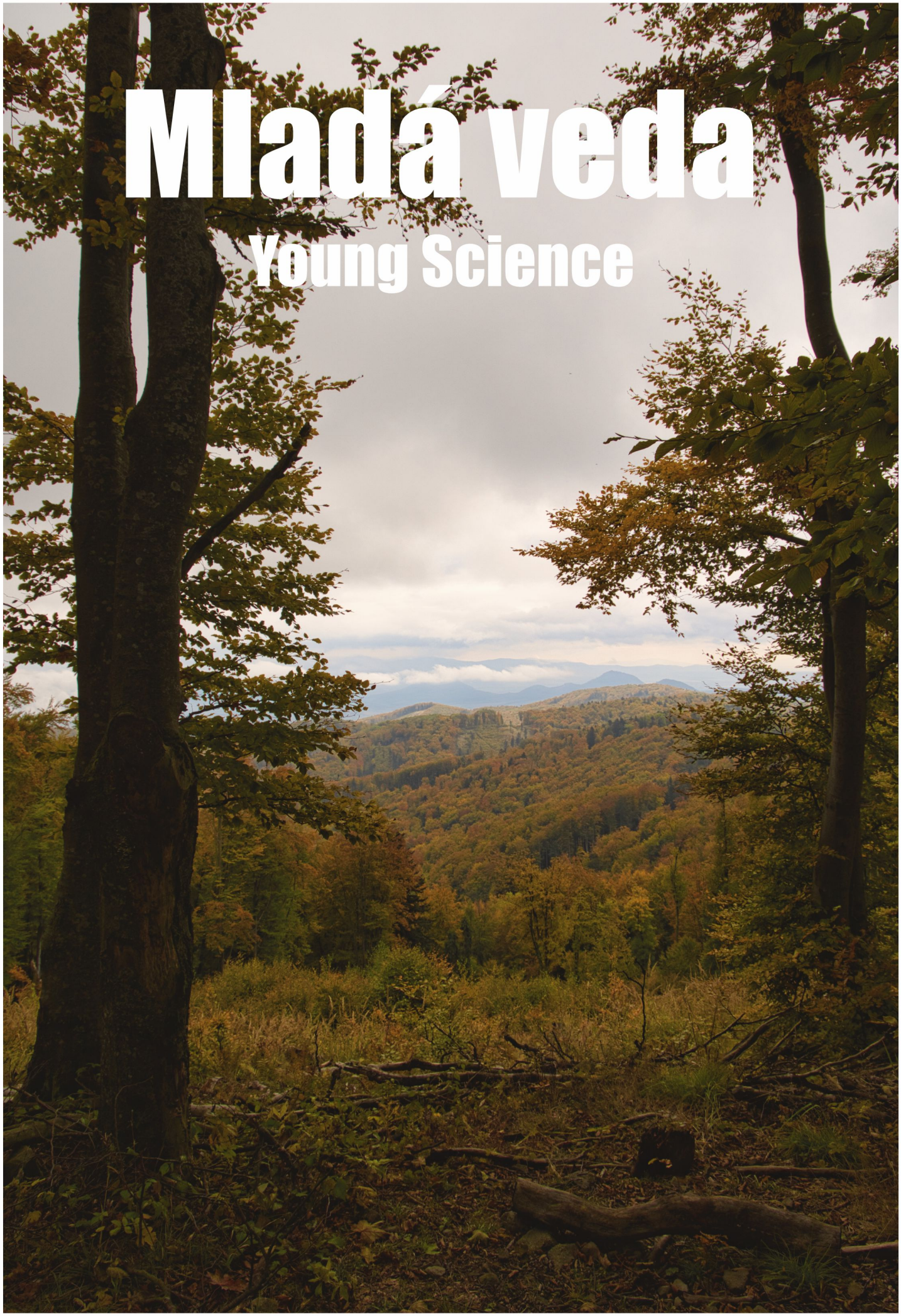
ISSN 1339-3189 5/2026

Mladá veda

Young Science



www.mladaveda.sk

Mladá veda
Young Science

MEDZINÁRODNÝ VEDECKÝ ČASOPIS MLADÁ VEDA / YOUNG SCIENCE
Číslo 5, ročník 14., vydané v septembri 2026
ISSN 1339-3189, EV 167/23/EPP
Kontakt: info@mladaveda.sk, tel.: +421 908 546 716, www.mladaveda.sk
Fotografia na obálke: Pohorie Čergov. © Branislav A. Švorc, foto.branisko.at

VYDAVATEĽ
Inštitút pre vedu, kultúru a spoločenský rozvoj
IČO: 57728038, Bajkalská 12B, 080 01 Prešov, Slovensko
v spolupráci s vydavateľstvom UNIVERSUM-EU, spol. s r. o.

Mladá veda
Young Science
ISSN 1339-3189

Vol. 14 (5), pp. 325-333

MODELY VZDELÁVANIA V KYBERNETICKEJ BEZPEČNOSTI VO VYBRANÝCH KRAJINÁCH EURÓPSKEJ ÚNIE A ICH RELEVANCIA PRE SLOVENSKÚ REPUBLIKU

CYBERSECURITY EDUCATION MODELS IN SELECTED EUROPEAN UNION COUNTRIES AND THEIR RELEVANCE FOR THE SLOVAK REPUBLIC

Norbert Molnár[1]

Norbert Molnár je externým doktorandom Vysokej školy bezpečnostného manažérstva v Košiciach v študijnom programe riadenie bezpečnostných systémov, študijný odbor bezpečnostné vedy. Vo svojom dizertačnom výskume sa venuje návrhu integrovaného systému kontinuálneho vzdelávania v kybernetickej bezpečnosti. Súčasne pôsobí ako konateľ Národnej akadémie pre kybernetickú bezpečnosť (NAKIB) a ako člen dozornej rady Komory manažérov kybernetickej bezpečnosti (KMKB).

Norbert Molnár is an external doctoral student at the University of Security Management in Košice, in the Security Systems Management study programme, field of study Security Sciences. In his dissertation research he focuses on the design of an integrated system of continuing education in cybersecurity. He also serves as Managing Director of the National Cybersecurity Academy (NAKIB) and as a member of the Supervisory Board of the Chamber of Cybersecurity Managers (KMKB).

Abstract

Continuing education of cybersecurity professionals has, following the transposition of Directive (EU) 2022/2555 (NIS2), become a legally relevant issue for a substantially wider range of organisations than before. Using comparative analysis, the paper examines cybersecurity education models in four European Union countries regarded within the professional community as reference cases: Estonia, Germany, France and the Netherlands, assessed against six criteria: the existence of a national competency framework, the role-based orientation of the educational offer, its modularity, its linkage to NIS2 requirements, the existence of a certification system, and the method of measuring educational effectiveness. The analysis identifies four distinct, mutually complementary model solutions: the Estonian

[1] Adresa pracoviska: Mgr. Norbert Molnár, externý doktorand, Vysoká škola bezpečnostného manažérstva v Košiciach, Ústav bezpečnostného manažérstva, Košťova 1, 040 01 Košice
E-mail: norbert.molnar@vsbm.sk

model of institutional linkage, the German model of a national certification authority, the French model of qualitative labelling of existing programmes, and the Dutch model of a long-term national strategy with a dedicated budget. In conclusion, the paper confronts these findings with the current state of the cybersecurity education ecosystem in Slovakia and formulates recommendations for its further development.
Key words: cybersecurity, continuing education, NIS2 Directive, competency framework, comparative analysis, European Union

Abstrakt
Kontinuálne vzdelávanie odborníkov v oblasti kybernetickej bezpečnosti sa v dôsledku transpozície smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 (NIS2) stalo právne relevantnou témou pre výrazne širší okruh organizácií, než tomu bolo doteraz. Príspevok formou komparatívnej analýzy skúma modely vzdelávania v kybernetickej bezpečnosti v štyroch krajinách Európskej únie, ktoré sú v odbornej komunite považované za referenčné: v Estónsku, Nemecku, Francúzsku a Holandsku, a to podľa šiestich kritérií: existencia národného kompetenčného rámca, rolová orientácia vzdelávacej ponuky, jej modulárnosť, previazanosť s požiadavkami NIS2, existencia certifikačného systému a spôsob merania efektívnosti vzdelávania. Na základe analýzy sú identifikované štyri odlišné, vzájomne sa dopĺňajúce modelové riešenia: estónsky model inštitucionálneho prepojenia, nemecký model národného certifikačného orgánu, francúzsky model kvalitatívneho značkovania (labellingu) existujúcich programov a holandský model dlhodobej národnej stratégie s vyčleneným rozpočtom. V závere príspevok konfrontuje tieto zistenia so súčasným stavom vzdelávacieho ekosystému kybernetickej bezpečnosti na Slovensku a formuluje odporúčania pre jeho ďalší rozvoj.
Kľúčové slová: kybernetická bezpečnosť, kontinuálne vzdelávanie, smernica NIS2, kompetenčný rámec, komparatívna analýza, Európska únia

Úvod

Nedostatok kvalifikovaných odborníkov patrí medzi najčastejšie diskutované bariéry účinnej kybernetickej bezpečnosti v Európskej únii. Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) už niekoľko rokov upozorňuje na značný a pretrvávajúci nedostatok kvalifikovaných odborníkov naprieč členskými štátmi (ENISA, 2021). Na celosvetovej úrovni ho správa ISC2 Cybersecurity Workforce Study odhaduje na štyri milióny pracovných miest (ISC2, 2023). Tento kvantitatívny deficit sprevádza aj kvalitatívny problém. Existujúca vzdelávacia ponuka je vo väčšine krajín roztrieštená medzi akademický sektor, priemyselné certifikačné schémy a jednorazové školenia zamerané na zvyšovanie povedomia. Chýba jej systémová previazanosť na konkrétne pracovné roly aj mechanizmus, ktorý by jej obsah aktualizoval v tempe, akým sa menia kybernetické hrozby.

Túto situáciu mení smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS2). Smernica výrazne rozšírila okruh regulovaných subjektov. V článku 21 ods. 2 písm. g) navyše po prvýkrát na úrovni práva Európskej únie explicitne zaraďuje „základné postupy kybernetickej hygieny a odbornú prípravu v oblasti kybernetickej bezpečnosti“ medzi povinné

opatrenia riadenia kybernetického rizika (Európsky parlament a Rada, 2022, s. 127). Zámerne pritom nešpecifikuje, akým spôsobom a v akom rozsahu má byť táto povinnosť plnená. Operacionalizáciu ponecháva na členské štáty a jednotlivé regulované subjekty. Vzniká tak otázka presahujúca rámec jednej krajiny: aké systémové modely vzdelávania v kybernetickej bezpečnosti sa v Únii osvedčujú, a čo z nich možno prevziať tam, kde systém kontinuálneho vzdelávania v tejto oblasti, tak ako na Slovensku, ešte nie je inštitucionálne ustálený.

Autor sa touto otázkou zaoberá aj mimo akademického kontextu. Ako konateľ Národnej akadémie pre kybernetickú bezpečnosť a člen dozornej rady Komory manažérov kybernetickej bezpečnosti sa opakovane stretáva s organizáciami, ktoré legislatívnu povinnosť vzdelávať zamestnancov v oblasti kybernetickej bezpečnosti majú, no nemajú k dispozícii referenčný rámec, podľa ktorého by mali postupovať. Cieľom tohto príspevku je na základe komparatívnej analýzy štyroch krajín Európskej únie identifikovať odlišné modelové prístupy k riešeniu tejto otázky a formulovať z nich odporúčania využiteľné pre ďalší rozvoj vzdelávacieho ekosystému kybernetickej bezpečnosti v Slovenskej republike.

Legislatívny rámec Európskej únie a jeho dôsledky pre vzdelávanie

Popri smernici NIS2 formuje európsky legislatívny rámec vzdelávania v kybernetickej bezpečnosti aj nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 o agentúre ENISA a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií, známe ako Cybersecurity Act (ďalej len „CSA“) (Európsky parlament a Rada, 2019). Nariadenie zavádza jednotný európsky rámec certifikačných schém pre produkty, procesy a služby v oblasti kybernetickej bezpečnosti. V článku 58 ukladá členským štátom povinnosť určiť národný certifikačný orgán (National Cybersecurity Certification Authority), ktorý certifikačné schémy v danom štáte vykonáva a dohliada na ne. Práve spôsob, akým jednotlivé členské štáty túto povinnosť naplnili, je jedným z kritérií komparatívnej analýzy predloženej v tomto príspevku.

Treťou relevantnou normou je medzinárodná norma ISO/IEC 27001:2022, celosvetovo najrozšírenejší štandard pre manažérstvo bezpečnosti informácií. Jej klauzuly 7.2 (Competence) a 7.3 (Awareness) vyžadujú, aby organizácia systematicky určila, zabezpečila a zdokumentovala kompetentnosť osôb ovplyvňujúcich bezpečnosť informácií (ISO/IEC, 2022). Rovnako ako NIS2 aj táto norma formuluje meta-požiadavku, teda auditovateľný prístup ku kompetenciám, bez toho, aby stanovila jej konkrétny obsah.

Žiadny z týchto troch nástrojov nešpecifikuje, čo a ako majú organizácie svojich zamestnancov v oblasti kybernetickej bezpečnosti učiť. Túto medzeru majú v jednotlivých členských štátoch vypĺňať národné kompetenčné rámce a inštitucionálne mechanizmy, ktorých komparácia je predmetom tohto príspevku. Na úrovni celej Únie existujú dva kompetenčné rámce s ambíciou stať sa spoločnou referenciou. Prvým je European Cybersecurity Skills Framework (ECSF), vyvinutý agentúrou ENISA a publikovaný v roku 2022 (ENISA, 2022a; ENISA, 2022b), ktorý definuje dvanásť rolových profilov previazaných s Európskym kvalifikačným rámcom. Druhým je americký NICE Framework (National Initiative for Cybersecurity Education), ktorého aktuálna revízia definuje viac než päťdesiat pracovných rolí prostredníctvom granulárnych položiek úloh, znalostí a zručností (Petersen et al., 2020). Ani jeden z týchto rámcov však sám osebe nedefinuje úrovne odbornosti ani

odporúčané vzdelávacie postupnosti. Je to priestor, ktorý v jednotlivých krajinách vypĺňajú národné inštitucionálne riešenia.

Metodika komparatívnej analýzy

Pre komparatívnu analýzu boli vybrané štyri krajiny Európskej únie: Estónsko, Nemecko, Francúzsko a Holandsko. Odborná komunita kybernetickej bezpečnosti ich opakovane uvádza ako referenčné príklady systémového prístupu k vzdelávaniu. Súčasne predstavujú štyri odlišné inštitucionálne tradície (baltskú, stredoeurópsku federálnu, francúzsku centralizovanú a holandskú konsenzuálnu), čo umožňuje širšie zovšeobecnenie zistení, než by prinieslo porovnanie krajín s podobnou správnou tradíciou. Analýza vychádza z verejne dostupných zdrojov národných orgánov zodpovedných za kybernetickú bezpečnosť a vzdelávanie v jednotlivých krajinách (BSI, n.d.; cyber.gouv.fr, n.d.; CyberHubs, 2025; Ministerie van Justitie en Veiligheid, 2022) a z odbornej literatúry venovanej európskemu rámcu kybernetickej bezpečnosti.

Krajiny sú porovnávané podľa šiestich kritérií, odvodených z požiadaviek, ktoré na vzdelávací systém kladie kombinácia smernice NIS2, nariadenia CSA a normy ISO/IEC 27001: existencia národného kompetenčného rámca previazaného s medzinárodnými štandardmi; rolová orientácia vzdelávacej ponuky, teda diferenciácia obsahu podľa pracovnej role namiesto jednotného obsahu pre všetkých; modulárnosť systému umožňujúca kombinovať a priebežne aktualizovať jednotlivé vzdelávacie zložky; explicitná väzba na požiadavky NIS2; existencia certifikačného systému previazaného s CSA; a spôsob, akým je meraná efektívnosť vzdelávania nad rámec formálnej evidencie účasti.

Národné modely vzdelávania v kybernetickej bezpečnosti

Estónsko

Estónsko je v medzinárodnej odbornej literatúre dlhodobo uvádzané ako vzorový príklad kyberneticky odolného štátu a jeho vzdelávací systém je pomerne podrobne zdokumentovaný. Formálne vzdelávanie zabezpečuje predovšetkým Tallinnská technická univerzita (TalTech), ktorá ponúka bakalársky program kybernetického bezpečnostného inžinierstva so 40 až 60 absolventmi ročne, a spolu s Univerzitou v Tartu aj magisterský program so zameraním na digitálnu forenznú analýzu a kryptografiu (CyberHubs, 2025). Popri akademickom vzdelávaní pôsobí národný systém prognózovania kompetenčných potrieb OSKA, ktorý prevádzkuje Estónsky úrad pre kvalifikácie (Kutsekoda) a ktorý formou pravidelných sektorových analýz priebežne mapuje aj kompetenčné potreby v oblasti kybernetickej bezpečnosti (CEDEFOP, 2023). Štátnym orgánom zodpovedným za kybernetickú bezpečnosť je Estónsky úrad pre informačné systémy (RIA), ktorý popri regulačnej funkcii aj priebežne eviduje bezpečnostné incidenty (len v roku 2024 ich zaznamenal vyše 3 300) a tieto zistenia premieta do priorít vzdelávania a zvyšovania povedomia (CyberHubs, 2025).

Estónsky model je zaujímavý v tom, ako sú akademický sektor, štátna správa a systém kompetencií vzájomne prepojené. OSKA priebežne signalizuje, aké kompetencie sú pre trh práce potrebné, RIA tieto potreby dopĺňa vlastnými prevádzkovými dátami o incidentoch a univerzity musia na to reagovať aktualizáciou študijných programov. Vzdelávacia ponuka tak nie je jednoducho viazaná iba na akademický kurikulárny cyklus.

Nemecko

Nemecko rieši certifikačnú stránku kybernetickej bezpečnosti inak: prostredníctvom silnej pozície jedinej štátnej inštitúcie. Spolkový úrad pre bezpečnosť informačných technológií (BSI) plní úlohu národného certifikačného orgánu (National Cybersecurity Certification Authority) na základe zákona BSIG a článku 58 nariadenia CSA (BSI, n.d.). Vykonáva pritom dve oddelené funkcie: samotnú certifikáciu a dohľad nad jej dodržiavaním, vrátane oprávnenia vyžadovať súčinnosť, vykonávať audity a odobrať vydaný certifikát podľa článku 65 CSA. BSI je zároveň zapojený do Európskej skupiny pre certifikáciu kybernetickej bezpečnosti, kde vykonáva partnerské preskúmania certifikačných orgánov iných členských štátov a predkladá výročné správy agentúre ENISA a Európskej komisii.

Táto zdvojená činnosť, t.j. certifikačná aj dohľadová právomoc jednej inštitúcie, je z porovnávaných modelov najsilnejšie legislatívne ukotvená a najpriamejšie previazaná s celoeurópskym certifikačným rámcom podľa CSA.

Francúzsko

Francúzsko namiesto certifikácie jednotlivcov alebo priameho riadenia vzdelávacej ponuky zvolilo tretiu cestu: hodnotenie existujúcich vzdelávacích programov. Národná agentúra pre bezpečnosť informačných systémov (ANSSI) prevádzkuje dva značkovacie (labelling) systémy: SecNumedu pre počiatočné, vysokoškolské programy v kybernetickej bezpečnosti a SecNumedu-FC pre programy kontinuálneho, celoživotného vzdelávania (cyber.gouv.fr, n.d.). Označenie potvrdzuje, že program spĺňa kritériá ANSSI na obsah, rozsah praktickej výučby a kvalitu výstupov, čím sa stáva dôveryhodnou značkou kvality naprieč desiatkami francúzskych vysokých škôl a súkromných vzdelávacích inštitúcií.

Francúzsky model pokrýva to, čo štát nerobí. Nebuduje paralelnú štruktúru ani nevydáva certifikáty jednotlivým odborníkom, iba posudzuje súlad už existujúcej ponuky s národne stanovenými kritériami. Nejde teda o model centralizovaného poskytovania.

Holandsko

Najširší časový aj inštitucionálny záber má holandský prístup. Holandsko zakotvilo vzdelávaciu dimenziu kybernetickej bezpečnosti priamo v národnej stratégii The Netherlands Cybersecurity Strategy 2022–2028, ktorej štvrtý pilier je venovaný „človeku za technológiou“ (Ministerie van Justitie en Veiligheid, 2022). Stratégia formuluje sedem cieľov v oblasti rozvoja zručností: od základnej občianskej kybernetickej hygieny cez zaradenie digitálnych zručností do národných učebných osnov základných a stredných škôl až po systematickú analýzu nedostatku pracovnej sily v odvetví a rozšírenie vysokoškolského a celoživotného vzdelávania zosúladeného s trhom práce. Na jej realizáciu vyčlenila holandská vláda na obdobie rokov 2022 až 2028 sumu 111 miliónov eur naprieč ôsmimi ministerstvami.

Holandsko na rozdiel od ostatných krajín nerieši vzdelávanie v oblasti kybernetickej bezpečnosti ako agendu jedného rezortu alebo ako otázku výlučne pre už pôsobiacich odborníkov, ale ako kontinuum od základného školstva po celoživotné vzdelávanie, podložené vyčleneným a časovo rozvrhnutým rozpočtom.

Komparatívna syntéza

Tabuľka 1 zhŕňa výsledky komparatívnej analýzy podľa šiestich zvolených kritérií. Symbol „++“ označuje, že krajina v danom kritériu predstavuje silný, systémovo rozpracovaný príklad; „+“ označuje čiastočné alebo formujúce sa naplnenie kritéria.

Kritérium	Estónsko	Nemecko	Francúzsko	Holandsko
Národný kompetenčný rámec	** (OSKA)	*	*	** (národná stratégia)
Rolová orientácia ponuky	**	*	** (podľa typu programu)	*
Modulárnosť systému	*	*	*	**
Väzba na NIS2 / CSA	*	** (BSI ako NCCA)	*	** (explicitný pilier stratégie)
Certifikačný systém	*	** (BSI, čl. 58 CSA)	** (SecNumedu/-FC)	*
Meranie efektívnosti	*	*	* (kritériá labellingu)	** (7 cieľov s harmonogramom)

Tabuľka 1 – Výsledky komparatívnej analýzy vzdelávacích modelov
Zdroj: vlastné spracovanie

Z porovnania vystupujú štyri odlišné, vzájomne sa dopĺňajúce modely. Estónsko kladie dôraz na priebežnú výmenu informácií medzi akademickým sektorom, štátom a systémom prognózovania kompetencií. Nemecko koncentruje certifikačnú aj dohľadovú právomoc do jednej inštitúcie. Francúzsko namiesto riadenia ponuky hodnotí jej kvalitu. Holandsko si zakladá na dlhodobej vízii a vyčlenenom rozpočte naprieč celým vzdelávacím systémom. Ani jedna krajina nenapĺňa všetky kritériá súčasne v maximálnej miere, čo potvrdzuje, že nejde o jeden „najlepší“ univerzálny model, ale o štyri legitímne, kombinovateľné stratégie. Pre krajinu, ktorá, tak ako Slovensko, svoj vzdelávací systém v oblasti kybernetickej bezpečnosti ešte len organizačne buduje, z toho vyplýva jasný metodický záver. Namiesto prevzatia jedného zahraničného vzoru v celom rozsahu je vhodnejšie inšpirovať sa jednotlivými vrstvami z viacerých modelov podľa toho, ktorá vlastná inštitucionálna medzera má byť prioritne riešená.

Súčasný stav a implikácie pre Slovenskú republiku

Vzdelávací ekosystém kybernetickej bezpečnosti na Slovensku je v porovnaní so štyrmi analyzovanými krajinami výrazne mladší a inštitucionálne menej prepojený. Na akademickej úrovni ho zabezpečujú predovšetkým Žilinská univerzita v Žiline, Slovenská technická univerzita v Bratislave, Akadémia Policajného zboru v Bratislave, Akadémia ozbrojených síl generála M. R. Štefánika v Liptovskom Mikuláši a Vysoká škola bezpečnostného manažérstva v Košiciach, ktorá sa profiluje ako špecializovaná inštitúcia zameraná na bezpečnostné vedy vrátane kybernetickej bezpečnosti na doktorandskej úrovni. Popri akademickom sektore pôsobia traja ďalší kľúčoví aktéri. Národná akadémia pre kybernetickú bezpečnosť (NAKIB) sa v súčasnosti sústreďuje predovšetkým na zvyšovanie povedomia a

jednorazové kurzy. Certifikačná autorita kybernetickej bezpečnosti (KCCAB), zodpovedná za certifikáciu fyzických osôb podľa CSA, prevádzkuje certifikačný systém, ktorý je k dátumu spracovania tohto príspevku funkčný zatiaľ len pre dve role, manažéra kybernetickej bezpečnosti a audítora kybernetickej bezpečnosti. Komora manažérov kybernetickej bezpečnosti (KMKB), stavovská komora s viac než tristo členmi, zasa realizuje kontinuálny vzdelávací proces formou pravidelných webinárov, ročných workshopov a odbornej konferencie Cyber Summit.

Transpozícia smernice NIS2 do zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti výrazne rozšírila okruh subjektov, ktoré majú zákonnú povinnosť zabezpečovať odbornú prípravu svojich zamestnancov (NR SR, 2018). Táto povinnosť však ani po transpozícii nie je bližšie operacionalizovaná. Porovnanie so štyrmi analyzovanými krajinami je v tomto kontexte užitočné práve preto, že ukazuje, akými odlišnými, no realistickými cestami sa dá takáto medzera vyplniť.

Nemecký model národného certifikačného orgánu je priamo analogický funkcii, ktorú na Slovensku plní KCCAB, zatiaľ však len pre role manažéra a audítora kybernetickej bezpečnosti. Nemecká skúsenosť naznačuje, že táto funkcia si vyžaduje nielen certifikačnú, ale aj dohľadovú kompetenciu vrátane možnosti certifikát odobrať, nielen ho jednorazovo vydať. Francúzsky model kvalitatívneho značkovania ponúka realistickú alternatívu k budovaniu úplne novej vzdelávacej štruktúry od základov: KCCAB by mohla plniť analogickú funkciu vo vzťahu k existujúcim programom NAKIB, KMKB a slovenských vysokých škôl, namiesto toho, aby s nimi budovala paralelnú, konkurenčnú ponuku. Holandský model dlhodobej národnej stratégie je zo štyroch najambicióznejší a v krátkodobom horizonte najmenej priamo prenositeľný. Je založený na princípe vzdelávania v kybernetickej bezpečnosti ako kontinua a nie izolovanej agendy jedného rezortu, je však relevantný pre budúcu tvorbu národnej stratégie kybernetickej bezpečnosti. Estónsky model napokon pripomína niečo, čo sa v slovenskom prostredí ľahko prehliadne. Samotná existencia jednotlivých aktérov nestačí, pokiaľ medzi nimi chýba systémový mechanizmus priebežnej výmeny informácií o kompetenčných potrebách trhu práce. Práve tento mechanizmus medzi NAKIB, KCCAB, KMKB a akademickým sektorom na Slovensku k dátumu spracovania tohto príspevku chýba.

Z uvedeného porovnania vyplývajú tri odporúčania. Dokončenie certifikačného systému KCCAB by malo od začiatku zahŕňať aj dohľadovú funkciu analogickú nemeckému modelu, nie iba jednorazové vydávanie certifikátov. Namiesto budovania novej, centrálne riadenej vzdelávacej ponuky je metodicky vhodnejšie zvážiť francúzsky inšpirovaný model kvalitatívnej certifikácie existujúcej ponuky NAKIB, KMKB a vysokých škôl podľa jednotných, národne stanovených kritérií previazaných s rolovými profilmi ECSF a NICE. A dlhodobá udržateľnosť celého systému si vyžaduje mechanizmus podobný estónskemu, teda formálny, pravidelne aktualizovaný kanál, ktorým sa kompetenčné potreby zamestnávateľov premietajú do obsahu vzdelávacej ponuky naprieč všetkými zúčastnenými inštitúciami.

Záver

Komparatívna analýza štyroch krajín Európskej únie ukázala, že smernica NIS2 síce ukladá všetkým členským štátom rovnakú povinnosť zabezpečovať odbornú prípravu v oblasti kybernetickej bezpečnosti. Jej realizácia sa však v jednotlivých krajinách uberá výrazne odlišnými, no vzájomne legitímnymi cestami. Estónsko stavia na priebežnej výmene informácií medzi akademickým sektorom, štátom a systémom prognózovania kompetencií, Nemecko na silnej dohľadovej právomoci národného certifikačného orgánu, Francúzsko na kvalitatívnom hodnotení existujúcej ponuky a Holandsko na dlhodobej stratégii. Žiadny z týchto modelov nie je univerzálne najlepší. Ich hodnota pre krajinu, akou je Slovensko, spočíva práve v tom, že ponúkajú štyri odlišné, kombinovateľné inšpirácie pre riešenie štyroch odlišných, súčasne existujúcich inštitucionálnych medzier slovenského vzdelávacieho ekosystému kybernetickej bezpečnosti.

Tento článok odporúčal na publikovanie vo vedeckom časopise Mladá veda:
doc. JUDr. Mgr. Miloš Svrček, PhD., LL.M, MSc.

Tento príspevok vychádza z čiastkových zistení prebiehajúceho dizertačného výskumu autora, zameraného na návrh integrovaného systému kontinuálneho vzdelávania v kybernetickej bezpečnosti pre podmienky Slovenskej republiky. Predložená komparatívna analýza tvorí jeden z jeho teoretických a analytických vstupov. Jej ďalšie rozpracovanie, doplnené o empirické overenie kompetenčných potrieb slovenských organizácií, je predmetom nadväzujúcej dizertačnej práce.

Použitá literatúra

1. BSI, n.d. *Nationale Behörde für Cybersicherheitszertifizierung (NCCA)*. Bonn: Bundesamt für Sicherheit in der Informationstechnik. Dostupné na: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/NCCA/ncca_node.html
2. CEDEFOP, 2023. *OSKA – System of Labour Market Monitoring and Future Skills Forecasting*. Thessaloniki: European Centre for the Development of Vocational Training. Dostupné na: https://www.cedefop.europa.eu/en/tools/matching-skills/all-instruments/oska-system-labour-market-monitoring-and-future-skills-forecasting
3. CYBER.GOUV.FR, n.d. *Formations labellisées par l'ANSSI (SecNumedu, SecNumedu-FC)*. Paris: Agence nationale de la sécurité des systèmes d'information. Dostupné na: https://cyber.gouv.fr/formations-labellisees
4. CYBERHUBS, 2025. *Cybersecurity Skills Strategy – Estonia*. CyberHubs Project (Erasmus+). Dostupné na: https://cyberhubs.eu/wp-content/uploads/2025/02/Cybersecurity-skills-strategy_Estonia_FINAL.pdf
5. ENISA, 2021. *Addressing the EU Cybersecurity Skills Shortage and Gap through Higher Education*. Athens: European Union Agency for Cybersecurity. ISBN 978-92-9204-540-1. DOI 10.2824/033355.
6. ENISA, 2022a. *European Cybersecurity Skills Framework (ECSF) – User Manual*. Athens: European Union Agency for Cybersecurity. ISBN 978-92-9204-583-8. DOI 10.2824/95989.
7. ENISA, 2022b. *European Cybersecurity Skills Framework (ECSF) – Role Profiles*. Athens: European Union Agency for Cybersecurity.

8. EURÓPSKY PARLAMENT A RADA, 2019. *Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (Cybersecurity Act)*. Úradný vestník Európskej únie L 151, 7. 6. 2019, s. 15 – 69.
9. EURÓPSKY PARLAMENT A RADA, 2022. *Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS2)*. Úradný vestník Európskej únie L 333, 27. 12. 2022, s. 80 – 152.
10. ISC2, 2023. *ISC2 Cybersecurity Workforce Study 2023*. Alexandria, VA: ISC2.
11. ISO/IEC, 2022. *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. 3. vyd. Geneva: International Organization for Standardization.
12. MINISTERIE VAN JUSTITIE EN VEILIGHEID, 2022. *The Netherlands Cybersecurity Strategy 2022–2028*. Den Haag: Ministry of Justice and Security. Dostupné na: https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2022/december/06/the-netherlands-cybersecurity-strategy-2022-2028/TheNetherlandsCybersecurityStrategy2022-2028.pdf
13. NR SR – Národná rada Slovenskej republiky, 2018. *Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov*. Dostupné na: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/
14. PETERSEN, R. – SANTOS, D. – SMITH, M. C. – WETZEL, K. A. – WITTE, G., 2020. *Kompetenčný rámec pre kybernetickú bezpečnosť (NICE koncepcia)*. Špeciálna publikácia NIST č. 800-181, verzia 1. Gaithersburg, MD: National Institute of Standards and Technology.

Mladá veda

Young Science

ISSN 1339-3189