2 |  | 2 | 4 |
| 5. | Personálna bezpečnosť | 2 |  |  | 2 |
| 6. | Fyzická bezpečnosť a bezpečnosť prostredia | 2 |  | 2 | 4 |
| 7. | Správa počítačov a sietí | 2 |  |  | 2 |
| 8. | Digitálna identita a riadenie prístupu k sieťam a informačným systémom | 4 |  | 2 | 6 |
| 9. | Procesy riadenia dodávateľov a tretích strán | 2 |  |  | 2 |
| 10. | Riadenie kontinuity činností |  |  | 2 | 2 |
| 11. | Riadenie súladu v informačnej bezpečnosti | 4 |  | 2 | 6 |
| **1. semester – skúška** | | **24** |  | **12** | **36** |

Tabuľka č. 14 Tematický plán predmetu Základy kybernetickej bezpečnosti

Zdroj: autor

**Tematický plán predmetu: Teória kybernetickej bezpečnosti I.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **P. č.** | **Názov témy** | **P** | **S** | **C** | **Spolu** |
| 1. | Teoretické východiská kybernetickej bezpečnosti | 2 |  |  | 2 |
| 2. | Systém zabezpečovania internetovej infraštruktúry | 2 |  |  | 2 |
| 3. | Systém základnej a digitálnej služby | 2 |  | 2 | 4 |
| 4. | Systém bezpečnostného opatrenia | 4 |  | 2 | 6 |
| 5. | Rozsah bezpečnostnej dokumentácie | 4 |  |  | 4 |
| 6. | Riadenie hrozieb a rizík, základy analýzy rizika | 4 |  | 2 | 6 |
| 7. | Riadenie prístupov | 2 |  | 4 | 6 |
| 8. | Kryptografia I. | 4 |  | 2 | 6 |
| **3. semester – hodnotenie** | | **24** |  | **12** | **36** |

Tabuľka č. 15 Tematický plán predmetu Teória kybernetickej bezpečnosti I.

Zdroj: autor

**Tematický plán predmetu: Teória kybernetickej bezpečnosti II.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **P. č.** | **Názov témy** | **P** | **S** | **C** | **Spolu** |
| 1. | Základy bezpečnostnej architektúry | 2 |  | 2 | 4 |
| 2. | Základy bezpečnosti elektronickej komunikácie | 2 |  | 2 | 4 |
| 3. | Životný cyklus systémov | 2 |  |  | 2 |
| 4. | Monitoring bezpečnostných udalostí | 2 |  | 4 | 6 |
| 5. | Bezpečnosť priemyselných systémov | 2 |  |  | 2 |
| 6. | Kybernetický bezpečnostný incident | 2 |  |  | 2 |
| 7. | Riešenie kybernetických bezpečnostných incidentov |  |  | 2 | 2 |
| 8. | Incidenty z trestno-právneho hľadiska a digitálna stopa | 2 |  | 4 | 6 |
| 9. | Overovanie úrovne kybernetickej bezpečnosti | 4 |  | 2 | 6 |
| 10. | Počítačové siete | 2 |  | 2 | 4 |
| 11. | Kryptografia II. | 4 |  | 2 | 6 |
| 12. | Simulácia riadenia bezpečnostného incidentu |  |  | 4 | 4 |
| **4. semester – skúška** | | **24** |  | **24** | **48** |

Tabuľka č. 16 Tematický plán predmetu Teória kybernetickej bezpečnosti II.

Zdroj: autor

**Záver**

Realizáciou medzinárodného výskumu na policajných školách na účel zisťovania úrovne povedomia a znalostí študentov z oblasti ochrany informácií spracúvaných v informačných systémoch PZ sa, žiaľ, na Slovensku aj vo Francúzsku potvrdila platnosť tejto hypotézy:

***„Existujú rezervy pri vzdelávaní aktérov pristupujúcich k dátam spracovávaným v informačných systémoch PZ o požadovanej úrovni ochrany týchto dát.“***

Overenie tejto hypotézy bolo cieľom výskumu, ku ktorému bola vypracovaná predkladaná vedecká štúdia. V štúdii sú okrem vyhodnotenia výskumu popísané i návrhy metód ochrany informácií na rôznych úrovniach, ale hlavný návrh bol smerovaný na oblasť vzdelávania.

V oboch krajinách sa potvrdili značné rezervy vo vedomostiach študentov zo skúmanej oblasti, čo bol dôvodom na ponúknutie návrhu metód ochrany informácií na procesnej, technickej, mechanickej, režimovej a softvérovej úrovni, na úrovni prístupov a na úrovni vzdelávania a osvety. V štúdii sa osobitne venujeme návrhu metód ochrany na úrovni vzdelávania, a to konkrétne formou návrhov tematických plánov pre nové predmety „základy kybernetickej bezpečnosti“, „teória kybernetickej bezpečnosti I“. a „teória kybernetickej bezpečnosti II.“, ktoré odporúčame implementovať do výučby na Akadémii Policajného zboru v Bratislave v študijných programoch bezpečnostnoprávna ochrana osôb a majetku a bezpečnostnoprávne služby vo verejnej správe.

Súčasne navrhujeme v najbližšom období doplnenie vyučovacích hodín o riešenie praktických situácií v rámci odborne zameraných seminárov, ktoré momentálne nie sú implementované v učebných osnovách a vypracovanie tematických plánov pre tieto semináre. Náplňou predmetných seminárov by mohlo byť príprava prezentácií konkrétnych útokov na dáta uložené nielen v informačných systémoch PZ, ale aj útokov na dáta iných inštitúcií, napr. útoky na dáta Úradu geodézie, kartografie a katastra Slovenskej republiky a Sociálnej poisťovne, ku ktorým by študenti aktívnym spôsobom navrhovali opatrenia proti prezentovaným útokom. Vzájomnou spoluprácou by stimulovali podnety, ktoré by mohli uplatňovať vo svojej budúcej bezpečnostnej praxi. Vďaka týmto podnetom by mohlo vzniknúť veľké množstvo výskumných projektov v oblasti bezpečnostnoprávnej ochrany osôb a majetku a bezpečnostnoprávnej služby vo verejnej správe. Niektoré z týchto projektov by mohli byť riešené na medzinárodnej úrovni a dotované z prostriedkov Interpolu a Europolu – konkrétne Európskym centrom boja proti počítačovej kriminalite.

Za dôležité považujeme závery realizovaného výskumu, ktoré boli, sú a aj budú podnetom pre pedagógov škôl z oboch krajín pre potenciálne inovácie učebných osnov a tematických plánov, prostredníctvom ktorých by chceli dosiahnuť vyššiu úroveň vedomostí svojich študentov i absolventov v oblasti ochrany informácií v informačných systémoch.

**Literatúra**

ANDRAŠKO a kol. *Právo kybernetickej bezpečnosti*. Bratislava: Právnická fakulta UK, 2022. ISBN: 978-80-716-0632-1.

DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Computer Press Praha, 2004. ISBN: 80-251-0106-1.

HANÁČEK, Petr a Jan STAUDEK. *Bezpečnost informačních systémů*. Úřad pro státní informační systém. Praha, 2000. ISBN 80-238-5400-3.

HENDL, Jan. Přehled statistických metod zpracování dat. Analýza a metaanalýza dat. Praha: Vydavateľstvo Portál, 2006. ISBN 80-7367-123-9.

HVORECKÝ, Jozef. *Databázové technológie.* Vydavateľstvo EQUILIBRIA, 2013. ISBN 978-8081430824.

KOSTREC, Matej a Eva KOSTRECOVÁ. Výskum informovanosti a povedomia z oblasti informačnej bezpečnosti*.* In: *Virtuální vědecká konference s mezinárodní účastí „Scientific reflection of new trends in management“ – sborník z konference*, s. 79 – 86. ISBN 978-80-7251-405-2.

KOSTREC, Matej. Classification of Data and Information and their Protection. In: *Sdělovací Technika telekomunikace-elektrotechnika-multimédia 05/2015*. Vydavateľ: Sdělovací technika s.r.o. Praha, 2015, s. 54 – 55. ISSN 0036-9942 DUBEN 2015

KOSTRECOVÁ, Eva. *Informačná bezpečnosť.* Bratislava: Slovenská technická univerzita, 2013. ISBN: 978-80-227-3927-6.

LEVICKÝ, Dušan. *Úvod do kybernetickej bezpečnosti*. Košice: Elfa, 2020. ISBN: 978-80-808-6276-3

ŠTĚDROŇ, Bohumír a Miroslav LUDVÍK. *Právo v informačních technologiích.* Computer Media, 2008. ISBN 978-8086686361.

**Elektronické publikácie**

[online]. [cit. 25. januára 2025]. Dostupné na internete: <https://www.nbu.gov.sk/612-sk/narodna-strategia-a-akcny-plan-kybernetickej-bezpecnosti>

[online]. [cit. 25. januára 2025]. Dostupné na internete: <http://www.ucps.sk/Dohovor_o_pocitacovej_kriminalite>

[online]. [cit. 25. januára 2025]. Dostupné na internete: <https://cybercompetence.sk>

**Key words:** scientific research, information protection, design of protection methods, teaching process, design of measures

**Summary**

The author of the scientific study aimed to verify the level of students' knowledge of information protection in information and communication systems through international research. Respondents from the Academy of the Police Corps in Bratislava and the French Police Academy (ENP) in Montbéliard participated in this research. In both countries, the research confirmed significant gaps in students' knowledge of the studied area, which was the reason for the author of the study to offer a proposal for methods of information protection at different levels (process, technical, mechanical, mode, software, access, and education and awareness levels). Specially in the study, the author addressed the proposal of methods of protection at the level of education, specifically in the form of proposals of Thematic Plans for new courses "Fundamentals of Cyber Security", "Cyber Security Theory I." and "Cyber Security Theory II.", which he recommends for implementation in the teaching at the Academy of the Police Corps in Bratislava.

*JUDr. Matej Kostrec, PhD.*

*Katedra informatiky a manažmentu*

*Akadémia PZ v Bratislave*

*Sklabinská 1, 835 17 Bratislava 35*

*e-mail: matej.kostrec@*[*akademiapz.sk*](mailto:email@email.cz)

Recenzenti: doc. Radim Valenčík, CSc.

doc. Mgr. Daniela Chudá, PhD.

1. KOSTREC, M. a E. KOSTRECOVÁ. *Metódy ochrany policajne relevantných informácií. Záverečná správa*

   *čiastkovej vedecko-výskumnej úlohy*, s. 80. [↑](#footnote-ref-1)
2. V súčasnosti sa používa aj názov École Nationale de Police de Montbéliard (ENP).

   Kontakt: 1 rue du Maréchal Juin, BP 68395 – 25208 MONTBÉLIARD, telefónne číslo: 03 81 31 60 60

   Dostupné na internete: <https://www.police-nationale.interieur.gouv.fr/nous-rejoindre/echangez-avec-nous/contacts-locaux/contacts-locaux/ecole-nationale-de-police-de-8> [↑](#footnote-ref-2)
3. KOSTREC, M. a E. KOSTRECOVÁ. *Metódy ochrany policajne relevantných informácií. Záverečná správa*

   *čiastkovej vedecko-výskumnej úlohy*, s. 10 –14. [↑](#footnote-ref-3)
4. KOSTREC, M. a E. KOSTRECOVÁ. *Metódy ochrany policajne relevantných informácií. Záverečná správa*

   *čiastkovej vedecko-výskumnej úlohy*, s. 70. [↑](#footnote-ref-4)
5. [online]. [cit. 25. januára 2025]. Dostupné na internete: https://www.proofpoint.com/fr/threat-reference/data-classification [↑](#footnote-ref-5)
6. KOSTREC, M. a E. KOSTRECOVÁ. *Metódy ochrany policajne relevantných informácií. Záverečná správa*

   *čiastkovej vedecko-výskumnej úlohy*, s. 70. [↑](#footnote-ref-6)
7. Tamtiež, s. 72. [↑](#footnote-ref-7)
8. Tamtiež, s. 73. [↑](#footnote-ref-8)