MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PROJEKTOVÝ ZÁMER

podľa vyhlášky MIRRI č. 401/2023 Z. z.

Povinná osoba	*Univerzita Pavla Jozefa Šafárika v Košiciach (UPJŠ v Košiciach)*
Názov projektu	Kybernetická a informačná bezpečnosť na UPJŠ v Košiciach
Zodpovedná osoba za projekt	*doc. RNDr. JUDr. Pavol Sokol, PhD.*
Realizátor projektu	*UPJŠ v Košiciach*
Vlastník projektu	*UPJŠ v Košiciach*

Schvaľovanie dokumentu

Položka	**Meno a priezvisko**	**Organizácia**	**Pracovná pozícia**	**Dátum**	**Podpis** (alebo elektronický súhlas)
Vypracoval	doc. RNDr. JUDr. Pavol Sokol, PhD.	UPJŠ v Košiciach	Vedúci úseku informačnej a kybernetickej bezpečnosti	31.5.2024	

1. HISTÓRIA DOKUMENTU

Verzia	**Dátum**	**Zmeny**	**Meno**
0.1	15.05.2024	Pracovný návrh	Pavol Sokol
1.0	31.05.2024	Finálna verzia v súlade so žiadosťou o NFP	Pavol Sokol

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

V súlade s Vyhláškou MIRRI č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy (ďalej len „Vyhláška o riadení projektov“) je dokument I-02 Projektový zámer určený na rozpracovanie detailných informácií prípravy projektu, aby bolo možné rozhodnúť o pokračovaní prípravy projektu, pláne realizácie, alokovaní rozpočtu a ľudských zdrojov.

Dokument Projektový zámer v zmysle *Vyhlášky o riadení projektov* a prílohy č. 8 výzvy PSK-MIRRI-614-2024-DV-EFRR (Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejné a štátne vysoké školy) má obsahovať manažérske zhrnutie, rozsah, ciele a motiváciu na realizáciu projektu, zainteresované strany, alternatívy, návrh merateľných ukazovateľov, detailný opis požadovaných projektových výstupov, detailný opis obmedzení, predpokladov, tolerancií a návrh organizačného zabezpečenia projektu, detailný opis rozpočtu projektu a jeho prínosov, náhľad architektúry a harmonogram projektu so zoznamom rizík a závislostí.

2.1 Použité skratky a pojmy

Z hľadiska formálneho sú použité skratky a pojmy rámci celého dokumentu definované priebežne, štandardne pri prvom použití v zátvorke označením („ďalej len“).

2.2 Konvencie pre typy požiadaviek (príklady)

V rámci projektu budú definované tri základné typy požiadaviek:

1) **funkčné (používateľské) požiadavky** majú nasledovnú konvenciu:
   Fxx (F – funkčná požiadavka, xx – číslo požiadavky)

2) **Nefunkčné (kvalitatívne, výkonové - Non Functional Requirements - NFR) požiadavky** majú nasledovnú konvenciu:
   Nxx (N – nefukčná požiadavka (NFR), xx – číslo požiadavky)

3) **Technické požiadavky** majú nasledovnú konvenciu:
   Txx (T – technická požiadavka, xx – číslo požiadavky)

3. DEFINOVANIE PROJEKTU

3.1 Manažérske zhrnutie

Cieľom predloženého projektu je v období 10/2024 - 9/2026 zvýšiť informačnú a kybernetickú bezpečnosť Univerzity Pavla Jozefa Šafárika v Košiciach, najmä zvýšiť schopnosť detegovať bezpečnostné udalosti a adekvátne reagovať na bezpečnostné incidenty. Keďže univerzita vyvíja akademický informačný systém AiS2, ktorý ma vyše 75.000 používateľov (v 17 organizáciách), časť projektu sa zameriava na zvýšenie bezpečnosti tohto vývoja. S rozvojom informačných technológií dochádza k postupnej zmene bezpečnostných hrozieb. To sa prejavuje v zmene intenzity, povahy, ale aj dopadu, ktorý tieto bezpečnostné hrozby môžu spôsobiť. Je nutné, aby organizácie vedeli adekvátne zareagovať na tieto bezpečnostné hrozby a ich zmeny v čase, najmä čo sa týka ich povahy a intenzity. Aby bolo možné lepšie reagovať na tieto hrozby, organizácie zavádzajú riadenie informačnej a kybernetickej bezpečnosti a prijímajú bezpečnostné opatrenia, či už v oblasti prevencie kybernetických bezpečnostných incidentov alebo adekvátnej reakcie na nich. Cieľom predloženého projektu je vzhľadom na bezpečnostné hrozby a ich vývoj a súčasne na vývoj legislatívnych požiadaviek kladených, zvýšenie úrovne a odolnosti kybernetickej a informačnej bezpečnosti, najmä kritickej infraštruktúry v prostredí UPJŠ. Po ukončení projektu sa predpokladá, že UPJŠ bude mať nastavené všetky nutné procesy v rámci riadenia informačnej a kybernetickej bezpečnosti a v určitých oblastiach dôjde k implementácií konkrétnych bezpečnostných opatrení. Dôjde k zvýšeniu úrovne a odolnosti kybernetickej a informačnej bezpečnosti UPJŠ a súčasne dôjde k zvýšeniu schopnosti UPJŠ a jej bezpečnostného tímu (CSIRT) včasne identifikovať a adekvátne riešiť kybernetické bezpečnostné incidenty.

3.2 Motivácia a rozsah projektu

S rozvojom informačných technológií dochádza k postupnej zmene bezpečnostných hrozieb. To sa prejavuje v zmene intenzity, povahy, ale aj dopadu, ktorý tieto bezpečnostné hrozby môžu spôsobiť. Je nutné, aby organizácie vedeli adekvátne zareagovať na tieto bezpečnostné hrozby a ich zmeny v čase, najmä čo sa týka ich povahy a intenzity. Aby bolo možné lepšie reagovať na tieto hrozby, organizácie zavádzajú riadenie informačnej a kybernetickej bezpečnosti a prijímajú bezpečnostné opatrenia, či už v oblasti prevencie kybernetických bezpečnostných incidentov alebo adekvátnej reakcie na nich. Keďže 100% bezpečnosť neexistuje, je nutné v rámci organizácii uvažovať ako adekvátne a rýchlo reagovať na kybernetické bezpečnostné incidenty

Súčasne UPJŠ je dodávateľom akademického informačného systému AiS2, ktorý predstavuje pre vysokú školu jeden z najkritickejším systémov a narušenie bezpečnosti tohto systému môže výrazne narušiť základné procesy na vysokých školách (najmä poskytovanie vzdelávania). Z tohto dôvodu výskyt kybernetického bezpečnostného incidentu môže mať vplyv nielen na 9.500 používateľov UPJŠ, ale aj na ďalších 65.500 používateľov vysokých škôl, ktoré využívajú tento akademický systém.

Predmetom realizácie projektu sú nasledujúce biznis procesy:

- *riadenie kybernetickej bezpečnosti - tento proces zahŕňa identifikáciu, hodnotenie a riadenie rizík spojených s kybernetickou bezpečnosťou, vrátane zavedenia bezpečnostných opatrení a riadenia bezpečnostných incidentov.*
- *riadenie prevádzky sietí a informačných systémov – tento proces*
- *zaznamenávanie bezpečnostných udalostí, identifikácia a riešenie bezpečnostných incidentov*

Projekt sa venuje oblasti informačnej a kybernetickej bezpečnosti v kontexte akademického prostredia, s dôrazom na Univerzitu Pavla Jozefa Šafárika v Košiciach (UPJŠ) a jej základné informačné systémy, ako je akademický informačný systém AiS2 a Microsoft 365.

Základnou agendou univerzity je vykonávať vzdelávanie na všetkých stupňoch vzdelávania vrátate rozširujúceho vzdelávania alebo kontinuálneho vzdelávania.

Súčasťou univerzity je aj realizácia výskumných aktivít, ktoré sú späté napríklad s podporu ich publikačnej činnosti, prípravy a realizácia rôznych typov projektov.

CSIRT-UPJS v spolupráci s vedením UPJŠ schválili interné politiky a procesy na posilnenie bezpečnostného povedomia, riešenie bezpečnostných incidentov a monitorovanie infraštruktúry UPJŠ, ktoré sú aktívne implementované. Napriek tomu však chýbajú viaceré systémy, ktoré zahŕňajú centrálne zariadenie na zber logov a vyhodnocovanie bezpečnostných udalostí a informácií. V oblasti riadenia informačnej a kybernetickej bezpečnosti prebehla analýza rizík a čiastočná identifikácia aktív. Hoci sú implementované rôzne technické bezpečnostné opatrenia, dokumentácia a nastavenie procesov UPJŠ ešte nie sú celistvé a vzájomne sa dopĺňajúce.

Informačné systémy UPJŠ:

Kód ISVS *(z MetaIS)*	**Názov ISVS**	**Typ IS VS**
14274	Akademický informačný systém Ais2	Agendový
14275	Microsoft 365 - UPJŠ	Agendový
14276	Knižničný informačný systém Aleph	Agendový
14277	E-learning Moodle	Agendový
14278	Portál CCVaPP	Agendový
14279	CMS webového sídla univerzity	Prezentačný

Kód ISVS *(z MetaIS)*	**Názov ISVS**	**Typ IS VS**
14280	Správa siete UPJŠ	Agendový
14281	Registratúrny systém	Ekonomický a administratívny chod inštitúcie

Vzhľadom na rozsah a komplexnosť riadenia informačnej a kybernetickej bezpečnosti, ako aj povahu jednotlivých bezpečnostných opatrení, projekt je rozdelený do niekoľkých podaktivít (čiastkových úloh):

(A) Riadenie informačnej a kybernetickej bezpečnosti

V rámci projektu dôjde k vypracovaniu, resp. doplneniu dokumentácie nevyhnutnej k riadeniu informačnej a kybernetickej bezpečnosti na UPJŠ. Súčasťou projektu bude vypracovanie bezpečnostnej stratégie a bezpečnostnej politiky a doplnenie inventarizácie aktív, analýzy aktív, bezpečnostných hrozieb, zraniteľností, rizík a dopadov. Pre každú oblasť bezpečnostných opatrení uvedených vo vyhláške NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška NBU“) dôjde k spracovaniu nevyhnutnej dokumentácie a nastaveniu príslušných procesov. Dôjde k realizácii nasledujúcich podaktivít (činností):

1) Vypracovanie a aktualizácia bezpečnostnej dokumentácie
   - vypracovanie a implementácia špecifických interných riadiacich aktov pre vybrané oblasti kybernetickej a informačnej bezpečnosti,
   - vypracovanie/aktualizácia bezpečnostnej stratégie,
   - vypracovanie štatútu bezpečnostného výboru,
   - vypracovanie bezpečnostnej politiky.

2) Pre oblasť riadenia rizík:
   - Identifikácia aktív súvisiacich so zariadeniami na spracovanie informácií a centrálne zaznamenávanie inventáru týchto aktív podľa ich hodnoty vrátane určenia ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu,
   - Vykonanie klasifikácie informácií a kategorizácia sietí a informačných systémov,
   - implementáciu systému pre inventarizáciu aktív,
   - vypracovanie interného riadiaceho aktu riadenia rizík kybernetickej a informačnej bezpečnosti,
   - vykonanie riadenie rizík pozostávajúce z identifikácie zraniteľností, identifikácie hrozieb, identifikácie a analýzy rizík podľa metodiky Národného bezpečnostného úradu s ohľadom na aktívum, určenie vlastníka rizika,
   - implementácie organizačných a technických bezpečnostných opatrení,
   - analýzy funkčného dopadu (BIA) a pravidelného preskúmavania identifikovaných rizík v závislosti od aktualizácie prijatých bezpečnostných opatrení.

3) Pre oblasť personálne bezpečnosti:
   - vypracovanie interného riadiaceho aktu s bezpečnostnými zásadami pre koncových používateľov,
   - vypracovanie postupov a procesov upravujúcich personálnu bezpečnosť organizácie prostredníctvom interného riadiaceho aktu,
   - vypracovanie postupov pri zaradení osoby do niektorých z bezpečnostných rolí,
   - vypracovanie postupov pri skončení pracovnoprávneho vzťahu alebo iného obdobného vzťahu,
   - vypracovanie postupov pri porušení bezpečnostných politík.

4) Pre oblasť riadenia prístupov:
   - vypracovanie postupov a procesov upravujúcich riadenie prístupov organizácie a
   - vypracovanie zásad riadenia prístupov osôb k sieti a informačnému systému.

5) Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami
   - vypracovanie interného riadiaceho aktu upravujúceho zásady kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami.

6) Bezpečnosť pri prevádzke informačných systémov a sietí
   - vypracovanie interného riadiaceho aktu v oblasti riadenia zmien, riadenia kapacít, inštalácie softvéru v sieťach a informačných systémoch, inštalácia zariadení v sieťach a informačných systémoch, zaznamenávanie bezpečnostných záznamov a zaznamenávanie a vyhodnocovanie prevádzkových záznamov.

7) V oblasti hodnotenie zraniteľností a bezpečnostné aktualizácie

- vypracovanie interného riadiaceho aktu upravujúceho proces riadenia implementácie bezpečnostných aktualizácií a záplat.

8) V oblasti ochrany proti škodlivému kódu
   - vypracovanie interného riadiaceho aktu s požiadavkami na určenie zodpovednosti používateľov, pravidiel pre inštaláciu a monitorovania potenciálnych ciest prieniku škodlivého kódu.

9) V oblasti sieťovej a komunikačnej bezpečnosti
   - vypracovanie interného riadiaceho aktu upravujúceho pravidlá sieťovej a komunikačnej bezpečnosti.

10) V oblasti akvizície, vývoja a údržby informačných technológií verejnej správy
    - vypracovanie interného riadiaceho aktu upravujúceho požiadavky na akvizíciu, vývoj a údržbu sietí a informačných systémov, ktoré sa uplatňujú na obstarávané, vyvíjané a udržiavané komponenty s digitálnymi prvkami,
    - vypracovanie metodiky softvérového vývoja v podobe interného riadiaceho aktu, definujúce bezpečnostné požiadavky na všetky fázy životného cyklu vývoja SW (SSDLC) pre vyvíjané produkty – Akademický informačný systém AiS2, portál pre správu projektov CCVaPP.

11) V oblasti zaznamenávanie udalostí a monitorovania
    - vypracovanie dokumentácie spôsobu monitorovania a fungovania Log manažment systému a centrálneho nástroja na bezpečnostné monitorovanie a zadefinovanie spôsobu evidencie prevádzkových záznamov, ich vyhodnocovania, spôsobu hlásenia podozrivej aktivity, zodpovednej osoby a ďalších povinností;
    - vypracovanie interného riadiaceho aktu, ktorý obsahuje a upravuje povinnosti definované platnou legislatívou pre oblasť zaznamenávanie udalostí a monitorovania.

12) V oblasti fyzickej bezpečnosti a bezpečnosti prostredia
    - vypracovanie interného riadiaceho aktu upravujúceho fyzickú bezpečnosť a bezpečnosť prostredia.

13) V oblasti kryptografických opatrení
    - definovanie pravidiel využitia kryptografických prostriedkov používajúcich dostatočne odolné kryptografické mechanizmy na ochranu údajov pri ich prenose alebo uložení v rámci sietí a informačných systémov,
    - vypracovanie interného riadiaceho aktu upravujúceho systém správy kryptografických kľúčov a certifikátov.

14) V oblasti kontinuity prevádzky
    - vypracovanie interného riadiaceho aktu obsahujúceho a upravujúceho kontinuitu prevádzky následkom kybernetického bezpečnostného incidentu alebo inej krízovej situácie,
    - vykonanie analýzy dopadov na informačné systémy a siete univerzity,
    - vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na informačné systémy a siete univerzity, najmä pre oblasť malvéru, ransomvéru, úniku údajov, rozsiahleho DDoS útoku,
    - vypracovanie postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu alebo inej krízovej situácie.

15) V oblasti auditu a kontrolných činností
    - vypracovanie interného riadiaceho aktu pre oblasti auditu a kontrolných činností v oblasti informačnej a kybernetickej bezpečnosti.

(B) Oblasť riadenie prístupov

V oblasti riadenia prístupov dôjde k revízii aktuálnej bezpečnostnej politiky. UPJŠ si je vedomá toho, že v oblasti riadenia prístupov sú privilegovaní používatelia tou skupinou používateľov, ktorých získanie privilégií má pre organizáciu väčší dopad. V rámci projektu dôjde k zavedeniu prísnejších bezpečnostných opatrení smerom k privilegovaným používateľom z IT oddelení univerzity. To vyžaduje aj zavedenie viacfaktorového overenia vo všetkých systémoch, ktoré to umožňujú.

(C) Oblasť hodnotenia zraniteľností a bezpečnostných aktualizácii

Identifikácia bezpečnostných zraniteľností a následná aplikácia vhodnej formy mitigácie danej zraniteľnosti (napr. vo forme aktualizácie) predstavuje jednu z dôležitých preventívnych opatrení. UPJŠ pravidelne vyhľadáva bezpečnostné zraniteľnosti v rámci svojej infraštruktúry a IT oddelenia jednotlivých pracovísk spoločne s bezpečnostným CSIRT tímom ich následne odstraňujú.

Cieľom tejto podaktivity je rýchla a efektívna identifikácia bezpečnostných zraniteľností a ich odstraňovanie.

V rámci projektu dôjde k revízii bezpečnostnej politiky, identifikácii a hodnotenia zraniteľností a realizácie bezpečnostných aktualizácii, k zakúpeniu licencie nástroja na vyhodnocovanie bezpečnostných zraniteľností a k realizácii minimálne dvoch vyhodnocovaní bezpečnostných zraniteľností.

(D) Oblasť zaznamenávania udalostí a monitorovanie

Zaznamenávanie udalostí z infraštruktúry organizácie je nevyhnutné k tomu, aby bolo možné následne identifikovať vzniknuté bezpečnostné incidenty. UPJŠ disponuje vlastným CSIRT tímom, ktorého úlohou je aj monitorovanie infraštruktúry a správa bezpečnostných technológií pre takýto monitoring. Tento bezpečnostný tím pracuje s bezpečnostnými technológiami od spoločností Microsoft a ESET a využíva aktuálne dostupné možnosti týchto technológií. To sa v súčasnej dobe ukazuje ako nedostačujúce a je nevyhnutné implementovať plnohodnotný SIEM systém.

V rámci tejto aktivity je plánované obstaranie hardvérových a softvérových častí pre dohľadovú časť bezpečnostného tímu. To si bude vyžadovať implementáciu centrálneho manažmentu logov a SIEM systému v prostredí UPJŠ. Bude zavedené pre kritické sieťové prvky UPJŠ, centrálny sieťový prvok a kritické informačné systémy a služby univerzity. Predpokladá sa zapojenie 120 týchto systémov, sieťových prvkov, centrálneho firewallu vrátane infraštruktúry nevyhnutnej pre vývoj akademického informačného systému AiS2.

Cieľom tejto podaktivity je rýchla a efektívna identifikácia bezpečnostných udalostí a kybernetických bezpečnostných incidentov.

(E) Oblasť riešenia kybernetických bezpečnostných incidentov

Ako už bolo vyššie spomenuté UPJŠ disponuje vlastným bezpečnostným tímom (CSIRT-UPJS) a súčasne aj procesným riadením riešenia kybernetických bezpečnostných incidentov.

V rámci projektu je cieľom zvýšiť adekvátnosť reakcie na kybernetické bezpečnostné incidenty, ale aj schopnosti predchádzať týmto bezpečnostným incidentom. V rámci projektu dôjde k zakúpeniu internej infraštruktúry bezpečnostného tímu, ktorá slúži na prevádzku systémov pre vyhľadávanie bezpečnostných zraniteľností, evidenciu bezpečnostných incidentov, vyhľadávanie verejne dostupných zdrojov a informácii o bezpečnostných hrozbách a pod.

(I) Sieťová a komunikačná bezpečnosť

Počítačová sieť a iné komunikačné siete v súčasnej dobe predstavujú neoddeliteľnú súčasť poskytovania rôznych služieb. V rámci projektu plánujeme obstarať Firewall novej generácie (rozpočtové položky – Firewall a Záložný zdroj 1), ktoré umožnia UPJŠ lepšie zabezpečenie perimetra lokálnej počítačovej siete SAUNET a efektívnejšie riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami. Navyše nový typ Firewallu bude umožňovať efektívnejší manažment pravidiel, identifikáciu neoprávnených sieťových spojení na hranici s vonkajšou sieťou, blokovanie neoprávnených spojení, monitorovanie bezpečnosti, detekciu prienikov a prevenciu prienikov (IPS a IDS) identifikáciou nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky.

Cieľom tejto podaktivity je súčasne aj zefektívnenie identifikácie bezpečnostných udalostí tým, že sa budú zasielať sieťové záznamy a netflow z centrálneho sieťového zariadenia do LMS/ SIEM.

(P) Audit a kontrolné činnosti

V rámci dokončovacej fázy projektu budú realizované dve aktivity, ktorých účelom je overenie kvality implementovaných procesov a bezpečnostných opatrení. Dôjde k realizácii auditu kybernetickej bezpečnosti v zmysle zákona o kybernetickej bezpečnosti a vykonávacieho právneho predpisu. Tento externý audit považujeme za vhodné zhodnotenie stavu informačnej a kybernetickej bezpečnosti na konci realizovaného projektu. Navyše dôjde k realizácii bezpečnostného auditu webovej aplikácie akademického informačného systému AiS2.

Dôležitým a špecifickým aspektom projektu je zvýšenie bezpečnosti vývoja Akademického informačného systému AiS2. Ako sme už vyššie uviedli, tento informačný systém sa využíva na 17 univerzít vyše 75.000 používateľmi. Výskyt bezpečnostného incidentu, resp. objavenie bezpečnostnej zraniteľnosti môže mať negatívny vplyv na informačnú a kybernetickú bezpečnosť ďalších 16 inštitúcii. Z tohto dôvodu všetky plánované činnosti (podaktivity) sa zameriavajú aj na tento vývoj. Implementácia LMS a SIEM zahrnie aj vývojovú infraštruktúru AIS2. V projekte bude vypracovaná a aplikovaná metodika softvérového vývoja v podobe interného riadiaceho aktu, definujúce bezpečnostné požiadavky na všetky fázy životného cyklu vývoja SW (SSDLC) pre tento informačný systém.

Doplniť informačné systémy

3.3 Zainteresované strany/Stakeholderi

ID	AKTÉR / STAKEHOLDER	SUBJEKT (názov / skratka)	ROLA (vlastník procesu/ vlastník dát/zákazník/ užívateľ …. člen tímu atď.)	Informačný systém (MetaIS kód a názov ISVS)
1.	Administrátor IKT	UPJŠ	Člen tímu	14274, 14275, 14276, 14277, 14278, 14279, 14280,
2.	Manažér kybernetickej a informačnej bezpečnosti	UPJŠ	Vlastník procesu	14275, 14280
3.	Člen bezpečnostného tímu	UPJŠ	Člen tímu	14275, 14280

4.	Zamestnanec	UPJŠ	užívateľ	14274, 14275, 14276, 14277, 14278, 14281
5.	Študent	UPJŠ	užívateľ	14274, 14275, 14276, 14277,
6.	Externá stakeholder - Občan / podnikateľ / externá organizácia / OVM	UPJŠ	užívateľ	14277, 14278, 14279, 14281

3.4 Ciele projektu

ID	Názov cieľa	Názov strategického cieľa	Spôsob realizácie strategického cieľa
1	RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy	Zlepšovanie technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti KIB v prostredí orgánov štátnej a verejnej správy.	Implementáciou predmetného projektu
2	Zvýšenie kvality organizácie kybernetickej a informačnej bezpečnosti	Dôveryhodný štát pripravený na hrozby	Vypracovanie bezpečnostnej dokumentácie, interných riadiacich aktov, zavedenie procesov a činností na podporu kybernetickej a informačnej bezpečnosti
3	Zvýšenie kvality riadenia rizík kybernetickej a informačnej bezpečnosti	Dôveryhodný štát pripravený na hrozby	Spracovanie inventarizácie aktív, vypracovanie a implementácia potrebných dokumentov vrátane vypracovania a implementácie interného riadiaceho aktu riadenia rizík kybernetickej a informačnej bezpečnosti
4	Zabezpečenie bezpečnosti prevádzky IKT a IS vrátane sieťovej a komunikačnej bezpečnosti	Dôveryhodný štát pripravený na hrozby	Zakúpenie a implementácia sieťových zariadení zabezpečujúcich oddelenie internej siete od internetu, monitoring a filtráciu kompletného toku dát medzi nimi.
5	Zvýšenie schopnosti organizácie zbierať bezpečnostné udalosti a detegovať bezpečnostné incidenty	Dôveryhodný štát pripravený na hrozby	Dobudovanie dohľadového centra, centrálneho log manažmentu a SIEM

3.5 Merateľné ukazovatele (KPI)

ID	ID/Názov cieľa	Názov ukazovateľa (KPI)	Popis ukazovateľa	Merná jednotka	AS IS merateľné hodnoty (aktuálne)	TO BE Merateľné hodnoty (cieľové hodnoty)	Spôsob ich merania	Pozn.
1	PO095 / PSKPS OI12	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov	Počet verejných inštitúcií, ktoré sú podporované za účelom rozvoja a modernizácie kybernetických služieb, produktov, procesov a zvyšovania vedomostnej úrovne napríklad v kontexte opatrení smerujúcich k elektronickej bezpečnosti verejnej správy	Verejné Inštitúcie	0	1	Meranie sledovaním počtu verejných inštitúcií, ktoré sú aktívne zapojené do programov podpory a rozvoja v oblasti kybernetických služieb, produktov a procesov.	
2	PR017 / PSKPR CR11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov.	používatelia / rok	0	6000	V čase udržateľnosti projektu, podľa aktuálneho počtu zamestnancov a študentov.	Ide o počet používateľov, ktorí priamo využívajú IS.

.

3.6 Riziká a závislosti

Zoznam rizík a závislostí je detailne rozpracovaný v prílohe tohto dokumentu: **P_01_Register_rizik_zavislosti_v1.0_UPJS.xlsx**
Tento zoznam bude počas celej realizácie projektu priebežne aktualizovaný.

3.7 Stanovenie alternatív v biznisovej vrstve architektúry

Posudzovanie alternatív riešenia vychádza z viacerých možností. V prípade UPJŠ, ktorá má zabezpečenú čiastočnú úroveň kybernetickej bezpečnosti prichádzajú do úvahy nasledovné 3 alternatívy:

1. **Ponechanie súčasného stavu** - súčasný stav plní iba niektoré z predpísaných štandardov a noriem pre kybernetickú bezpečnosť, čím ponecháva viaceré bezpečnostné riziká neošetrené. Na univerzite funguje bezpečnostný tím a reakcia na identifikované bezpečnostné incidenty.
2. **Obmedzený variant** - tento variant sa zameriava na úspory a realizuje iba najprioritnejšie aktivity, hoci všetky aktivity sú považované za dôležité. K realizovaným aktivitám patrí vytváranie a aktualizácia dokumentácie, postupov a procesov. Zakúpila by sa licencia pre nástroj na vyhľadávanie zraniteľností. Tento prístup rieši iba zlepšenie pripravenosti na riešenie incidentov, čo samozrejme zníži škody spôsobené vzniknutým bezpečnostným incidentom, ale ani zďaleka to nepokrýva požiadavky na informačnú a kybernetickú bezpečnosť, ktorých štandard upravuje aktuálne platný právny rámec.
3. **Optimálny variant** - Realizácia jednotlivých aktivít projektu v celom ich rozsahu so zreteľom na východiskový stav. Všetky aktivity projektu boli navrhnuté na základe vyhodnotenia akútnych kybernetických hrozieb pôsobiacich na UPJŠ ako aj legislatívnych požiadaviek, ktoré zabezpečia ochranu UPJŠ pred hrozbami s najväčšou pravdepodobnosťou alebo dopadom, pričom by šlo o in house riešenie (dohľad nad všetkými systémami vo vlastnej réžii UPJŠ). Z tohto dôvodu je tento variant optimálny, pretože zabezpečuje plné splnenie požiadaviek právnej úpravy so „state of art“ prístupom ochrany informačných systémov.

Z hľadiska identifikovaných procesov v kapitole 3.2.2 alternatíva 1 nepokryje riešenie žiadneho z identifikovaného problémov. V prípade čiastkového riešenia (alternatíva 2) by boli zvolené iba niektoré z procesov, ktoré by boli projektom vyriešené. V prípade alternatívy 3 budú podporené všetky procesy v oblasti kybernetickej a informačnej bezpečnosti, ktoré sú potrebné pre účely ochrany informačných systémov a iných aktív UPJŠ.

Na základe zhodnotenia sa ukazuje ako najprijateľnejšia alternatíva možnosť 3, kedy dôjde k značnému zvýšeniu stavu kybernetickej a informačnej bezpečnosti na univerzite a nebude ohrozená udržateľnosť z dôvodu finančnej náročnosti.

3.8 Multikriteriálna analýza

Multikriteriálna analýza je v tomto prípade redukovaná na tri kritériá:

1. Potrebu **zosúladenia úrovne kybernetickej bezpečnosti s požiadavkami právnej úpravy** na maximálnu možnú dosiahnuteľnú úroveň. Táto požiadavka sa dotýka všetkých stakeholderov a predstavuje KO kritérium. Ak nemá dôjsť k zásadnému zvýšeniu kybernetickej a informačnej bezpečnosti, t.j. ak má zostať ponechaný stav alebo iba dôjde k čiastočnému zlepšeniu, nebude možné považovať realizovaný projekt za úspešný.
2. Parameter **ľudských zdrojov** zahŕňa kvalifikáciu a odborné znalosti personálu, ich dostupnosť a pracovnú kapacitu, efektívne využitie zamestnancov a zabezpečenie ich kontinuálneho rozvoja a podpory. Posudzuje, či sú zamestnanci dostatočne kvalifikovaní a či majú potrebné odborné znalosti na implementáciu a údržbu bezpečnostných opatrení. Zohľadňuje tiež počet dostupných zamestnancov a ich schopnosť efektívne vykonávať pridelené úlohy bez preťaženia.
3. **Udržateľnosť riešenia** sa týka schopnosti dlhodobého udržania a aktualizácie bezpečnostných opatrení, vrátane finančnej a organizačnej stability. Zohľadňuje, či má univerzita dostatočné zdroje na pravidelnú údržbu, aktualizáciu technológií a školenie personálu, aby mohla efektívne čeliť novým hrozbám.

Z vyššie uvedených možných alternatív vyplýva, že s ohľadom na potreby a finančné možnosti UPJŠ v rámci udržateľnosti a s ohľadom na dostatok ľudských zdrojov je najvýhodnejšia a dlhodobo udržateľná alternatíva 3.

	KRITÉRIUM	ZDÔVODNENIE KRIÉRIA	UPJŠ	EXTERNÍ STAKEHOLDERI
BIZNIS VRSTVA	Kritérium A (KO). Súlad úrovne kybernetickej bezpečnosti s požiadavkami zákona o kybernetickej bezpečnosti a zákona o ISVS	Je nevyhnutné zabezpečiť zhodu s právnou úpravou (napr. so zákonom o KB)	X	X
	Kritérium B (KO). Ľudské zdroje.	Posudzuje, či sú zamestnanci dostatočne kvalifikovaní a či majú potrebné odborné	X	X

		znalosti na implementáciu a údržbu bezpečnostných opatrení. Zohľadňuje tiež počet dostupných zamestnancov.		
	Kritérium C (KO) Udržateľnosť riešenia.	Zohľadňuje, či má univerzita dostatočné zdroje na pravidelnú údržbu, aktualizáciu technológií a školenie personálu, aby mohla efektívne čeliť novým hrozbám.	X	X

Zoznam kritérií	Alternatíva 1	Spôsob dosiahnutia	Alternatíva 2	Spôsob dosiahnutia	Alternatíva 3	Spôsob dosiahnutia
Kritérium A	N/A		Nie		Áno	Všetky aktivity projektu boli navrhnuté na základe legislatívnych požiadaviek.
Kritérium B	N/A		Áno	UPJŠ disponuje postačujúcimi ľudskými zdrojmi pre zlepšenie pripravenosti na riešenie incidentov.	Áno	UPJŠ disponuje postačujúcimi ľudskými zdrojmi pre implementáciu in house riešenia.
Kritérium C	N/A		Áno	Nakoľko táto alternatíva nezahŕňa rozvoj infraštruktúry a dohľadových systémov, bude udržateľnosť zachovaná.	Áno	Celý projekt je navrhnutý s plánovanou udržateľnosťou do 09/2031.

3.9 Stanovenie alternatív v aplikačnej vrstve architektúry

Alternatívy na úrovni aplikačnej architektúry reflektujú alternatívy vypracované na základe „nadradenej“ architektonickej biznis vrstvy, pričom vďaka uplatneniu nasledujúcich princípov aplikačná vrstva architektúry dopĺňa informácie k alternatívam stanoveným pomocou biznis architektúry.

Dodávaný hardvér, softvér, resp. služby vrátane podpora musia zodpovedať požiadavkám definovaným v projekte a požiadavkám definovanými právnou úpravou, najmä zákonom o KB. Realizácia všetkých bezpečnostných opatrení v rámci univerzity bude na úrovni kombinácie In-House riešenia a Outsourcingu

3.10 Stanovenie alternatív v technologickej vrstve architektúry

Z hľadiska použitých technológií nie sú stanovené konkrétne alternatívy. Požiadavky na technológie sú definované všeobecne tak, aby bolo možné použiť akúkoľvek softvérovú a hardvérovú technológiu, ktorá splní stanovené požiadavky koncového používateľa, na realizáciu projektu.

4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU) DONE

Po ukončení projektu sa predpokladá, že UPJŠ bude mať nastavené všetky nutné procesy v rámci riadenia informačnej a kybernetickej bezpečnosti v a určitých oblastiach dôjde k implementácií konkrétnych bezpečnostných opatrení. Pôjde najmä o oblasť sieťovej bezpečnosti, riadenia prístupov, manažmentu zraniteľností, kybernetických bezpečnostných incidentov a manažmentu logov. Týmto dôjde k zvýšeniu úrovne a odolnosti kybernetickej a informačnej bezpečnosti UPJŠ a súčasne dôjde k zvýšeniu schopnosti UPJŠ a jej bezpečnostného tímu (CSIRT) včasne identifikovať a adekvátne riešiť kybernetické bezpečnostné incidenty.

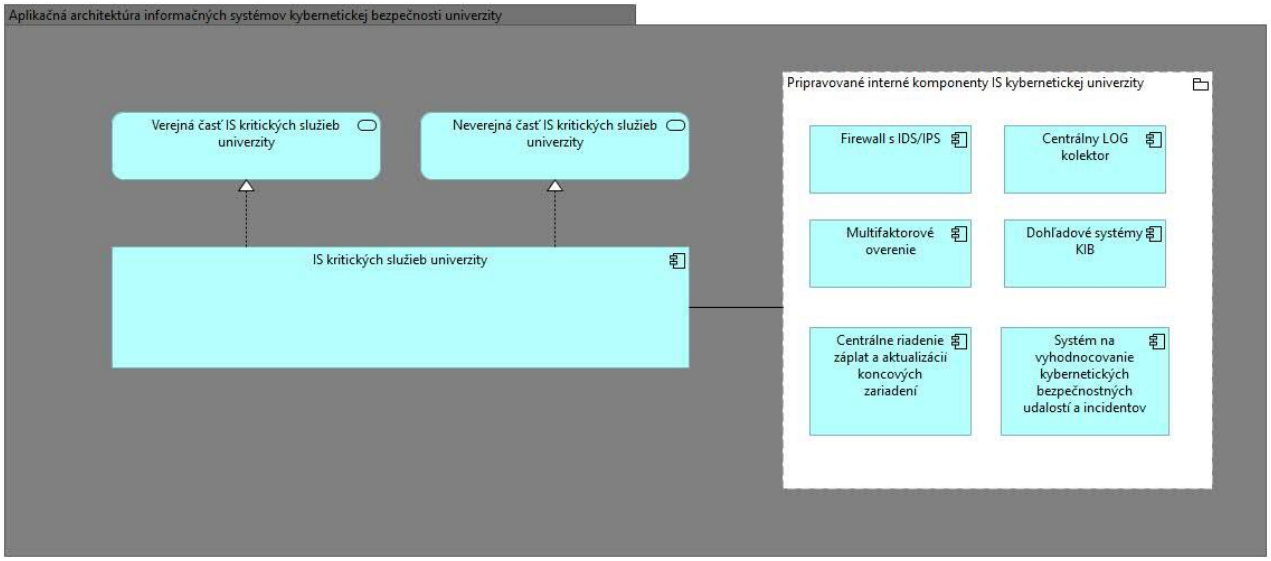
Výstupom tohto projektu (produktom) budú nasledujúce položky:

- projektové výstupy podľa vyhlášky o riadení projektov relevantné pre predmetný typ projektu,
- vytvorená, resp. aktualizovaná dokumentácia potrebná na riadenie informačnej a kybernetickej bezpečnosti na UPJŠ (zoznam je uvedený v časti Motivácia a rozsah projektu),
- implementácia technických bezpečnostných opatrení pre oblasť informačnej a kybernetickej bezpečnosti (zoznam je uvedený v časti Motivácia a rozsah projektu),
- auditné a kontrolné činnosti v rozsahu auditu kybernetickej bezpečnosti podľa platnej právnej úpravy a auditu bezpečnosti aplikácií akademického informačného systému AiS2

5. NÁHĽAD ARCHITEKTÚRY

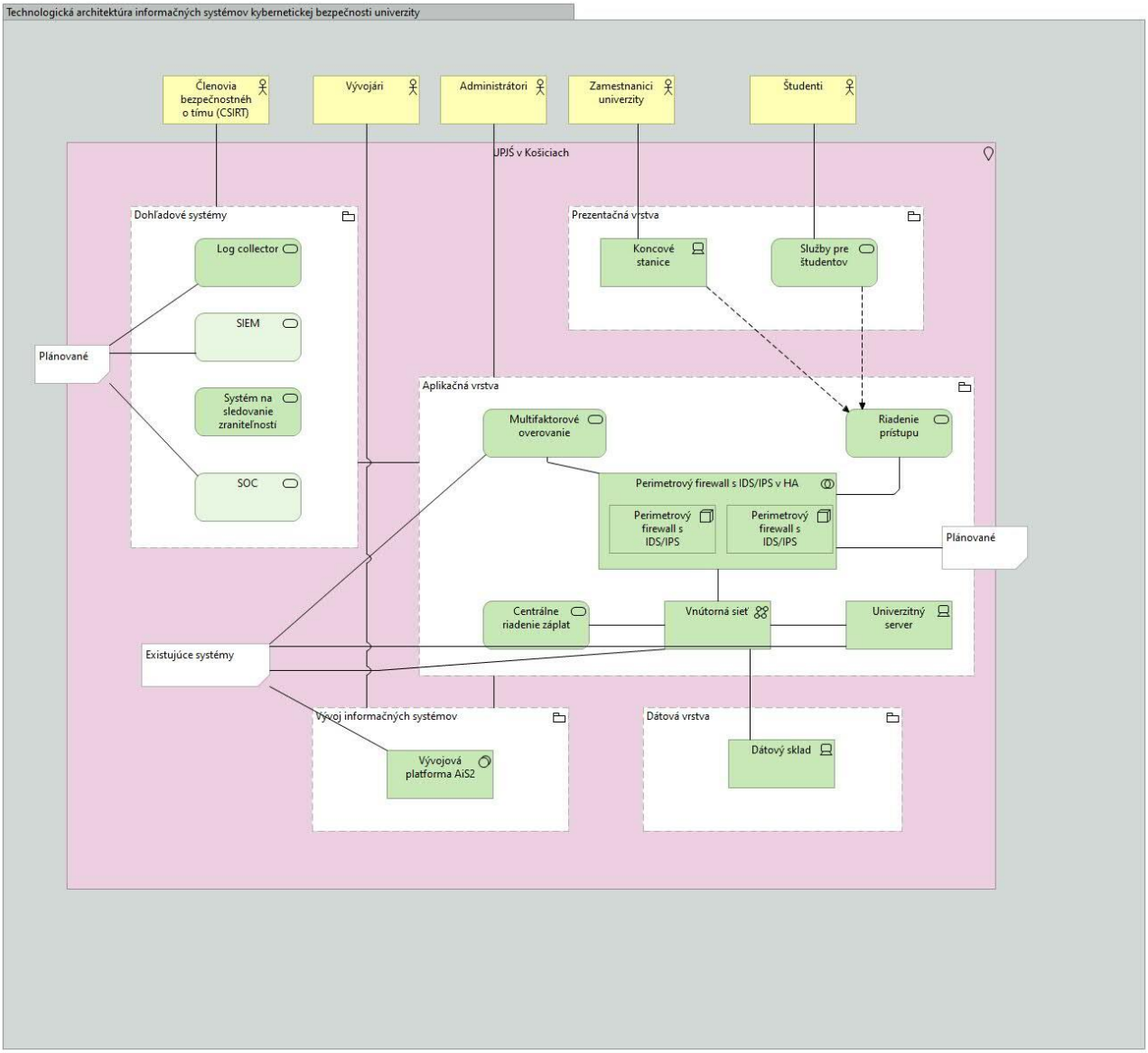
Architektúra celého riešenia je navrhovaná tak, aby bolo z projektu zrejmé, ktoré komponenty v rámci realizácie projektu budú vytvorené (realizácia opatrení kybernetickej a informačnej bezpečnosti).

Aplikačná architektúra projektu pre daný projekt je zobrazená na Obr. 1. Tvoria ju riešenia pre oblasť informačnej a kybernetickej bezpečnosti zobrazené na Obr. 1. K pripravovaným interným komponentom IS patrí **firewall s IDS/IPS** na kontrolu sieťovej prevádzky s funkciou detekcie a prevencie narušenia, **Centrálny LOG kolektor** na zber a centralizáciu logovacích údajov, zavedenie **multifaktorového overenia**, implementácia **dohľadových systémov a systému na vyhodnocovanie kybernetických bezpečnostných udalostí**, ktoré identifikujú potenciálne bezpečnostné hrozby. Súčasťou bude aj **centrálne riadenie záplat a aktualizácií**, čo umožní rýchlo reagovať na nové zraniteľnosti koncových zariadení.



Obr. 1 Aplikačná architektúra projektu

Technologická architektúra projektu pre daný projekt je zobrazená na Obr. 2. Vyznačené sú aktuálne a plánované prvky. K plánovaným prvkom patrí perimetrový firewall (2ks), infraštruktúra pre SOC, SIEM a log kolektor (s uchovaním dát po dobu 18 mesiacov).



Obr. 2 Technologická architektúra projektu

6. LEGISLATÍVA

Nie sú potrebné žiadne zmeny v oblasti legislatívy pre naplnenie cieľov a dodanie výstupov projektu. Projekt je realizovaný za účelom dosiahnutia súladu s platnou legislatívou a to najmä:

- *zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov*
- *zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov*
- *zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov*
- *zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e- Governmente)*
- *vyhláška 362/2018 Z. z. o obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení)*
- *vyhláška č.78/2020 Z. z. o štandardoch pre ITVS*
- *vyhláška 179/2020 Z. z. o obsahu bezpečnostných opatrení ITVS*
- *vyhláška č.401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy*
- *vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z o audite kybernetickej bezpečnosti.*

7. ROZPOČET A PRÍNOSY

7.1 Sumarizácia nákladov a prínosov

Náklady	Infraštruktúra k zvyšovaniu informačnej a kybernetickej bezpečnosti	Dokumentácia a procesy riadenia informačnej a kybernetickej bezpečnosti	Audit a kontrolné činnosti
Všeobecný materiál			
IT - CAPEX			
Aplikácie			
SW	*6.067 €*		
HW	*285.225 €*		
Služby		*47.680 €*	*23.922 €*
IT - OPEX- prevádzka			
Aplikácie			
SW	*6.000 €*		
HW	*37.000 €*		
Prínosy			
Finančné prínosy			
Administratívne poplatky			
Ostatné daňové a nedaňové príjmy			
Ekonomické prínosy			
Občania (€)			
Úradníci (€)			
Úradníci (FTE)			
Kvalitatívne prínosy			

Pri projektoch, ktorých predmetom je implementácia riadenia informačnej a kybernetickej bezpečnosti vrátane implementácie bezpečnostných opatrení, je vyčíslenie prínosov pomerne náročný proces. Jeden z možných prístupov, ako identifikovať možné prínosy projektu je zamerať sa na analýzu možných dopadov, ktoré so sebou prináša narušenie informačnej a kybernetickej bezpečnosti (napr. výskytom bezpečnostného incidentu). V analýze prínosov sme sa zamerali na dopady v rámci možných rizík:

Reputačné riziko – vzhľadom na postavenie UPJŠ ako vzdelávacej a výskumnej inštitúcie s povinnosťami obsiahnutými v právnej úprave je dopad tohto rizika potenciálne vysoké. Neplnenie legislatívnych požiadaviek podľa nariadenia GDPR, resp. konkrétnych ustanovení zákona o ITVS, reálny výpadok prevádzky informačných systémov univerzity, únik citlivých dát a prípadná medializácia môžu mať značné negatívne dôsledky.

Finančné riziko - prínosy projektu je možné vypočítať aj na základe zákona o KB (napriek tomu, že aktuálne na verejné vysoké školy sa nevzťahuje. V zmysle § 31 ods. 2 písm. c tohto zákona zákonodarca ustanovil pokutu do 1 % obratu, maximálne 300 000 € za každé porušenie. Vzhľadom na zmeny v bezpečnostnom prostredí, ako je zvýšená frekvencia útokov, výskyt bezpečnostných zraniteľností a ich dopadov, je rozumné predpokladať, že dnes by zákonodarca túto hodnotu ešte zvýšil. Preto považujeme za hodnotu "non-compliance" práve sumu 300:000 €.

8. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU A METÓDA JEHO RIADENIA

- Začiatok projektu: 10/2024
- Koniec projektu: 9/2026
- Fakturačné míľniky: 12/2025 (dokumentácia), 03/2026 (IKT), 09/2026 (audity)

- Míľniky Verejného obstarávania (VO): 12/2024, 04/2026

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA
1.	Prípravná fáza a Iniciačná fáza	10/2024	12/2024	Príprava súťažných podkladov a obchodných podmienok projektovým tímom v súlade so ZVO a jednotnou príručkou k VO. Iniciačná fáza bude ukončená dokončením procesu obstarávania
2.	Realizačná fáza	01/2025	03/2026	
2a	Analýza a Dizajn	01/2025	03/2025	
2b	Nákup technických prostriedkov, programových prostriedkov a služieb	04/2025	06/2025	
2c	Implementácia a testovanie	07/2025	03/2026	
2d	Nasadenie a postimplementačná podpora	11/2025	03/2026	
3.	Dokončovacia fáza	04/2026	09/2026	Realizácia auditu KB a penetračného testovania aplikácií IS AIS2.
4.	Podpora prevádzky (SLA)	10/2026	09/2031	Po finančnom ukončení projektu začína fáza udržateľnosti projektu, t.z. podpora prevádzky (SLA). V rámci danej fázy bude prijímateľ udržiavať a využívať implementované systémy. Vzniknuté náklady v tejto fáze projektu bude hradiť z vlastných výdavkov, na čo v rozpočte každoročne vyčlení dostatok finančných prostriedkov.

Realizácia a riadenie projektu bude prebiehať metódou Waterfall s jednoznačným naplánovaním jednotlivých krokov, s logickými nadväznosťami realizácie jednotlivých fáz na základe funkčnej a technickej špecifikácie, ktorá vzíde v rámci prípravnej fázy projektu. Bezpečnostné opatrenia je potrebné nasadzovať postupne vo vzájomných súvislostiach. Niektoré bezpečnostná opatrenia budú realizované paralelne avšak s ohľadom na prevádzkové požiadavky UPJŠ v Košiciach.

9. PROJEKTOVÝ TÍM

Pre účely realizácie projektu sa zostavuje **Riadiaci výbor (RV)** v nasledovnom zložení:

- Predseda RV – prof. MUDr. Pavol Jarčuška, PhD.
- Biznis vlastník - doc. RNDr. JUDr. Pavol Sokol, PhD.
- Zástupca prevádzky – Ing. Jozef Jantošovič
- Projektový manažér objednávateľa (PM) – Ing. Katarína Pezlarová

Pre účely realizácie projektu sa zostavuje **Projektový tím objednávateľa** v nasledovnom zložení:

- manažér IT prevádzky - Ing. Miroslav Pomikala
- manažér IT prevádzky – RNDr. Radovan Engel, PhD.
- IT analytik – Bc. Michal Šafranko
- Architekt IT – Mgr. Slavomír Varchula
- kľúčový používateľ – Bc. Jakub Mohler
- kľúčový používateľ – Bc. Monika Rapavá
- kľúčový používateľ – Bc. Zuzana Hennelová
- kľúčový používateľ – Ing. Ján Ondrej
- kľúčový používateľ – Mgr. Miroslav Baranko
- kľúčový používateľ – Ing. Patrícia Kočiščáková

- kľúčový používateľ – Mgr. Katarína Varchulová

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte
1.	prof. MUDr. Pavol Jarčuška, PhD.	Prorektor UPJŠ	Rektorát UPJŠ	Predseda riadiaceho výboru
2.	Ing. Jozef Jantošovič	Riaditeľ CIaKT	CIaKT UPJŠ	Zástupca prevádzky
3.	doc. RNDr. JUDr. Pavol Sokol, PhD.	Vedúci úseku informačnej a kybernetickej bezpečnosti CIaKT	CIaKT UPJŠ - CSIRT-UPJS	Manažér kybernetickej a informačnej bezpečnosti / Biznis vlastník
4.	Ing. Katarína Pezlarová	Projektový manažér	CCVaPP UPJŠ	Projektový manažér
5.	Ing. Miroslav Pomikala	Vedúci úseku Správca operačných systémov	CIaKT UPJŠ	manažér IT prevádzky
6.	RNDr. Radovan Engel, PhD.	Vedúci vývojového tímu AiS2	CIaKT UPJŠ – vývoj AiS2	manažér IT prevádzky
7.	Bc. Michal Šafranko	Člen bezpečnostného tímu, bezpečnostný analytik	CIaKT UPJŠ - CSIRT-UPJS	IT analytik
8.	Mgr. Slavomír Varchula	Člen vývojového tímu AiS2, architekt	CIaKT UPJŠ – vývoj AiS2	Architekt IT
9.	RNDr. Patrik Pekarčík	Člen bezpečnostného tímu, administrátor internej infraštruktúry	CIaKT UPJŠ - CSIRT-UPJS	kľúčový používateľ
10.	Bc. Jakub Mohler	Člen bezpečnostného tímu, incident handler	CIaKT UPJŠ - CSIRT-UPJS	kľúčový používateľ
11.	Bc. Monika Rapavá	Členka bezpečnostného tímu, incident handler	CIaKT UPJŠ - CSIRT-UPJS	kľúčový používateľ
12.	Bc. Zuzana Hennelová	Členka bezpečnostného tímu, incident handler	CIaKT UPJŠ - CSIRT-UPJS	kľúčový používateľ
13.	Ing. Ján Ondrej	Administrátor centrálnej infraštruktúry	CIaKT UPJŠ	kľúčový používateľ
14.	Mgr. Miroslav Baranko	Administrátor centrálnej infraštruktúry	CIaKT UPJŠ	kľúčový používateľ
15.	Ing. Patrícia Kočiščáková	Administrátor vývojovej infraštruktúry AiS2	CIaKT UPJŠ – vývoj AiS2	kľúčový používateľ
16.	Mgr. Katarína Varchulová	Špecialista zákazníckej podpory	CIaKT UPJŠ – vývoj AiS2	kľúčový používateľ

9.1 PRACOVNÉ NÁPLNE

Pracovné náplne pre vyššie uvedené projektové role:

Predseda riadiaceho výboru - zodpovedá za celkové riadenie a dohľad nad projektom.

1. Koordinuje činnosť riadiaceho výboru, vedie zasadnutia a zodpovedá za schvaľovanie hlavných rozhodnutí projektu.
2. Zabezpečuje, aby projekt napĺňal svoje ciele a bol v súlade s dohodnutým harmonogramom a rozpočtom.
3. Zabezpečuje komunikáciu s vedením univerzity, predkladá správy o projekte vedeniu, predkladá podklady na schválenie vedeniu univerzity.

Zástupca prevádzky - je zodpovedný za prevádzkové aspekty projektu.

1. Zabezpečuje, aby implementácia a prevádzka riešení prebiehala hladko a efektívne.
2. Poskytuje podporu a informácie potrebné pre úspešné dokončenie projektu a riešenie prevádzkových problémov.
3. Rieši rozpory medzi prevádzkou IT infraštruktúry a zabezpečením IT.
4. Pripravuje technické podklady pre riadenie projektu.
5. V prípade neprítomnosti predsedu riadiaceho výboru ho zastupuje na jednaniach.

Manažér kybernetickej a informačnej bezpečnosti - zodpovedá za dodržanie princípov a štandardov kybernetickej a informačnej bezpečnosti.

1. Koordinuje a riadi činnosť v oblasti kybernetickej a informačnej bezpečnosti.
2. Navrhuje implementácie bezpečnostných opatrení a kontroluje ich dodržiavanie.
3. Realizuje testy bezpečnostných opatrení a kybernetickej bezpečnosti.
4. Poskytuje poradenstvo v oblasti kybernetickej a informačnej bezpečnosti.
5. Zabezpečuje súlad s legislatívnymi požiadavkami.
6. Špecifikuje a analyzuje funkčné požiadavky na kybernetickú a informačnú bezpečnosť.
7. Pripravuje technické podklady pre riadenie projektu.

Biznis vlastník - zodpovedá za procesy a výstupy projektu, ktoré sú určené pre konečných používateľov. Zodpovedá za prínos projektových riešení pre konečných používateľov.

1. Schvaľuje biznis požiadavky a zabezpečuje, aby projektové riešenia prinášali požadovanú hodnotu a prínosy..
2. Definuje očakávania na kvalitu projektu a schvaľuje akceptačné kritériá..
3. Definuje schvaľovanie akceptačných kritérií.

Projektový manažér - zodpovedá za riadenie projektu počas jeho celého životného cyklu.

1. Riadi projektové zdroje.
2. Zabezpečuje tvorbu obsahu a neustále odôvodňovanie projektu.
3. Koordinuje činnosti členov projektového tímu.
4. Sleduje dodržiavanie harmonogramu a rozpočtu.
5. Rieši riziká súvisiace s implementáciou projektu.

Manažér IT prevádzky - zodpovedá za riadenie, prevádzku, alebo vývoj informačných a komunikačných technológií a informačných systémov (v rozsahu zodpovednosti v rámci organizačnej štruktúry organizácie tak, aby spĺňal požiadavky a potreby projektu).

1. Zabezpečuje plynulý chod informačných a komunikačných technológií.
2. Spravuje hardvérové a softvérové vybavenie.
3. Rieši technické problémy v rámci projektu..
4. Koordinuje činnosť tímu administrátorov.
5. Zaisťuje bezpečnosť a efektívnosť IT prevádzky.

IT analytik - zodpovedá za zber a analýzu funkčných požiadaviek, tvorbu špecifikácií a návrh riešení v rámci projektu.

1. Spolupracuje na vývoji nových aplikácií a vylepšovaní existujúcich systémov.
2. Vykonáva zber a analýzu funkčných požiadaviek.
3. Tvorí špecifikácie a návrhy riešení.
4. Analyzuje potreby zákazníka a poskytuje vstupy pre architektov a vývojárov riešení.
5. Spolupracuje na vývoji nových aplikácií a vylepšovaní existujúcich systémov.
6. Poskytuje vstupy pre ostatných členov projektového tímu.

Architekt IT - zodpovedá za návrh architektúry IT riešení a implementáciu technológií systémov (v rozsahu zodpovednosti v rámci organizačnej štruktúry organizácie tak, aby spĺňal požiadavky a potreby projektu).

1. Navrhuje systémy tak, aby dosahovali najlepšiu efektivitu a flexibilitu.
2. Implementácia technológií.
3. Zabezpečuje technickú dokumentáciu
4. Kontroluje súlad implementácie s návrhom.
5. Posudzuje vhodnosť navrhnutých riešení.

Kľúčový používateľ - zodpovedá za prevádzku projektových produktov, ich plnohodnotné využitie v zmysle projektu.

1. Navrhuje a špecifikuje funkčné a technické požiadavky.
2. Vykonáva akceptačné testovanie
3. Zabezpečuje, aby riešenia spĺňali potreby koncových používateľov.
4. Definuje požiadavky a potreby koncových používateľov.

10. ODKAZY

Irelevantné.

11. PRÍLOHY

Príloha : Zoznam rizík a závislostí (Excel): **P_01_Register_rizik_zavislosti_v1.0_UPJS.xlsx**