Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Analýza študijných programov slovenských vysokých škôl z pohľadu rozvoja kyberbezpečnostných kapacít

Účel materiálu	Posúdiť, do akej miery jednotlivé vysoké školy na Slovensku vytvárajú predpoklady pre prípravu absolventov použiteľných v oblasti technickej kyberbezpečnosti, informačnej bezpečnosti, bezpečnostného manažmentu a príbuzných disciplín.

Analýza vznikla v rámci projektu Nitrianske kompetenčné centrum pre kybernetickú bezpečnosť č. 17R05-04-V01-00003, financovaného z Plánu obnovy a odolnosti Slovenskej republiky.

Autori: PaedDr. Peter Švec, Ph.D.

RNDr. Ján Skalka, PhD

Nitra, marec 2026

1 Účel materiálu a výskumná otázka

Cieľom tohto materiálu je posúdiť, do akej miery jednotlivé vysoké školy v Slovenskej republike vytvárajú predpoklady pre prípravu absolventov využiteľných v oblasti technickej kyberbezpečnosti, informačnej bezpečnosti, bezpečnostného manažmentu a príbuzných disciplín. Predmetom analýzy nie je všeobecná kvalita vysokých škôl ani formálne akreditačné hodnotenie študijných odborov, ale verejne overiteľná podoba ich študijnej ponuky, profilov absolventov, predmetovej skladby a bezpečnostne relevantných kompetencií. Východiskovým rámcom sú najmä akreditované študijné programy evidované v registri Portálu VŠ a ich doplnenie o oficiálne verejne dostupné informácie z webových sídiel univerzít, fakúlt, katedier a verejných informačných systémov štúdia.

Materiál vychádza z predpokladu, že rozvoj kyberbezpečnostných kapacít nemožno posudzovať iba podľa názvu študijného programu alebo podľa toho, či škola používa označenie „kyberbezpečnosť“ či „informačná bezpečnosť“. Pre potreby štátu, verejnej správy, kritickej infraštruktúry a súkromného sektora sú rovnako dôležité aj programy, ktoré pripravujú odborníkov v oblastiach správy sietí a systémov, kryptografie, bezpečnosti softvéru, riešenia incidentov, riadenia rizík, kontinuity činností, bezpečnostného manažmentu a právno-regulačného zabezpečenia kybernetickej bezpečnosti. Takéto chápanie zodpovedá aj vyhláške NBÚ č. 492/2022 Z. z., ktorá ustanovuje znalostné štandardy prostredníctvom jednotlivých rolí kybernetickej bezpečnosti, a tiež európskemu rámcu ECSF, ktorý prepája profesionálne roly s úlohami, znalosťami, zručnosťami a kompetenciami.

Význam takejto analýzy zosilňuje aj regulačné prostredie Európskej únie. Smernica NIS2 vytvára spoločný regulačný rámec kybernetickej bezpečnosti v EÚ a vyžaduje od členských štátov posilňovanie kybernetických kapacít, zavádzanie opatrení riadenia kybernetických rizík a rozvoj schopností v kritických sektoroch. Z tohto pohľadu je vysoké školstvo jedným z kľúčových mechanizmov, prostredníctvom ktorých možno dlhodobo budovať odborné, manažérske a analytické kapacity potrebné na plnenie požiadaviek verejného aj súkromného sektora.

Hlavná výskumná otázka dokumentu preto znie: “Do akej miery slovenské vysoké školy prostredníctvom svojich študijných programov, fakúlt, katedier a verejne identifikovateľných predmetov vytvárajú podmienky na prípravu absolventov využiteľných pre potreby technickej kyberbezpečnosti, informačnej bezpečnosti, bezpečnostného manažmentu a súvisiacich bezpečnostných rolí?”

Táto otázka bude ďalej rozpracovaná do viacerých čiastkových otázok:

- ktoré školy majú explicitný alebo implicitný informatický a bezpečnostný profil;
- kde je bezpečnostná zložka sústredená do samostatných programov a kde je rozptýlená medzi predmety;
- ktoré bezpečnostné domény sú vo verejne dostupných kurikulách pokryté najvýraznejšie;
- kde sa naopak prejavujú medzery z pohľadu znalostných štandardov, rolí a potrieb praxe.

Z preskúmanej verejne dostupnej ponuky študijných programov a informačných listov predmetov vyplýva, že na Slovensku existujú iba tri vysoké školy so zreteľne identifikovateľným, priamo technicky orientovaným kyberbezpečnostným profilom:

- Slovenská technická univerzita v Bratislave (FIIT, program Informačná bezpečnosť)
- Technická univerzita v Košiciach (FEI, program Kyberbezpečnosť)
- Žilinská univerzita v Žiline (FRI, program Informačné a sieťové technológie)

Ďalšiu skupinu tvoria školy s kvalitným všeobecným informatickým základom, ktoré môžu slúžiť ako zdroj budúcich kyberšpecialistov po doplnení špecializačných predmetov, laboratórií a partnerstiev s praxou. Do tejto skupiny patria najmä UK, UPJŠ, UKF, UCM a Paneurópska vysoká škola.

Samostatnú kategóriu tvoria školy so silnou väzbou na bezpečnostné riadenie, obranu alebo policajnú prax. Tie sú dôležité pre rezortné roly, ale spravidla nie sú hlavným zdrojom technických kyberšpecialistov. Ide najmä o Akadémiu ozbrojených síl, Akadémiu Policajného zboru a Vysokú školu bezpečnostného manažérstva v Košiciach.

Väčšina ostatných škôl buď nemá vo verejnej ponuke identifikovaný relevantný informatický/kyberbezpečnostný program, alebo ide len o nepriamy presah (napr. učiteľstvo informatiky, digitálne umenia).

Materiál má slúžiť ako strategicko-analytický podklad pre ďalšie rozhodovanie o smerovaní podpory, rozvoji študijných programov, tvorbe partnerstiev s praxou a nastavovaní verejných intervencií v oblasti kyberbezpečnostného vzdelávania. Zároveň má vytvoriť porovnateľný a metodicky obhájiteľný základ pre ďalšie časti dokumentu, v ktorých budú jednotlivé školy analyzované podľa jednotného interpretačného rámca a iba na základe verejne dostupných zdrojov.

2 Metodika a interpretačný rámec

2.1 Východiská analýzy

Analýza je založená na verejne dostupných zdrojoch, ktoré sú dostupné aj budúcim čitateľom výsledného materiálu. Základný evidenčný rámec tvorí Portál VŠ, ktorý sprístupňuje register akreditovaných študijných programov a verejné profily vysokých škôl, fakúlt a študijných programov. Tento register slúži ako východisko na identifikáciu inštitúcií a programov, ktoré vstupujú do hodnotenia.

Druhú vrstvu zdrojov tvoria oficiálne webové sídla univerzít, fakúlt a katedier, najmä stránky študijných programov, profily absolventa, odporúčané študijné plány, zoznamy predmetov a tematické zamerania pracovísk. Tretiu vrstvu predstavujú verejne dostupné informačné listy predmetov a verejné výstupy z AIS alebo obdobných akademických systémov, ak sú dostupné bez interného prihlásenia. Do analýzy sa nezahŕňajú interné podklady, nepublikované sylaby ani dokumenty, ktoré čitateľ výslednej správy nebude vedieť samostatne overiť. Tento princíp je zámerný: cieľom dokumentu je vytvoriť verifikovateľný analytický podklad, nie rekonštruovať interné kurikulum jednotlivých pracovísk.

2.2 Predmet analýzy a jednotka hodnotenia

Predmetom hodnotenia nie je vysoká škola ako celok v zmysle jej všeobecnej kvality, reputácie alebo výskonnosti. Predmetom analýzy je verejne identifikovateľná schopnosť vysokej školy vytvárať podmienky pre prípravu absolventov využiteľných v oblasti technickej kyberbezpečnosti, informačnej bezpečnosti, bezpečnostného manažmentu a príbuzných bezpečnostných disciplín. Základnou jednotkou hodnotenia je preto kombinácia vysoká škola – fakulta – katedra alebo pracovisko – študijný program – predmetová skladba. Takéto členenie umožňuje zachytiť aj situácie, keď bezpečnostná línia nie je sústredená v jednom samostatnom programe, ale vzniká kombináciou viacerých predmetov, špecializácií alebo spolupráce viacerých pracovísk v rámci tej istej školy.

Za relevantné sa nepovažujú iba programy s explicitným názvom „kyberbezpečnosť“ alebo „informačná bezpečnosť“. Do hodnotenia vstupujú aj programy, ktoré majú informatické, sieťové, softvérové, informačno-systémové, bezpečnostno-manažérske, právne, forenzné, obranné alebo iné príbuzné jadro, ak sa pri nich dá z verejných zdrojov doložiť väzba na ochranu informačných aktív, systémov, sietí, prevádzky alebo bezpečnostných procesov. Tento širší prístup je v súlade s tým, že slovenská vyhláška NBÚ č. 492/2022 Z. z. aj európsky rámec ECSF nechápu kybernetickú bezpečnosť ako jedinú úzko technickú profesiu, ale ako súbor rôznych rolí s technickými, organizačnými a riadiacimi presahmi.

2.3 Vymedzenie základných pojmov

Pre potreby tohto materiálu sa za informaticky orientovaný program považuje taký študijný program, ktorý je vedený v odbore informatika alebo má zreteľný technologický základ v oblastiach ako aplikovaná informatika, počítačové siete, informačné systémy, softvérové inžinierstvo, počítačové inžinierstvo, dátové technológie, umelá inteligencia, automatizácia a

ďalšie technické smery, ktoré môžu vytvárať predpoklady pre bezpečnostnú špecializáciu. Pri príbuzných programoch sa sleduje najmä to, či profil absolventa, pracovisko a predmetová skladba vytvárajú preukázateľné prepojenie na bezpečnostné kompetencie.

Za bezpečnostný predmet alebo bezpečnostný modul sa považuje každý verejne identifikovateľný predmet, zameranie alebo výučbový blok, ktorého obsah sa explicitne dotýka aspoň jednej z nasledujúcich oblastí: kybernetická bezpečnosť, informačná bezpečnosť, sieťová bezpečnosť, bezpečnosť operačných systémov, kryptografia, penetračné testovanie, digitálna forenzika, riešenie bezpečnostných incidentov, bezpečnostný monitoring, riadenie rizík, bezpečnostné politiky, audit, governance, compliance, ochrana súkromia, bezpečnosť vývoja softvéru, ochrana kritickej infraštruktúry, bezpečnosť priemyselných a kyber-fyzikálnych systémov, právne a regulačné aspekty bezpečnosti, fyzická bezpečnosť, kontrola prístupu, personálna bezpečnosť, kontinuita činností alebo bezpečnostný manažment. Takéto široké vymedzenie je metodicky odôvodnené tým, že NIS2 výslovne zahŕňa medzi opatrenia riadenia kybernetických rizík nielen technické témy, ale aj incident handling, business continuity, supply chain security, security in network and information systems acquisition, development and maintenance, policies and procedures to assess effectiveness, basic cyber hygiene, cryptography, human resources security, access control policies a asset management.

Za technickú kyberbezpečnostnú prípravu sa v tomto materiáli považuje predovšetkým príprava zameraná na ochranu sietí, systémov, aplikácií, dát a digitálnej infraštruktúry prostredníctvom technických a analytických metód prevencie, detekcie, testovania a reakcie. Za informačnú bezpečnosť sa považuje širší rámec ochrany dôvernosti, integrity a dostupnosti informácií a informačných aktív. Za bezpečnostný manažment sa považuje príprava v oblastiach riadenia rizík, bezpečnostných procesov, auditov, compliance, kontinuity činností, ochrany aktív a organizačných opatrení. Za príbuzný bezpečnostný profil sa považujú aj právne, forenzné, obranné, policajné, fyzicko-bezpečnostné a rezortné línie, pokiaľ sú preukázateľne previazané s ochranou informačných systémov, digitálnych dôkazov, kritickej infraštruktúry alebo kybernetických procesov. Toto rozlíšenie umožňuje zachytiť aj školy, ktoré nepripravujú primárne „security engineerov“, ale produkujú absolventov pre roly v oblasti compliance, auditov, vyšetrovania, bezpečnostnej politiky alebo riadenia bezpečnosti.

2.4 Dvojúrovňový pohľad na bezpečnostné kapacity

Materiál pracuje s dvoma analytickými rovinami, ktoré sa hodnotia súbežne.

Prvou rovinou je jadrová technická kyberpríprava. Do nej patria najmä programy, predmety a pracoviská, ktoré sa priamo venujú technickej ochrane sietí, systémov, aplikácií, dátových tokov a infraštruktúr. Ide napríklad o predmety a moduly z oblasti kyberbezpečnosti, informačnej bezpečnosti, sieťovej bezpečnosti, bezpečnosti operačných systémov, kryptografie, penetračného testovania, digitálnej forenziky, malware analýzy, bezpečnostného monitoringu, incident response alebo ochrany priemyselných riadiacich systémov. Táto rovina je rozhodujúca pri posudzovaní schopnosti školy pripravovať absolventov pre technické bezpečnostné roly.

Druhou rovinou je širší bezpečnostný profil relevantný pre rozvoj kyberbezpečnostných kapacít. Do nej patria predmety, moduly a programy, ktoré síce nemusia byť jadrovo technické, ale vytvárajú dôležité kapacity v oblastiach právnej regulácie, bezpečnostného manažmentu, auditu, riadenia rizík, fyzickej bezpečnosti, kontroly prístupu, ochrany kritickej infraštruktúry, personálnej bezpečnosti, kontinuity činností, rezortnej obrany, policajného vyšetrovania alebo digitálnej forenziky. Zaradenie tejto roviny je metodicky potrebné, pretože NIS2 aj vykonávacie akty EÚ výslovne prepájajú kybernetickú bezpečnosť s access control policies, human resources security a manažérskou zodpovednosťou, zatiaľ čo vyhláška NBÚ aj ECSF pracujú s rolami, ktoré nie sú len technické, ale aj procesné, organizačné a riadiace.

Táto dvojúrovňová logika je dôležitá najmä preto, aby výsledná analýza nepreceňovala školy s výraznou manažérskou alebo právnou bezpečnostnou vetvou ako ekvivalent technických cyber engineering pracovísk, ale zároveň ich neignorovala ako nerelevantné. Výsledkom má byť ucelený pohľad na bezpečnostný ekosystém vysokého školstva, v ktorom technické, právne, procesné, fyzické a rezortné línie plnia odlišné, no komplementárne funkcie.

2.5 Pravidlá hodnotenia a sila dôkazu

Pri hodnotení sa dôsledne rozlišuje medzi existenciou programu, deklarovaným profilom programu a verejne doloženým obsahom programu. Samotný názov študijného programu nie je považovaný za dostatočný dôkaz o skutočnom bezpečnostnom profile. Vyššiu váhu preto dostávajú tie školy a pracoviská, pri ktorých možno okrem samotnej existencie programu identifikovať aj profil absolventa, predmetovú mapu, sylaby, informačné listy alebo aspoň explicitne pomenované tematické bezpečnostné okruhy. Nižšiu váhu majú všeobecné prezentačné texty bez jasnej väzby na konkrétne predmety alebo študijné výstupy.

Pre potreby porovnania sa zavádza pomocná škála sily dôkazu:

- S – silný dôkaz: program aj jeho bezpečnostná zložka sú verejne doložené kombináciou Portálu VŠ a konkrétnych oficiálnych stránok programu, študijných plánov, informačných listov alebo verejných predmetových rozpisov.
- M – stredný dôkaz: program je verejne potvrdený a bezpečnostná línia je naznačená oficiálnym opisom programu, profilom absolventa, katedrovým zameraním alebo zoznamom predmetov, ale bez úplne čitateľnej predmetovej mapy.
- N – nízky dôkaz: existuje iba nepriamy alebo čiastkový verejný signál a bezpečnostnú zložku nemožno bez ďalšieho verejného potvrdenia považovať za dostatočne doloženú.

Táto škála nie je hodnotením kvality školy. Ide o metodický nástroj na odlíšenie toho, ako silno možno obhájiť daný záver.

2.6 Klasifikačný model škôl

Na základe verejne doloženého profilu budú školy v ďalších častiach dokumentu priebežne zaraďované do pomocných kategórií:

- Kategória A – priama technická kyberpríprava - školy, pri ktorých je z verejných zdrojov doložiteľný explicitný program kybernetickej bezpečnosti alebo informačnej bezpečnosti, prípadne veľmi zreteľná a systematicky vybudovaná technická bezpečnostná línia v jadre informatiky. Pre toto zaradenie nestačí samotný názov programu; rozhodujúce je, aby sa popri programe dali verejne identifikovať aj konkrétne predmety alebo moduly z oblastí ako sieťová bezpečnosť, bezpečnosť operačných systémov, kryptografia, digitálna forenzika, penetračné testovanie, bezpečnostný monitoring alebo riešenie incidentov.
- Kategória B – silný informatický základ s bezpečnostným presahom - školy, ktoré majú verejne potvrdený informatický alebo príbuzný technologický program a pri ktorých sa zároveň dajú verejne identifikovať bezpečnostné predmety, tematické bloky, zamerania alebo iné bezpečnostne relevantné prvky. Ide o školy, ktoré síce nemajú bezpečnosť ako hlavný názov programu alebo dominantné jadro svojej ponuky, ale vytvárajú preukázateľný základ pre prípravu absolventov využiteľných v bezpečnostných rolách alebo pre ich ďalšiu bezpečnostnú profiláciu.
- Kategória C – bezpečnostno-manažérsky, rezortný, právno-forenzný alebo kriticko-infraštruktúrny profil - školy, ktoré sú relevantné pre rozvoj bezpečnostných kapacít, ale nie primárne ako jadro civilnej technickej kyberprípravy. Ide najmä o programy a línie v oblastiach bezpečnostného manažmentu, práva, auditu, compliance, obrany, policajnej praxe, vyšetrovania, digitálnej forenziky, fyzickej bezpečnosti, ochrany kritickej infraštruktúry, priemyselnej bezpečnosti alebo informačno-systémového riadenia. Zaradenie do tejto kategórie znamená, že škola rozvíja bezpečnostné kapacity dôležité pre širší bezpečnostný ekosystém štátu, verejnej správy alebo organizácií, ale nie primárne cez jadro technického cyber engineeringu.
- Kategória D – nepriamy digitálny alebo pedagogický presah - školy, pri ktorých možno z verejných zdrojov potvrdiť digitálny, informatický, AI alebo pedagogický presah, ale nie bezpečnostný profil v zmysle predchádzajúcich kategórií. Ide napríklad o učiteľstvo informatiky, učiteľstvo matematiky a informatiky, digitálne umenia, umelecké programy s využitím AI alebo iné odbory, ktoré rozvíjajú digitálne kompetencie, no nie priamo kyberbezpečnostné alebo bezpečnostno-manažérske kapacity.
- Kategória E – bez verejne potvrdeného relevantného profilu v tomto screeningu - školy, pri ktorých sa v čase spracovania nepodarilo z verejných zdrojov potvrdiť samostatný informatický alebo bezpečnostne relevantný profil s dostatočnou väzbou na ciele tejto analýzy. Takéto zaradenie neznamená, že škola nemá žiadne digitálne alebo bezpečnostné prvky; znamená iba to, že ich nebolo možné verejne a metodicky dostatočne potvrdiť na úrovni programu, pracoviska alebo predmetovej skladby.

Tento model má čisto analytickú funkciu. Nepredstavuje rebríček kvality škôl, ale pomôcku na systematické usporiadanie zistení. Jeho použitie je opodstatnené práve preto, že NBÚ aj ECSF pracujú s rôznymi typmi bezpečnostných rolí a NIS2 kladie dôraz aj na netechnické bezpečnostné opatrenia, takže rozvoj kyberkapacít nemožno redukovať na jediný typ študijného programu.

2.7 Interpretačný rámec analýzy

Interpretačný rámec dokumentu stojí na troch oporných osiach.

Prvou je verejne overiteľná akademická ponuka, teda to, čo školy navonok deklarujú prostredníctvom akreditovaných programov, profilov absolventa, fakúlt, katedier a verejných študijných dokumentov. Druhou je rolový a kompetenčný rámec, odvodený od vyhlášky NBÚ č. 492/2022 Z. z. a od ENISA ECSF. Vyhláška NBÚ výslovne uvádza, že znalostné štandardy sú určené na preukazovanie minimálnych požiadaviek na výkon konkrétnej roly a budovanie bezpečnostného povedomia, pričom znalostné štandardy pre určitú rolu môžu byť splnené aj kolektívne ich vzájomným zdieľaním. ENISA ECSF zas ponúka európsky referenčný rámec pre prepájanie rolí, úloh, znalostí, zručností a kompetencií.

Treťou osou je regulačný a strategický kontext EÚ, reprezentovaný najmä smernicou NIS2 a nadväzujúcimi vykonávacími pravidlami. Tieto akty ukazujú, že kybernetická bezpečnosť sa v súčasnom európskom prostredí chápe ako kombinácia technických, organizačných, personálnych, prístupových a riadiacich opatrení. Z tohto dôvodu budú v ďalších častiach dokumentu za relevantné považované nielen technické predmety, ale aj tie vzdelávacie línie, ktoré pripravujú absolventov na právne, riadiace, auditné, forenzné, fyzicko-bezpečnostné alebo rezortné roly, pokiaľ sú preukázateľne previazané s ochranou informačných aktív, systémov alebo kritických procesov.

Na tomto základe budú školy interpretované podľa toho, aký typ bezpečnostných kapacít sú schopné verejne doložiteľne vytvárať: technické, kombinované technicko-organizačné, manažérske, právne, forenzné, fyzicko-bezpečnostné alebo rezortné. Takto nastavený rámec lepšie zodpovedá realite slovenského vysokoškolského prostredia aj súčasným požiadavkám praxe.

2.8 Limity metodiky

Použitá metodika má svoje limity. Verejne dostupné zdroje nemusia zachytiť plnú podobu reálne vyučovaného kurikula, vnútorné laboratórne kapacity, rozsah spolupráce s praxou, nepublikované voliteľné predmety ani kvalitu pedagogického zabezpečenia. Niektoré školy zverejňujú podrobné študijné plány a informačné listy, iné iba stručné opisné profily programov. Výsledky preto treba čítať ako analýzu verejne doložiteľných predpokladov, nie ako úplný audit reálneho fungovania jednotlivých pracovísk.

Rovnako platí, že zaradenie právnych, fyzických, procesných alebo rezortných bezpečnostných prvkov do hodnotenia neznamená ich automatické stotožnenie s technickou kyberprípravou. Ich úloha je v materiáli komplementárna: dopĺňajú obraz celkových bezpečnostných kapacít vysokého školstva, ale nenahrádzajú technické jadro tam, kde je cieľom príprava sieťových, systémových alebo aplikačných bezpečnostných špecialistov. Výsledná interpretácia preto bude v ďalších častiach dôsledne rozlišovať medzi jadrovou technickou kyberprípravou a širším bezpečnostným profilom relevantným pre rozvoj kyberbezpečnostných kapacít.

3. Pravidlá práce so zdrojmi

3.1 Zásada verejnej overiteľnosti

Tento materiál je založený výlučne na verejne dostupných a samostatne overiteľných zdrojoch. Do analytického korpusu sa zaraďujú len také zdroje, ku ktorým má prístup aj budúci overovateľ výsledného dokumentu bez potreby interného oprávnenia, prihlasovacích údajov alebo neverejnej distribúcie. Základným cieľom tejto zásady je zabezpečiť, aby boli všetky tvrdenia v materiáli spätne dohľadateľné, kontrolovateľné a obhájiteľné.

Táto zásada má aj metodický dôsledok: ak určitý program, predmet, špecializácia alebo profil absolventa nie je možné potvrdiť z verejne dostupných zdrojov, v dokumente sa s ním nepracuje ako s potvrdeným faktom, ale nanajvýš ako s nepreukázaným alebo len čiastočne doloženým prvkom. Absencia verejného dôkazu preto neznamená, že daná výučba na škole neexistuje; znamená len to, že ju nemožno zodpovedne použiť v analytickom hodnotení založenom na verejnej verifikovateľnosti.

3.2 Hlavné skupiny použitých zdrojov

Prvú a základnú skupinu zdrojov tvorí Portál VŠ, najmä register študijných programov a verejné profily škôl, fakúlt a programov. Portál VŠ slúži ako východisková evidencia akreditovaných študijných programov a ako referenčný nástroj na identifikáciu škôl, fakúlt, stupňov štúdia, odborov a názvov programov. V materiáli sa preto používa ako primárny register na overenie, či je daný program verejne evidovaný a v akom základnom profile je prezentovaný.

Druhú skupinu zdrojov tvoria oficiálne stránky univerzít, fakúlt, katedier a študijných programov. Tieto zdroje sú rozhodujúce tam, kde Portál VŠ potvrdzuje existenciu programu, ale neposkytuje dostatočnú hĺbku pre posúdenie jeho bezpečnostného profilu. Z oficiálnych stránok sa využívajú najmä profily absolventa, tematické zameranie pracoviska, odporúčané študijné plány, verejné zoznamy predmetov, špecializačné vetvy a opis spolupráce medzi fakultami alebo katedrami. V prípade rozporu medzi všeobecným opisom školy a konkrétnou programovou stránkou má vyššiu váhu programová alebo fakultná stránka.

Tretiu skupinu tvoria verejne dostupné informačné listy predmetov, verejné AIS výstupy a iné oficiálne predmetové rozpisy, ak sú zverejnené bez prihlasovania. Tieto zdroje majú pre samotné hodnotenie mimoriadny význam, pretože práve ony umožňujú zistiť, či sa bezpečnostná zložka na škole prejavuje len na úrovni všeobecnej deklarácie, alebo aj v konkrétnej výučbe. Ak je dostupný informačný list predmetu alebo verejný študijný plán, má pri hodnotení vyššiu váhu než všeobecný marketingový opis programu.

Štvrtú skupinu tvoria normatívne a rámcové zdroje, ktoré sa nepoužívajú na overovanie existencie konkrétnych programov, ale na ich interpretáciu. Patria sem najmä vyhláška NBÚ č. 492/2022 Z. z., smernica NIS2 a rámec ENISA ECSF. Vyhláška NBÚ ustanovuje znalostné štandardy prostredníctvom jednotlivých rolí kybernetickej bezpečnosti a určuje ich na preukazovanie minimálnych požiadaviek na výkon konkrétnej roly a budovanie bezpečnostného povedomia. ENISA ECSF definuje 12 typických profesionálnych rolí a prepája ich s úlohami, znalosťami,

zručnosťami a kompetenciami. NIS2 zasa vytvára spoločný európsky rámec opatrení na riadenie kybernetických rizík a tým rozširuje interpretáciu bezpečnostných kapacít aj na organizačné, procesné a riadiace oblasti.

Pri spracovaní sa používa hierarchia dôveryhodnosti zdrojov. Na najvyššej úrovni stoja oficiálne právne a regulačné zdroje, teda Slov-Lex, EUR-Lex a ENISA, pokiaľ ide o definície rolí, štandardov a interpretačných rámcov. Pri identifikácii konkrétnych študijných programov je základným referenčným zdrojom Portál VŠ. Pri posudzovaní obsahu programu majú najvyššiu váhu verejné študijné plány, informačné listy predmetov a oficiálne programové stránky fakúlt a katedier.

Prakticky to znamená, že ak Portál VŠ potvrdzuje existenciu programu, ale oficiálna stránka programu alebo verejný študijný plán ukazujú presnejší obsah, pri analytickom posúdení sa vychádza z detailnejšieho a obsahovo bližšieho zdroja. Ak je naopak dostupný len všeobecný opis programu bez predmetového rozpadu, záver musí zostať opatrnejší. Hierarchia teda nie je len technická, ale aj obsahová: vyššiu váhu má zdroj, ktorý sa nachádza bližšie ku konkrétnemu jadru výučby.

3.3 Pravidlá výberu zdrojov pre jednotlivé školy

Pri každej škole sa výber zdrojov riadi rovnakým sledom. Najprv sa overuje existencia relevantného programu v registri Portálu VŠ. Následne sa vyhľadávajú oficiálne programové stránky danej univerzity alebo fakulty. Potom sa podľa dostupnosti dopĺňajú katedrové stránky, verejné študijné plány, odporúčané predmetové skladby a informačné listy predmetov. Až na záver sa používajú širšie kontextové zdroje, napríklad informácie o profilácii pracoviska, partnerstvách alebo laboratóriách, a to len vtedy, ak už existuje jasný programový základ.

Tento postup bráni tomu, aby sa analytické závery opierali len o všeobecné sebaprezentačné tvrdenia univerzity bez jasného spojenia s konkrétnym študijným programom. Rovnako bráni tomu, aby sa z jednej zaujímavej katedrovej aktivity automaticky vyvodzoval záver o celkovom profile fakulty alebo školy. Zdroj musí byť v materiáli vždy naviazaný na konkrétnu úroveň hodnotenia: škola, fakulta, katedra, program alebo predmet.

3.4 Pravidlá pri práci s predmetmi a bezpečnostnými prvkami

Vzhľadom na účel dokumentu sa pri posudzovaní predmetov neprihliada len na technické disciplíny typu sieťová bezpečnosť, bezpečnosť operačných systémov či kryptografia. Do zdrojovej analýzy sa zahŕňajú aj tie predmety a zamerania, ktoré sú verejne doložiteľne previazané s ochranou informačných aktív, systémov, prevádzky alebo bezpečnostných procesov, teda napríklad právo kybernetickej bezpečnosti, riadenie rizík, bezpečnostný audit, kontinuita činností, fyzická bezpečnosť, kontrola prístupu, ochrana kritickej infraštruktúry, digitálna forenzika alebo bezpečnostný manažment. Takýto prístup je v súlade s vyhláškou NBÚ, s ENISA ECSF aj s NIS2, ktoré bezpečnosť nechápu čisto technicky, ale ako kombináciu technických, organizačných, právnych a riadiacich opatrení.

Zároveň platí, že samotná prítomnosť právneho, fyzicko-bezpečnostného alebo manažérskeho predmetu ešte neznamená, že škola disponuje technickým kyberbezpečnostným jadrom. Pri práci

so zdrojmi sa preto tieto prvky dokumentujú a berú do úvahy, ale v interpretácii sa dôsledne odlišujú od jadrovej technickej kyberprípravy. Zdrojové pravidlá teda nevylučujú širší bezpečnostný profil, ale vyžadujú jeho vecné oddelenie od technických bezpečnostných kapacít.

3.5 Pravidlá pri rozpore alebo neúplnosti zdrojov

Ak sa medzi zdrojmi objaví rozpor, uplatňuje sa pravidlo, že vyššiu váhu má konkrétnejší a bližší zdroj. To znamená, že verejný študijný plán alebo informačný list predmetu má väčšiu váhu než všeobecný opis programu; programová stránka má väčšiu váhu než všeobecná domovská stránka univerzity; a oficiálny právny predpis má väčšiu váhu než sekundárny opis rámca. Tento princíp je rozhodujúci najmä pri školách, kde sú marketingové tvrdenia širšie než verejne doložiteľná predmetová skladba.

Ak sú zdroje neúplné, materiál to priznáva priamo v texte. V takom prípade sa škola alebo program nezaradí na základe domnienky, ale len na základe úrovne, ktorú možno verejne potvrdiť. Tento postup je dôležitý pre metodickú poctivosť: cieľom dokumentu je ukázať stav, ktorý je z verejnej dokumentácie čitateľný a porovnateľný.

3.6 Pravidlá citovania a dokumentovania tvrdení

V ďalších častiach materiálu sa každé nosné tvrdenie opiera o konkrétny verejný zdroj alebo súbor zdrojov. Pri každej škole bude preto potrebné uvádzať aspoň:

- zdroj potvrdzujúci existenciu programu,
- zdroj potvrdzujúci relevantnú fakultu alebo pracovisko,
- zdroj potvrdzujúci predmety, zameranie alebo profil absolventa.

Takýto postup znižuje riziko, že by sa analytický záver oprel len o jeden čiastkový údaj. Zároveň umožňuje rozlišovať medzi tvrdením „škola má informatický program“, tvrdením „škola má bezpečnostný predmet“ a tvrdením „škola má systematickú bezpečnostnú líniu“. Každé z týchto tvrdení vyžaduje inú úroveň zdrojovej opory.

3.7 Limity zdrojovej základne

Aj pri dôslednom dodržaní vyššie uvedených pravidiel ostáva potrebné počítať s tým, že verejná zdrojová základňa je medzi školami nerovnomerná. Niektoré univerzity a fakulty publikujú detailné študijné plány, informačné listy a tematické rozpisy, zatiaľ čo iné zverejňujú len základný opis programu. Dokument preto nehodnotí len samotnú prítomnosť bezpečnostného obsahu, ale aj jeho verejnú čitateľnosť a preukázateľnosť, čo znamená, že výsledná analýza bude nevyhnutne citlivejšia na transparentnosť jednotlivých škôl. Táto vlastnosť však nie je slabinou metodiky, ale súčasťou zistenia: z pohľadu verejnej politiky a porovnateľnosti je totiž relevantné aj to, nakoľko školy dokážu svoj bezpečnostne relevantný profil verejne a konkrétne komunikovať.

4. Sumarizačný prehľad vysokých škôl podľa identifikovaného bezpečnostného profilu

Táto sekcia zachytáva školy, pri ktorých sa podarilo potvrdiť informatický, kyberbezpečnostný alebo širší bezpečnostne relevantný profil na úrovni programu, fakulty, katedry alebo predmetu.

4.1 Školy s verejne potvrdenou priamou technickou kyberprípravou

Slovenská technická univerzita v Bratislave (FIIT STU) – kategória A / dôkaz S.

Na Fakulte informatiky a informačných technológií Slovenskej technickej univerzity v Bratislave je verejne potvrdený inžiniersky študijný program Informačná bezpečnosť na oficiálnej stránke programu (https://www.fiit.stuba.sk/studijne-programy/inzinierske/informacna-bezpecnost.html?page_id=4926) aj v registri Portálu VŠ (https://www.portalvs.sk/sk/studijny-program/stu-informacna-bezpecnost0).

Verejne dostupný katalóg predmetov FIIT pre akademický rok 2025/2026 je zverejnený na samostatnej adrese (https://www.fiit.stuba.sk/buxus/docs/Studium/katalog-predmetov_2025-26.pdf) a potvrdzuje existenciu bezpečnostne orientovaných predmetov v jadre študijnej ponuky.

Technická univerzita v Košiciach (FEI TUKE) – kategória A / dôkaz S.

Fakulta elektrotechniky a informatiky Technickej univerzity v Košiciach má verejne potvrdený bakalársky aj inžiniersky študijný program Kyberbezpečnosť v registri Portálu VŠ (https://www.portalvs.sk/sk/studijny-program/kyberbezpecnost, https://www.portalvs.sk/sk/studijny-program/kyberbezpecnost1). Fakulta zároveň na oficiálnej stránke študijných programov uvádza pri programe Kyberbezpečnosť priamy odkaz na študijný plán (https://fei.tuke.sk/sk/studijne-programy).

Samotné PDF študijných plánov sú verejne dostupné na presných adresách (https://api.prod.tuke.sk/smb/medias/2025/03/PS_2024_bc_kyberbezpecnost.pdf, https://api.prod.tuke.sk/smb/medias/2025/03/PS_2023_ing_Kyberbezpecnost.pdf).

Žilinská univerzita v Žiline (FRI UNIZA) – kategória A / dôkaz S.

Na Fakulte riadenia a informatiky Žilinskej univerzity v Žiline je verejne potvrdený študijný program Informačné a sieťové technológie (https://www.portalvs.sk/sk/studijny-program/informacne-a-sietove-technologie). Katedra informačných sietí na svojej oficiálnej stránke uvádza, že spolu s Katedrou technickej kybernetiky zabezpečuje tento študijný program a že jej vzdelávacie a výskumné aktivity sú orientované na počítačové komunikačné siete založené na IP a ich bezpečnosť (https://www.kis.fri.uniza.sk/katedra/, https://www.fri.uniza.sk/pracoviska/k-i-s).

Verejne sú zároveň dostupné konkrétne predmety Bezpečnosť informačných systémov (https://www.kis.fri.uniza.sk/bis-bezpecnost-informacnych-systemov/) a Riešenie

bezpečnostných incidentov (https://www.kis.fri.uniza.sk/rbi-riesenie-bezpecnostnych-incidentov/), pričom pri predmete Riešenie bezpečnostných incidentov je verejne doložená väzba na koncept Security Operations Center, monitorovanie bezpečnosti siete, analýzu narušenia bezpečnosti a reakciu na bezpečnostné incidenty.

4.2 Školy so silným informatickým základom a doloženou bezpečnostnou zložkou

Do tejto skupiny patria školy, pri ktorých je verejne potvrdený informatický alebo príbuzný technologický študijný program a súčasne sa pri nich dajú z verejných zdrojov identifikovať konkrétne bezpečnostné predmety, zamerania alebo bezpečnostné tematické línie. V tejto fáze sem patria najmä Univerzita Komenského v Bratislave, Univerzita Pavla Jozefa Šafárika v Košiciach, Univerzita Konštantína Filozofa v Nitre, Univerzita sv. Cyrila a Metoda v Trnave, Paneurópska vysoká škola, Univerzita J. Selyeho a informatická línia Univerzity Mateja Bela v Banskej Bystrici. Pri všetkých štyroch školách ide o pracoviská, kde bezpečnosť nevystupuje ako jediný nosný názov programu, ale je verejne doložiteľná ako súčasť širšieho informatického základu.

Univerzita Komenského v Bratislave (FMFI UK) – kategória B / dôkaz S.

Na FMFI UK je verejne potvrdený bakalársky študijný program Informatika na oficiálnej stránke programu (https://fmph.uniba.sk/studium/programy/informatika/) a zároveň aj program Aplikovaná informatika v registri Portálu VŠ (https://www.portalvs.sk/sk/studijny-program/uk-aplikovana-informatika). Oficiálna stránka programu Informatika výslovne uvádza, že v treťom ročníku bakalárskeho štúdia sa ponúkajú základy zameraní vrátane informačnej bezpečnosti. Verejne dostupné sú aj materiály k predmetu Úvod do informačnej bezpečnosti (https://www.dcs.fmph.uniba.sk/studium/UvodDoInformacnejBezpecnosti/).

Univerzita Pavla Jozefa Šafárika v Košiciach (PriF UPJŠ) – kategória B / dôkaz S.

Na UPJŠ sú verejne potvrdené programy Aplikovaná informatika (https://studijne-programy.upjs.sk/program/AIb) a Informatika (https://studijne-programy.upjs.sk/program/Im). Pri programe Aplikovaná informatika sa verejne uvádza, že absolvent má vytvorené predpoklady pre nadväzujúce štúdium so špecializáciami vrátane bezpečnosti počítačových sietí. Pri programe Informatika sa verejne uvádza, že vo vyšších ročníkoch sa študenti môžu špecializovať aj v oblasti bezpečnosti počítačových systémov, a pri magisterskom programe Informatika sa medzi uplatneniami absolventov uvádzajú aj bezpečnostní a sieťoví špecialisti.

Verejne dostupná je aj predmetová stránka Počítačová sieť Internet (https://siete.ics.upjs.sk/), ktorá potvrdzuje sieťovo-orientovanú technickú bázu programu.

Univerzita Konštantína Filozofa v Nitre (FPVaI UKF) – kategória B / dôkaz S.

Portál VŠ eviduje študijný program Aplikovaná informatika na FPVaI UKF (https://www.portalvs.sk/sk/studijny-program/ukf-aplikovana-informatika,

https://www.portalvs.sk/sk/studijny-program/ukf-aplikovana-informatika0). Verejne dostupný je aj kurz Koncepty počítačovej bezpečnosti (KI/KPB/22) na univerzitnom e-learningovom portáli (https://edu.ukf.sk/course/info.php?id=1429). Na úrovni fakulty je verejne potvrdené, že FPVaI UKF zabezpečuje vzdelávanie a výskum v oblasti informatiky (https://www.ukf.sk/fakulty-a-sucasti/fakulta-prirodnych-vied-a-informatiky), čo podopierajú profily absolventov na https://aplikovanainformatika.sk/ a detailný obsah sylabov jednotlivých predmetov na https://aplikovanainformatika.sk/ai_zone.

Univerzita sv. Cyrila a Metoda v Trnave (FPV UCM) – kategória B / dôkaz M až S.

UCM má verejne potvrdený bakalársky program Aplikovaná informatika (https://www.ucm.sk/sk/studuj-ucm/bakalarske-magisterske-studium/studijne-programy/studijne-programy-podla-fakult/fakulty/fpv/aplikovana-informatika-bc.html) aj magisterský program Aplikovaná informatika (https://www.ucm.sk/sk/studuj-ucm/bakalarske-magisterske-studium/studijne-programy/studijne-programy-podla-fakult/fakulty/fpv/aplikovana-informatika-mgr.html).

Pre magisterský stupeň je verejne dostupný presný učebný plán v PDF (https://fpv.ucm.sk/files/sk/studuj-fpv/studijne-programy/aplikovana-informatika-mgr/ucebny-plan_apin_mgd19_2025_2026.pdf). Fakulta a pracovisko zároveň verejne dokumentujú výučbovo-výskumné zameranie na sieťovú bezpečnosť a IoT bezpečnosť prostredníctvom projektových stránok (https://upti.fpv.ucm.sk/kega2021/, https://upti.fpv.ucm.sk/kega2024/) a projektovej stránky FPV (https://fpv.ucm.sk/sk/veda-vyskum/vyskum-fakulte/projekty-fakulte/sietova-bezpecnost-podporou-vypoctovej-inteligencie-iot.html).

Univerzita J. Selyeho v Komárne (UJS) – kategória B / dôkaz M.

Na Univerzite J. Selyeho je verejne potvrdený študijný program Aplikovaná informatika na bakalárskom aj magisterskom stupni prostredníctvom záznamov v registri Portálu VŠ (https://www.portalvs.sk/sk/studijny-program/ujs-aplikovana-informatika1, https://www.portalvs.sk/sk/studijny-program/aplikovana-informatika8). Z verejne dostupných zdrojov tak vyplýva existencia relevantného informatického základu, ktorý je použiteľný aj pre ďalšiu bezpečnostnú profiláciu.

Hoci v otvorene dostupných zdrojoch nie je bezpečnostná línia rozpracovaná tak explicitne ako pri UK, UPJŠ, UKF alebo UCM, UJS predstavuje školu s potvrdeným informatickým profilom, ktorú možno metodicky zaradiť medzi pracoviská so silným IT základom a potenciálom pre rozvoj bezpečnostne relevantných kompetencií. Z tohto dôvodu je vhodné UJS zaradiť do kategórie B, podobne ako Paneurópsku vysokú školu, pri ktorej je taktiež dominantný všeobecný informatický základ a bezpečnostná zložka je vo verejných zdrojoch čitateľná skôr nepriamo.

Univerzita Mateja Bela v Banskej Bystrici (informatická línia) – kategória B / dôkaz M.

Popri bezpečnostno-politickej a strategickej línii na Fakulte politických vied a medzinárodných vzťahov má Univerzita Mateja Bela v Banskej Bystrici verejne potvrdený aj informatický základ. V registri Portálu VŠ sú evidované programy Aplikovaná informatika a Aplikovaná informatika a vývoj softvéru (https://www.portalvs.sk/sk/studijny-program/umb-aplikovana-informatika1, https://www.portalvs.sk/sk/studijny-program/umb-aplikovana-informatika-a-vyvoj-softveru, https://www.portalvs.sk/sk/studijny-program/umb-aplikovana-informatika-a-vyvoj-softveru1). Tieto programy potvrdzujú, že UMB nevystupuje iba ako škola širšieho bezpečnostného alebo strategického profilu, ale aj ako pracovisko s relevantnou informatickou líniou, ktorá môže vytvárať základ pre ďalšiu bezpečnostnú profiláciu absolventov. Bezpečnostná zložka tejto informatickej vetvy nie je vo verejných zdrojoch rozpracovaná tak explicitne ako pri najsilnejších školách kategórie B, no existencia informatických programov oprávňuje zaradiť UMB aj do tejto kategórie.

Paneurópska vysoká škola (Fakulta informatiky PEVŠ) – kategória B / dôkaz M.

Na Paneurópskej vysokej škole je verejne potvrdená Fakulta informatiky a na nej študijný program Aplikovaná informatika na bakalárskom aj magisterskom stupni (https://www.paneurouni.com/fakulta-informatiky/, https://www.portalvs.sk/sk/studijny-program/pevs-aplikovana-informatika0, https://www.portalvs.sk/sk/studijny-program/pevs-aplikovana-informatika). Oficiálna stránka magisterského štúdia uvádza orientáciu na Podnikovú informatiku alebo Počítačovú grafiku a multimédiá, čo potvrdzuje širší informatický profil programu (https://www.paneurouni.com/fakulta-informatiky/magisterske-studium/). PEVŠ predstavuje školu s potvrdeným informatickým základom použiteľným pre ďalšiu bezpečnostnú profiláciu, aj keď v otvorene dostupných zdrojoch zatiaľ nevyplýva rovnako silná a explicitná bezpečnostná predmetová línia ako pri školách uvedených vyššie v tejto podsekcii.

***

Z verejne dostupných zdrojov teda vyplýva, že UK, UPJŠ, UKF, UCM a PEVŠ nepredstavujú jadro technickej kyberprípravy v rovnakom zmysle ako STU, TUKE alebo technická línia UNIZA, ale vytvárajú relevantný informatický základ, v rámci ktorého je bezpečnostná zložka verejne doložiteľná na úrovni zamerania, programu alebo konkrétnych predmetov. Práve preto sú v tejto analýze zaradené do kategórie B.

4.3 Školy s bezpečnostno-manažérskym, rezortným alebo právno-forenzným profilom

Do tejto skupiny patria školy a pracoviská, pri ktorých zdroje potvrdzujú bezpečnostno-manažérsky, právno-regulačný, forenzný, obranný, kriticko-infraštruktúrny alebo informačno-systémový profil relevantný pre rozvoj širších kyberbezpečnostných kapacít.

Žilinská univerzita v Žiline – Fakulta bezpečnostného inžinierstva (FBI UNIZA)

Na FBI UNIZA sú na oficiálnej stránke fakulty verejne uvedené študijné programy Bezpečnostný manažment, Krízový manažment a Záchranné služby (https://fbi.uniza.sk/stranka/studijne-programy-fbi). Verejne dostupný opis študijného programu Bezpečnostný manažment pre bakalársky stupeň uvádza, že profil absolventa je zameraný na ochranu osôb, majetku a informácií (https://www.uniza.sk/images/pdf/vnutorny-system-kvality/opis-SP/2025/21460_OpisStudijnehoProgramu.pdf). Verejne dostupný opis inžinierskeho stupňa zároveň uvádza možnosť profilácie v oblastiach manažérske systémy vybraných oblastí bezpečnosti, fyzická a objektová bezpečnosť a informačná bezpečnosť (https://www.uniza.sk/doc1/OPIS-SPRAVA/2024/21452_OpisStudijnehoProgramu.pdf).
Stránka so schémami predmetov fakulty navyše potvrdzuje, že FBI pracuje so špecializačnými a predmetovými líniami v programe Bezpečnostný manažment (https://fbi.uniza.sk/stranka/schemy-predmetov). Z verejných zdrojov preto vyplýva, že FBI UNIZA predstavuje dôležitú bezpečnostno-manažérsku a kriticko-infraštruktúrnu vetvu, ktorá dopĺňa technickú bezpečnostnú líniu FRI.

Vysoká škola bezpečnostného manažérstva v Košiciach (VŠBM)

Portál VŠ pri VŠBM verejne uvádza študijný program Riadenie bezpečnostných systémov a výslovne potvrdzuje, že škola ho organizuje v I., II. aj III. stupni vysokoškolského štúdia (https://www.portalvs.sk/sk/studijny-program/riadenie-bezpecnostnych-systemov). Na tom istom profile Portálu VŠ je zároveň uvedené, že študent si v 2. a 3. ročníku volí doplnkovú špecializovanú profiláciu, medzi ktorými je aj kybernetická bezpečnosť. Oficiálna stránka školy s informačnými listami a odporúčanými plánmi (https://www.vsbm.sk/inf_listy.html) a osobitná špecifikácia špecializovaného štúdia Kybernetická bezpečnosť (https://www.vsbm.sk/data/studium/specializacie/KB_specializacia.pdf) túto líniu ďalej rozvíjajú. Z odporúčaného bakalárskeho plánu je navyše verejne viditeľné, že súčasťou kurikula sú predmety ako Teória bezpečnosti, Informatika, Teória rizík, Integrovaný záchranný systém a Ochrana kritickej infraštruktúry (https://www.vsbm.sk/data/studium/Odporucany_plan_Bc_RBS_DF.pdf).

Akadémia Policajného zboru v Bratislave (APZ)

APZ má na oficiálnom webe samostatne zverejnené opisy študijných programov Bezpečnostnoprávne služby vo verejnej správe (https://akademiapz.sk/sk/opisy-bsvs) a Bezpečnostnoprávna ochrana osôb a majetku (https://www.akademiapz.sk/sk/opisy-boom). Portál VŠ pri programe Bezpečnostnoprávne služby vo verejnej správe uvádza uplatnenie absolventov v oblasti všeobecnej vnútornej správy, požiarnej ochrany, civilnej ochrany, obrany a krízového manažmentu (https://www.portalvs.sk/sk/studijny-program/bezpecnostnopravne-sluzby-vo-verejnej-sprave) a pri programe Bezpečnostnoprávna ochrana osôb a majetku uvádza uplatnenie v štátnych bezpečnostných službách a organizáciách realizujúcich špecializované bezpečnostné činnosti (https://www.portalvs.sk/sk/studijny-program/bezpecnostnopravna-

ochrana-osob-a-majetku). Akadémia zároveň na oficiálnom webe zverejňuje študijné plány programov BSVS a BOOM (https://www.akademiapz.sk/sk/studium/bakalarske-studium/denne) a má samostatnú Katedru informatiky a manažmentu (https://akademiapz.sk/sk/node/50). APZ má dominantne bezpečnostnoprávny, vyšetrovací a verejnosprávny profil s informaticko-manažérskym zázemím, nie však profil jadrovej technickej kyberprípravy.

Akadémia ozbrojených síl gen. M. R. Štefánika (AOS)

Portál VŠ pri AOS verejne eviduje študijný program Vojenské spojovacie a informačné systémy a uvádza, že absolvent získa vedomosti, schopnosti a zručnosti v oblasti teoretických základov, prevádzky a riadenia vojenských spojovacích a informačných systémov (https://www.portalvs.sk/sk/studijny-program/vojenske-spojovacie-a-informacne-systemy2). V oficiálnych dokumentoch AOS je rovnaký študijný program verejne dostupný aj v PDF podkladoch k štúdiu (https://aos.sk/www/data/uploads/files/studijne_programy/1stup-vsis.pdf, https://aos.sk/www/data/uploads/files/studijne_programy/3stup-vsis-e-sk.pdf).

Katedra informatiky AOS zároveň na oficiálnej stránke uvádza, že zabezpečuje prípravu špecialistov pre Ozbrojené sily SR v oblasti vojenských spojovacích a informačných systémov a odborné kurzy v oblasti IT, Cisco NetACAD a Palo Alto Networks Cybersecurity Academy (https://kti.aos.sk/page.php?contID=94&page=321, https://aos.sk/clanok/katedra-informatiky-cisco-netacad, https://aos.sk/clanok/katedra-informatiky-palo-alto-networks-cybersecurity-academy). AOS má tak jasne identifikovateľný obranný a rezortný informačno-bezpečnostný profil.

Ekonomická univerzita v Bratislave (Fakulta hospodárskej informatiky EUBA)

Na Portáli VŠ je pri Fakulte hospodárskej informatiky verejne potvrdený program Hospodárska informatika (https://www.portalvs.sk/sk/studijny-program/hospodarska-informatika3) a samostatne je verejne dostupný predmet Úvod do informačnej bezpečnosti (https://programy.euba.sk/predmet/iia21200/). V informačnom liste tohto predmetu sa výslovne uvádza, že študent má pochopiť základné pojmy kybernetickej bezpečnosti, diskutovať o informačnej a aplikačnej bezpečnosti, šifrovaní, kryptografii a útokoch na informačné aktíva a počítačové siete, a poznať bezpečnostné štandardy informačných systémov a legislatívu vrátane zákona o kybernetickej bezpečnosti. EUBA je relevantná najmä pre informačno-systémový, podnikovo-procesný a governance profil bezpečnosti, nie ako jadro technickej kyberprípravy.

Slovenská poľnohospodárska univerzita v Nitre (Technická fakulta SPU)

SPU pokrýva technicko-bezpečnostný a priemyselno-bezpečnostný profil na Technickej fakulte. Oficiálna stránka Technickej fakulty uvádza medzi bakalárskymi programami program Kvalita a bezpečnosť vo výrobných technológiách (https://tf.uniag.sk/sk/bakalarske-studium). Portál VŠ pri tomto programe verejne uvádza, že absolventi dokážu riešiť problémy spojené so zavádzaním a prevádzkou výrobno-technologických systémov a majú znalosti o kontrole výrobných procesov

a ich riadení (https://www.portalvs.sk/sk/studijny-program/spu-kvalita-a-bezpecnost-vo-vyrobnych-technologiach-2014). Na oficiálnom webe Technickej fakulty je zároveň zverejnená samostatná komisia pre súbeh študijného programu Kvalita a bezpečnosť vo výrobných technológiách (https://tf.uniag.sk/sk/komisia-pre-subeh-studijnych-programov-kvalita-a-bezpecnost-vo-vyrobnych-technologiach-a-vyrobne-technologie/) a študijná príručka programu (https://cdn.uniag.sk/contao/files/tf/documents/Studijna%20prirucka/2023_24/I_stupen/%C5%A0tudijn%C3%BD%20program%20KBI.pdf). Z verejných zdrojov preto vyplýva, že SPU je pre túto analýzu relevantná ako pracovisko s väzbou na bezpečnosť technických systémov, spoľahlivosť výrobných procesov a bezpečnú prevádzku priemyselných technológií.

Univerzita Mateja Bela v Banskej Bystrici (FPVaMV UMB)

Na Fakulte politických vied a medzinárodných vzťahov UMB je verejne potvrdený študijný program Bezpečnostné štúdiá na Portáli VŠ (https://www.portalvs.sk/sk/studijny-program/umb-bezpecnostne-studia1) a samostatne je verejne dostupná Katedra bezpečnostných štúdií (https://fpvmv.umb.sk/14833/katedra-bezpecnostnych-studii). Na stránke katedry sa výslovne uvádza, že jej cieľom je poskytovať poznatky o bezpečnostných teóriách, štúdiách a koncepciách, pričom hlavný dôraz je položený na bezpečnostnú politiku NATO, EÚ a SR. UMB je tak relevantná najmä pre strategický, geopolitický a bezpečnostno-politický rozmer prípravy absolventov; jej informatická línia na iných pracoviskách bude v dokumente posudzovaná samostatne.

***

Okrem škôl s jadrovou technickou kyberprípravou existuje na Slovensku aj výrazná skupina inštitúcií, ktoré rozvíjajú širšie bezpečnostné kapacity: bezpečnostný manažment, kritickú infraštruktúru, informačno-systémové governance, právno-forenzné a policajné línie, obranné a vojenské informačné systémy či strategické bezpečnostné štúdiá. Táto vrstva vysokého školstva je pre celkové budovanie kyberbezpečnostných kapacít dôležitá, aj keď jej ťažisko neleží primárne v technickom cyber engineeringu.

4.4 Školy s nepriamym digitálnym alebo pedagogickým presahom

Do tejto skupiny patria školy a pracoviská, pri ktorých verejne dostupné zdroje potvrdzujú digitálny, informatický, AI alebo pedagogický presah, ale nie jadrový profil technickej kyberprípravy ani bezpečnostno-manažérsku líniu v zmysle predchádzajúcich podsekcií. V tejto fáze ide najmä o programy učiteľstva informatiky, učiteľstva matematiky a informatiky a o umelecké programy prepájajúce tvorbu s digitálnymi technológiami.

Z verejne dostupných zdrojov vyplýva, že Katolícka univerzita v Ružomberku (Pedagogická fakulta) a Trnavská univerzita v Trnave (Pedagogická fakulta) reprezentujú najmä pedagogicko-didaktické presahy informatiky, zatiaľ čo Akadémia umení v Banskej Bystrici a Vysoká škola výtvarných umení v Bratislave predstavujú digitálne a AI presahy v umeleckých odboroch. Tieto školy sú pre celkový obraz digitálnych kompetencií vo vysokoškolskom prostredí relevantné, ale z hľadiska cieľa tejto analýzy ich nemožno zaradiť medzi jadro technickej kyberprípravy ani

medzi školy s dominantným bezpečnostno-manažérskym profilom. (https://www.portalvs.sk/sk/studijny-program/ucitelstvo-informatiky0, https://www.portalvs.sk/sk/studijny-program/ucitelstvo-pre-zakladne-skoly-pre-vzdelavaciu-oblast-matematika-a-informatika, https://www.portalvs.sk/sk/studijny-program/umenie-a-umela-inteligencia3, https://www.portalvs.sk/sk/studijny-program/digitalne-umenia)

4.5 Predbežné syntetické zistenia zo sumarizačného prehľadu

Zo sumarizačného prehľadu vyplýva, že na Slovensku možno na základe verejne dostupných zdrojov rozlíšiť tri hlavné vrstvy vysokoškolských kapacít relevantných pre rozvoj kyberbezpečnosti:

- jadro priamej technickej kyberprípravy,
- skupinu škôl so silným informatickým základom a doloženou bezpečnostnou zložkou
- skupinu škôl, ktoré rozvíjajú širší bezpečnostno-manažérsky, právno-forenzný, rezortný alebo kriticko-infraštruktúrny profil

Tab 1. Úplný zoznam hodnotených inštitúcií s analytickým zaradením

	Inštitúcia	Kat.	Stručné zaradenie	Programy/pracoviská	Verejné zdroje (raw URL)
1	Akadémia ozbrojených síl gen. M. R. Štefánika	C	Relevantná najmä pre obranný a rezortný informačno-bezpečnostný profil, nie ako jadro civilnej technickej kyberprípravy.	Vojenské spojovacie a informačné systémy; Katedra informatiky	https://www.portalvs.sk/sk/studijny-program/vojenske-spojovacie-a-informacne-systemy2 ; https://aos.sk/www/data/uploads/files/studijne_programy/1stup-vsis.pdf ; https://kti.aos.sk/page.php?contID=94&page=321 ; https://aos.sk/clanok/katedra-informatiky-cisco-netacad ; https://aos.sk/clanok/katedra-informatiky-palo-alto-networks-cybersecurity-academy
2	Akadémia Policajného zboru v Bratislave	C	Relevantná najmä pre bezpečnostnoprávny, vyšetrovací a policajný profil s informaticko-manažérskym zázemím.	Bezpečnostnoprávne služby vo verejnej správe; Bezpečnostnoprávna ochrana osôb a majetku; Katedra informatiky a manažmentu	https://akademiapz.sk/sk/opisy-bsvs ; https://www.akademiapz.sk/sk/opisy-boom ; https://www.portalvs.sk/sk/studijny-program/bezpecnostnopravne-sluzby-vo-verejnej-sprave2 ; https://www.portalvs.sk/sk/studijny-program/bezpecnostnopravna-ochrana-osob-a-majetku ; https://www.akademiapz.sk/sk/pracoviska/katedry/KIM
3	Akadémia umení v Banskej Bystrici	D	Relevantná cez digitálny a AI presah v umeleckom prostredí, nie ako kyberbezpečnostný profil.	Umenie a umelá inteligencia	https://www.portalvs.sk/sk/studijny-program/umenie-a-umela-inteligencia3 ; https://www.portalvs.sk/sk/vysoka-skola/akademia-umeni-v-banskej-bystrici
4	Bratislavská medzinárodná škola liberálnych štúdií	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://www.bisla.sk/
5	Ekonomická univerzita v Bratislave	C	Relevantná najmä pre informačné systémy, governance, compliance a podnikovo-procesný bezpečnostný profil.	Fakulta hospodárskej informatiky; Hospodárska informatika; Úvod do informačnej bezpečnosti	https://www.portalvs.sk/sk/fakulta/fakulta-hospodarskej-informatiky ; https://www.portalvs.sk/sk/studijny-program/hospodarska-informatika3 ; https://programy.euba.sk/predmet/iia21200/

6	Hudobná a umelecká akadémia Jána Albrechta	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://www.huaja.org/
7	Katolícka univerzita v Ružomberku	D	Relevantná najmä cez pedagogický presah informatiky, nie ako technický alebo bezpečnostný profil.	Učiteľstvo informatiky	https://www.portalvs.sk/sk/studijny-program/ucitelstvo-informatiky0
8	Paneurópska vysoká škola	B	Verejne je potvrdený informatický profil a použiteľný všeobecný IT základ; bezpečnostná zložka je vo verejných zdrojoch čitateľná skôr nepriamo.	Fakulta informatiky; Aplikovaná informatika	https://www.paneurouni.com/fakulta-informatiky/ ; https://www.portalvs.sk/sk/studijny-program/pevs-aplikovana-informatika0 ; https://www.portalvs.sk/sk/studijny-program/pevs-aplikovana-informatika ; https://www.paneurouni.com/fakulta-informatiky/magisterske-studium/
9	Prešovská univerzita v Prešove	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://www.unipo.sk/
10	Slovenská poľnohospodárska univerzita v Nitre	C	Relevantná nie ako všeobecný IT základ, ale cez technicko-bezpečnostný a priemyselno-bezpečnostný profil.	Technická fakulta; Kvalita a bezpečnosť vo výrobných technológiách	https://tf.uniag.sk/sk/bakalarske-studium ; https://www.portalvs.sk/sk/studijny-program/spu-kvalita-a-bezpecnost-vo-vyrobnych-technologiach-2014 ; https://tf.uniag.sk/sk/komisia-pre-subeh-studijnych-programov-kvalita-a-bezpecnost-vo-vyrobnych-technologiach-a-vyrobne-technologie/ ; https://cdn.uniag.sk/contao/files/tf/documents/Studijna%20prirucka/2023_24/I_stupen/%C5%A0tudijn%C3%BD%20program%20KBI.pdf
11	Slovenská technická univerzita v Bratislave	A	Verejne je doložený explicitný program informačnej bezpečnosti a širšia technická bezpečnostná línia v informatike.	FIIT STU – Informačná bezpečnosť; Informatika; FEI STU – Aplikovaná informatika	https://www.portalvs.sk/sk/studijny-program/stu-informacna-bezpecnost0 ; https://www.fiit.stuba.sk/studijne-programy/inzinierske/informacna-bezpecnost.html?page_id=4926 ; https://www.portalvs.sk/sk/studijny-program/stu-informatika ; https://www.portalvs.sk/sk/studijny-program/stu-aplikovana-informatika2 ; https://www.fiit.stuba.sk/buxus/docs/Studium/katalog-predmetov_2025-26.pdf
12	Slovenská zdravotnícka univerzita v Bratislave	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://www.szu.sk/
13	Technická univerzita v Košiciach	A	Verejne je potvrdený samostatný program Kyberbezpečnosť a otvorene publikované študijné plány FEI.	FEI TUKE – Kyberbezpečnosť (Bc., Ing.)	https://www.portalvs.sk/sk/studijny-program/kyberbezpecnost ; https://www.portalvs.sk/sk/studijny-program/kyberbezpecnost1 ; https://fei.tuke.sk/sk/studijne-programy ; https://api.prod.tuke.sk/smb/medias/2025/03/PS_2024_bc_kyberbezpecnost.pdf ; https://api.prod.tuke.sk/smb/medias/2025/03/PS_2023_ing_Kyberbezpecnost.pdf
14	Technická univerzita vo Zvolene	E	V tomto screeningu nebol verejne potvrdený	—	https://www.tuzvo.sk/

			relevantný informatický alebo bezpečnostný profil.		
15	Trenčianska univerzita Alexandra Dubčeka v Trenčíne	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://tnuni.sk/
16	Trnavská univerzita v Trnave	D	Relevantná najmä cez pedagogický presah matematiky a informatiky, nie ako technický alebo bezpečnostný profil.	Učiteľstvo pre základné školy pre vzdelávaciu oblasť matematika a informatika; Katedra matematiky a informatiky	https://www.portalvs.sk/sk/studijny-program/ucitelstvo-pre-zakladne-skoly-pre-vzdelavaciu-oblast-matematika-a-informatika ; https://pdf.truni.sk/studijne-programy ; https://pdf.truni.sk/katedry/kmi ; https://pdfweb.truni.sk/katedry/kmi/katedra
17	Univerzita J. Selyeho	B	Verejne je potvrdený informatický program a všeobecný IT základ; bezpečnostná zložka je vo verejných zdrojoch doložená slabšie.	Aplikovaná informatika (Bc., Mgr.)	https://www.portalvs.sk/sk/studijny-program/ujs-aplikovana-informatika1 ; https://www.portalvs.sk/sk/studijny-program/aplikovana-informatika8
18	Univerzita Komenského v Bratislave	B	Verejne je potvrdený silný informatický základ a priamo pomenovaná bezpečnostná vetva v rámci FMFI UK.	Informatika; Aplikovaná informatika; Úvod do informačnej bezpečnosti	https://fmph.uniba.sk/studium/programy/informatika/ ; https://www.portalvs.sk/sk/studijny-program/uk-informatika ; https://www.portalvs.sk/sk/studijny-program/uk-aplikovana-informatika ; https://www.dcs.fmph.uniba.sk/studium/UvodDoInformacnejBezpecnosti/
19	Univerzita Konštantína Filozofa v Nitre	B	Verejne je potvrdený informatický program a konkrétny bezpečnostný predmet.	Aplikovaná informatika; Koncepty počítačovej bezpečnosti	https://www.portalvs.sk/sk/studijny-program/ukf-aplikovana-informatika0 ; https://www.portalvs.sk/sk/studijny-program/ukf-aplikovana-informatika1 ; https://edu.ukf.sk/course/info.php?id=1429&lang=cs ; https://edu.ukf.sk/course/index.php?categoryid=180
20	Univerzita Mateja Bela v Banskej Bystrici	B, C	Kombinovaný profil: verejne sú potvrdené informatické programy a zároveň aj širší strategicko-bezpečnostný presah.	Aplikovaná informatika; Aplikovaná informatika a vývoj softvéru; Bezpečnostné štúdiá; Katedra bezpečnostných štúdií	https://www.portalvs.sk/sk/studijny-program/umb-aplikovana-informatika1 ; https://www.portalvs.sk/sk/studijny-program/umb-aplikovana-informatika-a-vyvoj-softveru ; https://www.portalvs.sk/sk/studijny-program/umb-aplikovana-informatika-a-vyvoj-softveru1 ; https://www.portalvs.sk/sk/studijny-program/umb-bezpecnostne-studia1 ; https://fpvmv.umb.sk/14833/katedra-bezpecnostnych-studii
21	Univerzita Pavla Jozefa Šafárika v Košiciach	B	Verejne je potvrdený informatický základ a špecializačný presah k bezpečnosti počítačových sietí; ďalší právno-regulačný presah sa rieši osobitne.	Aplikovaná informatika; Informatika; Počítačová sieť Internet	https://studijne-programy.upjs.sk/program/AIb ; https://studijne-programy.upjs.sk/program/Im ; https://siete.ics.upjs.sk/
22	Univerzita sv. Cyrila a Metoda v Trnave	B	Verejne je potvrdený informatický program a bezpečnostno-sieťový presah v študijnom pláne a na pracovisku.	Aplikovaná informatika (Bc., Mgr.)	https://www.portalvs.sk/sk/studijny-program/ucm-aplikovana-informatika7 ; https://www.portalvs.sk/sk/studijny-program/ucm-aplikovana-informatika8 ; https://fpv.ucm.sk/sk/studuj-fpv/bakalarske-studium/aplikovana-informatika/ ;

					https://fpv.ucm.sk/sk/studuj-fpv/magisterske-inzinierske-studium/aplikovana-informatika/ ; https://upti.fpv.ucm.sk/doc/IL/2025-2026-APIN-MgD19%20-%20apin.html ; https://upti.fpv.ucm.sk/kega2021/ ; https://upti.fpv.ucm.sk/kega2024/index.html
23	Univerzita veterinárskeho lekárstva a farmácie v Košiciach	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://www.uvlf.sk/
24	Vysoká škola bezpečnostného manažérstva v Košiciach	C	Relevantná najmä pre bezpečnostný manažment, ochranu kritickej infraštruktúry a širší bezpečnostný profil s kybernetickou špecializáciou.	Riadenie bezpečnostných systémov; špecializácia Kybernetická bezpečnosť	https://www.portalvs.sk/sk/studijny-program/riadenie-bezpecnostnych-systemov ; https://www.vsbm.sk/inf_listy.html ; https://www.vsbm.sk/data/studium/Odporucany_plan_Bc_RBS_DF.pdf ; https://www.vsbm.sk/data/studium/specializacie/KB_specializacia.pdf ; https://www.vsbm.sk/KBV.html
25	Vysoká škola Danubius	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://www.vssladkovicovo.sk/
26	Vysoká škola DTI	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://www.dti.sk/
27	Vysoká škola ekonómie a manažmentu v Bratislave	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://www.vsemvs.sk/
28	Vysoká škola manažmentu	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://www.vsm.sk/
29	Vysoká škola múzických umení v Bratislave	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://www.vsmu.sk/
30	Vysoká škola technická a ekonomická v Prešove	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://www.ismpo.sk/
31	Vysoká škola výtvarných umení v Bratislave	D	Relevantná cez digitálny technologický presah v umeleckom a dizajnérskom kontexte, nie ako kyberbezpečnostný profil.	Digitálne umenia	https://www.portalvs.sk/sk/studijny-program/digitalne-umenia ; https://www.portalvs.sk/sk/vysoka-skola/vysoka-skola-vytvarnych-umeni-v-bratislave
32	Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.	E	V tomto screeningu nebol verejne potvrdený relevantný informatický alebo bezpečnostný profil.	—	https://www.vssvalzbety.sk/

33	Žilinská univerzita v Žiline	A, C	Verejne je doložená technická bezpečnostná línia na FRI, doplnená širším bezpečnostno-manažérskym profilom na FBI.	Informačné a sieťové technológie; Bezpečnosť informačných systémov; Riešenie bezpečnostných incidentov; Bezpečnostný manažment	https://www.portalvs.sk/sk/studijny-program/informacne-a-sietove-technologie ; https://www.kis.fri.uniza.sk/katedra/ ; https://www.kis.fri.uniza.sk/bis-bezpecnost-informacnych-systemov/ ; https://www.kis.fri.uniza.sk/rbi-riesenie-bezpecnostnych-incidentov/ ; https://fbi.uniza.sk/stranka/studijne-programy-fbi ; https://www.uniza.sk/images/pdf/vnutorny-system-kvality/opis-SP/2025/21460_OpisStudijnehoProgramu.pdf

5 Výsledky

5.1 Jadro priamej technickej kyberprípravy

Z verejne dostupných zdrojov vyplýva, že jadro priamej technickej kyberprípravy na Slovensku je koncentrované do obmedzeného počtu univerzitných uzlov. V tejto skupine sa opakovane potvrdzujú najmä pracoviská a programy na Slovenskej technickej univerzite v Bratislave, Technickej univerzite v Košiciach a Žilinskej univerzite v Žiline. Spoločným znakom týchto uzlov je, že bezpečnostná línia sa pri nich neprejavuje iba na úrovni názvu programu alebo všeobecného opisu, ale aj prostredníctvom verejne čitateľných predmetov, študijných plánov, profilov absolventa alebo tematického zamerania pracovísk.

Tieto uzly zároveň predstavujú najsilnejšie verejne doložené prostredie pre prípravu absolventov v oblastiach, ako sú informačná bezpečnosť, sieťová bezpečnosť, ochrana systémov, riešenie bezpečnostných incidentov, bezpečnostné riadenie a ďalšie súvisiace technické alebo technicko-organizačné disciplíny. Neznamená to, že ide o jediné školy, ktoré sa bezpečnostným témam venujú, ale že práve pri nich je bezpečnostná profilácia verejne najzreteľnejšia a metodicky najlepšie obhájiteľná.

Zároveň je potrebné zdôrazniť, že aj v rámci tejto skupiny existujú rozdiely v profile. Niektoré uzly pôsobia viac ako explicitné technické programy kybernetickej alebo informačnej bezpečnosti, iné ako kombinácia technickej, sieťovej a manažérskej bezpečnostnej línie rozloženej medzi viaceré pracoviská alebo programy. Pre účely tohto materiálu je však rozhodujúce najmä to, že ide o najlepšie verejne doložené jadro technickej kyberprípravy v slovenskom vysokoškolskom prostredí.

5.2 Školy so silným IT základom a bezpečnostným presahom

Druhú skupinu tvoria školy, pri ktorých je verejne potvrdený informatický alebo príbuzný technologický základ a zároveň sa pri nich dajú identifikovať aj bezpečnostne relevantné predmety, tematické bloky alebo čiastkové špecializácie. V tejto skupine bezpečnosť spravidla nevystupuje ako dominantné jadro celej študijnej ponuky, ale ako súčasť širšieho informatického prostredia.

Z analytického pohľadu ide o dôležitú skupinu, pretože práve tieto školy môžu predstavovať významný zdroj budúceho kybertalentu, najmä ak by došlo k ďalšiemu rozšíreniu špecializovaných predmetov, laboratórnej výučby, spolupráce s praxou alebo cielenej profilácie na konkrétne bezpečnostné roly. Verejne dostupné zdroje pri týchto školách spravidla potvrdzujú existenciu kvalitného IT základu a aspoň čiastočne aj väzbu na informačnú alebo sieťovú bezpečnosť, no menej často už dokladajú plne vybudovanú a systematicky komunikovanú bezpečnostnú líniu porovnateľnú s jadrovými technickými uzlami.

Pre potreby tohto dokumentu je preto vhodné tieto školy interpretovať nie ako náhradu jadra technickej kyberprípravy, ale ako dôležitú druhú vrstvu vysokoškolského ekosystému. Ich význam spočíva najmä v tom, že môžu vytvárať regionálne a personálne zázemie pre ďalší rozvoj

kyberbezpečnostných kapacít, a to aj v prípadoch, keď ich verejne doložený bezpečnostný profil ostáva zatiaľ skôr čiastkový alebo rozptýlený.

5.3 Širší bezpečnostný, rezortný a manažérsky profil

Popri technickom jadre a školách so silným IT základom existuje aj samostatná skupina inštitúcií, ktoré rozvíjajú širší bezpečnostný profil relevantný pre štát, verejnú správu, obranu, reguláciu, bezpečnostné riadenie, ochranu kritickej infraštruktúry alebo vyšetrovanie. Pri týchto školách sa verejne potvrdzuje najmä bezpečnostno-manažérska, právna, rezortná, forenzná alebo organizačná línia.

Táto skupina je pre celkový obraz dôležitá, pretože kyberbezpečnostné kapacity nemožno redukovať iba na technické roly. Súčasná regulačná a praktická realita zahŕňa aj riadenie rizík, bezpečnostné procesy, audit, compliance, kontinuitu činností, ochranu informačných aktív, bezpečnostnú dokumentáciu, rezortné informačné systémy či vyšetrovanie incidentov a deliktov. Práve v týchto oblastiach predstavujú školy širšieho bezpečnostného profilu významnú súčasť bezpečnostného ekosystému.

Zároveň však platí, že tento profil nemožno automaticky zamieňať s jadrovou technickou kyberprípravou. Skutočnosť, že škola rozvíja bezpečnostný manažment, rezortnú bezpečnosť alebo právno-regulačné kompetencie, ešte sama osebe neznamená, že disponuje rovnako silnou technickou výučbou v oblastiach, ako sú ochrana sietí, systémov, aplikácií alebo praktické riešenie incidentov. Pre potreby tohto materiálu je preto dôležité tieto línie uznať ako relevantné, ale zároveň ich interpretačne odlišovať od technického jadra.

5.4 Hlavný obraz slovenského prostredia

Z celého screeningu vyplýva, že slovenské vysoké školstvo nevytvára jednotný a rovnomerne rozložený model prípravy pre kyberbezpečnosť, ale skôr viacvrstvový systém. Jeho prvú vrstvu tvorí úzke jadro pracovísk s verejne doloženou priamou technickou kyberprípravou. Druhú vrstvu predstavujú školy so silným informatickým základom, pri ktorých je bezpečnostný presah verejne čitateľný, ale spravidla nie tak centralizovaný alebo rozvinutý. Tretiu vrstvu tvoria školy so širším bezpečnostným, rezortným alebo manažérskym profilom.

Dôležitým zistením je aj to, že medzi školami existujú výrazné rozdiely v miere verejnej čitateľnosti ich kurikula. V niektorých prípadoch sú dostupné študijné plány, predmetové mapy a informačné listy, v iných prípadoch skôr iba všeobecné opisy programov alebo profilov absolventa. Z tohto dôvodu treba výsledky interpretovať ako obraz verejne doložiteľných predpokladov, nie ako úplné hodnotenie reálnej úrovne výučby, laboratórnych kapacít alebo uplatnenia absolventov.

Z pohľadu hlavnej výskumnej otázky teda screening ukazuje, že Slovenská republika má identifikovateľné jadro technickej kyberprípravy, širší okruh informatických pracovísk použiteľných pre ďalšiu profiláciu a samostatnú bezpečnostno-rezortnú vetvu. Zároveň však platí, že tieto tri vrstvy nemožno analyticky zlievať do jednej kategórie, pretože pripravujú odlišné typy absolventov a pokrývajú odlišné časti bezpečnostného ekosystému.

6 Posúdenie voči potrebám praxe a rámcom NBÚ, ECSF a NIS2

6.1 Vysoký súlad

Z porovnania verejne dostupných študijných programov, predmetových skladieb a profilov pracovísk vyplýva, že najsilnejší súlad s potrebami praxe a s rámcami NBÚ, ECSF a NIS2 sa koncentruje v tej časti vysokoškolského prostredia, kde je verejne doložená priama technická alebo technicko-organizačná bezpečnostná príprava. Ide najmä o uzly, pri ktorých sa bezpečnostná línia neprejavuje iba na úrovni deklarácie, ale aj prostredníctvom konkrétnych predmetov, študijných plánov alebo tematicky jasne profilovaných pracovísk.

Práve v tejto skupine možno najzreteľnejšie identifikovať pokrytie oblastí, ktoré sú relevantné pre súčasnú prax: bezpečnosť sietí a systémov, ochranu informačných aktív, riešenie bezpečnostných incidentov, riadenie bezpečnosti, kontinuitu činností, auditovateľné procesy a základné prepojenie technických a organizačných opatrení. Z pohľadu rámcov NBÚ a ECSF ide o tú časť akademického prostredia, kde sa dajú verejne najlepšie doložiť predpoklady pre prípravu absolventov využiteľných v technických, analytických a čiastočne aj riadiacich bezpečnostných roliach.

V kontexte NIS2 je dôležité aj to, že najsilnejšie profilované uzly spravidla nepokrývajú iba úzko technické témy, ale aspoň v určitej miere aj širšie oblasti riadenia kybernetických rizík, bezpečnostných procesov a organizačných opatrení. To zvyšuje ich relevanciu nielen pre technické pracovné pozície, ale aj pre prostredie organizácií, ktoré musia kombinovať technickú bezpečnosť s governance, dokumentáciou a zodpovednosťou manažmentu.

6.2 Čiastkový súlad

Druhú skupinu predstavujú školy a programy, pri ktorých je z verejných zdrojov zrejmý kvalitný informatický alebo bezpečnostno-manažérsky základ, no ich súlad s potrebami praxe a s rámcami NBÚ, ECSF a NIS2 ostáva skôr čiastkový alebo nerovnomerný. V jednej časti tejto skupiny ide o informatické programy, kde je bezpečnostný presah prítomný, ale nie je rozvinutý do podoby systematickej a jasne komunikovanej kyberbezpečnostnej línie. V druhej časti ide o školy s bezpečnostným, rezortným alebo manažérskym profilom, kde je bezpečnostná relevancia zrejmá, no technická vrstva ostáva slabšia alebo menej verejne čitateľná.

Z pohľadu potrieb praxe to znamená, že tieto školy môžu pripravovať absolventov využiteľných v širšom bezpečnostnom alebo IT prostredí, no menej presvedčivo sa pri nich dá z verejných zdrojov doložiť plné pokrytie technických rolí alebo vyvážené spojenie technickej, procesnej a regulačnej roviny. Pri informatických programoch je častým javom to, že poskytujú dobrý základ pre ďalšiu bezpečnostnú profiláciu, ale nie vždy už samy osebe predstavujú dostatočne vystavaný program pre priame pokrytie potrieb kybernetickej praxe. Pri manažérskych a rezortných programoch je zasa typické, že lepšie pokrývajú riadenie, organizáciu, reguláciu alebo bezpečnostné procesy než hlbšiu technickú prípravu.

Pre účely tohto dokumentu je preto vhodné túto skupinu chápať ako dôležitú, ale nie plne ekvivalentnú jadru technickej kyberprípravy. Jej význam spočíva skôr v tom, že vytvára širší

personálny a inštitucionálny základ pre bezpečnostný ekosystém a pri vhodnom doplnení môže posilniť niektoré konkrétne roly alebo doménové oblasti, nie však automaticky nahradiť technické jadro tam, kde je potrebná systematická príprava špecialistov.

6.3 Hlavné biele a šedé miesta

Zo screeningu vyplýva, že najvýraznejším bielym miestom slovenského vysokoškolského prostredia je obmedzený počet pracovísk, pri ktorých možno z verejne dostupných zdrojov doložiť súvislú a systematickú prípravu pokrývajúcu širší cyklus kybernetickej bezpečnosti. Technické jadro existuje, ale je koncentrované do relatívne úzkeho okruhu uzlov. Mimo neho sa bezpečnostná príprava často objavuje len ako čiastkový prvok širšieho informatického alebo bezpečnostného programu, nie ako ucelene vystavaná a jasne komunikovaná profilácia.

Za ďalšie biele miesto možno považovať slabšie verejne doložené pokrytie niektorých prakticky orientovaných bezpečnostných rolí mimo jadrových technických uzlov. Ide najmä o tie oblasti, ktoré si v praxi vyžadujú kombináciu technických, analytických a procesných kompetencií, napríklad pri bezpečnostnom monitoringu, riešení incidentov, cloudovej bezpečnosti, digitálnej forenzike alebo bezpečnostnej architektúre. Neznamená to, že sa takéto témy na slovenských vysokých školách vôbec nevyskytujú, ale že ich systematická a verejne čitateľná prítomnosť je mimo najsilnejších uzlov spravidla slabšia alebo menej jednoznačne doložená.

Za šedé miesta možno považovať najmä tie situácie, keď je bezpečnostný profil školy alebo programu naznačený, ale nie je verejne dostatočne čitateľný na úrovni konkrétnych predmetov, modulov, študijných výstupov alebo praktickej výučby. V takýchto prípadoch nemožno spoľahlivo rozlíšiť, či ide o skutočne systematickú bezpečnostnú profiláciu, alebo len o okrajový presah v rámci širšieho programu. Podobne sa ako šedé miesto ukazuje aj nerovnováha medzi technickou a organizačno-manažérskou zložkou: niektoré programy majú informatický základ bez výraznejšej bezpečnostnej profilácie, iné zasa rozvíjajú bezpečnostný manažment bez rovnako zreteľnej technickej opory.

Za šedé miesto možno považovať aj absenciu jednotnejšieho rámca, podľa ktorého by bolo možné porovnávať výstupy absolventov kyberbezpečnostne relevantných programov naprieč školami. Z pohľadu potrieb praxe a rámcov NBÚ, ECSF a NIS2 sa totiž ukazuje, že samotný názov programu alebo všeobecná deklarácia bezpečnostného zamerania nestačí na posúdenie toho, aký typ odbornosti dané štúdium v skutočnosti rozvíja. Bez jasnejšieho prepojenia medzi kurikulom, rolami a očakávanými výstupmi ostáva porovnanie škôl nevyhnutne len čiastočné.

Z pohľadu potrieb praxe a rámcov NBÚ, ECSF a NIS2 teda hlavný problém nespočíva len v počte škôl alebo programov, ale aj v ich profilovej nevyváženosti a v nerovnomernej verejnej preukázateľnosti. Slovenské vysokoškolské prostredie má identifikovateľné základy pre rozvoj kyberbezpečnostných kapacít, no mimo jadrových uzlov ostáva pokrytie často fragmentárne, rozptýlené alebo slabo komunikované. To je dôležité zistenie nielen pre interpretáciu výsledkov, ale aj pre ďalšie úvahy o tom, kde je vhodné podporovať jadrové technické kapacity a kde skôr dopĺňať existujúci informatický alebo bezpečnostný základ.

7 Implikácie pre rezortnú politiku

Zo zistení uvedených v predchádzajúcich kapitolách vyplýva, že rozvoj vysokoškolských kapacít v oblasti kybernetickej bezpečnosti nemožno stavať na jednotnom modeli podpory všetkých škôl. Slovenské vysokoškolské prostredie je v tejto oblasti diferencované: popri úzkom jadre pracovísk s verejne doloženou technickou kyberprípravou existuje širší okruh škôl so silným informatickým základom a samostatná skupina inštitúcií, ktoré rozvíjajú bezpečnostno-manažérske, rezortné alebo právno-organizačné kapacity. Z pohľadu rezortnej politiky preto dáva väčší zmysel diferencovaná podpora podľa typu príspevku k bezpečnostnému ekosystému než plošný prístup bez rozlišovania profilov.

7.1 Posilnenie jadra technickej kyberprípravy

Prvou implikáciou je potreba stabilizovať a ďalej rozvíjať jadro priamej technickej kyberprípravy. Práve tam, kde je už dnes verejne doložená súvislá technická alebo technicko-organizačná bezpečnostná línia, má verejná podpora najvyššiu pravdepodobnosť bezprostredného efektu. V tejto časti systému sa totiž koncentrujú tie pracoviská a programy, pri ktorých možno najpresvedčivejšie identifikovať väzbu na technické bezpečnostné roly a na systematickú prípravu absolventov využiteľných v oblastiach ochrany sietí, systémov, informačných aktív, riešenia incidentov či riadenia informačnej bezpečnosti.

Z pohľadu verejnej politiky je preto opodstatnené sústrediť do tejto vrstvy najmä podporu laboratórnych kapacít, personálneho zabezpečenia, rozvoja špecializovaných predmetov, prepojenia s výskumom a partnerstiev s verejným aj súkromným sektorom. Ak má štát posilňovať technické kapacity v oblastiach, ako sú bezpečnostná analytika, sieťová a systémová bezpečnosť, incident response, digitálna forenzika alebo bezpečnostná architektúra, práve táto vrstva predstavuje jeho najdôležitejší oporný bod. Nejde pritom len o podporu existujúcich študijných programov v ich súčasnej podobe, ale aj o vytváranie podmienok na ich ďalšie kvalitatívne prehlbovanie.

Dôležitou súčasťou tejto podpory by malo byť aj posilnenie ľudských kapacít. Bez stabilných odborných garantov, pedagógov a výskumníkov nebude možné dlhodobo udržiavať ani rozširovať kvalitnú technickú bezpečnostnú výučbu. Rezortná politika by preto mala v tejto oblasti myslieť nielen na materiálne vybavenie, ale aj na personálnu udržateľnosť, systematickú spoluprácu s praxou a rozvoj akademických pracovísk, ktoré môžu plniť úlohu národne významných technických uzlov.

7.2 Rozšírenie bezpečnostnej profilácie na školách so silným IT základom

Druhou implikáciou je potreba cielene rozširovať bezpečnostnú profiláciu na školách so silným informatickým základom. Pri tejto skupine škôl nie je prioritou budovať od začiatku plnohodnotné jadro technickej kyberprípravy na každom pracovisku, ale skôr dopĺňať existujúce informatické programy o bezpečnostné moduly, tematické vetvy, voliteľné predmety, spoločné výučbové aktivity a praktickú spoluprácu s praxou. V mnohých prípadoch totiž práve tieto školy disponujú

kvalitným všeobecným IT základom, ktorý môže byť pri vhodnom doplnení premenený na relevantný zdroj budúcich kyberbezpečnostných kapacít.

Z pohľadu regionálneho rozvoja ide o dôležitú vrstvu, pretože práve tieto školy môžu vytvárať širšiu základňu talentu a znižovať závislosť krajiny od veľmi úzkeho okruhu technických uzlov. Rezortná politika by preto mala podporovať aj tie intervencie, ktoré zvyšujú bezpečnostnú využiteľnosť existujúcich IT programov, nie iba zakladanie nových samostatných programov. V praxi môže ísť o rozšírenie študijných plánov o bezpečnostne orientované predmety, podporu spoločných kurzov medzi školami, zapájanie odborníkov z praxe, rozvoj letných škôl, krátkodobých intenzívnych programov alebo iných flexibilných foriem profilácie.

Dôležité je pritom aj to, aby sa pri tejto skupine škôl nehodnotil úspech iba podľa toho, či sa formálne vytvorí nový študijný program s bezpečnostným názvom. Podstatnejšie je, či sa v rámci existujúcich informatických programov reálne rozšíri obsah, ktorý bude zodpovedať potrebám praxe a umožní študentom nadobúdať využiteľné bezpečnostné kompetencie. Práve v tejto oblasti môže mať rezortná politika vysoký multiplikačný efekt, pretože aj relatívne menšie kurikulárne zásahy môžu vo výsledku rozšíriť počet absolventov so základnou alebo stredne pokročilou bezpečnostnou profiláciou.

7.3 Samostatná podpora rezortnej a manažérskej vetvy

Treťou implikáciou je potreba samostatne uchopiť školy so širším bezpečnostným, rezortným a manažérskym profilom. Tieto inštitúcie nemožno vnímať ako náhradu technického jadra, ale ani ako okrajový prvok bez významu. Ich prínos spočíva najmä v oblastiach riadenia bezpečnosti, krízových procesov, ochrany kritickej infraštruktúry, compliance, vyšetrovania, obranných a policajných kapacít či bezpečnostnej správy informačných systémov. Ide teda o tú časť bezpečnostného ekosystému, ktorá je dôležitá pre fungovanie štátu, verejnej správy a regulovaných organizácií, no pracuje s odlišným profilom kompetencií než technické kyberpracoviská.

Z pohľadu verejnej politiky to znamená, že táto vetva si vyžaduje osobitný typ podpory a iné očakávané výstupy než technické programy. Opatrenia v tejto oblasti by preto mali smerovať skôr k posilňovaniu procesných, riadiacich, forenzných a rezortných kompetencií než k predstieraniu, že ide o totožný model prípravy ako pri technických kyberpracoviskách. Vhodná je najmä podpora prepojenia bezpečnostného manažmentu s aktuálnymi regulačnými požiadavkami, s riadením rizík, auditom, kontinuitou činností, vyšetrovaním incidentov, bezpečnostnou dokumentáciou a ochranou kritických procesov.

Táto vetva môže zároveň plniť dôležitú funkciu pri prepájaní technickej kyberbezpečnosti s prostredím verejnej správy, ozbrojených zložiek, polície, krízového riadenia a ďalších sektorov, kde sú technické opatrenia len jednou časťou širšieho bezpečnostného rámca. Rezortná politika by preto mala pri tejto skupine škôl sledovať skôr to, aký typ bezpečnostných kapacít rozvíjajú a ako tieto kapacity dopĺňajú technické jadro, než sa snažiť posudzovať ich podľa rovnakých kritérií ako informatické fakulty.

7.4 Zavedenie rámca, monitoringu a ukazovateľov

Štvrtou implikáciou je potreba posilniť verejnú čitateľnosť, porovnateľnosť a strategické riadenie rozvoja študijných programov relevantných pre kyberbezpečnosť. Screening ukázal, že medzi školami existujú výrazné rozdiely v tom, nakoľko podrobne zverejňujú študijné plány, predmetové mapy, informačné listy alebo profilové zameranie programov. To komplikuje nielen analytické posudzovanie, ale aj strategické rozhodovanie štátu, partnerov z praxe a samotných uchádzačov o štúdium. Z pohľadu rezortnej politiky by preto bolo vhodné podporiť väčšiu transparentnosť v prezentácii študijných programov, najmä pri tých, ktoré chcú byť identifikované ako relevantné pre rozvoj kyberbezpečnostných kapacít.

S tým úzko súvisí aj potreba lepšie prepájať vysokoškolské vzdelávanie s rolami a znalosťami požadovanými v praxi. Dokument ukazuje, že mimo najsilnejších uzlov ostáva väzba medzi študijnými programami a konkrétnymi bezpečnostnými rolami často iba implicitná alebo fragmentárna. Rezortná politika by preto mala podporovať také nástroje, ktoré umožnia školám jasnejšie prepájať kurikulum s rolami a oblasťami znalostí podľa vyhlášky NBÚ, rámca ECSF a požiadaviek vyplývajúcich z NIS2. Nejde pritom len o formálnu úpravu názvov predmetov, ale o vecné zosúladenie výstupov štúdia s tým, aké typy odbornosti bude verejný aj súkromný sektor reálne potrebovať.

V tejto súvislosti by bolo vhodné uvažovať aj o vytvorení referenčného rámca, ktorý by umožňoval porovnateľnejšie mapovať študijné programy na skupiny rolí, znalostí a kompetencií. Takýto rámec by nemal nahrádzať akreditačné procesy ani akademickú autonómiu škôl, ale mohol by slúžiť ako spoločný orientačný nástroj pre školy, štát aj zamestnávateľov. Jeho prínos by spočíval najmä v tom, že by zlepšil zrozumiteľnosť toho, aký typ absolventa daný program pripravuje a v akých oblastiach sú jeho výstupy najsilnejšie.

Napokon, zo zistení vyplýva aj potreba dlhodobejšieho monitorovania kapacít. Ak má štát robiť informované rozhodnutia o podpore študijných programov, laboratórií, personálnych kapacít alebo regionálnych iniciatív, nestačí sledovať len názvy odborov alebo počet škôl, ktoré používajú bezpečnostnú terminológiu. Potrebné je pravidelne vyhodnocovať, kde existuje verejne doložené technické jadro, kde sa rozvíja využiteľný informatický základ, kde sú prítomné širšie bezpečnostné kapacity a kde naopak zostávajú biele alebo šedé miesta. Až na takomto základe možno nastaviť podporu, ktorá bude zodpovedať reálnej štruktúre slovenského vysokoškolského prostredia, a nie iba formálnemu dojmu vytvorenému názvami programov.

Súčasťou takéhoto monitoringu by mohli byť aj základné ukazovatele, ktoré by umožnili priebežne sledovať posun v systéme. Môže ísť napríklad o počet programov s verejne doloženou bezpečnostnou profiláciou, počet študentov a absolventov v relevantných programoch, mieru prepojenia kurikula na roly podľa NBÚ a ECSF, rozsah laboratórnej a praktickej výučby, počet spoločných iniciatív s praxou alebo úroveň verejnej transparentnosti študijných plánov a predmetových výstupov. Takéto ukazovatele samy osebe nenahradia kvalitatívne posúdenie, ale môžu vytvoriť potrebný rámec pre dlhodobejšie a systematickejšie riadenie verejnej podpory.

8 Záver

Predložený screening ukázal, že slovenské vysoké školstvo nevytvára jednotný a rovnomerne rozložený model prípravy pre oblasť kybernetickej bezpečnosti, informačnej bezpečnosti, bezpečnostného manažmentu a príbuzných disciplín, ale skôr viacvrstvový systém s rozdielnou mierou technickej, organizačnej a rezortnej orientácie. Na základe verejne dostupných zdrojov možno konštatovať, že na Slovensku existuje identifikovateľné jadro pracovísk, pri ktorých je bezpečnostná profilácia verejne doložená najpresvedčivejšie a kde sa technická alebo technicko-organizačná bezpečnostná línia prejavuje nielen na úrovni názvu programu, ale aj v predmetovej skladbe, profiloch pracovísk a tematickom zameraní výučby. Zároveň však platí, že toto jadro je pomerne úzke a mimo neho sa bezpečnostná príprava často objavuje skôr ako čiastkový prvok širšieho informatického alebo bezpečnostného programu než ako plne rozvinutá samostatná profilácia.

Výskumná otázka tohto materiálu znela: *Do akej miery jednotlivé vysoké školy na Slovensku vytvárajú predpoklady pre prípravu absolventov použiteľných v oblasti technickej kyberbezpečnosti, informačnej bezpečnosti, bezpečnostného manažmentu a príbuzných disciplín?* Na základe vykonaného screeningu možno odpovedať, že tieto predpoklady vytvárajú v rozdielnej miere a rozdielnym spôsobom. Len menšia časť škôl vytvára z verejne dostupných zdrojov jasne doložiteľné predpoklady pre priamu technickú kyberprípravu. Širší okruh škôl poskytuje kvalitný informatický základ, ktorý môže byť pri vhodnom doplnení bezpečnostných modulov, praktickej výučby a profilácie využiteľný na prípravu absolventov pre vybrané bezpečnostné roly. Popri tom existuje aj samostatná skupina škôl, ktoré pripravujú absolventov skôr pre oblasti bezpečnostného manažmentu, riadenia rizík, rezortnej bezpečnosti, ochrany kritickej infraštruktúry, compliance, vyšetrovania alebo bezpečnostnej správy systémov než pre jadrové technické roly.

Z tohto pohľadu teda nemožno hovoriť ani o tom, že by slovenské vysoké školy ako celok predstavovali homogénnu a plne rozvinutú základňu pre technickú kyberbezpečnosť, ani o tom, že by boli pre rozvoj kyberbezpečnostných kapacít ako celok nedostatočné. Presnejšie je povedať, že slovenské vysokoškolské prostredie už dnes obsahuje tri odlišné, navzájom sa dopĺňajúce vrstvy kapacít: úzke jadro priamej technickej kyberprípravy, širšiu skupinu škôl so silným IT základom a bezpečnostným presahom a samostatnú vetvu škôl so širším bezpečnostným, manažérskym, právnym alebo rezortným profilom. Každá z týchto vrstiev má iný význam pre štát, verejnú správu, kritickú infraštruktúru a súkromný sektor a pripravuje odlišné typy absolventov.

Súčasne sa ukázalo, že dôležitým limitom nie je len samotný počet relevantných pracovísk, ale aj nerovnomerná verejná čitateľnosť ich kurikula. Kým pri niektorých školách možno bezpečnostnú líniu doložiť pomerne presne prostredníctvom programov, predmetov a pracovísk, pri iných ostáva väzba na bezpečnostné kompetencie len čiastočne alebo nepriamo čitateľná. Výsledky tohto materiálu preto treba chápať ako hodnotenie verejne doložiteľných predpokladov, nie ako úplný audit reálnej kvality výučby, personálneho zabezpečenia, laboratórnych kapacít alebo uplatnenia absolventov.

Záver preto možno formulovať nasledovne: slovenské vysoké školy vytvárajú predpoklady pre prípravu absolventov použiteľných v oblasti technickej kyberbezpečnosti, informačnej bezpečnosti, bezpečnostného manažmentu a príbuzných disciplín len čiastočne diferencovaným a nerovnomerne rozloženým spôsobom. Najsilnejšie a najpresvedčivejšie verejne doložené predpoklady existujú v úzkom jadre technicky profilovaných pracovísk; širší informatický sektor predstavuje významný potenciál pre ďalšiu bezpečnostnú profiláciu; a rezortná, manažérska a právno-organizačná vetva dopĺňa bezpečnostný ekosystém v oblastiach, ktoré sú pre fungovanie štátu a regulovaných organizácií rovnako dôležité, hoci nie sú totožné s jadrovou technickou kyberprípravou.

Pre rezortnú politiku z toho vyplýva, že ďalší rozvoj kyberbezpečnostných kapacít nemožno stavať na jednotnom prístupe ku všetkým školám. Potrebná je diferencovaná podpora: stabilizácia a prehlbovanie technického jadra, rozširovanie bezpečnostnej profilácie na školách so silným IT základom a samostatné rozvíjanie rezortných, manažérskych a právno-organizačných bezpečnostných kapacít. Práve takýto prístup najlepšie zodpovedá reálnej štruktúre slovenského vysokoškolského prostredia, ako ju ukázal tento screening.

Prílohy

Príloha A - Zoznam hodnotených vysokých škôl

Hodnotených bolo 33 inštitúcií. Výstup je určený ako strategický podklad; nejde o akreditačné posúdenie ani o kvalitatívny audit jednotlivých študijných plánov.

1. Akadémia ozbrojených síl gen. M. R. Štefánika
2. Akadémia Policajného zboru
3. Akadémia umení v Banskej Bystrici
4. Bratislavská medzinárodná škola liberálnych štúdií
5. Ekonomická univerzita v Bratislave
6. Hudobná a umelecká akadémia Jána Albrechta
7. Katolícka univerzita v Ružomberku
8. Paneurópska vysoká škola
9. Prešovská univerzita v Prešove
10. Slovenská poľnohospodárska univerzita v Nitre
11. Slovenská technická univerzita v Bratislave
12. Slovenská zdravotnícka univerzita v Bratislave
13. Technická univerzita v Košiciach
14. Technická univerzita vo Zvolene
15. Trenčianska univerzita Alexandra Dubčeka v Trenčíne
16. Trnavská univerzita v Trnave
17. Univerzita J. Selyeho
18. Univerzita Komenského v Bratislave
19. Univerzita Konštantína Filozofa v Nitre
20. Univerzita Mateja Bela v Banskej Bystrici
21. Univerzita Pavla Jozefa Šafárika v Košiciach
22. Univerzita sv. Cyrila a Metoda v Trnave
23. Univerzita veterinárskeho lekárstva a farmácie v Košiciach
24. Vysoká škola bezpečnostného manažérstva v Košiciach
25. Vysoká škola Danubius
26. Vysoká škola DTI
27. Vysoká škola ekonómie a manažmentu v Bratislave
28. Vysoká škola manažmentu
29. Vysoká škola múzických umení v Bratislave
30. Vysoká škola technická a ekonomická v Prešove
31. Vysoká škola výtvarných umení v Bratislave
32. Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety
33. Žilinská univerzita v Žiline

Príloha B – Použité zdroje

Verejné dostupné opisy študijných programov

- Portál VŠ - FIIT STU: Informačná bezpečnosť (2026/2027). https://www.portalvs.sk/sk/studijny-program/stu-informacna-bezpecnost0
- Portál VŠ - FEI TUKE: Kyberbezpečnosť (Bc.). https://www.portalvs.sk/sk/studijny-program/kyberbezpecnost
- Portál VŠ - FEI TUKE: Kyberbezpečnosť (Ing.). https://www.portalvs.sk/sk/studijny-program/kyberbezpecnost1
- Portál VŠ - FRI ŽU: Informačné a sieťové technológie. https://www.portalvs.sk/sk/studijny-program/informacne-a-sietove-technologie
- Portál VŠ - FRI ŽU: Fakulta riadenia a informatiky / programy. https://www.portalvs.sk/sk/fakulta/fakulta-riadenia-a-informatiky
- Portál VŠ - FMFI UK: Informatika. https://www.portalvs.sk/sk/studijny-program/uk-informatika
- Portál VŠ - FMFI UK: Aplikovaná informatika. https://www.portalvs.sk/sk/studijny-program/uk-aplikovana-informatika
- Portál VŠ - UPJŠ: Aplikovaná informatika. https://www.portalvs.sk/sk/studijny-program/upjs-aplikovana-informatika0
- Portál VŠ - UKF: Aplikovaná informatika. https://www.portalvs.sk/sk/studijny-program/ukf-aplikovana-informatika0
- Portál VŠ - UCM: Aplikovaná informatika. https://www.portalvs.sk/sk/studijny-program/ucm-aplikovana-informatika7
- Portál VŠ - UMB: Aplikovaná informatika a vývoj softvéru. https://www.portalvs.sk/sk/studijny-program/umb-aplikovana-informatika-a-vyvoj-softveru1
- Portál VŠ - UJS: Aplikovaná informatika. https://www.portalvs.sk/sk/studijny-program/ujs-aplikovana-informatika1
- Portál VŠ - EUBA: Hospodárska informatika. https://www.portalvs.sk/sk/studijny-program/hospodarska-informatika3
- Portál VŠ - APZ: univerzitný profil a programy. https://www.portalvs.sk/sk/vysoka-skola/akademia-policajneho-zboru-v-bratislave
- Portál VŠ - VŠBM: Riadenie bezpečnostných systémov. https://www.portalvs.sk/sk/studijny-program/riadenie-bezpecnostnych-systemov4
- Portál VŠ - Paneurópska vysoká škola: Aplikovaná informatika. https://www.portalvs.sk/sk/studijny-program/pevs-aplikovana-informatika0
- Portál VŠ - Akadémia umení v Banskej Bystrici: študijné programy. https://www.portalvs.sk/sk/hladat?university=718000000
- Portál VŠ - VŠVU: Digitálne umenia. https://www.portalvs.sk/sk/hladat?university=706000000

- Portál VŠ - KU: Učiteľstvo informatiky. https://www.portalvs.sk/sk/studijny-program/ucitelstvo-informatiky0
- Portál VŠ - SZU: univerzitný profil. https://www.portalvs.sk/sk/vysoka-skola/slovenska-zdravotnicka-univerzita-v-bratislave
- Portál VŠ - VŠMU: univerzitný profil. https://www.portalvs.sk/sk/vysoka-skola/vysoka-skola-muzickych-umeni-v-bratislave
- Portál VŠ - Katolícka univerzita v Ružomberku: profil. https://www.portalvs.sk/sk/vysoka-skola/katolicka-univerzita-v-ruzomberku
- Portál VŠ - register študijných programov. https://www.portalvs.sk/sk/morho
- Portál VŠ - EUBA: Informačný manažment. https://www.portalvs.sk/sk/studijny-program/informacny-manazment0

Normatívne a rámcové zdroje

- Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 z 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS2), najmä čl. 20, 21 a 23.
- Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti.
- ENISA: European Cybersecurity Skills Framework (ECSF) – User Manual.
- ENISA: European Cybersecurity Skills Framework (ECSF) – Role Profiles.
- ENISA: Cybersecurity roles and skills for NIS2 Essential and Important Entities.