DataCentrum
medzi Vami a financiami

Cintorínska 5,
814 88 B r a t i s l a v a

ISO
QSCert
9001

Správa
o hodnotení plnenia úloh za rok 2017 vyplývajúcich
z „Kontraktu uzatvorenom medzi MF SR a DataCentrom
na rok 2017“

Bratislava marec 2018

Úvod

Správa o hodnotení plnenia úloh za rok 2017 vyplývajúcich z „Kontraktu uzatvorenom medzi Ministerstvom financií SR a DataCentrom na rok 2017“ sa predkladá na základe Interného riadiaceho aktu MF SR č. 5/2005 „Smernica na vypracovanie kontraktov medzi MF SR a rozpočtovými organizáciami v jeho pôsobnosti“ v znení Dodatku č. 1 s účinnosťou od 15. 11. 2008, Dodatku č. 2 s účinnosťou od 5. 2. 2010, Dodatku č. 3 s účinnosťou od 5.7.2015 a v súlade s „Kontraktom uzatvorenom medzi MF SR a DataCentrom na rok 2017“, čl. VI., bod 1., schváleným poradou vedenia MF SR a podpísaným dňa 20. 12. 2016. Kontrakt je plánovacím a organizačným aktom vymedzujúcim vecné, finančné a organizačné vzťahy medzi MF SR a DataCentrom, ktoré je v priamej riadiacej pôsobnosti MF SR a je napojené na rozpočet kapitoly rezortu MF SR.

DataCentrum, v zmysle štatútu, zabezpečuje predovšetkým správu a prevádzkovanie rozsiahlych projektov informačných systémov rezortu MF SR, vrátane celoštátne významných informačných systémov. Tieto činnosti spočívajú v overovaní, zavádzaní a prevádzkovaní jednotlivých informačných systémov (IS), v softvérových, technických a komunikačných riešeniach, ktoré vyplývali z obsluhy, údržby a rozširovania informačných systémov inštalovaných v DataCentre.

Všetky aktivity boli aj v roku 2017 vykonávané v súlade s potrebami a náležitosťami projektov a požiadavkami odberateľov výstupov.

Neoddeliteľnou časťou výkonov boli všetky činnosti vykonávané v rámci ekonomického, organizačného, metodického a koncepčného riadenia DataCentra a činnosti súvisiace so zabezpečovaním bežnej, rutinnej prevádzky a chodu DataCentra ako organizácie.

Z hľadiska výstupov poskytuje DataCentrum služby predovšetkým Ministerstvu financií SR, Štátnej pokladnici, ostatným orgánom a inštitúciám verejnej správy a niektorým neštátnym a komerčným organizáciám.

Užívateľmi výstupov boli predovšetkým organizačné útvary MF SR (sekcia rozpočtovej politiky, sekcia štátneho výkazníctva, sekcia finančného trhu, sekcia daňová a colná, , odbor informačných technológií, kancelária ministra), Štátna pokladnica a Finančná správa.

DataCentrum poskytovalo vybrané informácie aj ďalším ústredným orgánom štátnej správy (ŠÚ SR, MH SR, MPSVR SR, MPRV SR, MD SR, MŠVVaŠ SR a pod.), inštitúciám verejnej správy, niektorým neštátnym inštitúciám (ratingové spoločnosti) a bankovým subjektom. Informácie boli poskytované najmä z oblasti spracovania účtovných výkazov právnických a fyzických osôb, bankových účtovných výkazov, ako aj o hypotekárnych a stavebných úveroch.

Výstupy z riešení, najmä z projektu informačného systému výkazníctva, boli štandardne použité pri analytických prácach, pri zostavovaní štátneho rozpočtu, pri kontrole rozpisu štátneho rozpočtu, pri sledovaní plnenia príjmov a čerpania výdavkov štátneho rozpočtu.

V rámci prevádzky IS systému štátnej pokladnice (IS SŠP) DataCentrum poskytuje permanentne podporu užívateľom pre RIS (moduly ZoRo, MPR, RI, MUR) s následnou väzbou na modul finančného plánu a platobného styku štátnej pokladnice.

Výstupy za jednotlivé úlohy boli spracovávané v súlade s internými normami systému manažérstva kvality a zodpovedali požiadavkám jednotlivých odberateľov - k zasielaným výstupom neboli žiadne pripomienky.

Výkon komplexu činností pre používateľov KTI a informačných systémov prevádzkovaných DataCentrom, t. j. riešenie požiadaviek na podporu zo strany používateľov a aplikačnej, technologickej a metodickej pomoci zabezpečuje Centrum podpory užívateľov (CPU) ktoré DataCentrum prevádzkuje. Poskytované služby zabezpečujú odborné poradenstvo predovšetkým pre potreby úspešného fungovania rozpočtového informačného systému a pre IS systému štátnej pokladnice. CPU je podporované vytvorenou a nepretržite udržiavanou komunikačno-technologickou infraštruktúrou.

V roku 2017 poskytlo CPU služby potenciálne 61 146 používateľom, pričom počet organizácií používajúcich aspoň jeden informačný systém prevádzkovaný DataCentrom bol 8 755 a počet používateľov s aktívnym prístupom do IKT prevádzkovaných DataCentrom bol 28 787. Celkový počet kontaktovaní CPU používateľmi bol 49 524, z toho 32 380 telefonických. Počet uzatvorených, t.j. vyriešených hlásení jednotlivými pracovnými skupinami riešiteľov za rok 2017 bol 36 848. CPU v roku 2017 odoslalo používateľom 7 784 listových zásielok.

Okrem informačných systémov na podporu riadiacich aktivít MF SR je v DataCentre i naďalej úspešne prevádzkovaný projekt monitorovacieho systému pre štrukturálne fondy a kohézny fond (ITMS), portál ITMS, kde k 31.12.2017 bolo registrovaných celkom 21 622 aktívnych užívateľov z toho 15 353 za IITMS II a 6 269 za ITMS2014+, ktorý bol už nasadený do produkčnej prevádzky a pre užívateľov bola zabezpečovaná aj užívateľská podpora.

Dostupnosť produkčného systému ITMS Core a ITMS Portál bola 100%, pričom bolo vyriešených 1 513 hlásení užívateľov ITMS Core a 956 hlásení užívateľov ITMS Portál. K 31.12.2017 bolo v ITMS 1 739 aktívnych užívateľov a ITMS Portál využívalo aktívne 13 543 užívateľov.

IT monitorovací systém pre Európske štrukturálne a investičné fondy pre programové obdobie 2014-2020 (ITMS2014+ verejná a ITMS 2014+ neverejná časť) je v prevádzke už od 15.7.2015, pričom v roku 2017 sa v DataCentre realizovali činnosti súvisiace so zabezpečovaním jeho produkčnej prevádzky vedúce aj k skvalitňovaniu poskytovaných služieb, ako aj činnosti na odstránenie nedostatkov zistených vládnym auditom ITMS2014+. Dostupnosť ITMS2014+ (verejná i neverejná časť) bola v hodnotenom období 99,99%, bolo vyriešených celkom 5 539 hlásení a evidovaných v neverejnej časti 2 046 užívateľov a vo verejnej časti až 9 367 užívateľov.

V rámci zabezpečovania projektu informačného systému účtovníctva fondov (ISUF) - jeho aplikačnej, technickej, technologickej podpory a monitoringu, poskytovalo DataCentrum používateľom systému ISUF podporu 1. stupňa a v spolupráci s odbornými garantmi MF SR a dodávateľom systému ISUF aj podporu 2. a 3. stupňa prostredníctvom aplikácie HP Service Manager - v roku 2017 to bolo 111 užívateľom informačného systému ISUF, pričom počet hlásení bol 666 a všetky, t. j. 100%, boli vyriešené v súlade s požiadavkami klientov a hodnotiacimi kritériami úlohy. Počet incidentov zaznamenaných v rámci monitorovania CMP a následne vyriešených bol 47, z toho mimo času platnosti SLA až 36.

DataCentrum, ako prevádzkovateľ Registra účtovných závierok, aj v roku 2017 naďalej v zmysle § 23c zákona č.431/2002 Z. z. o účtovníctve v znení neskorších predpisov (zákona 333/2014 Z.z., ktorým sa mení a dopĺňa zákon č.595/2013 Z.z. o dani

z príjmov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony) a v súlade so zákonom č.145/1995 Z.z. o správnom konaní, vydávalo na základe žiadosti overené kópie dokumentov alebo časti dokumentov, ktoré sú uložené v Registri účtovných závierok. Činnosti boli zabezpečované osobitným špecializovaným pracoviskom (podateľňa RÚZ).

V roku 2017 bolo doručených celkom 173 žiadostí o poskytnutie údajov z RÚZ, z toho bolo 109 podaných osobne a 44 doručených poštou. V nadväznosti na uzatvorenú medzi MF SR a Slovenskou poštou a zmluvou DataCentra o umiestnení, prevádzkovaní technického vybavenia a o zapojení do systému centrálnej evidencie poplatkov e-Kolok boli zabezpečované aj v roku 2017 technologické i procesné podmienky súvisiace s prevádzkou tzv. softvérovej pokladne, ktorá umožňuje zamestnancom prijímať a evidovať úhrady za poplatky v centrálnom systéme evidencie. Všetky požiadavky klientov hlásené cez CPU boli zaznamenané v Service Manageri (445) boli vyriešené v stanovenom termíne a v súlade s požiadavkami SLA - t.j. bolo poskytnuté poradenstvo na telefonickej alebo e-mailovej úrovni, prípadne bola zabezpečená druhá úroveň podpory.

V rámci prevádzkovej podpory pre výpočtovú techniku a informačné systémy boli zaznamenávané požiadavky a incidenty od zamestnancov aj dodávateľov MF SR, ktoré boli nahlasované e-mailom na helpdesk@mfsr.sk (4140 správ), cez MFSR CRM systém (558) a tiež telefonicky na CPU DataCentra (393 - za posledné 4 mesiace) a osobne. Nahlásené požiadavky boli neodkladne vyriešené na prvej úrovni podpory alebo postúpené na vyššiu úroveň. Využili sa technické znalosti personálu ako aj príslušné servisné zmluvy. Všetky požiadavky boli v rámci technických a personálnych možností vyriešené v stanovenom termíne.

Úlohy, ktorých gestorom je špecializovaný útvar CSIRT.SK, boli riešené a zabezpečované v súlade s úlohami, ktoré boli definované pri zriadení útvaru a boli zabezpečované v zmysle harmonogramu poskytovania služieb špecializovaného útvaru CSIRT.SK schváleného uznesením vlády SR č. 479/2009 zo dňa 1. 7. 2009. V roku 2017 bolo zaznamenaných a riešených 230 počítačových incidentov, ktoré boli nahlásené klientelou CSIRT.SK, zahraničnými partnermi, subjektami Slovenskej republiky, alebo boli zistené monitoringom CSIRT.SK. Špecializovaný útvar CSIRT.SK prijal 838 422 hlásení o možnom výskyte škodlivej aktivity z IP adries v Slovenskej republike.

V roku 2017 sa DataCentrum aktívne zúčastnilo viacerých pracovných rokovaní a poskytovalo odbornú pomoc pri migrácii informačných systémov iných rezortov do Vládneho cloudu, ktorý je nasadený a housovaný v priestoroch dátovej sály DC Kopčianska. Boli vykonané viaceré pracovné stretnutia k zákonu o hazardných hrách a k vytvoreniu z neho vyplývajúceho registra vylúčených hráčov a konzultácie k problematike blokovania zakázaných ponúk v zmysle uplatňovania zákona o hazardných hrách.

Zo strany DataCentra bola v roku 2017 poskytovaná aj konzultačná podpora pre používateľov IS IOM.

Vnútorný kontrolný systém v DataCentre bol v roku 2017 realizovaný útvarom kontroly v súlade s „Plánom kontrolnej činnosti na rok 2017“, schváleným riaditeľom DataCentra. Zameranie vnútornej kontroly bolo orientované na rozhodujúce oblasti činnosti v nadväznosti na všeobecne záväzné právne predpisy a interné smernice. Ako súčasť svojej riadiacej práce, výkon kontroly zabezpečovali aj vedúci zamestnanci odborných útvarov.

V roku 2017 bolo uskutočnených celkom 28 kontrolných akcií interného charakteru. Kontroly boli vykonávané v týždenných, štvrťročných, polročných a ročných intervaloch. Pri kontrolách boli zistené iba drobné nedostatky, ktoré boli v priebehu kontroly odstránené. Nebolo zaznamenané hrubé porušenie všeobecne záväzných právnych predpisov a ani ostatných predpisov vydaných na ich základe. V súvislosti s ukončením pracovného pomeru zamestnankyne podateľne RÚZ bola vykonaná kontrola stavu hotovosti pokladnice RUZ a kompletnosti a správnosti súvisiacej dokumentácie, pri ktorej nebolo zistené žiadne pochybenie. Z vykonaných kontrol boli vypracované správy, ktoré spĺňajú všetky náležitosti a obsahujú relevantné informácie a zistenia.

Na útvare kontroly je vedená aj evidencia petícií a sťažností. V roku 2017 DataCentrum neevidovalo žiadne podanie petície podľa zákona o petičnom práve č. 85/1990 Zb. v znení neskorších predpisov, ani sťažnosti podľa zákona o sťažnostiach č. 9/2010 Z. z. v platnom znení.

V roku 2017 DataCentrum udržiavalo a skvalitňovalo systém riadenia kvality podľa medzinárodnej normy systému riadenia kvality EN ISO 9001 : 2015. V DataCentre sa pravidelne uskutočňuje kontrolný audit vykonávaný externou spoločnosťou pod vedením manažéra kvality. V novembri a decembri 2017 boli realizované interné audity interným audítorom a externým audítorom, na základe ktorých boli prijaté 2 nápravné opatrenia, V decembri 2017 bol vykonaný externý kontrolný audit zavedeného systému riadenia kvality. Auditmi neboli zistené žiadne nezhody a DataCentrum obhájilo certifikát ISO 9001 na ďalší rok.

Významnou časťou aktivít DataCentra je oblasť personálneho zabezpečenia chodu pracovísk a plnenia všetkých úloh. I naďalej pretrváva stav, kedy zabezpečovanie kvalifikovaných odborníkov je problematické a náročné, nakoľko jedným z rozhodujúcich a súčasne výrazne ovplyvňujúcich faktorov je motivácia prijímaných, ale aj súčasných zamestnancov v oblasti odmeňovania pri výkone práce vo verejnom záujme, keď vyššie príjmy v podnikateľskom sektore so zohľadnením stupňa spoločenskej požiadavky, vysokej odbornosti, náročnosti odvádzanej práce i regionalizácie výrazne ovplyvňujú rozhodovanie uchádzačov pri výbere budúceho zamestnávateľa. Táto skutočnosť negatívne ovplyvňuje reálne možnosti DataCentra pri včasnom dopĺňaní potrebného počtu kvalitných špecialistov nielen z oblasti informačnej bezpečnosti, informačných a komunikačných technológií, ale aj pri zabezpečovaní zamestnancov z oblasti ostatných podporných činností.

DataCentrum malo na rok 2017 rozpisom záväzných ukazovateľov štátneho rozpočtu Ministerstvom financií SR stanovený záväzný limit zamestnancov v počte 100 osôb.

Vykázaná skutočnosť v sledovanom období predstavuje v priemernom prepočítanom počte zamestnancov 100 osôb a v priemernom evidenčnom počte zamestnancov 101 osôb.

Skutočný evidenčný počet zamestnancov vo fyzických osobách ku dňu 31.12.2017 bol 101 zamestnancov, z toho 55 žien a 46 mužov. V tomto počte nie je započítaných šesť zamestnankýň vedených v mimo evidenčnom stave z dôvodu čerpania materskej a rodičovskej dovolenky. Prácu na kratší pracovný čas vykonávalo 5 zamestnancov.

V špecializovanom útvare CSIRT.SK bol na rok 2017 stanovený záväzný limit počtu zamestnancov 14 osôb. Vykázaná skutočnosť za hodnotené obdobie v priemernom prepočítanom počte zamestnancov je 9 osôb, priemernom evidenčnom počte zamestnancov 11 osôb, pričom fyzický stav zamestnancov k 31.12.2017 bol 10 osôb.

Zmena organizačnej štruktúry DataCentra v hodnotenom období nebola.

V roku 2017 v DataCentre *nastúpilo* 5 zamestnancov, prijatých z dôvodov opätovného obsadenia pracovných miest a *vystúpilo* 9 zamestnancov, pričom dôvody skončenia pracovného pomeru boli nasledovné:

- vzájomná dohoda na podnet zamestnanca z dôvodu:
  - zmeny zamestnávateľa v 4 prípadoch,
  - odchodu do starobného dôchodku v 1 prípade,
- výpoveď z pracovného pomeru daná zamestnancom z dôvodu odchodu do starobného dôchodku v 1 prípade,
- výpoveď z pracovného pomeru daná zamestnancom z dôvodu zmeny zamestnávateľa v 2 prípadoch.

Okrem toho v jednom prípade došlo k zániku pracovného pomeru z dôvodu úmrtia zamestnanca.

V priebehu roku 2017 mal stav zamestnancov mierne klesajúcu tendenciu, nakoľko sa nepodarilo zabezpečiť adekvátne náhrady za vystúpených zamestnancov a personálne obsadiť plánované pracovné miesta v špecializovanom útvare CSIRT.SK.

Zabezpečovanie kvalifikovaných odborníkov pri zvyšovaní stavu, resp. prijímaní zamestnancov DataCentra je aj naďalej problematické a náročné, nakoľko jedným z rozhodujúcich a súčasne výrazne ovplyvňujúcich faktorov je motivácia prijímaných, ale aj súčasných zamestnancov v oblasti odmeňovania pri výkone práce vo verejnom záujme, keď vyššie príjmy v podnikateľskom sektore so zohľadnením stupňa spoločenskej požiadavky, vysokej odbornosti, náročnosti odvádzanej práce i regionalizácie, výrazne ovplyvňujú rozhodovanie uchádzačov pri výbere budúceho zamestnávateľa. Táto skutočnosť negatívne ovplyvňuje reálne možnosti včasného doplnenia potrebného počtu kvalitných špecialistov nielen z oblasti informačnej bezpečnosti, informačných a komunikačných technológií, ale aj z oblasti ostatných podporných činností.

Kvalifikačná štruktúra zamestnancov k 31.12.2017 je nasledovná:

Vzdelanie	počet	v %
• vysokoškolské z toho: VŠ III. VŠ II. VŠ I.	59 3 51 5	58,42
• úplné stredné vzdelanie	37	36,63
• stredné odborné vzdelanie	5	4,95
Celkom	101	100,00

V hodnotenom období si kvalifikáciu zvyšovali:

- na I. stupni vysokoškolského vzdelania - 2 zamestnanci
- na II. stupni vysokoškolského vzdelania - 2 zamestnanci.

V špecializovanom útvare CSIRT.SK z celkového počtu 10 zamestnancov má k 31.12.2017 dosiahnuté vysokoškolské vzdelanie II. stupňa 8 zamestnancov a III. stupňa 2 zamestnanci.

Veková štruktúra zamestnancov DataCentra k 31.12. 2017 bola nasledovná:

Vekový interval	počet	v %
do 20 rokov	0	0,0
nad 20 do 30 rokov	12	11,88
nad 30 do 40 rokov	18	17,82
nad 40 do 50 rokov	21	20,80
nad 50 do 60 rokov	23	22,77
nad 60 rokov	27	26,73
S p o l u	101	100,00
Priemerný vek	48,5 roka	

V porovnaní s rokom 2016 priemerný vek zamestnancov DataCentra sa v sledovanom období zvýšil nepatrne o 0,3 roka, a to aj napriek posunu značnej časti zamestnancov do vyššieho vekového pásma. Priemerný vek zamestnancov špecializovaného útvaru CSIRT.SK v hodnotenom období dosiahol výšku 36,5 roka, čo je oproti roku 2016 zvýšenie o 1,5 roka.

Vzdelávanie, odborný rast a vedomostný rozvoj zamestnancov sú všeobecne považované za jeden z najdôležitejších nástrojov rozvoja organizácie a zvyšovania výkonnostného potenciálu zamestnancov. V hodnotenom období sa vzdelávanie zamestnancov DataCentra realizovalo na základe na Plánu vzdelávacích a školiacich aktivít pre rok 2017, v súlade s potrebami organizácie s dôrazom na priebežné prehlbovanie odborných vedomostí zamestnancov najmä v súvislosti s novými a rozvíjajúcimi sa kybernetickými hrozbami, v oblasti bezpečnosti cloudových riešení, administrácie a správy informačných systémov, informačnej

bezpečnosti a prevádzkovania dátových centier. Vzdelávanie bolo realizované aj zo zohľadnením niektorých individuálnych a neplánovaných požiadaviek.

Školiace aktivity boli smerované do nasledovných tematických okruhov:

1) získavanie nových poznatkov, prehĺbenie odborných znalostí a zručností v oblasti:
   - informačných a komunikačných technológií - 21 zamestnancov sa zúčastnilo na 9-tich špecializovaných kurzoch a seminároch v oblasti administrácie operačných systémov, databázového prostredia, bezpečnosti v oblasti IT, sieťových technológií, správy serverov, virtualizačných riešení a technológií a zálohovania,
   - manažérstva infraštruktúry - účasť 5 zamestnancov na 2 podujatiach,
   - správy, prevádzky a údržby dátových centier - účasť 3 zamestnancov na 1 podujatí,
   - informačnej bezpečnosti v špecifických oblastiach CSIRT.SK - ochrany kritickej informačnej infraštruktúry a bezpečnosti sietí, techník, postupov a nástrojov použiteľných pri riešení a testovaní incidentov v oblasti informačnej bezpečnosti - 33 účastí na 18 podujatiach,
   - procesnej bezpečnosti ISMS - 1 účasť na 1 podujatí,
   - štatistických metód a softvérových produktov na podporu rozhodovania - účasť 5 zamestnancov na I podujatí,
   - podporných a funkčných modulov RIS, správy služieb a riadenia podporných procesov - 13 účastí na 4 podujatiach,
   - stratégií a prístupov budovania informačnej spoločnosti - účasť 4 zamestnancov na 2 podujatiach;
2) aktualizácie a prehĺbenia odborných vedomostí a zručností z dôvodov zmien v príslušnej legislatíve v oblasti verejného obstarávania, pracovnoprávnych a mzdových predpisov, finančného účtovníctva - účasť 3 zamestnancov na 3 odborných seminároch;
3) cyklického preškolenia zamestnancov:
   - k zásadám informačnej bezpečnosti v DataCentre - 1 školenie organizované pre všetkých zamestnancov DataCentra,
   - k systému riadenia kvality ISO - 1 školenie organizované pre všetkých zamestnancov DataCentra,
   - z oblasti BOZP a OPP (zamestnanci a vedúci zamestnanci) - 3 školenia organizované pre všetkých zamestnancov DataCentra,
   - preškolenie z odbornej spôsobilosti podľa právnych predpisov - 3 účasti na 3 školeniach;
4) vstupné školenie pre novoprijatých zamestnancov - 5 účastí.

Okrem toho v roku 2017 v špecializovanom útvare CSIRT.SK priebežne prebiehalo interné vzdelávanie zamestnancov so zameraním predovšetkým na bezpečnostnú analýzu, praktické riešenie bezpečnostných incidentov a technické otázky informačnej bezpečnosti.

Odborné kurzy, tréningy, semináre a konferencie boli realizované prostredníctvom externých vzdelávacích inštitúcií, ako súčasť zmluvných dodávok technologických zariadení a služieb, partnerských organizácií v oblasti kybernetickej bezpečnosti na medzinárodnej úrovni a vlastnými vedúcimi zamestnancami DataCentra.

V hodnotenom období DataCentrum zabezpečilo pre zamestnancov celkom 51 vzdelávacích a školiacich aktivít. Externou formou absolvovalo 88 zamestnancov 43 vzdelávacích podujatí, z ktorých pre 39 účastníkov bolo 24 aktivít hradených z rozpočtových prostriedkov DataCentra. Z celkového počtu zamestnanci špecializovaného útvaru CSIRT.SK absolvovali 34 účastí na 19 externých vzdelávacích podujatiach a tréningoch. Pre 11 účastníkov bolo 8 odborných kurzov, praktických tréningov a účastí na konferenciách hradených z finančných prostriedkov NATO a partnerskými organizáciami CSERT.

V prepočte na priemerný evidenčný počet zamestnanci DataCentra v roku 2017 absolvovali v rámci externých a interných vzdelávacích aktivít v priemere 22,5 hodín vzdelávania na 1 osobu, čo predstavuje 3 osobodní. Z rozpočtových zdrojov na zrealizované vzdelávacie aktivity v roku 2017 boli vynaložené prostriedky v celkovej finančnej čiastke 63 545,58 €. K navýšeniu výdavkov oproti minulému roku došlo z dôvodu nutnosti absolvovania špecifických odborných školení zamestnancami špecializovaného útvaru CSIRT.SK zameraných na plnenie úloh obrany voči pokročilým kybernetickým hrozbám. Priemerný výdavok na vzdelávanie 1 zamestnanca DataCentra tak predstavoval celkom 529,20 € za hodnotené obdobie.

Okrem plnenia úloh kontrahovaných na rok 2017 zamestnanci DataCentra v rámci roku 2017 vykonávali administratívne práce a podporné činnosti v rozsahu 32 089 hodín, metodické a koncepčné práce v rozsahu 2 158 hodín, 2 501,5 hodín bolo čerpaných na riadiace a koordinačné činnosti, a práce súvisiace s kontrolnou činnosťou si vyžiadali celkom 1 966 hodín. Študijným a vzdelávacím aktivitám (vrátane samoštúdia a štúdia projektovej dokumentácie) sa venovali zamestnanci celkom 3 314 hodín, z toho zamestnanci špecializovaného útvaru CSIRT.SK 2 422 hodín. Kontrolné aktivity boli vykonané v rozsahu 1 966 hodín.

Celkové plnenie úloh kontrahovaných na rok 2017 možno hodnotiť ako veľmi dobré, zodpovedné a často aj nad rámec úrovne podmienok, ktoré boli determinované počtom kvalifikovaných zamestnancov a dostatku pridelených finančných prostriedkov. Percentuálne plnenie úloh, t.j. skutočné čerpanie kapacít je 169 303,5 hodín - t.j. 96,70 % a plne zodpovedá tomu, ako boli disponibilné kapacity skutočne využité v záujme zabezpečenia splnenia jednotlivých úloh. Pri započítaní času, ktorý zamestnanci venovali aj odbornému vzdelávaniu a zvyšovaniu odborných zručností, je celkové plnenie na úrovni 98,59 %.

Pôvodný rozpis rozpočtu na rok 2017 bol dodatkami ku Kontraktu na rok 2017 uzatvoreného medzi MF SR a DataCentrom upravený vo výške schváleného rozpočtového opatrenia so súhlasom Ministerstva financií SR - Dodatkom č.1 k 30.06.2017 a Dodatkom č.2 k 31.12.2017.

Čerpanie rozpočtu DataCentra - skutočnosť k 31.12.2017, je uvedené v ***Prílohe č. 1*** tejto správy.

Čerpanie kapacít DataCentra k 31.12.2017, plánovaných na plnenie úloh kontrahovaných pre rok 2017, je uvedené v ***Prílohe č. 2*** tejto správy.

Plnenie úloh DataCentra za rok 2017

111	Bezpečnosť informačných systémov DataCentra

Činnosti súvisiace s Bezpečnostným projektom IS v DataCentre v roku 2017 pozostávali z aktivít týkajúcich sa koordinácie procesov riadenia informačnej bezpečnosti v DataCentre, dodržiavaním legislatívy a právnych predpisov v oblasti BIS, ale aj identifikáciou nových bezpečnostných rizík a podpory pri ich riešení.

Pre oblasť bezpečnosti IS sa uskutočnili tieto aktivity:

- zabezpečovanie prevádzky bezpečnostných systémov a mechanizmov v gescii útvaru bezpečnosti (SKV, PTV, EPS, SHZ, EZP, BP, THAS),
- aktualizácia bezpečnostnej dokumentácie (Bezpečnostný projekt DataCentra, organizačné smernice),
- testovanie havarijných plánov ISUF, ITMS, KTI2, RIS, IS DC,
- aktualizácia plánov obnovy pre IS DC, ITMS, KTI2, RIS, IS DC.

Na základe analýzy rizík IS prevádzkovaných v DC a bezpečnostných auditov bola zabezpečená podpora pri implementácii bezpečnostných opatrení v súlade s bezpečnostnými požiadavkami výnosu MF SR o štandardoch pre IS verejnej správy, s požiadavkami zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 84/2014 Z. z (ďalej len „ zákon o ochrane osobných údajov“ - ZOOÚ) a ostatnou legislatívou súvisiacou s informačnou bezpečnosťou. Vzhľadom k dosiahnutiu súladu s nariadením GDPR bola vypracovaná rozdielová analýza súčasného stavu spracúvania osobných údajov voči požiadavkám nariadenia GDPR.

V rámci výkonu dohľadu nad ochranou osobných údajov sa poskytovali konzultácie, ohľadne zabezpečovania súladu s požiadavkami ZOOÚ jednotlivým organizačným útvarom DataCentra, ako aj ostatným organizáciám, ktorých systémy sú prevádzkované v DataCentre.

Nahlasovanie, evidencia a riešenie bezpečnostných incidentov v HP Service Manager prebieha v zmysle organizačných smerníc DataCentra.

Boli uskutočnené aktuálne školenia informačnej bezpečnosti zamestnancov a Phishingové testovanie v spolupráci s oddelením CSIRT.SK s cieľom zlepšiť dostatočnú úroveň bezpečnostného povedomia interných a externých zamestnancov DataCentra.

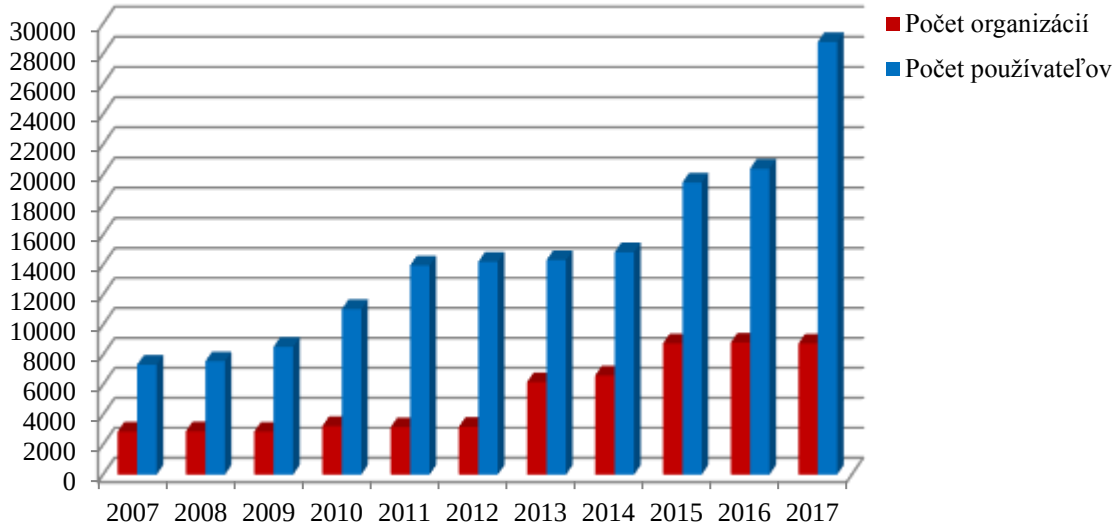
121	Centrum podpory užívateľov - CPU

V roku 2017 bol Centrom podpory používateľov (CPU) vykonaný komplex činností v prospech používateľov informačných systémov prevádzkovaných DataCentrom pre rezort Ministerstva financií SR.

CPU riešilo požiadavky zo strany organizácií a používateľov informačných systémov na aplikačnú, metodickú a technickú podporu a priebežne budovalo a dopĺňalo databázu často kladených otázok. Súčasne bola priebežne aktualizovaná databáza organizácií a používateľov pripojených k informačným systémom. Zmeny súviseli najmä s uvedením do prevádzky nových IS, prípadne ich modulov a so zánikom, vznikom a zlučovaním organizácií, respektíve s ich preradením pod iného zriaďovateľa a tiež zmenou právnej formy. Pribudli používatelia informačného systému RIS-SAM (Rozpočtový informačný systém pre samosprávy) – organizácie v zriaďovateľskej pôsobnosti obcí.

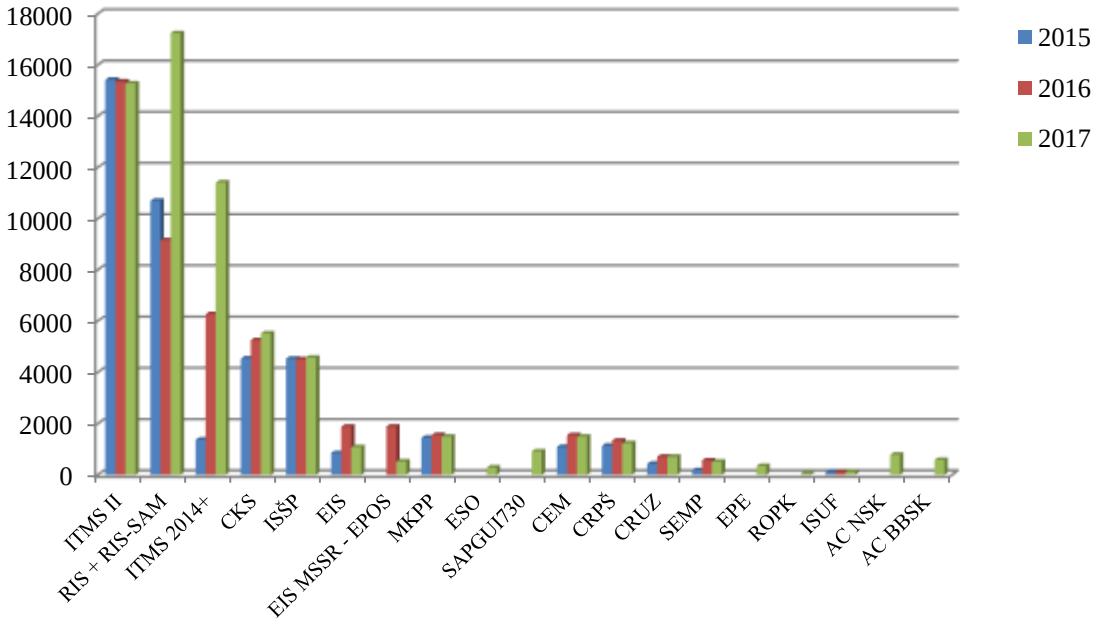
Počet organizácií používajúcich aspoň jeden informačný systém prevádzkovaný DataCentrom bol 8 755. Počet používateľov s aktívnym prístupom do infraštruktúry informačno-komunikačných technológií prevádzkovaných DataCentrom bol 28 787.

Zmena počtu organizácií a používateľov v porovnaní s predchádzajúcimi rokmi:



CPU eviduje pre jednotlivé služby nasledujúce počty používateľov (k 31.12.2017):

- 4 569 používateľov IS SŠP (Informačný systém systému štátnej pokladnice),
- 17 237 používateľov RIS (Rozpočtový informačný systém), z toho hlavne
  - 5 032 používateľov RIS (Rozpočtový informačný systém pre štátnu a verejnú správu)
  - 12 005 používateľov RIS-SAM (Rozpočtový informačný systém pre samosprávu)
  - cca 200 používateľov ostatných modulov RIS.
- 5 521 používateľov CKS (Centrálny konsolidačný systém),
- 15 282 používateľov ITMS II. (monitorovací systém účtovníctva fondov); z toho ITMS-core 1 739 a ITMS-portál 13 543 používateľom,
- 11 413 používateľov ITMS 2014+ (IT monitorovací systém pre Európske štrukturálne a investičné fondy pre programové obdobie 2014 až 2020); z toho neverejná časť 2 046 a neverejná časť 9 367,
- 111 používateľov ISUF (informačný systém účtovníctva fondov),
- 1 595 používateľov EIS - EPOS (ekonomické informačné systémy ministerstiev),
- 1 491 používateľov MKPP (multiklientsky platobný portál),
- 701 používateľov CRUZ (centrálny register účtovných závierok – neverejná časť)
- 512 používateľov SEMP (informačný systém Evidencia a monitoring štátnej pomoci),
- 1 486 používateľov CEM (informačný systém Centrálna evidencia majetku)
- 1 228 používateľov CRPŠ (Centrálny register pohľadávok štátu).



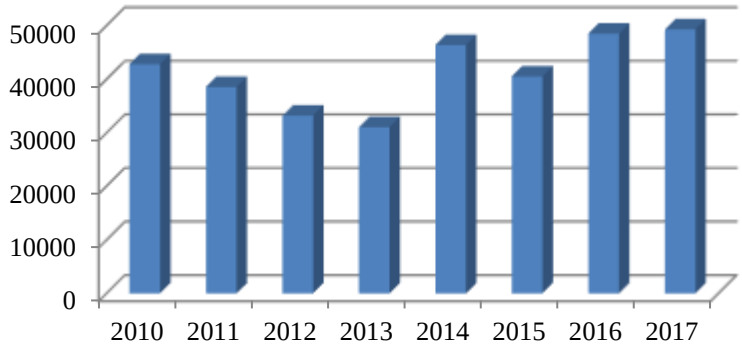
V priebehu roku 2017 používatelia kontaktovali CPU 49 305 krát, z toho:

- vykonali 32 380 telefonických volaní do CPU, čo predstavuje priemer 5 393 mesačne a 1 245 volaní týždenne,
- poslali 10 696 e-mailov s požiadavkou na službu CPU,
- cez internetové rozhranie vytvorili 1 883 požiadaviek na službu CPU,
- osobne predložili 1 214 požiadaviek,
- poštou poslali 3 132 požiadaviek,

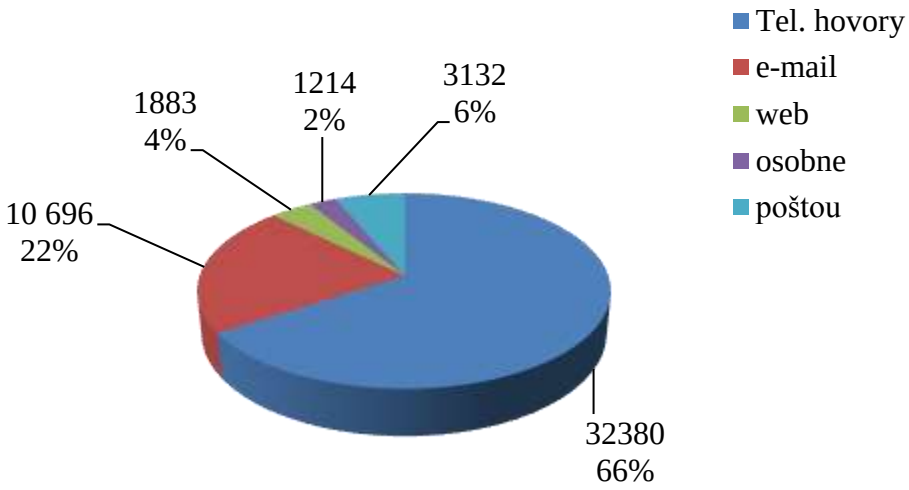
Počet kontaktovaní CPU v porovnaní s predchádzajúcimi rokmi:

2010	2011	2012	2013	2014	2015	2016	2017
42816	38550	33193	31040	46372	40456	48524	**49305**

V grafickom vyjadrení:



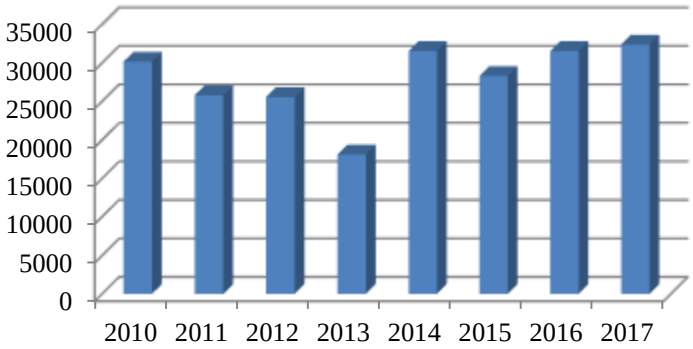
Typ kontaktov na CPU:



Počet telefonických volaní na CPU v porovnaní s predchádzajúcimi rokmi:

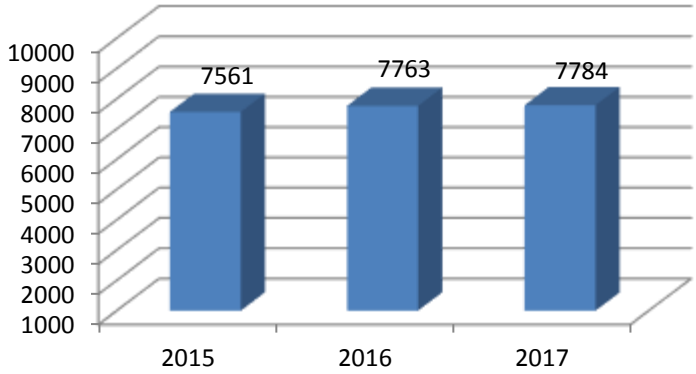
2010	2011	2012	2013	2014	2015	2016	2017
30155	25799	25558	18101	31543	28302	31543	**32380**

V grafickom vyjadrení:



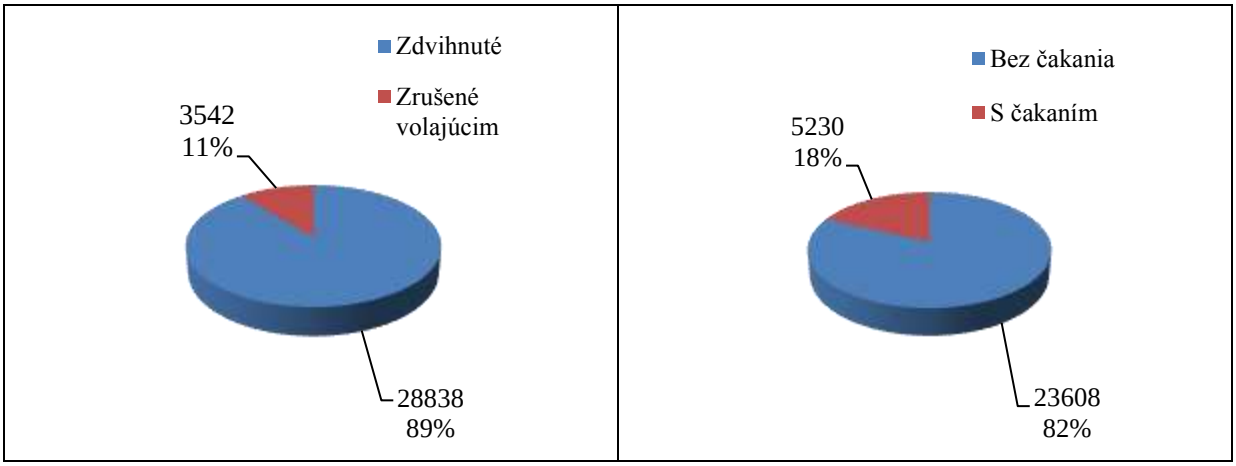
CPU v roku 2017 odoslalo používateľom 7 784 listových zásielok.

V porovnaní s predchádzajúcimi rokmi:



V hodnotenom období bolo zaregistrovaných 32 380 telefonických volaní do CPU.

Z toho bolo 28 838 volaní zdvihnutých (89,1 %) a 3 542 (10,9 %) bolo zrušených volajúcim. Z počtu zdvihnutých volaní bolo zdvihnutých bez čakania 23 608 (81,9%) a 5 230 (18,1%) volaní bolo zdvihnutých s čakaním, čo je graficky vyjadrené nasledovne:



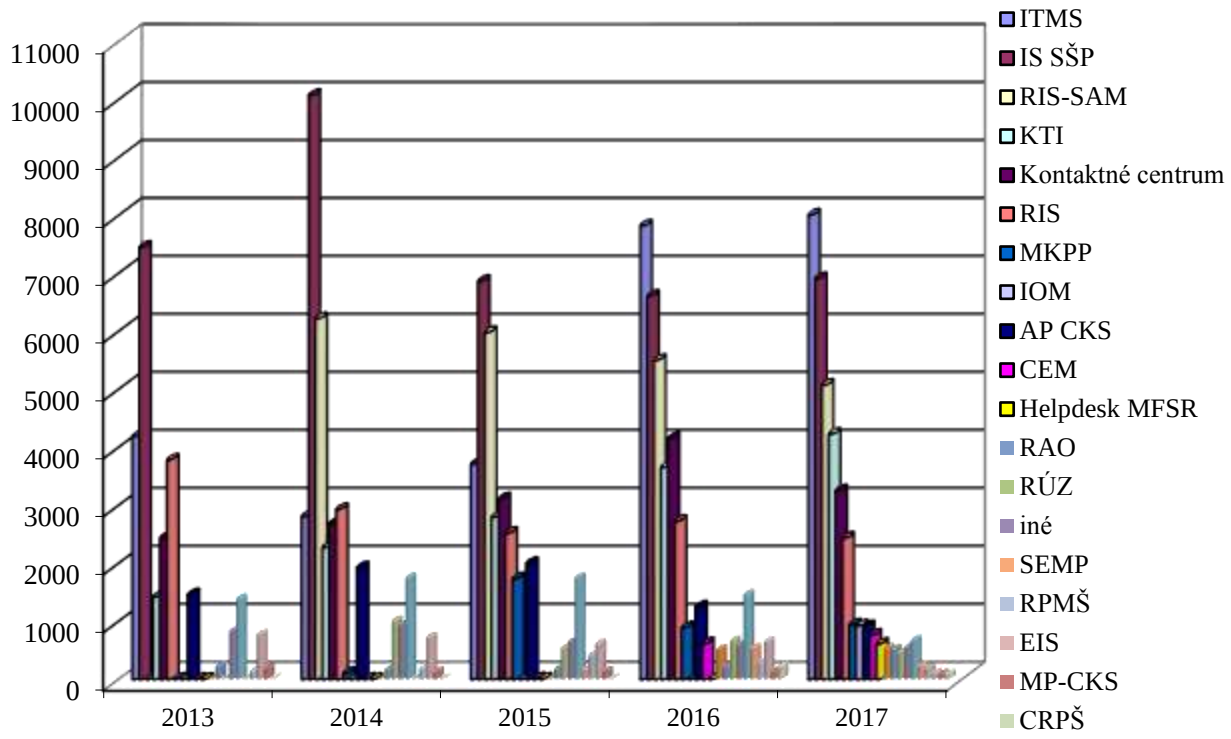
Počet hlásení uzatvorených jednotlivými pracovným skupinami riešiteľov v porovnaní s predchádzajúcimi rokmi:

Rok	2010	2011	2012	2013	2014	2015	2016	2017	%
ITMS	11056	7200	3294	4189	2808	3711	7822	8008	21,4
IS SŠP	10381	8717	7824	7452	10073	6863	6609	6911	18,5
RIS-SAM	*	*	*	*	6219	5979	5500	5073	13,6
KTI	2678	3059	1781	1421	2274	2797	3654	4226	11,3
Kontaktné centrum	5846	5802	4592	2434	2683	3112	4153	3250	8,7
RIS	6274	4893	3752	3782	2929	2518	2725	2436	6,5
MKPP	*	*	*	*	100	1733	889	936	2,5
IOM	*	*	*	*	*	*	*	922	2,5
AP CKS	1721	2421	2006	1456	1921	1998	1246	906	2,4
CEM	*	*	*	*	*	10	615	761	2,0
Helpdesk MFSR	*	*	*	*	*	*	*	606	1,6
CSRU	*	*	*	*	*	*	505	526	1,4
RAO	2152	1762	2201	211	159	165	208	506	1,4
RÚZ	*	*	*	*	1000	531	656	445	1,2
iné	1206	817	1376	822	927	638	579	539	1,4
ISUF	849	704	677	1382	1746	1747	1452	666	1,8
SEMP	*	*	*	*	*	153	529	214	0,6

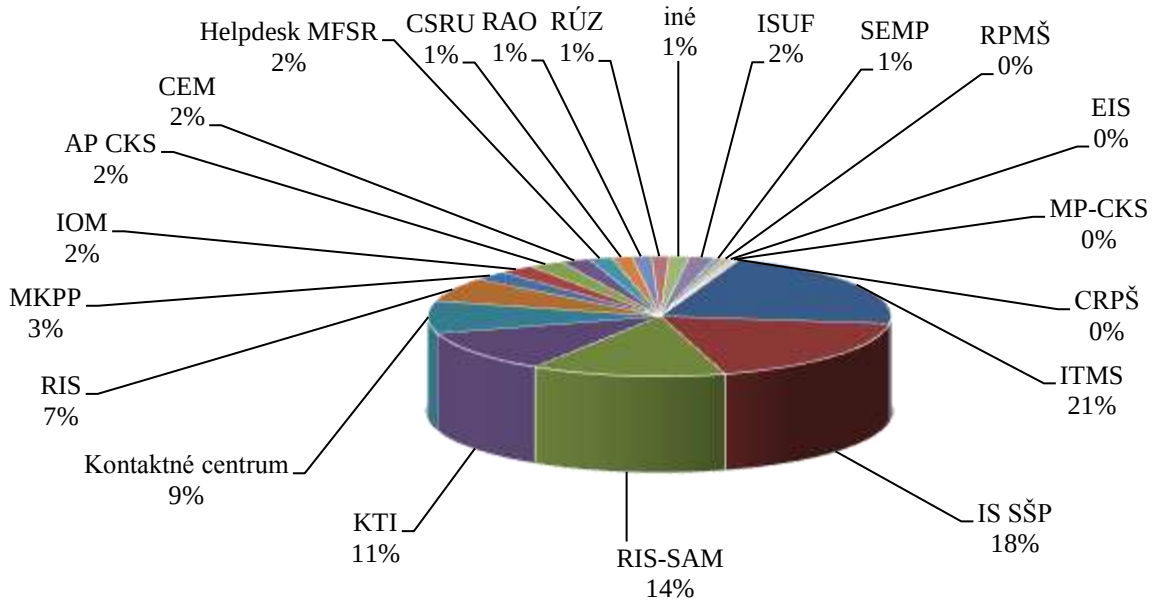
RPMŠ	71	118	148	129	169	413	268	183	0,5
EIS	491	412	797	769	718	606	641	93	0,2
MP-CKS	91	329	245	185	122	126	123	84	0,2
CRPŠ	*	*	*	*	*	*	209	79	0,2
Spolu	42 816	36 234	28 693	24 232	33 848	33 100	38 383	**37 370**	**100**

* / údaje nie sú k dispozícii

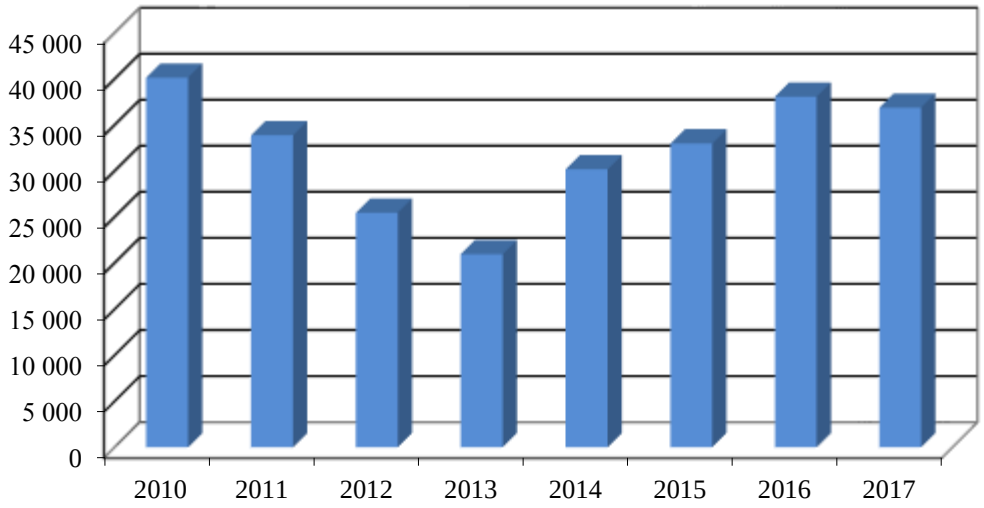
V grafickom vyjadrení počet hlásení uzatvorených jednotlivými pracovnými skupinami v porovnaní s predchádzajúcimi rokmi:



a v grafickom - percentuálnom vyjadrení:



Porovnanie počtu uzatvorených hlásení celkom s predchádzajúcimi rokmi v grafickom vyjadrení:



CPU aktívne prispieva k plneniu podmienok certifikátu kvality poskytovania služieb ISO 9001:2008, participuje na realizácii projektov Problem Management, Incident Management, Change Managment a Acces & Identity Management.

Poznámka:
CPU poskytuje služby podpory používateľom trojúrovňovo.
1. úroveň - kontaktné centrum – ide o komunikáciu s používateľmi, prijatie dopytu na službu, jeho zatriedenie, bližšie špecifikovanie, riešenie jednoduchších alebo často sa opakujúcich požiadaviek a postúpenie požiadaviek na 2.úroveň (poskytovateľ podpory: DataCentrum)
2. úroveň - aplikačná a technická podpora používateľov – ide o riešenie požiadaviek a problémov používateľov s funkcionalitou IS, s dostupnosťou IS cez komunikačno-technologickú infraštruktúru, správu používateľských oprávnení a technickú podpora HW a SW vybavenia u používateľa a postúpenie požiadaviek na 3. úroveň. (Poskytovateľ podpory: DataCentrum)

3. úroveň - metodická a systémová podpora - poskytuje ju metodik/garant vlastníka IS, resp. dodávateľ/riešiteľ IS – ide o riešenie a zodpovedanie metodických otázok, vývoj a aktualizácia IS na základe požiadaviek z praxe, požiadaviek vlastníka IS, prípadne zmeny legislatívneho prostredia.

122	Podpora používateľov informačného systému CKS

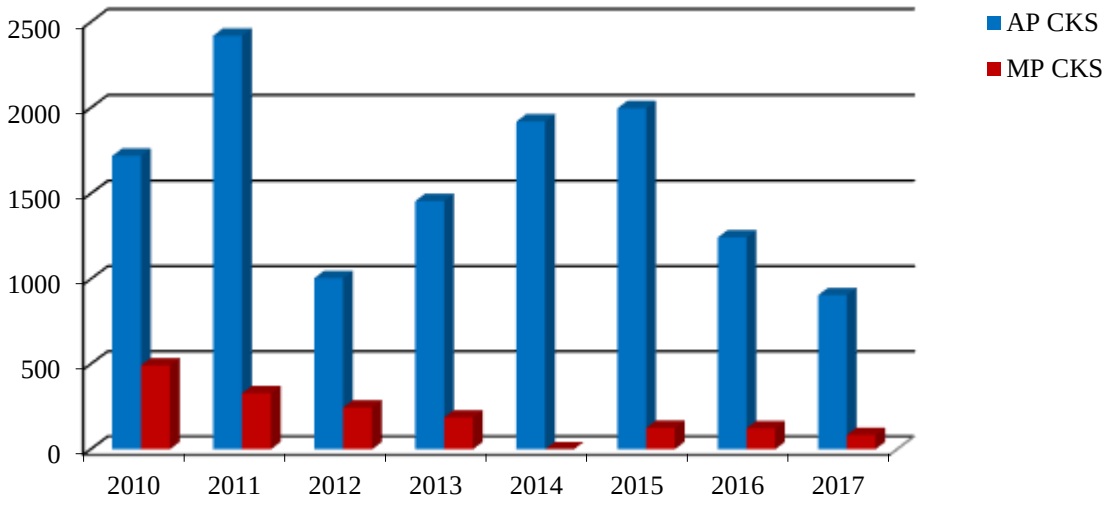
Pri plnení úlohy DataCentrum v hodnotenom období zabezpečovalo pomoc používateľom pri používaní Informačného systému Centrálny konsolidačný systém - CKS (Pozn.: v predošlých rokoch IS JÚŠ) pre účely konsolidácie a odsúhlasovania vzájomných vzťahov, pri odhaľovaní chýb a komplikácií v praktickej aplikácii a pri zbieraní a odovzdávaní námetov na ďalší rozvoj tohto systému vrátane metodickej podpory účtovníctva a konsolidácie. Súčasne boli plnené úlohy prislúchajúce technickému zabezpečeniu prevádzky systému.

Celkový počet hlásení týkajúcich sa aplikačnej a metodickej podpory IS CKS je v porovnaní s predchádzajúcim obdobím nasledovný:

Rok	2010	2011	2012	2013	2014	2015	2016	2017
AP CKS	1721	2421	2006	1457	1921	1998	1246	906
MP CKS	493	329	245	187	122	126	123	84

(Pozn.: AP – aplikačná podpora, MP – metodická podpora)

V grafickom vyjadrení:



151	Certifikácia DataCentra podľa normy EN ISO 9001

V roku 2017 DataCentrum udržiavalo a skvalitňovalo systém riadenia kvality podľa medzinárodnej normy systému riadenia kvality EN ISO 9001 : 2015. Všetky úlohy DataCentra vyplývajúce z uzavretého kontraktu pre rok 2017 boli splnené.

Priebežne počas roku 2017 DataCentrum na úseku riadenia kvality plnilo hlavne nasledujúce úlohy:

- bol udržiavaný a zlepšovaný systému manažérstva kvality,
- priebežne bola aktualizovaná interná riadená dokumentácia a zoznam externej riadenej dokumentácie:
  - aktualizovaných, alebo novo prijatých smerníc - 14
  - aktualizovaných, alebo novo prijatých pracovných postupov - 15
  - aktualizovaných, alebo novo prijatých formulárov - 43
- v novembri 2017 boli realizované interné audity interným audítorom a externým audítorom, na základe ktorých bolo prijaté 2 nápravné opatrenia, tiež v decembri 2017 bol realizovaný externý kontrolný audit zavedeného systému riadenia kvality externou spoločnosťou. Neboli zistené žiadne nezhody a DataCentrum obhájilo certifikát ISO 9001 na ďalší rok.

Stanovené hodnotiace kritériá úlohy - úspešné absolvovanie Kontrolného auditu, odstraňovanie zistených nedostatkov a zlepšovanie systému riadenia kvality - boli splnené.

Všetka interná riadená dokumentácia (príkazy riaditeľa, smernice, pracovné postupy a formuláre, nápravné a preventívne opatrenia, výsledky interných auditov) sú dostupné všetkým zamestnancom DataCentra na intranete, resp. ako kriteriálne výtlačky vo fyzickej podobe u manažéra kvality v DataCentre.

161	Centrum monitorovania prevádzky - CMP

Útvar CMP vykonáva monitorovanie/zisťovanie a prideľovanie kritických incidentov na riešenie riešiteľom a riešiteľským skupinám, následne sledovanie ich vyriešenia a ich uzavretia v systéme HP Service Manager.

Útvar CMP na požiadanie poskytuje používateľom informačných systémov sumárne informácie o kritických incidentoch, ktoré sa vyskytli na monitorovaných informačných systémoch prevádzkovaných v DataCentre za definované obdobie.

Zaradeniu nového informačného systému do monitorovania v DataCentre predchádza analýza a špecifikácia jeho stavov, ktoré budú monitorované.

V štandardnej procedúre kritické incidenty zistené monitorovacím systémom operátor CMP pridelí riešiteľom na riešenie. Incidenty, ktoré nie sú zistené automaticky, operátor CMP manuálne zaznamenáva v HP Service Manageri a informáciu o nich postupuje dodávateľovi monitorovacieho systému prostredníctvom jeho HelpDesku s cieľom doplnenia riešiteľov a štandardizácie procesov ich riešenia.

Riešenie incidentov, ktoré pridelí operátor CMP na riešenie riešiteľom sú vykonávané v úzkej spolupráci s pracovníkmi Konzoly 1 a Konzoly 2.

Celkový proces spracovania incidentov t.j. prideľovanie incidentov operátorom CMP riešiteľovi, následná notifikácia riešiteľa o incidentoch, sledovanie riešenia incidentov a po ich vyriešení ich uzavretie v HP Service Manageri, vedie ku korelácii kvality služieb dodávateľov v zmysle platných SLA.

Útvar CMP pracuje v nepretržitej prevádzke 24x7. Počas roka 2017 neboli realizované žiadne zmeny funkcionality monitorovacieho systému, ktoré by si vyžadovali zaškolenie operátorov.

Útvar CMP zabezpečuje aj ďalšie aktivity

- spracovanie uzávierok IS SŠP,
- kontrolu komunikačných kanálov pre IS SŠP,
- dohľad nad bezpečnosťou priestorov, v ktorých sú prevádzkované IS a KTI a v ktorých pracujú zamestnanci externých firiem
- dohľad nad podpornou infraštruktúrou (klimatizácie, EPS, zdroje el. energie. atď.) informačných systémov prevádzkovaných v DataCentre.

Riešenia neštandardných situácií sú podmetom na úpravy pracovných postupov s cieľom zlepšenia poskytovania komplexných informácií o monitorovaných systémoch, čo je východisko pre skvalitňovanie činností a upevňovanie postavenia a funkcie monitorovacieho centra CMP.

Útvar CMP plnil úlohy priebežne v nepretržitej prevádzke 7 dní x 24 hod. s využitím interných a externých zamestnancov. Všetky kritické incidenty, ktoré sa vyskytli na monitorovaných systémoch postúpilo CMP na riešenie.

Kvalita prác CMP bola vykonávaná v zmysle záväzkov definovaných v platných SLA.

201	Register účtovných závierok (RÚZ)

DataCentrum aj v roku 2017, ako prevádzkovateľ Registra účtovných závierok, v zmysle § 23c zákona č.431/2002 Z. z. o účtovníctve v znení neskorších predpisov a v súlade so zákonom č.145/1995 Z.z. o správnom konaní, vydávalo na základe doručenej žiadosti overené kópie dokumentov alebo časti dokumentov, ktoré sú uložené v Registri účtovných závierok.

Žiadateľ - účtovná jednotka alebo fyzická osoba, môže o kópiu dokumentu alebo časti dokumentu požiadať na základe písomnej žiadosti zaslanej doporučene poštou alebo doručenej osobne do podateľne RÚZ. Zamestnanci podateľne RÚZ, okrem vydávania výstupov z registra, poskytujú poradenstvo telefonicky, mailom alebo osobne aj v otázkach súvisiacich s ukladaním, zverejňovaním a vydávaním výstupov z RÚZ.

K 1. januáru 2016 nadobudol účinnosť zákon č. 333/2014 Z.z., ktorým sa mení a dopĺňa zákon č.595/2013 Z.z. o dani z príjmov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony. Zmeny, ktoré priniesol, ovplyvnili zavedené procesy a boli zapracované do pracovných postupov a prevádzky pracoviska RÚZ.

V nadväznosti na uzatvorenú medzi MF SR a Slovenskou poštou a zmluvou DataCentra o umiestnení, prevádzkovaní technického vybavenia a o zapojení do systému centrálnej evidencie poplatkov e-Kolok boli zabezpečované aj v roku 2017 technologické i procesné podmienky súvisiace s prevádzkou tzv. softvérovej pokladne, ktorá umožňuje zamestnancom prijímať a evidovať úhrady za poplatky v centrálnom systéme evidencie. Všetky požiadavky klientov hlásené cez CPU boli zaznamenané v Service Manageri (445) boli vyriešené v stanovenom termíne a v súlade s požiadavkami SLA - t.j. bolo poskytnuté poradenstvo na telefonickej alebo e-mailovej úrovni, prípadne bola zabezpečená druhá úroveň podpory.

V roku 2017, bolo vybavených celkom 173 žiadostí o poskytnutie údajov z registra účtovných závierok. Z tohoto počtu bolo osobne podaných a vybavených 109 žiadostí, poštou bolo doručených 44 žiadostí, z toho 51 žiadostí bolo vybavených bezplatne. V prípade osobného podania žiadosti a úhrady správneho poplatku v hotovosti alebo na základe potvrdenia pre evidenciu poplatku bol výstup vydávaný na počkanie.

Z celkového počtu zaregistrovaných žiadostí bolo po konzultácii s klientom 20 žiadostí dovybavených na okresnej úrovni.

V prípadoch, kedy nebolo možné žiadosť vybaviť hneď, nakoľko sa požadovaný dokument v registri nenachádzal, bolo potrebné zabezpečiť nápravu v spolupráci s Finančným riaditeľstvom v Banskej Bystrici, ktoré muselo zabezpečiť následné doplnenie a zverejnenie chýbajúcich dokumentov. V takýchto prípadoch je poverený zamestnanec podateľne RUZ kompetentný vydať potvrdenie o tom, že požadovaný dokument sa v registri nenachádza a postúpiť problém na riešenie správcovi registra RÚZ, prípadne ho uzavrieť až po doplnení dát v databáze registra.

V hodnotenom období neboli zaznamenané žiadne problémy s dostupnosťou a funkčnosťou Registra účtovných závierok.

202	Konzultačné služby pre odbor informačných technológií MF SR

V roku 2017 boli v rámci úlohy zo strany DataCentra riešené a zabezpečované nasledovné činnosti:

- poskytovali sme súčinnosť pri delimitácií kompetencií vo vzťahu k zabezpečeniu prevádzky Vládneho cloudu na Ministerstvo vnútra SR,
- uskutočnili sa pracovné stretnutia k zákonu o hazardných hrách a k vytvoreniu z neho vyplývajúceho registra vylúčených hráčov,
- poskytovali sme konzultácie k problematike blokovania zakázaných ponúk v zmysle uplatňovania zákona o hazardných hrách,
- poskytovali sme odbornú pomoc pri migrácií informačných systémov iných rezortov do Vládneho cloudu,
- poskytovali sme konzultácie pri realizácií podpory používateľov pre IS IOM.

211	IT monitorovací systém pre štrukturálne fondy a Kohézny fond pre programové obdobie 2007 - 2013 (ITMS II)

DataCentrum počas roku 2017 zabezpečovalo nasledovné činnosti súvisiace s prevádzkou ITMS Core a ITMS Portál:

1. Správa a prevádzka systému

DataCentrum, v spolupráci s dodávateľom ITMS II, zabezpečovalo prevádzkovanie a spravovanie produkčného, školiaceho a cvičného systému ITMS Core a ITMS Portál, zabezpečovalo technickú podporu pre systém a bežnú údržbu aplikačných systémov.

Aplikácia ITMS Core a ITMS Portál pracuje pod OS Linux. Aplikácia využíva ako fyzické servery len databázové servery a report server, všetky ostatné serverové komponenty architektúry sú realizované ako virtuálne servery.

Aplikácia ITMS II pracuje nad zjednotenou databázou pre verejnú aj neverejnú časť ITMS II, ktorá je umiestnená v rámci komunikačno-technologickej infraštruktúry DataCenta (KTI). K 31.12.2017 je v produkčnej prevádzke ITMS Core a ITMS Portál verzia 2.16.25.

Počas roku 2017 DataCentrum realizovalo činnosti vedúce ku skvalitneniu poskytovaných služieb aj pre ITMS II, ako aj na odstránenie nedostatkov zistených vládnymi auditmi ITMSII. Jednalo sa o nasledovné činnosti:

- realizácia nákupu podpory licencií mailového systému,
- realizácia nákupu podpory CITRIX licencii,
- realizácia nákupu podpory na VMware licencie,
- realizácia nákupu podpory na Symantec licencie,
- realizácia nákupu podpory na AUTOCAD licencie,
- realizácia nákupu podpory RED HAT produktov,
- realizácia nákupu licencií ESET,
- príprava a nákup Windows server a Windows Remote Desktop licencií,
- realizácia upgradu prostredia KTI,
- príprava a realizácia riešenia pre vzdialený administrátorský prístup,
- migrácia na nový systém SK-NIC,
- príprava redizajnu monitoringu počítačovej sály,
- rozšírenie kapacity diskového poľa,
- príprava migrácie zálohovacieho systému.

Počas sledovaného obdobia boli pravidelne dopĺňané údaje týkajúce sa ITMS II do konfiguračnej databázy, pravidelne sa vykonávala aj aktualizácia (patchovanie) operačného systému pre ITMS II.

Na firemnom projektovom portáli Atosu, ku ktorému má prístup projektový manažér DataCentra, je vykazované detailné plnenie úloh dodávateľa.

Pomocou nástroja CyberArk sa monitorovali aktivity/logy pracovníkov s pridelenými administrátorskými oprávneniami pre ITMS II.

Zamestnanci DataCentra vykonávali v hodnotenom období administráciu časti produkčného a cvičného systému ITMS Core a ITMS Portál - modulu Administrátorské nástroje - Správa orgánov a užívateľov, Správa priradenia užívateľských rolí, Správa rolí orgánu, Správa užívateľských rolí orgánu, Správu žiadostí o Konto Portál a Bezpečnostné nastavenia, a na základe žiadostí vykonávali aj úpravy v časti Správa subjektov.

Počas celej doby prevádzky ITMS Core a ITMS Portál boli dodržiavané všetky bezpečnostné opatrenia vyplývajúce z požiadaviek na bezpečnosť systému.

Dňa 26.12.2017 sa uskutočnilo pravidelné testovanie obnovy systému ITMS zo zálohy, pričom bola verifikovaná autentickosť a integrita archívu. Obnova dát zo zálohy prebehla úspešne.

ITMS Core a ITMS Portál sú začlenené do centrálneho monitoringu prevádzky v DataCentre, v rámci ktorého je nad systémom ITMS Core a ITMS Portál uskutočňovaný základný monitorig, ktorý sa zrealizuje pomocou nástroja BAC, a to spustením Žiadosti o aktiváciu pre ITMS Portál a prihlásením sa do aplikácie pre ITMS Core. Počas sledovaného obdobia neboli centrálnym monitoringom zaznamenané väčšie nedostupnosti systému ITMS Core a ITMS Portál, okrem nedostupnosti počas pravidelnej údržby systému ITMS a počas nasadzovania nových buildov pre systém ITMS. Dostupnosť produkčného systému ITMS Core a ITMS Portál bola v hodnotenom období 100 %.

2. Užívateľská, aplikačná, technická, technologická podpora a monitoring

Cieľom úlohy je zabezpečovať pomoc užívateľom pri práci s aplikáciou ITMS Core a ITMS Portál. DataCentrum počas roku 2017 poskytovalo 1. úroveň podpory, 2. úroveň podpory (aplikačnú, technickú a technologickú podporu) bola poskytovaná v spolupráci s dodávateľom ITMS.

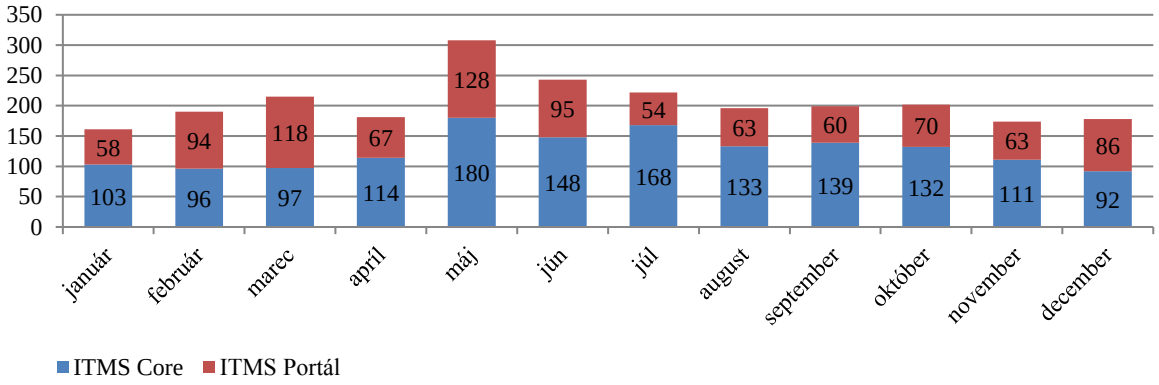
Všetky problémy užívateľov pri práci so systémom ITMS Core alebo ITMS Portál, hlásené prostredníctvom telefónu, e-mailu, alebo web rozhraním boli zaznamenané v aplikácii HP ServiceManager a riešené pracovníkmi 2. úrovne podpory.

Hlásenia zaznamenané v aplikácii HP ServiceManager boli vyriešené v stanovenom termíne podľa SLA.

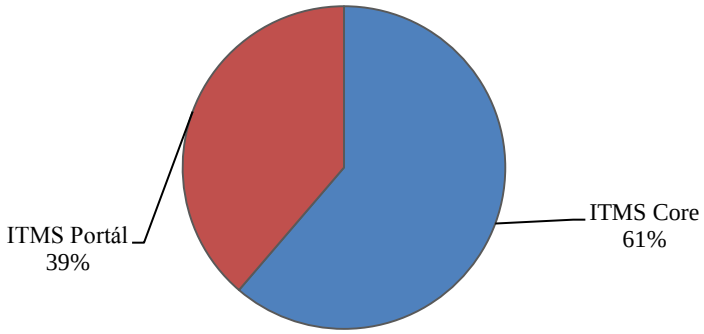
V sledovanom období bolo vyriešených 1 513 hlásení užívateľov pre ITMS Core a 956 hlásení užívateľov ITMS Portál. Prevažná časť hlásení sa týkala problémov s prihlásením sa do systému ITMS Core aj ITMS Portál (zabudnuté prihlasovacie údaje, strata Grid karty) a problémov pri vytváraní MS pri práci v inom prehliadači ako IE v 7.0 a vyššia.

Aplikačná podpora pre ITMS bola poskytovaná permanentne počas pracovných dní v čase od 8^{00} do 17^{00}, a v prípade mimoriadnych situácií aj mimo uvedených hodín.

Počet zaznamenaných a vyriešených hlásení užívateľov systému ITMS v roku 2017



Percentuálne zobrazenie vyriešených hlásení užívateľov systému ITMS v roku 2017



3. Koordinácia prác v procese zabezpečenia pripájania nových koncových bodov do KTI pre potreby ITMS

V procese zabezpečovania pripájania nových koncových bodov do KTI pre ITMS prebehla po centralizácii požiadaviek na pripojenie nových koncových bodov do KTI, analýza možností ich pripojenia a v spolupráci s útvarom CPU boli tieto pripojenia do KTI zrealizované.

4. Zabezpečovanie prístupov pre užívateľov systému

ITMS Core:

Úlohou DataCentra bol zber, registrácia, kontrola písomnej formy žiadosti o prístup pre užívateľov ITMS Core s elektronickou formou, a archivácia žiadostí o prístup. Zároveň DataCentrum zabezpečovalo a zriaďovalo prístup do produkčného systému ITMS

Core pre užívateľov na základe schválených žiadostí. Ku koncu sledovaného obdobia bolo v ITMS Core 1739 aktívnych užívateľov, z toho za sledované obdobie bolo spracovaných 195 nových žiadostí o prístup do ITMS Core, 54 užívateľských prístupov bolo aktualizovaných a 312 užívateľských účtov bolo zrušených (zablokovaných).

Zároveň boli vytvárané potrebné prístupy na základe poverenia pre administrátora na rezortoch a ich zástupcov.

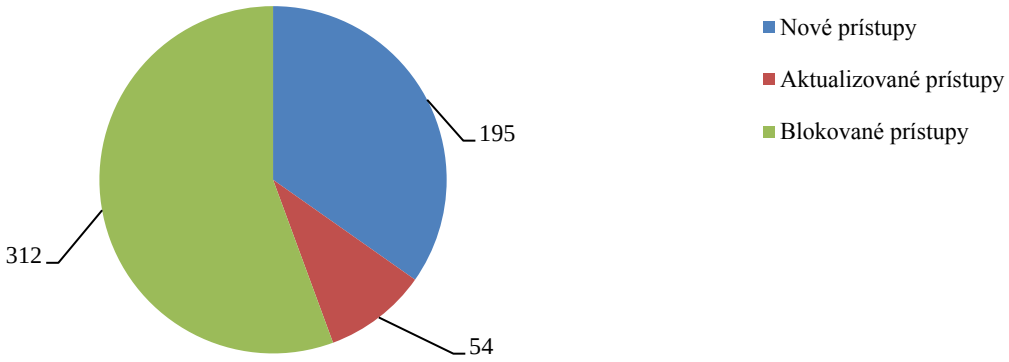
DataCentrum v rámci vytvárania prístupov pre užívateľov systému zabezpečovalo:

- centralizáciu Žiadostí o prístup do ITMS Core,
- kontrolu písomnej formy Žiadosti o prístup s elektronickou formou,
- vytvorenie, aktualizáciu alebo zrušenie prístupov pre užívateľov systému,
- zakladanie a archiváciu Žiadostí o prístup do ITMS Core,
- vytváranie nových orgánov, prideľovanie rolí orgánu, čítacích a aktualizačných vizibilít na základe požiadaviek CKO,
- aktualizáciu zoznamu orgánov a užívateľských rolí orgánu,
- zabezpečenie distribúcie prístupov užívateľom ITMS Core,
- vykonávanie pravidelnej previerky prístupov do systému a spracovanie záznamov z previerok prístupov.

Doba vytvorenia prístupu užívateľa do systému ITMS Core a doba aktualizácie orgánových a užívateľských rolí v systéme ITMS Core bola dodržiavaná v súlade s Manuálom pre prístupové práva do ITMS Core a interným Pracovným postupom č.07.

V dňoch 31.05.2017 a 12.12.2017 boli vykonané previerky prístupov do systému ITMS Core. Na kontrolovaných vzorkách prístupov do systému ITMS Core neboli zistené žiadne nedostatky. Z previerok boli vypracované záznamy.

Počet žiadostí o prístup do ITMS Core v roku 2017



ITMS Portál:

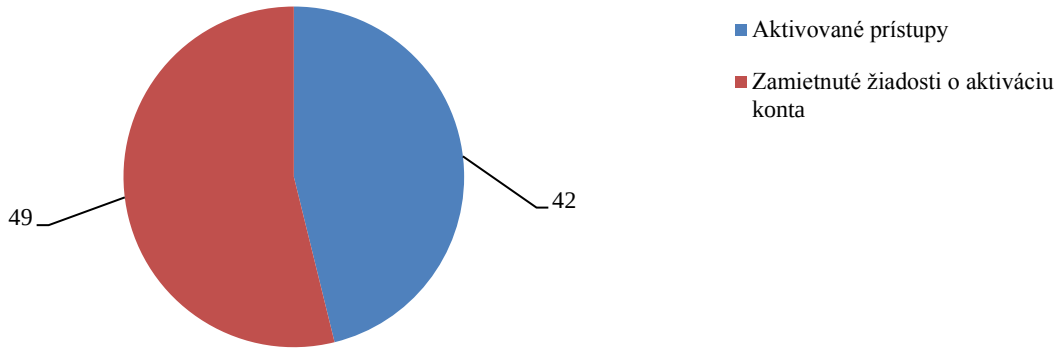
V rámci realizácie procesu spracovania žiadostí o aktiváciu konta do ITMS Portál boli DataCentrom vykonávané činnosti - zber, registrácia, kontrola písomnej formy žiadosti s elektronickou a archivácia žiadostí o aktiváciu konta do ITMS Portál. Následne, po úspešnej kontrole žiadosti, DataCentrum aktivovalo užívateľské konto a vydávalo GRID karty do ITMS Portál. V ITMS Portál je k 31.12.2017 aktívnych 13 543 užívateľov, z toho za sledované obdobie bolo aktivovaných 42 užívateľských účtov, 49 žiadostí o aktiváciu konta do ITMS Portál bolo zamietnutých. Najčastejším dôvodom zamietnutia žiadostí bolo už v minulosti vytvorené konto v ITMS Portál a vydaná Grid karta pre toho istého užívateľa (duplicitné žiadosti o prístup), prípadne omyl užívateľov, keď chceli vytvoriť prístup do ITMS2014+.

DataCentrum v rámci vytvárania prístupov pre užívateľov systému zabezpečovalo:

- centralizáciu žiadostí o aktiváciu konta do ITMS Portál,
- kontrolu písomnej formy žiadosti o aktiváciu konta do ITMS Portál s elektronickou formou,
- aktivovanie užívateľského konta do ITMS Portál a vydávanie GRID kariet do 1 pracovného dňa,
- zakladanie a archiváciu žiadostí o aktiváciu konta do ITMS Portál,
- zabezpečenie distribúcie prístupov užívateľom ITMS Portál.

Doba aktivácie užívateľského konta a vydanie GRID karty do systému ITMS Portál bola dodržiavaná v súlade s interným Pracovným postupom č.39.

Počet žiadostí o aktiváciu konta do ITMS Portál za rok 2017



5. Zabezpečenie bezpečnosti systému

Implementácia všetkých navrhovaných riešení z bezpečnostného projektu pre bezpečnosť ITMS II bola zrealizovaná, a všetky bezpečnostné opatrenia boli dodržiavané v spolupráci s útvarom bezpečnosti DataCentra, a za účasti garantov projektu ITMS II počas celej doby prevádzky systému ITMS II. V priebehu roku 2017 bol aktualizovaný Katalóg rizík pre systém ITMS, ktorý je súčasťou Bezpečnostného projektu pre ITMS.

6. Realizácia záložného systému ITMS

Z dôvodu nedostatku systémových prostriedkov (kapacita diskového poľa) nebolo možné realizovať záložné prostredie.

212	IT monitorovací systém pre Európske štrukturálne a investičné fondy pre programové obdobie 2014 - 2020 (ITMS2014+)

IT monitorovací systém pre Európske štrukturálne a investičné fondy pre programové obdobie 2014 - 2020 (ITMS2014+ verejná a ITMS2014+ neverejná časť) je v produkčnej prevádzke od júla 2015. V priebehu hodnoteného obdobia boli v prevádzke, prípadne boli uvedené v roku 2017 do prevádzky nasledovné integrácie s ITMS2014+:

- ISUF (MF SR)
- Register fyzických osôb (RFO - MV SR)
- IS CSRÚ - Register právnických osôb (RPO)
- Elektronický kontraktačný systém (EKS - MV SR)
- Vestník ÚVO
- IS CSRÚ - daňové nedoplatky (MF SR; Finančná správa Slovenskej republiky)
- Register úpadcov (MS SR)
- Obchodný register SR (MS SR)
- Register účtovných závierok (MF SR; Finančná správa Slovenskej republiky)
- Národný inšpektorát práce - Zoznam fyzických osôb a právnických osôb, ktoré porušili zákaz nelegálneho zamestnávania
- IS CSRÚ - IS SEMP: portál na evidenciu a monitorovanie pomoci
- CEDIS - audity

V priebehu roka 2017 boli pripravované integrácie, ktorých zavedenie do produkcie bude realizované v priebehu roka 2018:

- IS CSRÚ - Sociálna poisťovňa (MF SR)
- IS CSRÚ - všetky tri zdravotné poisťovne (MF SR)
- Register trestov (RT)
- Elektronické služby katastra nehnuteľností (ESKN)
- IS CSRÚ - Účastníci projektu

1. Správa a prevádzka systému

DataCentrum, v spolupráci s dodávateľom ITMS2014+, zabezpečovalo prevádzkovanie a spravovanie testovacieho, produkčného, školiaceho a cvičného systému ITMS2014+ neverejná časť a ITMS2014+ verejná časť (inštalácia servisných buildov, administrácia, management, zálohovanie...), zabezpečovalo technickú podporu pre systém a bežnú údržbu aplikačných systémov.

Aplikácia ITMS2014+ neverejná časť a ITMS2014+ verejná časť pracuje pod OS Linux. Aplikácia využíva ako fyzické servery len databázové servery a report server, všetky ostatné serverové komponenty architektúry sú realizované ako virtuálne servery.

Aplikácia ITMS2014+ pracuje nad zjednotenou databázou pre verejnú aj neverejnú časť ITMS2014+, ktorá je umiestnená v rámci komunikačno-technologickej infraštruktúry DataCenta (KTI). K 31.12.2017 je v prevádzke produkčný systém ITMS2014+ neverejná časť a ITMS2014+ verejná časť verzia 10.4.11. V prevádzke je tiež testovací, školiaci a cvičný systém ITMS2014+ neverejná časť a ITMS2014+ verejná časť.

V roku 2017 DataCentrum realizovalo činnosti súvisiace so zabezpečovaním produkčnej prevádzky ITMS2014+ a súčasne vedúce ku skvalitneniu poskytovaných služieb pre ITMS2014+, ako aj činnosti na odstránenie nedostatkov zistených vládnym auditom ITMS2014+.

Boli to nasledovné činnosti:

- realizácia nákupu podpory licencií mailového systému,
- realizácia nákupu podpory CITRIX licencii,
- realizácia nákupu podpory na VMware licencie,
- realizácia nákupu podpory na Symantec licencie,
- realizácia nákupu podpory na AUTOCAD licencie,
- realizácia nákupu podpory RED HAT produktov,
- realizácia nákupu licencií ESET,
- príprava a nákup Windows server a Windows Remote Desktop licencií,
- realizácia upgradu prostredia KTI,
- príprava a realizácia riešenia pre vzdialený administrátorský prístup,
- migrácia na nový systém SK-NIC,
- príprava redizajnu monitoringu počítačovej sály,
- rozšírenie kapacity diskového poľa,
- príprava migrácie zálohovacieho systému,
- realizácia prepojení na externé informačné systémy.

V priebehu sledovaného obdobia boli pravidelne dopĺňané údaje týkajúce sa ITMS2014+ do konfiguračnej databázy a pravidelne sa vykonávala aj aktualizácia (patchovanie) operačného systému pre ITMS2014+.

Zamestnanci DataCentra vykonávali v hodnotenom období administráciu časti produkčného, testovacieho a cvičného systému ITMS2014+ neverejná časť a ITMS2014+ verejná časť - modulu Orgány a používatelia - Orgány, Pracovné pozície, Používatelia, Žiadosti o aktiváciu konta, a na základe žiadostí zo strany používateľov sa vykonávali aj úpravy v časti Subjekty a osoby.

Počas celej doby prevádzky ITMS2014+ boli dodržiavané všetky bezpečnostné opatrenia vyplývajúce z požiadaviek na bezpečnosť systému (v roku 2015 bol vypracovaný a schválený Bezpečnostný projekt pre ITMS2014+, Bezpečnostný manuál pre koncových používateľov a manažérov ITMS2014+ a Katalóg rizík pre systém ITMS2014+).

Zálohovanie ITMS2014+ sa realizuje kopírovaním kľúčových dát (databáza aplikácie, databáza používateľov, dokumentácia) do záložného prostredia. Vzhľadom k tomu, že aplikácia ITMS2014+ je v pilotnej prevádzke, pravidelne sa vykonávala len obnova databázy aplikácie.

ITMS2014+ neverejná časť a ITMS2014+ verejná časť sú začlenené do centrálneho monitoringu prevádzky v DataCentre, v rámci ktorého je nad systémom ITMS2014+ neverejná časť a ITMS2014+ verejná časť uskutočňovaný základný monitoring, ktorý sa realizuje pomocou nástroja BAC, a to spustením Žiadosti o aktiváciu používateľského konta do ITMS2014+ verejná časť a prihlásením sa do aplikácie pre ITMS2014+ neverejná časť. Počas sledovaného obdobia neboli centrálnym monitoringom zaznamenané väčšie nedostupnosti systému ITMS2014+ neverejná časť a ITMS2014+ verejná časť, okrem nedostupnosti počas pravidelnej údržby systému ITMS a počas nasadzovania nových buildov pre systém ITMS. Dostupnosť produkčného systému ITMS2014+ neverejná časť a ITMS2014+ verejná časť bola v hodnotenom období 99,99 %.

2. Užívateľská, aplikačná, technická, technologická podpora a monitoring

Cieľom úlohy je zabezpečovať pomoc používateľom pri práci s aplikáciou ITMS2014+ neverejná časť a ITMS2014+ verejná časť. DataCentrum počas roku 2017 poskytovalo 1. úroveň podpory, 2. úroveň podpory (aplikačnú, technickú a technologickú podporu) bola poskytovaná v spolupráci s dodávateľom ITMS2014+.

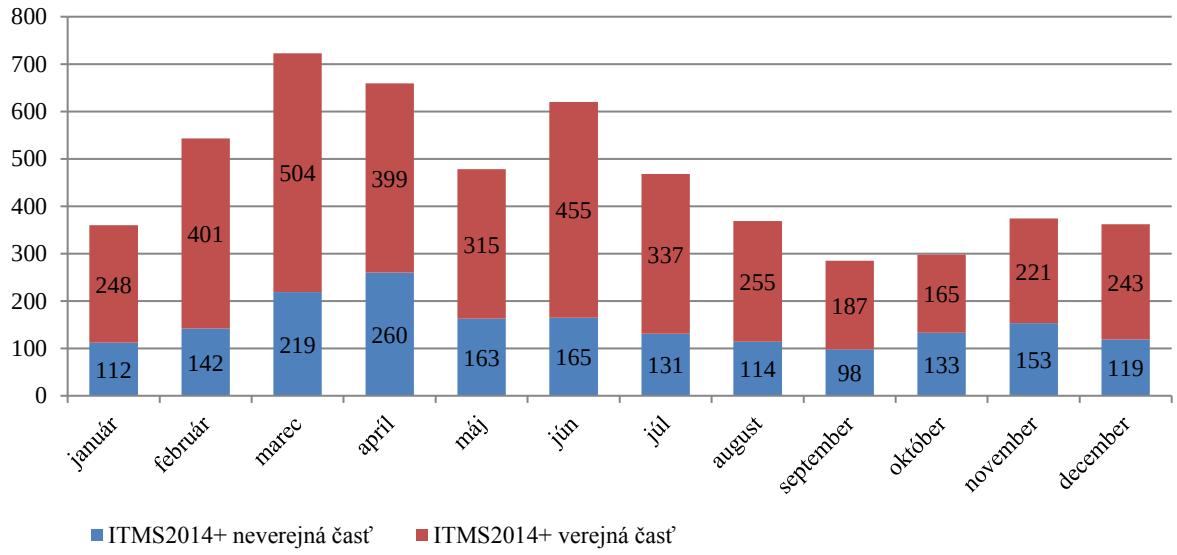
Všetky problémy používateľov pri práci so systémom ITMS2014+ neverejná časť alebo ITMS2014+ verejná časť, hlásené prostredníctvom telefónu, e-mailu, alebo web rozhraním boli zaznamenané v aplikácii HP ServiceManager a riešené pracovníkmi 2. úrovne podpory.

Hlásenia zaznamenané v aplikácii HP ServiceManager boli vyriešené v stanovenom termíne podľa SLA.

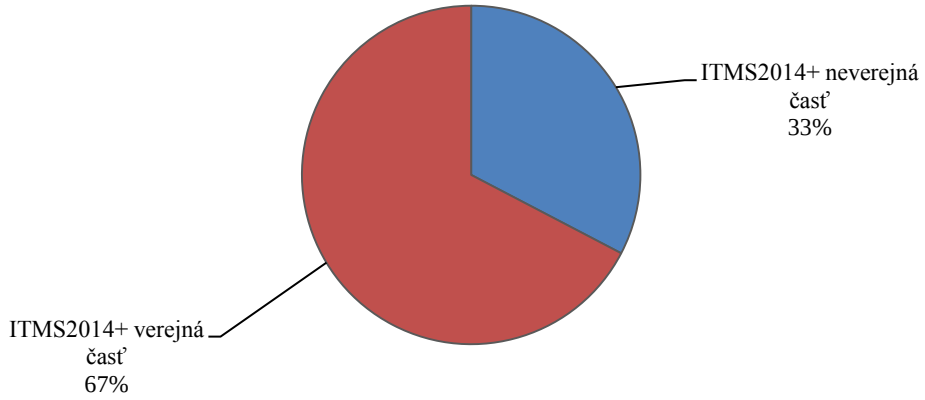
V sledovanom období bolo vyriešených 1 809 hlásení používateľov pre ITMS2014+ neverejná časť a 3 730 hlásení používateľov ITMS2014+ verejná časť. Prevažná časť hlásení sa týkala problémov s prihlásením sa do systému ITMS2014+ verejná časť (problémy používateľov pri vytváraní ŽoAK), problémov pri vytváraní ŽoNFP a VO, a tiež metodických usmernení používateľov neverejnej časti ITMS2014+.

Aplikačná podpora pre ITMS2014+ bola poskytovaná permanentne počas pracovných dní v čase od 8^{00} do 17^{00}, a v prípade mimoriadnych situácií aj mimo uvedených hodín.

Počet zaznamenaných a vyriešených hlásení užívateľov systému ITMS2014+ v roku 2017



Percentuálne zobrazenie vyriešených hlásení užívateľov systému ITMS2014+ v roku 2017



3. Zabezpečovanie prístupov pre používateľov systému

ITMS2014+ neverejná časť:

V rámci realizácie úlohy procesu spracovania žiadostí pre orgány a žiadostí o prístup do ITMS2014+ neverejná časť, boli v systéme ITMS2014+ vytvárané nové orgány v implementácii fondov a vytvárané nové používateľské kontá. Zároveň boli vytvárané potrebné prístupy na základe poverení pre manažérov ITMS2014+ na rezortoch.

Úlohou DataCentra bol zber, registrácia a kontrola písomnej formy žiadosti o prístup do ITMS2014+ neverejná časť a, po zapracovaní v systéme ITMS2014+, archivácia žiadostí o prístup do ITMS2014+. DataCentrum zriaďovalo prístup do produkčného systému ITMS2014+ neverejná časť, a pre manažérov ITMS2014+ aj do testovacieho systému ITMS2014+ neverejná časť na základe schválených žiadostí. Ku koncu sledovaného obdobia bolo v ITMS2014+ neverejná časť 2 046 aktívnych používateľov, z toho za sledované obdobie bolo spracovaných 576 nových žiadostí o prístup do ITMS2014+ neverejná časť, 172 prístupov do ITMS2014+ neverejná časť bolo aktualizovaných na základe formuláru F175 a 431 používateľských účtov bolo zrušených na základe formuláru F175 alebo hlásenia v HPSM. Zároveň bolo schválených a vytvorených 160 prístupov do ITMS2014+ cez Internet, 49 prístupov do verejnej časti ITMS2014+ pre používateľov neverejnej časti ITMS2014+ a vytvorených 22 prístupov pre Manažérov ITMS2014+.

Pre Manažérov ITMS2014+ bol súčasne zriaďovaný aj prístup do prostredia STG (testovacie) ITMS2014+ neverejná časť.

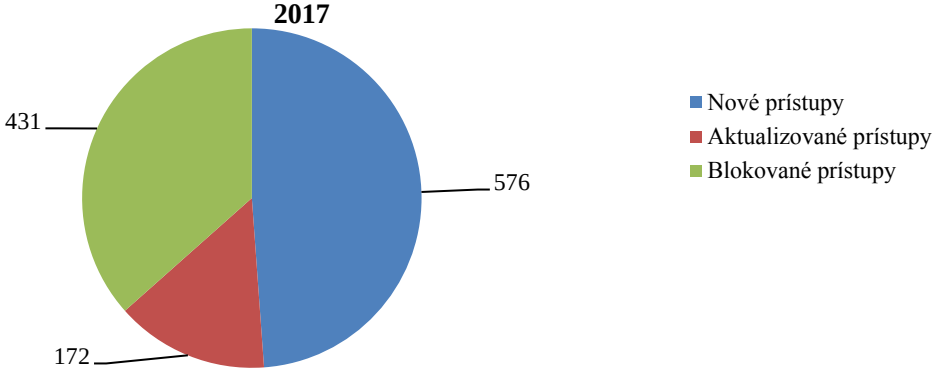
DataCentrum v rámci vytvárania prístupov pre používateľov systému zabezpečovalo:

- centralizáciu písomnej formy Žiadostí o prístup do ITMS2014+ neverejná časť,
- vytvorenie, aktualizáciu alebo zrušenie prístupov pre používateľov systému,
- zakladanie a archiváciu Žiadostí o prístup do ITMS2014+ neverejná časť,
- vytváranie nových orgánov, prideľovanie rolí orgánu, čítacích a aktualizačných vizibilít na základe požiadaviek CKO,
- aktualizáciu zoznamu orgánov a používateľských rolí orgánu,
- aktualizácia Pracovného postupu PP č.62, Vydanie 07,
- aktualizácia Manuálu pre prístupové práva do ITMS2014+ neverejná časť, Verzia 0.7,
- aktualizácia Formuláru F175 spolu s prílohami A,B,C,D (Žiadosť o prístup do ITMS2014+, Vydanie 07),
- zabezpečenie distribúcie všetkých relevantných dokumentov manažérom ITMS2014+ na rezortoch,
- vykonávanie pravidelnej previerky prístupov do systému a spracovanie záznamov z previerok prístupov.

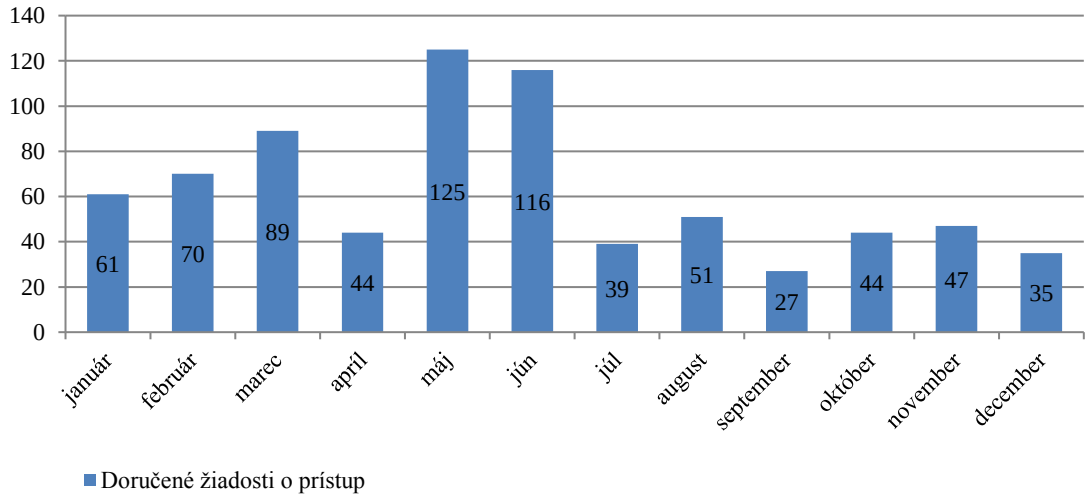
Doba vytvorenia prístupu do systému ITMS2014+ neverejná časť pre používateľa a doba aktualizácie orgánových a používateľských rolí v systéme ITMS2014+ neverejná časť bola dodržiavaná v súlade s Manuálom pre prístupové práva do ITMS2014+ neverejná časť a interným Pracovným postupom č.62.

V dňoch 31.05.2017 a 12.12.2017 boli vykonané previerky prístupov do systému ITMS2014+ neverejná časť. Na kontrolovaných vzorkách prístupov do systému ITMS2014+ neverejná časť neboli zistené žiadne nedostatky. Z previerok boli vypracované záznamy.

Počet spracovaných prístupov do ITMS2014+ neverejná časť v roku 2017



Počet žiadostí o prístup do ITMS2014+ neverejná časť v roku 2017



ITMS2014+ verejná časť:

V rámci realizácie procesu spracovania žiadostí o aktiváciu používateľského konta do ITMS2014+ verejná časť boli DataCentrom vykonávané činnosti - zber, registrácia, kontrola písomnej formy žiadosti s elektronickou a archivácia žiadostí o aktiváciu používateľského konta do ITMS2014+ verejná časť (ŽoAK). Následne, po úspešnej kontrole žiadosti, DataCentrum schválilo ŽoAK, a týmto bolo v systéme ITMS2014+ vytvorené žiadané používateľské konto. V ITMS2014+ verejná časť je k 31.12.2017

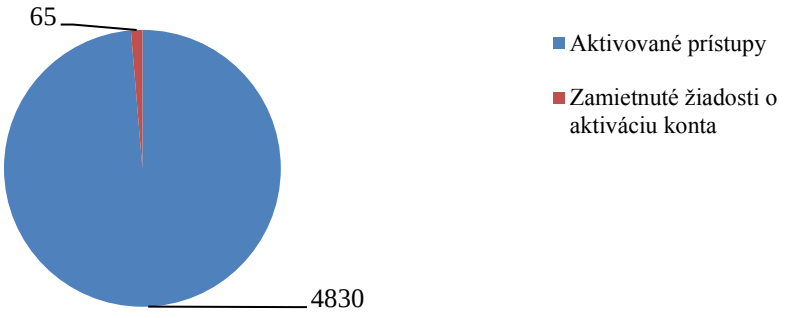
aktívnych 9 367 používateľov, z toho za sledované obdobie bolo aktivovaných 4 830 používateľských účtov, 65 žiadostí o aktiváciu konta do ITMS2014+ verejná časť bolo zamietnutých. Najčastejším dôvodom zamietnutia žiadostí bolo doručenie draftu žiadostí, doručenie žiadostí s chýbajúcim úradným overením podpisu štatutára, prípadne chýbajúcim podpisom používateľa.

DataCentrum v rámci vytvárania prístupov pre používateľov systému ITMS2014+ verejná časť zabezpečovalo:

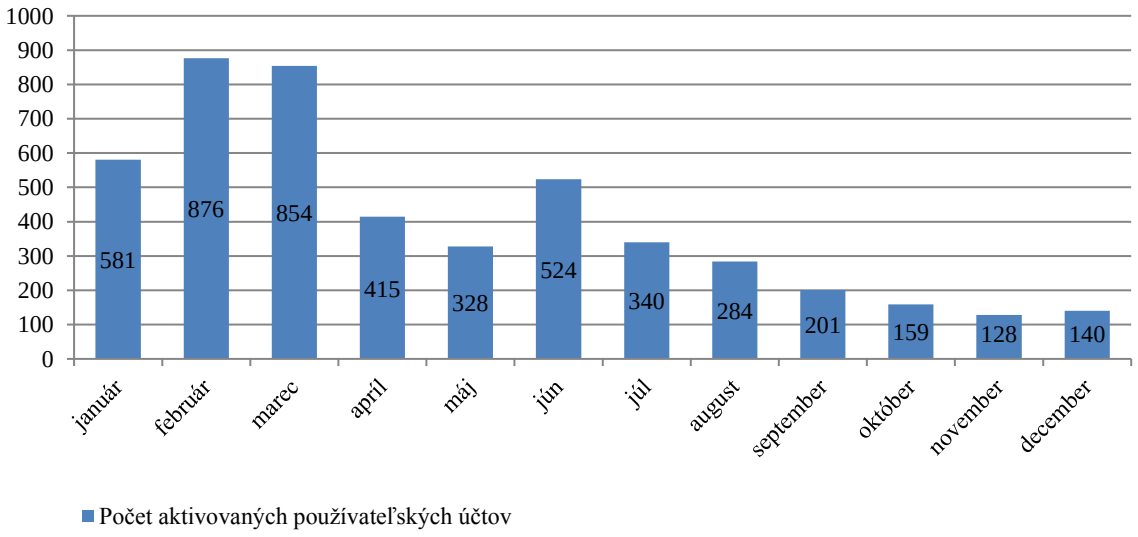
- centralizáciu žiadostí o aktiváciu používateľského konta do ITMS2014+ verejná časť,
- kontrolu písomnej formy žiadosti o aktiváciu používateľského konta do ITMS2014+ verejná časť s elektronickou formou,
- schválenie ŽoAK (aktivovanie používateľského konta do ITMS2014+ verejná časť) do 1 pracovného dňa,
- zakladanie a archiváciu žiadostí o aktiváciu používateľského konta do ITMS2014+ verejná časť.

Doba schválenia ŽoAK (aktivácie používateľského konta do systému ITMS2014+ verejná časť) bola dodržiavaná v súlade s interným Pracovným postupom č.63.

Počet žiadostí o aktiváciu používateľského konta do ITMS2014+ verejná časť za rok 2017



Počet aktivovaných používateľských účtov v ITMS2014+ verejná časť v roku 2017



4. Zabezpečenie bezpečnosti systému

Počas roku 2015 bol zo strany vlastníka systému ITMS2014+ (ÚV SR) vypracovaný a schválený Bezpečnostný projekt pre ITMS2014+, Bezpečnostný manuál pre koncových používateľov a manažérov ITMS2014+ a Katalóg rizík pre systém ITMS2014+.

Navrhované riešenia z Bezpečnostného projektu pre ITMS2014+ sú v štádiu implementácie, odporúčania z vládneho auditu A649 a č.K3959 boli zrealizované ešte počas roka 2015. Všetky bezpečnostné opatrenia boli dodržiavané v spolupráci s útvarom bezpečnosti DataCentra, a za účasti garantov projektu ITMS2014+ počas celej doby prevádzky systému ITMS2014+.

5. Realizácia záložného systému ITMS2014+

Počas hodnoteného obdobia bolo záložné prostredie pre ITMS2014+ vytvorené, a v prípade potreby je možná jeho aktivácia podľa platnej SLA.

221	Komunikačno-technologická infraštruktúra (KTI)

Hlavným cieľom úlohy je zabezpečovanie nepretržitej správy činnosti celého komunikačného systému, ktorý zabezpečuje spojenia a komunikáciu používateľov IS systému Štátnej pokladnice, informačného systému pre štrukturálne fondy a kohézny fond a tiež rezortnú počítačovú sieť.

Súčasťou starostlivosti o komunikačné spojenia je aj neustále doplňovanie systému monitoringu aktívnych liniek v DataCentre, ktoré slúži na sledovanie aktuálnej činnosti liniek a ich potenciálnych poruchových stavov.

Zamestnanci DataCentra spolupracovali pri údržbe a opravách zariadení komunikačného vybavenia a havarijných výpadkov liniek, pri prevádzkovaní šifrátorov, pri rôznych meraniach a pri údržbe optiky zaústenej priamo v stojanoch komunikačného uzla v DataCentre.

Aj v roku 2017 IP telefónia DataCentra pracovala bez problémov a v súlade s požiadavkami boli vykonávané potrebné zmeny v parametroch klapiek a priebežne boli odstraňované vzniknuté problémy. V tomto roku bol dokončený hardwarový aj softvérový upgrade IP telefónie. Tento upgrade v sebe zahŕňa výmenu serverov a inštaláciu nového operačného systému.

Naďalej pokračovalo skvalitňovanie monitorovania chodu počítačovej sály a zvýšil sa počet dohľadovaných zariadení. Stála dohľadová služba v DataCentre bola včas informovaná o výnimočných stavoch a mohla tak zabezpečiť rýchly zásah. Dohľad sa uskutočňuje aj zo záložného pracoviska.

Počas roku 2017 boli zrealizované pripojenia ďalších rack-ov na systém distribúcie elektrickej energie. Do napájacích vetiev boli inštalované merače prúdu a príkonu. Sústavne sú sledované odbery elektrickej energie v technologických priestoroch. Pravidelne je kontrolovaný stav oboch hlavných UPS a prebiehalo pravidelné testovanie a ošetrovanie nového a aj starého dieselgenerátora.

V rámci medzinárodnej spolupráce bol naďalej zabezpečovaný chod národného uzla TAXUD.

V súlade s potrebami užívateľov Ministerstva financií SR a Finančnej správy SR prebiehala spolupráca pri nasadzovaní nových aplikácií a pri riešení problémov v prevádzkovaných aplikáciách. Spolu s partnermi v CCN/TC v Bruseli boli pre nové aplikácie k nim vytvárané heslá, pridávané, odoberané a upravované kontá podľa požiadaviek a priebežne bola udržovaná aj potrebná dokumentácia. Nepretržite prebiehalo aj monitorovanie činnosti národného uzla CCN/CSI, pričom boli podľa potreby uskutočňované príslušné zásahy. Zálohovanie na pásky sa v súčasnosti vykonáva iba podľa požiadavky z Bruselu.

V roku 2017 pokračovala spolupráca so Štatistickým úradom SR na prevádzke celoeurópskej aplikácie SIMSTAT prepájajúcej štatistické úrady jednotlivých členských štátov Európskej únie.

DataCentrum pôsobilo od vzniku Finančnej správy SR ako systémový integrátor pri spúšťaní ISVS FS - predovšetkým s cieľom optimalizácie dizajnu KTI pre prepojenie dátových centier Colného riaditeľstva, Daňového riaditeľstva a DataCentra. Na základe takto získaných informácií bolo následne kreované IT prostredie pre AD, Microsoft Exchange, Sharepoint a realizované komunikačné prostredie ISVS FS SR.

Odborní garanti DataCentra kontinuálne zabezpečovali spoľahlivú a bezpečnú prevádzku KTI pre Ministerstvo financií SR, Štátnu pokladnicu, Agentúru riadenia dlhu a likvidity a Finančnú správu SR.

Pre potreby Finančnej správy SR zabezpečilo DataCentrum technologický upgrade hlavných uzlov WAN CR a WAN DR (CPE, LAN, FW) a spoľahlivú a bezpečnú prevádzku KTI. Do CMP DataCentra bol implementovaný systém sledovania štatistík vyťaženosti jednotlivých dátových okruhov Finančnej správy SR s cieľom aktívneho monitoringu prevádzky počas implementácie nových aplikácií Finančnej správy SR. Týmto spôsobom bola KTI priebežne (aktuálne) nastavovaná podľa aktuálnych záťaží jednotlivých liniek. DataCentrum zabezpečilo zjednotenie WAN sietí CR SR a DR SR do jednotnej WAN FS (Full mesh). Aktívnym prístupom k sledovaniu prevádzky WAN FS a expresným zabezpečovaním potrebných kapacít KTI boli eliminované problémy v dátových prenosoch.

KTI bola aktualizovaná v súlade s meniacimi sa funkčnými potrebami rezortu s ohľadom na zmeny v legislatíve.

V roku 2017 boli realizované implementačné práce pre upgrade farmy KTI. Prebehla inštalácia a konfigurácia HW a SW vybavenia, deployment finálnych verzií aplikácií na novú farmu, príprava a distribúcia inštalačného balíka a návodu, nakoniec prebehla taktiež zmigrácia používateľov na novú farmu, prebehla výmena centrálnych prepínačov siete KTI, výmena firewallov, s čím bola spojená potreba migrácie všetkých sieťových služieb, vrátane zabezpečených pripojení do tejto siete, na nové zariadenia a boli realizované nové prepojenia informačných systémov prevádzkovaných v prostredí KTI s informačnými systémami organizácií štátnej správy.

Dátové centrum Kopčianska

DataCentrum ako rozpočtová organizácia Ministerstva Financií SR nadobudla nové Dátové centrum, ktoré bolo financované z prostriedkov Operačného programu Informatizácie spoločnosti (OPIS) ešte v roku 2014.

Cieľom projektu bolo zriadenie budovy Dátového centra so základnou infraštruktúrou pre sieťovú konektivitu, napájanie, chladenie a bezpečnosť v zmysle definovaných požiadaviek a špecifikácií. Výsledkom je poskytovanie technologických služieb zabezpečenia a poskytovania infraštruktúry iným subjektom verejnej správy.

Implementácia projektu prináša niekoľko pozitív, ktoré sú dôležité pre poskytovanie elektronických služieb verejnosti a ďalší koncepčný rozvoj IKT vo verejnej správe smerom k moderným postupom a technológiám - je to predovšetkým:

- vyššia dostupnosť elektronických služieb,
- vyššia odbornosť zamestnancov zodpovedných za prevádzku informačných systémov,
- lepšia škálovateľnosť a efektivita využitia IKT vo verejnej správe.

DataCentrum na Kopčianskej ulici má k dispozícií dve IKT sály.

V priestoroch Dátového centra je inštalovaný poplachový systém na hlásenie narušenia doplnený aj kamerovým systémom a prístup do celého areálu a jednotlivých priestorov je riadený systémom kontroly vstupu. V roku 2017 bol objekt napojený aj na Pult Centrálnej Ochrany policajného zboru. Bezpečnostné systémy sú integrované do jedného monitorovacieho nástroja, ktorý umožňuje jednoduchšie riešenie incidentov a aj spätné vyhľadávanie informácií z minulosti. Všetky priestory dátového centra sú vybavené elektronickou požiarnou signalizáciou s opticko-dymovými hlásičmi. Všetky kritické technológie Dátového centra, najmä elektrické napájanie a chladenie sú nepretržite sledované prostredníctvom monitorovacieho systému, ktorý poskytuje komplexný prehľad o prevádzkových stavoch, aktuálnom zaťažení a obsadenosti Dátového centra.

222	Komunikačno - technologická infraštruktúra 2 (KTI2)

KTI2 je prístupová vrstva pre zabezpečenie bezpečného a flexibilného pripojenia koncových používateľov k publikovaným aplikačným rozhraniam.

Základným princípom riešenia je poskytnutie bezpečnostných komponentov ktoré zabezpečia ochranu rozhraní prevádzkovaných informačných systémov na úrovni prístupovej vrstvy. Prostredie KTI2 umožňuje využívať dvojfaktorovú autentifikáciu, čo je do budúcna možné využiť aj pre prístup k ďalším aplikáciám.

Prostredie KTI2 bolo vybudované predovšetkým pre zabezpečenie prístupu používateľov k Multiklientskému platobnému portálu určenému pre realizovanie platieb vyšších územných celkov z účtov vedených v Štátnej pokladnici. Ako prví sa pripojili k tomuto portálu používatelia Bratislavského samosprávneho kraja, pre organizácie ktorého DataCentrum zabezpečilo vzájomné sieťové prepojenie i prepojenie do DataCentra. V ďalšom období boli k tomuto portálu postupne pripájané ďalšie VÚC.

Prostredníctvom prostredia KTI2 sú okrem Multiklientskeho platobného portálu poskytované ďalšie portálové aplikácie ako EPE (Elektronická portálová evidencia), CKS (Centrálny konsolidačný systém - pôvodne JUŠ), SEMP (Systém pre evidenciu a monitorovanie pomoci), ďalej boli uvedené do prevádzky portály CEM a CRPŠ (Centrálna evidencia majetku, Centrálny register pohľadávok štátu) , AZU (asynchrónny zber údajov, testovací aj ostrý, odovzdané v decembri 2017, v záložnom prostredí nie je) a reportovaci systém BOBJ.

Pre Ministerstvo spravodlivosti SR bolo prostredníctvom prostredia KTI2 zabezpečené flexibilné a bezpečné pripojenie používateľov v pôsobnosti MS SR a ich organizácií ku IS ESO. Po implementácii 1. fázy riešenia boli na základe počtu používateľov a nárokov na ich správu rozšírené požiadavky na mieru integrácie správy používateľov a využitie autentifikačných metód.

Bola zabezpečená prevádzka záložného prostredia KTI2 v záložnom výpočtovom stredisku, ktorého úlohou je zabezpečiť dostupnosť aplikácií poskytovaných prostredníctvom primárneho prostredia KTI2 v prípade jeho výpadku.

V súvislosti s potrebou zabezpečenia prekladov mien na IP adresy boli do sietí Finnet vypublikované pre prostredie KTI2 DNS servre, ktoré zabezpečujú túto funkcionalitu. V rámci prevádzkových činností boli zabezpečované aktualizácie sieťových a bezpečnostných zariadení a ich signatúr, boli zabezpečované zmeny v nastaveniach používateľských účtov a ich privilégií. Okrem toho bol zabezpečovaný monitoring prevádzky a riešenie problémových a chybových stavov, kedy v prípade potreby sa uskutočnili rekonfigurácie zariadení, siete alebo systémov.

V roku 2017 bola vykonaná zmena dizajnu infraštruktúry KTI2 na umožnenie efektívnejšieho poskytovania služieb touto infraštruktúrou.

303	Časové rady v prostredí Lotus Notes

V roku 2017 boli v rámci tejto úlohy priebežne prenášané vhodne štrukturované údaje do aplikácie Časové rady v prostredí Lotus Notes na MF SR k užívateľom.

Peňažníctvo a menový vývoj - kvartálne údaje za 4. štvrťrok 2016 až 3. štvrťrok 2017 a mesačné údaje za november 2016 až október 2017.

Platobná bilancia SR - kvartálne údaje za 1. štvrťrok 2008 až 2. štvrťrok 2017 a mesačné údaje za január 2008 až september 2017.

311	Podpora používateľov pri práci s aplikáciami rozpočtového informačného systému - AP RIS (Aplikačná podpora RIS)

DataCentrum prostredníctvom CPU zabezpečovalo v roku 2017 pre správu a prevádzku informačného systému RIS pomoc používateľom pri používaní jednotlivých modulov, odhaľovanie nekorektnej funkcionality, zbieranie a odovzdávanie námetov na ďalší rozvoj RIS. Pracovisko aplikačnej podpory RIS sa podieľalo na riadiacich a koordinačných činnostiach. Pravidelne, raz mesačne, sa konali koordinačné porady, na ktorých sa riešili všetky vzniknuté problémy v prevádzke RIS a podnety pre ďalší vývoj.

Oddelenie aplikačnej podpory RIS:

- poskytovalo aplikačnú podporu používateľom pri práci s modulmi RIS:
    - ZoRo - Zostavenie rozpočtu,
    - MPR - Modul programové rozpočtovanie,
    - RI - Register investícií,
    - MÚR - Modul úprav rozpočtu,
    - ADI - Adicionality,
    - NU - Nefinančné ukazovatele,
    - MaH - Monitorovanie a hodnotenie programovej štruktúry,
    - KaA - Kontrola a audit,
    - RIS – mzdy,

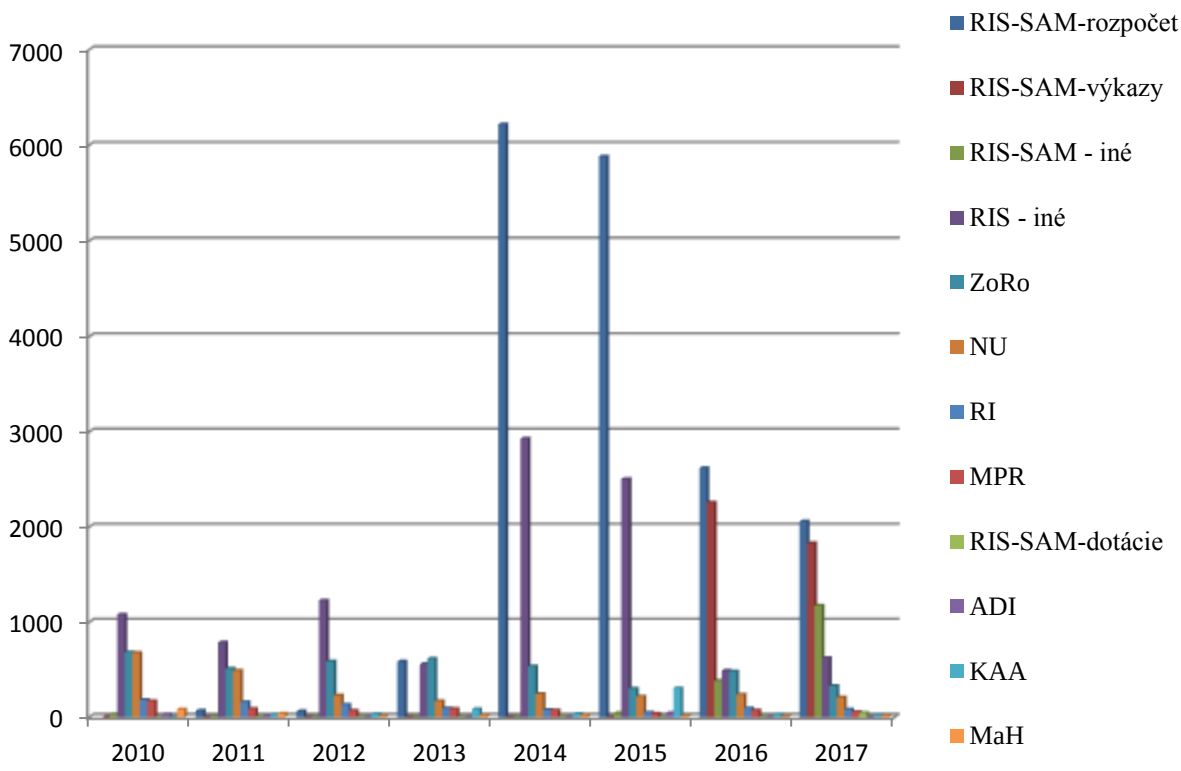
- a pri práci s modulmi RIS-SAM
    - RIS–SAM Rozpočet - Rozpočtový informačný systém pre samosprávu - rozpočet
    - RIS–SAM Výkazy - Rozpočtový informačný systém pre samosprávu – výkazy
    - RIS–SAM Dotácie - Rozpočtový informačný systém pre samosprávu - dotácie

- CPU priebežne sprostredkovávalo metodické a organizačné usmernenia medzi vlastníkom procesu, resp. metodickým garantom a používateľmi,
- zaznamenávalo problémy používateľov, ich požiadavky a poskytovalo tieto informácie tretej úrovni podpory, metodickému garantovi a dodávateľovi RIS za účelom analýzy najčastejšie sa vyskytujúcich požiadaviek, problémov a navrhovania úprav v jednotlivých moduloch. Pri poskytovaní podpory a služieb spolupracovalo s ostatnými pracoviskami a úrovňami CPU.

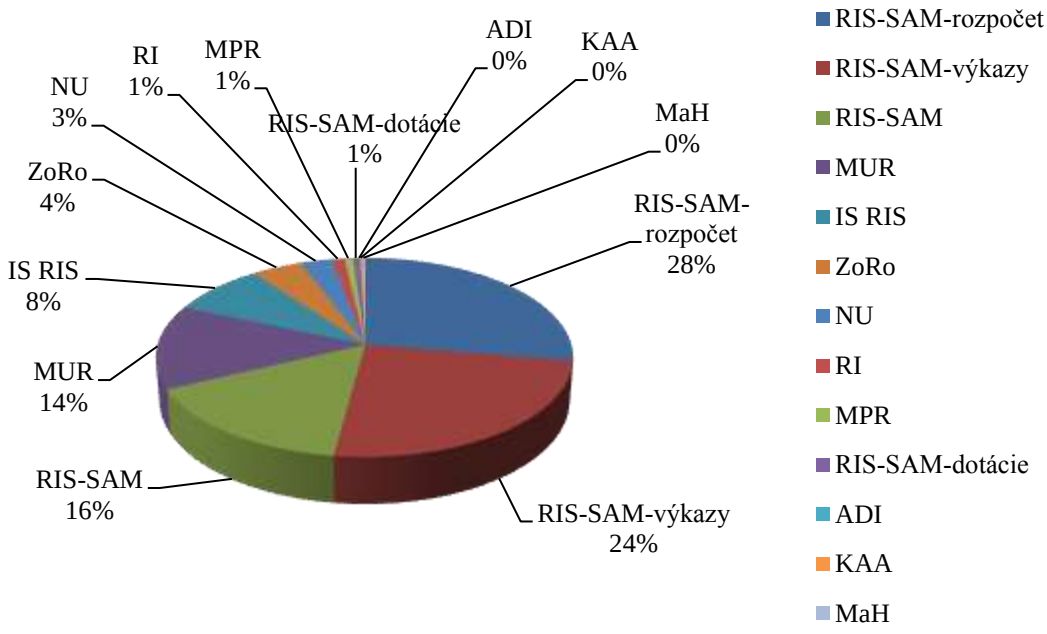
Celkový počet a percentuálny podiel vyriešených hlásení týkajúcich sa aplikačnej podpory RIS po jednotlivých moduloch a v porovnaní s predchádzajúcimi rokmi je uvedený v nasledujúcej tabuľke a grafe:

Moduly RIS	2010	2011	2012	2013	2014	2015	2016	2017
RIS-SAM-rozpočet		68	63	586	6219	5882	2620	2060
RIS-SAM-výkazy	*	*	*	*	*	*	2258	1830
RIS-SAM-iné	31	10	2	1	1	43	382	1173
MUR	2095	1709	1400	1580	1380	2188	1557	1024
IS RIS- iné	1080	787	1227	557	2929	2504	490	622
ZoRo	683	510	586	616	535	301	481	329
NU	676	489	230	170	245	217	238	209
RI	181	158	132	92	76	49	94	83
MPR	170	87	68	88	73	38	71	54
RIS-SAM-dotácie	*	*	*	*	*	*	*	45
ADI	31	10	2	1	1	43	2	0
KAA	*	26	32	85	36	304	28	20
MaH	82	37	12	19	18	14	6	15
SPOLU	5029	3 891	3 754	3 795	11 513	11 583	8 225	**7 464**

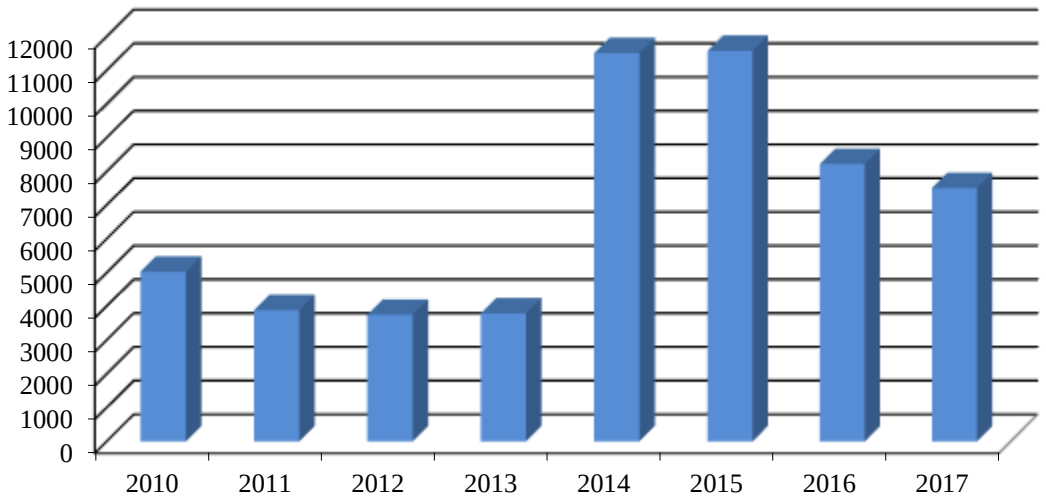
/* údaje nie sú k dispozícii



Počet vyriešených hlásení v roku 2017 podľa jednotlivých modulov RIS-u v %:



Celkový počet vyriešených hlásení týkajúcich sa aplikačnej podpory RIS v porovnaní s predchádzajúcimi rokmi:



313	Účtovný informačný systém miestnej samosprávy

V roku 2017 boli v rámci tejto úlohy vykonané nasledovné činnosti:

- úprava programovej aplikácie na uloženie a výber údajov v DataCentre v súvislosti so zmenami vo finančných a účtovných výkazoch pre koniec roka 2016 a pre rok 2017 pre spracovanie údajov obcí, rozpočtových a príspevkových organizácií v ich pôsobnosti a ostatných subjektov verejnej správy, ktoré majú povinnosť predložiť výkazy v zmysle platnej legislatívy,
- aktualizácia číselníka obcí, rozpočtových a príspevkových organizácií v ich pôsobnosti a ostatných subjektov verejnej správy, spracovanie finančných a účtovných výkazov obcí k 31.12.2016 (9 druhov výkazov), Poznámok k individuálnej účtovnej závierke (štruktúrovanej i neštruktúrovanej časti Poznámok) a Poznámok ku konsolidovanej účtovnej závierke (štruktúrovanej i neštruktúrovanej časti Poznámok) za rok 2016, finančných výkazov obcí k 31.03.2017, k 30.6.2017 a 30.9.2017 (7 druhov výkazov) za 2926 obcí, 2213 rozpočtových organizácií v pôsobnosti obcí, 251 príspevkových organizácií v pôsobnosti obcí a 458 ostatných subjektov verejnej a mesačné spracovanie finančného výkazu FIN 1-12 za vybrané ostatné subjekty verejnej správy, ktoré majú povinnosť predložiť výkaz v zmysle platnej legislatívy,
- kontrola správnosti logických väzieb údajov za jednotlivé druhy výkazov, oprava chybných údajov komunikáciou s predkladateľmi výkazov prostredníctvom metodikov obcí resp. priamo so subjektmi,
- nahratie údajov z informačného systému RIS.SAM za 4. štvrťrok 2016, mesačne a za 1. až 3.štvrťrok 2017 a vypracovanie programov pre štandardné zostavy (základné zostavy a zostavy pre potreby oddelenia rozpočtovej regulácie a analýz financovania územných samospráv) podľa požiadaviek pracovníkov MF SR, vytvorenie a odovzdanie všetkých požadovaných výstupov za obce pre Sekciu štátneho výkazníctva a Sekciu rozpočtovej politiky MF SR za 4. štvrťrok 2016 a 1. až 3. štvrťrok 2017 a mesačné spracovanie finančného výkazu FIN 1-12.

Okrem štandardných zostáv pre MF SR bolo odovzdaných 75 neštandardných výstupov podľa požiadaviek, ako aj poskytnutie vyžiadaných údajov podľa zákona o verejnom prístupe k informáciám, čo si vyžiadalo vypracovanie nových programov s časovou i vecnou náročnosťou spracovania týchto úloh, výber a prenos individuálnych údajov za obce, rozpočtové a príspevkové organizácie v ich pôsobnosti a ostatné subjekty verejnej správy do IS Štátnej pokladnice za 4.štvrťrok 2016 a 1. až 3.štvrťrok 2017 a mesačné spracovanie výkazu FIN 1-12 za vybrané ostatné subjekty verejnej správy, ktoré majú povinnosť predložiť výkaz v zmysle platnej legislatívy, vytvorenie a odovzdanie požadovaných výstupov Centru vedecko-technických informácií SR, Ministerstvu kultúry SR, Ministerstvu školstva, vedy, výskumu a športu SR, Najvyššiemu kontrolnému úradu a subjektom ŠÚ SR, Národná banka Slovenska a iným podnikateľským subjektom, s ktorými MF SR uzatvorilo Zmluvu o poskytovaní údajov. Bol aktualizovaný obsah prílohy č.1 a č.1A k dohode o vzájomnom poskytovaní údajov uzavretej medzi DataCentrom a ŠÚ SR.

Uvedený počet rozpočtových a príspevkových organizácií a ostatných subjektov verejnej správy je zo spracovania údajov k 30.09.2017. Tento počet je premenlivý, pretože pri spracovaní výkazov za daný štvrťrok sú dodané údaje za novovzniknuté rozpočtové a príspevkové organizácie v pôsobnosti obcí a ďalšie organizácie nepredkladajú údaje z dôvodu zániku organizácie.

V roku 2017 bola poskytnutá používateľská podpora pri práci so systémom RIS.SAM v súčinnosti s CPU DataCentra a zabezpečenie údajov pre informačné systémy CKS (Centrálny konsolidačný systém) a RÚZ (Register účtovných závierok).

314	Správa zberov v RIS.SAM

V roku 2017 v rámci tejto úlohy v systéme RIS.SAM bola vykonávaná správa zberov

- zber Finančné výkazy (2016 Finančné výkazy IV. kvartál, 2017 Finančné výkazy I. kvartál , 2017 Finančné výkazy II. kvartál , 2017 Finančné výkazy III .kvartál), Finančné výkazy Ostatné SVS (2016 Finančné výkazy December - Ostatné SVS, 2017 Finančné výkazy Január - Ostatné SVS, ... , 2017 Finančné výkazy November - Ostatné SVS), Individuálna UZ (2016 Individuálna UZ Obce, RO, PO, 2016 Individuálna UZ Ostatné SVS), Formulár vzájomných vzťahov (2016 Formulár vzájomných vzťahov), Konsolidovaná UZ (2016 Konsolidovaná UZ Obce, RO, PO, 2016 Konsolidovaná UZ Ostatné SVS) a Mimoriadna IUZ (2017 Mimoriadna IUZ Obce, RO, PO, 2017 Mimoriadna IUZ Ostatné SVS) a to otvorenie a zatvorenie príslušného zberu podľa legislatívnych termínov a pokynov z MF SR, aktualizácia účtovných jednotiek a ich vykazovacej povinnosti v jednotlivých zberoch RIS.SAM za príslušné obdobie, kontrola prostredníctvom funkcionality v RIS.SAM o úplnosti, správnosti predložených výkazov,

- bol upravený export z RIS.SAM (údaje za jednotlivé obce a ich rozpočtové, príspevkové organizácie a ostatné subjekty verejnej správy v textovom tvare) do prostredia IT Oracle, ktorý je vstupom pre úlohu Účtovný informačný systém miestnej samosprávy (úloha 313),

- bol vytvorený export súborov zo zberu Individuálna UZ, Formulár vzájomných vzťahov a Konsolidovaná UZ a tvorba súborov v predpísanom textovom tvare pre import do CKS (Centrálny konsolidačný systém), pre rozšírenie CKS o individuálne údaje z individuálnej účtovnej závierky, formulára vzájomných vzťahov a konsolidovanej účtovnej závierky za územnú samosprávu za účelom spracovania Súhrnnej účtovnej závierky Ministerstvom financií SR.

V roku 2017 bola poskytnutá používateľská podpora pri práci so systémom RIS.SAM v súčinnosti s CPU DataCentra.

316	Informačný systém pre centrálnu evidenciu zmlúv o hypotekárnych úveroch

Pri realizácii úlohy boli za hodnotené obdobie vykonané činnosti súvisiace s ukončením prác spracovania údajov za rok 2016:

- archivácia údajov databázy centrálnej evidencie k 31. 12. 2016,
- archivácia vstupných súborov predložených hypotekárnymi bankami,
- archivácia výstupných súborov, písomností a zostáv vytvorených v DataCentre za jednotlivé mesiace roka 2016,
- pre šifrovanie údajov predkladaných za rok 2017 boli programom PGP vygenerované kľúče oprávneným osobám DataCentra a zrealizovaná výmena verejných PGP kľúčov medzi oprávnenými osobami hypotekárnych bánk, DataCentra a MF SR potvrdená písomným protokolom.

Údaje o hypotekárnych úveroch sú do centrálnej evidencie predkladané v zmysle zákona o bankách na zistenie viacnásobného uplatnenia nároku na poskytnutie štátneho príspevku a štátneho príspevku pre mladých poberateľom hypotekárneho úveru.

Pri priebežnom mesačnom plnení úlohy boli údaje do centrálnej evidencie predkladané z hypotekárnych bánk formou šifrovaných elektronických súborov. Po overení platnosti elektronického podpisu bola vykonaná kontrola vstupných údajov. Nezrovnalosti v štruktúre, formáte a nedostatky vo vecnej správnosti predložených údajov boli oznámené príslušnej bank a po oprave a opätovnom predložení súboru korektných údajov zo strany bánk boli údaje spracované v zmysle požiadaviek MF SR.

Mesačné spracovanie údajov centrálnej evidencie zmlúv je vykonávané s cieľom vyhodnotiť nárok poberateľa úveru na poskytnutie štátneho príspevku samostatne za hypotekárne úvery so štátnym príspevkom a hypotekárne úvery so štátnym príspevkom pre mladých. Súčasťou spracovania bola mesačne vypočítavaná celková suma nárokovaného štátneho príspevku v eurách za jednotlivé banky a typ úveru. Vzniknuté rozdiely v celkovej výške nárokovaného štátneho príspevku vypočítaného z údajov centrálnej evidencie a skutočne nárokovaného štátneho príspevku hypotekárnymi bankami boli konzultované s oprávnenými osobami jednotlivých bánk. Následne došlo k zosúladeniu sumy nárokov na štátny príspevok za príslušné obdobie spracovania.

Štandardné výstupné zostavy boli predkladané na MF SR a hypotekárnym bankám opäť formou šifrovaných elektronických súborov. Písomné požiadavky na opravu údajov zo strany bánk boli so súhlasom MF SR priebežne zrealizované v databáze údajov centrálnej evidencie.

K mimoriadnym požiadavkám MF SR boli vyčíslené údaje o priemerných hodnotách vybraných položiek z evidencie štátneho príspevku pre mladých a údaje podľa katastrálneho územia. Mimoriadne výstupné zostavy boli vypracované pre potreby analýzy stavu poskytovania štátneho príspevku realizovanej Inštitútom finančnej politiky. Pre odbor štátneho dozoru MF SR bola vykonaná analýza údajov centrálnej evidencie pre výkon štátneho dozoru pri čerpaní prostriedkov zo štátneho rozpočtu určených na štátny príspevok k hypotekárnym úverom. Analýza predmetných údajov sa týkala zmlúv, ktoré boli do centrálnej evidencie predložené SLSP, a.s. a UniCredit Bank Czech Republic and Slovakia, a.s. za obdobie špecifikované v požiadavke odboru štátneho dozoru MF SR.

317	Podpora používateľov pri práci s aplikáciami IS ŠP - AP IS SŠP (modul *Výkazníctvo)*

DataCentrum aj v roku 2017 plnilo úlohu zabezpečenia pomoci koncovým používateľom pri používaní informačného systému ŠP, zabezpečovalo aplikačnú podporu v module Výkazníctvo pre koncových používateľov modulu, odhaľovanie nekorektností a disfunkcionalít v aplikácii, zber a odovzdávanie námetov pre ďalší rozvoj tohto informačného systému.

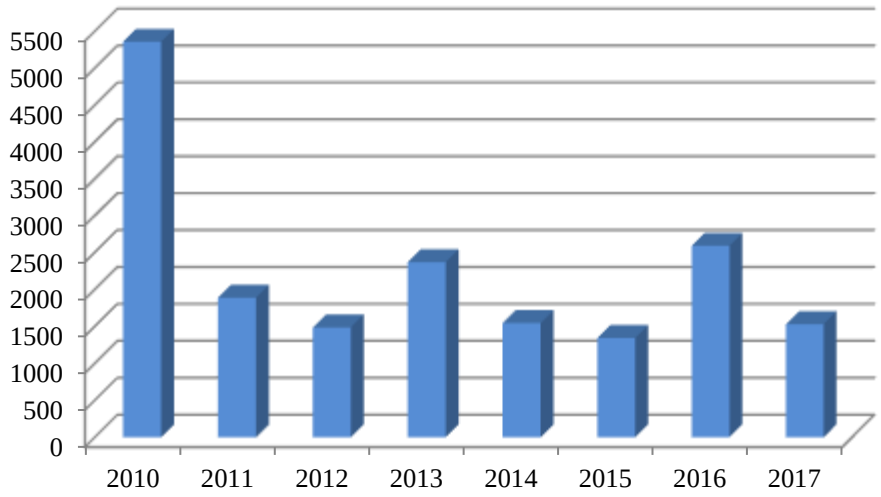
Pomoc používateľom modulu IS SŠP *Výkazníctvo* bola zabezpečovaná prostredníctvom metodického a organizačného usmernenia a komunikáciou s riešiteľmi na tretej úrovni podpory za účelom vyriešenia používateľského problému. Zaznamenávané boli aj používateľské pripomienky a požiadavky ako námety pre analýzy pre potreby rozvoja IS a bola budovaná databáza často kladených otázok a odpovedí. Plnenie úlohy sa realizovalo v úzkej spolupráci s ostatnými úrovňami a skupinami CPU.

Modul *Majetok* nebol využívaný v rutinnej prevádzke a tak nevznikali ani požiadavky na poskytovanie podpory používateľov pri práci s ním.

Celkový počet hlásení týkajúcich sa aplikačnej podpory modulu IS SŠP pre Výkazníctvo je v porovnaní s ostatnými rokmi nasledovný:

Modul	2010	2011	2012	2013	2014	2015	2016	2017
Výkazníctvo	5357	1890	1488	2370	1547	1346	2592	**1530**
Majetok	0	0	0	0	0	0	0	**0**

Počet uzatvorených hlásení k výkazníctvu v porovnaní s predchádzajúcimi rokmi:



318	Podpora používateľov pri práci a aplikáciami IS SŠP (modul *Riadenie výdavkov -ManEx*)

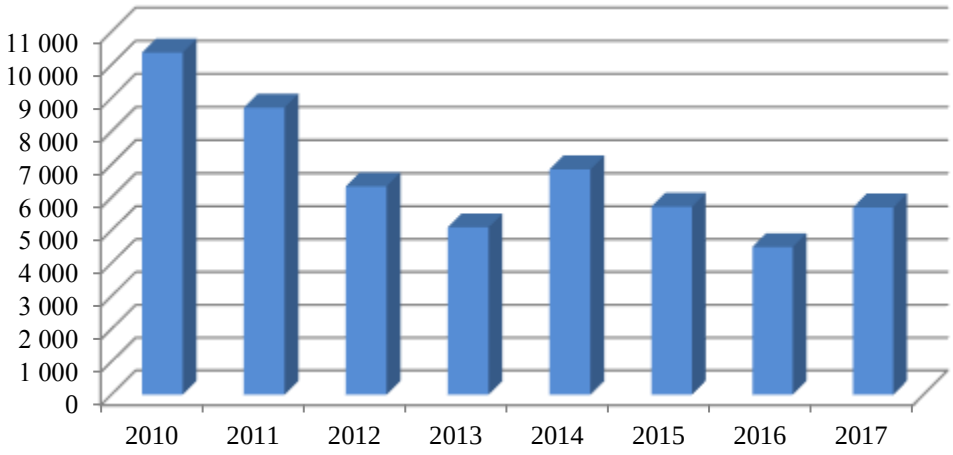
V hodnotenom období plnilo DataCentrum úlohu podpory používateľov zabezpečením pomoci koncovým používateľom pri používaní Informačného systému pre systém štátnej pokladnice, zabezpečením správy a prevádzky systému, zabezpečením aplikačnej podpory v module *Riadenia výdavkov* pre koncových používateľov modulu, odhaľovaním nekorektností a disfunkcionalít v aplikácii, zberom a odovzdávaním námetov pre ďalší rozvoj tohto informačného systému a participovalo tiež na spolupráci riešiteľov systémov RIS a IS SŠP.

Pomoc používateľom modulu IS SŠP pre riadenie výdavkov (ManEx) bola realizovaná prostredníctvom telefonickej komunikácie a priamou navigáciou na obrazovke. Používateľom boli sprostredkovávané metodické a organizačné usmernenia a komunikácia s riešiteľmi na tretej úrovni podpory za účelom vyriešenia používateľského problému. Okrem toho boli zaznamenávané používateľské pripomienky a požiadavky ako námety pre analýzy pre potreby rozvoja IS a bola budovaná databáza často kladených otázok a odpovedí. Plnenie úlohy sa realizovalo v úzkej spolupráci s ostatnými úrovňami a skupinami CPU.

Celkový počet hlásení týkajúcich sa aplikačnej podpory modulu IS SŠP pre riadenie výdavkov ManEx je nasledovný:

Modul	2010	2011	2012	2013	2014	2015	2015	2016	2017
Riadenie výdavkov	10 381	8 717	6 336	5 097	6 851	5 728	5 728	4 493	**5 701**

Počet hlásení súvisiacich s riadením výdavkov v porovnaní s predchádzajúcimi rokmi:



321	Spracovanie údajov o dani z nehnuteľností

V rámci úlohy boli zapracované zmeny do programového vybavenia úlohy pre spracovanie údajov z Výkazov o dani z nehnuteľností za rok 2016 v prostredí RIS SAM v súlade s opatrením Ministerstva financií SR z 9. novembra 2016 č. MF/015062/2016-726, ktorým sa stanovujú podrobnosti o predkladaní a poskytovaní údajov o dani z nehnuteľností.

DataCentrum zabezpečilo príjem elektronických formulárov. Spolu bolo doručených 2 839 výkazov, ktoré boli skontrolované a spracované podľa požiadaviek MF SR.

Boli vytvorené výstupy v papierovej forme - tabuľková časť obsahovala spracované údaje za Slovenskú republiku, kraje a okresy SR za rok 2016 a grafická časť obsahovala prehľad vývoja jednotlivých ukazovateľov za Slovenskú republiku a kraje za roky 2008 až 2016. Boli vytvorené výstupy aj v elektronickej forme v podobe súboru *pdf. Súbor v *pdf formáte obsahoval presne to čo výstupy v papierovej forme.

Na základe požiadavky bol:

- Inštitútu finančnej politiky vypracovaný a odoslaný súbor za ukazovatele: „ Daň z pozemkov, Daň zo stavieb, Daň z bytov a Daň z nehnuteľností spolu členený podľa obcí za rok 2016“,
- pre Ministerstvo pôdohospodárstva a rozvoja vidieka SR vypracovaný výber, ktorý obsahoval: Výsledky štatistického výkazu o dani z nehnuteľností za rok 2016 z časti „2. Daň z pozemkov“ v rozsahu ukazovateľov stĺpcov 1 až 9 za ornú pôdu, chmeľnice, vinice, ovocné sady, trvalé trávne porasty, záhrady a lesné pozemky, na ktorých sú hospodárske lesy v členení podľa obcí, okresov, krajov a spolu za SR,
- pre Technickú univerzitu vo Zvolene - Lesnícku Fakultu - Katedru ekonomiky a riadenia lesného hospodárstva vypracovaný výber, ktorý obsahoval: Výsledky štatistického výkazu o dani z nehnuteľností za rok 2013 – 2016 z časti „2. Daň z pozemkov“ v rozsahu ukazovateľov riadok 1, 2, 6, 7, 9 a všetky stĺpce, čiže 1 až 9 v bloku 2 daň z pozemkov. Okrem toho identifikačné údaje: kód okresu, IČO obce, kód obce, názov obce. Ďalej údaje o počte daňovníkov v bloku 1: počet daňovníkov obce spolu, počet daňovníkov oslobodených od dane z pozemkov, počet obyvateľov obce k 1. januáru zdaňovacieho obdobia.

323	Informačný systém pre centrálnu evidenciu zmlúv o stavebnom sporení

K lepšiemu hospodáreniu s prostriedkami štátneho rozpočtu prispievajú aj výsledky informačného systému pre centrálnu evidenciu a priebežné hodnotenie zmlúv o stavebnom sporení, pri ktorých sa uplatňuje nárok na štátnu prémiu u registrovaných stavebných sporiteľní. V rámci tejto úlohy boli pre zabezpečenie ochrany osobných údajov začiatkom roka vygenerované, vymenené a archivované verejné PGP kľúče oprávnených osôb na MF SR, v DataCentre a za bankové subjekty zapojené do prevádzky IS pre centrálnu evidenciu zmlúv o stavebnom sporení v roku 2017.

Mesačne boli vypracovávané štandardné výstupy z prémiovo zvýhodnených zmlúv fyzických osôb a štandardné výstupy z prémiovo zvýhodnených zmlúv právnických osôb za obdobia 12/2016 – 11/2017 pre MF SR. Pri spracovaní údajov boli zisťované počty nových stavebných sporiteľov a zmlúv za jednotlivé stavebné sporiteľne, odhalené viacnásobné nároky na poskytované výhody stavebného sporenia v rôznych stavebných sporiteľniach.

Tiež boli mesačne vypracovávané štandardné výstupy z prémiovo zvýhodnených zmlúv fyzických osôb a štandardné výstupy z prémiovo zvýhodnených zmlúv právnických osôb za obdobie 12/2016 – 11/2017 pre stavebné sporiteľne.

Bol vypracovaný výstup zo spracovania oprávnených finančných nárokov fyzických osôb a výstup zo spracovania oprávnených finančných nárokov právnických osôb za rok 2016 pre MF SR a aktualizácia programového vybavenia informačného systému platného od 1. 1. 2017.

Bola prevedená archivácia centrálnej databázy stavebných sporiteľov za rok 2016, vstupných a výstupných súborov a programového vybavenia úlohy za rok 2016.

341	Účtovný informačný systém právnických a fyzických osôb účtujúcich v sústave podvojného účtovníctva

V rámci tejto úlohy boli v roku 2017 vykonané nasledovné činnosti:

- bol aktualizovaný ročný harmonogram úlohy pre príjem, spracovanie a poskytovanie údajov zo súčastí riadnych účtovných závierok podnikateľov a mikroúčtovných jednotiek:

  a) za rok 2015: Súvaha Úč POD 1-01 a Výkaz ziskov a strát Úč POD 2-01 za účtovné obdobie hospodárskeho roka 2014/2015, Súvaha Úč POD 1-01, Výkaz ziskov a strát Úč POD 2-01, Súvaha Úč MÚJ 1-01 a Výkaz ziskov a strát Úč MÚJ 2-01 za účtovné obdobie kalendárneho roka 2015;

  b) za rok 2016: Súvaha Úč POD 1-01, Výkaz ziskov a strát Úč POD 2-01, Súvaha Úč MÚJ 1-01 a Výkaz ziskov a strát Úč MÚJ 2-01 za účtovné obdobie hospodárskeho roka 2015/2016 a kalendárneho roka 2016;

- údaje za rok 2015 boli priebežne preberané z Registra účtovných závierok (RÚZ) vo forme .csv súborov. Bolo ukončené štandardné spracovanie týchto údajov v celkovom objeme 199 504 súvah a výkazov ziskov a strát.

- konečný počet disponibilných údajov v rezortnej databáze je 195 210 dvojíc výkazov za rok 2015, z toho je 89 % správnych a 11 % chybných,

- bol vytvorený pracovný register účtovných jednotiek SR, v ktorom boli účtovným jednotkám so správnymi údajmi priradené štatistické klasifikácie,

- boli vytvorené nové a aktualizované existujúce programové aplikácie pre spracovanie údajov za rok 2015 a pre tvorbu výstupov agregovaných a individuálnych údajov v zmysle požiadaviek odberateľov,

- boli vytvorené a poskytnuté výstupy vo forme súborov agregovaných údajov, individuálnych údajov a individuálnych anonymizovaných údajov za rok 2015:

  a) pre MF SR: Generálny tajomník služobného úradu (pre externých odberateľov, s ktorými MF SR uzatvorilo zmluvu o poskytovaní údajov), Odbor pre legislatívu a metodiku účtovníctva - operatívne;

  b) pre ŠÚ SR v zmysle zmluvy;

  c) pre Slovak Business Agency v zmysle zmluvy, poverenia MF SR a objednávky;

  d) externému odberateľovi v zmysle objednávky;

- bolo dohodnuté s FR SR poskytnutie vybraných údajov za zdaňovacie obdobie 2016 z centrálneho registra daňových subjektov PO a FO a z evidencie o subjektoch s hospodárskym rokom; bola aktualizovaná príloha zmluvy k odberu údajov za rok 2016, uzavretá medzi DataCentrom a ŠÚ SR; bol aktualizovaný dodatok zmluvy k odberu údajov za rok 2016, uzavretý medzi DataCentrom a Slovak Business Agency;

- bola zabezpečená príprava Účtovného IS právnických a fyzických osôb účtujúcich v sústave podvojného účtovníctva pre spracovanie údajov zo súčastí účtovných závierok Úč POD a Úč MÚJ, ktorá predstavovala aktualizáciu existujúcich parametrov a programových aplikácií pre nové účtovné obdobie,

- bolo uskutočnené štandardné spracovanie údajov v objeme 205 517 súvah a výkazov ziskov a strát za rok 2016 preberaných z RÚZ. Z disponibilného počtu dvojíc výkazov 202 576 ku dňu 31.12.2017 bolo 90 % správnych a 10 % chybných. Spracovanie údajov predstavovalo: príjem údajov, nahrávanie údajov do rezortnej databázy, formálne a logické kontroly údajov, identifikáciu a záznam zistených chýb, rozdelenie údajov na správne, chybné a vylúčené, doplnenie chýbajúcich identifikačných kódov IČO, právnej formy a i., tvorba pracovného registra účtovných jednotiek so správnymi údajmi a priradenie štatistických klasifikácií týmto účtovným jednotkám. V zmysle požiadaviek ŠÚ SR boli do spracovania zaradené aj údaje nepodnikateľských subjektov, ktoré mali kód „11“ pre Nefinančné korporácie v položke sektorového členenia ESA v registri organizácií ŠÚ SR (od r. 2013). Súčasťou výstupov pre ŠÚ SR je aj protokol o najčastejšie sa vyskytujúcich chybách v súčastiach účtovných závierok Úč MÚJ a Úč POD.

- boli aktualizované existujúce programové aplikácie pre spracovanie údajov za rok 2016 a pre tvorbu výstupov agregovaných a individuálnych údajov v zmysle požiadaviek odberateľov,

- vo viacerých etapách boli vytvárané a poskytované výstupy vo forme súborov agregovaných údajov, individuálnych údajov a individuálnych anonymizovaných údajov za rok 2016:

  a) pre MF SR: Generálny tajomník služobného úradu (pre externých odberateľov, s ktorými MF SR uzatvorilo zmluvu o poskytovaní údajov);

  b) pre ŠÚ SR v zmysle zmluvy;

  c) pre Slovak Business Agency v zmysle poverenia MF SR a objednávky;

  d) pre NKÚ SR v zmysle objednávok;

  e) externému odberateľovi v zmysle objednávok;

- nad rámec kontraktu bolo zabezpečené preberanie skenov z RÚZ z Výkazov vybraných údajov z individuálnej účtovnej závierky podľa § 17a Zákona č. 431/2002 Z .z. o účtovníctve v znení neskorších predpisov, t. j. za spoločnosti, ktoré zostavujú účtovnú závierku podľa medzinárodných účtovných štandardov, a manuálne prepísanie údajov do preddefinovaných tabuliek. Manuálne boli vyťažené údaje z výkazov: VÚ POD 1-01, VÚ-B 1-01 a VÚ-P 1-04 za rok 2016 v počte 152 ks, ktoré boli spätne importované do RÚZ.

342	Účtovný informačný systém účtovných výkazov podnikateľskej sféry fyzických osôb účtujúcich v sústave jednoduchého účtovníctva

V prvom polroku 2017 boli preberané údaje prostredníctvom exportu dát z Registra účtovných závierok (RÚZ). Spracovanie týkajúce sa nahrávania, kontroly a korekcie určitého typu chýb prebehlo pre účtovné závierky roku 2015. Za účelom spresnenia identifikácie subjektov sme používali aj údaje z registra daňových platcov, ktorý sme si vyžiadali z FR SR. Na záver spracovania účtovného obdobia roku 2015 bola uskutočnená archivácia údajov ako aj registra účtovných jednotiek so štatistickými klasifikáciami do prezentačnej vrstvy v konečnom rozsahu 132 073 dvojíc výkazov.

Odberateľom zo ŠÚ SR boli poskytnuté agregované výstupné zostavy vytvorené z údajov ÚIS FO za rok 2015, ako aj súbory individuálnych dát reprezentujúcich toto obdobie vo dvoch dávkach. V januári to boli priebežné a koncom apríla definitívne výstupy.

Na konci prvého polroka boli prebraté údaje z RÚZ za účtovné výkazy Úč FO 2016.

Z týchto dát v objeme cca 102 tisíc subjektov boli vytvorené individuálne výstupy pre potreby Odboru analýz a syntéz ŠÚ SR.

Na začiatku 2. polroka podľa požiadavky Ministerstva pôdohospodárstva a rozvoja vidieka SR im boli odovzdané výbery z údajov za roky 2015 a 2016.

V 2. polovici roka pokračovalo priebežné preberanie údajov z výkazov za rok 2016 umiestnených v RÚZ. Prevzaté údaje sme pre potreby našej databázy aktualizovali prostredníctvom údajov z registrov dodávaných Štatistickým úradom SR a Finančným riaditeľstvom SR. Štandardné spracovanie sa ku koncu roka týkalo približne 121 tisíc dvojíc výkazov.

V niekoľkých dávkach v priebehu roka sme poskytovali výbery údajov za účtovné závierky rokov 2015 a 2016 pre firmu Centaurus ako aj pre ďalších odberateľov zo súkromného sektoru (SIMS, CRIF-SCB), s ktorými MF SR uzavrelo zmluvy o poskytovaní údajov. Pre Slovak Bussiness Agency boli zrealizované agregované výstupy z údajov výkazov Úč FO v marci za rok 2015 a v novembri prvá dávka anonymizovaných individuálnych údajov FO za rok 2016. Ministerstvu hospodárstva boli odovzdané anonymizované individuálne údaje z výkazov ÚčFO 2015 na základe nimi stanovených výberových kritérií vo dvoch dávkach, z predbežných aj z definitívnych údajov.

Pre odberateľov zo ŠÚ SR z Odboru sektorových účtov boli v 2. polroku vo dvoch dávkach vytvorené agregované výstupy podľa ich požiadaviek, súčasne s nimi sme poskytli rovnako vo dvoch dávkach Odboru metodiky registra a klasifikácií ŠÚ SR individuálne dáta výkazov Úč FO 1-01 a Úč FO 2-01 vytvorené zvlášť z údajov bezchybných a z údajov chybových. Odovzdávanie údajov pre všetkých odberateľov zo ŠÚ SR počas celého roka prebiehalo ftp prenosom.

Priebežne počas roka podľa našich potrieb dochádzalo ku konzultáciám s pracovníkmi Odboru pre legislatívu a metodiku účtovníctva MF SR.

343	Účtovný informačný systém neziskových účtovných jednotiek účtujúcich v sústave podvojného účtovníctva

V rámci tejto úlohy prebiehalo sťahovanie naskenovaných súborov z Registra účtovných závierok (RÚZ) za účtovné obdobie roku 2016, určených na typovanie a ich následná distribúcia medzi externé zdroje. Boli vypracované pracovné tabuľky za účelom evidencie natypovaných údajov z účtovných výkazov typu Úč NUJ 1–01 a Úč NUJ 2–01.

Boli zaktualizované metadátové tabuľky parametrov a príprava skriptov pre vytvorenie výstupných súborov typu .csv a vypracované výstupné súbory pre ŠÚ SR podľa zadaných požiadaviek – finálne údaje za rok 2015.

Priebežne pokračovalo sťahovanie skenov z RÚZ, ich typovanie a následné nahrávanie do RÚZ. Po skončení nahrávania skenov boli všetky údaje z RÚZ stiahnuté a nahraté do tabuliek disponibilnej DB centrálneho databázového systému v prostredí IT Oracle. V databáze bolo potrebné urobiť korekcie kvôli duplicitám a chybným identifikáciám. Boli vypracované výstupné súbory pre Štatistický úrad SR: údaje za rok 2016 z účtovných výkazov Súvaha Úč NUJ 1-01, Výkaz ziskov a strát Úč NUJ 2-01, zoznam spravodajských jednotiek, ktoré predložili výkazy Úč NUJ 1-01 a Úč NUJ 2-01, zoznam agregačných položiek použitých pri agregácii za požadované kategórie za výkazy Úč NUJ 1-01, Úč NUJ 2-01, individuálne údaje z účtovných výkazov Súvaha Úč NUJ 1-01 a Výkaz ziskov a strát Úč NUJ 2-01 za dobré a chybové údaje, zoznam spravodajských jednotiek, ktoré sa nenachádzajú v registri ŠÚ SR rozdelený na dva súbory .xls: dobré a chybné. Výstupné zostavy pre ŠÚ SR boli vytvorené v dvoch termínoch: k 31.8.2017 a k 31.12.2017.

344	Účtovný informačný systém účtovných výkazov neziskovej sféry - jednoduché účtovníctvo

V rámci tejto úlohy bola v roku 2017 vykonaná archivácia výkazov a údajov v databáze za výkazy Úč NO 1-01 a Úč NO 2-01 k 31. 12. 2015. ŠÚ SR boli odovzdané finálne zostavy za výkazy za rok 2015. Zároveň boli zaktualizované metadátové tabuľky parametrov a príprava skriptov pre výstupné zostavy pre ŠÚ SR. Boli vypracované pracovné tabuľky za účelom evidencie natypovaných údajov z účtovných výkazov typu Úč NO 1–01 a Úč NO 2–01. Počas celého obdobia prebiehalo sťahovanie naskenovaných výkazov z Registra účtovných závierok za rok 2016 určených na typovanie. Bola zabezpečená ich distribúcia, prevod do elektronickej podoby a následná aktualizácia Registra účtovných jednotiek. Pre potreby ŠÚ SR boli stiahnutými údajmi z Registra účtovných závierok naplnené databázové tabuľky v prostredí Oracle. Po doplnení a natypovaní dodatočne predložených výkazov bola uskutočnená aktualizácia databázových tabuliek, oprava chybných identifikácií výkazov v súlade s Registrom ŠÚ SR a Daňovým registrom a oprava opraviteľných chýb vo výkazoch. Výstupné zostavy boli odovzdané ŠÚ SR v dvoch termínoch: k 31.8. 2017 a k 31.12.2017.

345	Správa a spracovanie údajov registrov a číselníkov pre ÚIS účtovných výkazov podnikateľskej a neziskovej sféry

V priebehu prvého polroka 2017 bolo uskutočnené prevzatie a spracovanie údajov registra priestorových jednotiek, registra ekonomických subjektov zo ŠÚ SR za rok 2016 ako aj číselníkov prislúchajúcich tomuto registru a nahrané do prostredia Oracle, z FR SR boli prevzaté daňové registre organizácií za právnické a fyzické osoby za rok 2016, ktoré boli nahrané do prostredia Oracle a bol aktualizovaný register ekonomických subjektov podľa požiadaviek užívateľov.

351	Hlásenie o spotrebiteľských úveroch

V rámci tejto úlohy boli prijaté údaje o novoposkytnutých spotrebiteľských úveroch od všetkých veriteľov, ktoré sú z MF SR elektronickou poštou predkladané DataCentru v súboroch vo formáte .xml, ich kontrola a vyhodnotenie. Následne boli z týchto údajov vypočítané objemy novoposkytnutých spotrebiteľských úverov a kreditných kariet kumulatívne za všetkých veriteľov a osobitne za banky a pobočky zahraničných bánk, priemerné hodnoty RPMN (ročná percentuálna miera nákladov) za jednotlivé typy novoposkytnutých spotrebiteľských úverov (jedná sa o vážené priemery za všetkých veriteľov pričom váhovou informáciou je príslušný objem jednotlivých typov novoposkytnutých spotrebiteľských úverov) a osobitne za banky a pobočky zahraničných bánk. Zo súhrnnej tabuľky bol urobený výpočet vážených priemerov RPMN za jednotlivé obdobia zmluvnej splatnosti od 3 do 6 mesiacov, od 6 do 12 mesiacov, od 1 do 5 rokov, od 5 do 10 rokov, od 10 rokov a za jednotlivé typy spotrebiteľských úverov.

V roku 2017 bolo uskutočnené spracovanie údajov za 4.štvrťrok 2016, 1.štvrťrok, 2. štvrťrok a 3. štvrťrok 2017, pričom boli vypracované a odovzdané na MF SR súhrnné tabuľky, vrátane zoznamu subjektov, ktorých údaje boli do nich zahrnuté.

Za každého veriteľa sa vypočítal priemerný objem novoposkytnutých spotrebiteľských úverov a kreditných kariet za každý štvrťrok 2017.

352	Informačný systém pre centrálnu evidenciu zmlúv o mladomanželských úveroch

Za hodnotené obdobie boli pri plnení úlohy zrealizované činnosti súvisiace s ukončením prác spracovania údajov za rok 2016: archivácia údajov databázy centrálnej evidencie k 31. 12. 2016, archivácia vstupných súborov predložených bankami a výstupných súborov vytvorených v DataCentre za jednotlivé mesiace roka 2016. Pre rok 2017 boli šifrovacím programom PGP vygenerované kľúče oprávneným osobám DataCentra a zrealizovaná výmena verejných PGP kľúčov medzi oprávnenými osobami bánk, DataCentra a MF SR potvrdená písomným protokolom.

Údaje o mladomanželských úveroch sú do centrálnej evidencie predkladané v zmysle zákona o bankách na účel zistenia prípadného viacnásobného uplatnenia nároku na poskytnutie štátneho príspevku poberateľom mladomanželského úveru.

Pri priebežnom mesačnom spracovaní boli údaje predkladané do centrálnej evidencie z bánk formou šifrovaných elektronických súborov. Po overení platnosti elektronického podpisu bola vykonaná kontrola vecnej správnosti predložených údajov. Následne bolo vykonané spracovanie v zmysle požiadaviek MF SR.

Predmetom mesačného spracovania údajov centrálnej evidencie mladomanželských úverov bolo vyhodnotiť nárok na štátny príspevok a vypočítať výšku sumy nárokovaného štátneho príspevku za každú banku. Štandardné výstupné zostavy boli predkladané na MF SR a príslušným bankám formou šifrovaných elektronických súborov.

Pre odbor štátneho dozoru MF SR bola vykonaná analýza údajov centrálnej evidencie pre výkon štátneho dozoru pri čerpaní prostriedkov zo štátneho rozpočtu určených na štátny príspevok k mladomanželským úverom. Analýza predmetných údajov sa týkala zmlúv, ktoré boli do centrálnej evidencie predložené UniCredit Bank Czech Republic and Slovakia, a. s. za obdobie špecifikované v požiadavke odboru štátneho dozoru MF SR.

401	Technologická infraštruktúra dátovej sály MF SR

DataCentrum zabezpečovalo prevádzkové potreby technologickej infraštruktúry dátovej sály MF SR a realizovalo potrebnú odbornú starostlivosť o technologické zariadenia.

Zo strany DataCentra bolo zabezpečené vykonávanie pravidelných servisných prehliadok, servisná pohotovosť a riešenie servisných prípadov a opráv.

Bola zaktualizovaná relevantná prevádzková dokumentácia.

Všetky požadované činnosti sú zabezpečované a vykonávané v súčinnosti zamestnancov DataCentra s dodávateľom služieb.

402	Technická, komunikačná a systémová podpora projektov

Popri štandardnej každodennej administrácii ako je kontrola logov, diskových subsystémov, používateľských kont, zálohovania, riešenie incidentov prevádzky, riešenie hardvérových problémov atď., boli v roku 2017 v jednotlivých oblastiach činností vykonané nasledujúce aktivity:

Správa operačných systémov Windows server

V rámci správy operačných systémov Windows server boli prevádzkované dve oddelené domény pre správu počítačov a používateľov, fileserver, tlačové služby, poštový server, intranet, certifikačná autorita, servery pre monitoring prevádzky, zálohovanie, dochádzkový server. Priebežne boli vykonávané bežné administrátorské činnosti zamerané na predchádzanie výpadkov, ako je kontrola logov, diskových subsystémov, ďalej administrácia používateľských účtov. Aplikovali sa skupinové politiky podľa prevádzkových a bezpečnostných požiadaviek, vykonávalo sa zálohovanie, podpisovanie certifikátov, riešenie incidentov prevádzky, riešenie hardvérových a softvérových problémov, antivírová ochrana serverov a pracovných staníc, podpora používateľov, kontrola pracovných staníc prostredníctvom System Center Configuration Manager a aktualizácia

operačných systémov serverov a pracovných staníc prostredníctvom Windows Server Update Services. Zabezpečovali sa plánované odstávky a bezproblémový nábeh po odstávkach. Všetky zmeny operačných systémov boli zapracované do Centrálneho monitoringu prevádzky.

Na začiatku roku 2017 boli rozšírené diskové kapacity fileservera, V rámci adresárovej štruktúry fileservera sa riešili zmeny prístupových práv podľa potrieb a požiadaviek. Pre účely projektu monitorovania a riadenia bezpečnostných systémov bol pripravený server, bola poskytnutá súčinnosť pri inštalácii softvéru a server bol zahrnutý do správy operačných systémov.

Pripravil sa server pre upgrade dochádzkového systému, bola poskytnutá súčinnosť pri inštalácii softvéru a server bol zahrnutý do správy operačných systémov.

Správa domény *(Active Directory)*

Spravovali sa dve domény - jedna pre interných, druhá pre externých zamestnancov. V rámci úlohy sa vytvárali účty novým zamestnancom, zakazovali sa účty zamestnancom, ktorí odišli, menili sa prístupové práva preradeným zamestnancom, riešili sa zmeny prístupových práv podľa potrieb a požiadaviek a zabezpečovala sa konfigurácia DHCP a rezervácia IP adries podľa požiadaviek.

V priebehu roka sa poskytovala podpora doménovým používateľom a cez doménové politiky sa riešili prístupové práva používateľských účtov na zdroje v doméne, či už pri vytváraní účtu, preraďovaní zamestnanca alebo ďalších oprávnení k zdieľaným prostriedkom. Cez doménové politiky sa riešilo členstvo počítačov v skupinách tak, aby bola zabezpečená aktualizácia operačných systémov pracovných staníc. Boli implementované doménové politiky podľa požiadaviek bezpečnosti.

Správa operačných systémov Linux

V priebehu roku 2017 prebiehala potrebná aktualizácia operačných systémov Linux.

Okrem toho:

- upravovali sa a pridávali sa nové zónové konfigurácie na DNS serveroch podľa požiadaviek a potrieb používateľov a boli zrušené už neaktuálne DNS záznamy,
- zabezpečovalo sa monitorovanie v Konzole 2,
- na proxy serveri boli v rámci posilnenia bezpečnosti vytvorené nové politiky na obmedzenie internetu v DataCentre,
- v rámci ďalších nových projektov boli na VMware postavené nové servre; niektoré servre boli zrušené, nakoľko sa služby, ktoré poskytovali, zmigrovali
- bol zmenený, presunutý a začlenený web dzn.datacentrum.sk do webu datacentrum.sk

Naďalej bola vykonávaná profylaktika Unixových serverov a ich monitoring a za podpory dodávateľa:

- sa vytvárali účty novým zamestnancom, zakazovali účty zamestnancom, ktorí odišli, menili sa prístupové práva preradeným zamestnancom,
- riešila sa podpora doménových používateľov a prístupové práva používateľských účtov na zdroje v doméne, či už pri vytváraní účtu, preraďovaní zamestnanca alebo jeho priradení na riešenie určitého projektu.

Správa databáz a databázových serverov

Cieľom administrácie databáz je správa testovacieho a produkčného databázového prostredia, poskytovanie databázových služieb používateľom a technická podpora riešiteľov úloh. Na základe toho:

- sa vytvárali denné a týždenné riadne zálohy databáz a kontrolovali sa logy priebehu zálohovania; zálohovali sa príslušné archívne redology; vytvárali sa mimoriadne zálohy vybraných užívateľských objektov a ich obnova,
- priebežne boli inštalované patche pre databázový server a vykonával sa plánovaný reštart databáz,
- bola vykonaná archivácia údajov a pripravené prostredie pre spracovanie údajov ďalšieho účtovného obdobia,
- bola monitorovaná veľkosť a využitie tabuľkových priestorov, pričom neobsadený priestor bol dealokovaný,
- vykonala sa synchronizácia testovacieho a produkčného prostredia,
- boli sledované auditné záznamy databázových operácii a obsah alertlogov,
- bol vykonaný upgrade weblogic aplikačného servera, middleware a JAVA prostredia,
- boli inštalované patche Weblogic aplikačného servera a middleware
- podľa požiadaviek používateľov bolo modifikované produkčné a testovacie prostredie, bola poskytnutá podpora pre rozšírenie funkcionality aplikácie účtovného IS,
- na používateľských PC bol nainštalovaný softvér pre operačný systém Windows7 –Forms a Reports Builder, Oracle databázový klient, JAVA, softvér prístup do operačného systému servera, vývojové prostredie PL SQL developer,
- operatívne je používateľom databáz poskytovaná technická podpora.

Evidencia licencií Oracle produktov a ich maintenance podľa jednotlivých IS je priebežne udržiavaná a údaje sú poskytované ako podklady pre obnovenie maintenance a nákup nových licencií.

Administrácia LAN, WAN a redakčných systémov

Na prístupovej infraštruktúre DataCentra, ktorú využívajú používatelia pri prístupe ku aplikáciám z verejnej siete, prebehli a v súčasnej dobe stále ešte prebiehajú zmeny, ktorých účelom je zvýšiť priepustnosť a bezpečnosť tejto infraštruktúry. Prevádzané zmeny majú za úlohu zvýšenie ochrany samotných aplikácií i zabezpečenia prístupu k nim. Súčasťou týchto zmien je výmena prepínačov za prepínače s rozhraniami s vyššou prenosovou rýchlosťou (1Gbit/s), výmena už nepodporovanej firewallovej technológie za novú, podporovanú, s lepšími parametrami (rýchlosť rozhraní, firewallová priepustnosť, počet konkurentných spojení, atď.). Za účelom prevencie proti útokom sú prevádzkované intrusion prevention zariadenia, ktoré chránia

aplikácie pred útokmi z Internetu aj z vnútorných sietí na nižších vrstvách. Súčasťou prevádzaných zmien bol aj redizajn sieťovej topológie infraštruktúry za účelom jej zabezpečenia.

Z dôvodu zvyšovania bezpečnosti prístupovej siete používateľov sa začali nasadzovať nové prepínače s vyšším počtom portov, vyššou mierou zabezpečenia proti útoku zo strany používateľa a možnosťou vzdialenej správy.

Na základe požiadaviek systémov prevádzkovaných v DataCentre bola na počítačovej sále rozšírená optická a metalická dátová kabeláž v potrebnom množstve.

Na začiatku roka bolo doladené novonasadené kontaktné centrum pre CPU.

Správa systémov IPS

V hodnotenom období sa na bezpečnostných intrusion prevention zariadeniach vykonávali rutinné a štandardné činnosti súvisiace s administráciou týchto systémov. Každodenne bol monitorovaný stav jednotlivých bezpečnostných sond a bola vykonávaná aktualizácia reputačných databáz. Každý týždeň boli vykonávané aktualizácie Digitálnych vakcín a Auxiliary vakcín s následnou konfiguráciou jednotlivých bezpečnostných signatúr.

Kontrola udalostí, ktoré boli zaznamenané do centrálnej konzoly nezistila žiaden úspešný útok na monitorované súčasti infraštruktúry DataCentra, keďže u väčšiny bolo zistené že sa jedná o udalosť typu „false positive“, resp. o legálnu a povolenú komunikáciu niektorej aplikácie smerom z / do siete DataCentra, prípadne o udalosti ktoré boli vyvolané rôznymi agresívnymi reklamami na internetových stránkach.

V Októbri bola vykonaná výmena fyzických IPS zariadení, nakoľko bola odhalená výrobná chyba v pamäťovom module, ktorá spôsobovala náhodné reštartovanie zariadenia. Výmena prebehla v spolupráci s dodávateľom v rámci SLA.

Správa Lotus Domino serverov

Vykonávala sa štandardná údržba Lotus Domino servera, prebiehala administrácia poštových schránok a webových služieb.

Správa webových a aplikačných služieb servera Lotus Domino

Web server pracoval vo virtuálnom prostredí, ktoré efektívne využíva systémové zdroje a následne aj úsporu hardvéru. Na serveroch priebežne prebiehala štandardná správa a údržba.

Podľa požiadaviek a potrieb boli upravené nastavenia webových a mailových vstupných brán. Pravidelne sa kontrolovali a spravovali mailové karantény a riešilo sa prepúšťanie legitímnych mailov.

Správa pracovných staníc

V hodnotenom období prebiehala štandardná inštalácia a administrácia pracovných staníc. Vykonávala sa štandardná bežná denná údržba výpočtovej techniky - vrátane hardvérových a softvérových riešení problémov, ktoré sa vyskytli na PC u jednotlivých zamestnancov. Pokračovalo sa s upgradom pracovných staníc na Windows 7 a MS Office 2010.

Antivírusová, antispyverová a antispamová ochrana serverov, pracovných staníc a mailov

Antivírusová, antispyverová a antispamová ochrana serverov a pracovných staníc vo vnútornej sieti bola zabezpečovaná prostredníctvom manažovacieho servera a pomocou antivírusového a antispamového riešenia ešte pred vstupom do vnútornej siete. Antivírusové a antispamové servery boli kompletne aktualizované a boli upravené nastavenia politík a pravidiel podľa potrieb a požiadaviek. Bola vykonávaná pravidelná kontrola karantén a prepúšťanie zachytených legitímnych mailov ďalej k používateľom a kontrola fronty. Na všetkých serveroch je nastavená konfigurácia zvýšenej ochrany internetového prehliadača.

Nainštalovali sa servery s vyšším operačným systémom a vykonal sa upgrade verzie antivírového servera pre koncovú ochranu klientskych staníc a následne aj upgrade klientov.

V decembri bolo z licenčných dôvodov zmenené riešenie na ochranu mailov a na vnútorný mailový server bol nainštalovaný iný produkt.

Správa čipových kariet a USB tokenov IS ŠP

V roku 2017 prebiehala bežná rutinná prevádzka údržby a výroby USB tokenov a čipových kariet ako aj servis čipových kariet, ktorý sa týkal hlavne opráv čipových kariet a USB tokenov podľa požiadaviek používateľov.

Zabezpečenie činnosti záložného pracoviska

V roku 2017 prevádzka ZVS zabezpečovala správu, monitoring, údržbu a činnosť systémov, zariadení a aplikácii SAP, MANEX(QP0), RIS, KTI, ARDAL, Reuters. Bola realizovaná migrácia sieťových zariadení a inštalácia nového hardvéru, čím sa plnili úlohy vyplývajúce z potreby inovácie systémov.

Priebežne sa v ZVS realizovali bežné servisné zásahy a úspešne sa doladil beh klimatizácie počítačovej sály. Poruchy hardvéru boli opravené v zmysle zmluvného servisu, pričom funkčnosť systému nebola narušená. Nedostatky v synchronizácii záložných databáz s produkčnými boli odstraňované ihneď po ich vzniku a zistení.

Správa ServiceDesku a ServiceManagera

ServiceDesk sa v uvedenom období administroval už len v útlmovom režime, nakoľko 3.12.2012 bol nasadený do prevádzky jeho nástupca - HP ServiceManager. Vykonávala sa len kontrola dostupnosti, spracovávali sa ad hoc reporty na požiadanie používateľov a uvedenie systému do funkčného stavu po plánovaných reštartoch.

Po úspešnej migrácii posledných dát obsahujúcich evidenciu softwaru a licencií sa aplikačné servery definitívne vypli. Vypnutie databázových serverov sa uskutočnilo neskôr, bolo potrebné vyriešiť ich používanie testovacím prostredím RRP.

ServiceManager: okrem štandardných a rutinných činností ako správa užívateľských účtov a oprávnení, administrácie pracovných skupín, priebežnej kontroly fungovania integrácií, riešenia problémov klientov, hromadných updatov atď. sa do HPSM implementovali procesy pre podporu štyroch nových projektov:

- IOM
- MFSR Helpdesk
- Integrácia so SAP Solution Manager
- Integrácia s DICIT.

Formát notifikačných e-mailov bol zmenený z čistého textu na html. V priebehu októbra sa vyskytol problém s prihlasovaním klientov hlásiacich sa z Govnet-u.

HPSM bol v roku 2017 nedostupný cca. 35 minút, v dobe dvoch plánovaných a piatich nútených reštartov.

Správa produktov SAP

Plnenie úlohy spočívalo v nastavovaní prístupových oprávnení podľa doručených požiadaviek pre systémy SAP ESO, SAP ISUF a SAP EIS.

Všetky požiadavky na zmeny boli doručované cez systém Servis Manager, e-mailom alebo v písomnej forme. Následne bola vykonávaná optimalizácia a správa oprávnení pre jednotlivých používateľov, administrácia systémov SAP ESO, SAP ISUF, SAP EIS a generovanie nových oprávnení, reportov a monitorovanie systémov**.**

Zálohovanie

Zálohovanie prebiehalo v cykloch, ktoré sa opakovali každé štyri týždne. Počas víkendov sa robili plné zálohy pre 56 serverov a cez pracovný týždeň sa robili inkrementálne zálohy pre 8 serverov. Okrem toho sa ešte podľa potreby, resp. požiadavky vlastníka systému robili mimoriadne zálohy a obnovy požadovaných dát.

Pokračovalo sa v zálohovaní virtuálnych serverov prostredníctvom VMware VDP a priebežne sa riešili problémy so zálohovaním prostredníctvom VMware VDP, s funkcionalitou obnovy konkrétnych súborov a tiež aj priamo s podporou VMware.

V uplynulom období prebehla príprava migrácie zálohovacieho systému na vyššiu verziu, vrátane špecifikácie a zabezpečenia nového HW pre beh systému o novej páskovej knižnice. Samotná migrácia prebehne začiatkom roka 2018.

Ostatné činnosti

V roku 2017 bol v prostredí KTI prevádzkovaný nástroj na centralizovanú správu privilegovaných používateľských účtov.

Takisto bol prevádzkovaný systém pre podporu prevádzky informačných technológií, v rámci ktorého boli patchované operačné systémy aj aplikačný softvér.

V roku 2017 sa naďalej pracovalo aj na prevádzke Systému pre evidenciu a monitorovanie štátnej a minimálnej pomoci (IS SEMP). IS SEMP je postavený na funkčnosti pre oblasť riadenia žiadostí o schválenie poskytnutia štátnej pomoci a celkovej kontroly čerpania štátnej a minimálnej pomoci s doplnenou funkčnosťou portálu pre prístup z internetu, ktorý slúži na informovanie širokej verejnosti.

V roku 2017 DataCentrum poskytovalo podporu externým dodávateľom a spolupracovalo pri konfigurácii serverov a riešilo požiadavku na rozšírenie diskových priestorov.

V uvedenom období dokončovali práce na migrácii systému SAP-PI - presúvali sa pripojenia posledných organizácii a ich systémov zo starého systému SAP-PI na nový systém.

V roku 2017 prebehla migrácia pripojenia DataCentra do siete Govnet na novú infraštruktúru a IP adresáciu Govnet 2. S tým súvisela potreba readresovať poskytované služby do siete Govnet a zabezpečiť migráciu zabezpečených pripojení na nové adresy. Pri readresácii prebehla taktiež reorganizácia adresného plánu s cieľom umožnenia flexiblnejšej reakcie na prevádzkové potreby.

V uplynulom období prebehla migrácia dát na nové diskové pole, ktoré svojou kapacitou a prevádzkovými parametrami prevyšuje pôvodné diskové pole, pre ktoré už nebola podpora od výrobcu. Nové diskové pole umožňuje tiering dát, vďaka čomu je možné efektívnejšie využívať vynakladané finančné prostriedky. Pôvodné diskové pole je využívané pri prevádzke testovacích systémov.

Priebežne bola zabezpečovaná prevádzka registrovaných *.sk a *.eu cloud domén. DataCentrum zabezpečilo súčinnosť pri migrácii na nový informačný systém národného registrátora domén SK-NIC.

404	Prevádzkovanie Registra ponúkaného majetku štátu

V rámci úlohy boli:

- vykonávané bežné administrátorské činnosti ako sú aktualizácie, kontrola logov a riešenie prevádzkových problémov,
- zabezpečené plánované odstávky a bezproblémový nábeh po odstávkach,
- bola zabezpečená prevádzka bezpečnostných systémov a zariadení, ktoré chránia a zároveň kontrolujú prístupy ku registru a jeho službám,
- bolo zabezpečené pravidelné zálohovanie servera, jeho operačného systému a súborového systému, bol zabezpečený monitoring a dohľad servera i aplikácie.

Na základe hlásení na CPU boli riešené požiadavky používateľov všetkých častí aplikácie (Osobitné ponukové konania, Ponukové konania, Elektronické aukcie, Nájom) -bolo prijatých 184 hlásení, vyriešených 181 hlásení, 3 boli zrušené používateľom

Na základe používateľských požiadaviek boli priebežne vykonané aktualizácie viacerých funkcionalít a v rámci požadovaných zmien v súvislosti s úpravou webových stránok „ropk.sk“ boli na server aplikované nové skripty.

405	Poskytovanie odbornej podpory produktov spoločnosti Microsoft

Úloha bola riešená prostredníctvom CPU.

Zo strany potenciálnych používateľov boli uplatňované požiadavky, ktoré boli riešené v spolupráci so spoločnosťou Microsoft.

406	Prevádzka dátovej sály MF SR

V priebehu roka 2017 bola vykonávaná správa dátovej sály Ministerstva financií SR s dôrazom na zabezpečenie dostupnosti služieb a spoľahlivej prevádzky.

V rámci prevádzkovej podpory pre výpočtovú techniku a informačné systémy boli zaznamenávané požiadavky a incidenty od zamestnancov aj dodávateľov MF SR. Vzniknuté HW a SW problémy boli priebežne a neodkladne riešené. Integrácia do systému CMP bola úspešne zrealizovaná začiatkom septembra 2017. Prevádzkový denník na evidenciu a dokumentovanie prevádzkových zásahov na lokálnych a centrálnych systémoch MF SR je priebežne udržiavaný a aktualizovaný.

Zamestnanci MF SR boli na mesačnej báze ústne informovaní o stave informačných systémov na dátovej sále MF SR.

Okrem toho boli v požadovaných parametroch zabezpečované nasledovné činnosti:

- dostupnosť služieb AD, DHCP, DNS,
- dostupnosť elektronickej pošty,
- dostupnosť VPN služieb pre vzdialený prístup,
- dostupnosť tlačového servera,
- prístup do internetu,
- import dát zo SAP-u a následné zavedenie personálnych zmien,
- prístup do internetu,
- dostupnosť dochádzkového systému,

Pre zvýšenie bezpečnosti v sieti LAN boli v jednotlivých segmentoch siete LAN nasadené firewallové pravidlá pre komunikáciu jednotlivých zariadení.

Detailným návrhom sieťových nastavení vo vybraných segmentoch siete LAN pre nové systémy spúšťané na MF SR, ako aj úprava segmentov v ktorých boli umiestnené staršie systémy, bola dosiahnutá bezpečnosť a dátová priepustnosť. V roku 2017 bola zvýšená verzia informačného systému dochádzky zamestnancov MF SR.

Konfiguračné práce na informačných systémoch MS FR boli vykonávané podľa požiadaviek.

Bola vykonávaná denná záloha s reportom úspešnosti, ktorá je k nahliadnutiu v zálohovacom systéme DPM.

Od roku 2016 stále prebieha migrácia IS CEDIS do cloudu zabezpečovaného DataCentrom.

407	Informačný systém účtovníctva fondov (ISUF)

V roku 2017 bola DataCentrom poskytovaná a zabezpečovaná nepretržitá prevádzka a správa produkčného, školiaceho a testovacieho systému ISUF, ako aj vykonávaný pravidelný monitoring a vyhodnocovanie potreby aktualizácie (patchov) operačného systému servera ISUF.

V rámci aplikačnej, technickej, technologickej podpory a monitoringu poskytovalo DataCentrum používateľom systému ISUF podporu 1. stupňa a v spolupráci s odbornými garantmi MF SR a dodávateľom systému ISUF aj podporu 2. a 3. stupňa prostredníctvom aplikácie HP Service Manager.

V roku 2017 poskytlo CPU DataCentra služby 111 užívateľom informačného systému ISUF, pričom počet hlásení bol 666 a všetky, t. j. 100% (s prioritou 1 postúpených na druhú úroveň podpory v priemere do 1 hod. a vyriešených do 24 hod.) boli vyriešené v súlade s požiadavkami klientov a hodnotiacimi kritériami úlohy.

DataCentrum počas roku 2017 na základe doručených formulárov na pridelenie/odobratie oprávnení zabezpečovalo aj zakladanie, zmeny a výmazy používateľských účtov.

V roku 2017 bola vykonaná kontrola súladu bezpečnostných pravidiel platných pre externé informačné systémy s bezpečnostnými predpismi DataCentra vrátane systému ISUF.

K 5.4.2016 bola vykonaná analýza rizík BP ISUF, ktorá identifikovala 32 zraniteľností, z čoho bolo v priebehu hodnoteného obdobia 13 zraniteľností vyriešených, 18 je i naďalej v procese riešenia a 1 zraniteľnosť bola Riadiacim výborom ISUF akceptovaná.

V decembri 2017 bola vykonaná revízia BP ISUF, v rámci ktorého neboli identifikované nové významné organizačné a technické zmeny, neboli zistené nové, doteraz neuvažované riziká, nebol zvýšený počet bezpečnostných incidentov pri prevádzke systému ISUF. Zároveň bola vykonaná revízia dokumentu Analýza dopadov systému ISUF, pričom bolo v závere konštatované, že dokumenty sú v súlade s aktuálnym stavom.

Dňa 28.03.2017 prebehlo teoretické testovanie havarijných plánov ukončenia systému ISUF a havarijných plánov obnovy systému ISUF z hľadiska ich aktuálnosti a úplnosti a overenie znalostí rolí jednotlivých členov havarijného tímu pre ISUF.

Koncom roka 2017 bol úspešne realizovaný test obnovy údajov systému ISUF zo záložných médií.

Pravidelne na mesačnej báze bola spracovávaná správa z HP Service Managera o vyhodnotení riešenia incidentov a problémov ISUF, ktorá bola poskytovaná aj vlastníkovi informačného systému - Ministerstvu financií SR. Prostredníctvom CPU bolo v roku 2017 zo strany užívateľov zaznamenaných 445 hlásení - tieto boli následne vyriešené a uzatvorené jednotlivými pracovnými skupinami riešiteľov. V rámci monitorovania CMP bol v ISUF zaznamenaný celkový počet 47 incidentov, pričom počet incidentov, ktoré vznikli mimo časového rozmedzia platnosti SLA (7^{00} - 18^{00} hod) bol až 36.

Dostupnosť serverov ISUF (ostrého, školiaceho a testovacieho) bola zabezpečená bez zásadnejších problémov, čo predstavuje splnenie požiadavky MF SR.

V priebehu roka 2017 bol DataCentrom prevádzkovaný funkčný záložný systém ISUF.

Všetky úlohy vyplývajúce z kontraktu na rok 2017 boli splnené a vykonané v súlade s identifikačným listom úlohy a schváleným projektovým zámerom ISUF.

Úlohy BP ISUF a identifikované zraniteľnosti boli v roku 2017 plnené priebežne v zmysle návrhu opatrení a v určených termínoch. DataCentrum aj v roku 2017 aktualizovalo katalóg rizík ISUF.

V sledovanom období boli do konfiguračnej databázy pravidelne dopĺňané údaje týkajúce sa ISUF, pravidelne bola vykonávaná aj aktualizácia (patchovanie) operačných systémov serverov ISUF. Problémy v dostupnosti serverov neboli zaznamenané.

408	Ekonomické informačné systémy (EIS)

V roku 2017 DataCentrum zabezpečovalo štandardné prevádzkové služby pre produkčné, testovacie, vývojové a záložné prostredia ekonomických informačných systémov mnohých ministerstiev a ich niektorých podriadených organizácií a ekonomických informačných systémov vyšších územných celkov.

Okrem štandardných prevádzkových služieb bola zo strany DataCentra poskytovaná súčinnosť pri implementácií zmien, ich prvotnom testovaní ako aj ich samotné nasadzovanie v rámci testovacích a produkčných systémov.

Priebežne boli zo stany DataCentra zabezpečované činnosti spojené zo správou, údržbou a vytváraním prístupov pre existujúcich a nových užívateľov EIS systémov na prístupovej platforme KTI. Oddelením CPU boli zabezpečované služby spojené s nahlasovaním požiadaviek a problémov koncových užívateľov od ich evidencie, postúpenia na príslušné riešiteľské skupiny, monitoringu ich riešenia a následne ich pravidelného vyhodnocovania a reportingu.

DataCentrum zabezpečovalo pre používateľov EIS z iných rezortov priestory na školenia, ktoré vykonávali odborníci zo strany dodávateľov.

V rámci údržby a rozvoja boli v roku 2017 realizované upgrady systémov SAP a taktiež príslušných databáz.

Pre systém ESO boli v roku 2017 zrealizované činnosti spojené s prípravou migrácie a oddelenia databázovej a aplikačnej vrstvy systému. Oddelením aplikačnej a databázovej vrstvy sa zabezpečí efektívnejšie využívanie existujúcich databázových licencií. Samotná migrácia a oddelenie oboch vrstiev bude ukončené začiatkom roka 2018.

409	Riešenie požiadaviek a hlásení zamestnancov MF SR

V roku 2017 boli v súčinnosti s odborom informačných technológii pripravované technické podklady potrebné na začatie verejného obstarávania na HW a SW vybavenie pre potreby zamestnancov MF SR. Pri nasadzovaní nových informačných systémov do prevádzky na MF SR boli realizované konzultácie a pripomienkovania podkladov a dokumentov - konzultovali sa technické riešenia, návrhy na servisné kontrakty, obnova a nákup výpočtovej techniky ako aj sieťových tlačiarní.

V rámci prevádzkovej podpory pre výpočtovú techniku a informačné systémy boli zaznamenávané požiadavky a incidenty od zamestnancov aj dodávateľov MF SR, ktoré boli nahlasované e-mailom na helpdesk@mfsr.sk (4 140 správ), cez MF SR CRM systém (558) a tiež telefonicky na CPU DataCentra (393 - za posledné 4 mesiace roka) a osobne. Nahlásené požiadavky boli neodkladne vyriešené na prvej úrovni podpory alebo postúpené na vyššiu úroveň, pričom boli využité technické znalosti personálu ako aj príslušné servisné zmluvy. Všetky požiadavky boli v rámci technických a personálnych možností vyriešené v stanovenom termíne.

Pri vyradovaní zastaranej alebo nefunkčnej techniky bolo vyradených 20 ks osobných počítačov a 3 ks monitorov a 26 kusov tlačiarní. Na bezodplatný prevod išlo 184 zostáv ktoré sa museli vymazať a preinštalovať. Priebežne sa riešil plán na obnovu a opravu pokazených zariadení aby sa zabezpečila kontinuita poskytovania služieb bez citeľného dopadu na prevádzku a spokojnosť zamestnancov. V rámci tohoto sa nakúpilo 90 nových pracovných staníc.

V roku 2017 bolo v rámci prípravy výpočtovej techniky pre zamestnancov pripravených 96 pracovných staníc pre nových zamestnancov MF SR a zamestnancom, ktorí ukončili pracovný pomer, bolo odobraných 127 ks pracovných staníc. Boli realizované konfiguračné a inštalačné práce na novej výpočtovej technike, tlačiarňach a periférnych zariadeniach aby spĺňali požiadavky zapojenia do počítačovej siete LAN. Pri výmene či obnove techniky boli dolaďované automatizačné procesy ktoré dopomohli k zníženiu časového prestoja pri odobratí starej techniky a výdaji novej.

Priebežne bolo reinštalovaných 37 pracovných staníc. Reinštalácia lokálnych pracovných staníc bola automatizovaná pomocou systémových nástrojov SCCM a AD.

Pre nasadenie automatizovaného procesu výmeny techniky boli neustále aktualizované a dopĺňané image súbory pre uľahčenie inštalácie pracovných staníc a notebookov. Image súbory boli aktualizované podľa požiadaviek pre aktuálne softwarové vybavenie na MF SR. Pred nasadením image súborov do prevádzky boli všetky verzie otestované.

Pracovné stanice na MF SR boli centrálne spravované a pravidelne sa na nich inštalovali bezpečnostné záplaty pre operačný systém, programové vybavenie a udržiavala sa aktuálna antivírová databáza. Centrálne boli definované bezpečnostné politiky pre zabezpečenie vyššej bezpečnosti v súlade s bezpečnostnými odporúčaniami.

Evidencia a dokumentácia prevádzkových zásahov je evidovaná v elektronickej a papierovej forme. Požiadavky sa evidujú elektronicky do CRM HelpDesk systému „Microsoft Dynamics CRM" prevádzkovaného na MF SR. Prístup do HelpDesk systému CRM majú aj vedúci zamestnanci odboru informačných technológií - majú tak aktuálny prehľad o požiadavkách aj o stave ich riešenia a v prípade potreby si tak môžu priamo vytlačiť reporty zo systému.

Od septembra 2017 sa incidenty nahlasujú telefonicky do systému „HP Service Manager" prevádzkovaného v DataCentre. Na mesačnej báze sa odosielajú reporty o stave požiadaviek a incidentov na adresu *helpdesk@mfsr.sk.*

Okrem zabezpečovania technologickej platformy a užívateľskej podpory, bolo zabezpečované školenie zamestnancov MF SR o obsahu interného riadiaceho aktu o prevádzke a bezpečnosti LAN, ktoré sa zabezpečuje minimálne 1x mesačne (v priemere 2x za mesiac). Na podnet osobného úradu sa podľa počtu nástupov zamestnancov určovali termíny školení.

501	Projektové, ekonomické a organizačné riadenie, technická a prevádzková podpora DataCentra

Úloha zahŕňa všetky činnosti vykonávané v rámci ekonomického, organizačného, metodického a koncepčného riadenia DataCentra.

Ide o činnosti súvisiace so zabezpečením bezproblémového plnenia všetkých úloh vyplývajúcich pre DataCentrum z jeho štatútu, podpísaného kontraktu na príslušný rok a činnosti súvisiace s vytvorením a podporou pracovných podmienok k tomu potrebných.

701	Zabezpečenie prevádzky útvaru CSIRT.SK pre riešenie počítačových incidentov vo verejnej správe, vrátane informačných systémov kritickej informačnej infraštruktúry (KII)

Predmetom plnenia úlohy v roku 2017 bolo poskytovanie služieb potrebných na zvládnutie informačno-bezpečnostných incidentov v národnej informačnej a komunikačnej infraštruktúre, na odstránenie ich následkov a na následnú obnovu činnosti informačných systémov v spolupráci s prevádzkovateľmi, poskytovateľmi internetových služieb a inými štátnymi orgánmi. Okrem tejto základnej služby jednotka poskytovala aj ďalšie služby preventívneho a vzdelávacieho charakteru a zabezpečovala komunikáciu pri riešení bezpečnostných incidentov na medzinárodnej úrovni.

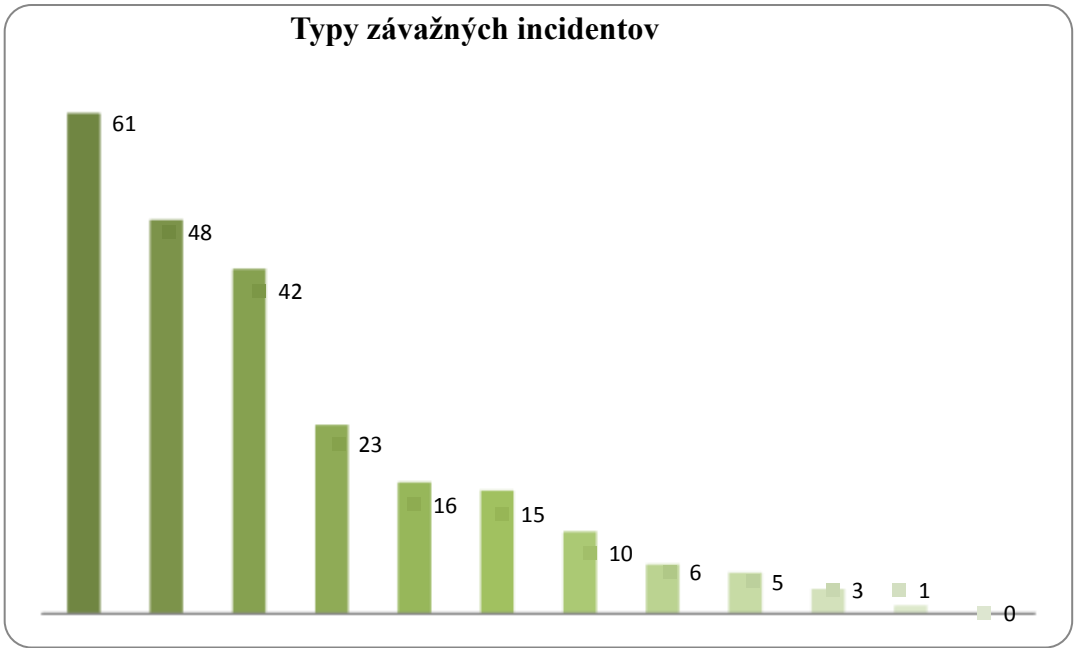
1. Riešenie informačno-bezpečnostných incidentov

V roku 2017 bolo zaznamenaných a riešených 230 počítačových incidentov, ktoré boli nahlásené klientelou CSIRT.SK, zahraničnými partnermi, subjektmi SR alebo boli zistené monitoringom CSIRT.SK. Incidenty boli riešené v spolupráci s:

- vlastníkmi a prevádzkovateľmi informačných systémov verejnej správy,
- vlastníkmi a prevádzkovateľmi vybraných prvkov kritickej informačnej infraštruktúry,
- vlastníkmi a prevádzkovateľmi národnej informačnej a komunikačnej infraštruktúry SR,
- telekomunikačnými operátormi a poskytovateľmi internetových služieb,
- CSIRT/CERT tímami v SR a zahraničí a ďalšími štátnymi orgánmi.

Počty jednotlivých typov závažných incidentov riešených CSIRT.SK v roku 2017:

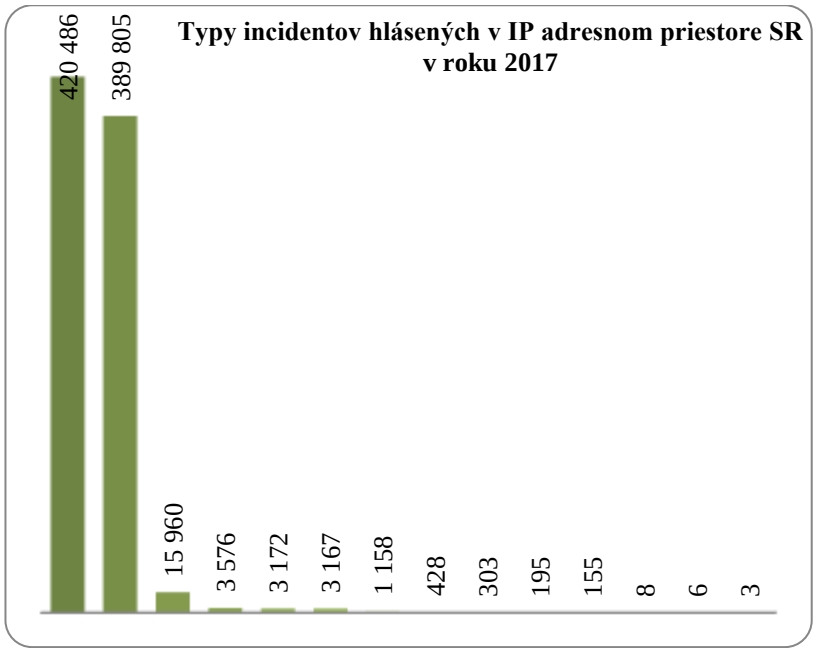
Typ škodlivej aktivity	**Počet**
Získavanie informácií – (phishing, social engineering, ...)	**61**
Zraniteľnosť	**48**
Škodlivý kód	**42**
Botnet	**23**
Pokus o prienik	**16**
Nežiaduci obsah (defacement, spam, ...)	**15**
Nedostupnosť (DoS, DDoS, ...)	**10**
Ostatné	**6**
Prienik do systému	**5**
Podvod	**3**
Neoprávnený prístup k informáciám/únik informácií	**1**
Neoprávnená modifikácia informácií	**0**
Celkom	**230**



Špecializovaný útvar CSIRT.SK poskytoval služby národného kontaktného miesta pre nahlasovanie škodlivej aktivity v IP adresnom priestore SR zahraničnými partnerskými tímami. V roku 2017 CSIRT.SK prijal 838 422 hlásení o možnom výskyte škodlivej aktivity z IP adries v Slovenskej republike. Hlásenia boli spracovávané denne špecializovanými automatizovanými systémami CSIRT.SK a po vyhodnotení ich závažnosti boli postupované poskytovateľom internetových služieb a inštitúciám, ktoré IP adresy podozrivé zo škodlivej aktivity používali.

Detailné počty a typy incidentov za sledované obdobie sú uvedené v nasledovnej tabuľke:

Typ incidentu	Počet
Bots	420 486
Vulnerabilities	389 805
Virut	15 960
Defacement	3 576
Malware	3 172
Spam	3 167
Malwareurl	1 158
Proxy	428
Bruteforce	303
Phishing	195
Citadel	155
Blaster	8
C&c	6
Zeus	3
Celkom	**838 422**



2. Proaktívne služby

a. Varovania

V priebehu roka 2017 boli v mesačnej periodicite publikované informácie o závažných bezpečnostných udalostiach a zraniteľnostiach informačných systémov a zariadení.
Na webovom portáli www.csirt.gov.sk publikovaných 5 oznámení pre odbornú verejnosť a boli spracované návrhy na elimináciu hrozieb ako napríklad http://www.csirt.gov.sk/informacna-bezpecnost/osvedcene-postupy/quick-wins-pre-zabezpecenie-organizacie-8a4.html.

Okrem týchto aktivít bolo kontaktným osobám inštitúcii verejnej správy a partnerom zaslaných 14 varovaní pred konkrétnymi hrozbami s možným dopadom na informačné systémy a elektronické služby.

b. Zvyšovanie bezpečnostného povedomia a vzdelávanie

V sledovanom období tím CSIRT.SK priebežne dopĺňal a aktualizoval sekciu osvedčené postupy a v nej umiestnené publikácie (http://www.csirt.gov.sk/osvedcene-postupy/nase-publikacie-85a.html).

Za účelom zvyšovania bezpečnostného povedomia občanov a priebežného monitorovania stavu IB špecializovaný útvar CSIRT.SK verejne publikoval výročnú správu o svojej činnosti, v ktorej prezentoval vybrané udalosti, incidenty, štatistiky, projekty a aktivity špecializovaného útvaru v roku 2017.

CSIRT.SK v spolupráci s Úradom podpredsedu vlády SR pre investície a informatizáciu aktualizoval Metodiku pre zabezpečenie organizácií v oblasti informačnej bezpečnosti (http://www.csirt.gov.sk/informacna-bezpecnost/osvedcene-postupy/metodika-zabezpecenia-ikt-8a6.html). Cieľom tohto dokumentu je vytvoriť ucelený podklad pre organizácie verejnej správy na systematické zabezpečenie informačnej bezpečnosti v organizácii, ktorý by odzrkadľoval aktuálne využívané technológie s dôrazom na nasadzovanie projektov implementovaných v rámci OPII.

CSIRT.SK tiež poskytol 6 školení na zvýšenie bezpečnostného povedomia o rizikách, kybernetických útokoch a možnostiach ochrany pred nimi organizáciám štátnej správy. Účastníci školení sa zorientovali v oblasti informačnej bezpečnosti, naučili sa odhaľovať potenciálny škodlivý kód, zvýšila sa ich obozretnosť pri práci s Internetom a elektronickou poštou a boli oboznámení s najzaujímavejšími kybernetickými incidentmi, ich príčinami a dôsledkami v posledných rokoch.

CSIRT.SK tiež vykonal test prostredníctvom simulovaného phishingového útoku. CSIRT.SK po dohode s vedúcim predstaviteľom dotknutej inštitúcie zaslal phishingový email, ktorý obsahoval maskovanú linku, ktorá pod zámienkou poskytnutia lákavých informácií používateľa presmerovala na podvrhnutú webovú stránku podobajúcu sa na stránku testovanej organizácie. Po vyhodnotení testu bol všetkým zamestnancom zaslaný informatívny email, ktorý ich oboznámil s konkrétnymi znakmi phishingového emailu, tiež bolo vykonané preškolenie zamestnancov a vykonaný tréning zameraný na odhaľovanie takýchto emailov.

c. *Spolupráca na národnej a medzinárodnej úrovni*

V roku 2017 špecializovaný útvar CSIRT.SK v oblasti riešenia bezpečnostných incidentov a zdieľania informácií o aktuálnych hrozbách a trendoch spolupracoval na národnej úrovni predovšetkým s bezpečnostnými útvarmi Ministerstva obrany SR, Ministerstva vnútra SR, Ministerstva zahraničných vecí a európskych záležitostí SR, Národného bezpečnostného úradu, úradu vlády SR a Slovenskej informačnej služby. CSIRT.SK v rámci poskytovania preventívnych služieb spolupracoval s ďalšími inštitúciami verejnej správy, prvkami kritickej infraštruktúry, akademickým a súkromným sektorom v rozsahu vecnej problematiky s dôrazom na ochranu informačných systémov verejnej správy a kritickej infraštruktúry. K 31.12.2017 má DataCentrum uzavretých 7 zmlúv o spolupráci v oblasti informačnej bezpečnosti so subjektami štátnej správy, akademického sektora, bankového sektora a poskytovateľmi služieb internetu.

Na medzinárodnej úrovni CSIRT.SK aktívne reprezentoval Slovenskú republiku v tzv. Sieti jednotiek CSIRT (CSIRTs Network), ktorá bola zriadená Smernicou NIS. Sieť jednotiek CSIRT pozostáva z jednotiek CSIRT členských štátov a jednotky CERT-EU, ktorá je CSIRT tímom európskych inštitúcií. Cieľom tejto siete je výmena informácií na dobrovoľnej báze o službách, činnostiach, spôsobilostiach a incidentoch na základe vybudovanej dôvery medzi jednotlivými tímami. V prípade incidentu môže táto sieť vymieňať, sprístupňovať a prerokúvať informácie a prediskutovať a vykonať koordinovanú reakciu na incident či poskytnúť podporu pri jeho riešení. V roku 2017 sa uskutočnili 3 oficiálne stretnutia tejto siete a to v Slieme (Malta), v Taline (Estónsko) a v Heraklione (Kréta).

CSIRT.SK tiež aktívne spolupracoval s Európskou agentúrou pre informačnú a sieťovú bezpečnosť (ENISA), zahraničnými CSIRT tímami Českej republiky, Rakúska, Nemecka, Maďarska, Poľska, Španielska, USA, Holandska a ďalších krajín a aktívne sa zapájal do medzinárodných projektov. CSIRT.SK je členom Stredoeurópskej platformy pre spoluprácu krajín V4 a Rakúska (CECSP) v oblasti kybernetickej bezpečnosti. CSIRT.SK spolupracuje s inštitúciou CERT-EU a združeniami CSIRT/CERT tímov TF-CSIRT a FIRST.

d. ***Cvičenia kybernetickej bezpečnosti***

V roku 2017 sa tím CSIRT.SK aktívne zapojil do prípravy a priebehu cvičenia Cyber Coalition 2017, ktoré bolo organizované Organizáciou Severoatlantickej zmluvy zamerané na oblasť kybernetickej obrany. Analytici CSIRT.SK v spolupráci so spoločnosťou ESET v rámci cvičenia riešili technické aspekty simulovanej bezpečnostnej udalosti s cieľom jej vyšetrenia a návrhu opatrení na obnovu riadnej prevádzky informačných systémov. Dôležitou súčasťou bolo preverenie spolupráce všetkých zapojených inštitúcií a subjektov na národnej úrovni.

V roku 2017 sa CSIRT.SK aktívne zapojil do prípravy cvičenia Cyber Europe 2018 a CyberSOPEx 2018. Cvičenia boli plánované počas dvoch plánovacích konferencií, ktoré sa uskutočnili v Aténach v Grécku. Cvičenie Cyber Europe sa postupom času stalo najväčším cvičením svojho druhu v Európe, ktoré je každé dva roky organizované Európskou agentúrou pre sieťovú a informačnú bezpečnosť.

V roku 2017 sa CSIRT.SK zúčastnil cvičenia Cyber Czech 2016. Cvičiacimi na tomto podujatí boli zástupcovia krajín Stredoeurópskej platformy pre počítačovú bezpečnosť (CECSP - Central European Cyber Security Platform). Konkrétne išlo o hráčov z Českej republiky, Maďarska, Rakúska a Slovenska.

CSIRT.SK sa v roku 2017 zúčastnil aj cvičenia Locked Shields, ktoré je každoročne organizované kybernetickým centrom NATO v Taline. Súťažiaci musia počas niekoľkodňového cvičenia ubrániť fiktívnu krajinu pred radom kybernetických útokov.

703	Prevádzka a rozvoj informačného systému včasného varovania, zdieľania informácií a reakcie na kybernetické hrozby, analýza škodlivého kódu a vykonávanie penetračných testov, vrátane testov zraniteľnosti pre subjekty v pôsobnosti útvaru CSIRT.SK

V sledovanom období bolo prevádzkované špecializované pracovisko útvaru CSIRT.SK, ktoré tvorí:

- pracovisko forenznej analýzy,
- pracovisko na penetračné testovanie,
- pracovisko na analýzu škodlivého kódu,

- sieťové laboratórium.

V rámci úlohy bola zabezpečená prevádzka sieťovej infraštruktúry, HW a SW zamestnancami CSIRT.SK. V rámci rozvoja a zabezpečenia funkcionality laboratórneho prostredia bolo implementované virtuálne prostredie pre možnosť simulácie rôznych komponentov a prepojení informačných systémov

CSIRT.SK poskytoval služby v oblastiach:

- forenznej analýzy pre potreby riešenia incidentov a návrhu opatrení,
- testovania zraniteľností a penetračného testovania,
- tvorby odporúčaní a bezpečnostných odporúčaní pre testované zariadenia,
- testovania bezpečnostných vlastností operačných systémov, bezpečnostných a sieťových prvkov,
- analýzy malware pre potreby riešenia incidentov, návrhu opatrení a vzdelávania,
- tvorby podporných materiálov pre národné a medzinárodné cvičenia v oblasti ochrany NIKI a informačnej bezpečnosti,
- vzdelávania zamestnancov CSIRT.SK a zamestnancov verejnej správy v oblasti IB
- poskytovanie odborných konzultácií, technickej podpory a vytváranie spoločných technických pracovísk
- analýza bezpečnostných problémov a návrh možných riešení, bezpečnostné konzultácie.

Počas roka 2017 bolo zamestnancami vykonaných 19 interných a externých penetračných testov. Z toho 14 nových testov a 5 opakovaných penetračných testov.

V rámci úlohy bol prevádzkovaný systém zdieľania informácií a včasného varovania Athena.