MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PROJEKTOVÝ ZÁMER

Manažérsky výstup I-02

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

Povinná osoba	*Slovenský hydrometeorologický ústav*
Názov projektu	*Rozvoj kybernetickej a informačnej bezpečnosti v SHMÚ*
Zodpovedná osoba za projekt	*Meno a priezvisko osoby, ktorá predkladá dokumenty (zamestnanec /Projektový manažér)*
Realizátor projektu	*Slovenský hydrometeorologický ústav*
Vlastník projektu	*Slovenský hydrometeorologický ústav*

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Schválenie	RNDr. Ondrej Tóth	SHMÚ	Poverený riaditeľ úseku informatika		

1. HISTÓRIA DOKUMENTU

Verzia	Dátum	Zmeny	Meno
0.1	30.4.2024	Pracovný návrh v súlade s vyhláškou č. 401/2023 Z. z.	OTO

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

Účelom tohto dokumentu je vytvoriť projektový zámer popisujúci rozšírenie súčasnej architektúry kybernetickej bezpečnosti v Slovenskom hydrometeorologickom ústave v rámci rozvoja informačnej a kybernetickej bezpečnosti pomocou finančných prostriedkov z európskych fondov.

V súlade s Vyhláškou 401/2023 Z. z. 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.

2.1 Použité skratky a pojmy

SKRATKA/POJEM	POPIS
AR	Analýza rizík
IS	Informačný systém
ITVS	Informačné technológie verejnej správy
KIB	Kybernetická a informačná bezpečnosť
METAIS	Centrálny metainformačný systém verejnej správy
SHMÚ	Slovenský hydrometeorologický ústav
VO	Verejné obstarávanie
ZoKB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
ZoITVS	Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

2.2 Konvencie pre typy požiadaviek (príklady)

Požiadavky majú nasledovnú konvenciu:

FWxx – požiadavky týkajúce sa bezpečnostného riešenia perimetra siete (firewall)

- xx – číslo požiadavky

BPxx – požiadavky týkajúce sa bezpečnostného riešenia pre oblasť zálohovania

- xx – číslo požiadavky

3. DEFINOVANIE PROJEKTU

3.1 Manažérske zhrnutie

Slovenský hydrometeorologický ústav (SHMÚ) je špecializovaná organizácia vykonávajúca hydrologickú a meteorologickú službu na národnej aj medzinárodnej úrovni. Činnosť SHMÚ sa riadi najmä zákonom 201/2009 Z. z. o štátnej hydrologickej službe a štátnej meteorologickej službe.

SHMÚ monitoruje kvantitatívne a kvalitatívne parametre stavu ovzdušia a vôd na území Slovenskej republiky, zhromažďuje, overuje, hodnotí, archivuje a interpretuje údaje a informácie o stave a režime ovzdušia a vôd, popisuje deje v atmosfére a hydrosfére, tvorí a vydáva meteorologické a hydrologické predpovede, výstrahy a informácie. Údaje, informácie a výsledky štúdií poskytuje užívateľom a verejnosti.
V jednotlivých činnostiach všetkých oblastí dochádza k neustálemu zvyšovaniu závislosti na informačných aktívach a IKT, čo zvyšuje hrozby, zraniteľnosti a riziká dopadov bezpečnostných incidentov v kybernetickom priestore.

SHMÚ je v zmysle ZoKB prevádzkovateľom základnej služby. V registri prevádzkovateľov základných služieb je zaradený v sektore Verejná správa. Ústredným orgánom je pre SHMÚ v zmysle ZoKB a riadiacim orgánom v zmysle ZoITVS Ministerstvo životného prostredia SR.

SHMÚ má zrealizované nasledovné aktivity v zmysle ZoKB a vyhlášky NBÚ č. 362/2018 Z.Z.

- Implementovaný systém riadenia kybernetickej bezpečnosti od 1.12.2020. V rámci implementácie bola:
- vytvorená stratégia kybernetickej bezpečnosti
- vytvorené bezpečnostné politiky kybernetickej bezpečnosti
- vykonaná inventarizácia aktív, klasifikácia informácií a kategorizácia sietí a informačných systémov
- realizovaná analýzu rizík a analýza dopadov, vrátane riadenia rizík
- vykonané dva zákonné audity kybernetickej bezpečnosti, naposledy v októbri 2023.

Zaradenie informačných systémov základnej služby v prostredí SHMÚ do kategórií v zmysle ZoKB:
kategória I – 2 ks informačných systémov
kategória II – 7 ks informačných systémov
Počet prvkov kritickej infraštruktúry – 4ks

Projekt adresuje dve oblasti, kde vykonaná analýza rizík identifikovala najzávažnejšie nedostatky v bezpečnostných opatreniach. Tieto nedostatky boli konštatované aj nezhodami z auditov a odporúčaniami audítora. Jedná sa o oblasť sieťovej bezpečnosti (bezpečnostné riešenie segmentu perimetra siete - firewall) a oblasti prevádzky informačných systémov a biznis kontinuity (zálohovanie). Obe oblasti sú podrobnejšie popísané v ďalších kapitolách. Predmet projektu sa týka úloh, ktoré nebolo možné do dnešného dňa splniť z dôvodu absencie finančných prostriedkov a je potrebné zabezpečiť ich splnenie v čo najkratšom čase. Obsahom projektu v oboch oblastiach je obstaranie bezpečnostného riešenia pozostávajúceho z HW komponentov, licencií, implementačných a podporných služieb. Ich konkrétna skladba je uvedená v kapitole technologickej vrstvy.

Analýza rizík aj záverečná správa auditu kybernetickej bezpečnosti konštatujú aj iné riziká v iných oblastiach podľa vyhlášky NBÚ č.362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. Oblasti pre tento projekt boli vybrané tak, aby nekolidovali s inými príležitosťami, ktoré chce SHMÚ realizovať na mitigáciu iných rizík/nesúladov. Na vysvetlenie, SHMÚ uzavrel Memorandum o spolupráci s Ministerstvom investícií, regionálneho rozvoja a informatizácie Slovenskej republiky v rámci projektu Posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov (ITVS). Menovaný projekt adresuje oblasti, ktoré sme do cieľov projektu v rámci tejto výzvy nezahrnuli.

Pomocou projektu budú zavedené opatrenia ako sú:

- inštalácia zariadení v internej sieti,
- inštalácie softvéru v interných sieťach a informačných systémoch,
- zaznamenávanie bezpečnostných záznamov
- zaznamenávanie a vyhodnocovanie prevádzkových záznamov
- obstaranie zariadení a 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 v inom objekte a minimalizovania rizika poškodenia alebo zničenia dátových nosičov archivačných záloh vplyvom prírodných živlov alebo havárie.

3.2 Motivácia a rozsah projektu

Cieľom tohto projektu je dosiahnuť zlepšenie miery súladu v oblastiach, kde SHMÚ vníma najväčšie nesúlady vyplývajúce z auditu kybernetickej bezpečnosti a analýzy rizík indikujúcej najväčšie dopady v prípade závažného bezpečnostného incidentu. Zároveň je cieľom projektu zabezpečenie súladu s legislatívnymi požiadavkami v oblasti kybernetickej a informačnej bezpečnosti v zmysle ZoKB a ZoITVS a zvýšenie úrovne bezpečnostných opatrení. V rámci auditu kybernetickej bezpečnosti bola konštatovaná súčasná implementácia bezpečnostných opatrení na 61% v súlade so zákonnými požiadavkami. Po ukončení projektu je plánované zabezpečenie súladu na 70-80%.

Popis východiskovej situácie

Oblasť bezpečnosť siete:

Perimeter siete v súčasnosti zabezpečujú komponenty inštalované v roku 2015 (firewall, VPN gateway, core switche). Zariadenia sú po životnosti bez možnosti ďalších bezpečnostných aktualizácií, takže sa prevádzkujú s niektorými neošetrenými zraniteľnosťami. SHMÚ nemá prístup ku všetkým komponentom manažmentu (vendor lock-in). Jedným z dôsledkov je aj to, že sa v dôsledku periodického zahltenia musí firewall proaktívne reštartovať dvakrát týždenne, čo má dopad (v rôznom rozsahu pre každé) na všetky existujúce spojenia v danej chvíli. VPN gateway neumožňuje efektívnym spôsobom nasadiť dvojfaktorovú autentifikáciu pre vzdialený prístup. Z dôvodu morálnej zastaranosti komponentov sa nedajú efektívne implementovať moderné prístupy pre zabezpečenie sieťovej prevádzky. Existujúce riešenie tiež obmedzuje do budúcnosti pokryť zvyšujúce sa nároky na priepustnosť siete.

Oblasť zálohovanie:

SHMÚ vykonáva zálohovanie podľa aktuálneho zálohovacieho plánu s použitím systému od výrobcu Veeam. Zálohy sa ukladajú na úložisko, ktoré je v tej istej budove asi 15 m od samotného dátového centra, čo je z hľadiska biznis kontinuity vyhodnotené ako riziko. V minulosti sa na mitigáciu tohto rizika vybrané zálohy kopírovali na záložnú lokalitu - prevádzkovanú NASES-om v Devínskej Novej Vsi v rámci Memoranda o spolupráci. Úložné kapacity na záložnej lokalite sú však v dôsledku riešenia rôznych

havarijných stavov v poruchovom stave a kopírovanie záloh na vzdialenú lokalitu sa momentálne nevykonáva, čo predstavuje veľké bezpečnostné riziko.

Nezálohovanie dát je jedným z najväčších rizík, ktorý SHMÚ môže čeliť. Hlavné oblasti, ktoré môžu zo situácie vyplynúť a ovplyvniť chod organizácie sú strata dát v dôsledku HW poruchy, vonkajšie útoky a poškodenia dát, ľudské chyby – napr. neúmyselné zmazanie. Ako organizácia kritickej infraštruktúry máme povinnosť udržať dáta v bezpečí. Stratou dôležitých dát môže prísť k narušeniu produktivity práce a ohrozeniu dlhodobých radov meraní, ktoré slúžia na spresnenie poskytovaných údajov a služieb štátu a iným organizáciám.

V prípade nerealizácie projektu môže závažný kybernetický bezpečnostný incident spôsobiť dopad na nasledujúce počty postihnutých osôb:

- SHMÚ prevádzkuje systémy, ktorých nedostupnosť by zasiahla viac ako 100 000 osôb. Jedná sa o právnické osoby ako aj fyzické osoby, jednotky krízového riadenia. Napr. agendové systémy majú závažný dopad na používateľov.
- SHMÚ prevádzkuje informačné systémy základnej služby pre používateľov na celom území SR. Výpadok základnej služby resp. ISVS a jej obmedzenie alebo narušenie prevádzky má dopad v rozsahu viac ako 100 000 používateľských hodín.
- V rámci súčasného stavu v prípade nefunkčnosti informačných systémov nie je k dispozícii náhradné riešenie.
- Nefunkčnosť systémov má vplyv na spoločenské činnosti, verejný poriadok a verejnú bezpečnosť napr. ohlasovanie výstrah na nebezpečné meteorologické alebo hydrologické javy
- SHMÚ zabezpečuje predpovedné služby pre civilné letectvo a prevádzku letísk

Aktuálne informácie o službách a informačných systémoch v SHMÚ, na ktoré má závažný bezpečnostný incident dopad, sú evidované v METAIS (v prevádzke alebo plánované naďalej používať a rozvíjať):

Kód MetaIS	Názov
isvs_10889	Evidenčný a notifikačný systém oprávnených meraní a technických činností
isvs_11047	IS SK BIO
isvs_11085	Zverejňovanie informácií na webovom sídle: https://oeab.shmu.sk/
isvs_308	Informačný systém Hydrologická informačná a predpovedná služba
isvs_309	Klimatologický a Meteorologický informačný Systém
isvs_310	Súhrnná evidencia o vodách
isvs_311	Čiastkový monitorovací systém "Rádioaktivita životného prostredia"
isvs_312	Informačný systém Kvalita ovzdušia
isvs_329	Národný register znečisťovania z oblasti vody, ovzdušia, odpadov a pôdy
isvs_7297	Mzdový a personálny systém SHMÚ Magma HCM
isvs_7298	Dochádzkový systém SHMÚ ID.EST Sense
isvs_7299	Ekonomický systém SHMÚ SOFTIP
isvs_7300	Registratúrny systém SHMÚ Nuntio
isvs_9523	Optimalizácia dátových tokov v oblasti kvantity a kvality vody
isvs_9525	Národný Emisný Informačný Systém
isvs_9526	Hydrologický informačný systém
isvs_9527	ZBERNÉ INFORMAČNÉ SYSTÉMY SHMÚ
isvs_9528	IS HYPOS – POVAPSYS
isvs_9649	Informačný systém pre operatívnu meteorológiu

Cieľom projektu je aplikovať opatrenia v lokálnej infraštruktúre SHMÚ. Potenciálny incident na prvku perimetra siete však môže znamenať dopad na všetky vymenované služby a systémy.

3.3 Zainteresované strany/Stakeholderi

Zoznam subjektov, ktorý sa zúčastňuje projektu a akú rolu zastáva

ID	AKTÉR / STAKEHOLDER	SUBJEKT (názov / skratka)	ROLA (vlastník procesu/ vlastník dát/zákazník/ užívateľ …. člen tímu atď.)	Informačný systém (MetaIS kód a názov ISVS)
1.	*Ministerstvo investícií, regionálneho rozvoja a informatizácie SR*	*MIRRI*	*Gestor ZoITVS*	*N/A*
2.	*Národný bezpečnostný úrad*	*NBÚ*	*Gestor ZoKB*	*N/A*
3.	*SHMÚ*	*SHMÚ*	*Prevádzkovateľ ZS, ISVS*	*Pozri tabuľku v časti Motivácia*
4.	*Ministerstvo životného prostredia SR*	*MŽP SR*	*Riadiaci orgán vo vzťahu k SHMÚ z pohľadu ZoKB, ZoITVS*	*N/A*

3.4 Ciele projektu

Cieľom tohto projektu je dosiahnuť zlepšenie miery súladu v oblastiach, kde SHMÚ vníma najväčšie nesúlady vyplývajúce z auditu kybernetickej bezpečnosti a zavedenie opatrení tam, kde analýza rizík indikuje najväčšie dopady v prípade závažného bezpečnostného incidentu. Zároveň je cieľom projektu zabezpečenie súladu s legislatívnymi požiadavkami v oblasti kybernetickej a informačnej bezpečnosti v zmysle ZoKB a zvýšenie úrovne bezpečnostných opatrení.
Pomocou projektu budú zavedené opatrenia:

- implementácia nástrojov na riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami,
- implementácia segmentácie sietí, implementácia alebo obnova firewall-u,
- revízia firewall pravidiel
- inštalácia zariadení v internej sieti,
- inštalácie softvéru v interných sieťach a informačných systémoch,
- zaznamenávanie bezpečnostných záznamov
- zaznamenávanie a vyhodnocovanie prevádzkových záznamov
- obstaranie zariadení a 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 v inom objekte a minimalizovania rizika poškodenia alebo zničenia dátových nosičov archivačných záloh vplyvom prírodných živlov alebo havárie.

ID	Názov cieľa	Názov strategického cieľa	Spôsob realizácie strategického cieľa
01.	Zvýšenie úrovne KIB v SHMÚ	Riešenie KIB v SHMÚ	Opatrenia v zmysle Auditu KIB z roku 2023
02.	Program Slovensko Priorita: 1P1 Veda, výskum a inovácie RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy	Národná stratégia KB na roky 2021 – 2025: Kybernetická bezpečnosť ako základná súčasť verejnej správy	1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie (Oblasť - Kybernetická a informačná bezpečnosť)
03		401101003 - RSO1.2. Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a	Vybudovanie technického / užívateľského prostredia schopného čeliť hrozbám, najmä pre tie informačné technológie, ktoré sú zaradené do kritickej infraštruktúry.

	Prínosy digitalizácie pre orgány verejnej správy a ich používateľov	orgány verejnej správy (EFRR) - menej rozvinuté 401101004 - RSO1.2. Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy (EFRR) - viac rozvinuté	

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**
PR017	Používateľ	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Žiadosť – inovuje produkt cez novú technológiu	Používatelia/ rok	0	400	METAIS
PO095	Verejné inštitúcie	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	Verejné inštitúcie	0	1	METAIS

3.6 Špecifikácia potrieb koncového používateľa

N/A

3.7 Riziká a závislosti

V prílohe projektového zámeru sú popísané RIZIKÁ a ZÁVISLOSTI (detail v prílohe ZOZNAM RIZÍK a ZÁVISLOSTÍ)

3.8 Stanovenie alternatív v biznisovej vrstve architektúry

Výstupy projektu nemajú dopad na samotné biznis procesy a/alebo životné situácie.

3.9 Multikriteriálna analýza

Kritérium A: Redukovať riziká Perimetra siete

Kritérium B: Získať plnú manažovateľnosť celého riešenia Perimetra siete

Kritérium C: Realizovať zálohovanie na vzdialenej lokalite

Alternatíva 0: nulový variant, ktorý sa neposudzuje v MCA a je automaticky porovnávajúcim variantom - NEBUDE SA REALIZOVAŤ PROJEKT

Alternatíva 1: preferovaný variant, ktorý splnil všetky kritéria MCA,- BUDE SA REALIZOVAŤ PROJEKT

Alternatíva 2,: „redukovaný variant“, ktorý vychádza z rovnakého variantu ako preferovaný variant, ale realizuje opatrenie iba pre jednu z navrhovaných oblastí, BUDE SA REALIZOVAŤ LEN PRE Oblasť perimetra siete alebo zálohovania

Zoznam kritérií	Alternatíva 0	Spôsob dosiahnutia	Alternatíva 1	Spôsob dosiahnutia	Alternatíva 2	Spôsob dosiahnutia	Alternatíva 3	Spôsob dosiahnutia
Kritérium A	nie	systém Perimetra po životnosti	áno	implementovať podporované riešenie	áno	podporované riešenie	nie	nerealizovaná časť Perimeter
Kritérium B	nie	nie je prístup k celému riešeniu Perimeter (vendor lock)	áno	pri implementácii prevziať prístupy najvyššej úrovne	áno	pri implementácii prevziať prístupy najvyššej úrovne	nie	nerealizovaná časť Perimeter
Kritérium C	nie	nefunkčný systém vzdialenej Zálohy	áno	nasadiť funkčný systém	nie	nerealizovaná časť Zálohovanie	áno	nasadiť funkčný systém

3.10 Stanovenie alternatív v aplikačnej vrstve architektúry

N/A

3.11 Stanovenie alternatív v technologickej vrstve architektúry

Žiadateľ spracoval požiadavky na bezpečnostné riešenia technologicky neutrálne. Návrh konkrétnej architektúry bezpečnostného riešenia závisí od samotného dodávateľa. Nakoľko je v požiadavkách aj podpora produktu na 1 rok, ponúknuté ceny v súťaži budú reprezentovať aj TCO.

V prípade podpory zálohovacieho SW Veeam žiadateľ vybral alternatívu jeho rozšírenia z dôvodu kompatibility z existujúcim prevádzkovaným riešením. Začlenenie SW iného výrobcu do existujúceho riešenia by zvýšilo nároky na manažment a riziko plynúce z nekompatibility.

4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

- POPIS PRODUKTU:
  - implementované bezpečnostné riešenia v zmysle zadania (vrátane prístupových práv najvyššej úrovne)
  - špecializovaná dokumentácia implementovaných riešení
  - podpora na 1 rok v zmysle zadania

5. NÁHĽAD ARCHITEKTÚRY

Výstupy projektu nemajú dopad na architektúru verejnej správy. Výstupy projektu majú dopad len na lokálnu infraštruktúru SHMÚ.

5.1 Prehľad e-Government komponentov

Výstupy projektu nemajú dopad na e-Government komponenty a ich evidenciu v METAIS.

6. LEGISLATÍVA

Naplnenie cieľov a dodanie výstupov projektu nemá dopad na zmenu legislatívy. Cieľom projektu je zvýšenie súladu s existujúcou legislatívou uvedenou nižšie.

Slovenská republika ITVS

- Zákon 95/2019 Z.z. o informačných technológiách vo verejnej správe (od 27.3.2019)
- Vyhláška 179/2020 Z.z. o obsahu bezpečnostných opatrení ITVS (od 30.6.2020)

Slovenská republika KB

- Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025
- Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025
- Uznesenie Bezpečnostnej Rady SR č. 656 k pravidlám pre blokovanie útokov
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- Vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
- Vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
- Vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
- Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- Vyhláška Národného bezpečnostného úradu 493/2022 Z. z. o audite kybernetickej bezpečnosti
- Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti

7. ROZPOČET A PRÍNOSY

Kvantitatívne prínosy v rámci navrhovaného projektu sú:
- Zníženie nákladov súvisiacich s odstraňovaním kybernetických incidentov.

Kvalitatívne prínosy v rámci navrhovaného projektu sú:
- Zníženie pravdepodobnosti a hodnoty dopadov rizika kybernetického incidentu.
- Zvýšenie súladu s platnou legislatívou.
- Zvýšenie úrovne riadenia kybernetickej a informačnej bezpečnosti v rezorte.
- Zvýšená dôveryhodnosť a spokojnosť používateľov.

P. č.	Skupina výdavkov	Spolu	Popis
1.	022 – Samostatné hnuteľné veci a súbory hnuteľných vecí	376 371,10 €	Realizácia hlavných aktivít projektu v zmysle popisu.
2.	518 - Ostatné služby	27 292,42 €	Realizácia hlavných aktivít projektu v zmysle popisu.
3.	112 - Zásoby	15 844,80 €	Realizácia hlavných aktivít projektu v zmysle popisu.
4.	907 – Nepriame výdavky	29 365,58 €	Nepriame výdavky zahŕňajú náklad na projektového manažéra, administratívne kapacity a súvisiace náklady
	Celkové náklady na projekt	**448 873,90 €**	Sumy sú uvádzané s DPH

8. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU A METÓDA JEHO RIADENIA

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA

1.	Prípravná fáza	08/2024	09/2024	
2.	Realizačná fáza	09/2024	03/2025	Príprava a realizácia VO až po dodanie
4.	Implementácia a testovanie	03/2025	05/2025	Príprava na nasadenie v prostredí SHMÚ
5.	Nasadenie	05/2025	06/2025	Nasadenie do ostrej prevádzky
6.	Dokončovacia fáza	06/2025	07/2025	Ukončenie projektu, zúčtovanie, vyhodnotenie
7.	Prevádzka	07/2025	-	Následné aktivity

9. PROJEKTOVÝ TÍM

Zostavuje sa Riadiaci výbor (RV), v minimálnom zložení:

- Predseda RV
- Biznis vlastník
- Konečný používateľ
- Zástupca dodávateľa (bez hlasovacieho práva)

Zostavuje sa Projektový tím

- Projektový manažér
- Manažér kybernetickej a informačnej bezpečnosti
- Vecne príslušný odborný garant (prevádzka, infraštruktúra)
- Expert dodávateľa (podľa jednotlivých oblastí a aktivít)

ID	Meno a Priezvisko	Pozícia	Oddelenie/úsek	Rola v projekte
1.	RNDr. Ondrej Tóth	Poverený riaditeľ úseku informatika	Informačné technológie	Manažér informačnej a kybernetickej bezpečnosti
2.	Ing. Martin Borecký	Vedúci odboru IT	Informačné technológie	Vecný garant
4.	Zatiaľ neobsadené	Projektové riadenie	Odbor prípravy a implementácie projektu	Projektový manažér
5.	Zatiaľ neobsadené	Zástupca dodávateľa	Dodávateľ	Expert dodávateľa

10. ODKAZY

N/A

11. PRÍLOHY

- Register rizík a závislostí
- Záverečná správa z auditu KB na SHMÚ (11/2023 – neverejné citlivé informácie)
- Opatrenia na odstránenie zistení z Auditu KB na SHMÚ (11/2023 – neverejné citlivé informácie)
- Prístup k projektu
- Katalóg požiadaviek