CyberCert-CZ

Smlouva o účasti na řešení projektu

Tato smlouva o účasti na řešení projektu CyberCert-CZ je uzavřená dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném znění.

Smluvní strany:

Koordinátor projektu: **Vysoká škola báňská – Technická univerzita Ostrava**

Fakulta elektrotechniky a informatiky

se sídlem: 17. listopadu 2172/15, 708 00 Ostrava – Poruba, Česká republika

IČO: 61989100

statutární zástupce: prof. Ing. Igor Ivan, Ph.D.

funkce: rektor

(dále jen „Koordinátor“)

Partner projektu: **Elektrotechnický zkušební ústav, s. p.**

se sídlem: Pod lisem 129/2, Troja, 182 00 Praha 8, Česká republika

IČO: 00001481

statutární zástupce: Ing. Miroslav Vlasák

funkce: ředitel

(dále jen „Partner“)

Koordinátor a Partner jsou dále společně označováni jako „Smluvní strany“.

Článek I.
Předmět smlouvy

1. Předmětem této smlouvy je úprava práv a povinností Smluvních stran při společném řešení projektu s názvem „CyberCert-CZ“ (dále jen „Projekt“).

2. Cílem Projektu je vybudování a akreditace certifikačního orgánu (CB) a zkušební laboratoře (ITSEF) v oblasti kybernetické bezpečnosti v České republice.

3. Projekt je realizován na základě žádosti o podporu předložené Národnímu koordinačnímu centru a v souladu s podmínkami poskytovatele dotace.

Článek II.
Doba trvání projektu

Tato smlouva se uzavírá na dobu určitou, a to od data podpisu oběma Smluvními stranami do **31. 10. 2026**, nebo do úplného vypořádání všech práv a povinností z ní vyplývajících.

Článek III.
Práva a povinnosti smluvních stran

1. Koordinátor odpovídá a je zároveň zmocněn k:
   a) podání žádosti o podporu projektu a její administraci;
   b) celkové řízení a koordinaci Projektu, včetně svolání pracovních schůzek a kontrolních dnů;
   c) komunikaci s poskytovatelem dotace a dalšími relevantními orgány;
   d) rozdělení finančních prostředků Partnerovi dle podmínek stanovených poskytovatelem;
   e) zajištění zpracování a předkládání monitorovacích zpráv a závěrečného vyúčtování;
   f) včasné informování Partnera o všech skutečnostech, které mohou mít vliv na realizaci Projektu.
   g) zachovávání mlčenlivosti o všech skutečnostech a informacích, které se dozví v souvislosti s realizací Projektu, a které nejsou veřejně přístupné
   h) podpisu „Smlouvy o poskytnutí finanční podpory (dotace) na řešení projektu s názvem „CyberCert-CZ" s poskytovatelem dotace."

2. Partner se zavazuje:
   a) aktivně se podílet na řešení Projektu dle specifikace uvedené v dokumentu „Žádost o podporu projektu CyberCert-CZ“;
   b) plnit úkoly a činnosti v dohodnutých termínech a kvalitě;
   c) poskytovat Koordinátorovi veškerou požadovanou součinnost při administraci Projektu a plnění podmínek poskytovatele dotace;

d) vést oddělenou evidenci nákladů vztahujících se k realizaci Projektu a umožnit jejich kontrolu;
e) informovat Koordinátora bez zbytečného odkladu o všech skutečnostech, které by mohly mít vliv na plnění předmětu této smlouvy;
f) dodržovat pravidla publicity stanovená poskytovatelem dotace;
g) zachovávat mlčenlivost o všech skutečnostech a informacích, které se dozví v souvislosti s realizací Projektu, a které nejsou veřejně přístupné;
h) umožnit poskytovateli dotace, Koordinátorovi nebo jiným oprávněným subjektům provádět kontrolu plnění závazků vyplývajících z této smlouvy.

Článek IV.
Financování

1. Financování činností Partnera bude zajištěno z finančních prostředků poskytnutých poskytovatelem dotace na realizaci Projektu, a to na základě podmínek stanovených ve smlouvě o poskytnutí dotace uzavřené mezi Koordinátorem a poskytovatelem.

2. Výše a struktura finančního příspěvku Partnera, včetně způsobilých nákladů a podílu na celkovém rozpočtu Projektu, je uvedena v dokumentu „Žádost o podporu projektu CyberCert-CZ".

3. Partner je oprávněn čerpat finanční prostředky pouze na způsobilé náklady související s realizací Projektu, v souladu s pravidly stanovenými poskytovatelem dotace, touto smlouvou a platnými právními předpisy.

4. Partner je povinen vést oddělenou evidenci přijatých prostředků a nákladů vynaložených na realizaci Projektu a poskytovat Koordinátorovi potřebné podklady k finančnímu vypořádání.

5. Koordinátor uvolní finanční prostředky Partnerovi na základě splnění podmínek stanovených v příloze této smlouvy a na základě předložení řádného vyúčtování a podkladů prokazujících účelné a efektivní vynaložení prostředků.

6. Partner nese odpovědnost za správné a účelné použití poskytnutých finančních prostředků. V případě zjištění neoprávněného použití nebo nevyužití prostředků je povinen tyto prostředky vrátit Koordinátorovi.

Článek V.
Duševní vlastnictví

1. Smluvní strany se dohodly, že práva k výsledkům vzniklým v rámci řešení Projektu (dále jen „Výsledky") se řídí tímto článkem, a není nutné uzavírat samostatné ujednání.

2. Výsledky vzniklé při řešení Projektu budou společným duševním vlastnictvím Smluvních stran v poměru odpovídajícím jejich podílu na vzniku těchto Výsledků,

přičemž tento podíl bude určen na základě věcného a finančního zapojení každé ze Smluvních stran, jak je specifikováno v dokumentu „Žádost o podporu projektu CyberCert-CZ".

3. Výsledky, které vzniknou samostatnou činností jedné ze Smluvních stran bez přispění druhé Smluvní strany, budou jejím výlučným duševním vlastnictvím.

4. Smluvní strany si navzájem poskytují bezúplatnou, nevýhradní, územně neomezenou licenci k využití Výsledků pro účely nezbytné k realizaci Projektu a plnění jeho cílů, včetně možnosti využití těchto Výsledků při plnění povinností vůči poskytovateli dotace.

5. Další nakládání s Výsledky (např. jejich zveřejnění a komercializace) bude možné pouze po vzájemné písemné dohodě Smluvních stran, která nebude bezdůvodně odepřena.

6. Smluvní strany se zavazují zajistit ochranu důvěrných informací, know-how a Výsledků vzniklých v rámci řešení Projektu, a to i po ukončení této smlouvy. Smluvní strany nebudou bez předchozího písemného souhlasu druhé Smluvní strany tyto informace a Výsledky zpřístupňovat třetím osobám ani je využívat jinak, než je stanoveno touto smlouvou.

7. Práva a povinnosti dle tohoto článku zůstávají v platnosti i po ukončení této smlouvy.

Článek VI.
Závěrečná ustanovení

1. Tato smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma Smluvními stranami.

2. Smlouva může být měněna pouze písemnými, očíslovanými dodatky podepsanými oběma Smluvními stranami.

3. Smluvní strany se zavazují plnit své povinnosti dle této smlouvy po celou dobu trvání Projektu, včetně plnění všech administrativních, věcných a finančních závazků, které vyplývají z této smlouvy a ze „Žádosti o podporu projektu CyberCert-CZ".

4. Veškeré právní vztahy vzniklé na základě této smlouvy se řídí právním řádem České republiky, zejména zákonem č. 89/2012 Sb., občanský zákoník, v platném znění.

5. Smluvní strany se zavazují řešit případné spory vzniklé z této smlouvy přednostně smírnou cestou. V případě, že nedojde ke smírnému řešení, budou spory řešeny věcně a místně příslušným soudem podle sídla Koordinátora.

6. Tato smlouva je vyhotovena ve dvou (2) stejnopisech s platností originálu, z nichž každá Smluvní strana obdrží jedno vyhotovení.

7. Nedílnou součástí této smlouvy jsou následující přílohy:

   a) Dokument „Žádost o podporu projektu CyberCert-cz“

V Ostravě, dne

.....
Vysoká škola báňská
Technická univerzita Ostrava
prof. Ing. Igor Ivan, Ph.D., rektor

V Praze, dne

.....
Elektrotechnický zkušební ústav, s.p.

Ing. Miroslav Vlasák, ředitel

Národní koordinační centrum

Formulář žádosti o podporu projektu

Název projektu: CyberCert-CZ

Předkladatel: Vysoká škola báňská – Technická univerzita Ostrava

1. Identifikační údaje

Název projektu: CyberCert-CZ

Název projektu – anglicky: CyberCert-CZ

1.1. Identifikace oblasti aktivit dle výzvy

- Budování a akreditace zkušebních laboratoří (ITSEF)
- Budování a akreditace certifikačních orgánů (CBs)

1.2. Název a IČO zapojených subjektů

Elektrotechnický zkušební ústav, s. p.
Pod lisem 129/2,
Troja, 182 00 Praha 8
Česká republika
IČO: 00001481

Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky (FEI)
17. listopadu 2172/15
708 00 Ostrava-Poruba
Česká republika
IČO: 61989100

2. Představení projektu

2.1. Předpokládaná doba trvání projektu

Předpokládané datum zahájení dílčího projektu: 1.5.2025
Předpokládané datum ukončení dílčího projektu: 31.10.2026

2.2. Shrnutí projektu

2.2.1. Abstrakt česky

Projekt CyberCert-CZ se zaměřuje na vybudování a akreditaci orgánu posuzování shody (CAB) v České republice s cílem posílit národní certifikační infrastrukturu v oblasti kybernetické bezpečnosti. Hlavním cílem projektu je vytvoření certifikačního orgánu (CB) a zkušební laboratoře (ITSEF), které budou schopny provádět nezávislé hodnocení a certifikaci ICT produktů a služeb podle evropského schématu certifikace kybernetické bezpečnosti (EUCC).

Projekt zahrnuje analýzu požadavků, návrh organizační a technické infrastruktury, proškolení odborného personálu, přípravu podkladů pro akreditaci (včetně žádosti o akreditaci) v souladu s ISO/IEC 17065 (pro CB) a ISO/IEC 17025 (pro ITSEF). Cílem je umožnit certifikaci kybernetické bezpečnosti na národní i evropské úrovni, zvýšit důvěryhodnost ICT produktů a podpořit konkurenceschopnost českých podniků na mezinárodním trhu.

Projekt přispěje k posílení kybernetické odolnosti a rozvoji ekosystému certifikace v souladu s evropským Aktem o kybernetické bezpečnosti (CSA), čímž podpoří bezpečnější digitální prostředí v České republice i celé EU. Velký dopad tato aktivita má také na Akt o kybernetické odolnosti (CRA).

2.2.2. Abstrakt anglicky

The CyberCert-CZ project aims to build and accredit a conformity assessment body (CAB) in the Czech Republic to strengthen the national certification infrastructure in the field of cyber security. The main objective of the project is to establish a Certification Body (CB) and a Testing Laboratory (ITSEF) that will be able to independently assess and certify ICT products and services according to the European Cybersecurity Certification Scheme (EUCC).

The project includes the analysis of requirements, design of organisational and technical infrastructure, training of professional staff, preparation of documents for accreditation (including application for accreditation) in accordance with ISO/IEC 17065 (for CB) and ISO/IEC 17025 (for ITSEF). The aim is to enable the certification of cyber security at national and European level, to increase the credibility of ICT products and to support the competitiveness of Czech companies on the international market.

The project will contribute to the strengthening of cyber resilience and the development of a certification ecosystem in line with the European Cyber Security Act (CSA), thus promoting a more secure digital environment in the Czech Republic and the EU as a whole. This activity also has a major impact on the Cyber Resilience Act (CRA).

2.2.3. Popis a zdůvodnění aktivit projektu

2.2.3.1. Popis uchazeče/uchazečů

Elektrotechnický zkušební ústav, s. p. (dále už jen EZÚ)

EZÚ je již akreditovaným subjektem podle ISO/IEC 17065 a zabývá se certifikacemi a posuzováním v oblasti kybernetické bezpečnosti. Osvědčení a jeho příloha je dostupné na webu podniku. Jeho zaměstnanci se činnostem v oblasti kybernetické bezpečnosti věnují zhruba 10 let a za tu dobu nabrali spoustu zkušeností. Tyto zkušenosti jsou používány také v rámci standardizačních činností v národních a mezinárodních pracovních skupin. Mechanismy a požadavky certifikací a certifikačních schémat jsou pochopeny a používány v rámci standardních činností podniku.

Vysoká škola báňská – Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky (VŠB-TUO, FEI, dále už jen VŠB-TUO nebo VŠB)

VŠB-TUO, Fakulta elektrotechniky a informatiky (FEI), je renomovaná akademická instituce s dlouholetou tradicí v oblasti aplikovaného výzkumu a vývoje v informatice, kybernetické bezpečnosti a umělé inteligenci. Výzkumná skupina NAVY se specializuje na pokročilé výpočetní metody, včetně kvantových algoritmů, evolučních metod, analýzy síťového provozu a malware. Skupina má bohaté zkušenosti s řešením mezinárodních výzkumných projektů a aktivně spolupracuje s průmyslovými partnery v oblasti bezpečnostních technologií. Členové skupiny se podílejí na výzkumných projektech (např. Chiméra – bezpečná komunikace pomocí mobilních zařízení, TAČR, oceněno čestným uznáním Vizionáři 2019; projekty s katedrou telekomunikací na post kvantovou kryptografii). V oblasti kybernetické bezpečnosti máme své absolventy i u Policie ČR a dalších organizací zabývajících se kybernetickou bezpečností. Získané znalosti a výsledky výzkumu jsou využívány v praktických aplikacích v oblasti kybernetické bezpečnosti a umělé inteligence.

2.2.3.2. Popis projektového záměru

Popis projektového záměru

Projekt si klade za cíl vybudovat CAB na základě strategického partnerství mezi Elektrotechnickým zkušebním ústavem (EZÚ) a Vysokou školou báňskou – Technickou univerzitou Ostrava (VŠB-TUO, FEI). CAB se zaměří na pokročilé bezpečnostní analýzy, penetrační testování, auditní procesy a implementaci regulací v souladu s evropským legislativním rámcem. To celé završí certifikačním procesem dle EUCC.

Hlavní oblasti činnosti CAB budou zahrnovat:

- **Forenzní a bezpečnostní analýzy** – identifikace, klasifikace a mitigace kybernetických hrozeb na základě dynamických bezpečnostních situací.
- **Pokročilé penetrační testování** – využití jak tradičních metod testování odolnosti systémů, tak i automatizovaných a AI-řízených penetračních testů, které reflektují nejmodernější přístupy k etickému hackingu a zjišťování bezpečnostních zranitelností.

- **Shoda s EUCC** – posouzení a certifikace ICT produktů podle požadavků EUCC.

CAB se stane inovativním centrem v oblasti kybernetické bezpečnosti, spojujícím akademický výzkum s reálnými aplikacemi v průmyslu a státní správě. Bude nejen testovacím a validačním prostředím pro ICT produkty, ale i platformou pro vývoj nových přístupů v oblasti bezpečnostních analýz a umělé inteligence.

Dlouhodobým cílem projektu je zvýšit úroveň kybernetické bezpečnosti v České republice i v rámci Evropské unie, posílit národní certifikační infrastrukturu a vytvořit referenční pracoviště pro testování bezpečnostních mechanismů v digitální éře.

Cíle projektu

Projekt CyberCert-CZ si klade za cíl vybudovat orgán posuzování shody (CAB) v oblasti kybernetické bezpečnosti, který bude poskytovat certifikační služby pro ICT produkty v souladu s evropským schématem EUCC. Klíčové cíle zahrnují:

- Zřízení CAB a zažádání o akreditaci certifikačního orgánu (CB) podle normy ISO/IEC 17065 pro EUCC.
- Vybudování laboratoře (ITSEF) a zažádání o akreditaci dle normy ISO/IEC 17025 pro EUCC.
- Proškolení posuzovatelů a odborných pracovníků, kteří budou zajišťovat certifikační procesy a testování bezpečnosti ICT produktů.
- Vytvoření technické a organizační infrastruktury, která umožní efektivní certifikační a procesy a testování.

Plánované výsledky projektu

Projekt bude realizován ve třech fázích:

- Fáze 1: Analýza a příprava (1.5.2025 - 31.10.2025)
  - Identifikace legislativních požadavků a akreditačních standardů.
  - Příprava organizační a procesní struktury CAB.
- Fáze 2: Budování kapacit a školení (1.11.2025 - 30.4.2026)
  - Proškolení min. 3 posuzovatelů pro certifikační orgán.
  - Proškolení min. 5 odborných pracovníků laboratoře.
  - Nákup a instalace vybavení pro zkušební laboratoř.
- Fáze 3: Akreditace a pilotní certifikace (1.5.2026 - 31.10.2026)
  - Vypracování podkladů pro žádost o akreditaci.
  - Podání žádosti o akreditaci u národního akreditačního orgánu.
  - Spolupráce v rámci akreditačního řízení s Českým institutem pro akreditaci.
  - Pilotní certifikace ICT produktu v souladu s EUCC.

3. Přínosy a dopady projektu

Projekt CyberCert-CZ přímo přispěje k rozvoji certifikační infrastruktury v České republice a podpoří:

- Zlepšení kybernetické odolnosti ICT produktů na českém i evropském trhu.
- Rozvoj certifikačních kapacit pro posuzování shody dle nejnovějších evropských standardů.
- Zajištění souladu s evropskou legislativou (Akt o kybernetické odolnosti).
- Podporu konkurenceschopnosti českých podniků v oblasti kybernetické bezpečnosti.

4. Klíčové indikátory výkonu (KPIs)

V rámci projektu budou sledovány následující klíčové indikátory:

- Kapacita orgánu posuzování shody: Min. 3 posuzovatelé schopní provádět certifikace ICT produktů.
- Kapacita laboratoře: Min. 5 specialistů pro zkušební testy bezpečnosti ICT produktů.
- Počet realizovaných certifikací: Min. 1 pilotní certifikace v rámci EUCC.

2.2.3.3. Pracovní balíčky a konkrétní aktivity

- **WP1: Projektové řízení a koordinace**
  - Odpovědnost: VŠB
  - Aktivity: Řízení projektu, administrativní podpora, monitoring a reporting.
  - Milníky: Pravidelné projektové zprávy.
- **WP2: Analýza požadavků a příprava dokumentace/postupů**
  - Odpovědnost: EZÚ & VŠB
  - Aktivity: Studie proveditelnosti, příprava metodik a dokumentace.
  - Milníky: Dokončení příruček pro CB a ITSEF.
- **WP3: Budování kapacit a školení**
  - Odpovědnost: EZÚ & VŠB
  - Aktivity: Školení posuzovatelů, laboratorních specialistů a dalších pracovníků zapojených do procesu, testovací tréninky.
  - Milníky: Proškolení min. 8 osob.

- WP4: Implementace laboratorní infrastruktury
    - Odpovědnost: VŠB
    - Aktivity: Pořízení laboratorního vybavení, tvorba konkrétních testovacích scénářů.
    - Milníky: Instalace a validace laboratorních zařízení a SW.
- WP5: Akreditace a pilotní certifikace
    - Odpovědnost: EZÚ & VŠB
    - Aktivity: Podání žádosti o akreditaci, provedení pilotní certifikace.
    - Milníky: Zažádání o akreditaci a realizace pilotní certifikace.

Řízení projektu

Projekt bude řízen společně EZÚ a VŠB formou pravidelných porad a koordinace aktivit mezi pracovními balíčky. VŠB bude zodpovědná za celkové řízení projektu, administrativu a laboratorní vybavení, zatímco EZÚ bude odpovědná za analýzy a odborné metodiky. Spolupráce bude zajištěna pravidelnými reporty a koordinací klíčových aktivit.

Pořadí pracovního balíčku: WP01

Název pracovního balíčku: Projektové řízení, koordinace a diseminace

Popis pracovního balíčku:

Tento pracovní balíček zahrnuje řízení celého projektu, administrativní podporu, zajištění komunikace mezi partnery, monitorování průběhu a pravidelný reporting. Cílem je zajistit efektivní koordinaci mezi pracovními balíčky a dosažení milníků v souladu s plánem projektu.

Klíčové aktivity (KA):

- **KA1.1:** Nastavení řídicí struktury projektu a definice odpovědností.
- **KA1.2:** Pravidelné projektové porady a koordinace mezi partnery.
- **KA1.3:** Monitoring pokroku jednotlivých pracovních balíčků.
- **KA1.4:** Průběžné a závěrečné reportování dle požadavků výzvy.
- **KA1.5:** Diseminace a komunikace průběžných a konečných výsledků projektu.

Časová realizace: Celé období projektu (05/2025 – 10/2026), probíhá souběžně se všemi WP.

Ověření ukončení:

- Pravidelné projektové zprávy.
- Interní zápisy z porad a hodnocení plnění milníků.
- Diseminované výsledky projektu

Pořadí pracovního balíčku: WP02

Název pracovního balíčku: Analýza požadavků a příprava dokumentace/postupů

Popis pracovního balíčku:
Cílem WP02 je provést detailní analýzu legislativních požadavků, standardů a akreditačních kritérií pro vytvoření certifikačního orgánu (CB) a zkušební laboratoře (ITSEF). Výstupy budou zahrnovat přípravu metodik, směrnic a procesních dokumentů pro další fáze projektu.

Klíčové aktivity (KA):

- **KA2.1:** Analýza relevantních evropských legislativních předpisů a mezinárodních norem (EUCC, CRA, ISO/IEC 17065 a ISO/IEC 17025).
- **KA2.2:** Definování požadavků na budoucí certifikační orgán a laboratoř.
- **KA2.3:** Vypracování metodik a příruček pro certifikace a testování.
- **KA2.4:** Interní revize dokumentace a připravenosti pro další fáze.

Časová realizace: 05/2025 – 10/2025.

Ověření ukončení:

- Schválené metodiky a směrnice.
- Interní dokumentace připravená pro školení a implementaci.

Pořadí pracovního balíčku: WP03

Název pracovního balíčku: Budování kapacit a školení

Popis pracovního balíčku:
Tento pracovní balíček je zaměřen na proškolení posuzovatelů a laboratorních specialistů, kteří budou pracovat v budoucím certifikačním orgánu a laboratoři. Součástí bude také praktický trénink a příprava testovacích procesů.

Klíčové aktivity (KA):

- **KA3.1:** Výběr a zapojení odborných pracovníků do školení.
- **KA3.2:** Organizace školení v oblasti certifikace a testování dle EUCC.
- **KA3.3:** Praktická cvičení a validace znalostí posuzovatelů a testerů.
- **KA3.4:** Zhodnocení úrovně připravenosti personálu.

Časová realizace: 11/2025 – 04/2026

Ověření ukončení:

- Proškolení min. 8 osob (osvědčení o absolvování).
- Záznamy o účasti a výsledcích školení.

Pořadí pracovního balíčku: WP04

Název pracovního balíčku: Implementace laboratorní infrastruktury

Popis pracovního balíčku:
Tento WP zahrnuje nákup, instalaci a validaci vybavení nutného pro provoz ITSEF. Součástí bude také implementace testovacích protokolů a ověření funkčnosti testovacích procesů.

Klíčové aktivity (KA):

- **KA4.1:** Specifikace a výběr laboratorního vybavení.
- **KA4.2:** Pořízení a instalace testovacích systémů.
- **KA4.3:** Ověření funkčnosti a validace testovacích procesů.
- **KA4.4:** Příprava infrastruktury pro pilotní certifikace.

Časová realizace: 02/2026 – 06/2026

Ověření ukončení:

- Dokumentace o instalaci a validaci systémů.
- Protokoly z prvních testovacích operací.

Pořadí pracovního balíčku: WP05

Název pracovního balíčku: Akreditace a pilotní certifikace

Popis pracovního balíčku:
Poslední pracovní balíček se zaměřuje na oficiální podání žádosti o akreditaci certifikačního orgánu (CB) a laboratoře (ITSEF) a na realizaci první pilotní certifikace ICT produktu dle EUCC.

Klíčové aktivity (KA):

- **KA5.1:** Podání žádosti o akreditaci a spolupráce s akreditačním orgánem.
- **KA5.2:** Implementace finálních bezpečnostních a certifikačních procesů.
- **KA5.3:** Realizace pilotní certifikace vybraného ICT produktu.
- **KA5.4:** Vyhodnocení certifikačního procesu a jeho efektivity.

Časová realizace: 06/2026 – 10/2026

Ověření ukončení:

- Podání žádosti o akreditaci CAB.
- Dokumentace z pilotní certifikace ICT produktu.

Časová návaznost a překryvy WP:

- **WP01** běží **celou dobu projektu**, zajišťuje koordinaci.
- **WP02** začíná **hned na startu (05/2025 – 10/2025)** a překrývá se s WP03.
- **WP03** běží **po dokončení WP02 (11/2025 – 04/2026)**, částečně se překrývá s WP04.
- **WP04** se realizuje **od 02/2026 do 06/2026**, částečně se překrývá s WP03 a WP05.
- **WP05** je závěrečný, probíhá **06/2026 – 10/2026**, kdy dochází k žádosti o akreditaci a první certifikaci.

Ganttův diagram

2.2.4. Popis výsledků a výstupů projektu

Projekt zahrnuje následující výstupy:

1. V001 – Metodika řízení projektu
2. V002 – Analýza požadavků a certifikační dokumentace
3. V003 – Školení odborníků
4. V004 – Implementace laboratoře
5. V005 – Akreditace certifikačního orgánu
6. V006 – Pilotní certifikace ICT produktu
7. V007 – Publikace a diseminace výsledků

Pořadí výstupu/výsledku: V001

Název výstupu/výsledku: Funkční řídicí struktura projektu a metodika řízení
Druh výstupu/výsledku: Interní dokumentace, projektové reporty
Termín dosažení výstupu/výsledku: 31/07/2025

Popis:
Tento výstup pokrývá nastavení efektivního řízení projektu a zahrnuje komplexní správu administrativních, finančních a odborných aspektů projektu. Klíčovým cílem je zajistit hladký průběh realizace projektu a jeho koordinaci mezi hlavními řešitelskými institucemi – Elektrotechnickým zkušebním ústavem (EZÚ) a Vysokou školou báňskou – Technickou univerzitou Ostrava (VŠB-TUO).

V rámci tohoto výstupu bude vypracována metodika řízení projektu, která stanoví postupy plánování, řízení rizik, rozpočtování a monitorování klíčových výsledků. Důležitou součástí bude také pravidelný reporting, zahrnující jak interní zprávy mezi partnery, tak výstupy pro poskytovatele financování a regulační orgány. Tyto zprávy budou obsahovat aktuální stav projektu, dosažené výsledky, analýzu překážek a navrhovaná opatření k jejich odstranění.

Pro zajištění efektivní komunikace a spolupráce mezi EZÚ a VŠB-TUO bude vytvořen systém pravidelných koordinačních schůzek, jejichž cílem bude sjednocení přístupu k certifikačním procesům, optimalizace využití laboratorní infrastruktury a řešení organizačních výzev.

Pořadí výstupu/výsledku: V002

Název výstupu/výsledku: Funkční řídicí struktura projektu a metodika řízení
Druh výstupu/výsledku: Interní dokumentace, projektové reporty
Termín dosažení výstupu/výsledku: 30/10/2026

Popis:
Jedná se o přehled realizovaných výsledků projektu, který umožní vyhodnocení dosažených cílů a plánu definovaného ve V001. Tento přehled poskytne podklady pro závěrečné hodnocení projektu.

Tento výstup zajistí transparentnost a vyhodnocení všech klíčových aktivit, což je zásadní pro úspěšnou realizaci projektu a následnou certifikaci kybernetické bezpečnosti v rámci EUCC.

Vazba na WP: WP01 – Projektové řízení, koordinace a diseminace

Pořadí výstupu/výsledku: V003

Název výstupu/výsledku: Analýza požadavků a dokumentace pro certifikaci
Druh výstupu/výsledku: Metodiky pro certifikační orgán (CB) a laboratoř (ITSEF)
Termín dosažení výstupu/výsledku: 30/10/2025

Popis:
Tento výstup zahrnuje podrobnou analýzu legislativních požadavků souvisejících s certifikací kybernetické bezpečnosti, včetně evropského schématu EUCC, CRA a norem ISO/IEC 17065 a ISO/IEC

17025. Cílem je zajistit, aby připravovaná laboratoř a certifikační orgán splňovaly všechny regulatorní a technické požadavky.

Součástí bude vypracování metodických příruček pro certifikační orgán (CB) a laboratoř (ITSEF), které budou obsahovat standardizované postupy pro testování a hodnocení ICT produktů. Tyto dokumenty poslouží jako základ pro akreditaci laboratoře a zavedení certifikačních procesů.

Výstup dále zahrnuje návrh struktury certifikačního procesu, včetně definice kontrolních mechanismů, požadavků na testování a schvalovací procedury. Tím se vytvoří ucelený rámec pro efektivní provádění certifikací v souladu s evropskými standardy.

Vazba na WP: WP02 – Analýza požadavků a příprava dokumentace

Pořadí výstupu/výsledku: V004

Název výstupu/výsledku: Školení a certifikace odborných posuzovatelů
Druh výstupu/výsledku: Proškolení personálu, školící programy
Termín dosažení výstupu/výsledku: 30/04/2026

Popis:
Tento výstup zahrnuje cílené školení odborníků, kteří budou zapojeni do certifikačních procesů a bezpečnostního testování ICT produktů. Školení se zaměří na certifikaci kybernetické bezpečnosti, požadavky EUCC a metodiky penetračního testování, aby účastníci získali nezbytné znalosti pro posuzování shody a testování kybernetické bezpečnosti ICT produktů.

Program zahrnuje teoretické i praktické bloky, přičemž odborníci projdou školením v oblastech certifikačních standardů, metod testování a posuzovacích postupů. Celkově bude proškoleno minimálně 8 osob, včetně posuzovatelů certifikačního orgánu a laboratorních specialistů, kteří budou zajišťovat praktické testování produktů a vyhodnocování jejich bezpečnosti.

Výstup zajistí vyšší odbornou způsobilost týmu a umožní efektivní provádění certifikací v souladu s EUCC.

Vazba na WP: WP03 – Budování kapacit a školení

Pořadí výstupu/výsledku: V005

Název výstupu/výsledku: Funkční laboratoř pro kybernetickou bezpečnost
Druh výstupu/výsledku: Technická infrastruktura, laboratorní procesy
Termín dosažení výstupu/výsledku: 30/06/2026

Popis:
Tento výstup zahrnuje návrh, vybudování a uvedení do provozu specializované laboratoře pro testování bezpečnostních vlastností ICT produktů. Laboratoř bude vybavena moderními nástroji pro analýzu

kybernetických hrozeb, provádění bezpečnostních auditů a penetrační testování, včetně metod využívajících umělou inteligenci.

Součástí výstupu bude pořízení a instalace laboratorního vybavení, které umožní automatizované testování, simulaci kybernetických útoků a validaci bezpečnostních opatření. Procesy v laboratoři budou standardizovány podle požadavků EUCC a ISO/IEC 17025, aby byla zajištěna jejich spolehlivost a shoda s certifikačními normami.

Dále bude provedena validace testovacích postupů, ověření funkčnosti laboratorního prostředí a příprava na budoucí testovací procesy. Tento výstup zajistí vytvoření plně funkčního testovacího prostředí, které bude sloužit i pro vývoj a validaci bezpečnostních technologií.

Vazba na WP: WP04 – Implementace laboratorní infrastruktury

Pořadí výstupu/výsledku: V006

Název výstupu/výsledku: Žádost o akreditaci CAB
Druh výstupu/výsledku: žádost o akreditaci na EUCC a průběh akreditačního řízení
Termín dosažení výstupu/výsledku: 31/07/2026

Popis:
Tento výstup zahrnuje komplexní proces akreditace CAB, který je nezbytný pro zahájení plnohodnotného poskytování služeb CAB v souladu s EUCC. Hlavním krokem bude podání žádosti o akreditaci u Českého institutu pro akreditaci (ČIA), přičemž bude nutné doložit splnění všech požadavků podle ISO/IEC 17065 pro certifikační orgány a ISO/IEC 17025 pro zkušební laboratoře.

V rámci tohoto procesu proběhne interní audit připravenosti, který ověří, zda jsou zavedeny všechny potřebné metodiky, testovací postupy a administrativní procesy požadované pro akreditaci. Následně bude probíhat komunikace s ČIA, jejichž hodnotitelé prověří nastavené postupy a shodu se standardy.

Vazba na WP: WP05 – Akreditace a pilotní certifikace

Pořadí výstupu/výsledku: V007

Název výstupu/výsledku: Pilotní certifikace ICT produktu dle EUCC
Druh výstupu/výsledku: výsledky z pilotní certifikace produktu
Termín dosažení výstupu/výsledku: 30/10/2026

Popis:
Tento výstup zahrnuje realizaci první pilotní certifikace ICT produktu podle evropského certifikačního schématu EUCC. Cílem je ověřit funkčnost celého certifikačního procesu, prověřit schopnosti nové laboratoře a poskytnout první reálný výstup, který prokáže připravenost certifikačního orgánu a laboratoře k plnohodnotnému provozu.

Nejprve proběhne výběr vhodného ICT produktu, který splňuje požadavky EUCC a bude použit jako referenční testovací případ. Následně bude tento produkt podroben kompletnímu procesu hodnocení, včetně analýzy bezpečnostních vlastností, zátěžových testů a simulací kybernetických hrozeb.

Proces certifikace bude realizován v několika fázích:

1. **Předběžná analýza a definice testovacích scénářů** na základě bezpečnostních požadavků EUCC.
2. **Laboratorní testování** zaměřené na detekci zranitelností, hodnocení odolnosti proti kybernetickým útokům a prověření souladu s požadavky EUCC.
3. **Vyhodnocení výsledků testování**, dokumentace nalezených nedostatků.
4. **Zpracování výstupů**, které budou obsahovat podrobné výsledky testování a rozhodnutí o udělení certifikace.

Tento výstup bude klíčovým ověřením funkčnosti nové certifikační infrastruktury, prokáže efektivitu testovacích a hodnoticích postupů a bude sloužit jako referenční případ pro budoucí certifikace. Úspěšná realizace pilotní certifikace zároveň zvýší důvěryhodnost laboratoře a certifikačního orgánu v národním i evropském měřítku.

Vazba na WP: WP05 – Akreditace a pilotní certifikace

Pořadí výstupu/výsledku: V008

Název výstupu/výsledku: Odborné publikace a diseminace výsledků
Druh výstupu/výsledku: Vědecké články, konference, prezentace
Termín dosažení výstupu/výsledku: 30/10/2026

Popis:
Součástí projektu bude aktivní akademická a diseminační činnost zaměřená na šíření výsledků výzkumu a získaných praktických poznatků. Cílem je zvýšit povědomí o certifikaci kybernetické bezpečnosti, sdílet nové postupy a přispět k rozvoji odborné komunity.

Tento výstup zahrnuje publikaci vědeckých článků v recenzovaných časopisech, které budou prezentovat inovativní přístupy k testování ICT produktů, využití AI při penetračním testování a implementaci požadavků EUCC. Dále bude řešitelský tým aktivně prezentovat výsledky projektu na mezinárodních i národních konferencích, kde proběhne odborná diskuze nad novými certifikačními postupy a standardizačními aktivitami.

Další důležitou součástí bude účast na odborných seminářích a workshopech, kde budou sdíleny praktické zkušenosti s vývojem certifikační infrastruktury, zaváděním bezpečnostních standardů a provozem zkušební laboratoře. Tyto aktivity umožní nejen propagaci výsledků projektu, ale také vytvoření užších vazeb mezi akademickou sférou, průmyslovými partnery a regulačními orgány.

Vazba na WP: WP01 – Projektové řízení, koordinace a diseminace

7.1.1. Analýza rizik ohrožující dosažení cíle projektu

V rámci realizace projektu CyberCert-CZ byla identifikována klíčová rizika, která by mohla ohrozit dosažení jeho cílů. Tato rizika zahrnují organizační a administrativní výzvy, technické komplikace, legislativní nejistoty a kybernetická ohrožení, která mohou ovlivnit funkčnost certifikačního procesu a provoz laboratoře.

Zvláštní důraz je kladen na nedostatek kvalifikovaných specialistů pro posuzování shody, což by mohlo zpomalit implementaci certifikačních procesů, a kybernetická rizika, která mohou přímo ovlivnit bezpečnost infrastruktury laboratoře.

Strategie řízení těchto rizik zahrnuje aktivní monitoring legislativních změn, flexibilní řízení projektu, školení odborníků v oblasti kybernetické bezpečnosti a pravidelné testování bezpečnostních mechanismů laboratoře. Každé identifikované riziko bylo analyzováno z hlediska pravděpodobnosti výskytu a dopadu na projekt, přičemž byla definována vhodná opatření ke zmírnění jeho vlivu.

Níže uvedená tabulka shrnuje hlavní identifikovaná rizika, jejich pravděpodobnost, dopad na projekt a plánovaná opatření ke snížení jejich dopadu.

ID Rizika	Popis Rizika	Pravděpodobnost (Nízká/Střední/Vysoká)	Dopad (Nízký/Střední/Vysoký)	Opatření ke zmírnění
R001	Překážky v akreditačním procesu	Nízká	Vysoký	Aktivní komunikace s akreditačním orgánem, průběžná kontrola dokumentace
R002	Nedostatek kvalifikovaných odborníků	Střední	Vysoký	Plán školení, spolupráce s univerzitami a experty
R003	Technologická zastaralost laboratoře	Nízká	Střední	Pravidelné upgrady, revize technologického plánu
R004	Nedostatečná spolupráce mezi členy konsorcia	Střední	Střední	Pravidelná setkání a koordinace aktivit
R006	Změny legislativy v	Střední	Vysoký	Monitoring legislativy, průběžná adaptace procesů

	oblasti certifikací			
R007	Kybernetické hrozby pro systémy laboratoře	Nízká	Vysoký	Implementace bezpečnostních standardů, pravidelná aktualizace
R008	Ztráta klíčových pracovníků	Střední	Vysoký	Plán zastupitelnosti, motivace a stabilizace týmu

8. Řešitelský tým

8.1. Hlavní řešitel projektu

[redacted]

Organizace: VŠB-TUO

8.2. Členové řešitelského týmu

Člen 1

[redacted]

Organizace: EZÚ

Člen 2

[redacted]

[redacted]

Organizace: EZÚ

Člen 3

[redacted]

Organizace: EZÚ

Člen 5

[redacted]

Organizace: EZÚ

Člen 6

[redacted]

Organizace: EZÚ

Člen 7

[redacted]

Organizace: VŠB-TUO

Člen 8

[redacted]

[redacted]

Organizace: VŠB-TUO

Člen 9

[redacted]

Organizace: VŠB-TUO

Člen 10

[redacted]

Organizace: VŠB-TUO

Člen 11

[redacted]

Organizace: EZÚ

Člen 12

[redacted]

Organizace: EZÚ

Člen 13

Organizace: VŠB-TUO

Člen 14:

Organizace: EZÚ

9. Finance

9.1. Souhrnný položkový rozpočet

Náklady	Celkem	2025	2026
Osobní náklady [Kč]			
Osobní náklady	3 346 000,00	1 396 000,00	1 950 000,00
Celkový počet úvazků [člověko-rok]	4,08	1,63	2,45
Průměrné osobní náklady na úvazek [Kč/člověko-rok]	819 428,57	854 693,88	795 918,37
Náklady na subdodávky [Kč]			
Ostatní přímé náklady [Kč]			
Cestovní náklady	180 000,00	70 000,00	110 000,00
Nákup služeb, materiálu, dlouhodobý hmotný a nehmotný majetek	700 000,00	300 000,00	400 000,00
Náklady na ochranu duševního vlastnictví	-	-	-

Další přímé náklady	445 000,00	365 000,00	80 000,00
Nepřímé náklady [Kč]			
Nepřímé náklady	326 970,00	149 170,00	177 800,00
Náklady celkem [Kč]			
Podíl nákladů na subdodávky k nákladům projektu [%]	-	-	-
Zdroje			
Podpora [Kč]	**2 498 985,00**	**1 140 085,00**	**1 358 900,00**
Neveřejné zdroje [Kč]	**2 498 985,00**	**1 140 085,00**	**1 358 900,00**
Zdroje celkem [Kč]	**4 997 970,00**	**2 280 170,00**	**2 717 800,00**
Intenzita podpory [%]	50 %	50 %	50 %

9.1.1. Komentář a zdůvodnění jednotlivých položek rozpočtu

V rámci této kapitoly je zachováno číslování členů řešitelského týmu z kap. 8.2 výše. Velikost úvazku alokovaná pro projekt je definována v kap. 8.2. Všichni členové řešitelského týmu jsou plánováni po celou dobu trvání projektu.

Hlavní uchazeč – VŠB-TUO

Osobní náklady

Hlavní řešitel: [redacted]

- Činnost:
  - Odborné vedení projektu, koordinace aktivit a výzkumných směrů.
  - Konzultace v souladu se zadávací dokumentací a požadavky výzvy na analýzu bezpečnostních situací, penetrační testování, certifikace a implementaci AI Act.
  - Supervize vývoje AI metod pro detekci kybernetických hrozeb a bezpečnostní analýzy.
  - Odborná podpora při vývoji metod pro testování bezpečnostních systémů a jejich certifikaci podle EUCC a dalších standardů.
  - Strategické řízení spolupráce s průmyslovými partnery a státní správou.
  - Zajištění souladu projektu s požadavky AI Act a dalších relevantních regulací EU.

Člen 7: [redacted]

- Činnost:
  - Penetrační testování IT systémů s využitím standardních a AI-řízených metod.
  - Forenzní analýzy bezpečnostních incidentů, návrh mitigací kybernetických útoků.
  - Vývoj testovacích scénářů pro certifikace kybernetické bezpečnosti.
  - Spolupráce na vývoji metod pro audit a shodu s AI Act.

Člen 8: [redacted]

- Činnost:
  - Vývoj a implementace moderních algoritmů pro podporu penetračního testování.
  - Programování nástrojů pro automatizovanou analýzu kybernetických hrozeb.
  - Testování a validace bezpečnostních opatření pro AI systémy.
  - Podpora při implementaci AI regulací do existujících bezpečnostních frameworků.

Člen 9: [redacted]

- Činnost:
  - Vývoj a optimalizace AI algoritmů pro síťovou bezpečnost a detekci anomálií.
  - Programátorská podpora při integraci bezpečnostních nástrojů.
  - Penetrační testování AI systémů a jejich robustnosti vůči kybernetickým útokům.
  - Analýza výstupů z penetračních testů a návrh bezpečnostních opatření.

Člen 10 [redacted]

- Činnost:
  - Administrativní řízení projektu, komunikace s partnery a řešitelským týmem.
  - Zajištění financování, správa smluv a kontrola plnění projektových milníků.
  - Příprava zpráv a podkladů pro hodnocení projektu.
  - Koordinace compliance s pravidly financování a legislativou EU.

Člen 13 [redacted]

- Činnost:
  - Konzultace v souladu se zadávací dokumentací a požadavky výzvy na analýzu bezpečnostních situací, penetrační testování a implementaci AI Act.
  - Supervize vývoje metod pro detekci kybernetických hrozeb a bezpečnostní analýzy v kontextu mobilních a bezdrátových sítí.
  - Odborná podpora při vývoji metod pro testování bezpečnostních systémů a jejich certifikaci podle EUCC a dalších standardů.
  - Zajištění souladu projektu s požadavky AI Act a dalších relevantních regulací EU týkajících se bezpečnosti mobilních a bezdrátových sítí.

- **Období zaměstnání:** Celou dobu trvání projektu

Náklady na subdodávky

N/A

Ostatní přímé náklady [Kč]

Cestovní náklady:

Cestovní náklady uvedené v kapitole 9.1 výše budou použity na účast na odborných konferencích, fórech a školeních. Tato školení mohou být i v zahraničí, pokud v tuzemsku nebude nalezen vhodný poskytovatel. Kromě toho budou náklady pokrývat tuzemské cesty, které jsou nezbytné pro zajištění spolupráce EZU.

Nákup služeb, materiál, dlouhodobý hmotný a nehmotný majetek:

V rámci těchto přímých nákladů budou peníze majoritně využity na nákup materiálu, přičemž většina z těchto prostředků bude směřována na pořízení drobného hardwaru k počítačům, který je nezbytný pro zajištění optimálního fungování našich technických zařízení. Tato investice zahrnuje například klávesnice, myši, externí disky a další podobné komponenty, které jsou nezbytné pro podporu každodenního provozu.

Další významná část prostředků bude alokována na pořízení dlouhodobého hmotného majetku, přičemž největší část těchto nákladů bude směřována na nákup počítačů. Počítače budou základem pro zajištění potřebného výkonu a kapacity pro naši práci, která zahrnuje analýzu kybernetických hrozeb, penetrační testování a detekci anomálií.

Součástí plánovaných výdajů bude rovněž investice do nehmotného majetku, zejména na nákup softwarových licencí. Tyto licence budou pokrývat různé potřebné nástroje a programy, jako jsou operační systémy, nástroje pro analýzu bezpečnosti, virtualizační software a další specializovaný software, který je nezbytný pro efektivní realizaci výzkumných aktivit a zabezpečení kybernetické bezpečnosti.

Další přímé náklady

V rámci dalších přímých nákladů budou zahrnuty výdaje spojené s poplatky za účast na odborných konferencích a fórech, které se konají jak v České republice, tak i v zahraničí. Tyto akce budou klíčové pro získání aktuálních poznatků a sdílení zkušeností v oblasti, která je předmětem našeho výzkumu. Součástí nákladů budou také výdaje na odborná školení pro naše zaměstnance, která mají za cíl zvýšit jejich odborné kompetence a dovednosti. Primární zaměření alokace těchto prostředků bude směřovat k zajištění školení a rozvoje posuzovatelů kybernetické bezpečnosti, kteří budou mít klíčovou roli při vytváření budoucí certifikace CB (certifikačního orgánu).

Další účastník projektu – EZÚ

Osobní náklady

Člen 1: [redacted]

- Činnost:
  - Řízení a koordinace projektu na straně EZÚ
  - Zajišťuje soulad certifikačních procesů s platnými normami a legislativou.

Člen 2: [redacted]

- Činnost:
  - Provádění odborných posouzení pro CO.
  - Zajištění souladu subjektu posuzování s požadavky relevantních standardů a regulací.
  - Vypracování definovaných výstupů z procesu posuzování.

Člen 3: [redacted]

- Činnost:
  - Provádění technických expertíz v rámci posouzení
  - Spolupráce s odbornými posuzovateli při hodnocení kybernetické bezpečnosti.

Člen 5: [redacted]

- Činnost:
  - Definice a rozvoj komunikačních a exploitačních strategií.
  - Jednání se stávajícími a potenciálními klienty - vč. zájemců o pilotní certifikace
  - Příprava obchodních smluv a NDA.

Člen 6: [redacted]

- Činnost:
  - Vrcholné řízení úseku certifikace EZÚ
  - Nese odpovědnost za rozhodnutí o udělení nebo neudělení certifikace.

Člen 11: [redacted]

- Činnost:
  - Vrcholově zajišťuje marketing a realizaci komunikační a exploitační strategie.
  - Podílí se na celkovém řízení projektu za EZÚ

Člen 12: [redacted]

- Činnost:
  - Provádění odborných posouzení pro CO.
  - Zajištění souladu subjektu posuzování s požadavky relevantních standardů a regulací.
  - Vypracování definovaných výstupů z procesu posuzování.

Člen 14: [redacted]

- Činnost:
  - Provádění technických expertíz v rámci posouzení
  - Spolupráce s odbornými posuzovateli při hodnocení kybernetické bezpečnosti.

Náklady na subdodávky

N/A

Ostatní přímé náklady [Kč]

Cestovní náklady:

Cestovní náklady uvedené v kap. 9.1 výše budou vynaloženy na tuzemské cesty nutné k zajištění odpovídající kooperace s hlavním řešitelem (VŠB). Dále k umožnění účasti na odborných konferencích, fórech a v neposlední řadě také odborných školeních. Odborná školení mohou mít i charakter zahraniční cesty, a to v případě, že nebude identifikován poskytovatel takového školení v tuzemsku.

Nákup služeb, materiál, dlouhodobý hmotný a nehmotný majetek:

V rámci této kategorie rozpočtu jsou započteny náklady na akreditační řízení části CAB – CB.

Náklady na ochranu práv duševního vlastnictví:

N/A

Další přímé náklady

V rámci dalších přímých nákladů počítáme s náklady za poplatky za účast na odborných konferencích/fórech v ČR i zahraničí a za odborná školení zaměstnanců. Primární alokace bude zaměřena na posuzovatele kybernetické bezpečnosti budoucího CB.

V ..... dne .....

.....

jméno a příjmení statutárního zástupce hlavního řešitele