projekt_2609_Projektovy_zamer_ramcovy

PROJEKTOVÝ ZÁMER

manažérsky výstup I-02

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

Povinná osoba	Trenčianska univerzita Alexandra Dubčeka v Trenčíne
Názov projektu	Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti v prostredí Trenčianskej univerzity
Zodpovedná osoba za projekt	Ing. Zuzana Jakubíková (projektový mnanažér - PM)
Realizátor projektu	Trenčianska univerzita Alexandra Dubčeka v Trenčíne
Vlastník projektu	Trenčianska univerzita Alexandra Dubčeka v Trenčíne

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Vypracoval	Ing. Zuzana Jakubíková	Trenčianska univerzita Alexandra Dubčeka v Trenčíne	PM	24.5.2024	

1.HISTÓRIA DOKUMENTU

Verzia	Dátum	Zmeny	Meno
0.1	*15.05.2024*	*Pracovný návrh*	Ing. Zuzana Jakubíková
1.0	*24.05.2024*	*Zapracovanie súladu s vyhláškou č. 401/2023 Z. z., finálna verzia v súlade so ŽoNFP*	Ing. Zuzana Jakubíková

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

V súlade s Vyhláškou 401/2023 Z.z. je 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 vyššie uvedenej vyhlášky 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) obsahuje manažérske zhrnutie, motiváciu a rozsah projektu, zainteresované strany, ciele projektu a merateľné ukazovatele, návrh organizačného zabezpečenia projektu, alternatívy, opis obmedzení, predpokladov, tolerancií, opis požadovaných výstupov, náhľad architektúry, opis rozpočtu, detailný popis nákladov a prínosov, postup a spôsob nacenenia projektu, harmonogram projektu a zoznamom rizík a závislostí.

V zmysle usmernenia MIRRI SR sa v projektovej dokumentácii (ani v ŽoNFP) nešpecifikujú detailne konkrétne riziká a dopady a nezverejňuje sa podrobná dokumentácia toho, kde sú najväčšie riziká IT systémov a uvádzajú sa iba oblasti identifikovaných rizík a dopadov. Rovnako sú v zmysle usmernenia MIRRI SR manažérske produkty napísané všeobecne.

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:

Funkčné (používateľské) požiadavky majú nasledovnú konvenciu:

Fxx

F – funkčná požiadavka xx – číslo požiadavky

Nefunkčné (kvalitatívne, výkonové - Non Functional Requirements - NFR) požiadavky majú nasledovnú konvenciu:

Nxx

N – nefukčná požiadavka (NFR) xx – číslo požiadavky

Technické požiadavky majú nasledovnú konvenciu:

Txx

T – technická požiadavka xx – číslo požiadavky

3. DEFINOVANIE PROJEKTU

3.1 Manažérske zhrnutie

Trenčianska univerzita v Trenčíne (ďalej „ TN UNI“) momentálne nespadá pod Zákon o kybernetickej bezpečnosti, ale s pripravovanou transpozíciou smernice NIS2 do slovenskej legislatívy bude musieť plniť požiadavky z tejto legislatívy vyplývajúce. TNUNI si samozrejme uvedomuje potrebu zvyšovania kybernetickej bezpečnosti nielen z legislatívnych dôvodov, ale aj z dôvodu zabezpečenia vlastných prevádzkovaných systémov voči narastajúcim kybernetickým hrozbám.

TN UNI si uvedomuje, že v zmysle požiadaviek zákona o kybernetickej bezpečnosti a zavedených opatrení v zmysle vyhlášky 362/2018 Z.z. (ďalej len ZoKB), ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška 362/2018 Z.z.) spĺňa len minimálnu úroveň ustanovených požiadaviek.

TNUNI plánovaným zapojením do projektu chce zvýšiť všeobecnú úroveň kybernetickej bezpečnosti realizovaním nasledovných krokov:

- vytvorením katalógu informačných aktív a realizovaním analýzy rizík na identifikovaných aktívach,
- vytvorením kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z.,
- zvýšením bezpečnosti pri prevádzke informačných systémov a sietí dobudovaním záložných dátových kapacít
- zvýšením sieťovej a komunikačnej bezpečnosti nasadením a implementáciou perimetrového firewallu,
- implementáciou systému na nepretržitú kontrolu dátových tokov v interných sieťach univerzity,
- implementáciou automatického nástroja na identifikáciu neoprávnených sieťových spojení na hranici s vonkajšou sieťou,
- implementáciou centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity s možnosťou korelácie incidentov a eventov a vytvárania alertov,
- implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov.

Ciele projektu

Ciele projektu sú definované v súlade s Národnou koncepciou informatizácie verejnej správy (ďalej len „NKIVS“):

Zabezpečenie organizácie kybernetickej a informačnej bezpečnosti

Zabezpečenie bezpečnosti prevádzky IS a sietí vrátane sieťovej a komunikačnej bezpečnosti

Zaznamenávanie udalostí a monitorovanie a riešenie KIB incidentov

Zabezpečenie kontinuity prevádzky

Dané ciele budú dosiahnuté realizáciou hlavnej aktivity projektu - Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti.

Cieľová skupina

Cieľovou skupinou sú zamestnanci TNUNI, študenti TNUNI, dodávatelia TNUNI a ostatné právnické osoby využívajúce systémy TNUNI.

Realizáciou aktivít projektu dosiahne TNUNI naplnenie hlavného cieľa, ktorým je zvýšenie informačnej a kybernetickej bezpečnosti a zabezpečenia ochrany údajov a elektronických dát, ktoré sú využívané TNUNI, zamestnancami ako aj študentmi.

Projekt je v súlade s intervenčnou stratégiou Programu Slovensko 2021-2027 v nasledovných oblastiach:

- súlad projektu so špecifickým cieľom: RSO1.2 (opatrenie 1.2.1)
- súlad s očakávanými výsledkami definovanými v Partnerskej dohode pre špecifický cieľ RSO 1.26 3) súlad s definovanými typmi oprávnených aktivít v rámci výzvy.

Realizáciou projektu budú naplnené nasledovné merateľné ukazovatele:

PO095 / PSKPSOI12 – cieľová hodnota 1

PR017 / PSKPRCR11 – cieľová hodnota 400

Miesto realizácie:

Trenčianska univerzita v Trenčíne.

Predpokladaný rozpočet projektu (oprávnených výdavkov) je: 379 997 EUR s DPH.

V prípade, že by mala TN UNI investovať do dobudovania kybernetickej bezpečnosti vlastné finančné prostriedky, je prakticky nereálne zrealizovať všetky povinnosti podľa zákona o kybernetickej bezpečnosti a zákona o informačných systémoch verejnej správy, nakoľko ide o pomerne vysoké náklady v krátkom časovom období.

S ohľadom na to, že univerzity majú limitované finančné zdroje na boj s kyberútokmi, a súčasne je ich povinnosťou dodržiavať ustanovenia zákona o ISVS a s vysokou pravdepodobnosťou bude musieť spĺňať aj požiadavky ZoKB o kybernetickej bezpečnosti, vyhlásilo MIRRI SR Výzvu, ktorá má umožniť aj inštitúciám ako TN UNI získať prostriedky na ochranu informačných systémov a dosiahnutie kybernetickej bezpečnosti na najvyššej úrovni pri minimálnych nákladoch.

Projekt je vypracovaný v súlade s nasledovným typom aktivity: Zlepšovanie technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti KIB v prostredí orgánov štátnej a verejnej správy s definovanou hlavnou aktivitou: Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti.

Sumarizácia hlavných parametrov hodnotenia predkladaného projektu:

P. č.	Názov hodnotiaceho kritéria	Parametre v projekte	Zdroj
1.	Miera rizík ohrozujúcich úspešnú realizáciu projektu	V rámci projektu bolo identifikovaných menej ako 10 % rizík z celkového počtu identifikovaných rizík v ŽoNFP s vysokou závažnosťou, ktoré ohrozujú úspešnú realizáciu projektu.	Príloha 2 zoznam rizík
2.	Administratívne, odborné a prevádzkové kapacity žiadateľa	Žiadateľ disponuje a plánuje (v súlade s podmienkami výzvy) dostatočné odborné kapacity s náležitou odbornou spôsobilosťou a know-how na riadenie a implementáciu projektu v danej oblasti. Popis zabezpečenia prevádzky riešenia je reálny, t. j. žiadateľ disponuje a plánuje (v súlade s podmienkami výzvy) personálne kapacity pre zabezpečenie prevádzky riešenia.	Informácie o projektovom tíme sú uvedené v PZ.

3.	Miera oprávnenosti výdavkov projektu	Všetky oprávnené aktivity vychádzajú z bodu 2 Výzvy a prílohy č. 8 Výzvy, ktorá definuje oprávnené podaktivity	V rámci projektu budú realizované nasledovné oprávnené podaktivity: · Organizácia kybernetickej a informačnej bezpečnosti · Riadenie rizík · Personálna bezpečnosť · Riadenie prístupov · Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami · Bezpečnosť pri prevádzke informačných systémov a sietí · Sieťová a komunikačná bezpečnosť · Zaznamenávanie udalostí a monitorovanie · Kontinuita prevádzky · Audit a kontrolné činnosti
4.	Dôležitosť kybernetickej bezpečnosti u žiadateľa a potencionálny dopad kybernetických incidentov	V zmysle kapitoly 3.2.5 PODPORA V OBLASTI KIB NA REGIONÁLNEJ ÚROVNI uvedenej v prílohe 2 Výzvy boli Identifikované jednotlivé kategórie.	§ 24 ods. 2 písm. a) – kategória: I § 24 ods. 2 písm. b) a c) – kategória: I § 24 ods. 2 písm. d) – kategória: III §24 ods. 2 písm. e) – kategória: I

3.2 Motivácia a rozsah projektu

Hlavnou motiváciou projektu je zvýšenie úrovne KIB, aby TN UNI bola lepšie pripravená čeliť interným a externým hrozbám v oblasti kybernetickej bezpečnosti. Na rozdiel od súčasného stavu bude disponovať výrazne vyššími schopnosťami detekcie škodlivých aktivít, technologické vybavenie bude umožňovať lepšiu ochranu pred útokmi z externého a interného prostredia, ako aj ochranu dát.

Medzi hlavné ciele systému riadenia KIB patria:

- zabezpečenie správnej a bezpečnej prevádzky prostriedkov spracúvajúcich informácie,

- monitorovanie prostredia,

- evidencia a ošetrovanie podozrivých udalostí a bezpečnostných incidentov s dôrazom na prevenciu ich opakovaného výskytu.

Vyhlásená výzva „Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejné a štátne vysoké školy" súvisí najmä s naplnením povinností:

- definovanými v zákone č. 69/2018 Z. z. Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o KB") a v zákone č. 95/2019 Z. z. Zákon o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS").
- opatreniami definovanými v § 20 zákona o KB.
- nutnosť zvýšenia úrovne a schopnosti zabezpečovať a riadiť informačnú a kybernetickú bezpečnosť vzhľadom na sústavne sa zvyšujúce hrozby a riziká,
- zabezpečenie realizácie spoločných blokov bezpečnostnej architektúry v súlade s NKIVS a strategickou prioritou informačnej a kybernetickej bezpečnosti,
- ako reakcia na aktuálny nedostatočný stav úrovne vyspelosti procesov riadenia KIB,
- ako reakcia na aktuálne zmeny v používaní IT, ako aj závažné útoky v oblasti kybernetickej bezpečnosti

Implementácia projektu bude prebiehať v nasledovných krokoch:

Hlavná aktivita: Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti

1. Prípravná fáza a Iniciačná fáza

2. Realizačná fáza

2a Analýza a Dizajn

2b Nákup technických prostriedkov, programových prostriedkov a služieb

2c Implementácia a testovanie

2d Nasadenie opatrení

3. Dokončovacia fáza

4. Podpora prevádzky (SLA)

Podporné aktivity – nepriame výdavky

- Podporná aktivita – Projektový manažér na riadenie hlavných aktivít projektu.
- Podporná aktivita – Publicita a informovanosť v zmysle manuálu

Súčasné bezpečnostné mechanizmy v oblasti monitoringu a hodnotenia zraniteľnosti implementované univerzitou tvoria základ, ktorý si vyžaduje ďalší rozvoj pre zaistenie primeranej ochrany spracúvaných informácií voči kybernetickým hrozbám a zároveň zabezpečenie súladu s povinnosťami vyplývajúcimi z ustanovení zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Okrem legislatívnych požiadaviek je nevyhnutné brať do úvahy aj aktuálny stav, ktorá je z časti spôsobený neschopnosťou včasnej detekcie možného kybernetického útoku z dôvodu absentujúcich bezpečnostných opatrení, chýbajúcich analytických nástrojov a nedostatku kvalitných zdrojov bezpečnostne relevantných záznamov.

3.2.1 Hlavný popis problému

Trenčianska univerzita v Trenčíne momentálne nespadá pod Zákon o kybernetickej bezpečnosti, ale s pripravovanou transpozíciou smernice NIS2 do slovenskej legislatívy bude musieť plniť požiadavky z tejto legislatívy vyplývajúce. TNUNI si samozrejme uvedomuje potrebu zvyšovania kybernetickej bezpečnosti nielen z legislatívnych dôvodov, ale aj z dôvodu zabezpečenia vlastných prevádzkovaných systémov voči narastajúcim kybernetickým hrozbám.

TNUNI si uvedomuje, že v zmysle požiadaviek zákona o kybernetickej bezpečnosti a zavedených opatrení v zmysle vyhlášky 362/2018 Z.z. (ďalej len ZoKB), ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška 362/2018 Z.z.) spĺňa len minimálnu úroveň ustanovených požiadaviek.

TNUNI plánovaným zapojením do projektu chce zvýšiť všeobecnú úroveň kybernetickej bezpečnosti realizovaním nasledovných krokov:

- vytvorením katalógu informačných aktív a realizovaním analýzy rizík na identifikovaných aktívach,
- vytvorením kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z.,
- zvýšením bezpečnosti pri prevádzke informačných systémov a sietí dobudovaním záložných dátových kapacít
- zvýšením sieťovej a komunikačnej bezpečnosti nasadením a implementáciou perimetrového firewallu,
- implementáciou systému na nepretržitú kontrolu dátových tokov v interných sieťach univerzity,
- implementáciou automatického nástroja na identifikáciu neoprávnených sieťových spojení na hranici s vonkajšou sieťou,
- implementáciou centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity s možnosťou korelácie incidentov a eventov a vytvárania alertov,
- implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov.

Vzhľadom na skutočnosť, že TN UNI nemá aktuálne prijatý ani najvyšší dokument na riadenie kybernetickej bezpečnosti - stratégiu kybernetickej bezpečnosti, cieľom projektu je vytvoriť a prijať všetky požadované náležitosti definované v prílohe č. 1 k vyhláške č. 362/2018 Z. z..

Nie je zavedený proces klasifikácie informácií je v súlade s požiadavkami vyhlášky č. 362/2018 Z. z. pre klasifikáciu informácií kategorizácia sietí a informačných systémov.

Najvyššia miera nesúladu s legislatívnymi požiadavkami kybernetickej bezpečnosti podľa ZoKB bola identifikovaná v nasledovných oblastiach:

- Potreba zavedenia formálneho riadenia KB primárne prípravou potrebných bezpečnostných smerníc, politík a nariadení
- Potreba implementácie HW a SW časti bezpečnosti siete a implementácie sieťovej bezpečnosti siete (dodávka firewallow a dohľadových systémov)
- Potreba riešenia problému absentujúceho systému pre zber a analýzu bezpečnostných udalostí (SIEM)
- Potreba zabezpečiť kontinuitu prevádzky, t.j. je potrebné zabezpečiť riadenie kontinuity kybernetickej bezpečnosti – túto problematiku je potrebné riešiť aj na úrovni BCM plánov a aj na úrovni technologickej.

S ohľadom na vyššie uvedené bude teda predmetom projektu riešenie problematiky z nasledovných oprávnených oblastí podľa výzvy:

- Organizácia kybernetickej a informačnej bezpečnosti
- Riadenie rizík
- Personálna bezpečnosť
- Riadenie prístupov
- Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami
- Bezpečnosť pri prevádzke informačných systémov a sietí
- Sieťová a komunikačná bezpečnosť
- Zaznamenávanie udalostí a monitorovanie
- Kontinuita prevádzky
- Audit a kontrolné činnosti

Hlavným problémom, ktorému TN UNI čelí je teda vyriešenie vyššie pomenovaných oblastí informačnej a kybernetickej bezpečnosti tak, aby bol dosiahnutý významný pokrok pri plnení súladu v oblasti príslušných predpisov KIB a súčasne aby boli technologické náležitosti KIB realizované tak, aby:

- chránili IT systémy, ktoré zabezpečujú prevádzku služieb univerzity pred kybernetickými útokmi
- plnili svoje úlohy počas implementácie i v čase udržateľnosti projektu,
- boli pripravené na ďalší rozvoj IT technológií a služieb poskytovaných univerzitou,
- a bolo možné ich flexibilne rozširovať bez ohrozenia prevádzkovaných i budúcich IT systémov.

3.2.2 Biznis procesy

Predmetom realizácie projektu bude zavedenie a IT podpora nasledovných business procesov:

- Riadenie prevádzky siete a informačného systému
- Zaznamenávanie, monitorovanie a riešenie incidentov kybernetickej bezpečnosti
- Zabezpečovanie kontinuity prevádzky

Okrem samotného zabezpečenia opatrení KIB v zmysle zákona o kybernetickej bezpečnosti a zákona o ISVS sa projekt bude dotýkať prakticky všetkých biznis procesov, ktoré sú vykonávané Trenčianskou univerzitou v Trenčíne, a ktoré sú realizované prostredníctvom informačných systémov TN UNI za účelom poskytovania univerzitných služieb.

3.2.3 Oblasti zamerania projektu

Projekt sa primárne zaoberá oblasťou zabezpečenia opatrení KIB v zmysle zákona o kybernetickej bezpečnosti a zákona o ISVS. Ako bude uvedené ďalej, tento projekt má priamy dopad na všetky ISVS a technologické platformy, ktoré sú určené na poskytovanie služieb univerzity TN UNI, nakoľko výsledky projektu budú ochraňovať všetky IS pred potenciálnymi hrozbami kybernetickej a informačnej bezpečnosti.

3.2.4 Rozsah projektu

Realizácia projektu sa dotkne nasledovných ISVS prevádzkovaných na úrovni TN UNI:

- isvs_14205 e-learning
- isvs_14204 Prístupový systém
- isvs_14202 Kamerový systém
- isvs_14201 Akademický informačný systém
- isvs_14203 Dochádzkový systém

Realizácia projektu sa dotkne nasledovných subjektov:

- Trenčianska univerzita Alexandra Dubčeka v Trenčíne
- Interní zamestnanci univerzity
- Externí zamestnanci univerzity
- Študenti
- Podnikatelia - dodávateľsko-odberateľské vzťahy

3.2.5 Motivácia a obmedzenia pre dosiahnutie cieľov projektu

Hlavnou motiváciou je realizácia opatrení KIB definovaných v zákone o kybernetickej bezpečnosti a v zákone o ISVS. Primárne ide o tie opatrenia, ktoré vykazujú najväčší nesúlad s uvedenými právnymi normami a vyhláškou 362/2018 Z. z.. Vďaka realizácii týchto opatrení budú IS TN UNI chránené v maximálnej možnej miere pred kybernetickým incidentom, ktorý by mohol mať na poskytovanie služieb a prevádzku IS TN UNI nasledovný dopad:

Dopad kybernetického bezpečnostného incidentu v závislosti	Kategória	Vysvetlenie
§ 24 ods. 2 písm. a) zákona 69/2018 Z.z. Počet používateľov základnej služby zasiahnutých kybernetickým bezpečnostným incidentom.	I.	Trenčianska univerzita disponuje systémami, ktorých výpadok zasiahne viac ako 25 000 užívateľov univerzity. To znamená študentov, zamestnancov a externých partnerov.
§ 24 ods. 2 písm. b) zákona 69/2018 Z.z. Dĺžka trvania kybernetického bezpečnostného incidentu (čas pôsobenia kybernetického bezpečnostného incidentu) a/alebo § 24 ods. 2 písm. c) zákona Geografické rozšírenie kybernetického bezpečnostného incidentu.	I.	Trenčianska univerzita prevadzkuje systémy pre interný personál , vedeckých pracovníkov a študentov, kde škoda, ktorá nastane je v rozsahu nad 15 000 používateľov.
§ 24 ods. 2 písm. d) zákona 69/2018 Z.z. Stupeň narušenia fungovania základnej služby.	III.	V prípade nefunkčnosti informačných systémov nie je k dispozícii náhradné riešenie.
§ 24 ods. 2 písm. e) zákona 69/2018 Z.z. Rozsah vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu	I.	Incident spôsobí škody, ktoré má/môže mať dopad na viac ako 25 000 osôb. V prípade napadnutia a uniku osobných dát, informáciách o postavení, platových podmienkach a krádeže Know how a vedeckých výskumov, by boli škody veľmi veľké a možno aj fatálne. Nefunkčnosť systémov má priamy vplyv na hospodárske alebo spoločenské činnosti. Nefunkčnosť ISVS má priamy súvis na finančné operácie medzi univerzitou a dodávateľmi, odberateľmi, štátnymi inštitúciami (napr. sociálne a zdravotné poisťovne, daňový úrad...). Úspešný kybernetický útok, ktorého cieľom by bolo získanie dát z univerzity môže viesť a pravdepodobne aj bude viesť k úniku osobných údajov a následnému porušeniu práv dotknutých osôb. Vzhľadom na znenie §104 zákona č.: 18/2018 Z. z. a obdobné sankcie uvedené v GDPR môže vzniknúť škoda univerzite až do výšky 20 mil. €. Vychádzajúc z praxe a známych prípadov porušenia zákona na ochranu osobných údajov na území Slovenska môže takto jednému užívateľovi ISVS vzniknúť škoda prevyšujúca 250 000 €.

Projekt je formulovaný tak, aby po jeho realizácii nastal čo najväčší súlad zabezpečenia kybernetickej a informačnej bezpečnosti so zákonom o kybernetickej bezpečnosti a so zákonom o ISVS.

Obmedzenia projektu:

Z hľadiska technického, personálneho, odborného, ale ani legislatívneho neevidujeme žiadne obmedzenia, ktoré by mohli ovplyvniť úspešnú realizáciu projektu.

3.3 Zainteresované strany/Stakeholder

ID	AKTÉR / STAKEHOLDER	SUBJEKT (názov / skratka)	ROLA (vlastník procesu/ vlastník dát/zákazník/ užívateľ …. člen tímu atď.)	Informačný systém (MetaIS kód a názov ISVS)
1.	Univerzita - Administrátor IT	Uni	Vlastník procesu/ vlastník dát/ prevádzkovateľ / Užívateľ IS Zabezpečuje prevádzku IT	isvs_14205 - e-learning isvs_14204 - Prístupový systém isvs_14202 - Kamerový systém isvs_14201 -Akademický informačný systém isvs_14203 -Dochádzkový systém
2	Manažér kybernetickej bezpečnosti	Uni	Zodpovedný za KIB	isvs_14205 - e-learning isvs_14204 - Prístupový systém isvs_14202 - Kamerový systém isvs_14201 -Akademický informačný systém isvs_14203 -Dochádzkový systém
3.	Zamestnanec	Uni	Využíva IS Uni	isvs_14205 - e-learning isvs_14204 - Prístupový systém isvs_14202 - Kamerový systém isvs_14201 -Akademický informačný systém isvs_14203 -Dochádzkový systém
4.	Študent	Uni	Využíva IS Uni	isvs_14205 - e-learning isvs_14204 - Prístupový systém isvs_14202 - Kamerový systém isvs_14201 -Akademický informačný systém isvs_14203 -Dochádzkový systém
5.	podnikateľ		Využíva služby prostredníctvom IS	isvs_14205 - e-learning isvs_14204 - Prístupový systém isvs_14202 - Kamerový systém isvs_14201 -Akademický informačný systém isvs_14203 -Dochádzkový systém
6.	Poskytovateľ IT služieb		Poskytuje služby IS	isvs_14205 - e-learning isvs_14204 - Prístupový systém isvs_14202 - Kamerový systém isvs_14201 -Akademický informačný systém isvs_14203 -Dochádzkový systém

3.4 Ciele projektu

Ciele projektu sú definované v súlade s Národnou koncepciou informatizácie verejnej správy (ďalej len „NKIVS“) a súčasne sú definované tak, aby boli v súlade s očakávanými výsledkami definovanými v Partnerskej dohode Slovenskej republiky na roky 2021 – 2027 (ďalej len „Partnerská dohoda“) pre špecifický cieľ RSO 1.2. Definície cieľov rovnako vychádzajú z národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025.

Partnerská dohoda definuje špecifický cieľ RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy a konkrétne opatrenie: 1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie, oblasť - Kybernetická a informačná bezpečnosť, pričom hlavným cieľom podpory je aj zabezpečenie kybernetickej bezpečnosti v súlade so Stratégiou digitálnej transformácie Slovenska. Stratégia digitálnej transformácie v oblasti kybernetickej bezpečnosti odkazuje na Národnú stratégiu kybernetickej bezpečnosti vydanú Národným bezpečnostným úradom (ďalej len „NBÚ“)

Národná koncepcia informatizácie verejnej správy určuje v rámci prioritnej osi 4 Kybernetická a informačná bezpečnosť strategickú prioritu Kybernetická a informačná bezpečnosť. Splnenie tejto strategickej priority má byť dosiahnuté nasledujúcimi dvoma cieľmi:

Cieľ 4.1 Zvýšenie schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe

Cieľ 4.2 Posilniť ľudské kapacity a vzdelávanie v oblasti kybernetickej a informačnej bezpečnosti patriace pod prioritnú os 4 Kybernetická a informačná bezpečnosť.

Z vyššie uvedených cieľov je pre projekt dôležitý cieľ 4.1 a v súlade sním je aj nižšie citovaný strategický cieľ.

Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025, ktorá vychádza z Partnerskej dohody definuje vo vzťahu k verejnej správe nasledovný strategický cieľ:

4.1 Dôveryhodný štát pripravený na hrozby.

V definícii tohto strategického cieľa uvádza, cit:

„Kybernetická bezpečnosť je zodpovednosťou každého obyvateľa Slovenskej republiky, no bezpečnosť nemôže fungovať bez existencie mechanizmov na národnej úrovni, ktoré určujú politiku kybernetickej bezpečnosti, systém jej riadenia, ale aj procesy na detekciu a riešenie kybernetických bezpečnostných incidentov, budovanie odborných kapacít a šírenie situačného a bezpečnostného povedomia. Zároveň štát musí pri budovaní dôveryhodnosti vykonávať vyššie uvedené aktivity v súlade s Ústavou Slovenskej republiky a ostatnými zákonmi a vstupovať do základných ľudských práv a slobôd len v nevyhnutnej miere.“

Cieľový stav uvedeného strategického cieľa je v Národnej stratégii kybernetickej bezpečnosti na roky 2021 až 2025 stanovený nasledovne, cit.:

„Vybudovanie dostatočného odborného personálneho základu pre systém riadenia informačnej a kybernetickej bezpečnosti nielen na národnej, ale aj sektorovej úrovni. Spolupráca štátu s občanom na úrovni poskytovania dostatočných informácií a odporúčaní a realizácia krokov, ktoré občan reálne pocíti ako zvýšenie vlastnej bezpečnosti a bezpečnosti národného kybernetického priestoru. Vytvorenie a používanie certifikačných schém na široké portfólio typov výrobkov, procesov a služieb. Kvalitnejšie technické, organizačné a personálne zabezpečenie, založené na využívaní moderných prístupov ku kybernetickej bezpečnosti pri detekcii a riešení kybernetických bezpečnostných incidentov. Vybudovanie spôsobilostí na detekciu a riešenie kybernetických bezpečnostných incidentov na všetkých úrovniach. Efektívna spolupráca zainteresovaných subjektov na všetkých úrovniach riešenia informačnej a kybernetickej bezpečnosti. Dobre nastavený proces technickej, ale aj politickej atribúcie kybernetických bezpečnostných incidentov. Systematické a kontinuálne riadenie rizík kybernetickej bezpečnosti v jednotlivých sektoroch. Zlepšenie detekcie a zisťovania kybernetických bezpečnostných incidentov na sektorovej úrovni, zlepšenie a zjednodušenie nahlasovania kybernetických bezpečnostných incidentov nielen zo strany povinných subjektov, ale aj v rovine dobrovoľných hlásení. Podpora spôsobilostí subjektov v oblasti riadenia kontinuity činností.“

Hlavným cieľom je do prostredia univerzity v zaviesť optimalizáciu procesov riadenia kybernetickej bezpečnosti, riadenie rizík, kontinuity činností a riadenie incidentov pomocou finančných prostriedkov z dopytovej výzvy „Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejné a štátne vysoké školy“. Po implementácii projektu bude proces zavedený a ďalej vykonávaný aj internými zamestnancami, predovšetkým manažérom kybernetickej bezpečnosti, manažérom informačnej bezpečnosti a ďalšími bezpečnostnými zamestnancami. Hlavným výsledkom realizácie projektu bude realizácia a optimalizácia procesov riadenia kybernetickej bezpečnosti, riadenia rizík, kontinuity činností a riadenia incidentov.

Všetky ciele projektu sú definované v súlade s vyššie uvedenými strategickými dokumentmi:

ID	Názov cieľa	Názov stragetického cieľa*	Spôsob realizácie strategického cieľa

1	Zabezpečenie organizácie kybernetickej a informačnej bezpečnosti Cieľ realizovaný v zmysle oprávnených podaktivít: organizácia kybernetickej a informačnej bezpečnosti, riadenie rizík, personálna bezpečnosť, riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami, audit a kontrolné činnosti.	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Vypracovanie a aktualizácia stratégie kybernetickej bezpečnosti a bezpečnostnej dokumentácie s prihliadnutím na štruktúru bezpečnostnej dokumentácie podľa prílohy č.1 vyhlášky 362/2018 Z.z.Vypracovaná dokumentácia bude pokrývať všetky požadované oblasti požadovanej legislatívy. Vypracovaný bude katalóg informačných aktív s určením vlastníkov a administrátorov jednotlivých aktív. Vypracovaný bude katalóg hrozieb a rizík a na základe týchto katalógov bude vypracovaná analýza rizík pre jednotlivé aktíva. Budú identifikované a skontrolované všetky zmluvy s tretími stranami, ktoré majú vplyv na poskytovanie dôležitých služieb univerzity a budú vypracované dodatky k jednotlivým zmluvám. Taktiež bude vypracovaný vzor kybernetických požiadaviek pre budúce zmluvy. Po skončení implementácie všetkých opatrení obsiahnutých v projekte bude vykonaný audit kybernetickej bezpečnosti.
2	Zabezpečenie organizácie kybernetickej a informačnej bezpečnosti Cieľ realizovaný v zmysle oprávnených podaktivít: Bezpečnosť pri prevádzke informačných systémov a sietí, Riadenie prístupov, Sieťová a komunikačná bezpečnosť	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Zakúpenie a implementácia sieťových zariadení zabezpečujúcich oddelenie internej siete od internetu, monitoring a filtrácia kompletného toku dát medzi nimi, poskytujúcich pokročilú ochranu siete a aplikácií pred škodlivou prevádzkou a hrozbami z internetu. Zariadenia budú poskytovať pokročilé funkcie ako hĺbková inšpekcia sieťovej prevádzky, detekcia a prevencia hrozieb, vzdialený prístup zapojených v HA móde. Návrh a realizácia segmentácie siete s určením komunikačných pravidiel pre prestup medzi jednotlivými segmentami siete. Pre vzdialený prístup bude využívané overenie pomocou dvojfaktorového overovania. Zakúpenie a implementácia nástroja na sledovanie interných dátových tokov pomocou zrkadlenia prevádzky za účelom identifikácie dátových tokov medzi jednotlivými zariadeniami v sieti.
3	Zabezpečenie organizácie kybernetickej a informačnej bezpečnosti Cieľ realizovaný v zmysle oprávnených podaktivít: Zaznamenávanie udalostí a monitorovanie, Riešenie kybernetických bezpečnostných incidentov	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Zakúpenie a implementácia zariadenia pre centrálny zber systémových logov z rôznych zariadení a systémov prevádzkovaných v sieti univerzity. Vypracovanie pravidiel pre nasadenie logovania na rôzne zariadenia a vytvorenie korelačných pravidiel za účelom notifikovania administrátorov ohľadom podozrivých aktivít v sieti a na systémoch. Implementácia dohľadového systému na sledovanie prevádzkových parametrov siete a systémov. Ide primárne o sledovanie dostupnosti jednotlivých zariadení, systémov a služieb a o sledovanie vyťaženosti systémov a služieb na týchto systémoch. Vytvorenie a zadefinovanie hraničných parametrov tak, že pri ich prekročení budú administrátori notifikovaní o vzniknutí tejto udalosti.
4	Zabezpečenie organizácie kybernetickej a informačnej bezpečnosti Cieľ realizovaný v zmysle oprávnených podaktivít: Bezpečnosť pri prevádzke informačných systémov a sietí, Fyzická bezpečnosť a bezpečnosť prostredia, Kontinuita prevádzky	Dôveryhodný štát pripravený na hrozby (Realizovanie opatrení kybernetickej a informačnej bezpečnosti)	Obstaranie a implementácia dátového úložiska pre potreby zálohy prevádzkových dát a archivačnej kópie pomocou obstarania záložných kapacít pre ukladanie prevádzkových dát, umiestnené v zabezpečenom priestore bezpečne vzdialenom zálohovanému zabezpečenému priestoru. Obstaranie služieb pre potreby správy prevádzkovej zálohy, kópie archivačnej zálohy a kópie inštalačných médií, vrátane určenia spôsobu ich ukladania, testov funkcionality dátových nosičov, testov obnovy, fyzického uloženia druhej kópie archivačnej zálohy, a minimalizovania rizika poškodenia alebo zničenia dátových nosičov archivačných záloh vplyvom prírodných živlov alebo havárie. Vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na poskytované služby, a vypracovanie plánov kontinuity prevádzky a ich prvotné otestovanie v reálnom prostredí organizácie a zapracovanie nedostatkov z výsledkov testovania.

* Definícia strategického cieľa vychádza zo strategického cieľa v Národnej stratégii kybernetickej bezpečnosti a nadväzuje na prioritný cieľ Národnej koncepcie informatizácie verejnej správy.

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	PO 095 / PS KPS 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 verejnejsprávy.	Verejné inštitúcie	0	1	Identifikácia počtu realizácie opatrení KIB pre inštitúciu – splnenie súladu KIB so zákonom o kybernetickej bezpečnosti a zákonom o ISVS Čas plnenia merateľného ukazovateľa projektu: Fyzické ukončenie realizácie hlavných aktivít projektu	Typ ukazovateľa: Výstup
	PR 017 / PS KPR CR 11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	používateli a / roK	0	400	Sumarizácia počtu používateľov nových a vylepšených digitálnych služieb – bude určené počtom prístupov v IAM, Databázou používateľov v oblasti KIB. V prípade univerzity ide o počet používateľov, ktorí priamo využívajú IS a priamo sa podieľajú na zabezpečovaní základnej služby. Čas plnenia merateľného ukazovateľa projektu: v rámci udržateľnosti projektu	Typ ukazovateľa: výsledok

3.5.1 Špecifikácia potrieb koncového používateľa

Z pohľadu TN UNI je koncovým používateľom IT oddelenie a sekundárne zamestnanci TN UNI a študenti, ktorí očakávajú, že nebude vplyvom kybernetických útokov dochádzať k výpadkom prevádzky IS univerzity a tým sa de facto znefunkční poskytovanie univerzitných služieb.

Trenčianska univerzita v Trenčíne momentálne nespadá pod Zákon o kybernetickej bezpečnosti, ale s pripravovanou transpozíciou smernice NIS2 do slovenskej legislatívy bude musieť plniť požiadavky z tejto legislatívy vyplývajúce. TNUNI si samozrejme uvedomuje potrebu zvyšovania kybernetickej bezpečnosti nielen z legislatívnych dôvodov, ale aj z dôvodu zabezpečenia vlastných prevádzkovaných systémov voči narastajúcim kybernetickým hrozbám.

TNUNI si uvedomuje, že v zmysle požiadaviek zákona o kybernetickej bezpečnosti a zavedených opatrení v zmysle vyhlášky 362/2018 Z.z. (ďalej len ZoKB), ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „vyhláška 362/2018 Z.z.) spĺňa len minimálnu úroveň ustanovených požiadaviek.

TNUNI plánovaným zapojením do projektu chce zvýšiť všeobecnú úroveň kybernetickej bezpečnosti realizovaním nasledovných krokov:

- vytvorením katalógu informačných aktív a realizovaním analýzy rizík na identifikovaných aktívach,
- vytvorením kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z.,
- zvýšením bezpečnosti pri prevádzke informačných systémov a sietí dobudovaním záložných dátových kapacít
- zvýšením sieťovej a komunikačnej bezpečnosti nasadením a implementáciou perimetrového firewallu,
- implementáciou systému na nepretržitú kontrolu dátových tokov v interných sieťach univerzity,
- implementáciou automatického nástroja na identifikáciu neoprávnených sieťových spojení na hranici s vonkajšou sieťou,
- implementáciou centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity s možnosťou korelácie incidentov a eventov a vytvárania alertov,
- implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov.

Predmetom plnenia bude:

1.Vytvorenie katalógu informačných aktív a realizovaním analýzy rizík na identifikovaných aktívach

Vypracovaný bude katalóg informačných aktív s určením vlastníkov a administrátorov jednotlivých aktív. Vypracovaný bude katalóg hrozieb a rizík a na základe týchto katalógov bude vypracovaná analýza rizík pre jednotlivé aktíva. Pri vytváraní katalógov sa bude postupovať podľa vydanej metodiky MIRRI.

2. Vytvorenie kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z.

Vypracovanie a aktualizácia stratégie kybernetickej bezpečnosti a bezpečnostnej dokumentácie s prihliadnutím na štruktúru bezpečnostnej dokumentácie podľa prílohy č.1 vyhlášky 362/2018 Z.z. Vypracovaná dokumentácia bude pokrývať všetky požadované oblasti požadovanej legislatívy. Pri vypracovávaní dokumentácie sa bude vychádzať z metodík vydaných MIRRI.

3. Zvýšenie bezpečnosti pri prevádzke informačných systémov a sietí dobudovaním záložných dátových kapacít

Obstaranie a implementácia dátového úložiska pre potreby zálohy prevádzkových dát a archivačnej kópie pomocou obstarania záložných kapacít pre ukladanie prevádzkových dát, umiestnené v zabezpečenom priestore bezpečne vzdialenom zálohovanému zabezpečenému priestoru.

Obstaranie služieb pre potreby správy prevádzkovej zálohy, kópie archivačnej zálohy a kópie inštalačných médií, vrátane určenia spôsobu ich ukladania, testov funkcionality dátových nosičov, testov obnovy, fyzického uloženia druhej kópie archivačnej zálohy, a minimalizovania rizika poškodenia alebo zničenia dátových nosičov archivačných záloh vplyvom prírodných živlov alebo havárie.

Vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na poskytované služby, a vypracovanie plánov kontinuity prevádzky a ich prvotné otestovanie v reálnom prostredí organizácie a zapracovanie nedostatkov z výsledkov testovania.

Tento bod bude splnený dodávkou HW zariadení na rozšírenie aktuálne prevádzkovaného diskového poľa NetApp. Potrebným navýšením diskových kapacít pre ukladanie zálohy prevádzkových dát a pomocou existujúceho softvéru na zálohovanie.

- Dodávka hardvéru na rozšírenie aktuálneho diskového poľa.
- Realizácia inštalačných a konfiguračných služieb, ktoré zabezpečia možnosť ukladania zálohy prevádzkových dát, vrátane testovacej obnovy dát

Výsledný systém zálohovania na zabezpečenie kontinuity prevádzky bude mať nasledovné kľúčové prvky:

- Dátový sklad musí byť navrhnutý a realizovaný tak, aby zabránil útočníkom v neoprávnenom zmenení alebo odstránení zálohovaných dát. To znamená, že raz uložené dáta nie sú zraniteľné voči zmenám alebo útokom, čím sa zabezpečuje ich dôveryhodnosť.
- Musí byť vybavený mechanizmami na overenie a šifrovanie, čo zvyšuje bezpečnosť uložených dát. Digitálne podpisy a šifrovanie musia pomôcť pri zabezpečovaní integrity a dôvernosti dát.
- Musi byť navrhnutý s dôrazom na správne riadenie prístupu. To znamená, že iba oprávnené osoby alebo procesy by mali mať prístup k zálohovaným dátam, a to na základe princípu najnižších pridelených oprávnení.

4. Zvýšenie sieťovej a komunikačnej bezpečnosti nasadením a implementáciou perimetrového firewallu v HA móde

Na univerzite nie je v súčasnosti využívaný perimetrový firewall s pokročilými bezpečnostnými funkcionalitami. Toto predstavuje značné riziko v kybernetickej bezpečnosti, nakoľko nie je možné odhaľovať a zamedzovať kybernetickým hrozbám na rozhraní internej siete univerzity a internetu.

Za účelom zvýšenia bezpečnosti budú zakúpené a implementované sieťové zariadenia zabezpečujúce oddelenie internej siete od internetu, monitoring a filtrácia kompletného toku dát medzi nimi, poskytujúcich pokročilú ochranu siete a aplikácií pred škodlivou prevádzkou a hrozbami z internetu. Zariadenia budú poskytovať pokročilé funkcie ako hĺbková inšpekcia sieťovej prevádzky, detekcia a prevencia hrozieb, vzdialený prístup a budú prevádzkované v HA móde.

Taktiež bude nasadený samostatný nástroj na zber a analýzu dát z týchto perimetrových firewallov, pomocou ktorého bude možné dohľadávať prípadné bezpečnostné informácie. Nástroj bude schopný taktiež generovať rôzne štatistické reporty ohľadom prenesených dát, bezpečnostných udalostí a iných parametrov.

Bude realizovaná segmentácia siete s určením komunikačných pravidiel pre prestup medzi jednotlivými segmentami siete. Jednotlivé segmenty budú zadefinované na základe analýzy siete a systémov a budú určené komunikačné pravidlá pre prestup medzi jednotlivými segmentami siete. Na segmentáciu siete budú využité súčasné sieťové prepínače a nové firewally.

5. Implementácia systémov na nepretržitú kontrolu dátových tokov v interných sieťach univerzity

Z dôvodu bezpečnosti internej prevádzky bude zakúpený a implementovaný nástroja na sledovanie interných dátových tokov pomocou zrkadlenia prevádzky za účelom identifikácie dátových tokov medzi jednotlivými zariadeniami v sieti. Tento nástroj bude implementovaný z dôvodu, že interné prenosy dát sa nemusia dostať až na perimetrový firewall, kde by boli skontrolované, prípadne zablokované.

Implementované bude samostatné hardvérové zariadenie, ktoré bude zbierať a vyhodnocovať zrkadlené dáta z portu na centrálnom prepínači. Tieto dáta budú priebežne monitorované a vyhodnocované. Systém taktiež umožňuje vytváranie pravidelných reportov ohľadom rôznych parametrov zachytených dátových prenosov.

6. Implementácia centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity s možnosťou korelácie incidentov a eventov a vytvárania alertov

Tento cieľ bude naplnený zakúpením a implementáciou zariadenia pre centrálny zber systémových logov z rôznych zariadení a systémov prevádzkovaných v sieti univerzity. Tento systém bude prevádzkovaný na samostatnom hardvérovom zariadení, čo zabezpečí uchovanie logov aj v prípade výpadku primárnej infraštruktúry využívaných na prevádzku univerzitných systémov. Systém bude poskytovať dostatočnú úložnú kapacitu na ukladanie logov. Systém bude umožňovať vyhľadávať a zobrazovať údaje pomocou prednastavených dashboardov a bude umožňovať vytvárať reporty na základe zadaných parametrov.

Dodaný systém bude umožňovať vytváranie korelačných pravidiel uložených logov za účelom notifikovania administrátorov ohľadom podozrivých aktivít v sieti a na systémoch. Budú zadefinované rôzne “use cases”, ktoré budú vyplývať z analýzy rizík a ohrození a na tieto prípady budú vytvorené pravidlá pre notifikáciu. Tieto pravidlá budú dopĺňané na základe potrieb a týmto postupom bude pokrytá aj problematika nasadenia SIEM.

7. Implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov.

Tento cieľ bude naplnený implementáciou dohľadového systému pre sledovanie prevádzkových parametrov všetkých systémov podieľajúcich sa na prevádzke alebo podpore poskytovaných služieb: sieťových zariadení, serverov, aplikácií a ďalších IT prostriedkov. Robustná open-source platforma určená na monitorovanie sietí, serverov a aplikácií. Jeho hlavnou úlohou je poskytovať komplexný prehľad o výkone a dostupnosti vašej IT infraštruktúry v reálnom čase, čo vám umožňuje efektívne predchádzať problémom skôr, než negatívne ovplyvnia chod IKT. Systém musí podporovať široké spektrum metód na zber dát vrátane agentov, SNMP, IPMI, JMX, trapy a log súbory, čo zaručí flexibilitu a kompatibilitu s rôznymi zariadeniami a aplikáciami. V prípade potreby musí byť možné využiť proxy, ktorý zníži záťaž na hlavný server a umožní efektívne monitorovanie geograficky vzdialených lokalít.

Kľúčové požadované vlastnosti:

- konfigurovateľné upozornenia a notifikácie, ktoré môžu byť zasielané prostredníctvom emailov, SMS, skriptov alebo webhookov,
- vizualizácia dát pomocou grafov, máp, prehľadov a dashboardov,
- šifrovaná komunikácia medzi serverom, agentmi a užívateľm, čo zaručuje ochranu citlivých informácií,
- podpora autentifikácie a rôznych úrovní prístupových práv zabezpečí, že prístup k monitorovacím dátam budú len oprávnené osoby.

Nasadenie monitorovacieho systému požadujeme na vlastných zdrojoch virtualizácie.

8. Vykonanie certifikovaného auditu kybernetickej bezpečnosti.

Tento cieľ bude naplnený vykonaním certifikovaného auditu kybernetickej bezpečnosti podľa ZoKB po implementácii všetkých nových systémov do prostredia univerzity.

3.6 Riziká a závislosti

Zoznam rizík a závislostí je detailne rozpracovaný v prílohe tohto dokumentu č. 1: Zoznam rizík a závislostí. Tento zoznam bude počas celej realizácie projektu aktualizovaný.

3.7 Stanovenie alternatív v biznisovej vrstve architektúry

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

1. Ponechanie existujúceho stavu – ide o nultý stav, v ktorom TN UNI spĺňa len minimálne požiadavky na kybernetickú bezpečnosť a ide o možné ohrozenie IS TN UNI.
2. Realizácia projektu KIB s doplnením vybraných opatrení (t.j. nie všetkých) – došlo by k zvýšeniu súladu s legislatívou a s požiadavkami na technické zabezpečenie KB, ale informačné systémy univerzity by boli naďalej kriticky ohrozené.
3. Realizácia opatrení na dosiahnutie zvýšenia súladu KIB s požiadavkami zákona o kybernetickej bezpečnosti a zákona o ISVS – pôjde o také zvýšenie súladu s požiadavkami príslušnej legislatívy v oblasti KIB, ktorá zabezpečí ochranu TN UNI pred najväčšími hrozbami, pričom by šlo o in house riešenie (dohľad nad všetkými systémami vo vlastnej réžii TN UNI).
4. Realizácia opatrení na dosiahnutie zvýšenia súladu KIB s požiadavkami zákona o kybernetickej bezpečnosti a zákona o ISVS – pôjde o také zvýšenie súladu s požiadavkami príslušnej legislatívy v oblasti KIB, ktorá zabezpečí ochranu TN UNI pred najväčšími hrozbami a služby dohľadu budú realizované ako externá služba (SIEM a SOC služby realizované ako služba).

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 KIB, ktoré je potrebné pre účely ochrany IS, a ktoré zabezpečujú prevádzku TN UNI. Alternatíva 4 rieši pokrytie všetkých procesov v oblasti KIB, ktoré sú potrebné pre účely ochrany IS, ale vyžadujú platbu externým subjektom minimálne počas doby udržateľnosti projektu.

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

3.8 Multikriteriálna analýza

Multikriteriálna analýza je v tomto prípade redukovaná na dva parametre:

1. Potrebu zosúladenia úrovne kybernetickej bezpečnosti s požiadavkami zákona o kybernetickej bezpečnosti a zákona o ISVS 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 TN UNI, t.j. ak má zostať ponechaný stav alebo iba dôjde k čiastočnému zlepšeniu, nebude možné považovať realizovaný projekt za úspešný.
2. Udržateľnosť riešenia.

Z vyššie uvedených možných alternatív vyplýva, že s ohľadom na potreby a finančné možnosti TN UNI v rámci udržateľnosti je najvýhodnejšia a dlhodobo udržateľná alternatíva 4.

3.9 Stanovenie alternatív v aplikačnej vrstve architektúry

HW a SW komponenty, rovnako ako služby, ktoré sú s nimi spojené musia zodpovedať požiadavkám definovaným v projekte koncovými používateľmi - tými sú v tomto prípade oddelenie informatiky, ktoré vychádza z požiadaviek zákona o kybernetickej bezpečnosti, zákona o ISVS, vyhlášky 362/2018 Z. z. a ďalších predpisov.

Aplikačná vrstva predpokladá dve alternatívy:

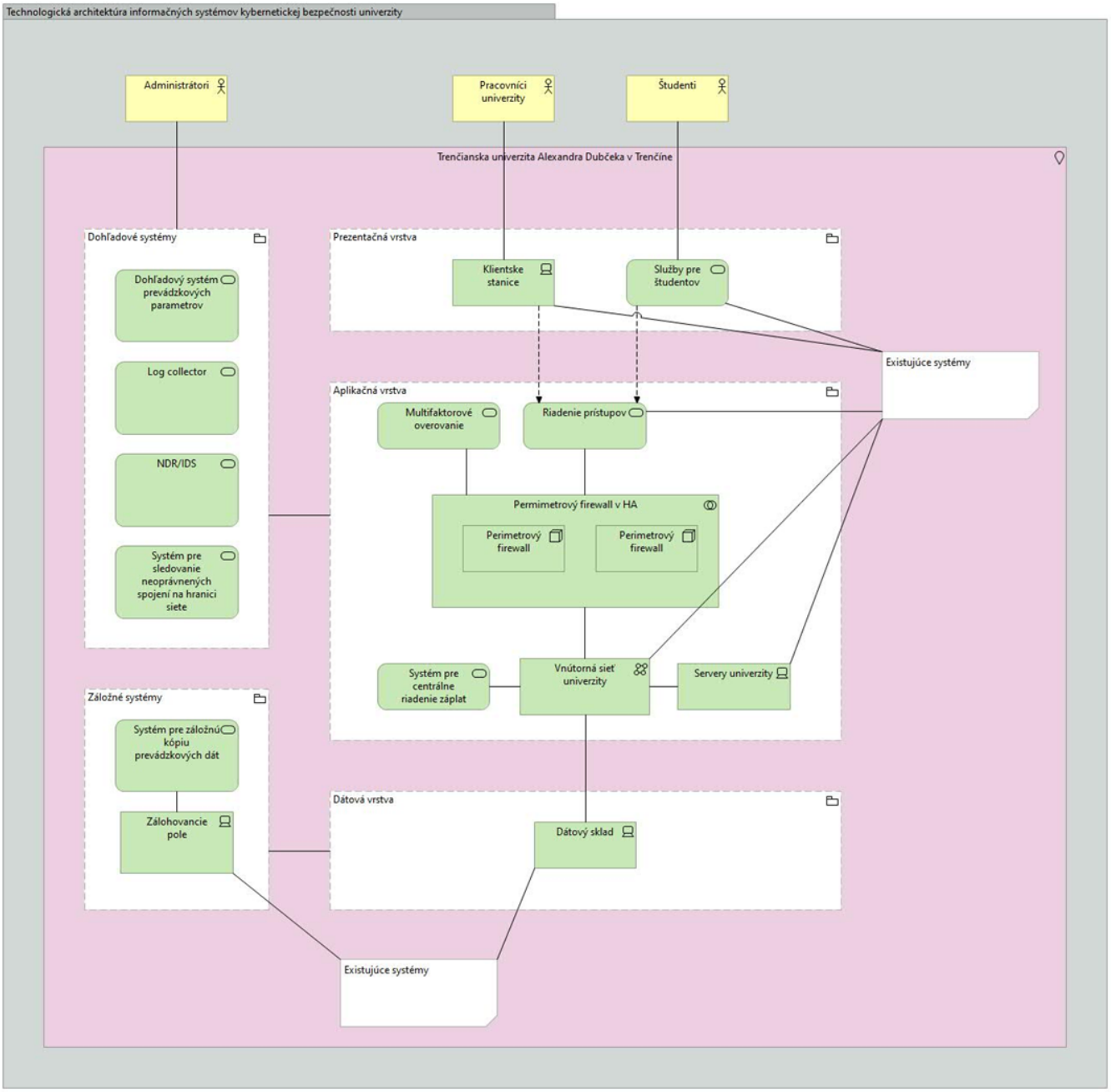
1. realizácia všetkých opatrení na úrovni TN UNI v zmysle definovaných požiadaviek, pričom všetky technológie na realizáciu opatrení KIB budú vytvorené ako IN-HOUSE riešenie vrátane SIEM - táto architektúra zodpovedá alternatíve 3 popísanej v multikriteriálnej analýze
2. realizácia všetkých opatrení na úrovni TN UNI v zmysle definovaných požiadaviek, pričom niektoré technológie na realizáciu opatrení KIB budú vytvorené ako IN-HOUSE riešenie a niektoré ako služba, konkrétne SIEM - táto architektúra zodpovedá alternatíve 4 popísanej v multikriteriálnej analýze.

Aplikačne teda bude zvolená architektúra II.

3.10 Stanovenie alternatív v technologickej vrstve architektúry

Z hľadiska použitých technológií nie sú definované alternatívy. Požiadavky na technológie sú definované všeobecne tak, aby ľubovoľnú SW a HW technológia, ktorá splní definované požiadavky koncového používateľa, bolo možné použiť na realizáciu projektu.

Technologickú architektúru riešenia definuje nasledovný obrázok:



4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

Výsledkom projektu budú:

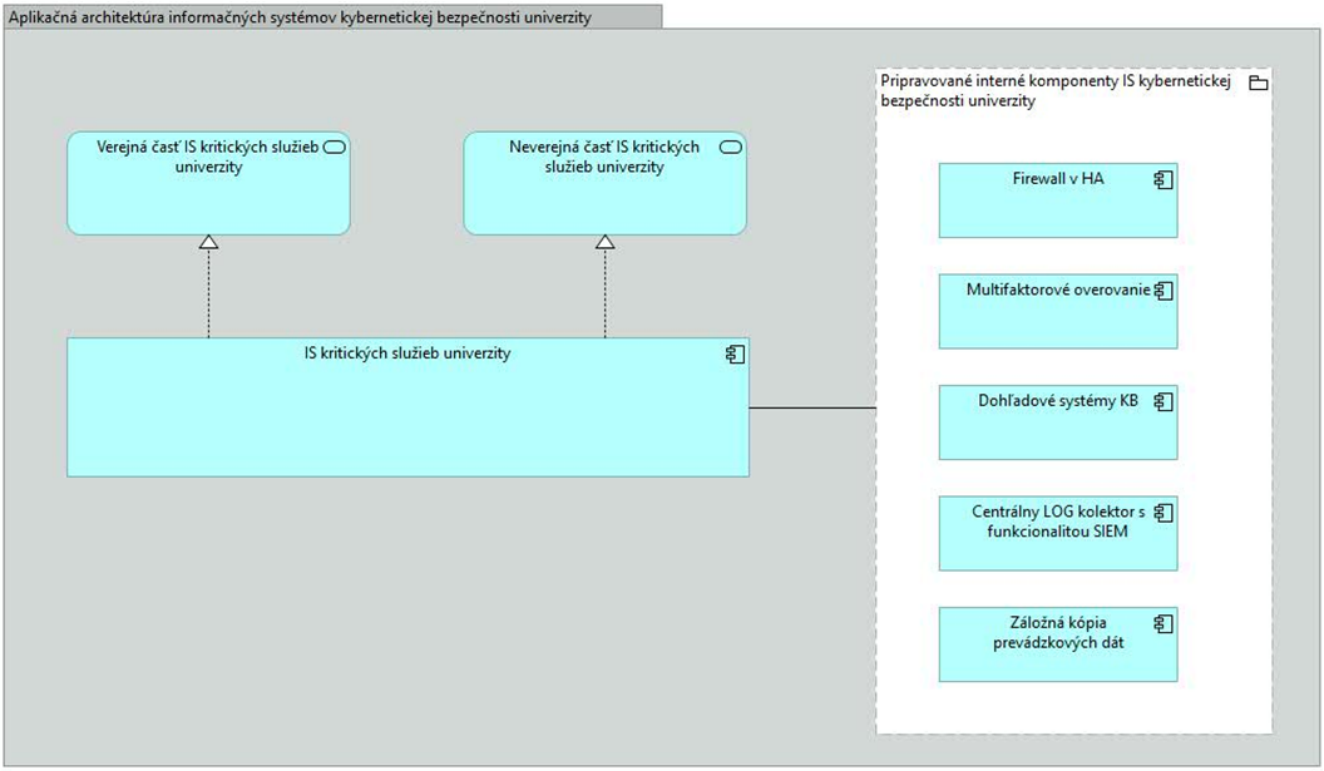
- Projektové výstupy v zmysle vyhlášky 401/2023 o riadení projektov. V prípade, že predmetom realizácie bude dielo (oceniteľné práva a/alebo zdrojový kód), získa TN UNI právo vykonávať autorské práva k tomuto dielu, vrátane výhradnej a územne neobmedzenej licencie. Tieto podmienky sa nevzťahujú na tzv. krabicový softvér, ktorý je predávaný ako produkt či už realizátora alebo tretej strany.
- Z hľadiska plnenia cieľov projektu bude výsledkom projektu naplnenie hlavného cieľa, t.j. súlad KIB so zákonom o kybernetickej bezpečnosti a so zákonom o ISVS, čo bude naplnené realizáciu nasledovných partikulárnych cieľov:
    - Organizácia kybernetickej a informačnej bezpečnosti
    - Riadenie rizík
    - Personálna bezpečnosť
    - Riadenie prístupov
    - Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami
    - Bezpečnosť pri prevádzke informačných systémov a sietí
    - Sieťová a komunikačná bezpečnosť

    - Zaznamenávanie udalostí a monitorovanie
    - Kontinuita prevádzky
    - Audit a kontrolné činnosti
- Technologicky a administratívne pôjde o realizáciu nasledovných cieľov:
    - vypracovanie a aktualizácia kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB,
    - obstaranie, implementácia a nasadenie firewallov a realizácia segmentácie siete,
    - obstaranie a implementácia nástroja na sledovanie dátových tokov,
    - obstaranie a implementácia nástroja na centrálne ukladanie systémových logov,
    - implementácia dohľadového systému na sledovanie prevádzkových parametrov siete,
    - obstaranie a implementácia nástrojov na sledovanie a detekciu neoprávnených spojení na hranici siete,
    - rozšírenie kapacít existujúceho diskového poľa pre potreby zálohy prevádzkových dát.

5. NÁHĽAD ARCHITEKTÚRY

Architektúra celého riešenia je v zmysle usmernenia MIRRI SR rámcová tak, aby bolo z projektu zrejmé, ktoré komponenty v rámci realizácie projektu budú vytvorené (a budú realizovať opatrenia KIB).

Primárne opatrenia kybernetickej bezpečnosti chránia IS TN UNI, ktoré sú určené na prevádzkovanie univerzitných služieb TN UNI. Z vyššie definovaných potrieb je zrejmé, o aké komponenty zabezpečenia pôjde - firewall, segmentácia siete, centrálny logovací nástroj, nástroj na sledovanie prevádzkových parametrov siete, nástroje na detekciu v sieti a na hranici siete, nástroj na analýzu dátových tokov v sieti, kompletná dokumentácia podľa ZoKB vrátane BCM plánov.



6. LEGISLATÍVA

V rámci platnej legislatívy nebude potrebné meniť žiadnu legislatívu. 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

Vyhláška č.78/2020 Z.z. o štandardoch pre ITVS

Vyhláška č.401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy

Vyhláška 179/2020 Z.z. o obsahu bezpečnostných opatrení ITVS

Vyhláška 362/2018 Z.z. o obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení)

7. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU a METÓDA JEHO RIADENIA

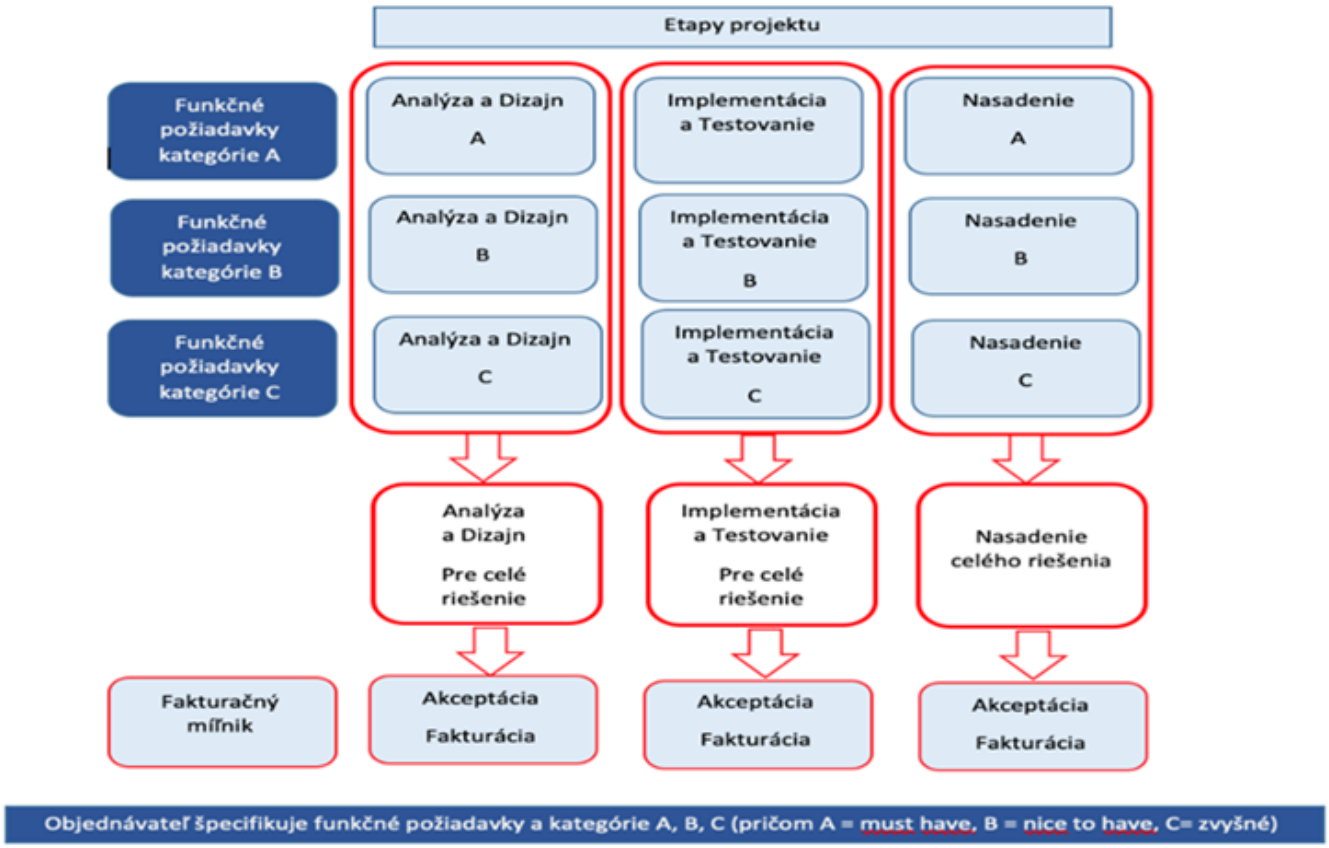
Harmonogram projektu je definovaný na základe odporúčania MIRRI SR, ktoré predpokladá trvanie projektu na úrovni približne jedného roka. S ohľadom na potreby nákupu a implementácie technológií vrátane potreby ich skúšobnej prevádzky sa s týmto časom stotožňujeme.

Začiatok realizačnej fázy projektu vyplýva z predpokladu, že realizácia projektu začne až po ukončení administratívneho a odborného hodnotenia a po podpise Zmluvy o NFP, pričom je definovaná dostatočná časová rezerva na tieto úkony. Rovnako na procesy verejného obstarávania, ktoré môžu potenciálne začať v krátkom čase po podaní žiadosti o NFP.

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA
1.	Prípravná fáza a Iniciačná fáza	4/2024	12/2024	Podpísanie zmluvy o NFP Spustenie procesov VO
2.	Realizačná fáza	01/2025	11/2025	Podpísanie zmlúv s dodávateľmi po ukončení VO,realizácia prokjektu
2a	Analýza a Dizajn	02/2025	05/2025	
2b	Nákup technických prostriedkov, programových prostriedkov a služieb	04/2025	08/2025	
2c	Implementácia a testovanie	08/2025	10/2025	Min. 2 mesiace test. prevádzky
2d	Nasadenie opatrení	10/2025	11/2025	
3.	Dokončovacia fáza	10/2025	12/2025	Počas dokončovacej fázy projektový manažér pripraví podklady a odovzdá na schválenie záverečnú žiadosť o platbu a záverečnú monitorovaciu správu.
4.	Podpora prevádzky (SLA)	01/2026	01/2031	Obdobie udržateľnosti

Ako metóda riadenia projektu bude použitá metóda „Waterall“. Táto metóda sa ukázala byť ako najvhodnejšia nakoľko svojimi charakteristikami a možnosťami plne zodpovedá požiadavkám a predstavám univerzity.

Schéma metódy projektového riadenia:



8. ROZPOČET A PRÍNOSY

V uvedenom projekte vychádzame pri stanovení rozpočtu z prieskumu trhu a pravidiel stanovených výzvou. S ohľadom na rozpočet projektu (projekt do 1 000 000,00,- EUR) nebola spracovaná Analýza nákladov a prínosov.

8.1 Sumarizácia nákladov a prínosov

Náklady	Infraštruktúra pre prevádzku kybernetickej bezpečnosti	Dokumentácia KB	Pre všetky podaktivity:
IT - CAPEX			
Aplikácie			
SW	34 461,60 Eur		
HW	141 600,00 Eur		
Práce/služby	33 600,00 Eur	67 200,00 Eur	
Mzdy interní zamestnanci			78 275,00 Eur
Paušálne výdavky			24 859,56 Eur
IT - OPEX- prevádzka			
Aplikácie			
SW	34 461,60Eur		
HW			

Sumarizácia podľa podaktivít:

Názov	HW	SW	Služby

1.Vytvorenie katalógu informačných aktív a realizovaním analýzy rizík na identifikovaných aktívach	-	-	5 400,- €
2.Vytvorenie kompletnej bezpečnostnej dokumentácie podľa požiadaviek ZoKB Prílohy č. 1 k vyhláške č. 362/2018 Z. z.	-	-	29 400,- €
3. Zvýšenie bezpečnosti pri prevádzke informačných systémov a sietí dobudovaním záložných dátových kapacít, vrátane vytvorenia súvisiacej dokumentácie a BCM plánov.	72 000,- €	3 600,- €	30 000,- €
4.Zvýšenie sieťovej a komunikačnej bezpečnosti nasadením a implementáciou perimetrového firewallu v HA móde	32 400,- €	21 600,- €	10 800,- €
5.Implementácia systémov na nepretržitú kontrolu dátových tokov v interných sieťach univerzity	15 840,- €	5 481,60- €	4 800,- €
6.Implementácia centrálneho log manažment systému pre zber a ukladanie logov zo systémov univerzity s možnosťou korelácie incidentov a eventov a vytvárania alertov	21 360,- €	3 780,- €	6 000,- €
7.Implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov.	-	-	6 000,- €
8.Vykonanie certifikovaného auditu kybernetickej bezpečnosti v súlade so ZoKB.	-	-	8 400,- €

V prípade projektov kybernetickej bezpečnosti je priame vyčíslenie návratnosti pomerne komplikované. Z pohľadu návratnosti je potrebné venovať sa hodnoteniu možných škôd, ktoré by vznikli v prípade, že nebude adekvátne riešená KIB na úrovni poskytovateľa základnej služby. Ide o nasledovné potenciálne škody:

Finančné riziko – dôsledky kybernetického útoku. Ide o možné sankcie vyplývajúce priamo z legislatívnych rámcov, prípadných súdnych sporov (v prípade napríklad úniku osobných údajov) ako aj nákladov spojených so sanáciou prípadného kybernetického incidentu. Tieto finančné prostriedky nie je možné momentálne vyčísliť, reálne však môže niekoľko násobne prekročiť straty interných finančných prostriedkov univerzity.

Reputačné riziko – vzhľadom na postavenie a oblasť spoločenskej dôležitosti a zákonných povinností univerzity, je toto riziko potenciálne vysoké – teda v prípade neplnenia legislatívnych požiadaviek v zmysle zákona o kybernetickej bezpečnosti a zákona o ISVS alebo vyhlášky 362 /2018 Z. z. či reálneho výpadku prevádzky základnej služby, úniku citlivých dát v kombinácii aj s prípadnou medializáciou a pod.

9. PROJEKTOVÝ TÍM

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

- Predseda RV – doc. Ing. Jozef Habánik, PhD.
- Biznis vlastník – Ing. Peter Franko
- Zástupca prevádzky - Martin Šedivá
- Projektový manažér objednávateľa (PM) – Ing. Zuzana Jakubíková, PhD
- Iný člen RV - Ing. Mária Šedivá
- Iný člen RV - Ing. Slavomír Beznák

Projektový tím objednávateľa:

- Manažér kybernetickej bezpečnosti (Juraj Porubčan) - životopis v prílohe
- Kľúčový používateľ (Ing. Peter Franko)
- IT analytik (Martin Šedivý)
- IT architekt (Slavomír Beznák)
- Projektový manažér objednávateľa (PM) – Ing. Zuzana Jakubíková, PhD

ID	Meno a Priezvisko	Pozícia	Oddelenie	Rola v projekte
1.	Ing. Zuzana Jakubíková, PhD	Projektový manažér	Oddelenie riadenia projektov	Projektový manažér
2.	Juraj Porubčan	Manažér kybernetickej bezpečnosti		Manažér kybernetickej bezpečnosti
3.	Martin Šedivý	odborný zamestnanec IT	Centrum informačných technológií	IT analytik
4.	Slavomír Beznák	odborný zamestnanec IT	Centrum informačných technológií	IT architekt

Pracovné náplne projektového tímu sú prílohou názvom: pracovné náplne PT univerzita Trenčín.

Všetci členovia tímu sú internými zamestnancami TN UNI ku dňu podania ŽoNFP (okrem MKB, ktorý bude zamestnaný).

Stručne zodpovednosti jednotlivých rolí:

Projektová rola: Biznis vlastník

Zodpovedný za:

- Realizáciu dohľadu nad súladom projektových výstupov s požiadavkami koncových používateľov.
- Spoluprácu pri riešení odpovedí na otvorené otázky a riziká projektu.
- Posudzovanie, pripomienkovanie, testovanie a protokolárne odsúhlasovanie projektových výstupov v príslušnej oblasti (v biznis procese) po vecnej stránke (najmä procesnej a legislatívnej) · Riešenie problémov a požiadaviek v spolupráci s odbornými garantmi,
- Spoluprácu pri špecifikácii a poskytuje súčinnosť pri riešení zmenových požiadaviek · Schválenie funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu z pohľadu používateľov koncového produktu
- Definovanie očakávaní na kvalitu projektu, kritérií kvality projektových produktov, prínosov pre koncových používateľova požiadaviek na bezpečnosť, · Definovanie merateľných výkonnostných ukazovateľov projektov a prvkov,
- Sledovanie a odsúhlasovanie nákladovosti, efektívnosti vynakladania finančných prostriedkov a priebežné monitorovanie a kontrolu odôvodnenia projektu (BC/CBA)
- Schválenie akceptačných kritérií,
- Riešenie problémov používateľov
- Akceptáciu rozsahu a kvality dodávaných projektových výstupov pri dosiahnutí platobných míľnikov,
- Vykonanie UX a UAT testovania
- Odsúhlasenie spustenia výstupov projektu do produkčnej prevádzky,
- Dostupnosť a efektívne využitie ľudských zdrojov alokovaných na realizáciu projektu,
- Vykonávanie monitorovania a hodnotenia procesov v plánovaných intervaloch.
- Poskytovanie vyjadrení k zmenovým požiadavkám, k ich opodstatnenosti a prioritizácii
- Zisťovanie efektívneho spôsobu riadenia a optimalizácie zvereného procesu, vrátane analyzovanie všetkých vyskytujúcich sa nezhôd,
- Okrem zvažovaní rizík prevádzkových alebo podporných procesov súčasne vlastník napomáha identifikovať príležitosti,
- Zlepšovanie a optimalizáciu procesov v spolupráci s ďalšími prepojenými vlastníkmi procesov a manažérom kvality,
- Odsúhlasenie akceptačných protokolov zmenových konaní
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1 plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

-

Projektová rola: Projektový manažér objednávateľa (PM)

Zodpovedný za:

- Riadenie projektu podľa pravidiel stanovených vo Vyhláške 401/2023 Z. z.
- Riadenie prípravy, inicializácie a realizácie projektu
- Identifikovanie kritických miest projektu a navrhovanie ciest k ich eliminácii ·
- Plánovanie, organizovanie, motivovanie projektového tímu a monitorovanie projektu
- Zabezpečenie efektívneho riadenia všetkých projektových zdrojov s cieľom vytvorenia a dodania obsahu a zabezpečenie naplnenie cieľov projektu
- Určenie pravidiel, spôsobov, metód a nástrojov riadenia projektu a získanie podpory Riadiaceho výboru (RV) pre riadenie, plánovanie a kontrolu projektu a využívanie projektových zdrojov
- Zabezpečenie vypracovania manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z. Z., Prílohou č.1
- Zabezpečenie realizácie projektu podľa štandardov definovaných vo Vyhláške 78/2020 Z.z.
- Zabezpečenie priebežnej aktualizácie a verzionovania manažérskej a špecializovanej dokumentácie v minimálnom rozsahu Vyhlášky 401/2023 Z. , Prílohy č.1
- Vypracovanie, pravidelné predkladanie a zabezpečovanie prezentácie stavov projektu, reportov, návrhov riešení problémov a odsúhlasovania manažérskej a špecializovanej dokumentácie v rozsahu určenom Vyhláškou 401/2023 Z. z., Prílohou č.1 na rokovanie RV
- Riadenie a operatívne riešenie a odstraňovanie strategických / projektových rizík a závislostí
- Predkladanie návrhov na zlepšenia na rokovanie Riadiaceho výboru (RV)
- Zabezpečenie vytvorenia a pravidelnej aktualizácie BC/CBA a priebežné zdôvodňovanie projektu a predkladanie na rokovania RV
- Celkovú alokáciu a efektívne využívanie ľudských a finančných zdrojov v projekte
- Celkový postup prác v projekte a realizuje nápravné kroky v prípade potreby
- Vypracovanie požiadaviek na zmenu (CR), návrh ich prioritizácie a predkladanie zmenových požiadaviek na rokovanie RV
- Riadenie zmeny (CR) a prípadné požadované riadenie konfigurácií a ich zmien
- Riadenie implementačných a prevádzkových aktivít v rámci projektov.
- Aktívne komunikuje s dodávateľom, zástupcom dodávateľa a projektovým manažérom dodávateľa s cieľom zabezpečiť úspešné dodanie a nasadenie požadovaných projektových výstupov,
- Formálnu administráciu projektu, riadenie centrálneho projektového úložiska, správu a archiváciu projektovej dokumentácie
- Kontrolu dodržiavania a plnenia míľnikov v zmysle zmluvy s dodávateľom,
- Dodržiavanie metodík projektového riadenia,
- Predkladanie požiadaviek dodávateľa na rokovanie Riadiaceho výboru (RV),
- Vecnú a procesnú administráciu zúčtovania dodávateľských faktúr

Projektová rola: KĽUČOVÝ POUŽIVATEĽ (end user)

Zodpovedný za:

- Návrh a špecifikáciu funkčných a technických požiadaviek
- Jednoznačnú špecifikáciu požiadaviek na jednotlivé projektové výstupy (špecializované produkty a výstupy) z pohľadu vecno-procesného a legislatívy
- Vytvorenie špecifikácie, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, · Špecifikáciu požiadaviek koncových používateľov na prínos systému
- Špecifikáciu požiadaviek na bezpečnosť,
- Návrh a definovanie akceptačných kritérií,
- Vykonanie používateľského testovania funkčného používateľského rozhrania (UX testovania)
- Finálne odsúhlasenie používateľského rozhrania
- Vykonanie akceptačného testovania (UAT)
- Finálne odsúhlasenie a akceptáciu manažérskych a špecializovaných produktov alebo projektových výstupov
- Finálny návrh na spustenie do produkčnej prevádzky,
- Predkladanie požiadaviek na zmenu funkcionalít produktov
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1
- Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu
- Realizáciu kvalitatívneho používateľského výskumu (nastavenie požiadaviek na regrutáciu, návrh scenára, vedenie rozhovoru a vyhodnotenie výskumu).
- Realizáciu kvantitatívneho používateľského výskumu (nastavenie požiadaviek na regrutáciu, návrh scenára, vedenie dotazníku a vyhodnotenie výskumu).
- Syntetizáciu biznis, technických a používateľských požiadaviek.
- Realizáciu formatívnych a sumatívnych testovaní použiteľnosti (nastavenie požiadaviek na regrutáciu, návrh scenára, vedenie rozhovoru a vyhodnotenie výskumu).
- Návrh informačnej architektúry a to najmä metódami triedenia kariet (card sorting), návrhom mapy stránky a screen flow.
- Tvorbu, testovanie a iteráciu prototypov – napr. pomocou Axure, Sketch, Figma alebo Adobe XD
- Mapovanie zákazníckych ciest
- Analýzu a návrh riešenia problematiky prístupnosti webových sídiel,
- Podporu a spoluprácu pri tvorbe Stratégie riadenia kvality (princípy, kritériá kvality),
- Spoluprácu pri vytváraní funkčných požiadaviek na výstupy z pohľadu dohľadu a UX,
- Vedenie a aktualizáciu príslušných projektových výstupov a registrov,
- Hodnotenie jednotlivých verzií výstupov projektu z pohľadu dohľadu, kontroly a UX v jednotlivých etapách,
- Vytváranie hodnotiacich kritérií na dohľad výstupov a príslušných záznamov, o ktorých reportuje projektovému manažérovi objednávateľa,
- Nastavenie a dohľad nad procesom testovania a pripomienkovanie stratégie testovania, plánov a testovacích scenárov,
- Účasť na kontrolných aktivitách počas implementácie výstupov
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1
- Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

-

Projektová rola: IT analytik

Zodpovedný za:

- Vykonanie analýzy procesných a ďalších požiadaviek a vytvorenie špecifikácie súčasného alebo budúceho užívateľa softwaru („zákazníka“) a následne navrhuje dizajn a programátorské riešenie.
- Participáciu na vývoji nových, ale i vylepšovaní existujúcich aplikácií v rámci celého vývojového cyklu – systémová analýza, dizajn, kódovanie, užívateľské testovanie, implementácia, podpora, dokumentácia. Úzko spolupracuje aj s IT architektom.
- Analýza potrieb zákazníka vrátane tvorby úplnej analytickej dokumentácie a vstupov do verejného obstarávania (VO).
- Mapovanie požiadaviek do návrhu funkčných riešení.
- Návrh a správa katalóg požiadaviek - registra požiadaviek riešenia
- Analýza funkčných a nefunkčných požiadaviek,
- Návrh fyzického a logického modelu,
- Návrh testovacích scenárov,
- V priebehu implementácie robí dohľad nad zhodou výstupov s pôvodným analytickým zadaním.
- Zodpovednosť za dodržovanie správnej metodiky pri postupe analýzy
- Definovanie akceptačných kritérií v projekte
- Odsúhlasenie opisu produktov, ktoré predstavujú vstupy alebo výstupy (priebežné alebo konečné) úloh dodávateľov, alebo ktoré ich priamo ovplyvňujú a zabezpečovať akceptáciu produktov po ich dokončení
- Priraďuje priority a poskytuje stanoviská používateľov na rozhodnutia Riadiaceho výboru projektu – k realizácii zmenových požiadaviek
- Poskytuje merania aktuálneho stavu pre potreby porovnania s výsledkami projektu vzhľadom na realizáciu prínosov
- Rieši požiadavky používateľov a konflikty iných priorít
- Posúdenie prevádzkovo-infraštruktúrnej dokumentácie pred akceptáciou a prevzatím od dodávateľa
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1
- Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

-

Projektová rola: IT architekt

Zodpovedný za:

- Navrhovanie architektúry IT riešení s cieľom dosiahnuť najlepšiu efektivitu.
- Transformovanie cieľov, prísľubov a zámerov projektu do tvorby reálnych návrhov a riešení.
- Navrhovanie takých riešení, aby poskytovali čo najvyššiu funkčnosť a flexibilitu. ·
- Posudzovanie vhodnosti navrhnutých riešení s ohľadom na požiadavky projektu. ·
- Zodpovednosť za technické navrhnutie a realizáciu projektu.
- Zodpovednosť za vytvorenie technickej IT dokumentácie a jej následná kontrola. ·
- Zodpovednosť za definovanie integračných vzorov, menných konvencií, spôsobov návrhu a spôsobu programovania.
- Definovanie architektúry systému, technických požiadaviek a funkčného modelu (Proof Of Concept.)
- Vytvorenie požiadaviek na HW/SW infraštruktúru IS
- Udržiavanie a rozvoj konzistentnej architektúry s dôrazom na architektúru aplikačnú, dátovú a infraštruktúru
- Analýzu a odhad náročnosti technických požiadaviek na vytvorenie IS alebo vykonanie zmien v IS
- Navrhovanie riešení zohľadňujúce architektonické štandardy, časové a zdrojové obmedzenia,
- Navrhovanie dátových transformácií medzi dátovými skladmi a aplikáciami
- Vyhodnocovanie implementačných alternatív z pohľadu celkovej IT architektúry
- Ladenie dátových štruktúr za účelom dosiahnutia optimálneho výkonu
- Prípravu akceptačných kritérií · Analýza nových nástrojov, produktov a technológií
- Správa, rozvoj a dohľad nad dodržiavaním integračných štandardov
- Priebežné posudzovanie vecných výstupov dodávateľa v rámci analýzy, návrhu riešenia vrátane Detailného návrhu riešenia (DNR) z pohľadu analýzy a návrhu riešenia architektúry IS
- Vykonáva posudzovanie a úpravu testovacej stratégie, testovacích scenárov, plánov testov, samotné testovanie a účasť na viacerých druhoch testovania
- Vykonanie záťažových, výkonnostných a integračných testov a navrhnutie následných nápravných
- Nasadenie a otestovanie migrácie, overenie kvality dát a navrhnutie nápravných opatrení
- Participáciu na výkone bezpečnostných testov,
- Participáciu na výkone UAT testov,
- Posúdenie prevádzkovo-infraštruktúrnej dokumentácie pred akceptáciou a prevzatím od dodávateľa
- Aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1
- Plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

Projektová rola: manažér kybernetickej a informačnej bezpečnosti

Zodpovedný za:

- špecifikovanie štandardov, princípov a stratégií v oblasti ITB a KIB,
- ak je projekt primárne zameraný na problematiku ITB a KIB – je priamo zodpovedný za špecifikáciu a analýzu funkčných požiadaviek na ITB a KIB,
- špecifikovanie požiadaviek na ITB a KIB, kontroluje ich implementáciu v realizovanom projekte,
- špecifikovanie požiadaviek na bezpečnosť vývojového, testovacieho a produkčného prostredia,
- špecifikovanie funkčných a nefunkčných požiadaviek pre oblasť ITB a KIB,
- špecifikovanie požiadaviek na bezpečnosť v rámci bezpečnostnej vrstvy,
- špecifikovanie požiadaviek na školenia pre oblasť ITB a KIB,
- špecifikovanie požiadaviek na bezpečnostnú architektúru riešenia a technickú infraštruktúru pre oblasť ITB a KIB,
- špecifikovanie požiadaviek na dostupnosť, zálohovanie, archiváciu a obnovu IS vzťahujúce sa na ITB a KIB,
- realizáciu posúdenie požiadaviek agendy ITB a KIB na integrácie a procesov konverzie a migrácie, identifikácia nesúladu a návrh riešenia
- špecifikovanie požiadaviek na ITB a KIB, bezpečnostný projekt a riadenie prístupu,
- špecifikovanie požiadaviek na testovanie z hľadiska ITB a KIB, realizáciu kontroly zapracovania a retestu,
- špecifikovanie požiadaviek na obsah dokumentácie v zmysle legislatívnych požiadaviek pre oblasť ITB a KIB, ako aj v zmysle "best practies",
- špecifikovanie požiadaviek na dodanie potrebnej dokumentácie súvisiacej s ITB a KIB kontroluje ich implementáciu v realizovanom projekte,
- špecifikovanie požiadaviek a konzultácie pri návrhu riešenia za agendu ITB a KIB v rámci procesu „Mapovanie a analýza technických požiadaviek - detailný návrh riešenia (DNR)“,
- špecifikáciu požiadaviek na bezpečnosť IT a KIB v rámci procesu "akceptácie, odovzdania a správy zdroj. kódov“
- špecifikáciu akceptačných kritérií za oblasť ITB a KIB,
- špecifikáciu pravidiel pre publicitu a informovanosť s ohľadom na ITB a KIB,
- poskytovanie konzultácií pri tvorbe šablón a vzorov dokumentácie pre oblasť ITB a KIB,
- získavanie informácií nutných pre plnenie úloh v oblasti ITB a KIB,
- špecifikáciu podmienok na testovanie, reviduje výsledky a výstupy z testovania za oblasť ITB a KIB,
- konzultácie a vykonávanie kontrolnej činnosť zameranej na obsah a komplexnosť dok. z hľadiska ITB a KIB,
- špecifikáciu požiadaviek na bezpečnostný projekt pre oblasť ITB a KIB,
- realizáciu kontroly zameranej na naplnenie požiadaviek definovaných v bezp. projekte za oblasť ITB a KIB
- realizáciu kontroly zameranú na správnosť nastavení a konfigurácii bezpečnosti jednotlivých prostredí,
- realizáciu kontroly zameranú realizáciu procesu posudzovania a komplexnosti bezpečnostných rizík, bezpečnosť a kompletný popis rozhraní, správnu identifikácia závislostí,

- realizáciu kontroly naplnenia definovaných požiadaviek pre oblasť ITB a KIB,
- realizáciu kontroly zameranú na implementovaný proces v priamom súvise s ITB a KIB,
- realizáciu kontroly súladu s planou legislatívou v oblasti ITB a KIB (obsahuje aj kontrolu leg. požiadaviek)
- realizáciu kontroly zameranú zabezpečenie procesu, interfejsov, integrácii, kompletného popisu rozhraní a spoločných komponentov a posúdenia z pohľadu bezpečnosti, · poskytovanie konzultácií a súčinnosti pre problematiku ITB a KIB,
- získavanie a spracovanie informácií nutných pre plnenie úloh v oblasti ITB a KIB,
- aktívnu účasť v projektových tímoch a spoluprácu na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Vyhláškou 401/2023 Z.z., Prílohou č.1 plnenie pokynov projektového manažéra a dohôd zo stretnutí projektového tímu

10. PRÍLOHY

Príloha : 1 – Pracovné náplne,

2 - Zoznam rizík a závislostí,

3 - Dopad kybernetického bezpečnostného incidentu v závislosti (§ 24 ods. 2 písm. a) až e) zákona 69/2018 Z.z)