UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ

2026

Návrh úloh k Akčnému plánu k Národnej stratégii kybernetickej bezpečnosti na roky 2026 – 2030

(odborné stanovisko)

Projekt Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ (KCKB UPJŠ) financovaný Európskou úniou z prostriedkov Plánu obnovy a odolnosti Slovenskej republiky, kód projektu: 17R05-04-V01-00007.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

OBSAH

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

ÚVOD

Univerzita Pavla Jozefa Šafárika v Košiciach (ďalej len „UPJŠ“) prostredníctvom Kompetenčného centra kybernetickej bezpečnosti na UPJŠ (ďalej len „KC KB UPJŠ“) si dovoľuje reagovať na žiadosť Ministerstva školstva, výskumu, vývoja a mládeže SR o zaslanie návrhov opatrení do **Akčného plánu k Národnej stratégii kybernetickej bezpečnosti na roky 2026 – 2030**. V žiadosti sa uvádza, že vysokého školstva sa v rámci národnej stratégie dotýka predovšetkým Pilier 4: Vzdelávanie, zručnosti a povedomie.

Podľa poskytnutých informácií je cieľom pripravovaného akčného plánu systematicky posilniť kapacity vo vzdelávaní a v rozvoji odborných zručností v oblasti kybernetickej bezpečnosti, a to najmä prostredníctvom modernizácie študijných programov, podpory interdisciplinárneho vzdelávania, rozvoja praktických kompetencií a prehlbovania spolupráce medzi akademickým sektorom, verejnou správou a súkromným sektorom. Súčasne sa predpokladá zvýšenie dôrazu na budovanie bezpečnostného povedomia naprieč všetkými úrovňami vzdelávania vrátane celoživotného vzdelávania a špecializovaných tréningov pre odbornú prax.

V nadväznosti na uvedené skutočnosti KC KB UPJŠ v predkladanom materiáli navrhuje viaceré konkrétne úlohy a opatrenia, ktorých cieľom je prispieť k budovaniu udržateľného a koordinovaného ekosystému vzdelávania a výskumu v oblasti kybernetickej bezpečnosti. Tieto návrhy zároveň nepriamo smerujú k zvýšeniu úrovne ochrany a odolnosti Slovenskej republiky voči kybernetickým bezpečnostným hrozbám, a to prostredníctvom systematického rozvoja ľudských zdrojov, podpory výskumných aktivít a efektívnejšieho prepojenia teórie s praxou.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1 PREDSTAVENIE KC KB UPJŠ

Kompetenčné centrum kybernetickej bezpečnosti na Univerzite Pavla Jozefa Šafárika v Košiciach predstavuje kompetenčné centrum, v rámci ktorého sú realizované aktivity zamerané na vzdelávanie, výskum a expertnú činnosť v oblasti informačnej a kybernetickej bezpečnosti, ochrany dát, kyberkriminality a ochrany pred dezinformáciami. Súčasne KC KB UPJŠ realizuje medzinárodnú spoluprácu s akademickými partnermi zo zahraničia a poskytuje konzultácie pre možnosť prípravy a podania projektov v oblasti kybernetickej bezpečnosti.

Vytvorenie KC KB UPJŠ reflektuje viacero problémov, ktoré možno v súčasnosti identifikovať v oblasti informačnej a kybernetickej bezpečnosti (ďalej aj „KIB“):

- zvýšenie bezpečnostného povedomia relevantných subjektov zahŕňajúcich predovšetkým zamestnancov verejnej správy a študentov vysokoškolského a stredoškolského štúdia,
- vzdelávanie a výchova nových odborníkov pôsobiacich v tejto oblasti,
- výskum kybernetických hrozieb a identifikácia adekvátnych reakcií na tieto hrozby,
- zvýšenie operatívnej bezpečnosti v rámci verejnej správy poskytovaním expertných činností zo strany CSIRT tímu.

V rámci KC KB UPJŠ sa pripravoval študijný plán magisterského stupňa študijného programu aplikovaná informatika, ktorého jedna vetva sa zameriava na kybernetickú bezpečnosť. K tomuto študijnému plánu budú vytvorené, resp. modifikované viaceré predmety. Súčasne sa ako výstup kompetenčného centra vytvára ponuka **vzdelávania** pre rôzne cieľové skupiny zamestnancov verejnej správy.

V kontexte projektu sa súčasne posilňuje **spolupráca so strednými školami**, najmä vo forme činnosti **KyberTímov**, ich vzdelávania a následného zapojenia do šírenia bezpečnostného povedomia medzi širokou verejnosťou.

V rámci vzdelávacích aktivít sa sumarizujú nové poznatky a skúsenosti z oblasti KIB, ale aj príbuzných oblastí. Tie sú aktuálne doplnené o rôzne formy zážitkového vzdelávania.

V rámci **výskumnej** činnosti dochádza v už existujúcich výskumných oblastiach k publikovaniu viacerých vedeckých výstupov a k vytvoreniu nových možných výskumných spoluprác na posilnenie výskumného a vývojového potenciálu KC KB UPJŠ.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

2 NÁVRH ÚLOH

Táto kapitola predstavuje súbor návrhov úloh do Akčného plánu k Národnej stratégii kybernetickej bezpečnosti na roky 2026 – 2030 so zameraním najmä na Pilier 2: Budovanie národných kapacít a Pilier 4: Vzdelávanie, zručnosti a povedomie. Navrhované úlohy reflektujú potrebu systematického a integrovaného prístupu k rozvoju kybernetickej bezpečnosti, ktorý prepája vzdelávanie, výskum a praktickú aplikáciu v prostredí verejnej správy aj vzdelávacích inštitúcií.

Predložené návrhy vychádzajú zo skúseností akademického prostredia a kompetenčných centier kybernetickej bezpečnosti, pričom kladú dôraz na efektívne využitie existujúcich kapacít, ich koordináciu a ďalší rozvoj. Zároveň zohľadňujú aktuálne výzvy vyplývajúce z dynamického vývoja kybernetických bezpečnostných hrozieb, rastúce nároky na odborné zručnosti a potrebu systematického budovania bezpečnostného povedomia.

V rámci tohto odborného stanoviska uvádzame nasledujúce úlohy:

- Systematické využitie kompetenčných centier kybernetickej bezpečnosti na poskytovanie expertných služieb, metodickej podpory a vzdelávania pre verejnú správu.
- Zriadenie virtuálneho akademického CSIRT tímu na podporu preventívnych a reaktívnych činností a zvýšenie odolnosti vzdelávacích inštitúcií.
- Zavedenie predmetu zameraného na kybernetickú a informačnú bezpečnosť pre študentov všetkých študijných odborov vysokých škôl.
- Zavedenie predmetu zameraného na kybernetickú a informačnú bezpečnosť pre žiakov stredných škôl.
- Systematická podpora výskumu v oblasti kybernetickej a informačnej bezpečnosti so zameraním na nové technológie a hrozby.
- Vytvorenie prepojeného vzdelávacieho ekosystému medzi strednými a vysokými školami v oblasti kybernetickej bezpečnosti.
- Zvyšovanie odolnosti základných a stredných škôl voči kybernetickým hrozbám a incidentom.
- Podpora odborných kapacít školských IT pracovníkov (správcov digitálnych technológií a digitálnych koordinátorov) v oblasti kybernetickej bezpečnosti.

2.1 NÁVRH ÚLOHY Č. 1

Kód úlohy	*Bude vyplnený po spracovaní všetkých úloh Akčného plánu a bude určený na základe príslušnosti k danému pilieru a cieľu.*
Cieľ	Pilier 4 – Vzdelávanie, zručnosti a povedomie Cieľ 4.1: Budovanie národných znalostných kapacít a vzdelávanie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

	Pilier 2 - Budovanie národných kapacít v oblasti kybernetickej bezpečnosti Cieľ 2.1: Integrovaná architektúra riadenia kybernetickej bezpečnosti Cieľ 2.3: Reakcia na kybernetické bezpečnostné incidenty, kybernetické krízy a spolupráca s justičnými orgánmi
Popis úlohy	Systematické využitie existujúcich Kompetenčných centier kybernetickej bezpečnosti na poskytovanie expertných služieb, metodickej podpory a vzdelávania zamestnancov verejnej správy.
Ako úloha prispeje k cieľu	Úloha posilní odborné kapacity verejnej správy, zvýši kvalitu rozhodovania a reakcie v oblasti kybernetickej bezpečnosti a podporí zvyšovanie bezpečnostného povedomia zamestnancov verejnej správy.
Spôsob naplnenia	• realizácia školení, workshopov, • realizácia expertných konzultácií, • realizácia expertnej činnosti.
Zodpovedný subjekt	Ministerstvo školstva, výskumu, vývoja a mládeže SR Ministerstvo investícií, regionálneho rozvoja a informatizácie SR
Spolupracujúce subjekty	Vysoké školy / kompetenčné centrá na vysokých školách, KC KB
Termín	Priebežne (2026 – 2030)
Zdroj financovania	Štátny rozpočet, prostriedky EÚ
Monitoring	*Na základe dohody.*

2.2 NÁVRH ÚLOHY Č. 2

Kód úlohy	*Bude vyplnený po spracovaní všetkých úloh Akčného plánu a bude určený na základe príslušnosti k danému pilieru a cieľu.*
Cieľ	Pilier 2 – Budovanie národných kapacít Cieľ 2.3: Reakcia na kybernetické bezpečnostné incidenty, kybernetické krízy a spolupráca s justičnými orgánmi
Popis úlohy	Zriadenie virtuálneho akademického CSIRT tímu zapojeného do preventívnych a reaktívnych činností za účelom zvyšovania odolnosti vzdelávacích inštitúcií voči kybernetickým hrozbám.

Ako úloha prispeje k cieľu	Úloha prispeje k zvýšeniu odolnosti vzdelávacích inštitúcii voči kybernetickým hrozbám.
Spôsob naplnenia	• riešenie kybernetických bezpečnostných incidentov • spolupráca v oblasti implementácie bezpečnostných opatrení • spolupráca s národným a sektorovými CSIRT tímami
Zodpovedný subjekt	Ministerstvo školstva, výskumu, vývoja a mládeže SR Ministerstvo investícií, regionálneho rozvoja a informatizácie SR Národný bezpečnostný úrad
Spolupracujúce subjekty	Vysoký školy
Termín	Priebežne (2026 – 2030)
Zdroj financovania	Štátny rozpočet, prostriedky EÚ
Monitoring	*Na základe dohody.*

2.3 NÁVRH ÚLOHY Č. 3

Kód úlohy	*Bude vyplnený po spracovaní všetkých úloh Akčného plánu a bude určený na základe príslušnosti k danému pilieru a cieľu.*
Cieľ	Pilier 4 – Vzdelávanie, zručnosti a povedomie Cieľ 4.1: Budovanie národných znalostných kapacít a vzdelávanie
Popis úlohy	Zavedenie voliteľného alebo povinne voliteľného predmetu zameraného na informačnú a kybernetickú bezpečnosť pre študentov všetkých študijných odborov vysokých škôl.
Ako úloha prispeje k cieľu	Úloha zvýši základnú úroveň bezpečnostného povedomia absolventov vysokých škôl bez ohľadu na ich odborné zameranie.
Spôsob naplnenia	• príprava jednotnej osnovy predmetu, • vyškolenie pedagógov vysokých škôl, • pilotné zavedenie na vybraných univerzitách, • rozšírenie na všetkých vysokých školách.
Zodpovedný subjekt	Ministerstvo školstva, výskumu, vývoja a mládeže SR

Spolupracujúce subjekty	Vysoké školy, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
Termín	Priebežne (2026 – 2030)
Zdroj financovania	Štátny rozpočet, prostriedky EÚ
Monitoring	*Na základe dohody.*

2.4 NÁVRH ÚLOHY Č. 4

Kód úlohy	*Bude vyplnený po spracovaní všetkých úloh Akčného plánu a bude určený na základe príslušnosti k danému pilieru a cieľu.*
Cieľ	Pilier 4 – Vzdelávanie, zručnosti a povedomie Cieľ 4.1: Budovanie národných znalostných kapacít a vzdelávanie
Popis úlohy	Zavedenie predmetu zameraného na informačnú a kybernetickú bezpečnosť pre žiakov stredných škôl.
Ako úloha prispeje k cieľu	Úloha zvýši základnú úroveň bezpečnostného povedomia absolventov stredných škôl bez ohľadu na ich odborné zameranie.
Spôsob naplnenia	• príprava jednotnej osnovy predmetu, • vyškolenie pedagógov stredných škôl, • pilotné zavedenie na vybraných stredných školách, • rozšírenie na všetkých stredných školách.
Zodpovedný subjekt	Ministerstvo školstva, výskumu, vývoja a mládeže SR
Spolupracujúce subjekty	Vysoký školy, stredné školy, zriaďovatelia, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
Termín	Priebežne (2026 – 2030)
Zdroj financovania	Štátny rozpočet, prostriedky EÚ
Monitoring	*Na základe dohody.*

2.5 NÁVRH ÚLOHY Č. 5

Kód úlohy	*Bude vyplnený po spracovaní všetkých úloh Akčného plánu a bude určený na základe príslušnosti k danému pilieru a cieľu.*
Cieľ	Pilier 4 – Vzdelávanie, zručnosti a povedomie Cieľ 4.1: Budovanie národných znalostných kapacít a vzdelávanie
Popis úlohy	Systematická podpora výskumu v oblasti kybernetickej a informačnej bezpečnosti so zameraním na nové technológie, kybernetické hrozby a ochranné mechanizmy.
Ako úloha prispeje k cieľu	Úloha posilní technologickú suverenitu SR v oblasti kybernetickej bezpečnosti a obrany štátu a podporí vznik inovatívnych riešení využiteľných v praxi. To bude mať pozitívny vplyv aj na vzdelávací proces na vysokých školách.
Spôsob naplnenia	• vyhlasovanie výskumných výziev v oblasti kybernetickej bezpečnosti, • podpora interdisciplinárnych tímov z viacerých vysokých škôl pri riešení konkrétnych výskumných otázok • podpora zapájania výskumných tímov do medzinárodných projektov
Zodpovedný subjekt	Ministerstvo školstva, výskumu, vývoja a mládeže SR
Spolupracujúce subjekty	Vysoký školy, Slovenská akadémia vied, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
Termín	Priebežne (2026 – 2030)
Zdroj financovania	Štátny rozpočet, prostriedky EÚ
Monitoring	*Na základe dohody.*

2.6 NÁVRH ÚLOHY Č. 6

Kód úlohy	*Bude vyplnený po spracovaní všetkých úloh Akčného plánu a bude určený na základe príslušnosti k danému pilieru a cieľu.*
Cieľ	Pilier 4 – Vzdelávanie, zručnosti a povedomie Cieľ 4.1: Budovanie národných znalostných kapacít a vzdelávanie

Popis úlohy	Vytvorenie prepojeného vzdelávacieho ekosystému medzi strednými a vysokými školami v oblasti kybernetickej a informačnej bezpečnosti.
Ako úloha prispeje k cieľu	Úloha podporí zvýšenie kvality vzdelávania kybernetickej a informačnej bezpečnosti na stredných školách a zabezpečí kontinuitu vzdelávania a včasnú identifikáciu talentov v oblasti kybernetickej a informačnej bezpečnosti.
Spôsob naplnenia	• organizácia letných škôl a iných vzdelávacích a popularizačných aktivít. • organizácia súťaží v oblasti kybernetickej bezpečnosti, • mentoring pedagógov a žiakov stredných škôl zo strany vysokých škôl.
Zodpovedný subjekt	Ministerstvo školstva, výskumu, vývoja a mládeže SR
Spolupracujúce subjekty	Vysoký školy, stredné školy, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
Termín	Priebežne (2026 – 2030)
Zdroj financovania	Štátny rozpočet, prostriedky EÚ
Monitoring	*Na základe dohody.*

2.7 NÁVRH ÚLOHY Č. 7

Kód úlohy	*Bude vyplnený po spracovaní všetkých úloh Akčného plánu a bude určený na základe príslušnosti k danému pilieru a cieľu.*
Cieľ	Pilier 2: Budovanie národných kapacít v oblasti kybernetickej bezpečnosti Cieľ 2.3: Reakcia na kybernetické bezpečnostné incidenty, kybernetické krízy a spolupráca s justičnými orgánmi
Popis úlohy	Zvyšovanie odolnosti základných a stredných škôl v oblasti kybernetickej a informačnej bezpečnosti, najmä zvýšenie schopnosti predchádzať, detegovať, odolávať a zotaviť sa z kybernetických hrozieb a kybernetických bezpečnostných incidentov.
Ako úloha prispeje k cieľu	Úloha prispeje k zvýšeniu odolnosti základných a stredných škôl voči kybernetickým hrozbám, ako aj k ochrane detí a mládeže v digitálnom

	priestore a k znižovaniu rizík kybernetických bezpečnostných incidentov v školskom prostredí.
Spôsob naplnenia	• realizácia analýzy existujúceho stavu kybernetickej a informačnej bezpečnosti na základných a stredných školách. • realizácia prieskum stavu ohrozenia detí a mládeže v kybernetickom priestore na základe široko spektrálneho prieskumu. • vzdelávanie pedagógov základných a stredných škôl, • tvorba metodických materiálov pre základné a stredné školy, • spolupráca v oblasti implementácie bezpečnostných opatrení a riešenia kybernetických bezpečnostných incidentov.
Zodpovedný subjekt	Ministerstvo školstva, výskumu, vývoja a mládeže SR
Spolupracujúce subjekty	Základné a stredné školy, zriaďovatelia, Národné centrum pre digitálnu transformáciu vzdelávania
Termín	Priebežne (2026 – 2030)
Zdroj financovania	Štátny rozpočet, prostriedky EÚ
Monitoring	*Na základe dohody.*

2.8 NÁVRH ÚLOHY Č. 8

Kód úlohy	*Bude vyplnený po spracovaní všetkých úloh Akčného plánu a bude určený na základe príslušnosti k danému pilieru a cieľu.*
Cieľ	Pilier 4 – Vzdelávanie, zručnosti a povedomie Cieľ 4.1: Budovanie národných znalostných kapacít a vzdelávanie
Popis úlohy	Podpora školského správcu digitálnych technológií a školského digitálneho koordinátora v oblasti kybernetickej a informačnej bezpečnosti.
Ako úloha prispeje k cieľu	Úloha prispeje k zvýšeniu odbornosti osôb zapojených do vnútorných procesov súvisiacich s oblasťou kybernetickej a informačnej bezpečnosti a následne k zvýšeniu odolnosti základných a stredných škôl voči kybernetickým hrozbám.
Spôsob naplnenia	• realizácia vzdelávania školského správcu digitálnych technológií a školského digitálneho koordinátora, • realizácia odborných konzultácií.

Zodpovedný subjekt	Ministerstvo školstva, výskumu, vývoja a mládeže SR
Spolupracujúce subjekty	Základné a stredné školy, zriaďovatelia, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti, Národné centrum pre digitálnu transformáciu vzdelávania
Termín	Priebežne (2026 – 2030)
Zdroj financovania	Štátny rozpočet, prostriedky EÚ
Monitoring	*Na základe dohody.*

ZÁVER

Navrhované úlohy predstavujú ucelený a vzájomne prepojený rámec opatrení, ktorý reaguje na aktuálne potreby Slovenskej republiky v oblasti kybernetickej a informačnej bezpečnosti. Ich spoločným menovateľom je dôraz na systematické budovanie odborných kapacít, rozvoj vzdelávania na všetkých úrovniach a posilnenie spolupráce medzi akademickým prostredím, verejnou správou a ďalšími relevantnými aktérmi. Takto koncipovaný prístup umožňuje nielen efektívnejšie využitie existujúcich zdrojov, ale aj ich ďalší rozvoj a koordináciu v súlade s národnými strategickými cieľmi.

Významným prínosom navrhovaných opatrení je ich orientácia na prepojenie teórie s praxou, čo sa odráža najmä v návrhoch na zapojenie kompetenčných centier kybernetickej bezpečnosti, zriadenie akademických CSIRT tímov a podporu aplikovaného výskumu. Tieto prvky prispievajú k posilneniu schopnosti štátu efektívne reagovať na kybernetické bezpečnostné hrozby a kybernetické bezpečnostné incidenty. Zároveň sa kladie dôraz na budovanie bezpečnostného povedomia a základných digitálnych kompetencií už od úrovne základného a stredného školstva, čím sa vytvára predpoklad pre dlhodobé zvyšovanie odolnosti spoločnosti.

Dôležitým aspektom je aj podpora kontinuity vzdelávania a identifikácie talentov, a to prostredníctvom vytvárania prepojeného vzdelávacieho ekosystému medzi strednými a vysokými školami. Tento prístup umožňuje systematicky rozvíjať odborníkov v oblasti kybernetickej a informačnej bezpečnosti a reagovať na rastúci dopyt po kvalifikovaných pracovných silách.

Implementácia navrhovaných úloh si vyžaduje koordinovaný prístup zodpovedných subjektov, stabilné financovanie a priebežné monitorovanie ich plnenia. V tomto kontexte je nevyhnutné zabezpečiť efektívnu spoluprácu medzi ministerstvami, akademickými inštitúciami (vrátane kompetenčných centier kybernetickej bezpečnosti) a ďalšími súkromnými a verejnoprávnymi partnermi, ako aj vytvoriť mechanizmy na hodnotenie ich prínosu a dopadu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

POUŽITÉ ZDROJE

[1] Národný bezpečnostný úrad. (2021). *Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025*. Dostupné na: https://www.nbu.gov.sk/narodna-strategia-kybernetickej-bezpecnosti-na-roky-2021-az-2025/

[2] Národný bezpečnostný úrad. (2021). *Akčný plán kybernetickej bezpečnosti na roky 2021 až 2025*. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Akcny-plan-kybernetickej-bezpecnosti.pdf

[3] Národný bezpečnostný úrad. (2023). *Odpočet implementácie akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025*. Dostupné na: https://www.nbu.gov.sk/data/att/398.pdf

[4] Národný bezpečnostný úrad. (2026). *Národná stratégia kybernetickej bezpečnosti na roky 2026 – 2030*. Dostupné na: https://rokovania.gov.sk/RVL/Material/31549/1

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY