Vytvorenie Kompetenčného centra kybernetickej bezpečnosti

Vzor Kompetenčného centra kybernetickej bezpečnosti

MIRRI, Bratislava, 2022

Obsah

[**1 Zdôvodnenie vytvorenia Kompetenčného centra kybernetickej bezpečnosti** 3](#_Toc114671048)

[**2 Zariadenie a vybavenie Kompetenčného centra** 7](#_Toc114671049)

[**3 Výzva na vytvorenie Kompetenčného centra** 10](#_Toc114671050)

# **1 Zdôvodnenie vytvorenia Kompetenčného centra kybernetickej bezpečnosti**

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „MIRRI“) ako realizátor Reformy č. 5 „Skvalitnenie vzdelávania a zabezpečenie spôsobilosti v oblasti KIB „Komponentu 17 , Plánu obnovy a odolnosti Slovenskej republiky, , pripravuje **Výzvu na vytvorenie Kompetenčných centier kybernetickej bezpečnosti** (ďalej len „výzva“).

Výzva by mala umožniť čerpanie finančných prostriedkov z mechanizmu na vybudovanie a prevádzku Kompetenčných centier kybernetickej bezpečnosti (ďalej len „Kompetenčné centrá“) na vysokých školách pôsobiacich v Slovenskej republike (ďalej len „VŠ“). Budú zamerané najmä:

* na systematickú spoluprácu pri vzdelávaní pre zabezpečenie potrebných kapacít a zručností,
* metodickej pomoci verejnej správe,
* vývoj nových bezpečnostných riešení a
* nadviazanie medzinárodnej spolupráce s relevantnými medzinárodnými centrami excelentnosti a využívanie ich expertíz.

Hlavnými výzvami sú:

* vzdelávanie v oblasti kybernetickej a informačnej bezpečnosti (ďalej len „KIB“) je nedostatočné,
* absencia programu vzdelávania a zvyšovania bezpečnostného povedomia vrátane testovania znalostí (verejná správa, manažéri KIB, špecialisti KIB, bezpečnostné povedomie zamestnancov a verejnosti, príprava KIB expertov, oblasť boja proti dezinformáciám a kyberšikane, spolupráca so súkromným sektorom),
* absencia celoživotného vzdelávania ako podpora pre počiatočné nastavenie úrovne a dlhodobú udržateľnosť kompetencií v oblasti KIB,
* nedostatok kapacít kvalifikovaných odborníkov na centrálnej úrovni aj na kľúčových rezortoch,
* absencia odbornej spolupráce s univerzitami a akademickou obcou a investície do spoločných projektov v oblasti monitorovania talentovaných študentov,
* chýba vhodný organizačný model riadenia KIB a kompetenčné centrá (centrá excelentnosti) pre KIB na vysokých školách v SR v prostredí verejnej správy.

Dôvodom vytvárania Kompetenčných centier je spolupráca pri vzdelávaní a metodickej pomoci verejnej správe, pre zabezpečenie potrebných kapacít a zručností, ako aj vývoj nových bezpečnostných riešení a nadviazanie medzinárodnej spolupráce s relevantnými medzinárodnými centrami excelentnosti v oblasti boja proti kybernetickým a hybridným hrozbám, a využívanie ich expertíz. Medzi ďalšie dôvody je možné zaradiť aj zapojenie odborne kvalifikovaných pracovníkov do pracovných skupín zameraných na problematiku KIB v SR i EÚ.

Vytvorením Kompetenčných centier v nadväznosti na už uvedené, je možné zároveň:

1. sústreďovať odborné personálne kapacity v oblasti KIB,
2. riešiť strategické úlohy v oblasti KIB,
3. pripravovať odborníkov pre potreby verejnej správy,
4. vzdelávať jednotlivcov z praxe v oblasti KIB,
5. sústreďovať a vyvíjať špičkového výskumu v oblasti KIB,
6. spolupracovať so zahraničím,
7. pripravovať materiály a dokumentáciu pre vzdelávanie v oblasti kybernetickej bezpečnosti (obsah a metodika vzdelávania, študijné materiály) a
8. vykonávať iné súvisiace úlohy.

Otvára sa tak široké spektrum možností pre realizáciu ďalších činností, okrem už uvedených, ktorých výstupy by mohli byť ďalším významným prínosom Reformy Vzdelávania, i keď nad rámec požiadaviek Plánu obnovy a odolnosti SR, ale ktoré je však možné považovať za dôležité pri dosahovaní kvalitného vzdelávania a poskytovania materiálov a metodických usmernení pre celú verejnú správu. Prehľad a popis jednotlivých činností je uvedený v tabuľke č. 1.

Tabuľka č. 1 Opis činností Kompetenčného centra

|  |  |
| --- | --- |
| **Činnosti** Kompetenčných centier | **Opis činností**  |
| Príprava špecialistov  | * podpora vzdelávania na vysokých školách a v rámci celoživotného vzdelávania (kontinuálne vzdelávanie),
* metodická a kapacitná podpora zriadenia, implementácie a výučby v rámci špecializovaných študijných programov a predmetov z oblasti kybernetickej bezpečnosti a pod.
 |
| Spolupráca so zahraničím  | * vzájomná výmena informácií a poznatkov,
* spoločné projekty alebo v podobe pozorovania či hodnotenia pri vyhodnocovaní politík a opatrení vo verejnej správe,
* spoločné výskumné projekty a výstupy, ktoré môžu priniesť dodatočné financovanie a odborné kapacity a pod.
 |
| Výskumná činnosť  | * sústredenie a vývoj špičkového výskumu v oblasti kybernetickej a informačnej bezpečnosti,
* realizácia základného a aplikovaného výskumu, čím sa vytvorí sústredenie výskumníkov v danej oblasti,
* hľadanie spôsobov a kapacít na rozšírenie výskumných oblastí s ohľadom na aktuálne trendy,
* prehĺbenie spolupráce medzi akademickým a súkromným sektorom v oblasti kybernetickej bezpečnosti,
* získanie nových poznatkov z oblasti kybernetickej bezpečnosti a pod.
 |
| Expertná činnosť  | * expertná činnosť pre orgány verejnej správy v oblasti kybernetickej a informačnej bezpečnosti,
* riešenie strategických úloh v oblasti kybernetickej a informačnej bezpečnosti,
* podieľanie sa na príprave správ, koncepcií  a formovaní legislatívnych dokumentov v oblasti kybernetickej a informačnej bezpečnosti, či už v podobe účastí v expertných skupinách, pripomienkovania alebo odborných stanovísk k zaslaným dokumentom a pod.
 |
| Udržiavanie terminológie  | * udržiavanie konzistentnej terminológie a rozširovanie tezauru kybernetickej a informačnej bezpečnosti prostredníctvom udržiavania systému na tvorbu slovníkov a publikovania výkladového slovníka kybernetickej a informačnej bezpečnosti,
* vydávanie špecializovaných slovníkov ako príloh učebníc, koncepcií, metodických materiálov a pod.
 |
| Celoživotné vzdelávanie  | * flexibilný systém celoživotného vzdelávania (kontinuálneho vzdelávania) pre skupiny ľudí s rozličnými potrebami vzhľadom na rozsah kurzov, ich zameranie a úroveň expertízy,
* základné kurzy pre širokú verejnosť v oblasti kybernetickej a informačnej bezpečnosti a pod.
 |
| Odborné poradenstvo  | * odborné poradenstvo pri príprave a implementácii projektov realizovaných najmä akademickým sektorom so zameraním na štruktúrované štrukturálne fondy EÚ, Plán obnovy a odolnosti, ale aj cezhraničné fondy a tzv. bruselské výzvy ako napr. Horizon2020 European Research Council.
 |
| Prínosy Kompetenčného centra | * zvyšovanie bezpečnostného povedomia,
* zvyšovanie kybernetickej odolnosti sektora verejnej správy,
* zvyšovanie odbornej úrovne bezpečnostných špecialistov KIB,
* zvyšovanie bezpečnostného povedomia používateľov  verejnej správy,
* sústredenie odborných kapacít v kybernetickej a informačnej bezpečnosti,
* rozvoj medzinárodnej spolupráce prostredníctvom tvorby konzorcií na podávanie projektov, výmenných pobytov výskumníkov alebo stážistov, účasti v sieti podobne zameraných centier, či výmenu know-how v oblasti kybernetickej a informačnej bezpečnosti,
* budovanie a rozvíjanie odbornej komunity prostredníctvom odborných seminárov a konferencií pre širokú, ale aj expertnú verejnosť a pod.
 |

# **2 Zariadenie a vybavenie Kompetenčného centra**

Za účelom plnenia činností a úloh Kompetenčného centra je potrebné zabezpečiť priestor,
v ktorom bude Kompetenčné centrum vytvorené a vybaviť ho potrebnou infraštruktúrou technickými a technologickými zariadeniami či personálnymi kapacitami.

1. **Priestorové zabezpečenie, v ktorom bude vytvorené Kompetenčné centrum**

Priestor, v ktorom bude vytvorené Kompetenčné centrum má byť majetkom žiadateľa/VŠ
vo vlastníctve alebo v prenájme, čo je žiadateľ povinný preukázať.

Akceptované sú len minimálne stavebné úpravy vnútorného priestoru.

1. **Infraštruktúra, resp. technické zázemie projektu - Vybavenie Kompetenčného centra v rozsahu napr.:**
* nábytok, zariadenia:
	+ skrine, poličky,
	+ katedra,
	+ pracovné stoly,
	+ stoličky,
	+ tabule (interaktívna, keramická, dataprojektor a pod.),
	+ nástenky,
	+ kancelárske potreby,
	+ špecializované výučbové pomôcky, školiace materiály, školiace potreby,
	+ žalúzie;
* infraštruktúra:
	+ elektroinštalácia, zdroj napätia a elektrického prúdu, panely s elektrickými zásuvkami,
	+ pripojenie na internet, počítačová sieť (LAN, pokrytie WiFi), dátové zásuvky,
	+ kabeláž,
	+ požiarna ochrana,
	+ sieťové zariadenia a sieťová infraštruktúra,
	+ zariadenia pre fyzickú a objektovú bezpečnosť (zámky, požiarne a bezpečnostné dvere, alarmy a detektory pohybu, brány na vstup cez prístupové karty, kamerový systém a pod.),
	+ predlžovacie káble;
* softvérové a hardvérové vybavenie:
	+ HW a SW pre sieťové služby,
	+ aktívne sieťové komponenty,
	+ bezpečnosť sietí (zariadenia a softvér pre bezpečnosť a bezpečnostný monitoring samotného Kompetenčného centra),
	+ softvérová a hardvérová podpora bezpečnosti samotného Kompetenčného centra (firewally, SIEM/IDS/IPS a pod.)
	+ pracovné stanice a vybavenie - počítače/notebooky, webkamery, klávesnice, myši, tablety, LCD monitory, tlačiarne, skenery,
	+ prezentačná technika, TV obrazovky,
	+ virtualizácia, OS, a aplikácie,
	+ SW a HW podpora, licencie,
	+ výučbové a prezentačné softvérové nástroje,
	+ SW, HW pre riadenie dokumentácie, poskytovanie web služieb a zabezpečenie emailovej komunikácie,
	+ komunikačné nástroje na online výučbu,
	+ grafický editor, softvérové nástroje na tvorbu publikácií a kníh,
	+ nástroje na vizualizáciu a analýzu procesov a nástroje na vizualizáciu a analýzu topológie sietí,
	+ servery a infraštruktúra a podporné technológie a priestory na ich umiestnenie (technologické miestnosti, priestory v datacentre),
	+ diskové polia a diskové úložiská, prepínače pre servery a infraštruktúru a pod.,
	+ klimatizačné zariadenia,
	+ záložné zdroje UPS;
* špecializované nástroje/ softvér pre oblasť kybernetickej bezpečnosti:
	+ nástroje na
		- simuláciu a výpočty,
		- riadenie aktív,
		- riadenie a analýzu rizík , hrozieb a zraniteľností,
		- detegovanie a zaznamenávanie existujúcich zraniteľností technických prostriedkov,
		- riadenie zmien, riadenie záplat a aktualizácií, riadenie kapacít a pod.,
		- riadenie prístupov,
		- bezpečnostný monitoring siete, detekciu anomálií, monitoring aplikácií,
		- monitoring priemyselného prostredia (SIEM, Log manažment a pod.),
		- riešenie a vyšetrovanie kybernetických bezpečnostných incidentov,
		- forenznú analýzu a forenzné vyšetrovanie,
		- penetračné testovanie, sociálne inžinierstvo,
		- analýzu OSINT, a
		- ďalšie špecializované nástroje na výučbu, výskum a vývoj v oblasti KIB.

V prípade špecializovaného vybavenia Kompetenčného centra bude oprávneným výdavkom aj uvedenie do prevádzky a zaškolenie personálu.

*Pozn.:*

*Ide o uvedenie zoznamu najdôležitejších zariadení, prístrojov a iného vybavenia (spolu
so stručným opisom ich funkcií a vlastností), ktoré súvisia s napĺňaním cieľov výzvy. Žiadateľ v rámci projektu uvedie zoznam zariadení, prístrojov a iného vybavenia, ktoré bude v súlade s Projektovým zámerom na vytvorenie Kompetenčného centra.*

1. **Dostupné odborné, riadiace a administratívne kapacity - Organizačné a personálne zabezpečenie** (v kompetencii VŠ – zamestnanci VŠ)

Riadiace a administratívne kapacity:

* projektový manažér,
* finančný manažér,
* pracovník pre verejné obstarávanie,
* manažér pre monitorovanie projektu,
* manažér publicity projektu/komunikačný manažér projektu, asistenti a zamestnanci pre ďalšie podporné služby (napr. personalistika, účtovníctvo mzdy),

Odborné kapacity:

* garant projektu – zodpovedná osoba za zachovanie kvality výstupu aktivity z hľadiska jej odbornosti,
* interný odborný personál (členovia projektu) – zamestnaní na základe TPP alebo dohôd,
* odborné externé kapacity (experti, konzultanti) – pokiaľ nie sú súčasťou interného tímu,
* odborný technický personál na zabezpečenie chodu infraštruktúry Kompetenčného centra (administrátori, podpora sieťových služieb, technici a pod.),

Pozn.:

Podmienkou bude:

* Vypracovanie pracovných balíkov (personálnej matice) s popisom činností/aktivít,
na ktorej sa odborný pracovník bude podieľať, predpokladaný rozsah práce v hodinách a preukázaním požadovanej odbornosti (opis kompetentnosti).
* Určenie, kto bude po vytvorení Kompetenčného centra (po ukončení projektu) jeho garantom/vedúcim, kto bude oprávnený vstupovať do Kompetenčného centra, vykonávať ďalšie činnosti (vzdelávanie, veda a výskum a pod.).
* Kooperácia, komplementarita a zastupiteľnosť.

Možné výdavky projektu:

* kapitálové výdavky,
* mzdové náklady a účtovníctvo, odpisy,
* pracovné cesty – tuzemské, zahraničné,
* nájom zariadenia a vybavenia (ak sa vyžaduje),
* nájom priestorov na realizáciu aktivity,
* spotrebný a prevádzkový materiál,
* telekomunikačné poplatky, poštovné, konektivita na internet,
* energie, údržba,
* právne poradenstvo,
* letáky, plagáty, brožúrky, označovanie projektu ,
* expertízy,
* ostatné výdavky súvisiace s vytváraním a prevádzkou Kompetenčného centra (napr.
na upratovacie služby, zabezpečením nápojov a stravy),
* dopravné prostriedky,
* webová stránka projektu určená pre publicitu projektu.

*Pozn.:*

*Činnosť Kompetenčných centier nie je možné komercionalizovať.*

# **3 Výzva na vytvorenie Kompetenčného centra**

V rámci výzvy na predkladanie žiadostí o poskytnutie prostriedkov mechanizmu, ktorá bude financovaná z Plánu obnovy a ktorú pripravuje MIRRI, bude potrebné splniť podmienky stanovené výzvou a zároveň predložiť žiadosť o prostriedky mechanizmu. Prílohou tejto žiadosti bude, okrem iného, **Projektový zámer** vybudovania Kompetenčného centra, v ktorom žiadateľ popíše:

* vytvorenie Kompetenčného centra;
* personálne a technické vybavenie Kompetenčného centra;
* fungovanie prevádzky vybudovaného Kompetenčného centra v rámci doby realizácie projektu, ktorá bude stanovená na maximálne 24 mesiacov;
* fungovanie prevádzky vybudovaného Kompetenčného centra po ukončení realizácie projektu, t. j. v dobe udržateľnosti, ktorá bude stanovená na 3 roky.

Prílohou Projektového zámeru bude **rozpočet** zostavený v zmysle Príručky pre žiadateľa, resp. pravidiel oprávnenosti výdavkov.

**Partnerstvo so strednými školami**

Počet prípadov útokov medzi mládežou v online prostredí vo forme kyberšikany, nevhodného obsahu (intímne alebo sexuálne explicitné obrázky či videá), sextingu (posielanie sexuálne explicitných správ a intímnych fotiek), sextortionu (útočník požaduje výkupné v opačnom prípade zverejní intímne fotografie obete), nadmerného zdieľania osobných údajov či online predátorstva, má stúpajúcu tendenciu. Preto je nevyhnutné, priam žiadúce, zvyšovať bezpečnostné povedomie medzi študentami. Cieľom je, aby študenti, v prípade kybernetického bezpečnostného incidentu obdobného charakteru, ako je už uvedené, vedeli vhodne reagovať. Jedným zo spôsobov, ako takéto zvyšovanie bezpečnostného povedomia zabezpečiť, je aj spolupráca s VŠ. Preto je podpora pri poskytovaní prostriedkov mechanizmu orientovaná na tie VŠ, ktoré už preukázateľným spôsobom spolupracujú so strednými školami v oblasti KIB. Takáto forma spolupráce VŠ so strednou školou je jedným z hodnotiacich a výberových kritérií pre odborné hodnotenie žiadostí o poskytnutie prostriedkov mechanizmu.

**Udržateľnosť výsledkov projektu**

* nadväzujúce aktivity po ukončení projektu, udržateľnosť projektu a využívanie výsledkov
po jeho ukončení

Zameranie na plánované aktivity a očakávané úžitky projektu nasledujúce po skončení realizácii projektu, ktoré budú nadväzovať na výsledky realizácie aktivít projektu. Uviesť spôsob zabezpečenia udržania kvality poskytovaných úžitkov po skončení projektu, resp. ako bude zabezpečený ich transfer do praxe. Uviesť inštitucionálne predpoklady pre výkon aktivít, ktoré generujú úžitky aj po skončení projektu.