1. Vybudovanie nosnej infraštruktúry bezpečného informačno-komunikačného systému FS SR

29. 5. 2019

Tento dokument obsahuje 40 strán.

Obsah

1 Základné informácie
1.1 Prehľad
1.2 Dôvod
1.3 Rozsah
1.4 Použité skratky a značky
2 Manažérske zhrnutie
2.1 Motivácia
2.2 Popis aktuálneho stavu
2.2.1 Legislatíva
2.2.2 Architektúra
2.2.3 Prevádzka
2.3 Alternatívne riešenia
2.3.1 Alternatíva A – „Zachovanie aktuálneho stavu"
2.3.2 Alternatíva B – „Implementácia riešenia navrhovaného v tejto štúdii uskutočniteľnosti"
2.3.3 Alternatíva C – „Implementácia minimalistického riešenia"
2.4 Popis budúceho stavu
2.4.1 Legislatíva
2.4.2 Architektúra
2.4.3 Prevádzka
2.4.4 Ekonomická analýza

Zoznam tabuliek

Tabuľka 1 Základné informácie - zhrnutie
Tabuľka 2 Skratky a značky
Tabuľka 3 Motivácia – budúci stav
Tabuľka 4 Legislatíva – aktuálny stav
Tabuľka 5 Biznis architektúra - aktuálny stav
Tabuľka 6 Architektúra informačných systémov - aktuálny stav
Tabuľka 7 Technologická architektúra - aktuálny stav
Tabuľka 8 Bezpečnostná architektúra - aktuálny stav
Tabuľka 9 Prevádzka - aktuálny stav
Tabuľka 10 Legislatíva - budúci stav
Tabuľka 11 Biznis architektúra – budúci stav
Tabuľka 12 Architektúra informačných systémov - budúci stav
Tabuľka 13 Technologická architektúra - budúci stav
Tabuľka 14 Implementácia a migrácia
Tabuľka 15 Bezpečnostná architektúra - budúci stav
Tabuľka 16 Prevádzka - budúci stav
Tabuľka 17 Ekonomická analýza - budúci stav

2. Základné informácie

2.1. Prehľad

Kto tvorí štúdiu, ktoré organizácie budú implementovať projekt, identifikácia organizácii v zriaďovateľskej pôsobnosti, identifikácia príslušného úseku verejnej správy, agendy verejnej správy a životnej situácie.
Tabuľka 1 Základné informácie - zhrnutie

Zdôvodnenie využitia národného projektu a vylúčenia výberu projektu prostredníctvom výzvy
Navrhovaný projekt „Vybudovanie nosnej infraštruktúry bezpečného informačno-komunikačného systému FS SR“ súvisí so zvýšením úrovne kybernetickej bezpečnosti informačno-komunikačného prostredia Finančnej správy Slovenskej republiky (ďalej len „FS SR“), vybudovaním nosnej infraštruktúry FS SR na monitoring, analýzu a aktívnu ochranu pred kybernetickými hrozbami, ako aj informačného systému na bezpečnú a monitorovanú manipuláciu s citlivými a utajovanými informáciami v elektronickej podobe. Riešenie pre zvýšenie úrovne kybernetickej bezpečnosti je koncipované ako komplexný mechanizmus, ktorý chráni FS SR pred vonkajšími ako aj vnútornými rizikami a hrozbami. Tento mechanizmus môže byť účinný len v prípade, že jeho jednotlivé časti a komponenty budú navzájom previazané a budú úzko spolupracovať. Zvýšenie úrovne kybernetickej bezpečnosti pomocou tohto riešenia sa predpokladá najmä v oblasti: • ochrany perimetra, bezpečnostného monitoringu a analytiky, • digitalizácie, šifrovania a riadenia prístupu v rámci tvorby, uchovávania a výmeny citlivých informácií a utajovaných skutočností. Predkladaná štúdia uskutočniteľnosti je vypracovaná v súlade s požiadavkami pre nové programové obdobie 2014 až 2020 pre Operačný program Integrovaná infraštruktúra, Prioritná os číslo 7 Informatizácia spoločnosti. Odzrkadľuje aj požiadavky platného zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej aj „Zákon o KyB“). Požiadavkou projektu je v zmysle schválenej Národnej koncepcie informatizácie verejnej správy Slovenskej republiky (ďalej aj „NKIVS“) – časť Bezpečnostná architektúra a Zákona o KyB nadviazať na nosné bloky bezpečnostnej architektúry a tieto stavebné prvky v prostredí FS SR maximálne využiť. Štúdia, vychádzajúc z vyhodnotenia možností dosiahnutia požadovaného nového cieľového stavu, sa zameriava predovšetkým na posúdenie možností implementácie nového bezpečnostného informačného systému, ktorý bude prostredníctvom nových elektronických služieb slúžiť na podporu plnenia úloh a činnosti FS definovaných zákonom, ktoré spadajú do jej pôsobnosti. Navrhované riešenie nadväzuje a vychádza najmä z nasledujúcich strategických dokumentov: • Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES. • Operačný program Integrovaná infraštruktúra 2014 – 2020, Prioritná os číslo 7 Informatizácia spoločnosti. • Národná koncepcia informatizácie verejnej správy Slovenskej republiky. • Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020. • Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020. • Dohovor Rady Európy o predchádzaní terorizmu. • Medzinárodný dohovor o potláčaní financovania terorizmu. • Európsky dohovor o potláčaní terorizmu. • Dohovor OSN proti nadnárodnému organizovanému zločinu. • Dohovor vypracovaný na základe článku K.3 Zmluvy o Európskej únii o vzájomnej pomoci a spolupráci medzi colnými správami (oznámenie č. 245/2009 Z. z.). • Rozhodnutie Rady 2009/917/SVV z 30. novembra 2009 o využívaní informačných technológií na colné účely (Ú. v. EÚ, L323, 10.12.2009). • Akčný plán EÚ na posilnenie boja proti daňovým podvodom a daňovým únikom, KOM(2012) 722, Brusel, 6.12.2012. • Akčný plán boja proti daňovým podvodom na roky 2012 až 2016, schválený uznesením Vlády SR č. 235 z 31.5.2012, Akčný plán boja proti daňovým podvodom na roky 2017 až 2018, schválený uznesením Vlády SR č. 206 z 26.4.2017, Akčný plán boja proti daňovým podvodom na roky 2018 až 2020. • Národná stratégia ochrany finančných záujmov EÚ v SR, schválená uznesením Vlády SR č. 18 zo 7.1.2015. • Návrh smernice Európskeho parlamentu a Rady o predchádzaní využívania finančného systému na účely prania špinavých peňazí a financovania terorizmu, KOM(2013) 45, Brusel, 5.2.2013. • Návrh riadenia Európskeho parlamentu a Rady o údajoch, ktoré sprevádzajú prevody finančných prostriedkov, KOM (2013) 44, Brusel, 5.2.2013. • Akčný plán EÚ pre boj proti terorizmu, 2011. • Národný akčný plán boja proti terorizmu schválený uznesením Vlády SR č. 316 z 18.5.2011. • Národný akčný plán boja proti terorizmu na roky 2015 – 2018 schválený uznesením Vlády SR č. 213/2015 z 29.4.2015.
Prijímateľ/partner národného projektu a dôvod jeho určenia

Prijímateľ projektu:	Finančné riaditeľstvo SR
IČO:	42499500
Právna forma:	321 Rozpočtová organizácia
Adresa sídla:	Lazovná ulica č. 63, 974 01 Banská Bystrica
Kód SK NACE:	84110 Všeobecná verejná správa
Kód OKEČ:	75110 Všeobecná verejná správa

FS SR plní úlohy podľa zákona č. 333/2011 Z. z. v rozsahu svojej pôsobnosti a aj ďalšie úlohy podľa osobitných zákonov a úloh vyplývajúcich taktiež z medzinárodných zmlúv a dohôd o spolupráci s orgánmi a medzinárodnými organizáciami a inštitúciami v rámci spolupráce členských štátov EÚ, ktorými je SR viazaná.

Príslušnosť národného projektu k relevantnej časti PO7 OPII	Realizáciou projektu bude podporený špecifický cieľ 7.9: Zvýšenie kybernetickej bezpečnosti v spoločnosti. Kód intervencie 78: Služby a aplikácie elektronickej verejnej správy vrátane elektronického obstarávania, opatrení IKT na podporu reformy verejnej správy, kybernetickej bezpečnosti, opatrení na ochranu dôvernosti a súkromia, elektronickej justície a elektronickej demokracie. Merateľný ukazovateľ P0048 Dodatočný počet informačných systémov verejnej správy s implementovaným nástrojom na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov. (Indikatívna cieľová hodnota - 60 %). INVESTIČNÁ PRIORITA 2c): Posilnenie aplikácií IKT v rámci elektronickej štátnej správy, elektronického vzdelávania, elektronickej inklúzie, elektronickej kultúry a elektronického zdravotníctva
Indikatívna výška finančných prostriedkov určených na realizáciu národného projektu	43 374 581 EUR s DPH

2.2. Dôvod

Dôvod vykonania štúdie uskutočniteľnosti. Definovanie IT stratégie a vízie architektúry organizácie verejnej správy.

FS predstavuje významný subjekt kontroly finančného hospodárstva SR, ktorý riadi a kontroluje daňové úrady, colné úrady a Kriminálny úrad finančnej správy. Plní úlohy vo veciach ochrany hospodárskych záujmov štátu v rozsahu vymedzenom zákonom [1] . FS na základe uzatvoreného dohovoru vypracovaného v súlade s článkom K.3 Zmluvy o Európskej únii o vzájomnej pomoci a spolupráci medzi colnými správami plní prostredníctvom príslušných úradov úlohy centrálnej koordinačnej jednotky a taktiež zabezpečuje ďalšie úlohy vyplývajúce z medzinárodných zmlúv v colnej oblasti. Pri plnení svojich úloh FS úzko spolupracuje s inými orgánmi štátnej správy, ako aj s orgánmi iných štátov obdobného zamerania a pôsobnosti a medzinárodnými organizáciami. Pri svojej činnosti získava, zhromažďuje, uchováva, spracúva, vyhodnocuje, odovzdáva, využíva, ochraňuje a vyraďuje informácie o daňových a colných subjektoch a ich aktivitách v rámci SR a v zahraničí.

V súvislosti s informatizáciou FS využíva a prevádzkuje vlastné informačné systémy a zodpovedá za spoločný informačný systém aplikovaný výlučne na účely plnenia úloh FS vyplývajúcich jej zo zákona. Na riadne plnenie svojich úloh musí FS využívať informačné technológie a technické prostriedky adekvátne súčasnej dobe, stupňu informatizácie, bezpečnosti, úrovni technických a technologických prostriedkov spolupracujúcich inštitúcií, ako aj úlohám, ktoré musí zo zákona plniť. Z tohoto dôvodu FS pristupuje k digitalizácii a elektronizácii svojich služieb prostredníctvom viacerých projektov,

ktorými nadväzuje na aktivity realizované v súčasnom období v oblasti zavádzania služieb eGovernmentu v SR, nadväzuje na strategické a koncepčné dokumenty v oblasti digitalizácie a elektronizácie služieb verejnej správy schválené Vládou SR, ako aj na aktivity v rámci EÚ, ktoré sú v tejto oblasti relevantné.

Dôvodom vypracovania tejto štúdie je posúdenie podmienok a vytvorenie predpokladov pre realizáciu projektu zabezpečujúceho bezpečnosť a ochranu pre ostatné IS FS SR a všetky informačné aktíva FS a jeho financovanie z prostriedkov OPII.

Riešenie bude zapadať do celkovej stratégie budovania IS v gescii FS SR. Bude zohľadňovať špecifiká prostredia FS SR a technologické požiadavky pre začlenenie do celkovej architektúry IS FS SR a bude tvoriť ucelený systém pre zabezpečenie kybernetického priestoru a IKT prostredia FS SR. FS SR očakáva, že implementáciou IS pre vytváranie, evidovanie, uchovávanie, výmenu a manipuláciu s citlivými a utajovanými skutočnosťami v elektronickej podobe (ďalej tiež „ISUS-FS“) sa vytvorí základ pre postupné budovanie a publikovanie elektronických služieb FS v súlade s Národnou koncepciou informatizácie verejnej správy predovšetkým v oblastiach: Formovanie infraštruktúry a Digitalizácia úsekov správy.

Víziou FS SR je vytvorenie spoľahlivého a najmä bezpečného riešenia, ktoré bude zabezpečovať podporu činností FS SR efektívnejším spôsobom, ako to je v súčasnosti. Implementácia riešenia bude viesť k zvýšeniu úrovne bezpečnosti a ochrany informačných aktív FS a celej IKT infraštruktúry FS, k zvýšeniu efektívnosti práce v gescii FS SR pri výmene citlivých informácií a utajovaných skutočností a k zníženiu nákladov spojených s touto výmenou v aktuálnom stave.

Navrhované bezpečnostné riešenie je relevantné pre monitorovanie bezpečnostných rizík najmä v oblasti boja proti organizovanej trestnej činnosti a terorizmu, legalizácii príjmov pochádzajúcich z trestnej činnosti a boja proti aktivitám, ktoré by mohli vážne ohroziť alebo poškodiť hospodárske záujmy alebo bezpečnosť Slovenskej republiky (ďalej len „SR“) alebo Európskej únie (ďalej len „EÚ“).

Dôvodom pre vypracovanie tejto štúdie uskutočniteľnosti a projektu je predovšetkým riešenie nižšie uvedených problémov a zároveň naplnenie uvedených príležitostí súčasnej doby:

- Problém: Na základe interných analýz a posudzovaní stavu bezpečnosti IS FS SR možno konštatovať, že aktuálny stav obsahuje značné množstvo zraniteľností, ktoré je potrebné adresovať, aby nedošlo k ich zneužitiu.
- Problém: Súčasný bezpečnostný systém funguje na zastaranej architektúre a nepokrýva všetky informačné aktíva FS SR. V rámci svojej infraštruktúry eviduje FS SR desiatky informačných systémov, z toho vyše 20 dôležitých.
- Problém: Infraštruktúra v súčasnosti obsahuje izolované prvky bezpečnostnej architektúry, ktoré primárne fungujú len na vybraných zariadeniach a systémoch, teda nie sú nasadené plošne.
- Problém: Aktuálny systém zabezpečenia a ochrany nespĺňa všetky požiadavky legislatívy (najmä zákona o KyB). Pokuta za nedodržanie legislatívnych požiadaviek zákona o utajovaných skutočnostiach je 10 miliónov EUR, v prípade incidentu z dôvodu nedodržania požiadaviek 20 miliónov EUR.
- Problém: Systém nie je prispôsobený na súčasné bezpečnostné požiadavky, čoho dôsledkom je, že nemusia byť identifikované všetky bezpečnostné incidenty. Priemerná výška ekonomických dopadov jedného incidentu je 103 045,09 EUR.
- Problém: Výmena citlivých informácií a utajovaných skutočností je aktuálne založená na manuálnom prenose v rámci pracovísk FS dislokovaných v celej SR. Počet písomností za rok, ktoré sa distribuujú manuálne, je 3418 a zamestnanci najazdia počas ich prenosu 1,2 milióna kilometrov.
- Príležitosť: Možnosť nasadenia pokročilých bezpečnostných opatrení a sofistikovaných bezpečnostných mechanizmov monitoringu, ktoré budú zaisťovať požadovanú úroveň ochrany všetkých bezpečnostne relevantných informačných aktív FS a celej IKT infraštruktúry FS.
- Príležitosť: Možnosť nasadenia prostriedkov a prvkov KyB ochrany a monitorovania, ktoré budú identifikovať možné bezpečnostné incidenty aj v reálnom čase.
- Príležitosť: Možnosť vytvorenia tímu a technických prostriedkov pre efektívne riešenie bezpečnostných incidentov.
- Príležitosť: Používanie nástrojov a techník, ktoré odhalia zraniteľnosti a slabiny IS a aplikácií FS skôr ako dôjde k ich zneužitiu neoprávnenou osobou.
- Príležitosť: Možnosť nasadenia analytických nástrojov nad veľkým množstvom údajov (Big-data) v reálnom čase, ktoré vyhodnocujú rizikovosť subjektov a ich správanie nielen na základe informácií previazaných so subjektom, ale aj na základe jeho väzieb na okolité rizikové subjekty a ich správanie.
- Príležitosť: Umožnenie elektronickej výmeny citlivých informácií a utajovaných skutočností a tým zabezpečenie zvýšenia časovej efektivity spracovania.

Hlavným dôvodom je teda modernizácia celého systému bezpečnosti a ochrany informačných aktív a IKT infraštruktúry FS a umožnenie elektronickej výmeny citlivých informácií a utajovaných skutočností a zároveň aj zabezpečenie dostatočnej ochrany (dôvernosti, integrity a dostupnosti) vymieňaných citlivých informácií a utajovaných skutočností.

Zákon o KyB definuje základnú sadu požiadaviek (tzv. security baseline), ktorú je každý poskytovateľ základnej služby povinný implementovať na základe prístupu založenom na analýze rizík (risk based approach). Je potrebné si uvedomiť skutočnosť, že navrhované riešenie (v podobe dvoch základných modulov, t.j. monitoring bezpečnosti a výmena citlivých informácií a utajovaných skutočností) reprezentuje len časť z celkových požiadaviek (definovaných v §20 zákona o KyB), ktoré by mali byť v prostredí FS SR implementované.

Riešenie navrhované v tejto štúdii predstavuje realizáciu len časti bezpečnostných opatrení, ktoré by mala FS SR prijať v zmysle §20 zákona o KyB. Konkrétne ide len o časť opatrení v rámci oblasti kryptografických opatrení (§20 ods. 3 písm. i) a riešenia kybernetických bezpečnostných incidentov (§20 ods. 3 písm. j).

Zvyšné bezpečnostné opatrenia budú v prostredí FS SR implementované v budúcnosti postupne na základe dostupnosti ďalších finančných prostriedkov.

Cieľovou skupinou pre realizáciu príležitostí na zlepšenie sú najmä úradníci (zamestnanci VS, resp. FS). Realizácia systému bezpečnosti a ochrany informačných aktív však zabezpečí aj nepriame prínosy pre občanov a podnikateľov v tom, že ich citlivé dáta a osobné údaje budú čiastočne chránené pred prípadnou stratou ich dôvernosti, integrity alebo dostupnosti.

Potreba realizácie tohto projektu vyplýva aj z postupnej informatizácie jednotlivých orgánov štátnej správy, s ktorými FS spolupracuje v rozsahu potrebnom na plnenie úloh stanovených zákonom, z nevyhnutnosti prispôsobiť svoje informačné systémy potrebám, úrovni a požiadavkám týchto kooperujúcich systémov verejnej správy, požiadavkám a potrebám informačno-komunikačných systémov partnerských medzinárodných organizácií, predovšetkým v rámci EÚ, a najmä z nevyhnutnosti zefektívniť a skvalitniť prácu a výstupy činností FS pri dodržaní platnej legislatívy SR v oblasti ochrany utajovaných skutočností [2], bezpečnosti informačných systémov verejnej správy [3] a požiadaviek bezpečnostných štandardov. [3,4]

Negatívny stav v prípade, ak projekt nebude realizovaný:

V prípade, že navrhovaný bezpečnostný systém nebude realizovaný, nevytvoria sa predpoklady pre dostatočnú ochranu informačných aktív a IKT infraštruktúry FS SR pred rizikami a hrozbami z vonkajšieho prostredia, ako aj z vnútorného prostredia FS SR. V praxi tak zostane stav, ktorý neumožňuje efektívnu a hlavne elektronickú výmenu citlivých informácií a utajovaných skutočností.

Zároveň bude:

- Ohrozené efektívne a spoľahlivé monitorovanie bezpečnostných rizík najmä v oblasti boja proti organizovanej trestnej činnosti a terorizmu, legalizácii príjmov pochádzajúcich z trestnej činnosti, boja proti aktivitám, ktoré by mohli vážne ohroziť alebo poškodiť hospodárske záujmy alebo bezpečnosť SR a EÚ.
- Ohrozená efektívna a spoľahlivá ochrana citlivých informácií a dát (najmä osobných a iných citlivých údajov) občanov a podnikateľov, ktorých dáta FS SR spracúva.

---

[1] Zákon č. 333/2011 Z. z. o orgánoch štátnej správy v oblasti daní, poplatkov a colníctva v znení neskorších predpisov
[2] Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (v ďalšom len „Zákon o ochrane utajovaných skutočností“)
[3] Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (v ďalšom len „Zákon o ISVS“)
[4] Výnos MF SR č. 55/2014 o štandardoch pre informačné systémy verejnej správy (v ďalšom len „Štandardy pre ISVS“)
[5] Rozhodnutie Rady EU 2013/488/EU z 23.9.2013 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ

2.3. Rozsah

Rozsah oblastí, v ktorom sa štúdia venuje projektu, do akej hĺbky sa venuje jednotlivým oblastiam.

Predložená štúdia vychádza z architektonického rámca verejnej správy a z Architektonickej vízie verejnej správy. Štúdia vznikla pre potrebu analýzy aktuálneho stavu, návrhu riešenia a vyhodnotenia jeho realizovateľnosti za účelom implementácie projektu. Štúdia nadväzuje na strategické a koncepčné dokumenty schválené Vládou SR v oblasti digitálnej agendy, informatizácie spoločnosti a verejnej správy, ako aj na ďalšie aktivity, ktoré sú v tejto oblasti realizované.

Štúdia posudzuje uskutočniteľnosť navrhovaného riešenia a odporúča optimálny plán implementácie projektu. Zaoberá sa ekonomickou analýzou nákladov na realizáciu a prevádzku systému bezpečnosti a ochrany, popisuje prínosy ako aj obmedzenia pri implementácii projektu. Upozorňuje na možné riziká súvisiace s projektom a navrhuje opatrenia na minimalizáciu uvádzaných rizík.

Štúdia definuje predpoklady a požiadavky pre riadne a plnohodnotné fungovanie novovybudovaného systému bezpečnosti a ochrany a zároveň vymedzuje, ktoré z týchto požiadaviek budú zabezpečené realizáciou uvedeného projektu a ktoré nie sú predmetom plnení v rámci tohto projektu, ale ktorých existencia, dostupnosť a primeraná kvalita parametrov sa predpokladá najneskôr v priebehu implementácie systému.

Cieľom tejto štúdie je poskytnúť strategický rámec, plánovaný rozsah, očakávaný časový harmonogram, závislosti na iné projekty a odporúčania ďalších aktivít, z ktorých je potrebné pri realizácií implementácie vychádzať.

Štúdia sa zameriava najmä na:

- Kybernetickú ochranu, perimetrovú ochranu IKT prostredia a sietí, analytiku a bezpečnostný monitoring stavu IB a KyB v informačnom prostredí FS SR, najmä implementáciou nástroja SIEM a implementáciou pokročilých, moderných a automatizovaných nástrojov na

identifikáciu a analýzu hrozieb a anomálií v rámci sieťových tokov a sieťovej prevádzky (IDS, IPS, UTM, ADS, ATA, a pod.), ako aj nástrojov zabezpečujúcich ochranu perimetra na úrovni databáz, webových portálov a domén (NGFW, WAFW, DBFW a pod.), s prepojením na centrálny systém SIEM.
- Proces výmeny citlivých informácií a utajovaných skutočností v rámci interného prostredia a pracovísk FS SR a aj medzi spolupracujúcimi subjektmi, najmä implementáciou HW a SW prostriedkov prepojených na centrálny systém SIEM.

Tieto oblasti sú logicky rozdelené, ale v praxi ide o úzko prepojené technické riešenia, nakoľko výstupy získané v rámci jedného systému slúžia ako vstupy pre ďalší systém. Jednotlivé systémy by bez vzájomnej podpory nedokázali dostatočne plniť svoje úlohy a nedosahovali tak cieľ definovaný v tejto štúdii uskutočniteľnosti, ktorým je komplexné zabezpečenie informačnej a kybernetickej bezpečnosti v prostredí FS SR.

Vymedzenie subjektov, ktorých sa dotýka navrhované riešenie projektu:

- Problém výmeny citlivých informácií a utajovaných skutočností sa okrem pracovníkov FS SR dotýka aj iných štátnych orgánov, ktoré potrebujú informácie od FS SR na zamedzenie protiústavnej alebo inej protiprávnej činnosti, na zachovanie verejného poriadku alebo pre ich vlastnú činnosť a rozhodovanie (napr. NBÚ). V neposlednej rade prijímateľmi informácií z nového ISUS-FS budú aj určené inštitúcie EÚ, s ktorými si FS SR vymieňa informácie v rámci medzinárodnej spolupráce.
- Problém kybernetickej ochrany a bezpečnostného monitoringu IKT infraštruktúry FS SR sa priamo dotýka len pracovníkov FS SR a bezpečnostných administrátorov bezpečnostných systémov FS SR.

Z hľadiska FS SR uvedené oblasti spadajú pod nasledovný úsek:

- U00024 Dane a poplatky
- U00025 Colníctvo
- U00026 Finančná kontrola

Aktér	Rola	ISVS
Pracovník FS SR	Poskytovateľ a konzument údajov v rámci výmeny citlivých informácií a utajovaných skutočností	ISUS-FS
Pracovník VS/EÚ	Poskytovateľ a konzument údajov v rámci výmeny citlivých informácií a utajovaných skutočností	ISUS-FS
Bezpečnostný administrátor FS SR	Administrátor bezpečnostných systémov FS SR	Bezpečnostné systémy FS SR

2.4. Použité skratky a značky

Tabuľka 2 Skratky a značky

Skratka / Značka	Vysvetlenie
ADS	Systém na detekciu anomálií (Anomaly Detection System)
AN	Analytický nástroj
APV	Aplikačné programové vybavenie
AR	Analýza rizík
ATA	Systém na pokročilú analýzu hrozieb (Advanced Threat Analytics)
B2B	Business to Business
BCM	Riadenie kontinuity činností (Business Continuity Management)
BCP	Plán riadenia kontinuity činností (Business Continuity Plan)
BIA	Analýza dopadov (Business Impact Analysis)
CBA	Nákladovo-prínosová analýza (Cost-Benefit Analysis)

CSIRT	Computer Security Incident Response Team
DB	Databáza
DBFW	Databázový firewall (Database Firewall)
DC	Data Classification (klasifikácia dát)
DLP	Prevencia úniku dát (Data Leak Prevention)
DMS	Systém manažmentu elektronických dokumentov (Document Management System)
DRP	Plán obnovy po havárii (Disaster Recovery Plan)
EK	Európska komisia
EP	Európsky Parlament
EPP	Ochrana koncových zariadení (End-Point Protection)
ES	Európske spoločenstvo
EÚ	Európska únia
FINNET 3	Sieť vybudovaná pre prepojenie finančných inštitúcií SR s DataCentrom
FOB	Fyzická a objektová bezpečnosť
FR SR	Finančné riaditeľstvo SR
FS / FS SR	Finančná správa / Finančná správa Slovenskej republiky
GIS	Geografický informačný systém
G2B	Služby pre podnikateľov (Government-to-Business)
G2C	Služby pre občanov (Government-to-Citizen)
G2G	Služby pre verejnú správu (Government-to-Government)
G2E	Interné služby pre verejnú správu (Government-to-Employee)
GOVNET	Vládna sieť vybudovaná a spravovaná NASES
GUI	Grafické používateľské rozhranie (Graphical User Interface)
HW	Hardvér
IAM	Správa identít a prístupov (Identity and Access Management)
IB	Informačná bezpečnosť
IKT	Informačno-komunikačné technológie
IP	Internet protokol, štandardizovaný sieťový protokol 3. vrstvy ISO/OSI komunikačného modelu
IP VPN	Virtuálna privátna sieť vytvorená na báze IP protokolu
IPS	Systém na prevenciu prienikov (Intrusion Prevention System)
IS	Informačný systém
ISUS-FS	Informačno-komunikačný systém pre vytváranie, uchovávanie a výmenu citlivých a utajovaných skutočností Finančnej správy Slovenskej republiky v elektronickej podobe
ISVS	IS verejnej správy
IT	Informačné technológie

ITP	Informačno–technické prostriedky
KB DB	Knowledge Database (znalostná databáza)
KUFS	Kriminálny úrad finančnej správy
LAN	Lokálna dátová sieť (Local Area Network)
MF SR	Ministerstvo financií Slovenskej republiky
MV SR	Ministerstvo vnútra Slovenskej republiky
NASES	Národná agentúra pre sieťové a elektronické služby; organizácia zriadená v pôsobnosti Úradu vlády SR
NBÚ	Národný bezpečnostný úrad
NFP	Nenávratný finančný príspevok
NGFW	Firewall novej generácie (Next Generation Firewall)
NKIVS	Národná koncepcia informatizácie verejnej správy
OOU	Ochrana osobných údajov
OPII	Operačný program Integrovaná infraštruktúra
OUS	Ochrana utajovaných skutočností
OVM	Orgány verejnej moci
PKI	Infraštruktúra verejného kľúča (Public Key Infrastructure)
PŠOI	Prostriedok šifrovej ochrany informácií
PZ SR	Policajný zbor SR
RO	Riadiaci orgán
SIEM	Nástroj na manažment bezpečnostných informácií a udalostí (Security Information and Event Management)
SOC	Pracovisko pre riadenie bezpečnosti (Security Operation Center)
SORO	Sprostredkovateľský orgán pod Riadiacim orgánom štrukturálnych projektov
SR	Slovenská republika
SSO	Systém jednotného prihlásenia (Single Sign-On)
SW	Softvér
ŠOI	Šifrová ochrana informácií
ŠU	Štúdia uskutočniteľnosti
TCP	Štandardizovaný prenosový komunikačný protokol 4. vrstvy ISO/OSI komunikačného modelu
TCP/IP	Štandardizovaný prenosový komunikačný protokol medzi dvomi entitami s potvrdzovaním prenesených dát a s využitím štandardizovaného sieťového protokolu IP
TP	Technický prostriedok
US	Utajované skutočnosti
VDI	Infraštruktúra virtualizácie pracovnej stanice (Virtual Desktop Infrastracture)
VPN	Virtuálna privátna sieť
WAFW	Webový aplikačný firewall (Web Application Firewall)

WAN	Prenosová dátová sieť (Wide Area Network)
ŽoNFP	Žiadosť o nenávratný finančný príspevok

3. Manažérske zhrnutie

FS SR na základe uzatvoreného dohovoru vypracovaného v súlade s článkom K.3 Zmluvy o Európskej únii o vzájomnej pomoci a spolupráci medzi colnými správami plní úlohy centrálnej koordinačnej jednotky a taktiež zabezpečuje ďalšie úlohy vyplývajúce z medzinárodných zmlúv vo vymedzenej oblasti.

Účelom projektu uvádzaného v tejto Štúdii je podporiť program digitalizácie a elektronizácie služieb verejnej správy SR s cieľom zefektívniť procesy činnosti FS SR, nadviazať na aktivity realizované v súčasnom období v oblasti zavádzania eGovernmentu v SR, nadviazať na strategické a koncepčné dokumenty v oblasti digitalizácie a elektronizácie služieb verejnej správy schválené Vládou SR, ako aj na aktivity v rámci EÚ, ktoré sú v tejto oblasti realizované a to pri zabezpečení vysokej miery kybernetickej bezpečnosti.

Cieľom projektu je:

- Zabezpečenie súladu s požiadavkami legislatívy, najmä zákona o KyB.
- Implementovanie moderných a efektívnych nástrojov a technológií pre kybernetickú ochranu a monitorovanie bezpečnostných incidentov (aj v reálnom čase) a poskytnutie efektívnych nástrojov a prostriedkov pre riadenie prípadných bezpečnostných incidentov a obnovu prevádzkovaných systémov FS SR.
- Implementovanie nástrojov identifikácie a analýz hrozieb a anomálií v rámci sieťových tokov a sieťovej prevádzky a nástrojov zabezpečujúcich ochranu sieťového perimetra FS SR s prepojením na centrálny monitorovací systém.
- Riadenie a správa agendy súvisiacej s vytváraním, výmenou a manipuláciou s citlivými a utajovanými skutočnosťami v oblastiach vymedzených pre FS SR zákonom, jej modernizácia a odbúranie jej papierovej podoby s prepojením na centrálny monitorovací systém.

Takto koncipovaný projekt zabezpečí:

- efektívnejšiu prácu útvarov FS SR (znížením administratívneho zaťaženia a skrátením času potrebného na vykonávanie úkonov spojených s administratívnou bezpečnosťou pri manipulácii s citlivými a klasifikovanými informáciami),
- vysokú kvalitu práce a pracovného prostredia pracovníkov (možnosť práce s citlivými a klasifikovanými informáciami od pracovného stola, možnosť využitia jednej pracovnej stanice na manipuláciu s informáciami rôzneho stupňa bezpečnostnej klasifikácie),
- vyššiu úroveň informačnej a kybernetickej bezpečnosti v rámci procesov monitoringu a riadenia bezpečnostných incidentov a riadenia vonkajších aj vnútorných hrozieb.

Potreba realizácie projektu vyplýva z postupnej informatizácie spoločnosti a jednotlivých orgánov štátnej správy, s ktorými FS SR spolupracuje v rozsahu potrebnom na plnenie úloh ustanovených zákonom, z nevyhnutnosti prispôsobiť informačné systémy FS SR potrebám, úrovni a požiadavkám systémov partnerských inštitúcií v rámci SR, ale aj v rámci členských krajín EÚ a nevyhnutnosti zefektívniť a skvalitniť prácu a výstupy činnosti FS SR.

V súčasnosti je výkon činností FS SR podporovaný samostatnými informačnými systémami. Neustále narastá množstvo údajov z vlastných, verejných aj neverejných informačných zdrojov, ktorých podstatná časť nie je v elektronickej podobe, a ktoré je pri činnosti FS SR nevyhnutné spracovávať, pričom na riadne a včasné plnenie úloh FS SR musí vynakladať čoraz väčšie administratívne úsilie, aby kvalita a včasnosť výstupov bola zodpovedajúca požiadavkám a očakávaniam ich prijímateľov.

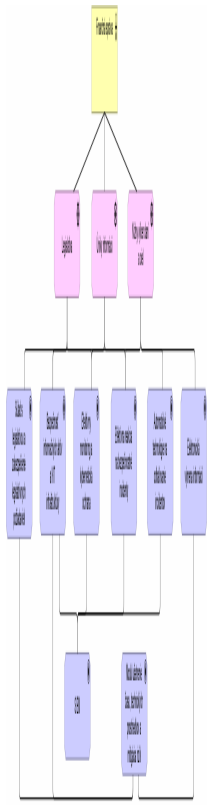
Súčasný stav vykazuje nedostatky taktiež v prípadoch, keď je potrebné spracovávať citlivé a utajované informácie rôzneho charakteru, ako napríklad pri riešení rozsiahlych daňových a colných podvodov. Tento typ podvodov zapríčiňuje každý rok výpadky miliónov EUR v štátnom rozpočte, čím sa poškodzujú finančné záujmy SR ako aj EÚ. Preto patrí riešenie týchto problémov, s cieľom znížiť daňové úniky a zlepšiť výber daní, spolu s ochranou hospodárskych a ekonomických záujmov SR, k aktuálnym prioritám Vlády SR a je tak aj jednou z hlavných priorít činností FS SR.

Predkladaný projekt je v súlade s národnou a európskou stratégiou boja proti daňovým podvodom a daňovým únikom, boja proti organizovanému zločinu, legalizácii príjmov pochádzajúcich z trestnej činnosti, závažných daňových a colných podvodov a v súlade s bezpečnostnými požiadavkami SR a EÚ.

Priestor pre sumárny obrázok

3.1. Motivácia

Tabuľka 3 Motivácia – budúci stav

Súhrnný popis
Dôvodom vypracovania predkladanej Štúdie je analýza aktuálneho stavu súčasných procesov v oblasti riadenia IB a KyB, špecifikovania požiadaviek na nový stav, návrhu riešenia na dosiahnutie nového stavu a na posúdenie možností a predpokladov jeho realizovateľnosti. Implementáciou nového IS sa vytvorí základ a bezpečné prostredie pre budovanie a publikovanie nových elektronických služieb FS SR v súlade s Národnou koncepciou informatizácie verejnej správy predovšetkým v oblastiach: Formovanie infraštruktúry a Digitalizácia úsekov správy. Vybudovanie ISUS-FS umožní realizovať zabezpečenie ochrany citlivých informácií a utajovaných skutočností v elektronickej podobe voči úniku a neoprávnenej manipulácii, komplexnú bezpečnú správu citlivých informácií a utajovaných skutočností, riadený prístup pre oboznamovanie sa s citlivými informáciami a utajovanými skutočnosťami, bezpečný prenos utajovaných skutočností/citlivých informácií, centralizáciu služieb spojených s elektronickou evidenciou a administráciou utajovaných skutočností a citlivých informácií, zníženie administratívneho zaťaženia útvarov FS SR, zvýšenie transparentnosti procesov, skrátenie času vybavovania súvisiacich agend a vytvorenie spoločnej zabezpečenej komplexnej infraštruktúry pre elektronické služby pre prácu s utajovanými skutočnosťami a citlivými informáciami v rámci FS SR. Realizácia projektu prispeje k zvýšeniu efektívnosti a zníženiu časovej náročnosti procesov súvisiacich s tvorbou, prenosom a ukladaním citlivých informácií a utajovaných skutočností. Prostredníctvom ich elektronizácie umožní FS SR správne, flexibilne a pružne plniť úlohy vymedzené zákonom a poskytovať adekvátnu súčinnosť iným štátnym orgánom a medzinárodným organizáciám na základe bilaterálnych a multilaterálnych dohôd. Zvýšenie kybernetickej bezpečnosti, zefektívnenie výkonu a zníženie nákladov na fungovanie verejnej správy patria k hlavným očakávaným prínosom informatizácie verejnej správy definovaným v Národnej koncepcii informatizácie verejnej správy. Zákon o KyB vyžaduje, aby prevádzkovatelia základných služieb implementovali a dodržiavali konkrétne bezpečnostné procesy prostredníctvom moderných bezpečnostných technológií a ukladá im povinnosť odhaliť prípady ohrozenia počítačovej bezpečnosti vo veľkých sieťach a komunikačných alebo informačných systémoch. FS SR je povinná pre všetky svoje informačné systémy pravidelne vyhodnocovať, či tieto kritériá sú dodržiavané alebo či boli prekročené, a v tom prípade je povinná túto skutočnosť ohlásiť NBÚ SR. Pre tie systémy, ktoré NBÚ SR zaradí do zoznamu základných služieb, musí FS SR do 6 mesiacov implementovať opatrenia stanovené vyhláškou NBÚ SR č. 362/2018 Z. z. o bezpečnostných opatreniach. Obdobne na vytvorenie bezpečnostných podmienok spracovania informácií platia na informačné systémy FS SR aj požiadavky zákonov prijatých už pred Zákonom o KyB. Sú to hlavne zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov a zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Dňa 1. 1. 2020 nadobúda platnosť aj Vyhláška 48/2019 Z.z., ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností. Táto vyhláška má za cieľ, aby všetky orgány štátnej správy evidovali utajované skutočnosti v elektronickej podobe. Hlavným cieľom týchto legislatívnych predpisov a v nich definovaných požiadaviek je implementovať účinné opatrenia na vytvorenie bezpečného prostredia informačných systémov verejnej správy. Jednotlivé požadované opatrenia legislatívy sa v mnohých častiach prekrývajú, a preto je vhodné vytvoriť jednotnú koncepciu zabezpečenia ochrany informačných systémov FS SR. Z pohľadu potrieb Zákona o KyB je potrebné prijať bezpečnostné opatrenia, ktoré predstavujú úlohy, procesy, roly a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Opatrenia je potrebné prijímať na základe klasifikácie informácií a kategorizácie sietí a informačných systémov na zabezpečenie predchádzania kybernetickým bezpečnostným incidentom a minimalizovanie vplyvov kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania služieb, ktoré sú životne nevyhnutné pre plnenie úloh FS SR vyplývajúcich so zákona. Zákon o KyB presne definuje, v ktorých oblastiach je potrebné opatrenia prijať a čo majú bezpečnostné opatrenia v sebe zahŕňať. Dôležitým dodatkom v rámci definície opatrení v § 20 Zákona o KyB je požiadavka, že bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu príslušného informačného systému.


Navrhovaný projekt je finančne a investične náročný a v rámci zákonom pridelených rozpočtových prostriedkov FS SR nerealizovateľný. Za účelom efektívnejšieho plnenia úloh FS SR vyplývajúcich zo zákona a z národných stratégií prijatých SR na základe implementácie európskej politiky v oblasti bezpečnosti a ochrany finančných záujmov EÚ pristúpila FS SR k možnosti čerpania finančných prostriedkov zo zdrojov EÚ. Vzhľadom na rozsah projektu, potrebné financovanie a dostupné možnosti čerpania finančných prostriedkov EÚ, FS SR zamerala svoju pozornosť na získanie týchto prostriedkov z Operačného programu Integrovaná infraštruktúra, prioritnej osi č. 7 „Informačná spoločnosť".

Základné požiadavky, ktoré projekt naplní, sú nasledovné:

- Požiadavky FS SR / eGovernmentu:
  - zabezpečenie elektronickej výmeny citlivých informácií a utajovaných skutočností,
  - zníženie nákladov na prenos citlivých informácií a utajovaných skutočností,
  - zabezpečenie dôvernosti, integrity a dostupnosti všetkých informačných aktív FS SR.
- Požiadavky používateľov iných OVM a inštitúcií EÚ:
  - zvýšenie efektivity práce a zníženie času potrebného na prenos citlivých informácií alebo utajovaných skutočností.
- Požiadavky používateľov FS SR:
  - zvýšenie efektivity práce a zníženie času potrebného na prenos citlivých informácií alebo utajovaných skutočností.
- Požiadavky bezpečnostného manažéra a bezpečnostných administrátorov FS SR:
  - zabezpečenie dôvernosti, integrity a dostupnosti informačných aktív FS SR,
  - zabezpečenie efektívneho monitoringu a riešenia bezpečnostných incidentov,
  - zabezpečenie sieťovej prevádzky a sieťového perimetra FS SR,
  - zabezpečenie efektívnej, spoľahlivej a bezpečnej komunikácie a výmeny informácií v rámci FS SR aj mimo FS SR (tretie strany a iné OVM).

Pri realizácii je možné sledovať nasledovné projektové merateľné ukazovatele:

- Počet nasadených nástrojov nástrojov na rozpoznávanie, monitorovanie, analýzu a riadenie bezpečnostných incidentov.
- Počet informačných systémov FS SR zapojených do centrálneho systému monitorovania bezpečnosti.
- Počet pracovísk FS SR, v ktorých bol nasadený modul bezpečnej elektronickej tvorby, výmeny a uchovávania citlivých dát a utajovaných skutočností.

Aktér	Cieľ	Požiadavky	KPI	Hodnota KPI	Časový horizont	Obmedzenie
FS SR	Zvýšenie efektivity monitorovania, analýzy a reakcie na bezpečnostné incidenty	implementácia navrhovaných bezpečnostných systémov	Počet nasadených nástrojov na rozpoznávanie, monitorovanie, analýzu a riadenie bezpečnostných incidentov	ASIS: 1 TOBE: 2	2022	Úspešné zavedenie systému a zmien procesov
FS SR	Zvýšenie rozsahu monitorovania, analýzy a reakcie na bezpečnostné incidenty	implementácia navrhovaných bezpečnostných systémov	Počet informačných systémov FS SR zapojených do centrálneho systému monitorovania bezpečnosti	ASIS: 1 TOBE: 20	2022	Úspešné zavedenie systému a zmien procesov
FS SR	Zavedenie bezpečnej elektronickej platformy na tvorbu, výmenu a uchovávanie citlivých údajov a utajovaných skutočností	implementácia navrhovaných bezpečnostných systémov	Počet pracovísk FS SR, v ktorých bol nasadený modul bezpečnej elektronickej tvorby, výmeny a uchovávania citlivých dát a utajovaných skutočností	ASIS: 0 TOBE: 263	2022	Úspešné zavedenie systému a zmien procesov
FS SR	Zníženie rizika úniku citlivých údajov a utajovaných skutočností počas ich životného cyklu prostredníctvom interného personálu	implementácia navrhovaných bezpečnostných systémov	Počet pracovníkov prichádzajúcich do styku s citlivými údajmi a utajovanými skutočnosťami	ASIS: 100 % [1] TOBE: 50 %	2022	Úspešné zavedenie systému a zmien procesov

[1] Hodnota 100 % predstavuje počet ľudí prichádzajúcich do styku s utajovanými skutočnosťami v súčasnosti (cca. 25 osôb), ktorá sa po realizácii projektu zníži minimálne o polovicu (na menej ako 12 osôb).

Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R_M1: Nesplnenie KPI definovaných v rámci špecifického cieľa 7.9 Zvýšenie kybernetickej bezpečnosti v spoločnosti.	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

3.2. Popis aktuálneho stavu

3.2.1. Legislatíva

Tabuľka 4 Legislatíva – aktuálny stav

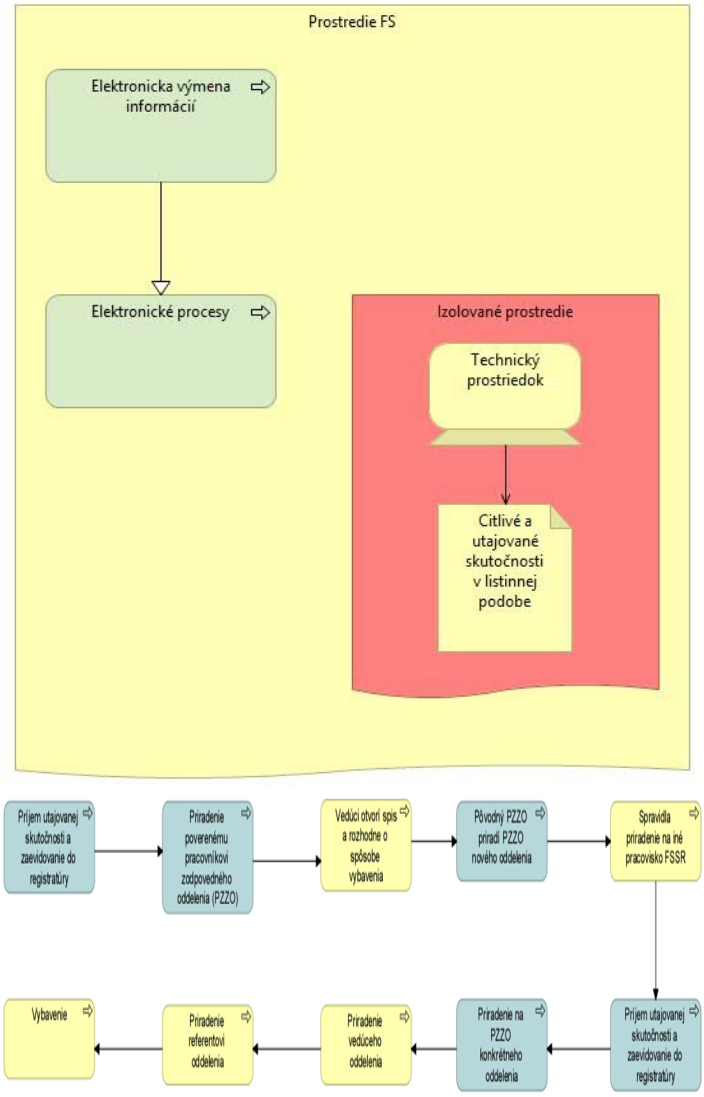
Súhrnný popis	
Navrhované riešenie vychádza z nasledujúcej legislatívy: • Zákon č. 333/2011 Z. z. o orgánoch štátnej správy v oblasti daní, poplatkov a colníctva v znení neskorších predpisov. • Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES. • Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. • Zákon č. 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o eGovernmente), v znení neskorších predpisov. • Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. • Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. • Zákon č. 171/1993 Z. z. o Policajnom zbore v znení neskorších predpisov. • Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. • Rozhodnutie Rady EU 2013/488/EU z 23.9.2013 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ. • Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov. • Zákon č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.	
Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.	
Súvisiaca legislatíva: • Výnos Ministerstva financií SR č. 55/2014 o štandardoch pre informačné systémy verejnej správy, a výnos č. 137/2015 Z. z. ktorým sa mení a dopĺňa predošlý výnos č. 55/2014., • Vyhláška NBÚ č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby), • Vyhláška NBÚ č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov, • Vyhláška NBÚ č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov, • Vyhláška NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení. • Vyhláška NBÚ č. 48/2019 Z.z., ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností.	
Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R_AL1: Nepokrytie činností definovaných v legislatívnych požiadavkách.	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

3.2.2. Architektúra

3.2.2.1. Biznis architektúra

Tabuľka 5 Biznis architektúra - aktuálny stav

Súhrnný popis
V súčasnosti FS SR využíva rádovo desiatky IS, ktoré nie sú navzájom prepojené, pričom každý využíva vlastné informačné zdroje a databázu. Tieto informačné systémy pracujú v internom prostredí FS SR a neposkytujú žiadne koncové služby. Z procesného hľadiska nie je používaný žiaden technický prostriedok alebo systém, ktorý by jednotlivé IS prepájal a umožňoval tak zamestnancom efektívne elektronicky vymieňať citlivé informácie a utajované skutočnosti v rámci týchto IS. Táto práca sa vykonáva prostredníctvom kuriéra a zapečatených obálok. Tento proces je zdĺhavý, nedostatočne zabezpečený voči úniku informácií a vyžaduje si značné finančné prostriedky. Proces výmeny ostatných informácií a údajov sa uskutočňuje prostredníctvom e-mailovej komunikácie. Množstvo izolovaných IS má za následok veľký počet vytváraných log záznamov. V rámci FS SR zatiaľ neexistuje jednoduchý spôsob prístupu k týmto záznamom a manipulácie s nimi, a teda nie je všeobecne zavedený proces automatizovaného spracovávania týchto záznamov. Čiastočne túto úlohu plní systém SIEM (ID: isvs_9412 Bezpečnosť IS), ktorý však pracuje len s vybranými agendovými IS. V oblasti personálnej bezpečnosti sa FS SR riadi špeciálnou legislatívou. Na jej základe má vypracované interné smernice v oblasti personálnej bezpečnosti. Tieto smernice však ešte nie sú zosúladené s požiadavkami zákona o KyB. V súčasnom stave sú útvary bezpečnosti a prevádzky FS SR personálne poddimenzované.



Procesná mapa popisuje približný životný cyklus utajovanej skutočnosti. Momentálne pracuje s utajovanými skutočnosťami veľké množstvo personálu - vedúci oddelení, referenti, sekretárky, poverení pracovníci / kuriéri. Utajované skutočnosti sú medzi jednotlivými oddeleniami v rámci FS SR prenášané manuálne a registratúra je papierová.

Tmavou farbou sú znázornené články, ktoré budú v dôsledku elektronizácie agendy automatizované, čím sa zníži počet pracovníkov, ktorí prídu do styku s utajovanou skutočnosťou.

Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.

R_AB1: Nedostatočné zabezpečenie monitorovacích a logovacích služieb.

R_AB2: Nedostatočné zabezpečenie výmeny citlivých údajov a utajovaných skutočností.

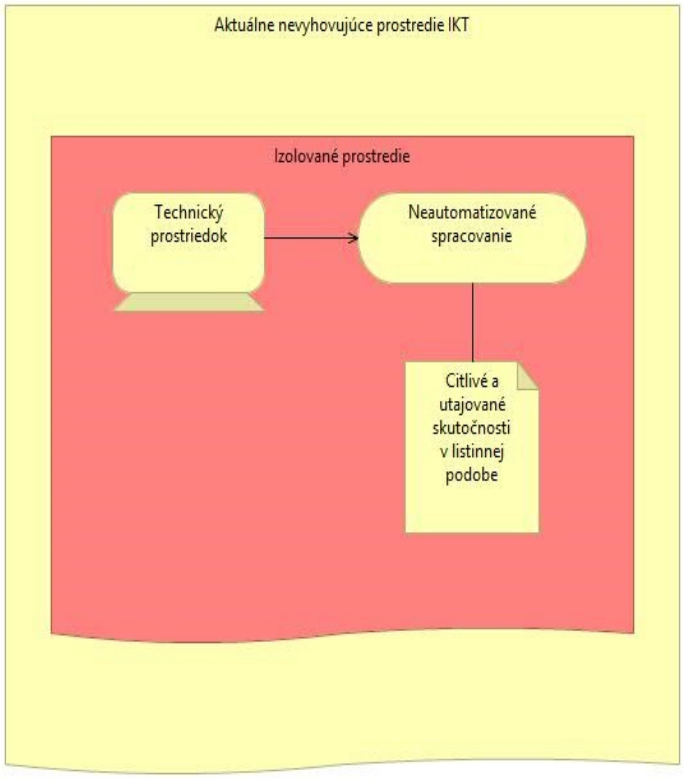
R_AB3: Nedostatočná perimetrová ochrana.

R_AB4: Ohrozenie zdravia zamestnancov počas služobných ciest.

Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

3.2.2.2. Architektúra informačných systémov

Tabuľka 6 Architektúra informačných systémov - aktuálny stav

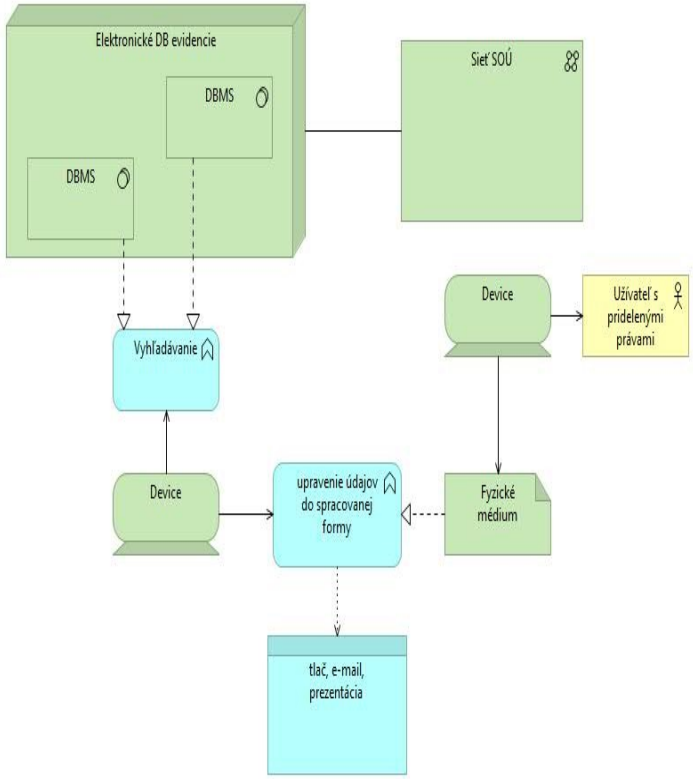
Súhrnný popis
V súčasnosti sú v rámci FS SR využívané izolované, samostatné informačné systémy. Každý z týchto systémov využíva vlastné informačné zdroje, informačné zdroje zdieľané inými zložkami FS SR alebo informačné zdroje iných orgánov štátnej správy. Komunikácia, zdieľanie a synchronizácia dát medzi jednotlivými IS sú náročné a neefektívne. Logická architektúra pre jednotlivé IS je založená na modeli „hviezda“ – pracovníci sa cez koncové zariadenia pripájajú k jednému informačnému zdroju, resp. databáze. Na uskutočnenie týchto pripojení sa využívajú štandardné prvky IKT prostredia – „klient-server“ pripojenie cez Ethernet na báze protokolu TCP/IP. Na spracovávanie všetkých údajov a informácií z IS (vrátane citlivých údajov a utajovaných skutočností) slúžia štandardné nástroje Microsoft Office – Word, Excel, Outlook, Access. Dokumenty vytvárané týmito nástrojmi sú vo veľkej miere následne vyhotovované aj v papierovej forme. Kriminálny úrad FS SR, využívajúci vlastné špeciálne aplikačné nástroje, tvorí v rámci FS SR výnimku. V rámci plnenia svojich úloh má možnosť pristupovať k dostupným registrom, databázam a ostatným informačným zdrojom, kde môže vyhľadávať, triediť a spracovávať údaje.


Ďalšie informácie	
Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R_AI1: Nekonzistentnosť údajov v rôznych IS. R_AI2: Neaktuálne a neúplné logy. R_AI3: Časová náročnosť výmeny údajov.	

Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

3.2.2.3. Technologická architektúra

Tabuľka 7 Technologická architektúra - aktuálny stav

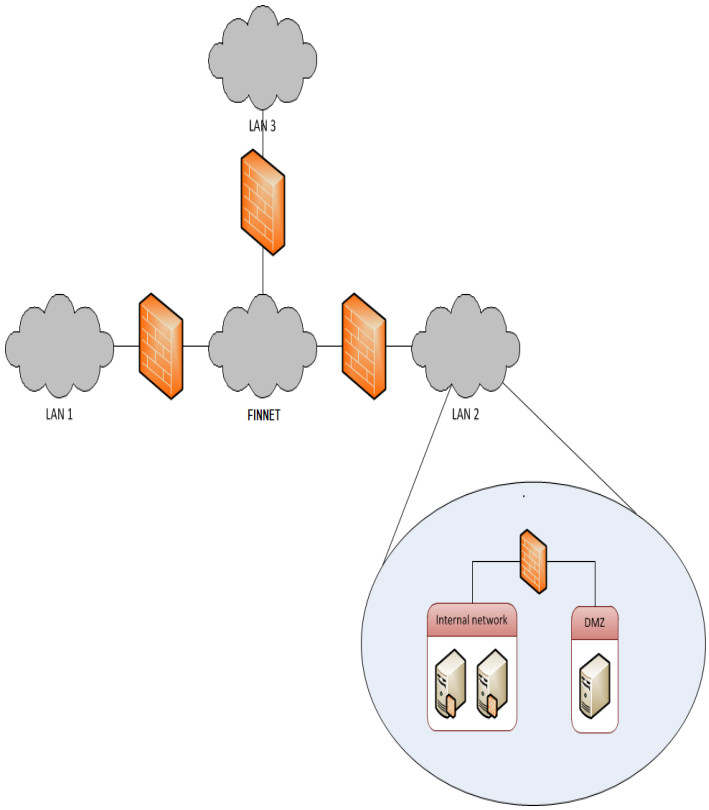
Súhrnný popis
IS a nástroje, ktoré FS SR využíva pri plnení svojich úloh, využívajú prevažne štandardné IKT prostredie – LAN typu Ethernet, pripojenie „klient-server“ na báze TCP/IP protokolu. Nástroje MS Office sú spúšťané na jednotlivých pracovných staniciach a termináloch pracovníkov FS SR s operačným systémom MS Windows. Serverová infraštruktúra poskytuje virtuálne prostredie a clustering pomocou platformy Microsoft a VMware. Jednotlivé útvary FS SR medzi sebou komunikujú prostredníctvom IP VPN, ktorá je vytvorená nad sieťou FINNET 3. Zdieľanie informácií medzi jednotlivými IS prebieha formou prenosných elektronických médií (USB kľúče, CD-ROM), ako aj v papierovej forme. Súčasný systém SIEM využíva riešenie MicroFocus ArcSight.


Ďalšie informácie	
Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R_AT1: Strata fyzických médií.	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

3.2.2.4. Bezpečnostná architektúra

Tabuľka 8 Bezpečnostná architektúra - aktuálny stav

Súhrnný popis
Infraštruktúra v súčasnosti obsahuje izolované prvky bezpečnostnej architektúry, ktoré primárne fungujú len na vybraných zariadeniach a systémoch, teda nie sú nasadené plošne. Konkrétne sa jedná o: • monitorovanie bezpečnosti vybraných IS, • monitorovanie privilegovaného prístupu do vybraných IS, • monitorovanie interaktívnych činností správcov na vybraných produkčných serveroch, • ochrana webových komponentov vybraných IS, • ochrana e-mailovej a webovej komunikácie, • ochrana pred malware na koncových zariadeniach, • riadenie vzdialeného prístupu, • segmentácia sieťového prostredia. V nasledovných oblastiach nemá bezpečnostná architektúra zavedené dostatočné opatrenia vyžadované zákonom o KyB a zákonom o ochrane osobných údajov: • riadenie vývoja a údržby IS, • riadenie technických zraniteľností zariadení a IS, • riadenie prístupov pre všetkých používateľov, • kryptografické opatrenia, • detekcia, evidencia a riešenie kybernetických bezpečnostných incidentov pre všetky zariadenia a IS, • monitorovanie, testovanie bezpečnosti a bezpečnostný audit, • ochrana pred únikom osobných údajov. Autentizačné systémy pre riadenie prístupu sú implementované pre vzdialený prístup (IP VPN s dvojfaktorovou autentizáciou pomocou tokenu), bezdrôtovú sieť (Wi-Fi) a pre správu niektorých bezpečnostných a sieťových zariadení. Napriek tomu, že FS SR disponuje bezpečnostnými prvkami, je pre splnenie požiadaviek platnej legislatívy nevyhnutné zaviesť také technologické prvky a opatrenia, ktoré sú schopné zabezpečiť potrebné služby a procesy v dostatočnej miere.



Ďalšie informácie	
Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R_AS1: Nedodržiavanie organizačných bezpečnostných opatrení a procesov.	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

3.2.3. Prevádzka

Tabuľka 9 Prevádzka - aktuálny stav

Súhrnný popis	
Prevádzku IS FS zabezpečuje Odbor prevádzky IS a Odbor podpory koncových užívateľov. Z hľadiska infraštruktúry a aplikácií zabezpečuje prevádzku IS Odbor prevádzky IS. Odbor dohliada na súlad vykonávaných procesov s platnými internými smernicami a riadiacimi aktmi Finančného riaditeľstva SR. Zabezpečuje organizačno-technické prostriedky, dôvernosť, dostupnosť a integritu dát spracovávaných IS. Odbor podpory koncových užívateľov slúži ako kontaktné miesto podpory v oblasti IT pre zamestnancov. Zabezpečuje prevádzku výpočtovej techniky pre všetkých koncových užívateľov (s výnimkou užívateľov v rámci KUFS). Zabezpečuje vykonávanie procesov „Manažment konfigurácií“, „Manažment incidentov“, „Manažment problémov“, „Manažment zmien“, „Release manažment“ a „Manažment kontinuity IT služieb“ v zmysle zavedených štandardov ITIL. Odbor prijíma a vyhodnocuje hlásenia o neštandardných udalostiach v oblasti IT, komunikuje s koncovými užívateľmi, spracúva ich požiadavky, prideľuje požiadavky internému riešiteľskému tímu a uzatvára ich. Odbor podpory koncových užívateľov zároveň zabezpečuje prevádzku IKT koncových používateľov. Momentálne neexistuje v rámci FS SR pracovisko špecializovaného bezpečnostného tímu (Security Operation Center – SOC) a rovnako FS SR nie je napojená na jednotku CSIRT nadriadenej organizácie. Monitoring pomocou technológie SIEM pre vybrané systémy zaznamenáva a analyzuje udalosti prijaté len z vybraných operačných systémov, vybraných sieťových bezpečnostných zariadení a vybraných webových a klientskych aplikácií. Prevádzku SIEM zabezpečuje z dôvodu nedostatočného personálu sekcia inšpekcie a vnútornej kontroly FS SR. SIEM teda nie je prevádzkovaný oddelením bezpečnosti, pod ktoré by mal tento systém spadať.	
Priestor pre sumárny obrázok	
Ďalšie informácie	
Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R_AP1: Nedostatočné personálne, znalostné a technické (HW a SW) vybavenie.	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

3.3. Alternatívne riešenia

3.3.1. Alternatíva A – „Zachovanie aktuálneho stavu"

Súhrnný popis
V súčasnosti FS SR využíva niekoľko IS, ktoré nie sú navzájom prepojené, pričom každý využíva vlastné informačné zdroje a databázu. Z procesného hľadiska nie je používaný žiaden technický prostriedok alebo systém, ktorý by jednotlivé IS prepájal a umožňoval tak zamestnancom vytvárať, manipulovať a vymieňať citlivé informácie a utajované skutočnosti v rámci týchto IS. Táto práca sa vykonáva prostredníctvom kuriéra a zapečatených obálok. Tento proces je zdĺhavý, nedostatočne zabezpečený voči úniku informácií a vyžaduje si značné finančné prostriedky. Množstvo izolovaných IS má za následok veľký počet vytváraných log záznamov. V rámci FS SR zatiaľ neexistuje jednoduchý spôsob prístupu k týmto záznamom a manipulácie s nimi, a teda nie je všeobecne zavedený proces automatizovaného spracovávania týchto záznamov. Čiastočne túto úlohu plní systém SIEM, ktorý však pracuje len s vybranými IS. Aktuálny systém ochrany a bezpečnosti informačných aktív a IKT infraštruktúry FS SR neumožňuje elektronickú výmenu citlivých informácií a utajovaných skutočností a zároveň neposkytuje dostatočnú úroveň zabezpečenia (dôvernosť, integrita a dostupnosť) vymieňaných citlivých informácií a utajovaných skutočností. Výhody: • Nie je nutné školiť zamestnancov na nový systém. Nevýhody: • Výmena citlivých informácií a utajovaných skutočností je aktuálne založená na manuálnom prenose v rámci pracovísk FS SR dislokovaných v celej SR. • Súčasný bezpečnostný systém funguje na zastaranej architektúre a nepokrýva všetky informačné aktíva FS SR. • Infraštruktúra v súčasnosti obsahuje izolované prvky bezpečnostnej architektúry, ktoré primárne fungujú len na vybraných zariadeniach a systémoch, teda nie sú nasadené plošne. • Aktuálny systém zabezpečenia a ochrany nespĺňa všetky požiadavky legislatívy (najmä zákona o KyB). • Systém nie je prispôsobený na súčasné bezpečnostné požiadavky, čoho dôsledkom je, že nemusia byť identifikované všetky bezpečnostné incidenty.
Priestor pre sumárny obrázok
Ďalšie informácie
Dôvod zamietnutia riešenia: Nevýhody spomenuté vyššie a najmä nemožnosť zabezpečenia súladu s požiadavkami aktuálnej legislatívy (najmä zákona o KyB) a neprispôsobenie sa požiadavkám elektronickej verejnej správy.

3.3.2. Alternatíva B – „Implementácia riešenia navrhovaného v tejto štúdii uskutočniteľnosti"

Súhrnný popis

Vzhľadom na skutočnosť, že riešenie navrhované v tejto štúdii predstavuje realizáciu len časti bezpečnostných opatrení, ktoré by mala FS SR prijať v zmysle §20 zákona o KyB, ide v podstate o minimalistický variant a teda v žiadnom prípade o riešenie, ktoré by pokrývalo bezpečnosť IKT prostredia FS SR v plnom rozsahu.

Implementácia navrhovaného riešenia spočíva v zavedení najmä:

- informačno-komunikačného systému pre bezpečnú výmenu citlivých informácií a utajovaných skutočností v elektronickej podobe (vytvorenie bezpečnej komunikačnej infraštruktúry),
  - elektronického systému (špeciálnej softvérovej aplikácie) na manipuláciu s citlivými a utajovanými informáciami s integrovanou elektronickou registratúrou a digitalizovanými internými procesmi a s integrovanými silnými bezpečnostnými prvkami,
- systému bezpečnostného monitoringu a riadenia incidentov a udalostí (SIEM), ktorý umožní monitorovanie, rýchlu diagnostiku a reakciu na prípadné bezpečnostné incidenty v kybernetickom priestore FS SR a ich vyšetrovanie, vrátane možnosti budúceho nasadenia pokročilých analytických nástrojov nad veľkým množstvom údajov (Big-data) v reálnom čase, ktoré vyhodnocujú rizikovosť subjektov a ich správanie.
- systému perimetrovej ochrany sietí a IKT prostredia FS SR implementáciou pokročilých, moderných a automatizovaných nástrojov na identifikáciu a analýzu hrozieb a anomálií v rámci sieťových tokov a sieťovej prevádzky (IDS, IPS, UTM, ADS, ATA, a pod.), ako aj nástrojov zabezpečujúcich ochranu perimetra na úrovni databáz, webových portálov a domén (NGFW, WAFW, DBFW a pod.), s prepojením na centrálny SIEM systém.

Výhody:

- Umožnenie elektronickej výmeny citlivých informácií a utajovaných skutočností a tým zabezpečenie zvýšenia časovej efektivity ich spracovania, odbúranie nadmerných administratívnych úkonov a zvýšenie bezpečnosti manipulácie s nimi.
- Možnosť nasadenia prostriedkov a prvkov KyB ochrany a monitorovania, ktoré budú identifikovať možné bezpečnostné incidenty aj v reálnom čase.
- Možnosť vytvorenia tímu a technických prostriedkov pre efektívne riešenie bezpečnostných incidentov.
- Možnosť nasadenia pokročilých bezpečnostných opatrení a sofistikovaných bezpečnostných mechanizmov a nástrojov, ktoré budú zaisťovať požadovanú úroveň ochrany sietí a sieťového perimetra FS SR.
- Používanie nástrojov a techník, ktoré odhalia zraniteľnosti a slabiny IS a aplikácií FS SR skôr ako dôjde k ich zneužitiu neoprávnenou osobou.
- Možnosť budúceho nasadenia analytických nástrojov nad veľkým množstvom údajov (Big-data) v reálnom čase, ktoré vyhodnocujú rizikovosť subjektov a ich správanie nielen na základe informácií previazaných so subjektom, ale aj na základe jeho väzieb na okolité rizikové subjekty a ich správanie.

Nevýhody:

- Nutnosť zaškolenia pracovníkov na nový systém.

Priestor pre sumárny obrázok

Ďalšie informácie

Dôvod výberu riešenia: Spomenuté výhody vyššie a hlavne zabezpečenie plnej elektronickej a bezpečnej výmeny citlivých informácií a utajovaných skutočností a zabezpečenie súladu s požiadavkami legislatívy (najmä zákona o KyB).

3.3.3. Alternatíva C – „Implementácia minimalistického riešenia"

Súhrnný popis

Minimalistická alternatíva predstavuje zníženie počtu zabezpečených PC na úroveň 1 PC na pracovisko (z úrovne 923 na úroveň počtu pracovísk (+ tenkí klienti), t.j. spolu 263 + 40 kusov). Táto úroveň umožní zrušiť fyzický prenos dokumentov pomocou kuriéra, nakoľko bude každe pracovisko technicky vybavené na elektronický prenos. Zároveň však tento variant znižuje prínosy systému v oblasti ochrany citlivých informácii, keďže nie všetci pracovníci s "need to know" prístupom majú prístup k zabezpečenému elektronickému prenosu informáci. Toto následne zvyšuje počet ľudí, ktorí majú prístup k utajovaným skutočnostiam, čo priamo znižuje prínos v tejto oblasti. Detailné porovnanie sa nachádza v kapitole ekonomická analýza.

Výhody:

- Nízke náklady na implementáciu.
- Technické vybavenie všetkých pracovísk FS SR.

Nevýhody:

- Nebolo by dosiahnuté požadované zníženie počtu pracovníkov, ktorí prichádzajú do styku s citlivými údajmi a tým pádom ani požadované zníženie rizík ich úniku.
- Výmena citlivých údajov by stále nebola dostatočne zabezpečená na úrovni jednotlivých pracovísk.
- Nutnosť zaškoliť všetkých pracovníkov na nový systém.

Priestor pre sumárny obrázok
Ďalšie informácie
Dôvod zamietnutia riešenia: Implementácia projektu v minimalistickom rozsahu by napriek vynaloženým prostriedkom neposkytla dostatočnú úroveň informačnej a kybernetickej bezpečnosti FS SR a prínosy by tak nedosiahli výšku nákladov vynaložených na realizáciu projektu.

Multikriteriálna analýza

Na posúdenie alternatív z hľadiska splnenia cieľov vytýčených v motivačnej časti štúdie je použitá multikriteriálna analýza (MCA), ktorá vychádza z nasledovných kritérii jednotlivých stakeholderov:

Kritérium	Úradník	FS SR	Iné OVM (eGov/VS)	Zdôvodnenie
Súlad s legislatívou a zabezpečenie legislatívnych požiadaviek	x	x	x	Základná požiadavka a nutnosť pre každý OVM
Elektronická výmena informácií	x	x	x	Požiadavka NKIVS a zákona o eGov
Bezpečnosť informačných aktív a IKT infraštruktúry		x	x	Požiadavka legislatívy (najmä zákon o KyB a zákon o ochrane OÚ)
Efektívny monitoring a kybernetická ochrana		x		Možnosť a schopnosť identifikácie bezpečnostných incidentov (aj v reálnom čase)
Efektívna reakcia na bezpečnostné incidenty		x		Možnosť a schopnosť adekvátnej reakcie na prípadné bezpečnostné incidenty
Využívanie moderných a automatických technológií a nástrojov na odhaľovanie hrozieb a anomálií v sieťovej prevádzke		x		Možnosť a schopnosť detekcie rizík a útokov identifikáciou možných anomálií a iných hrozieb

Vyhodnotenie jednotlivých alternatívnych riešení na základe MCA, t.j. či alternatíva spĺňa definované kritéria je nasledovné:

Kritérium	Alt. A	Spôsob dosiahnutia
Súlad s legislatívou a zabezpečenie legislatívnych požiadaviek	N	N/A - v tejto alternatíve nie je možné dosiahnuť naplnenie uvedeného kritéria
Elektronická výmena informácií	N	N/A - v tejto alternatíve nie je možné dosiahnuť naplnenie uvedeného kritéria
Bezpečnosť informačných aktív a IKT infraštruktúry	N	N/A - v tejto alternatíve nie je možné dosiahnuť naplnenie uvedeného kritéria
Efektívny monitoring a kybernetická ochrana	Č	Aktuálne len pre vybrané systémy
Efektívna reakcia na bezpečnostné incidenty	Č	Aktuálne len pre vybrané systémy
Využívanie moderných a automatických technológií a nástrojov na odhaľovanie hrozieb a anomálií v sieťovej prevádzke	N	N/A - v tejto alternatíve nie je možné dosiahnuť naplnenie uvedeného kritéria

Kritérium	Alt. B	Spôsob dosiahnutia
Súlad s legislatívou a zabezpečenie legislatívnych požiadaviek	A	Implementáciou projektu a definovaných funkcionalít
Elektronická výmena informácií	A	Implementáciou projektu a definovaných funkcionalít
Bezpečnosť informačných aktív a IKT infraštruktúry	A	Implementáciou projektu a definovaných funkcionalít
Efektívny monitoring a kybernetická ochrana	A	Implementáciou projektu a definovaných funkcionalít
Efektívna reakcia na bezpečnostné incidenty	A	Implementáciou projektu a definovaných funkcionalít
Využívanie moderných a automatických technológií a nástrojov na odhaľovanie hrozieb a anomálií v sieťovej prevádzke	A	Implementáciou projektu a definovaných funkcionalít

Kritérium	Alt. C	Spôsob dosiahnutia
Súlad s legislatívou a zabezpečenie legislatívnych požiadaviek	N	Implementácia tejto alternatívy neposkytne dostatočné naplnenie uvedeného kritéria
Elektronická výmena informácií	Č	Implementácia - zabezpečí len medzi pracoviskami, nie v rámci pracovísk
Bezpečnosť informačných aktív a IKT infraštruktúry	N	Implementácia tejto alternatívy neposkytne dostatočné naplnenie uvedeného kritéria
Efektívny monitoring a kybernetická ochrana	Č	Implementácia - zabezpečí monitoring, ale nie dostatočne komplexný a efektívny
Efektívna reakcia na bezpečnostné incidenty	N	Implementácia tejto alternatívy neposkytne dostatočné naplnenie uvedeného kritéria
Využívanie moderných a automatických technológií a nástrojov na odhaľovanie hrozieb a anomálií v sieťovej prevádzke	Č	Implementácia - zabezpečí ochranu, ale nie dostatočne komplexnú a efektívnu

Legenda: A - áno - kritérium spĺňa, N - nie - kritérium nespĺňa, Č - čiastočne - kritérium spĺňa čiastočne s rizikami, N/A - neaplikovateľné.

Na základe vyhodnotenia kritérií v rámci MCA vzišla ako optimálna alternatíva B, ktorú odporúčame realizovať.

3.4. Popis budúceho stavu

3.4.1. Legislatíva

Tabuľka 10 Legislatíva - budúci stav

Súhrnný popis	
Pre účely nasadenia zavedenia komplexného riešenia bezpečnosti nie je potrebná zmena už existujúcich zákonných ustanovení. Celé riešenie je navrhnuté podľa aktuálne platných zákonov.	
Priestor pre sumárny obrázok	
Ďalšie informácie	
Kritériá kvality	Spresnenie kritérií kvality: Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.
VP_1: Súlad s legislatívou	
Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R_TL1: Riešenie nezabezpečí dostatočne súlad so zákonom o utajovaných skutočnostiach a zákonom o KyB.	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

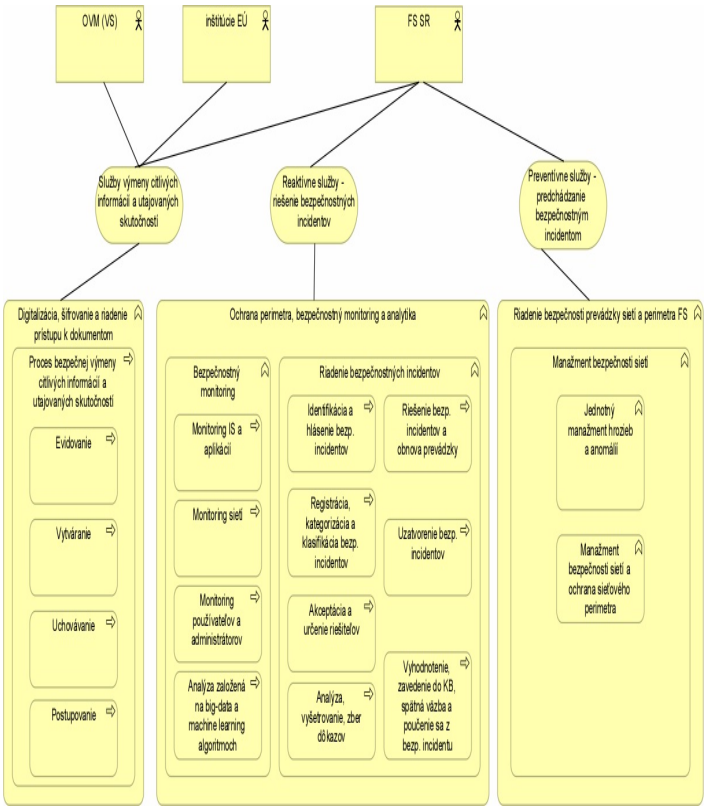
3.4.2. Architektúra

3.4.2.1. Biznis architektúra

Tabuľka 11 Biznis architektúra – budúci stav

Súhrnný popis

Budúce riešenie kybernetickej bezpečnosti FS SR na úrovni biznis architektúry bude pozostávať z nasledovných biznis funkcií:
• Ochrana perimetra, bezpečnostný monitoring a analytika:
  • Bezpečnostný monitoring, pozostávajúci z nasledovných procesov:
  • monitoring IS, platforiem, aplikácií a používateľských činností a aktivít,
  • monitoring sietí,
  • monitoring činností a aktivít privilegovaných používateľov,
  • analýza založená na big-data a machine learning algoritmoch,
  • Riadenie bezpečnostných incidentov, pozostávajúce z nasledovných procesov:
  • identifikácia a hlásenie bezpečnostných incidentov,
  • registrácia, kategorizácia a klasifikácia bezpečnostných incidentov,
  • akceptácia bezpečnostných incidentov a určenie riešiteľov,
  • analýza a vyšetrovanie bezpečnostných incidentov a zber dôkazov.
  • riešenie bezpečnostných incidentov a obnova prevádzky,
  • uzatvorenie bezpečnostných incidentov,
  • vyhodnotenie bezpečnostných incidentov, zavedenie do KB DB, spätná väzba a poučenie sa z bezpečnostného incidentu.
  • Riadenie bezpečnosti prevádzky sietí a perimetra FS, pozostávajúce z nasledovných procesov:
  • Jednotný manažment hrozieb a anomálií (nasadenie moderných a automatizovaných nástrojov pre detekciu a analýzu hrozieb a anomálií v sieťovej prevádzke a v sieťových tokoch),
  • manažment bezpečnosti sietí a ochrana sieťového perimetra (nasadenie nových moderných sieťových prvkov),
• Digitalizácia, šifrovanie a riadenie prístupu k dokumentom:
  • Proces bezpečnej výmeny citlivých informácií a utajovaných skutočností v internom prostredí a medzi spolupracujúcimi OVM a inštitúciami EÚ (implementovaním certifikovaných prostriedkov šifrovej ochrany informácií).



Navrhovaný bezpečný systém na výmenu a správu citlivých dokumentov a utajovaných skutočností musí spĺňať všetky požiadavky platnej legislatívy o utajovaných skutočnostiach a o kybernetickej bezpečnosti. Zároveň by mal prispieť k efektívnejšiemu plneniu úloh FS SR (výrazná úspora času, ľudských zdrojov, finančných a materiálnych prostriedkov, väčšia odolnosť voči úniku a neoprávnenej manipulácii s citlivými dokumentami a utajovanými skutočnosťami).

Zavedenie procesu plošného, komplexného, automatizovaného spracovávania log záznamov z jednotlivých systémov by výrazne sprehľadnilo a zjednodušilo monitorovací proces, čo by malo za následok zlepšenie bezpečnosti celej IKT infraštruktúry FS SR.

Kritériá kvality	Spresnenie kritérií kvality: Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.

VP_2: Eliminácia výmeny údajov za použitia fyzických médií. Skrátenie doby potrebnej na výmenu údajov.

VP_3: Počet IS zapojených do centrálneho monitorovacieho nástroja SIEM. Počet detekovaných bezpečnostných incidentov.

VP_4: Počet detekovaných a eliminovaných bezpečnostných incidentov.

VP_5: Akceptovateľný výstup bezpečnostného auditu.

Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.

R_TB1: Zamestnanci FS SR budú aj naďalej využívať manuálnu výmenu citlivých údajov v rámci pracoviska.

R_TB2: Neefektívny proces monitorovania a logovania.

R_TB3: Nefektívne zabezpečenie perimetrovej ochrany.

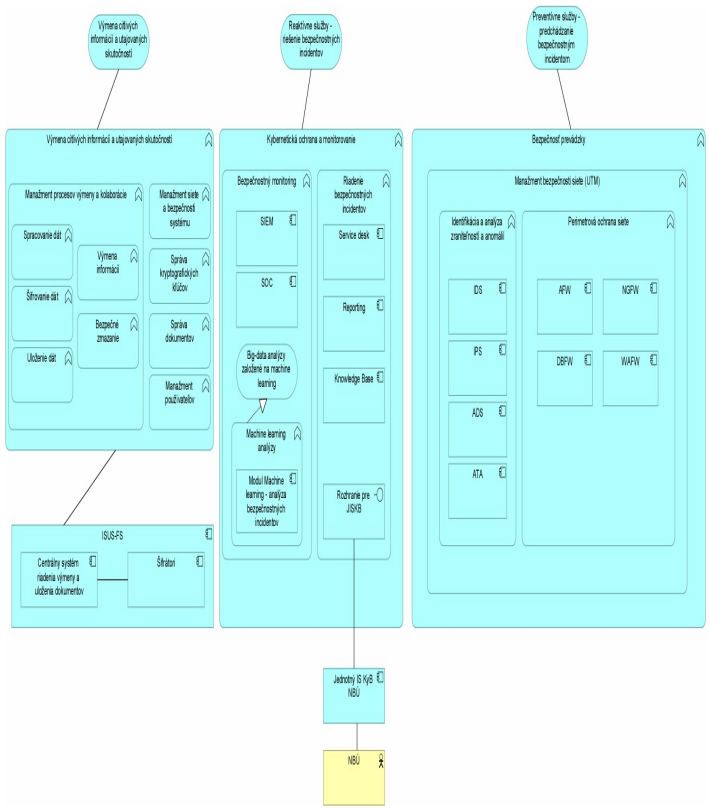
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

3.4.2.2. Architektúra informačných systémov

Tabuľka 12 Architektúra informačných systémov - budúci stav

Súhrnný popis

Budúce riešenie kybernetickej bezpečnosti FS SR na úrovni architektúry informačných systémov pozostáva zo súboru navzájom prepojených softwarových aplikácií a nástrojov.
 	
Celoplošný monitorovací systém SIEM bude zabezpečovať komplexný nepretržitý monitoring bezpečnostnej situácie FS SR. Jeho hlavnými úlohami sú:
 	
• monitoring agendových IS, platforiem, aplikácií a používateľov,
• monitoring sietí,
• monitoring činností a aktivít privilegovaných používateľov,
• ukladanie log záznamov pre prípad potreby vykonania auditu, forenznej analýzy alebo vyšetrovania bezpečnostného incidentu,
• analýza záznamov založená na big-data a machine learning algoritmoch.
 	
Oblasť bezpečnosti prevádzky sietí bude podporená implementáciou jednotného systému pre manažment hrozieb (Unified Threat Management – UTM), ktorý bude nasadený v rámci každej lokality na všetkých vstupných a výstupných sieťových linkách FS SR a ktorý bude pozostávať primárne z nasledovných aplikačných modulov:
 	
• automatizované nástroje pre detekciu a analýzu hrozieb a anomálií:
  • systém na detekciu prienikov (Intrusion Detection System – IDS),
  • systém na prevenciu prienikov (Intrusion Prevention System – IPS),
  • systém na detekciu anomálií (Anomaly Detection System – ADS),
  • systém na pokročilú analýzu hrozieb na úrovni domény (Advanced Threat Analytics – ATA),
  • sondy a kolektory sieťovej komunikácie,
• pokročilé sieťové prvky:
  • firewall novej generácie (Next Generation Firewall - NGFW),
  • databázový firewall (Database Firewall – DBFW) pre všetky databázy s citlivými údajmi a utajovanými skutočnosťami,
  • webový aplikačný firewall (Web Application Firewall – WAFW) pre webový portál FS SR podporujúci funkciu SSL Offloading na zvýšenie robustnosti servera pri vysokej záťaži.
 	
V rámci UTM budú všetky systémy a moduly prepojené s monitorovacím nástrojom SIEM a poskytnú tak komplexné riešenie pre manažment bezpečnosti prevádzky a riadenie hrozieb.
 	
V oblasti digitalizácie a bezpečnosti komunikácie budú nasadené nasledovné aplikačné nástroje a systémy:
 	
• Implementácia koncových staníc s integrovaným certifikovaným prostriedkom šifrovej ochrany informácií, zabezpečujúcim šifrovanie disku, šifrovanie súborov a adresárov, ako aj šifrovanie informácií ukladaných na externých médiách.
• Implementácia centralizovaného systému, ktorý umožní efektívnu a bezpečnú výmenu a zdieľanie citlivých informácií a utajovaných skutočností.
 	
Pôjde o komplexnú implementáciu certifikovaného informačného systému na ochranu utajovaných skutočností, vrátane jeho testovania a nasadenia do produkčnej prevádzky, vrátane dodávky a nasadenia potrebnej hardvérovej a softvérovej infraštruktúry.



Riadenie bezpečnostných incidentov bude v súlade s platnou legislatívou prepojené na JISKB, ktorý je spravovaný NBÚ. Závažné kybernetické incidenty tak budú automaticky nahlasované do tohto systému.

Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.

R_TI1: Nesprávna integrácia systémov na SIEM.

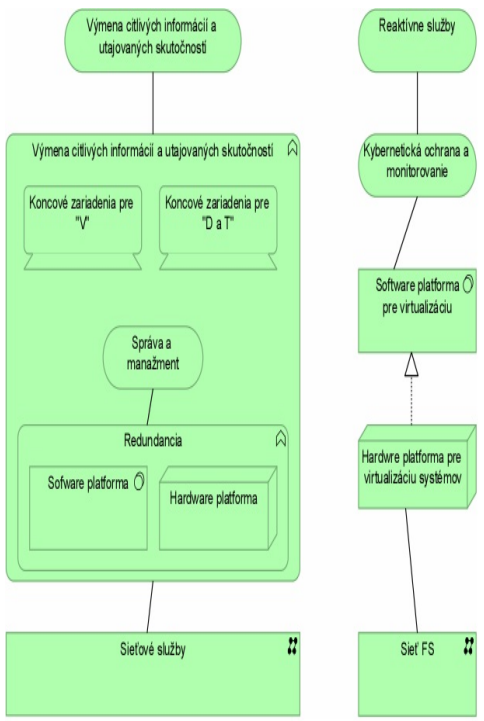
R_TI2: Riešenie nebude dostatočne flexibilné.

Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

3.4.2.3. Technologická architektúra

Tabuľka 13 Technologická architektúra - budúci stav

Súhrnný popis
Technologická architektúra vychádza z navrhovanej architektúry IS a z požiadaviek definovaných v rámci biznis architektúry. Technologická architektúra je nevyhnutným elementom na to, aby bolo možné prevádzkovať a zabezpečovať všetky úrovne služieb, funkcií, modulov a systémov. Samotný systém môže byť prevádzkovaný vo virtualizovanom prostredí s load balancingom, dostatočne rezervovaným výkonom, kapacitou a vhodnou systémovou a databázovou platformou, čím sa okrem iného zabezpečí aj úspora prevádzkových nákladov (energetická efektívnosť, zredukovanie počtu fyzických počítačov a zvýšenie pomeru serverov na správcu), transparentné sieťové služby a prenositeľnosť dát. Z pohľadu definovaných služieb virtuálneho Cloudu budú vyžadované nasledovné hlavné služby: • virtuálny diskový server/servre (bez viazanosti), • diskový priestor (redundantné diskové pole, bez viazanosti), • firewall a aplikačný firewall (pre bezpečnosť komunikácie a prístupov), • load balancing (pre rozloženie záťaže), • služby pripojenia do nadrezortnej informačnej siete (FINNET 3). Predpokladá sa úplná virtualizácia systému s osobitným zameraním na bezpečnosť riešenia a striktné riadenie prístupu. S ohľadom na význam poskytovaných služieb sa predpokladá zapojenie v režime vysokej dostupnosti a prevádzka v dvoch geograficky odlišných lokalitách. HW centrálneho uzla (Cloudu) bude bude umiestnený v chránených priestoroch FR SR. Zároveň sa na týchto miestach budú nachádzať aj pracoviská centrálneho uzla a zabezpečené dátové úložisko. Dátové úložisko bude tvoriť platformu na ukladanie citlivých informácií a utajovaných skutočností. Bude vybavené technickým riešením zabezpečujúcim dátovú redundanciu pre zamedzenie straty alebo poškodenia dát. Prístup k dátovému úložisku bude monitorovaný, pre potreby auditu alebo forenznej analýzy v prípade bezpečnostného incidentu. Na koncových zariadeniach bude nasadený virtualizačný SW, ktorý oddelí pracovné prostredie pre prácu s citlivými informáciami a informáciami klasifikovanými ako "Vyhradené", "Dôverné" a "Tajné". Zároveň budú disponovať ďalším softvérom, ktorý zaistí bezpečné prihlásenie k centrálnemu uzlu, systémom pre monitorovanie prístupov, monitorovanie bezpečnosntých incidentov, systémom pre správu zariadenia a balíkom pre tvorbu a úpravu dokumentov obsahujúcich citlivé informácie. Autentizácia užívateľov koncových zariadení bude dvojfaktorová. K centrálnemu uzlu budú koncové zariadenia pripojené pomocou zabezpečeného vzdialeného prístupu (IP VPN). Všetky technické prvky a kryptografické opatrenia budú spĺňať potreby a požiadavky aktuálne platných zákonov, bezpečnostných noriem a štandardov.

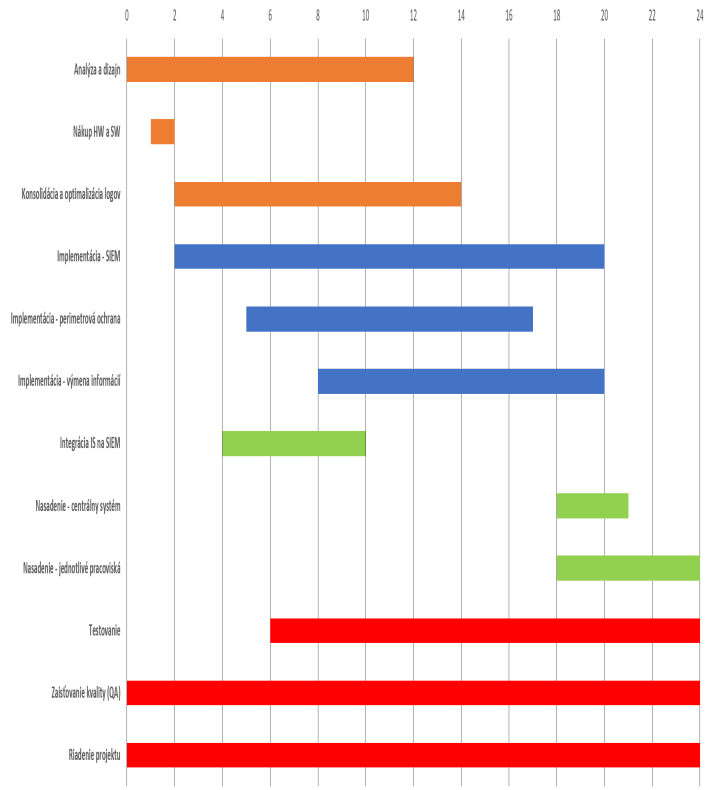


Ďalšie informácie	
Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R_TT1: Zložitosť a časová náročnosť riešenia. R_TT2: Nedosiahnutie stanovených technických parametrov.	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

3.4.2.4. Implementácia a migrácia

Tabuľka 14 Implementácia a migrácia

Súhrnný popis
Implementácia je predpokladaná v štyroch fázach: Fáza I. – Analýza a príprava (Analýza a dizajn): • konzultačno-analytické práce spojené s identifikáciou potrebných zdrojov a možností realizácie, • výber spôsobu technologického riešenia, testovanie prototypov, • tvorba modelu údajov pre výmenu citlivých informácií a utajovaných skutočností, • definícia rolí, oprávnení a bezpečnostných politík, • koncepčný návrh riešenia informačnej a kybernetickej bezpečnosti. Fáza II. – Realizácia riešenia (Implementácia): • modifikácia používateľskej softvérovej aplikácie pre bezpečnú výmenu a manipuláciu s citlivými informáciami a utajovanými skutočnosťami podľa špecifických potrieb FS SR, • agilná implementácia a nasadenie v súlade s bežným SDLC (pre neštandardné komponenty), • vytvorenie potrebných konektorov a integrácie, • modernizácia a rozšírenie informačno-komunikačnej platformy, • integrácia nového informačného systému s existujúcou IKT infraštruktúrou, • obvyklé testovanie používateľskej softvérovej aplikácie pre bezpečnú výmenu a manipuláciu s citlivými informáciami a utajovanými skutočnosťami, vrátane testovania komponentov nového IS s internými aj externými používateľmi, • migrácia a čistenie údajov, testovanie po migrácii údajov, • implementácia bezpečnostných opatrení v súlade s koncepčným návrhom riešenia informačnej a kybernetickej bezpečnosti. Fáza III. – Skúšobná prevádzka (Testovanie): • ostrá migrácia údajov, • vulnerability testovanie a ladenie bezpečnostných nastavení systémov, • realizácia všetkých potrebných školení (školenia administrátorov, bezpečnostných správcov a používateľov), • testovanie, zapracovávanie pripomienok a zistení používateľov, administrátorov a bezpečnostných správcov, ladenie. Fáza IV. – Uvedenie systému do riadnej prevádzky (Nasadenie) • Po dokončení a vyladení systému prechod na plnú prevádzku systému už plne v gescií FS SR. • Predpokladá sa technická podpora správy a údržby informačného systému počas nasledujúcich 10 rokov. Samostatnou fázou, resp. aktivitou je Nákup HW a krabicového SW. Vzhľadom na výšku nákladov sa jedná o pomerne veľký projekt, pričom cieľom je, aby jeho riadenie zahŕňalo poučenia z projektov realizovaných v rámci programu OPIS. Je potrebné klásť dôraz najmä na: • podľa možností agilný prístup k nasadzovaniu technických komponentov a vývoju, • zabezpečenie dostatočného projektového tímu na strane zákazníka minimálne na úrovni garantov, ktorí sa vedia projektu venovať na dennej báze, • dodržiavanie princípov projektového riadenia PRINCE2 (definované produkty s akceptačnými kritériami, zmenový rozpočet, tolerancie jednotlivých míľnikov, etáp a aj samotných produktov), • knowledge transfer – transfer vedomostí od dodávateľa členom tímu klienta. Poznámka: Vzhľadom na charakter projektu - kde neprebieha vývoj SW - nie sú fázy v tomto dokumente pomenované presne podľa príručky pre žiadateľa. Aktivity v CBA však sú zadelené do aktivít podľa príručky OPII, pričom analýza a príprava zodpovedá aktivite Analýza a dizajn, Realizácia je Implementácia, Skúšobná prevádzka predstavuje Testovanie a Uvedenie systému do prevádzky predstavuje Nasadenie. Pre zjednodušenie toto uvádzame aj v zátvorke za názvami aktivít vyššie.



Tabuľka s harmonogramom sa nachádza v prílohe k tejto štúdii uskutočniteľnosti.	
Kritériá kvality	Spresnenie kritérií kvality: Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.
VP_6: Dodržiavanie plánu projektu. VP_7: Funkčné projektové registre a manažment zmien.	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

3.4.2.5. Bezpečnostná architektúra

Tabuľka 15 Bezpečnostná architektúra - budúci stav

Súhrnný popis	
Nakoľko tento projekt nerealizuje typický agendový systém ale celý projekt pojednáva o bezpečnosti informačných aktív a IKT infraštruktúry FS SR, je táto kapitola neaplikovateľná.	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení

3.4.3. Prevádzka

Tabuľka 16 Prevádzka - budúci stav

Súhrnný popis	
Úvodné informácie Vybudovanie nosnej infraštruktúry bezpečného informačno-komunikačného systému FS SR bude svojím charakterom dôležitým bezpečnostným prvkom v celkovej bezpečnostnej architektúre FS SR zahŕňajúcim desiatky agendových IS FS SR. Vzhľadom na túto skutočnosť budú na tento bezpečnostný systém kladené vysoké požiadavky týkajúce sa jeho prevádzky a spoľahlivosti. Nedostupnosť systému alebo jeho nespoľahlivosť môžu mať významné negatívne dopady a dôsledky na chod celej organizácie, prípadne aj na chod organizácií, s ktorými si FS SR vymieňa citlivé údaje a utajované skutočnosti. Samotná prevádzka riešenia bude prebiehať v datacentre FS SR. Z hľadiska prevádzky systému sú (predbežne) definované nasledujúce požiadavky: • Prevádzka systému: 24x7, • Miera dostupnosti: min. 98,5-99,5%, • Forma podpory: telefonická, email, ServiceDesk, podpora priamo na mieste, • Riešenie redundancie prostriedkov: cluster, geo-cluster. Prevádzka bude zabezpečená pracovníkmi IT a bezpečnostného oddelenia FS SR (správa a používanie bezpečnostných aplikácií a modulov). Využije sa trojvrstvová úroveň podpory: • prvú úroveň podpory (L1) bude zabezpečovať bezpečnostné oddelenie FS SR, ktoré bude riešiť predovšetkým infraštruktúrne a technologické požiadavky, • aplikačná podpora druhej úrovne (L2) bude zabezpečovaná oddelením IT a bezpečnostným oddelením FS SR, • tretia úroveň podpory (L3), bude zabezpečovaná dodávateľmi jednotlivých riešení (modulov a aplikácií). V rámci prvej úrovne podpory bude realizovaný príjem a identifikácia požiadaviek s následným smerovaním na konkrétneho riešiteľa v rámci IT alebo bezpečnostného oddelenia FS SR. Druhá úroveň podpory, poskytovaná priamo IT a bezpečnostným oddelením FS SR, bude rozdelená na viac oblastí podľa jednotlivých biznis bezpečnostných funkcií systému a jeho modulov (výmena informácií, monitoring, perimetrová ochrana). Tretia úroveň bude podľa potreby zabezpečovaná dodávateľmi softvérového a hardvérového vybavenia. Za týmto účelom bude pripravená SLA dohoda na obdobie 10 rokov, ktorá pokryje SW a HW podporu všetkých bezpečnostných modulov, ktoré sú predmetom projektu. V rámci metodickej podpory bude IT a bezpečnostné oddelenie FS SR zabezpečovať najmä: • odbornú prípravu a školenia operátorov a administrátorov bezpečnostných systémov, • tvorbu metodických postupov a usmernení pre zabezpečenie plynulej a spoľahlivej prevádzky bezpečnostných systémov a obnovy prevádzky monitorovaných systémov FS SR, • tvorbu metodických postupov a usmernení v oblastí identifikácie a analýzy rizík a zraniteľností. Cieľom pri zabezpečení prevádzky je dosiahnuť, aby rozsah aplikačnej podpory prenášanej na dodávateľa bol minimalizovaný, t. j. aby maximum prác súvisiacich so správou a podporou prevádzky bolo realizovaných pracovníkmi IT a bezpečnostného oddelenia FS SR.	
Priestor pre sumárny obrázok	
Ďalšie informácie Prevádzkovanie bezpečnostných systémov bude personálne zabezpečené dostatočným počtom riešiteľov (garantov za prevádzku IT a jednotlivé oblasti riadenia bezpečnosti). Aktuálne má FS SR na zabezpečenie realizácie projektu alokovaných 5 pracovníkov IT oddelenia a 2 pracovníkov oddelenia bezpečnosti. Plánovaný je nárast o ďalšie 3 miesta (pozície IT operátorov a administrátorov) a 5 miest odborných garantov za oblasť riadenia IB a KyB (operátorov a administrátorov bezpečnostných systémov a systémov monitoringu /najmä SIEM/) pred nasadením systému do ostrej prevádzky. Počas prípravy projektu a jeho ďalších fáz je nutné postupne definovať, optimalizovať a konsolidovať logy a auditné záznamy z jednotlivých agendových IS, ktoré budú predmetom bezpečnostného monitoringu. Definovanie, optimalizácia a konsolidácia logov bude musieť prebehnúť spolu s biznis vlastníkmi jednotlivých systémov (útvarov FS SR). Účelom tejto aktivity je zabezpečiť čo najefektívnejší proces zberu a vyhodnocovania logov a auditných záznamov s cieľom minimalizácie falošných poplachov a minimalizácie stavov kedy nie je identifikovaný reálny bezpečnostný incident.	
Kritériá kvality	Spresnenie kritérií kvality: Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.

VP_8: Miera dostupnosti a spoľahlivosti VP_9: Zabezpečenie testovania, školení a dokumentácie VP_10: Nízka miera incidentov na aplikačnej úrovni VP_11: Kontinuálny rast kvality a efektivity procesov monitoringu bezpečnostných incidentov	
Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R_TP1: Nedostatok finančných prostriedkov na pokrytie prevádzky. R_TP2: Neefektívne nastavenie procesov bezpečnostného monitoringu - zlyhanie fázy optimalizácie a konsolidácie logov. R_TP3: Nedostatočná kvalita poskytovaných služieb bezpečnosti. R_TP4: Neskoré vybudovanie personálnej štruktúry s dostatočnými skúsenosťami a kvalifikáciou.	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

3.4.4. Ekonomická analýza

Tabuľka 17 Ekonomická analýza - budúci stav

Súhrnný popis
Čistá súčasná ekonomická hodnota (ENPV) = 34 535 897 Rok návratu investície (PBP) = 6

Aktivita	Cena
Nákup HW a krabicového softvéru - HW	21 739 961 €
Nákup HW a krabicového softvéru - SW	9 876 604 €
Analýza a dizajn	2 086 560 €
Implementácia	4 021 920 €
Testovanie	1 965 600 €
Nasadenie	2 328 480 €
Projektové riadenie	1 355 456 €
Publicita a informovanosť	0 €
Rozpočet spolu s DPH	43 374 581 €

Náklady na projekt pozostávajú z nákladov na dva moduly, ktoré sú predmetom projektu. Sú to:

- Manuálna výmena údajov citlivých informácií a utajovaných skutočností - náklady vo výške 31 mil. EUR
- Kybernetická ochrana a monitoring - náklady vo výške 11 mil. EUR

Prínosy systému sú nasledovné:

- zníženie únikov informácii, ktoré je ocenené na základe rizikovej analýzy, historických údajov a skúseností FS SR vo výške 16 mil. EUR ročne,
- prínosy z nahradenia transportu informácii elektronickou výmenou dát a z toho vyplývajúceho ušetrenia času, pohonných hmôt a amortizácie aút vo výške 0,7 mil. EUR ročne.

Detailné informácie k prínosom sú uvedené v CBA, pričom nie všetky informácie sú verejné.

Porovnanie preferovanej a minimalistickej alternatívy je uvedené v tabuľke nižšie.

Parameter	Preferovaná alt.	Minimalistická alt
BCR	1,62	0,59
ENPV	34 535 897	-21 555 536
Návratnosť	6	-

Priestor pre sumárny obrázok
Ďalšie informácie

Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.

R_E1: Nepodarí sa dosiahnuť preukázateľné úspory podľa plánu.

R_E2: Náklady na vybudovanie alebo prevádzku presiahnu plánovanú hodnotu.

Prílohy
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.