



DataCentrum

# **Správa o hodnotení plnenia úloh za rok 2025 vyplývajúcich z Kontraktu medzi MF SR a DataCentrom na rok 2025**

## Úvod

Správa o hodnotení plnenia úloh za rok 2025 vyplývajúcich z Kontraktu medzi Ministerstvom financií SR (ďalej len „MF SR“) a DataCentrom na rok 2025 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 05. 02. 2010, Dodatku č. 3 s účinnosťou od 05. 07. 2015, Dodatku č. 5 s účinnosťou od 01. 10. 2020, Dodatku č. 6 s účinnosťou od 01. 01. 2026 a v súlade s Kontraktom medzi MF SR a DataCentrom na rok 2025, čl. VI bod 1., podpísaným dňa 22. 11. 2024.

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 zapojené na rozpočet kapitoly 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 vyplývajú z obsluhy, údržby a rozširovania informačných systémov inštalovaných v DataCentre.

Všetky aktivity boli v roku 2025 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, rutínnej prevádzky a chodu DataCentra ako organizácie.

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

Používateľmi výstupov boli predovšetkým organizačné útvary MF SR (sekcia rozpočtovej politiky, sekcia štátneho výkazníctva, sekcia finančného trhu, sekcia daňová a colná, sekcia informačných technológií, kancelária ministra), Štátna pokladnica a Finančné riaditeľstvo SR.

DataCentrum poskytovalo vybrané informácie aj ďalším ústredným orgánom štátnej správy (ŠÚ SR, MH SR, MPSVR SR, MPRV SR, MD SR, MŠVVM SR a pod.), inštitúciám verejnej správy, niektorým neštátnym inštitúciám 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 štátnej pokladnice (ďalej len „IS ŠP“) DataCentrum poskytovalo permanentnú podporu používateľom pre RIS (moduly ZoRo, MPR, RI, MUR) s následnou väzbou na modul finančného plánu a platobného styku Štátnej pokladnice.

Na zabezpečenie spracovávaných dát a informačných systémov boli v oblasti kybernetickej bezpečnosti vykonané viaceré aktivity – bola vykonaná analýza a zabezpečovanie súladu DataCentra s požiadavkami zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZoKB“) a súvisiacich vyhlášok Národného bezpečnostného úradu. Požiadavky tohto zákona boli priebežne počas roka zapracovávané do bezpečnostnej dokumentácie a interných predpisov DataCentra. Bola vykonaná analýza a zabezpečovanie súladu DataCentra s požiadavkami zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, aktualizácia Krízového plánu a plánu obnovy činnosti DataCentra, aktualizácia a teoretické testovanie plánov obnovy pre ISUF, CES, KTI, KTI2.

Útvar bezpečnosti v oblasti kybernetickej bezpečnosti komunikoval s tímom CSIRT MF SR, Národným bezpečnostným úradom, Vládnou jednotkou CSIRT.SK MIRRI SR, správcom siete Govnet (NASES) a tímom GOVCERT SK. Zabezpečoval kontaktný bod pre príjem hlásení o bezpečnostných incidentoch a koordinoval ich riešenie. Priebežne útvar bezpečnosti posudzoval implementáciu zmien IKT z hľadiska informačnej bezpečnosti.

DataCentrum vypracúva pravidelný prehľad o stave kybernetickej bezpečnosti za rok 2025, najmä o detegovaných kybernetických bezpečnostných incidentoch (ďalej len „KBI“), ich druhoch, závažnosti, true positive/false positive rate hlásení bezpečnostných udalostí, priemernom čase detekcie a reakcie na KBI, vyhodnotenie bezpečnostných trendov a efektivity prijatých bezpečnostných opatrení a informácie týkajúce sa manažmentu zraniteľností, identifikovaných a opravených zraniteľností v závislosti od ich kategorizácie. Tento prehľad o stave kybernetickej bezpečnosti DataCentrum zasiela MF SR.

V roku 2025 boli ad-hoc vydávané varovania pred podvodnými správami (phishing) a v oblasti zraniteľnosti informačných a komunikačných zariadení a tiež boli realizované školenia informačnej bezpečnosti s cieľom zvyšovať úroveň bezpečnostného povedomia interných zamestnancov DataCentra a zamestnancov tretích strán.

V rámci výkonu dohľadu nad ochranou osobných údajov boli poskytované konzultácie jednotlivým organizačným útvarom DataCentra a tiež organizáciám, ktorých informačné systémy sú prevádzkované v DataCentre. Medzi DataCentrom a MF SR bola pripravená sprostredkovateľská zmluva, kde MF SR je v pozícii sprostredkovateľa a DataCentrum v pozícii prevádzkovateľa pri spracovaní osobných údajov organizácie DataCentrum.

Existujúce zmluvy boli v roku 2025 prehodnotené a v prípade potreby aktualizované a dodatkovane.

V rámci poskytovania služieb tretími stranami boli v súlade s požiadavkami nariadenia č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (z angl. „General data protection regulation – GDPR“, ďalej len: „GDPR“) a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZOOÚ“) identifikované a vypracované sprostredkovateľské zmluvy s tretími stranami, prostredníctvom ktorých DataCentrum prenieslo časť zodpovednosti za bezpečnosť spracovania osobných údajov na tretie strany.

Vzájomná komunikácia medzi MF SR a DataCentrom prebieha na úrovni zodpovednej osoby z hľadiska GDPR a ZOOÚ na strane MF SR a zodpovednej osoby z hľadiska GDPR na strane DataCentra priebežne telefonicky a e-mailom.

V rámci interného auditu, ktorého časť sa týkala aj ochrany osobných údajov, neboli identifikované nedostatky vo vzťahu k poskytovaným službám, pričom v rámci jednotlivých úloh boli na spracovanie osobných údajov dodržané pokyny prevádzkovateľa.

V roku 2025 nebol v DataCentre zaznamenaný závažný kybernetický incident.

Výkon komplexu činností pre používateľov KTI a informačných systémov prevádzkovaných DataCentrom, t. j. riešenie požiadaviek na podporu zo strany používateľov a aplikačnej, technologickej a metodologickej pomoci, zabezpečuje Centrum podpory používateľov (ďalej len „CPU“), ktoré DataCentrum prevádzkuje. Poskytované služby spočívajú v zabezpečovaní odborného poradenstva predovšetkým pre potreby úspešného fungovania rozpočtového informačného systému (ďalej len „RIS“), IS ŠP, Centrálného ekonomického systému (ďalej len „CES“) a ďalších informačných systémov. CPU je podporované vytvorenou a nepretržite udržiavanou komunikačno-technologickou infraštruktúrou.

V roku 2025 poskytlo CPU služby používateľom informačných systémov, pričom počet organizácií používajúcich aspoň jeden informačný systém prevádzkovaný DataCentrom bol 9 706 a počet používateľov s aktívnym prístupom do IKT prevádzkovaných DataCentrom bol 86 148.

Celkový počet kontaktov CPU používateľmi bol 126 028, z toho 43 371 telefonických, 39 879 e-mailových, 4 300 listových a 38 478 cez internetové rozhranie. CPU odoslalo používateľom 4 454 listových zásielok.

Okrem informačných systémov na podporu riadiacich aktivít MF SR je v DataCentre aj naďalej úspešne prevádzkovaný projekt monitorovacieho systému pre štrukturálne fondy a kohézny fond (ITMS II a ITMS 2014+), portál ITMS 2014+ a portál ITMS21+.

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. 07. 2015, pričom v roku 2025 sa v DataCentre aj naďalej realizovali činnosti súvisiace so zabezpečovaním jeho produkčnej prevádzky. **1 724** hlásení používateľov pre ITMS2014+ neverejná časť a **3 275** hlásení používateľov ITMS2014+ verejná časť. Dostupnosť produkčného systému ITMS2014+ neverejná časť a ITMS2014+ verejná časť bola v hodnotenom období 99,90 %.

Prostredníctvom informačného systému ITMS2014+ bola do 12. 06. 2024 technicky zabezpečovaná aj úvodná fáza implementácie programového obdobia 2021 - 2027. ITMS2014+ (pôvodne využívaný iba pre implementáciu programového obdobia 2014 - 2020) bol v nevyhnutnej miere upravený a doplnený tak, aby zabezpečil potreby implementácie programového obdobia 2021 - 2027 dočasne, do nasadenia ITMS21+ do prevádzky.

V priebehu hodnoteného obdobia DataCentrum vykonávalo aj činnosti na zabezpečenie prevádzky systému, činnosti potrebné na ďalší rozvoj a zabezpečenie bezpečnosti systému ITMS21+, schvaľovalo prístupy pre používateľov a poskytovalo aplikačnú podporu používateľom systému ITMS21+. V roku 2025 bolo vyriešených **3 363** hlásení používateľov pre ITMS21+ neverejná časť a **10 272** hlásení používateľov ITMS21+ verejná časť.

Od 29. 05. 2024 sa začali realizovať prípravné fázy migrácie z ITMS2014+ do ITMS21+. Hlavná fáza migrácie údajov z ITMS2014+ prebehla dňa 06. 06. 2024.

Migrácia údajov z ITMS2014+ bola úspešne ukončená dňa 12. 06. 2024 a od tohto dátumu bola v systéme ITMS2014+ ukončená editácia a práca v evidenciách programového obdobia

2021 - 2027, okrem používateľov s pracovnou pozíciou kontrolór, ktorí v systéme ITMS2014+, pod orgánmi 21\_RO\_PSK\_MIRRI SR a 21\_SO\_PSK\_ÚV SR zabezpečovali kontrolu vykonávania úloh zo strany sprostredkovateľského orgánu podľa zmluvy o vykonávaní časti úloh riadiaceho orgánu sprostredkovateľským orgánom.

Funkcionalita výkonu kontroly sprostredkovateľského orgánu podľa zmluvy o vykonávaní časti úloh riadiaceho orgánu sprostredkovateľským orgánom v systéme ITMS21+ zatiaľ nebola implementovaná, preto bolo potrebné počas roku 2025 vytvoriť prístupy pre vybraných používateľov v systéme ITMS2014+, pod orgánmi 21\_RO\_PSK\_MIRRI SR a 21 SO\_PSK\_ÚV SR.

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-a. V roku 2025 to bolo 182 zaevidovaných používateľov informačného systému ISUF, pričom počet hlásení bol 510 a všetky, t. j. 100 %, boli vyriešené v súlade s požiadavkami klientov a hodnotiacimi kritériami úlohy. V rámci zabezpečenia prevádzky a funkčnosti tohto IS bol zabezpečovaný súlad bezpečnostnej politiky a analýzy rizík s GDPR a zákonom o kybernetickej bezpečnosti.

DataCentrum aj v roku 2025, ako prevádzkovateľ Registra účtovných závierok, v zmysle § 23c zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov v súlade so zákonom č. 71/1967 Z. z. o správnom konaní a zákonom č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov, vydávalo na základe doručenej žiadosti overené kópie dokumentov alebo časti dokumentov, ktoré sú uložené v Registri účtovných závierok (ďalej len „RÚZ“).

V roku 2025 bolo podaných a doručených celkovo 148 žiadostí o poskytnutie údajov z RÚZ, pričom všetkých 148 žiadostí bolo vybavených, čo predstavuje 100 % úspešnosť vybavenia.

Z uvedeného počtu bolo 53 žiadostí podaných a vybavených osobne a 93 žiadostí bolo doručených a vybavených poštou. Jedna žiadosť bola vybavená prostredníctvom e-mailu a jedna žiadosť bola zrušená. Z celkového počtu riešených žiadostí bolo 94 žiadostí vybavených bezplatne, 53 za úhradu v hotovosti v súlade so zákonom č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov. V prípade osobného podania žiadosti a úhrady správneho poplatku v hotovosti alebo na základe potvrdenia pre evidenciu poplatku, bol výstup vydávaný na počkanie. V prípadoch, keď nebolo možné žiadosť vybaviť hneď, keďže sa požadovaný dokument v registri nenachádzal, bolo potrebné zabezpečiť nápravu v spolupráci s Finančným riaditeľstvom SR, ktoré na základe nášho upozornenia zabezpečilo následné doplnenie a zverejnenie chýbajúcich dokumentov. V takýchto prípadoch je poverený zamestnanec podateľne RÚZ 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.

Prostredníctvom Service Manager-a je evidovaných 880 používateľov, ktorí boli v roku 2025 aktívni a vstupovali aj do verejnej časti RÚZ. Všetky požiadavky klientov hlásené cez CPU boli zaznamenané v Service Manager-i a boli vyriešené v stanovenom termíne a v súlade s požiadavkami SLA, t. j. bolo poskytnuté poradenstvo na telefonickú alebo e-mailovú úroveň, 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 (2 013 správ), cez MF SR SCSM systém (3 151 požiadaviek) a tiež telefonicky alebo e-mailom na CPU DataCentra (1 020) a osobne. Nahlasené 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. Zamestnancom pracujúcim v režime Home office, bola poskytovaná identická podpora s využitím technických prostriedkov pre vzdialený prístup.

DataCentrum v roku 2025 zabezpečilo nepretržitú prevádzku technologickej infraštruktúry dátovej sály na MF SR bez neplánovaných výpadkov, aj vďaka neustálemu monitoringu zariadení a požadovaných parametrov pre dátovú sálu. Zabezpečovali sa pravidelné servisné kontroly, opravy, zákonom stanovené revízie a odborné skúšky na jednotlivých zariadeniach.

V prípade zmien bola aktualizovaná relevantná prevádzková dokumentácia. Všetky činnosti súvisiace so zabezpečením nepretržitej prevádzky boli konzultované a vykonávané v súčinnosti zamestnancov DataCentra, MF SR a dodávateľa služieb. Plánované odstávky boli vopred nahlásené a schválené MF SR. Vďaka nášmu úsiliu a súčinnosti MF SR bola garantovaná dostupnosť poskytovaných služieb v režime 24/7/365.

V priebehu roka 2025 bola zabezpečená nepretržitá prevádzka dátovej sály a boli garantované poskytované IT služby. V rámci prevádzkovej podpory rezortu MF SR sa vykonávali komplexné činnosti v prospech používateľov informačných systémov. Požiadavky a incidenty od zamestnancov súvisiace s IT prevádzkou boli zaznamenané a neodkladne riešené.

DataCentrum aj v roku 2025 vykonávalo pre MF SR aktivity súvisiace s poskytovaním sprostredkovateľských činností a povinnosťou dodržiavať požiadavky legislatívy v oblasti ochrany osobných údajov ZOOÚ a požiadaviek nariadenia GDPR (2016/679), ZoKB, ktoré sa týkajú spracúvania osobných údajov. Pri týchto spracovateľských činnostiach je MF SR v pozícii prevádzkovateľa a DataCentrum v pozícii sprostredkovateľa.

Už v roku 2019 bol DataCentrom prevádzkovaný Register vylúčených osôb (ďalej len „RVO“) v nadväznosti na zákon č. 30/2019 Z. z. o hazardných hrách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, podľa ktorého je fyzická osoba, ktorá dovŕšila 18 rokov veku, vylúčená z účasti na hazardných hrách. V produkčnom prostredí bolo spustené importovanie zoznamov osôb vylúčených z hrania hazardných hier prostredníctvom Centrálného systému referenčných údajov (ďalej len „CSRÚ“). Priebežne sa do systému nahrávajú prostredníctvom CSRÚ dáta z Ministerstva práce sociálnych vecí a rodiny SR. Na základe žiadosti Úradu pre reguláciu hazardných hier (ďalej len „ÚRHH“) bola implementovaná kontrola na správnosť zadávania rodného čísla pri lustrácii a ďalšie požiadavky na možnosti lustrácie.

V rámci CPU je zaevidovaných 3 558 používateľov RVO a v roku 2025 bolo riešených 94 hlásení.

V súlade s požiadavkami GDPR sú priebežne vymazávané osobné údaje zamestnancov správcov majetku a záujemcov o majetok štátu.

V roku 2025 bol Systém vysledovateľnosti tabakových výrobkov prevádzkovaný v režime 24/7/365 s dostupnosťou na úrovni 100 % počas celého roka.

Počet registrovaných hospodárskych subjektov bol 13 129, počet registrovaných prevádzok hospodárskych subjektov bol 24 501. Celkový počet registrovaných používateľov predstavoval 12 394.

Systémom pre vytváranie a vydávanie jedinečných identifikátorov na účely systému vysledovateľnosti tabakových výrobkov bolo v priebehu uplynulého roka vydaných celkom 359 909 934 jedinečných identifikátorov (jedinečné identifikátory jednotkového balenia a jedinečné identifikátory agregovaného balenia).

Vnútorňa kontrolná činnosť v DataCentre bola v roku 2025 realizovaná v súlade s „Plánom kontrolnej činnosti na rok 2025“ schváleným riaditeľom DataCentra. Zameranie vnútornej kontroly bolo orientované na rozhodujúce oblasti činnosti v nadväznosti na všeobecne záväzné právne predpisy a interné smernice.

V roku 2025 bolo v DataCentre uskutočnených 5 kontrolných akcií na úrovni útvaru kontroly.

V kontrolovanom období neboli zistené závažné porušenia všeobecne záväzných právnych predpisov a interných predpisov DataCentra.

DataCentrum v roku 2025 nevidovalo žiadne podania podľa zákona č. 85/1990 Zb. o petičnom práve v znení neskorších predpisov a ani podľa zákona č. 9/2010 Z. z. o sťažnostiach v znení neskorších predpisov.

DataCentrum malo **rozpisom záväzných ukazovateľov** štátneho rozpočtu na rok 2025 stanovený záväzný limit zamestnancov v počte 111 osôb.

Vykázaná skutočnosť v sledovanom období predstavuje v:

- priemernom prepočítanom počte zamestnancov 105 osôb,
- priemernom evidenčnom počte zamestnancov 106 osôb.

Skutočný evidenčný počet zamestnancov vo fyzických osobách ku dňu 31. 12. 2025 bol 106 zamestnancov, z toho 64 žien a 42 mužov.

Traja zamestnanci vykonávali prácu v kratšom pracovnom čase.

V roku 2025 bol v DataCentre zaznamenaný nasledovný **pohyb zamestnancov**:

1) *nastúpilo 10 zamestnancov* prijatých z dôvodov:

- opätovného obsadenia pracovných miest uvoľnených zamestnancami končiacimi pracovný pomer,
- potreby rozšírenia personálnych kapacít na zabezpečenie aplikačnej, metodologickej a technickej podpory pre prevádzkované a nové IS, ako aj zabezpečenie právnej agendy.

2) *vystúpilo 10 zamestnancov*, pričom dôvody skončenia pracovného pomeru boli nasledovné:

- vzájomná dohoda na podnet zamestnanca z dôvodu:
  - zmeny zamestnávateľa v 6 prípadoch,
  - odchodu do starobného dôchodku v 1 prípade,
- výpoveď na podnet zamestnanca z dôvodu:
  - zmeny zamestnávateľa v 2 prípadoch,
- skončenie počas skúšobnej doby:
  - zo strany zamestnávateľa v 1 prípade.

**Veková štruktúra** zamestnancov DataCentra k 31. 12. 2025 bola nasledovná:

Vekový interval	počet	v %
Do 20 rokov	0	0,00
21 - 30 rokov	3	3,18
31 - 40 rokov	18	19,08
41 - 50 rokov	29	30,74
51 - 60 rokov	28	29,68
Nad 60 rokov	28	29,68
Priemerný vek	50,7 rokov	

Priemerný vek zamestnancov sa výrazne nemení. Z rozloženia vyplýva, že najväčší podiel 30,74 % predstavovali zamestnanci vo vekovej kategórii 41 - 50 rokov.

**Kvalifikačná štruktúra** zamestnancov k 31. 12. 2025 bola nasledovná:

Vzdelanie	počet	v %
• vysokoškolské	58	54,72
z toho: VŠ III.	3	
VŠ II.	47	
VŠ I.	8	
• úplné stredné vzdelanie	45	42,45
• stredné odborné vzdelanie	3	2,83
Celkom	106	100,00

V porovnaní s rokom 2024 v oblasti kvalifikačnej štruktúry výrazná zmena nenastala.

Aj v roku 2025 najpočetnejšiu a podielovo najvýraznejšiu skupinu tvorili zamestnanci s vysokoškolským vzdelaním.

**Vzdelávanie, odborný rast a rozvoj vedomostí** zamestnancov patria medzi kľúčové nástroje rozvoja organizácie a zvyšovania výkonnostného potenciálu jej ľudských zdrojov. V hodnotenom období bolo vzdelávanie zamestnancov DataCentra realizované v súlade s potrebami organizácie, s dôrazom na priebežné prehľbovanie odborných znalostí najmä v oblasti informačných systémov, bezpečnosti cloudových riešení, administrácie a správy informačných systémov, informačnej a kybernetickej bezpečnosti, prevádzky dátových centier, manažérskeho vzdelávania, ako aj účasti na odborných seminároch zameraných na konkrétne témy nevyhnutné pre plnenie pracovných úloh.

Interné vzdelávanie bolo realizované predovšetkým formou vstupného školenia nových zamestnancov. Pravidelne prebiehalo aj periodické vzdelávanie zamerané na oblasť bezpečnosti a ochrany zdravia pri práci a ochrany pred požiarmi (BOZP a OPP), informačnú a kybernetickú bezpečnosť, ochranu osobných údajov a systém manažérstva kvality.

Odborné kurzy, tréningy, semináre a konferencie boli zabezpečované prostredníctvom externých vzdelávacích inštitúcií, externých dodávateľov v rámci zmluvných dodávok technologických zariadení a služieb, ako aj vlastnými vedúcimi zamestnancami DataCentra.

V hodnotenom období DataCentrum zabezpečilo spolu 32 vzdelávacích a školiacich aktivít. Externou formou sa na 26 vzdelávacích podujatiach zúčastnilo celkom 37 účastníkov (zamestnancov), pričom 14 aktivít pre 26 účastníkov bolo hradených z rozpočtových prostriedkov DataCentra.

V prepočte na priemerný evidenčný počet zamestnancov DataCentra v roku 2025 absolvoval jeden zamestnanec v rámci interných a externých vzdelávacích aktivít v priemere 8 hodín vzdelávania, čo predstavuje 1 osobodeň.

Na vzdelávacie aktivity bolo v roku 2025 z rozpočtových prostriedkov vynaložených celkovo 6 714,37 eur. Priemerný výdavok na vzdelávanie jedného zamestnanca DataCentra za hodnotené obdobie predstavoval 63,34 eur.

Aj v roku 2025 prebehlo školenie zamerané na prácu v Centrálnom ekonomickom systéme. Tohto školenia sa zúčastnila zamestnankyňa z odboru ekonomiky.

Celkové plnenie úloh kontrahovaných na rok 2025 možno hodnotiť ako veľmi dobré, zodpovedné a často aj nad rámec úrovne podmienok, ktoré boli determinované počtom kvalifikovaných zamestnancov a pridelenými finančnými prostriedkami. Pôvodný rozpis rozpočtu na rok 2025 bol dodatkami ku Kontraktu na rok 2025 medzi MF SR a DataCentrom upravený vo výške schváleného rozpočtového opatrenia so súhlasom MF SR - Dodatkom č. 1 k 17. 07. 2025 a Dodatkom č. 2 k 11. 12. 2025.

Čerpanie rozpočtu DataCentra - skutočnosť k 31. 12. 2025 bolo predmetom Dodatku č. 2 a je uvedené v Prílohe č. 1 tejto správy.

Skutočné čerpanie kapacít DataCentra k 31. 12. 2025 plánovaných na plnenie úloh kontrahovaných na rok 2025 je uvedené v Prílohe č. 2 tejto správy.

## Plnenie úloh DataCentra za rok 2025

### 111 Bezpečnosť informačných systémov DataCentra

Zabezpečovanie činností súvisiacich s Bezpečnostným projektom IS v DataCentre v roku 2025 pozostávalo z činností týkajúcich sa koordinácie procesov riadenia informačnej bezpečnosti v DataCentre. Útvar bezpečnosti aktívne identifikuje požiadavky legislatívy a právnych predpisov v oblasti bezpečnosti informačných systémov a implementuje jednotlivé požiadavky pre činnosti, ktoré vykonáva a zabezpečuje.

Pre oblasť bezpečnosti IS boli realizované nasledovné činnosti:

- aktualizácia bezpečnostnej dokumentácie v gescii útvaru bezpečnosti,
- súčinnosť pri aktualizácii internej riadenej dokumentácie (IRD) v gescii iných odborných útvarov na účely zosúladenia s požiadavkami legislatívy v oblasti bezpečnosti a bezpečnostných požiadaviek,
- analýza a zabezpečovanie súladu DataCentra s požiadavkami zákona č. 95/2019 Z. z. o informačných technológiách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o ITVS“),
- zavedenie integrovaného manažérskeho systému podľa noriem ISO 9001:2015 Manažerstvo kvality a ISO/IEC 27001:2022 Systém manažerstva informačnej bezpečnosti; nezhôd: 0, odporúčaní: 6,
- aktualizácia postupov pre kritické procesy interných systémov v prípade vzniku mimoriadnej situácie,
- aktualizácia Krízového plánu a plánu obnovy činnosti DataCentra,
- testovanie havarijných plánov obnovy informačných systémov - HP SM, KTI, KTI2, ID Issuer, RRP, VAP, WEB stránka, Oracle, AD a poštový systém DataCentra,
- aktualizácia havarijných plánov interných a externých systémov,
- aktualizácia Plánov zálohovania pre interné a externé systémy,
- aktualizácia Krízového Plánu hospodárskej mobilizácie DataCentra,
- aktualizácia analýzy rizík v zmysle požiadaviek legislatívy a interných auditov,
- odpočet plánu zvládania rizík za rok 2025:

<b>Celkový počet zraniteľností:</b>	<b>133</b>
• vyriešené/overené	82
• vyriešené/neoverené	8
• čiastočne vyriešené	5
• v riešení	13
• neriešené	4
• akceptované	11
• odstránené	3
+	
nové zraniteľnosti	7

Pre oblasť ochrany osobných údajov boli vykonané tieto činnosti:

- analýza a zabezpečenie súladu DataCentra s požiadavkami legislatívy v oblasti ochrany osobných údajov podľa ZOOÚ a požiadaviek GDPR,
- vypracovanie a aktualizácia záznamov o spracovateľských činnostiach,

- aktualizácia informačných povinností pre dotknuté osoby,
- zabezpečenie výkonu dohľadu nad ochranou osobných údajov a poskytovanie konzultačnej podpory.

V rámci výkonu dohľadu nad ochranou osobných údajov boli poskytované konzultácie jednotlivým organizačným útvarom DataCentra a tiež organizáciám, ktorých informačné systémy sú prevádzkované v DataCentre. Medzi DataCentrom a MF SR bola uzavretá sprostredkovateľská zmluva, kde MF SR je v pozícii sprostredkovateľa a DataCentrum v pozícii prevádzkovateľa pri spracovaní osobných údajov organizácie DataCentrum v CES. Existujúce zmluvy boli v roku 2025 prehodnotené a v prípade potreby aktualizované a dodatkovane.

Pre oblasť kybernetickej bezpečnosti boli vykonané nasledovné činnosti:

- analýza a zabezpečovanie súladu DataCentra s požiadavkami novelizácie ZoKB,
- zapracovávanie požiadaviek ZoKB do bezpečnostnej dokumentácie a interných predpisov DataCentra,
- úprava zmluvných podmienok s ohľadom na požiadavky § 19 ZoKB,
- plnenie úloh z auditu kybernetickej bezpečnosti,
- prehodnocovanie Plánu zvládania rizík na Bezpečnostných výboroch DataCentra.

Pre oblasť kritickej infraštruktúry boli vykonané nasledovné činnosti:

- zabezpečovanie súladu DataCentra s požiadavkami zákona č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov,
- aktualizácia bezpečnostnej dokumentácie.

Útvar bezpečnosti v oblasti kybernetickej bezpečnosti komunikoval s tímom CSIRT MF SR, Národným bezpečnostným úradom, Vládnou jednotkou CSIRT.SK MIRRI SR, správcom siete Govnet (NASES) a tímom GOVCERT SK. Zabezpečoval kontaktný bod pre príjem hlásení o bezpečnostných incidentoch a koordinoval ich riešenie. Priebežne útvar bezpečnosti posudzoval implementáciu zmien IKT z hľadiska informačnej bezpečnosti.

V roku 2025 boli ad-hoc vydávané varovania pred podvodnými správami (phishing) a v oblasti zraniteľnosti informačných a komunikačných zariadení a tiež boli realizované školenia informačnej bezpečnosti s cieľom zvyšovať úroveň bezpečnostného povedomia interných zamestnancov DataCentra a zamestnancov tretích strán.

<b>112</b>	<b>Poskytovanie sprostredkovateľských činností DataCentra pre MF SR v súlade s GDPR a zákonom o ochrane osobných údajov (DataCentrum v postavení sprostredkovateľa)</b>
------------	---

Na základe úloh popísaných v IL112 DataCentrum vykonáva pre MF SR spracovateľské činnosti, ktoré sa týkajú spracúvania osobných údajov. Pri týchto spracovateľských činnostiach je MF SR v pozícii prevádzkovateľa a DataCentrum v pozícii sprostredkovateľa.

DataCentrum na základe definovaných úloh v tejto oblasti zabezpečilo úroveň informačnej bezpečnosti a naplnenie legislatívnych požiadaviek, ktoré stanovuje GDPR a ZOOÚ.

Medzi najdôležitejšie aktivity patrili:

- vyjasnenie právnych základov a postavenia DataCentra a MF SR pri spracovateľských činnostiach,
- aktualizovanie záznamov o spracovateľských činnostiach pre systémy, pre ktoré je DataCentrum v postavení sprostredkovateľa,
- poskytnutie súčinnosti pri aktualizácii bezpečnostného projektu a bezpečnostnej dokumentácie MF SR vo vzťahu k podpornej infraštruktúre pre informačné systémy MF SR,
- nastavenie systému evidencie a hlásenia bezpečnostných incidentov súvisiacich s porušením bezpečnosti osobných údajov,
- podporné činnosti pri definovaní informačných povinností dotknutým osobám,
- podporné činnosti pri formulovaní otázok na ÚOOÚ na účely vyjasnenia problémových vecí v oblasti spracúvania osobných údajov.

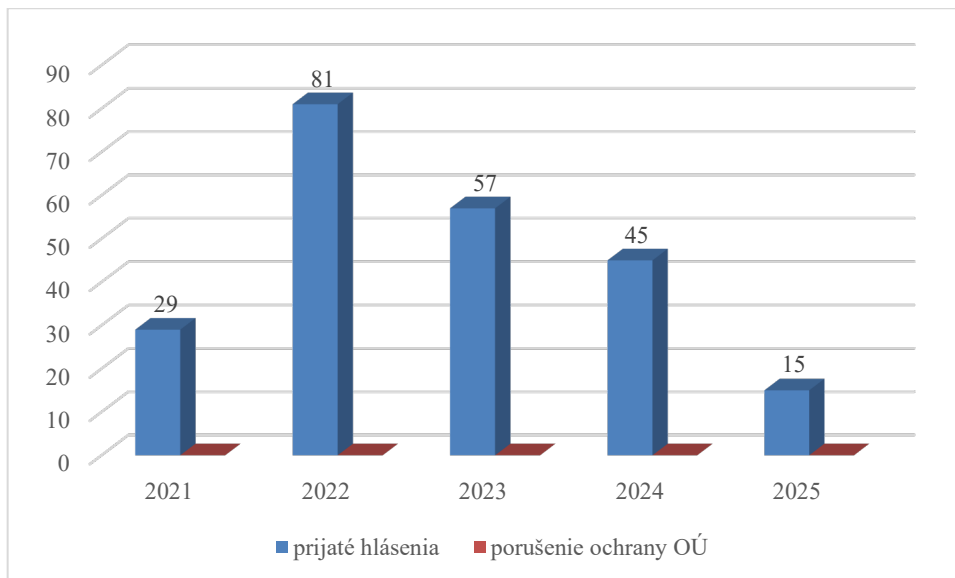
Pre niektoré spracovateľské činnosti DataCentrum využíva služby tretích strán, ktoré sa aktívne podieľajú na zabezpečovaní ochrany osobných údajov vo vzťahu k poskytovaným službám pre MF SR.

Pre riešenie požiadaviek GDPR a ZOOÚ týkajúcich sa služieb poskytovaných tretími stranami sú identifikované a vypracované sprostredkovateľské zmluvy s týmito tretími stranami, prostredníctvom ktorých DataCentrum prenieslo časť zodpovednosti za bezpečnosť spracovania osobných údajov na tretie strany.

V DataCentre bol vykonaný interný audit, ktorého časť sa týkala aj ochrany osobných údajov, kde neboli identifikované nedostatky vo vzťahu k poskytovaným službám pre MF SR.

Vzájomná komunikácia medzi MF SR a DataCentrom prebieha na úrovni zodpovednej osoby z hľadiska GDPR a ZOOÚ na strane MF SR a zodpovednej osoby z hľadiska GDPR a ZOOÚ na strane DataCentra priebežne telefonicky a e-mailom. Na e-mailovú adresu osobneudaje@datacentrum.sk prišlo za rok 2025 celkovo 15 správ, z toho 0 sa týkalo porušenia ochrany osobných údajov. V porovnaní prijatých správ za rok 2024 je to o 30 správ menej, keďže za rok 2024 prišlo celkovo 45 správ, z toho 0 sa týkalo porušenia ochrany osobných údajov.

V rámci jednotlivých úloh boli na spracovanie osobných údajov dodržané pokyny prevádzkovateľa.



<b>113</b>	<b>Poskytovanie sprostredkovateľských činností DataCentra pre MF SR v súlade s GDPR a zákonom o ochrane osobných údajov (DataCentrum v postavení ďalšieho sprostredkovateľa)</b>
------------	--

Na základe úloh popísaných v IL113 DataCentrum vykonáva pre MF SR spracovateľské činnosti, ktoré sa týkajú spracúvania osobných údajov. Pri týchto spracovateľských činnostiach je MF SR v pozícii sprostredkovateľa a DataCentrum v pozícii ďalšieho sprostredkovateľa.

DataCentrum na základe definovaných úloh v tejto oblasti zabezpečilo úroveň informačnej bezpečnosti a naplnenie legislatívnych požiadaviek, ktoré stanovuje GDPR a ZOOÚ. Medzi najdôležitejšie aktivity patrili:

- vypracovanie a aktualizácia záznamov o spracovateľských činnostiach, pri ktorých je DataCentrum v postavení ďalšieho sprostredkovateľa,
- podporné činnosti pri formulovaní otázok na ÚOOÚ na účely vyjasnenia nejasností v oblasti spracúvania osobných údajov,

DataCentrum využíva na spracúvanie osobných údajov služby tretích strán, v spolupráci s ktorými sa aktívne podieľa na zabezpečovaní ochrany osobných údajov vo vzťahu k poskytovaným službám pre MF SR.

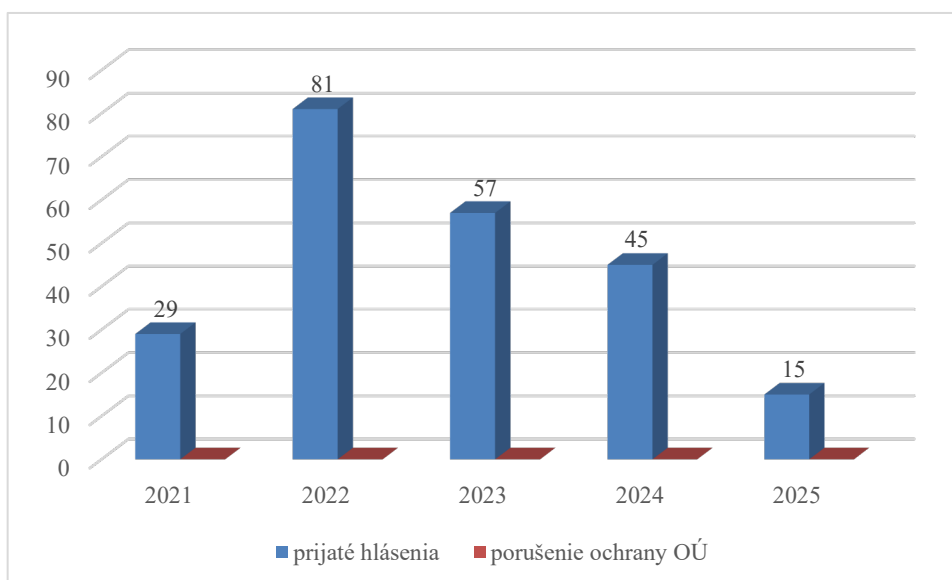
Pre riešenie požiadaviek GDPR a ZOOÚ týkajúcich sa služieb poskytovaných tretími stranami, boli identifikované a vypracované sprostredkovateľské zmluvy s týmito tretími stranami, prostredníctvom ktorých DataCentrum prenieslo časť zodpovednosti za bezpečnosť spracúvania osobných údajov na tretie strany.

V DataCentre bol vykonaný interný audit, ktorého časť sa týkala aj ochrany osobných údajov, kde neboli identifikované nedostatky vo vzťahu k poskytovaným službám pre MF SR.

Vzájomná komunikácia medzi MF SR a DataCentrom prebieha na úrovni zodpovednej osoby z hľadiska GDPR a ZOOÚ na strane MF SR a zodpovednej osoby z hľadiska GDPR a ZOOÚ na strane DataCentra priebežne telefonicky a e-mailom. Na e-mailovú adresu

osobneudaje@datacentrum.sk prišlo za rok 2025 celkovo 15 správ, z toho 0 sa týkalo porušenia ochrany osobných údajov. V porovnaní prijatých správ za rok 2024 je to o 30 správ menej, keďže za rok 2024 prišlo celkovo 45 správ, z toho 0 sa týkalo porušenia ochrany osobných údajov.

V rámci jednotlivých úloh boli na spracovanie osobných údajov dodržané pokyny sprostredkovateľa.



114	<b>Zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ZoKB)</b>
-----	--

Cieľom úlohy kontraktu je:

- vytvorenie formálneho rámca medzi MF SR a DataCentrom na zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností podľa ZoKB,
- definovanie rozsahu bezpečnostných opatrení a činností DataCentra pre zaistenie kybernetickej bezpečnosti pri prevádzke IS a sietí základných služieb MF SR,
- zabezpečenie riadenia bezpečnosti v rámci celého reťazca dodávateľov technológií, poskytovateľov služieb a tretích strán DataCentra a zabezpečenie ich spolupráce pri riešení kybernetických bezpečnostných incidentov.

Bezpečnostné opatrenia boli realizované v určenom rozsahu informačných systémov MF SR (CKS, RIS, ISUF, EIS, CRÚ a CES) pre oblasti:

- personálnej bezpečnosti,
- technických zraniteľností systémov a zariadení,
- oblasť riadenia bezpečnosti sietí a informačných systémov,
- riadenia prístupov,
- riešenia kybernetických bezpečnostných incidentov,
- monitorovania, testovania bezpečnosti a bezpečnostných auditov,
- fyzickej bezpečnosti,
- riadenia kontinuity procesov.

Uvedené informačné systémy sú prevádzkované v infraštruktúre DataCentra, ktorá je základnou službou (ZoKB). Táto infraštruktúra, ako aj bezpečnostné funkcie zabezpečujúce jej ochranu boli spravované v súlade s požiadavkami ZoKB a vyhlášky Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach (ďalej len „vyhláška NBÚ“).

V sledovanom období roka 2025 DataCentrum zaviedlo integrovaný manažérsky systém podľa noriem ISO 9001:2015 Manažérstvo kvality a ISO/IEC 27001:2022 Systém manažérstva informačnej bezpečnosti.

Pri výkone činností súvisiacich s prevádzkou základnej služby MF SR boli ďalej realizované aj nasledovné činnosti:

- komunikácia a koordinácia aktivít súvisiacich so zabezpečovaním súladu prevádzkovaných služieb a technológií s požiadavkami ZoKB a IL 114 s odborom informačnej bezpečnosti a kybernetickej bezpečnosti MF SR,
- vypracovanie plánov zálohovania pre systémy MF SR prevádzkované v DataCentre,
- testovanie havarijných plánov obnovy informačných systémov: CKS, RIS, ISUF, EIS, CRÚ a spustenie projektu vytvorenia prostredia CES v záložnej lokalite,
- monitoring informačnej bezpečnosti, distribúcia hlásení varovaní vydaných NBÚ, CSIRT.SK a NASES,
- koordinácia riešenia zraniteľností v IS a sieťach DataCentra s dodávateľmi, ktorí podporujú ich prevádzku,
- aktualizácia bezpečnostnej dokumentácie DataCentra súvisiacej so systémami MF SR prevádzkovanými v DataCentre,
- zabezpečovanie odstraňovania zistení z auditu kybernetickej bezpečnosti DataCentra,
- aktualizácia stavu ošetrovania rizík z analýzy rizík MF SR za opatrenia v kompetencii DataCentra.
- bolo identifikovaných 7 rizík s priemernou hodnotou 7,14 (v rozsahu 1 - 8).

Pre oblasť riadenia poskytovania služieb tretími stranami boli realizované nasledovné činnosti:

- komunikácia s tretími stranami DataCentra, ktoré participujú na realizácii činností pre udržanie a zlepšovanie úrovne kybernetickej bezpečnosti DataCentra,
- vykonanie školení o bezpečnostných opatreniach a pravidlách, ktorých dodržiavanie je nevyhnutné na zabezpečenie informačnej a kybernetickej bezpečnosti prevádzkovaných technológií,
- priebežné sledovanie a vyhodnocovanie činnosti tretích strán v oblasti kybernetickej bezpečnosti.

DataCentrum vypracúva pravidelný prehľad o stave kybernetickej bezpečnosti za rok 2025, najmä o detegovaných kybernetických bezpečnostných incidentoch (KBI), ich druhoch, závažnosti, true positive/false positive rate hlásení bezpečnostných udalostí, priemernom čase detekcie a reakcie na KBI, vyhodnotenie bezpečnostných trendov a efektivity prijatých bezpečnostných opatrení a informácie týkajúce sa manažmentu zraniteľností, identifikovaných a opravených zraniteľností v závislosti od ich kategorizácie. Tento prehľad o stave kybernetickej bezpečnosti DataCentrum zasiela MF SR.

V sledovanom období nebol v DataCentre zaznamenaný závažný kybernetický bezpečnostný incident.

V roku 2025 bol Centrom podpory používateľov (CPU) vykonaný komplex činností v prospech používateľov informačných systémov prevádzkovaných DataCentrom pre rezort MF SR.

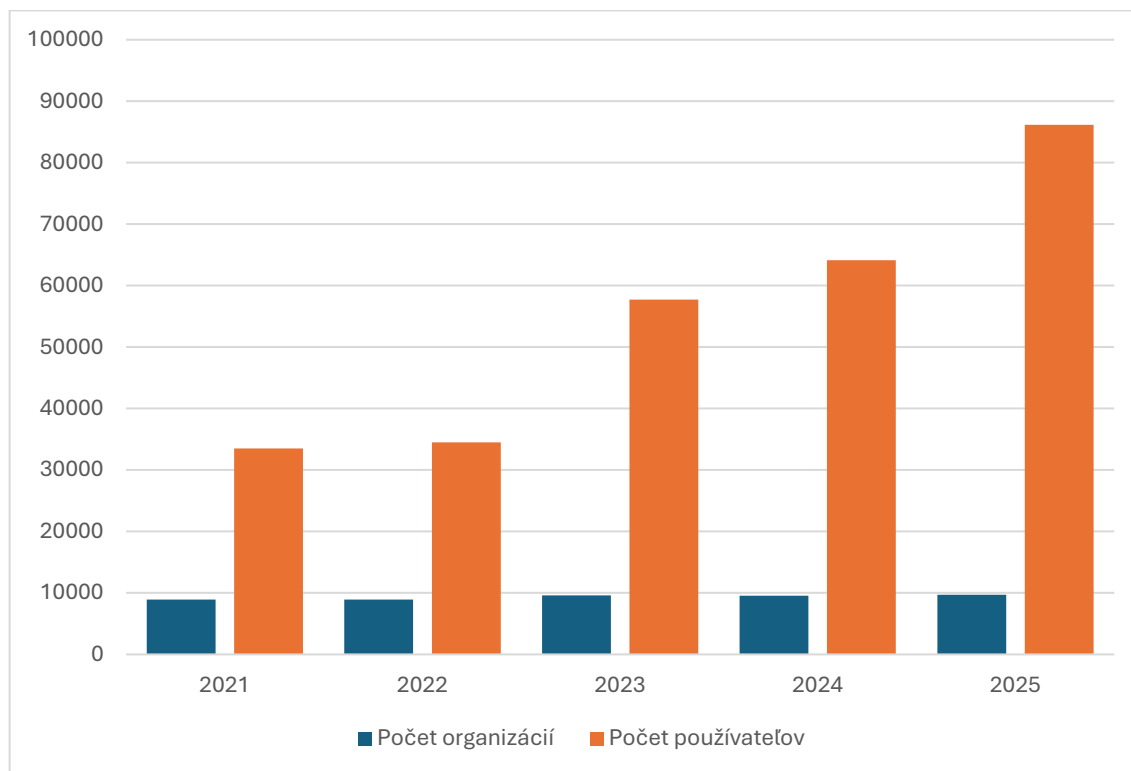
CPU riešilo požiadavky zo strany organizácií a používateľov informačných systémov na aplikačnú, metodickú a technickú podporu a priebežne budovalo a dopĺňalo databázu často kladených otázok. Súčasne bola priebežne aktualizovaná databáza organizácií a používateľov používajúcich informačné systémy a komunikačno-technologickú infraštruktúru (KTI).

Zmeny súviseli najmä s uvedením nových IS do prevádzky, prípadne ich modulov a so zánikom, vznikom a zlučovaním organizácií, respektíve s ich preradením pod iného zriaďovateľa, zmenou právnej formy organizácií a aj s fluktuáciou zamestnancov.

Počet organizácií používajúcich aspoň jeden informačný systém prevádzkovaný DataCentrom bol 9 706.

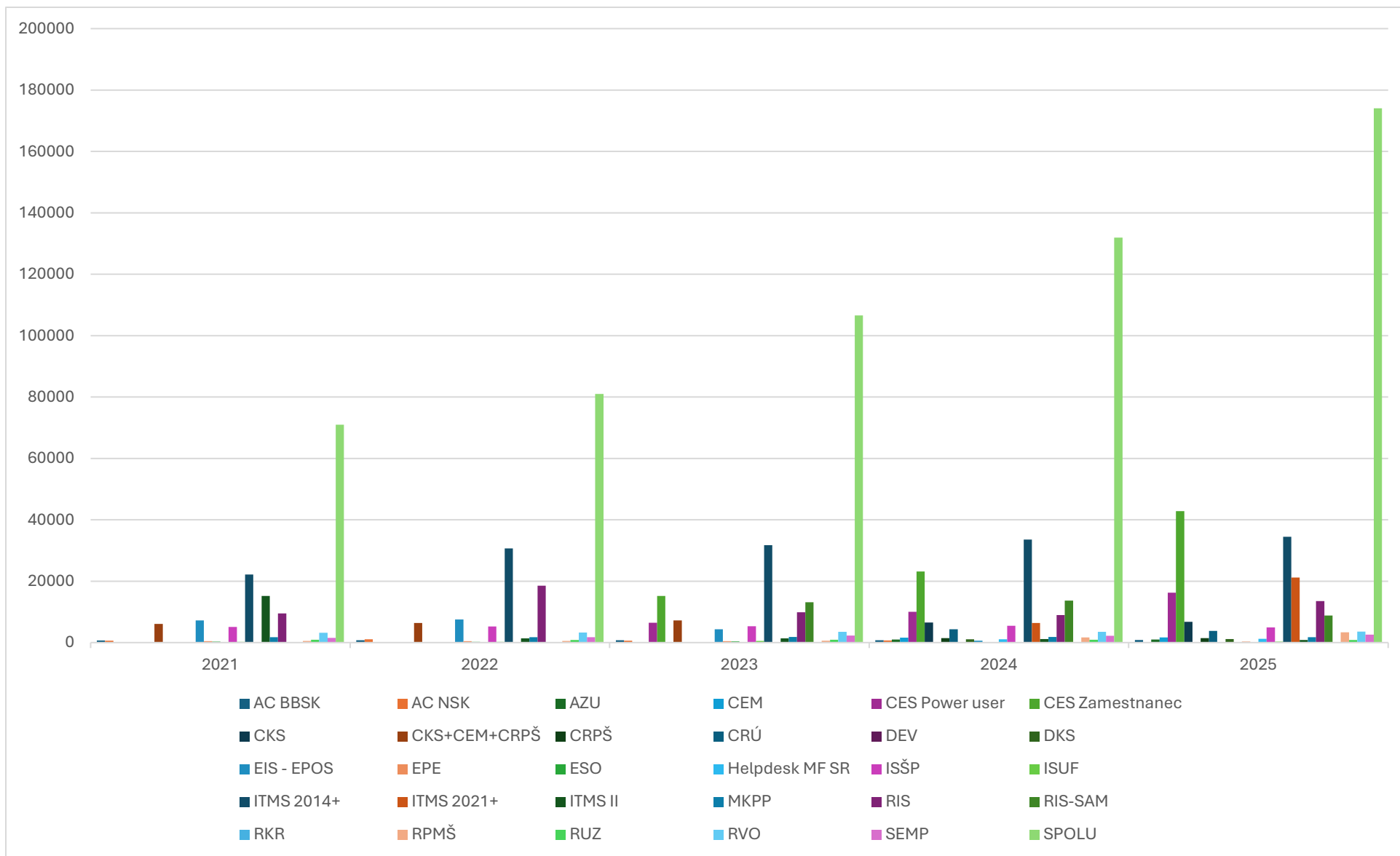
Počet používateľov s aspoň jedným aktívnym prístupom do infraštruktúry informačno-komunikačných technológií prevádzkovaných DataCentrom bol 86 148. Nárast počtu používateľov nastal v dôsledku rozširovania CES, v ktorom sú evidovaní všetci zamestnanci pripojených organizácií, nie iba používatelia modulov CES.

Počet organizácií a používateľov v porovnaní s predchádzajúcimi rokmi:



CPU ku dňu 31. 12. 2025 eviduje pre jednotlivé informačné systémy nasledujúce počty používateľov:

Počet používateľov	Názov systému
4 909	IS ŠP (Informačný systém štátnej pokladnice)
22 384	RIS (rozpočtový informačný systém) z toho: 8 833 ks v RIS (Rozpočtový informačný systém pre štátnu a verejnú správu), 13 551 ks v RIS.SAM (Rozpočtový informačný systém pre samosprávu)
6 801	CKS (centrálny konsolidačný systém)
1 653	CEM (informačný systém centrálna evidencia majetku)
1 470	CRPŠ (centrálny register pohľadávok štátu)
814	ITMS Core (monitorovací systém účtovníctva fondov)
34 497	ITMS 2014+ (IT monitorovací systém pre Európske štrukturálne a investičné fondy pre programové obdobie 2014 - 2020)
21 188	ITMS21+ (IT monitorovací systém pre Európske štrukturálne a investičné fondy pre programové obdobie od r. 2021)
182	ISUF (informačný systém účtovníctva fondov)
1 787	MKPP (multiklientský platobný portál VÚC)
839	AC BBSK (administratívne centrum BBSK)
193	AC NSK (administratívne centrum NSK)
287	EPE (portál MZV SR)
142	ESO (ekonomický systém MF)
880	RÚZ (centrálny RÚZ – neverejná časť)
2 559	SEMP (informačný systém Evidencia a monitoring štátnej pomoci)
3 558	RVO (register vylúčených osôb)
3 323	RPMŠ (register ponúkaného majetku štátu)
98	DEV (rozvoj)
59 110	CES (centrálny ekonomický systém) z toho: 42 825 ks ako CES zamestnanec, 16 285 ks ako CES power user.
3 789	CRÚ (centrálny register účtov)
1 226	Helpdesk MF SR
1 018	AZÚ (analytický zber údajov)
1 172	DKS (dokumentačný IS pre MF SR)



Zmeny v počtoch aktívnych používateľov sú pri jednotlivých informačných systémoch z nasledovných dôvodov:

- IS ŠP – prebiehalo aktualizovanie databázy RRP od neaktívnych používateľov,
- RIS a RIS.SAM – zlučovanie organizácií a tým znížený počet používateľov, prebiehalo aktualizovanie databázy RRP od neaktívnych používateľov,
- ITMS – zvýšený záujem používateľov o zapojenie sa do výziev,
- AC NSK – prebiehalo aktualizovanie databázy RRP od neaktívnych používateľov,
- RPMŠ – zvýšil sa záujem o ponuky typu nájom, ide o záujemcov ako fyzické osoby, SZČO a firmy, ktorí sa registrovali, aby boli notifikovaní o ponukách,
- CES – spustenie II. vlny nových používateľov,
- CRÚ – používatelia zrušili svoje prístupy, keďže vyhodnotili, že nebudú pristupovať do systému (nový IS z roku 2024).

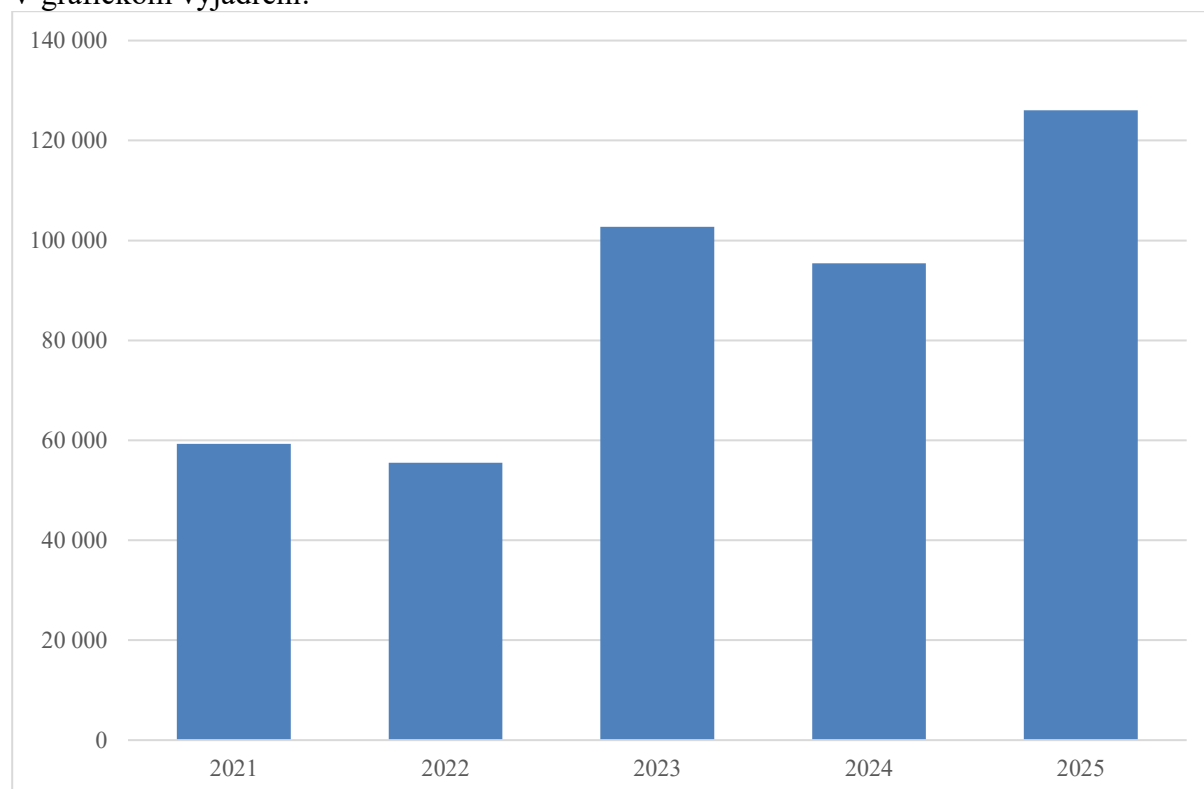
V priebehu roku 2025 používatelia kontaktovali CPU 126 028x, z toho:

- vykonali 43 371 telefonických volaní do CPU, čo predstavuje priemerne 3 614 mesačne a 834 volaní týždenne,
- používatelia poslali 39 879 e-mailov s požiadavkou na službu CPU,
- cez internetové rozhranie vytvorili 38 478 požiadaviek na službu CPU,
- poštou poslali 4 300 požiadaviek.

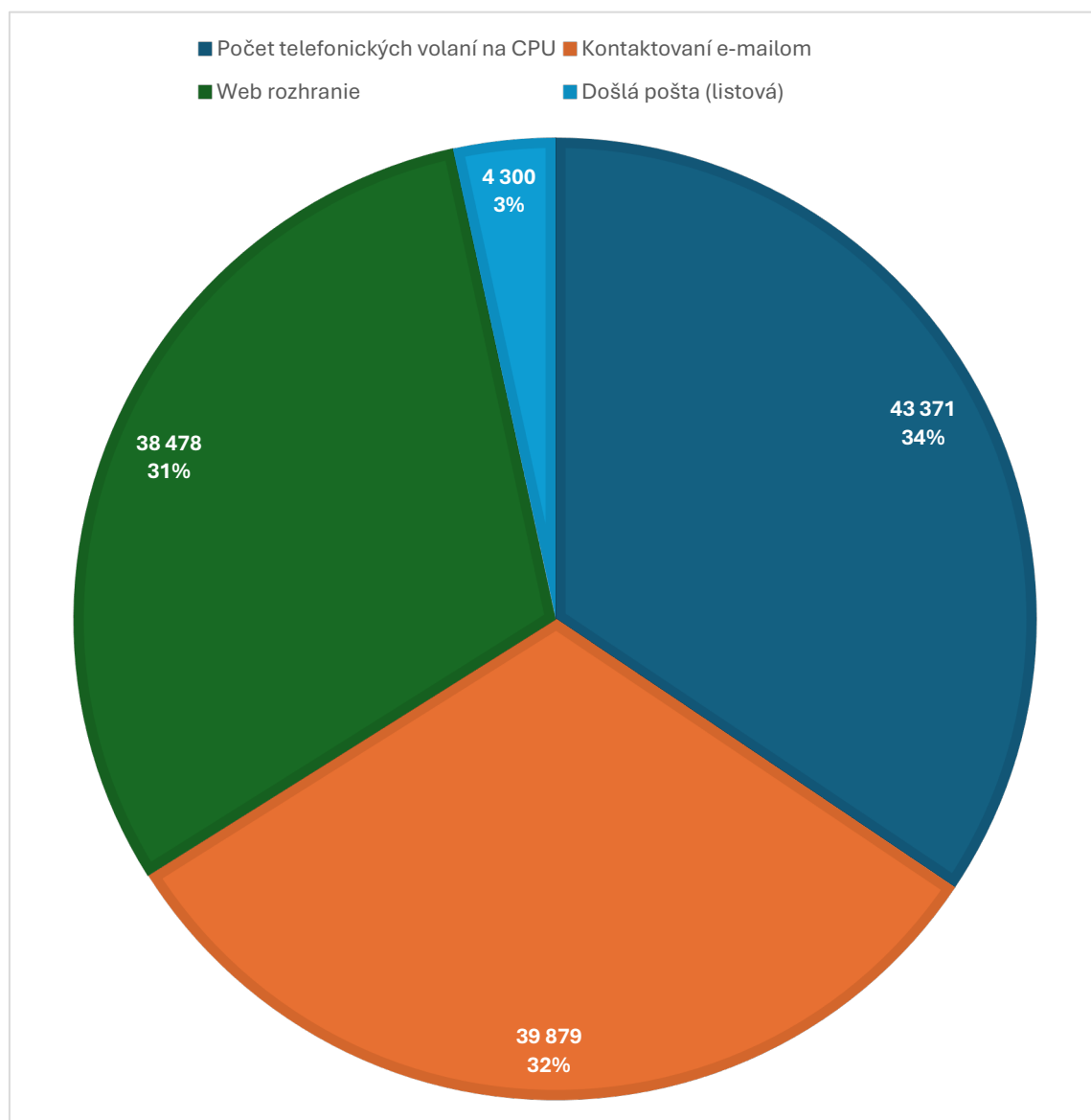
Počet kontaktovaní CPU v porovnaní s predchádzajúcimi rokmi:

2020	2021	2022	2023	2024	2025
72 725	59 319	55 512	102 710	95 432	126 028

V grafickom vyjadrení:



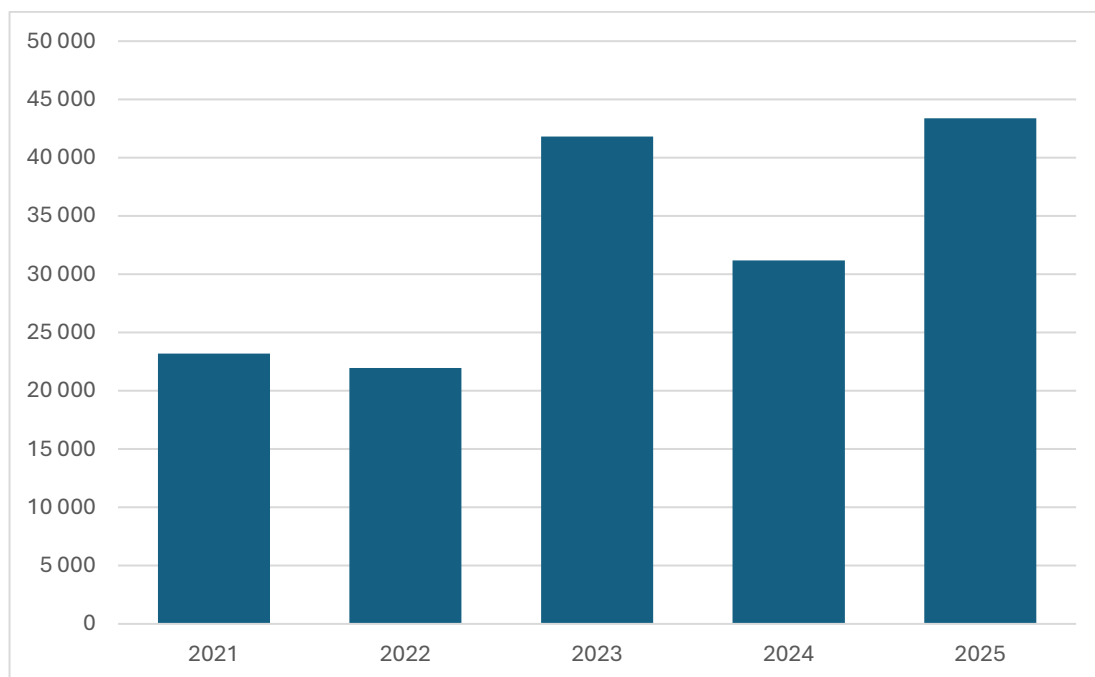
## Typ kontaktov na CPU za rok 2025:



## Počet uskutočnených telefonických volaní na CPU v porovnaní s predchádzajúcimi rokmi:

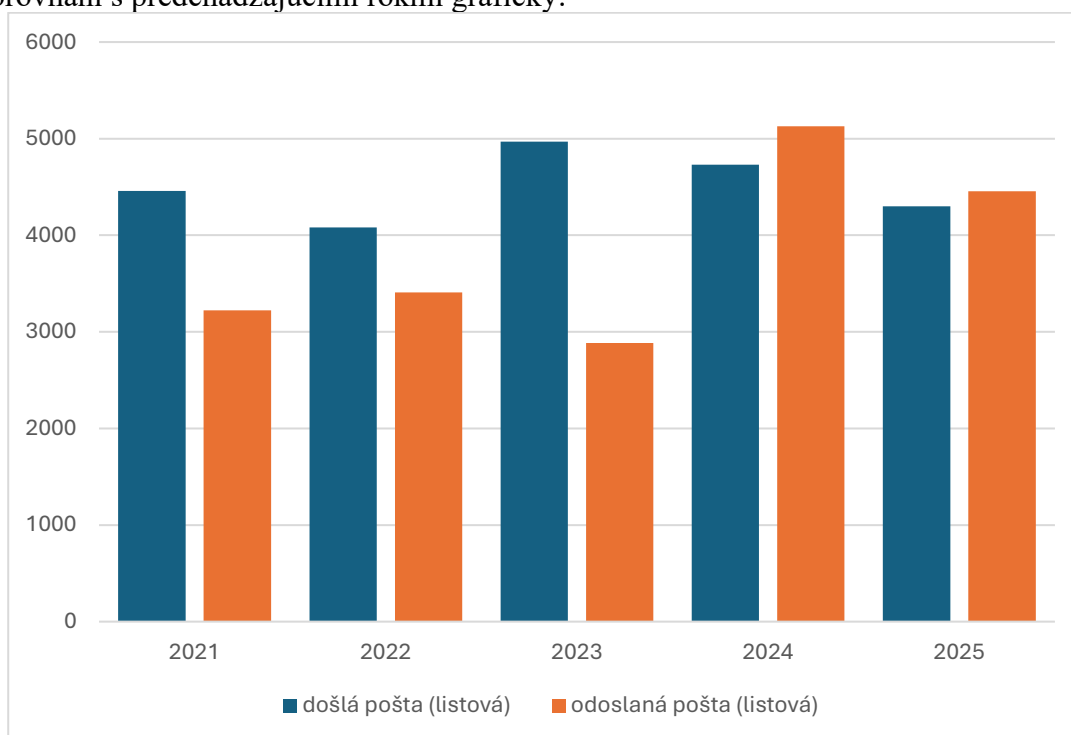
2020	2021	2022	2023	2024	2025
27 966	23 183	21 953	41 813	31 176	43 371

V grafickom vyjadrení:



CPU v roku 2025 prijalo 4 300 listových požiadaviek na službu a odoslalo používateľom 4 454 listových zásielok. Ich počet navzájom nekorešponduje, keďže nie vždy ide o rovnaký typ agendy a zahŕňa všetky oddelenia odboru.

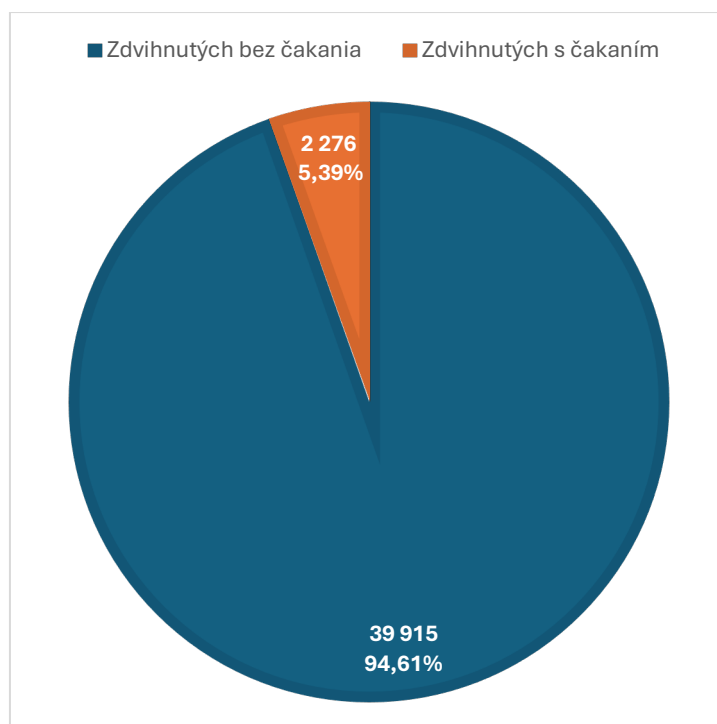
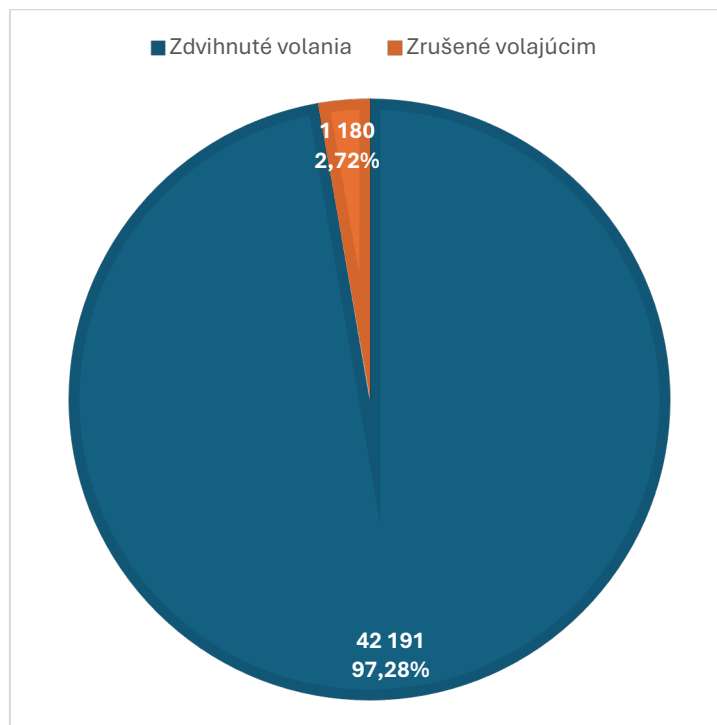
V porovnaní s predchádzajúcimi rokmi graficky:



V hodnotenom období bolo zaregistrovaných 43 371 telefonických volaní do CPU. Z toho bolo 42 191 (97,28 %) volaní zdvihnutých a 1 180 (2,72 %) bolo zrušených volajúcim.

Z počtu zdvihnutých volaní bolo zdvihnutých bez čakania 39 915 (94,61 %) a 2 276 (5,39 %) volaní bolo zdvihnutých s čakaním, čo znamená, že hovor nebol zdvihnutý ihneď, ale užívateľ musel počkať na uvoľnenie linky pre nasledovné spojenie s operátorom.

Údaje sú graficky vyjadrené nasledovne:



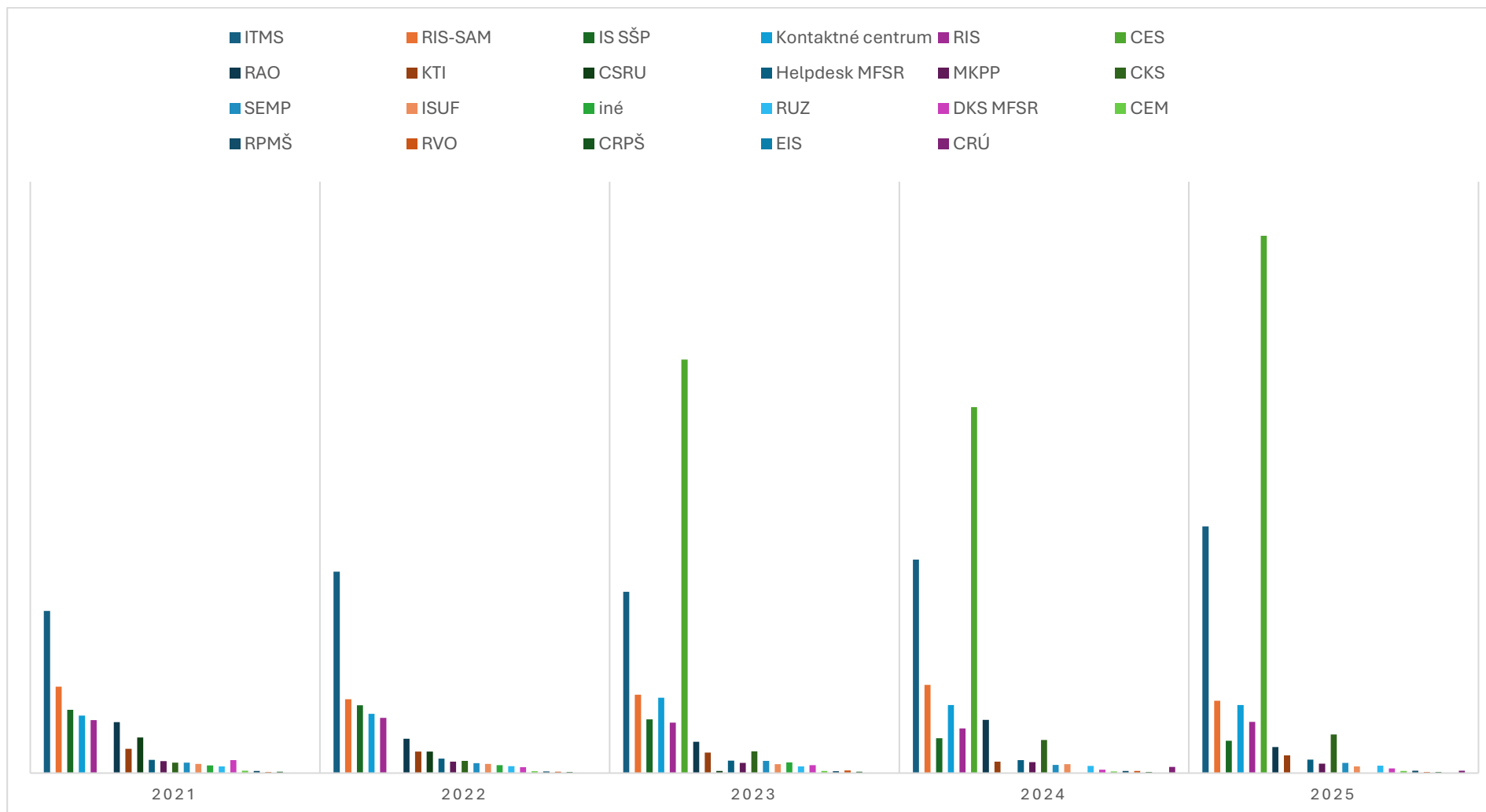
Počet hlásení uzatvorených jednotlivými pracovnými skupinami v porovnaní s predchádzajúcimi rokmi:

<b>Rok</b>	<b>2021</b>	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>2025</b>
ITMS	12 343	15 321	13 802	16 256	18 776
RIS.SAM	6 580	5 623	5 960	6 705	5 513
IS ŠP	4 819	5 167	4 081	2 654	2 455
Kontaktné centrum	4 384	4 511	5 743	5 173	5 180
RIS	4 038	4 199	3 846	3 404	3 904
CES	*	*	31 472	27 850	40 896
RAO	3 877	2 609	2 389	4 054	1 987
KTI	1 858	1 639	1 557	873	1 342
CSRU	2 719	1 637	164	0	*
Helpdesk MF SR	1 014	1 093	940	990	1 020
MKPP	902	866	774	840	716
CKS	793	926	1 654	2 512	2 942
SEMP	796	759	935	618	775
ISUF	702	707	685	687	510
iné	583	612	822	0	0
RÚZ	513	521	512	538	561
DKS MF SR	987	442	605	267	346
CEM	185	149	168	126	162
RPMŠ	156	124	146	158	185
RVO	91	115	193	165	94
CRPŠ	98	81	101	81	78
EIS	2	6	1	5	**
CRÚ	*	*	*	478	189
<b>Spolu</b>	<b>47 440</b>	<b>47 107</b>	<b>76 550</b>	<b>74 434</b>	<b>87 631</b>

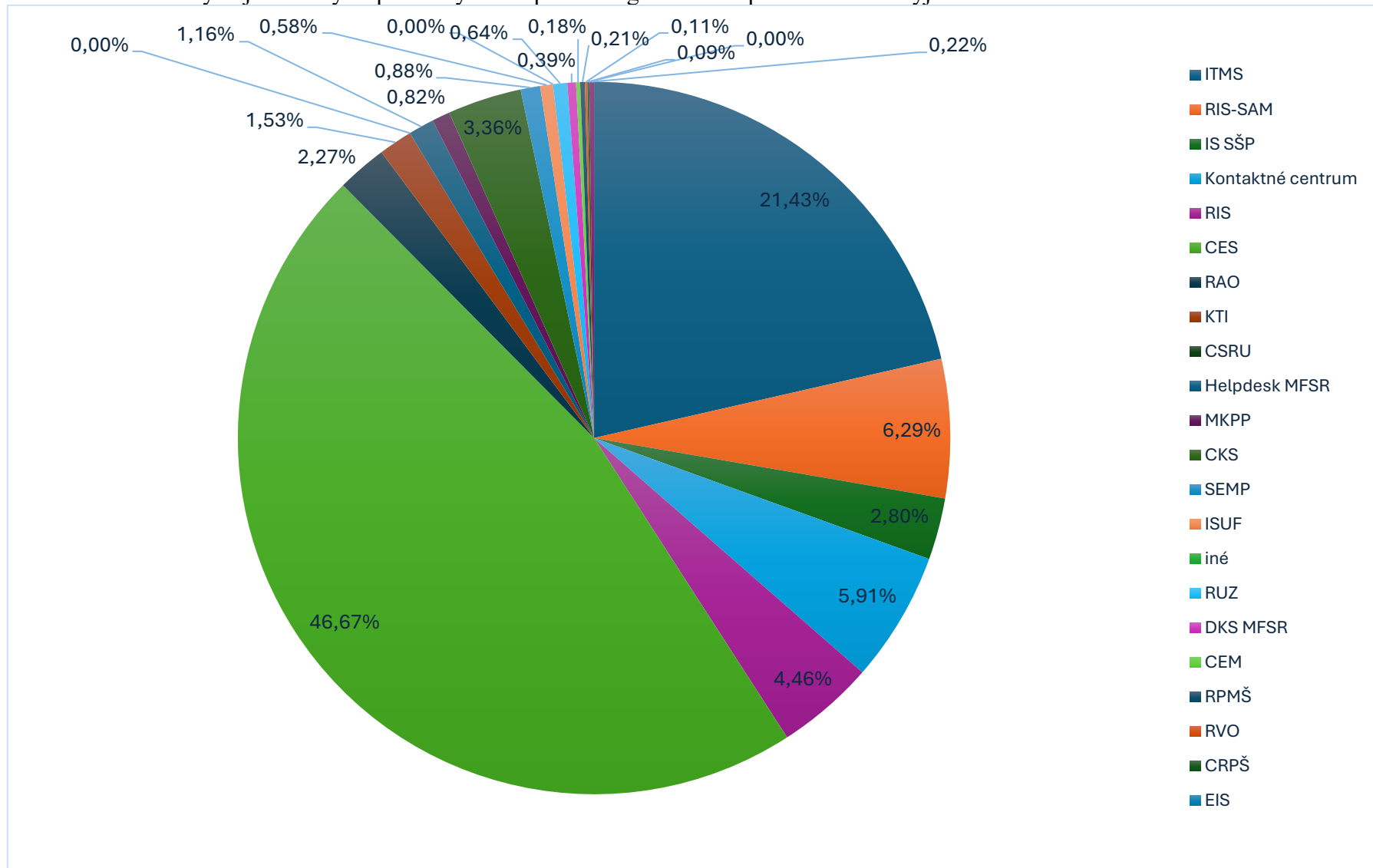
\* údaje nie sú k dispozícii

\*\* modul prešiel pod aplikáciu CES

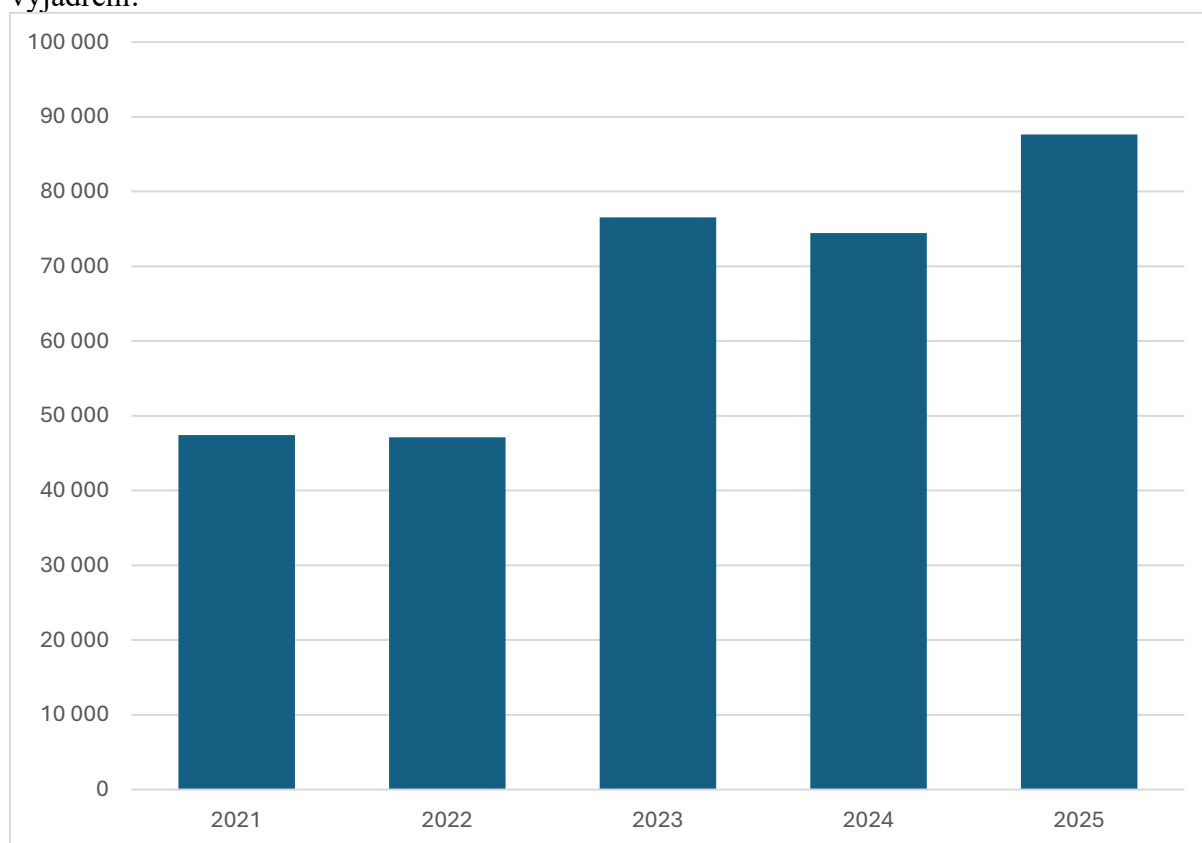
V grafickom vyjadrení počet hlásení uzatvorených jednotlivými pracovnými skupinami v porovnaní s predchádzajúcimi rokmi:



Počet hlásení uzatvorených jednotlivými pracovnými skupinami v grafickom - percentuálnom vyjadrení:



Porovnanie počtu uzatvorených hlásení „spolu“ s predchádzajúcimi rokmi v grafickom vyjadrení:



V roku 2025 CPU poskytovalo aplikačnú podporu na úrovni L1 pre informačný systém DKS MF SR.

Počet požiadaviek na podporu v roku 2025 - podľa jednotlivých modulov informačného systému:

<b>DKS/DKS SLA - MF SR</b>	<b>2025</b>
Absencia	0
Autodoprava	0
MF SR DKS - Manager	134
Nezaradené	102
Podania	0
Požiadavky na objednávku	14
Pracovné cesty	0
Pripomienkové konania	0
Spoločné	0
Správa registratúry	106
Zmluvy a dohody	9
<b>SPOLU</b>	<b>365</b>

Vyhodnotenie hodnotiacich kritérií:

Hodnotiace kritérium	2025	%	splnené
vyriešených do 24 hod.	65 724	75 %	A
vyriešených do 48 hod.	17 526	20 %	A
nad 48 hod.	4 381	5 %	A
reklamácie a sťažnosti	0	0 %	A
<b>spolu</b>	<b>87 631</b>	<b>100 %</b>	<b>A</b>

Hodnotiace kritérium je v súčasnosti vyhodnocované na základe kvalifikovaného odborného odhadu, keďže aktuálne používaný systém neumožňuje automatizované sledovanie a jednoznačné vyčíslenie daného SLA parametra. Po nasadení nového systému, ktorý bude poskytovať presné a merateľné údaje o plnení SLA ukazovateľov, bude toto hodnotiace kritérium vyhodnocované priamo na základe týchto exaktných dát.

CPU aktívne prispieva k plneniu podmienok certifikátu kvality poskytovania služieb ISO 9001:2008, participuje na realizácii projektov Problem Management, Incident Management, Change Management a Access & 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 podporu hardvérového a softvérového vybavenia u používateľa a postúpenie požiadaviek na 3. úroveň. (Poskytovateľ podpory: DataCentrum, dodávateľ).

**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.

<b>122</b>	<b>Podpora používateľov informačného systému CKS</b>
------------	--

Pri plnení úlohy DataCentrum v hodnotenom období zabezpečovalo pomoc používateľom pri používaní Informačného systému Centrálny konsolidačný systém (ďalej len „CKS“) na 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. V roku 2024 prevzalo CPU úlohu poskytovania podpory pri navigácii používateľov IS CKS na účely podpory zberu finančných a účtovných výkazov, konsolidácie, odsúhlasovania vzájomných vzťahov, ukladania účtovných závierok a ďalších dokumentov. Súčasne sú plnené úlohy prislúchajúce technickému zabezpečeniu prevádzky systému. Keďže sú všetky hlásenia uzatvárané na úrovni L2 (CKS DC), nevieme v súčasnom tiketovacom nástroji odlišiť, ktoré boli riešené aj s pomocou

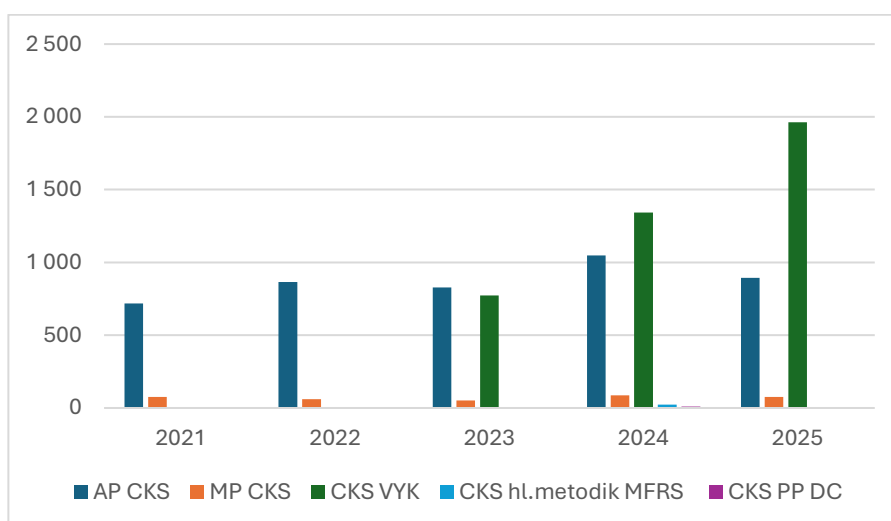
podpory na MF SR. V roku 2026 prejde CPU na nový tiketovací nástroj, kde už bude táto štatistika dostupná.

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

Rok	2020	2021	2022	2023	2024	2025
AP CKS	745	718	865	829	1 048	895
MP CKS	95	75	61	52	88	77
CKS VYK	*	*	*	773	1 342	1 964
CKS hl.metodik MF SR	*	*	*	*	24	3
CKS PP DataCentrum	*	*	*	*	10	3
<b>Spolu</b>	<b>840</b>	<b>793</b>	<b>926</b>	<b>1 654</b>	<b>2 512</b>	<b>2 942</b>

(Pozn.: AP – aplikačná podpora, MP – metodická podpora, VYK – výkazníctvo, PP – prevádzková podpora)

V grafickom vyjadrení:



Vyhodnotenie hodnotiacich kritérií:

Hodnotiace kritérium	2025	%	splnené
vyriešených do 24 hod.	2 559	87 %	A
vyriešených do 48 hod.	207	7 %	A
nad 48 hod.	176	6 %	A
reklamácie a sťažnosti	0	0 %	A
<b>spolu</b>	<b>2 942</b>	<b>100 %</b>	<b>A</b>

Hodnotiace kritérium je v súčasnosti vyhodnocované na základe kvalifikovaného odborného odhadu, keďže aktuálne používaný systém neumožňuje automatizované sledovanie a jednoznačné vyčíslenie daného SLA parametra. Po nasadení nového systému, ktorý bude poskytovať presné a merateľné údaje o plnení SLA ukazovateľov, bude toto hodnotiace kritérium vyhodnocované priamo na základe týchto exaktných dát.

**123 Systémová a metodická podpora používateľov informačného systému CES**

Systémová, metodická a aplikačná podpora pre používateľov CES (Centrálny ekonomický systém) bola poskytovaná realizáciou ucelenej sady činností zahŕňajúcej riešenie problémov s prihlásením, vytvorením konta používateľa, nastavením rolí, kompetencií, realizáciou transakcií a ovládaním funkcionalít pri používaní nástrojov informačného systému určeného na zabezpečenie konkrétnej technologickej funkčnosti alebo na zabezpečenie elektronického výkonu činností implementovaných modulov CES.

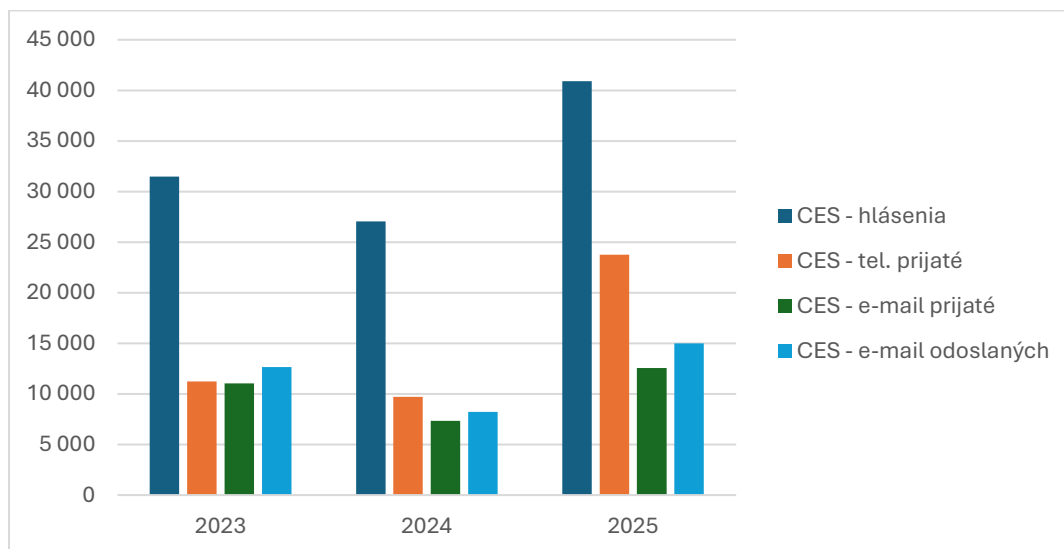
Metodická podpora bola realizovaná poskytovaním informácií, konzultačnými činnosťami a sprostredkovaním riešenia požiadaviek s kompetentnými pracovníkmi MF SR. Aplikačná podpora bola realizovaná poskytovaním, sprostredkovaním informácií, konzultácií, návodov, inštrukcií, odpovedí, dokumentov a postupov vecne relevantných s agendou aplikovanou v CES.

V danom roku pri realizácii úlohy eviduje CPU 77 210 požiadaviek na podporu CES, z toho 40 896 cez tiketovací nástroj SOLMAN, 23 756 telefonických volaní na číslo CPU-CES. Bolo prijatých 12 558 e-mailových požiadaviek na službu a odoslaných odhadom 15 000 e-mailových správ.

Rok	2025
CES - hlásenia	40 896
CES - e-mailové požiadavky prijaté	12 558
CES - telefonické volania prijaté	23 756
<b>Spolu</b>	<b>77 210</b>

Rok	2025
CES – odoslaných e-mailových správ	15 000

V grafickom vyjadrení:



Podľa zmluvy o implementácii CES a poskytovaní aplikačnej podpory nie je pre L1, ktorú prevádzkuje CPU, stanovená SLA. Z tohoto dôvodu nie je možné určiť jej plnenie. Ukazovateľ, ktorý máme k dispozícii, je počet reklamácií, ktoré sa týkali prevažne aplikácie samotnej a nie podpory CPU CES.

Hodnotiace kritérium	2025	%	splnené
reklamácie a sťažnosti neuznané	36	35 %	A
reklamácie a sťažnosti uznané	67	65%	A
<b>spolu</b>	<b>103</b>	<b>100 %</b>	<b>A</b>

Hodnotiace kritérium je v súčasnosti vyhodnocované na základe kvalifikovaného odborného odhadu, keďže aktuálne používaný systém neumožňuje automatizované sledovanie a jednoznačné vyčíslenie daného SLA parametra. Po nasadení nového systému, ktorý bude poskytovať presné a merateľné údaje o plnení SLA ukazovateľov, bude toto hodnotiace kritérium vyhodnocované priamo na základe týchto exaktných dát.

## 151 Integrovaný manažérsky systém DataCentra

DataCentrum v priebehu roka 2024 a 2025 zaviedlo integrovaný manažérsky systém v zmysle požiadaviek noriem ISO 9001:2015 (Systém manažérstva) a ISO 27001:2018 (Systém manažérstva informačnej bezpečnosti).

V roku 2025 DataCentrum v súvislosti so systémom integrovaného manažérstva kvality plnilo hlavne nasledujúce úlohy:

- riadenie dokumentácie,
- riadenie rizík,
- realizácia auditov,
- realizácia nápravných opatrení,
- zvyšovanie povedomia zamestnancov o zavedenom systéme riadenia kvality.

V roku 2025 bola vykonaná pravidelná revízia internej riadenej dokumentácie (politiky, príručka systémov integrovaného manažérstva, smernice, príkazy riaditeľa, pracovné postupy) a externej riadenej dokumentácie. V prípade potreby bola interná riadená dokumentácia aktualizovaná, prípadne vydaná nová. V priebehu roka 2025 bolo aktualizovaných 21 smerníc a 17 pracovných postupov, a zároveň bolo vydaných 5 nových smerníc. Rovnako boli aktualizované aj zoznamy externej riadenej dokumentácie.

Celá interná riadená dokumentácia je dostupná všetkým zamestnancom DataCentra prostredníctvom intranetu a kriteriálne výtlačky internej riadenej dokumentácie sú uložené vo fyzickej podobe u manažéra IMS v DataCentre.

V roku 2025 bolo vykonané pravidelné prehodnotenie analýzy rizík a plánu zvládania rizík. Zároveň bola vykonaná kontrola plnenia prijatých opatrení vyplývajúcich z plánu zvládania rizík, príp. vyhodnotená efektívnosť implementovaných opatrení.

V roku 2025 boli realizované dva hlavné audity, a to v mesiaci 04/2025 interný audit a v mesiaci 06/2025 externý recertifikačný, ktoré boli zamerané na preverenie plnenia požiadaviek systému integrovaného manažerstva kvality v DataCentre. Interné audity preukázali dodržiavanie štandardu kvality, ale zároveň odhalili aj niektoré nedostatky a možnosti na zlepšovanie.

Zistené nedostatky a odporúčania na zlepšovanie z interných auditov, externých auditov, ako aj podnety od samotných zamestnancov DataCentra boli riešené formou prijímania nápravných opatrení a ich realizáciou kontinuálne počas celého roku 2025.

V máji 2025 bolo realizované školenie o zavedenom integrovanom manažérskom systéme s cieľom zvyšovať povedomie zamestnancov DataCentra v tejto oblasti.

V rámci recertifikačného auditu neboli identifikované nezhody a DataCentrum si obhájilo certifikát v zmysle požiadaviek noriem ISO 9001:2015 (Systém manažerstva) a ISO 27001:2018 (Systém manažerstva informačnej bezpečnosti).

Hodnotiace kritériá úlohy - úspešné absolvovanie kontrolného auditu, odstraňovanie zistených nedostatkov a zlepšovanie integrovaného manažérského systému - boli splnené.

<b>161</b>
------------

<b>Centrálny monitoring a prevádzka dátového centra – CMPDC</b>
---

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

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

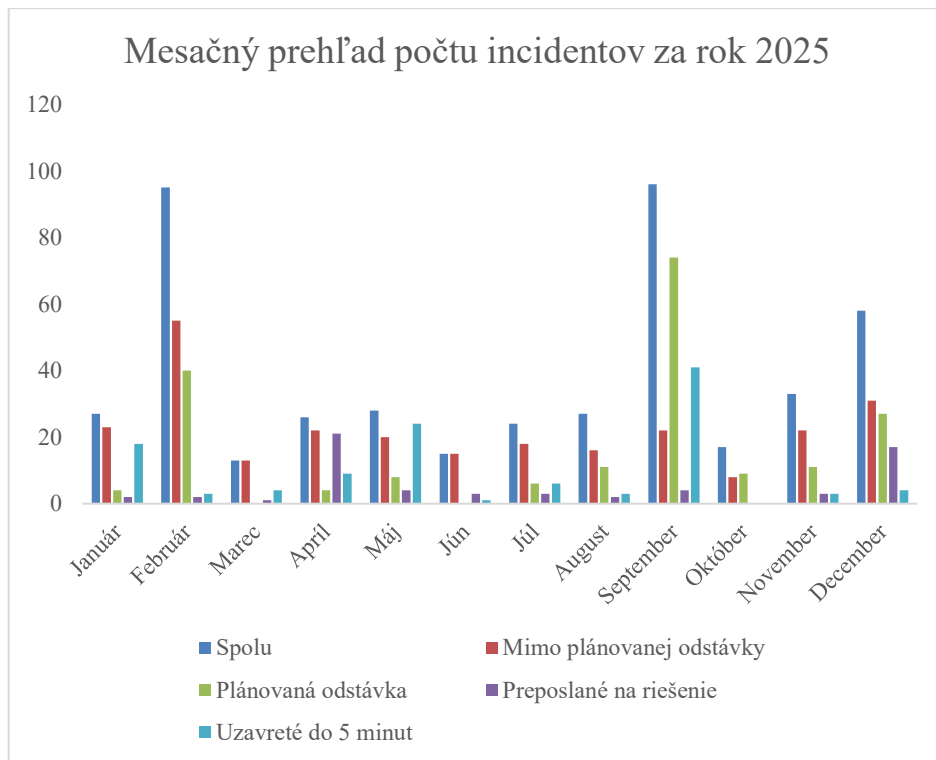
Zaradeniu každého nového informačného systému do monitorovania v DataCentre predchádza analýza a špecifikácia jeho stavov, ktoré budú monitorované.

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

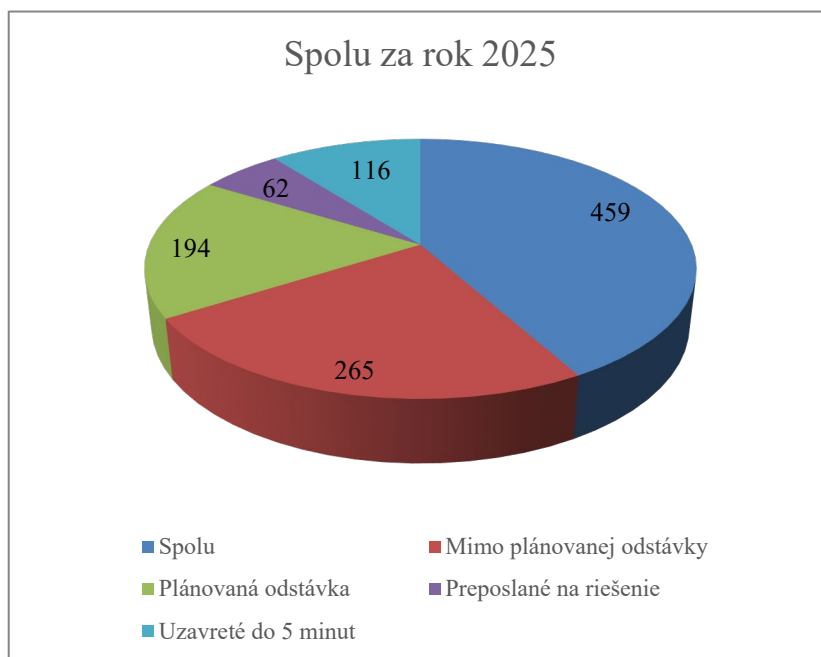
Riešenie incidentov, ktoré pridelí operátor CMPDC na riešenie riešiteľom, sú vykonávané v úzkej spolupráci s pracovníkmi Konzoly 1 a Konzoly 2.

Pridelenie incidentov operátorom CMPDC riešiteľovi, následná notifikácia riešiteľa o incidentoch, sledovanie procesu riešenia incidentov a po ich vyriešení ich uzavretie v HP Service Manager-i vedie ku korelácii kvality služieb dodávateľov v zmysle platných SLA.

Zjednodušený mesačný a ročný prehľad incidentov, riešených oddelením CMPDC uvádzame na nasledujúcich dvoch obrázkoch.



Obrázok 1 - Mesačný prehľad incidentov 2025.



Obrázok 2 - Ročný prehľad incidentov 2025.

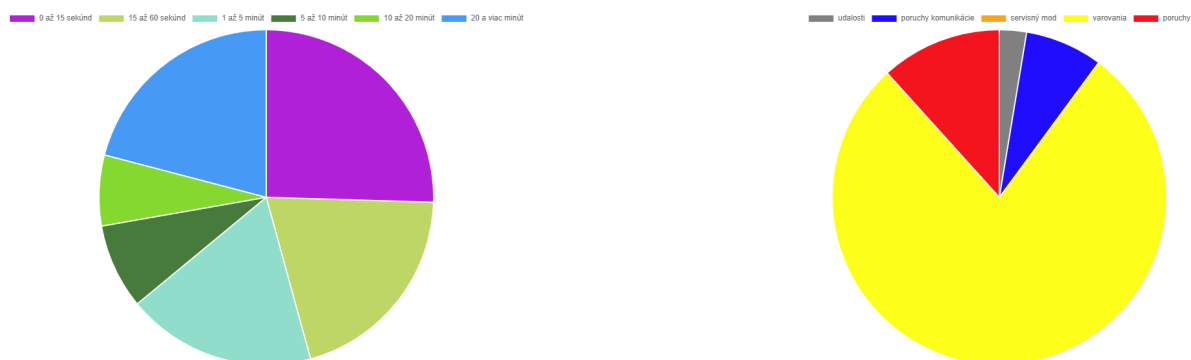
Oddelením CMPDC bolo v roku 2025 riešených viac ako 450 incidentov, z čoho najčastejšie boli riešené incidenty mimo plánovanej odstávky v počte 265 ks.

Operátori CMPDC pracujú v nepretržitej prevádzke 24/7/365. Počas roka 2025 neboli realizované žiadne zmeny funkcionality monitorovacieho systému, ktoré by si vyžadovali zaškolenie operátorov. Všetci operátori CMPDC absolvovali pravidelné ročné preškolenie na prácu s monitorovacím systémom. V prípade potreby zaškolenia sa však takéto školenia vykonávajú počas pracovnej doby, bez prerušenia prevádzky.

Oddelenie CMPDC tiež zabezpečuje:

- spracovanie uzávierok IS ŠP, kontroly komunikačných kanálov pre IS ŠP, kontrolné prihlásenia do vybraných systémov IS ŠP, dohľad nad bezpečnosťou priestorov, v ktorých sú prevádzkované IS a KTI a v ktorých pracujú zamestnanci externých firiem,
- dohľad nad podpornou infraštruktúrou dátových centier DC-C a DC-K (klimatizácie, UPS, zdroje el. energie) a prevádzkovaných informačných systémov.

Zjednodušený sumár alarmov z dohľadu nad podpornou infraštruktúrou DC-C uvádzame na nasledujúcom obrázku.

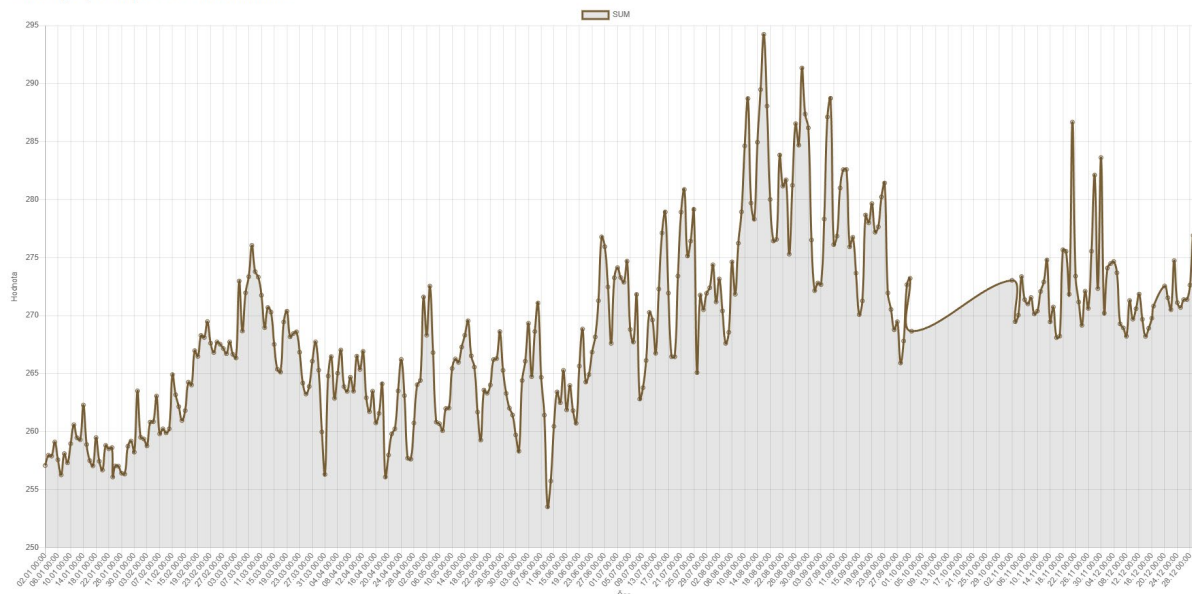


Obrázok 3 - Sumár alarmov podpornej infraštruktúry DC-C za rok 2025.

V tomto prípade sú najpočetnejšie alarmy typu „varovania“ v počte 3 106 ks, ktoré informujú napríklad o zmene stavu monitorovaných zariadení a môžeme ich zaradiť k bežným prevádzkovým stavom dátového centra. Nasledujú bežné „poruchy“ v počte 465 ks a „poruchy komunikácie“ jednotlivých zariadení v počte 298 ks.

V súčinnosti s dohľadom nad podpornou infraštruktúrou, prebieha aj monitorovanie výkonu dátového centra, na ktorý má výrazný vplyv nárast požiadaviek na výkon jednotlivých informačných systémov, ako aj nárast počtu jednotlivých prevádzkovaných informačných systémov. V roku 2025 sa celkový priemerný výkon dátového centra pohyboval na úrovni približne 275 kW elektrickej energie, ako je uvedené na obrázku číslo 4.

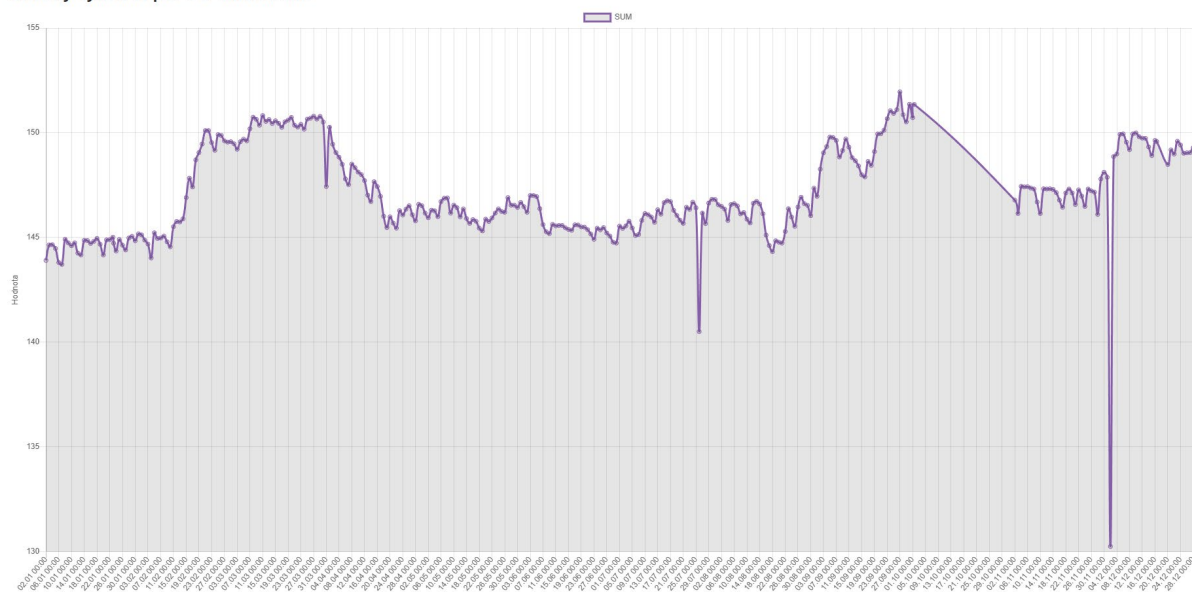
#### Celkový výkon pre DC Cintorinska



Obrázok 4 - Celkový výkon dátového centra v roku 2025

Samotnú spotrebu prevádzkovaných informačných technológií, uvádza obrázok číslo 5 a v ročnom priemere ide o hodnotu približne 150 kW.

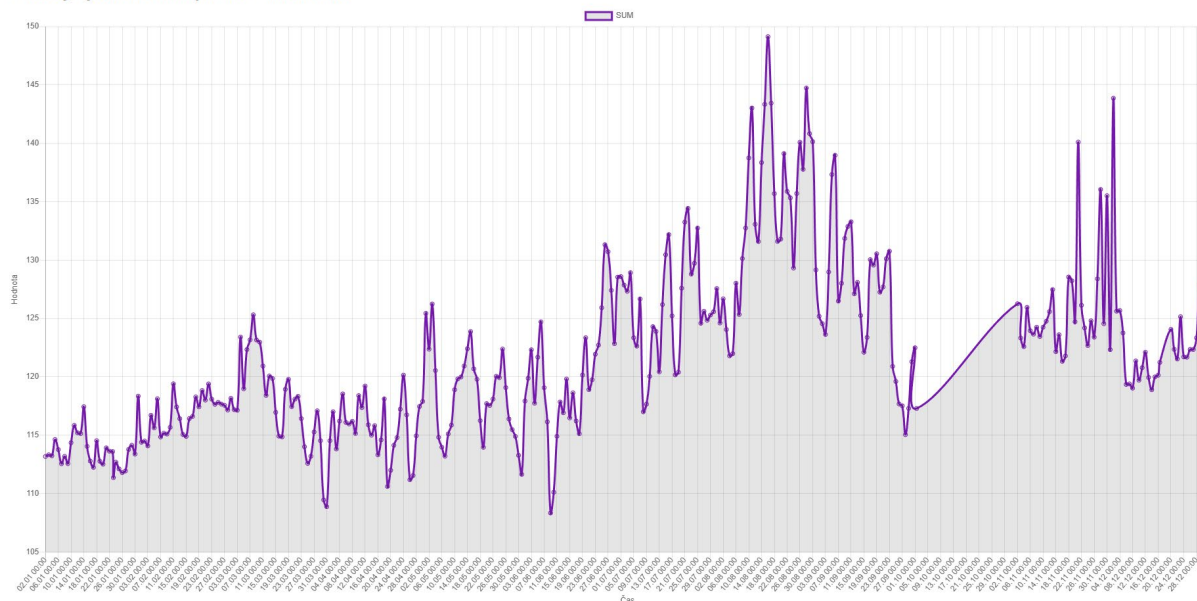
#### Celkový výkon IT pre DC Cintorinska



Obrázok 5 - Celkový výkon IT v roku 2025

Spotreba informačných technológií má priamy vplyv na spotrebu Non-IT zariadení, teda podpornej infraštruktúry dátového centra, ako uvádzame na obrázku číslo 6 a v ročnom priemere ide o hodnotu približne 130 kW.

Celkový výkon NONIT pre DC Cintorinska



Obrázok 6 - Celkový výkon NON-IT v roku 2025

Úlohy pridelené oddeleniu CMPDC sú plnené priebežne.

### Dátové centrum Kopčianska (DC-K)

DataCentrum ako rozpočtová organizácia MF SR nadobudla dátové centrum, ktoré bolo financované z prostriedkov Operačného programu Informatizácie spoločnosti (OPIS), v roku 2014. DataCentrum na Kopčianskej ulici (ďalej len „DC-K“) má k dispozícii dve IKT sály.

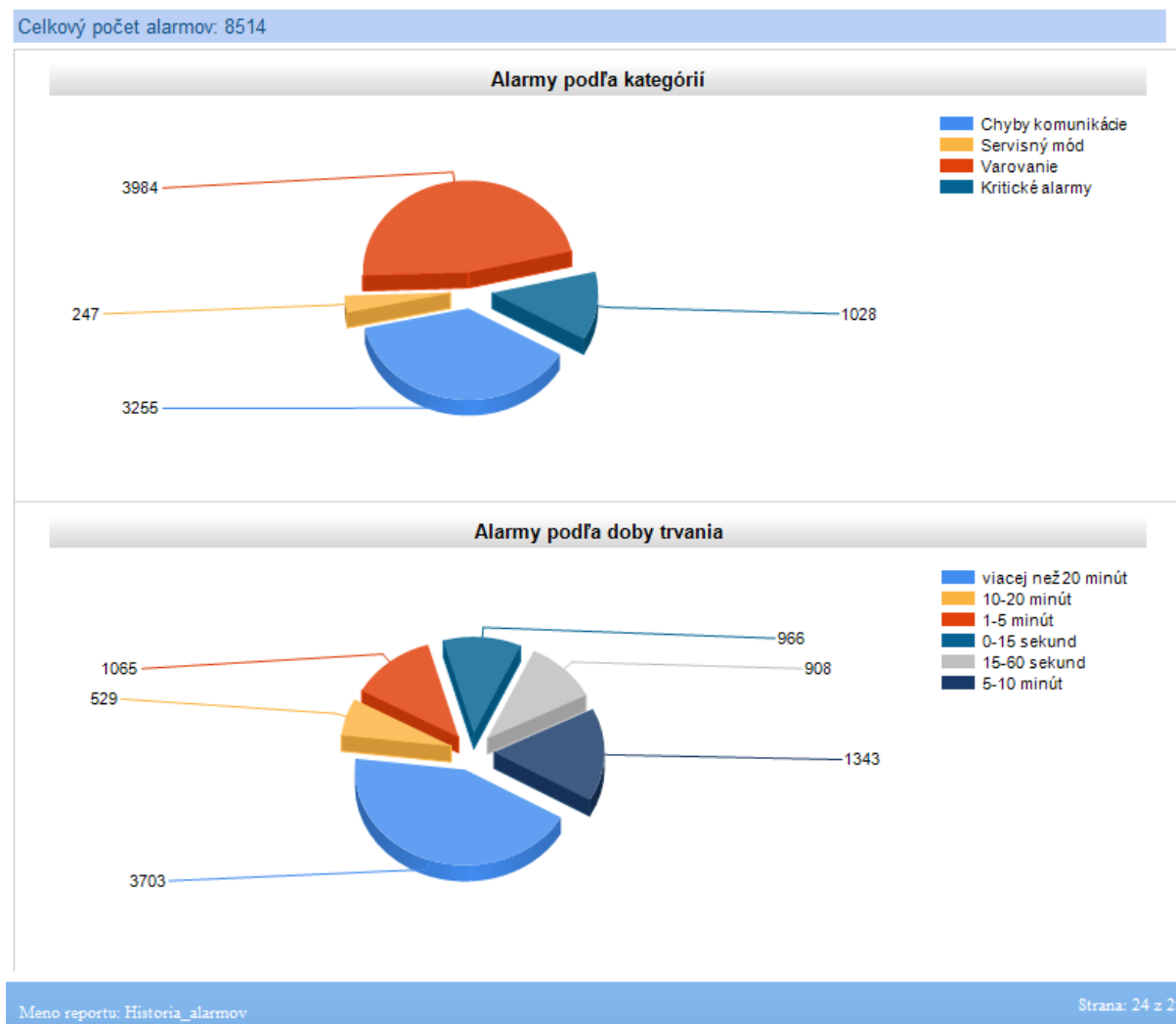
Cieľom projektu bolo zriadenie budovy dátového centra so základnou infraštruktúrou pre sieťovú konektivitu, napájanie, chladenie a bezpečnosť v zmysle definovaných požiadaviek a špecifikácií. Výsledkom je poskytovanie technologických služieb zabezpečenia a poskytovania infraštruktúry iným subjektom verejnej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

V priestoroch DC-K je inštalovaný poplachový systém na hlásenie narušenia doplnený aj kamerovým systémom a prístup do celého areálu a jednotlivých priestorov je riadený systémom kontroly vstupu. Bezpečnostné systémy sú integrované do jedného monitorovacieho nástroja, ktorý umožňuje jednoduchšie riešenie incidentov a aj spätné vyhľadávanie informácií z minulosti. Všetky priestory DC-K sú vybavené elektronickou požiarou 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.

Dohľad nad podpornou infraštruktúrou DC-K (klimatizácie, UPS, zdroje el. energie, atď.) prevádzkovaných informačných systémov, zabezpečuje oddelenie CMPDC a zjednodušený sumár alarmov z dohľadu nad podpornou infraštruktúrou uvádzame na obrázku číslo 7.

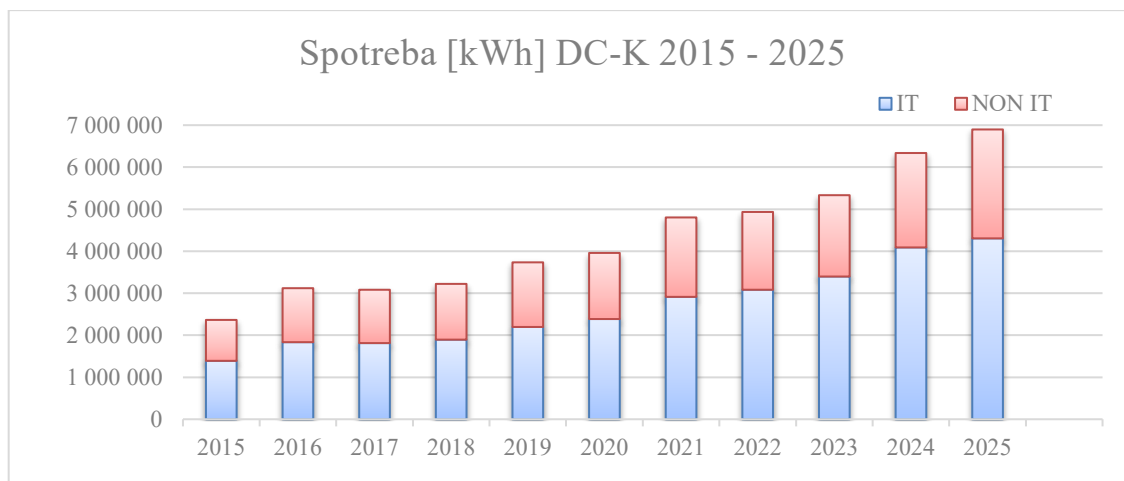


Obrázok 7- Počet alarmov podpornej infraštruktúry DC-K za rok 2025.

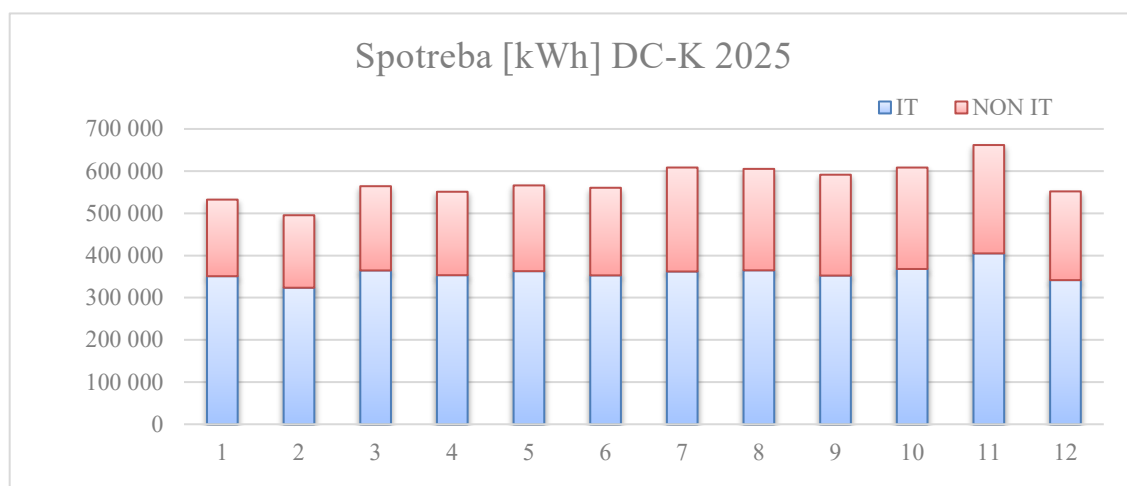
Najpočetnejšie sú alarmy typu „varovania“ v počte 3 984 ks, ktoré informujú napríklad o zmene stavu monitorovaných zariadení a môžeme ich zaradiť k bežným prevádzkovým stavom dátového centra. Nasledujú „poruchy komunikácie“ jednotlivých zariadení v počte 3 225 ks, ktoré vznikajú prevažne pri výkone profylaktických kontrol, a to pri odpojení a kontrole zariadenia, nasledujú bežné poruchy, ktoré vytvárajú „kritické alarmy“ v počte 1 028 ks.

V roku 2025 sa naďalej zvyšovali energetické nároky na dátové centrum v rámci rozvoja a modernizácie, ako vlastnej, tak aj prevádzkovanej infraštruktúry. Počet prevádzkovaných štátnych inštitúcií je 24. Alokácia plochy na oboch IT sálach sa blíži k 100 % obsadenosti.

Rozvoju zodpovedá aj nárast ročnej spotreby elektrickej energie, ktorá vzrástla oproti roku 2024 o 8,85 % na 6 897 830 kWh, ako môžeme vidieť na obrázku číslo 8.



Obrázok 8 - Celková spotreba DC-K v roku 2025



Obrázok 9 - Celková spotreba DC-K v roku 2025 po mesiacoch.

Na objekte sú vykonávané pravidelné kontroly celej podpornej infraštruktúry a monitoringu, na ktorých prebieha pravidelný servis, údržba a výmena opotrebovaných súčastí. Počas roka 2025 bola dostupnosť dátového centra 100 % - okrem plánovaných výpadkov počas ročnej profylaktiky.

Vyhodnocovanie dostupnosti infraštruktúrnych systémov dátovej sály bolo v hodnotenom období realizované na základe stavového princípu, t. j. posúdením výskytu poruchových (červených) alarmov v centrálnom monitorovacom a dohľadovom systéme. Tento prístup vychádza z predpokladu, že infraštruktúrny systém je považovaný za dostupný, pokiaľ počas prevádzky nedôjde k vzniku poruchového stavu, ktorý by ohrozoval stabilitu alebo bezpečnosť prevádzky dátovej sály.

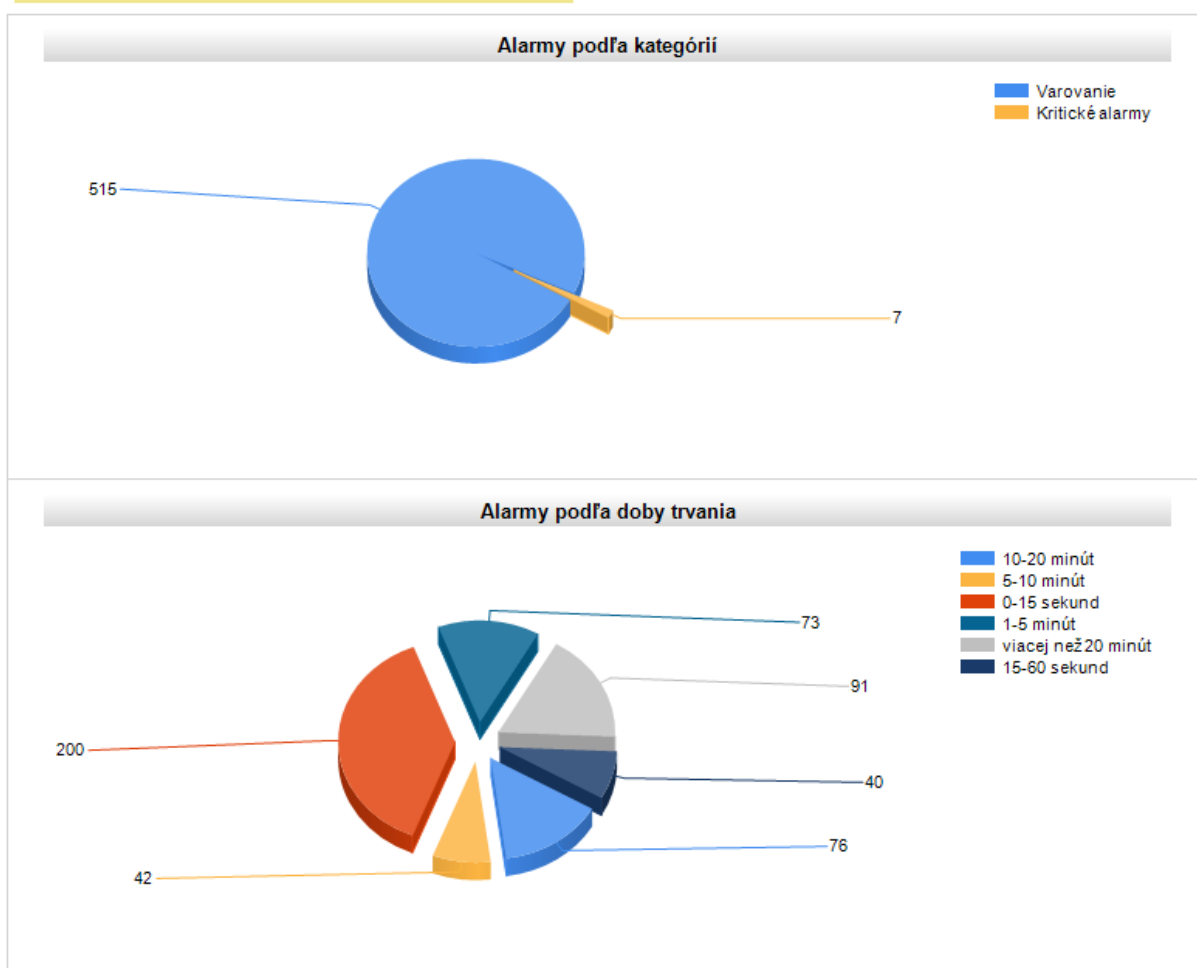
Do hodnotenia boli zahrnuté kľúčové infraštruktúrne systémy, najmä systémy napájania elektrickou energiou, chladenia a klimatizácie, monitoringu a dohľadu, ako aj systémy fyzickej bezpečnosti a riadenia prístupu. Červený alarm bol definovaný ako kritická udalosť signalizujúca nefunkčnosť systému, prekročenie hraničných prevádzkových parametrov alebo zlyhanie všetkých dostupných redundantných prvkov, pričom jeho výskyt predstavuje stav nedostupnosti z pohľadu SLA. Výskyt varovných alebo informačných hlásení nižšej úrovne nebol považovaný za porušenie dostupnosti.

Vyhodnotenie dostupnosti bolo vykonané analýzou záznamov monitorovacieho systému. V prípade, že počas hodnoteného obdobia nebol zaznamenaný žiadny červený alarm vzťahujúci sa na posudzovaný infraštruktúrny systém, považovala sa jeho dostupnosť za splnenú. Výsledky tohto vyhodnotenia boli zapracované do záverečnej správy o prevádzke ako podklad pre konštatovanie plnenia SLA parametrov v oblasti dostupnosti infraštruktúrnych systémov.

Práce CMPDC boli vykonávané v zmysle záväzkov definovaných v platných SLA a report dodržania SLA pre jednotlivé dátové sály, uvádzame na nasledujúcich dvoch obrázkoch.

<b>Popis:</b>	Report zobrazuje SLA parametre pre sálu 1.
<b>Parametre reportu</b>	
<b>Časový rozsah:</b>	1. 1. 2025 0:00:00 - 1. 1. 2026 0:00:00

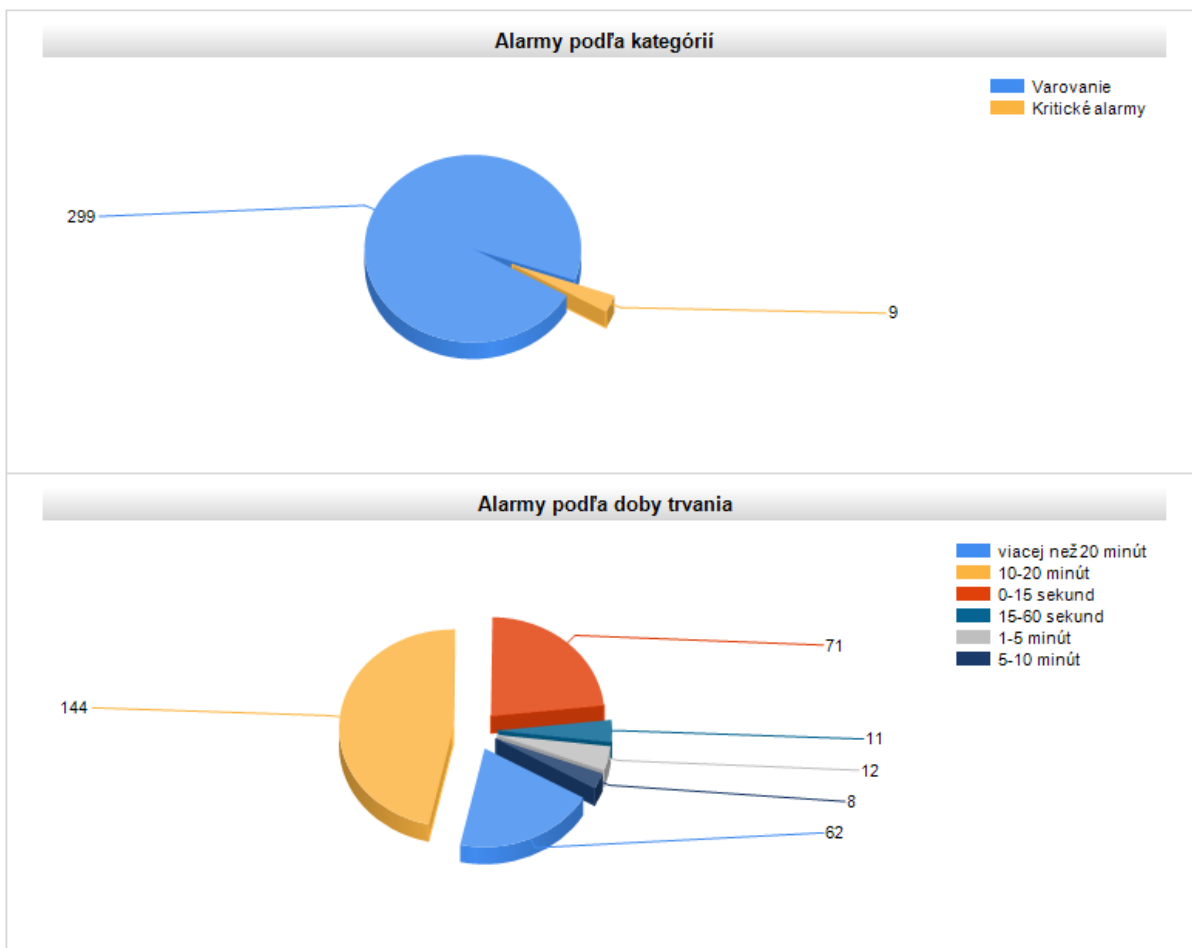
<b>Dodržanie SLA</b>	<b>Nedodržanie SLA</b>
100,000%	0.0s
Celkový počet alarmov: 522	



Obrázok 10 - SLA/Sála 1

<b>Popis:</b>	Report zobrazuje SLA parametre pre sálu 2.
<b>Parametre reportu</b>	
<b>Časový rozsah:</b>	1. 1. 2025 0:00:00 - 1. 1. 2026 0:00:00

<b>Dodržanie SLA</b>	<b>Nedodržanie SLA</b>
100,000%	0.0s
Celkový počet alarmov: 308	



Obrázok 11- SLA/Sála 2

Oddelenie CMPDC plnilo v roku 2025 úlohy priebežne v nepretržitej prevádzke 24/7/365 s využitím interných zamestnancov a zmluvných dodávateľov služieb. V roku 2025 postúpilo na riešenie všetky kritické incidenty, ktoré sa vyskytli na monitorovaných systémoch.

Riešenia neštandardných situácií sú podnetom na úpravy pracovných postupov s cieľom zlepšenia poskytovania komplexných informácií o monitorovaných systémoch, čo je súčasne aj predpokladom skvalitňovania činností a upevňovania váhy prevádzkového a monitorovacieho centra CMPDC.

DataCentrum aj v roku 2025 ako prevádzkovateľ RÚZ v zmysle § 23c zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov, v súlade so zákonom č. 71/1967 Zb. o správnom konaní a zákonom č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov, vydávalo na základe doručenej žiadosti overené kópie dokumentov alebo časti dokumentov, ktoré sú uložené v RÚZ.

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

Všetky požiadavky klientov hlásené cez CPU boli zaznamenané v Service Manager-i a boli vyriešené v stanovenom termíne a v súlade s požiadavkami SLA, t. j. bolo poskytnuté poradenstvo na telefonickú alebo e-mailovú úroveň, prípadne bola zabezpečená druhá úroveň podpory.

Celkovo bolo k 31. 12. 2025 prostredníctvom CPU evidovaných 880 používateľov na základe žiadosti o vstup do verejnej časti.

V roku 2025 bolo podaných a doručených celkovo 148 žiadostí o poskytnutie údajov z RÚZ, pričom všetkých 148 žiadostí bolo vybavených, čo predstavuje 100 % úspešnosť vybavenia.

Z uvedeného počtu bolo 53 žiadostí podaných a vybavených osobne a 93 žiadostí bolo doručených a vybavených poštou. Jedna žiadosť bola vybavená prostredníctvom e-mailu a jedna žiadosť bola zrušená. Z celkového počtu riešených žiadostí bolo 94 žiadostí vybavených bezplatne, 53 za úhradu v hotovosti v súlade so zákonom č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov. V prípade osobného podania žiadosti a úhrady správneho poplatku v hotovosti alebo na základe potvrdenia pre evidenciu poplatku, bol výstup vydávaný na počkanie. V prípadoch, kedy nebolo možné žiadosť vybaviť hneď, keďže sa požadovaný dokument v registri nenachádzal, bolo potrebné zabezpečiť nápravu v spolupráci s Finančným riaditeľstvom SR, ktoré na základe nášho upozornenia zabezpečilo následné doplnenie a zverejnenie chýbajúcich dokumentov. V takýchto prípadoch je poverený zamestnanec podateľne RÚZ 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 roku 2025 bolo prostredníctvom CPU zaevidovaných a uzatvorených 561 hlásení používateľov RÚZ.

Služby zákazníkom boli aj naďalej poskytované ústretovým prístupom aj podľa ich potrieb a požiadaviek, pričom bol často využívaný telefonický kontakt, konzultácia a v prípade potreby dohovor konkrétneho termínu vystavenia výstupu a overovacej doložky v tlačenej podobe.

V hodnotenom období neboli zaznamenané žiadne problémy s dostupnosťou a funkčnosťou RÚZ ani nespokojnosť klienta a všetky hodnotiace kritériá boli splnené.

<b>202</b>	<b>Konzultačné služby pre sekciu informačných technológií MF SR</b>
------------	---

V roku 2025 boli pre MF SR zo strany DataCentra a v spolupráci so sekciou informačných technológií MF SR riešené a zabezpečované priebežne viaceré činnosti súvisiace so zabezpečovaním aktuálnych a aj priebežne vznikajúcich dielčích úloh súvisiacich s plánovanými, ako aj novými pripravovanými projektami.

V tejto súvislosti to boli predovšetkým:

- uskutočnilo sa viacero pracovných rokovaní v súvislosti s projektom CES,
- uskutočnilo sa viacero pracovných stretnutí k príprave a nasadeniu IS CIS k jeho funkcionalite a nasadeniu do prevádzky,
- uskutočnili sa pracovné stretnutia k príprave migrácie IS do RPC,
- uskutočnili sa pracovné stretnutia k príprave migrácie IS ŠP do RPC,
- uskutočnili sa pracovné stretnutia k nasadeniu modulu eÚhrady pre ŠP,
- uskutočnili sa pracovné stretnutia k obnove komunikačnej infraštruktúry pre MF SR,
- uskutočnili sa pracovné stretnutia k zväženiu nasadenia SAP RISE,
- uskutočnili sa pracovné stretnutia k zabezpečeniu komunikačnej infraštruktúry pre ARDAL,
- DataCentrum poskytovalo konzultácie pre plánovanie nasadzovania a migrácií IS VS do RPC,
- DataCentrum poskytovalo konzultácie spoločnosti Slovenská elektrizačná prenosová sústava, a.s., v oblasti návrhu a prevádzky informačno-komunikačných technológií.

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

IT monitorovací systém pre štrukturálne fondy a Kohézny fond pre programové obdobie 2004 - 2006 a 2007 - 2013 (ITMS II) je tvorený neverejnou časťou (ITMS Core) a verejnou časťou (ITMS Portál).

**Prevádzka verejnej časti ITMS Portál bola k 31. 01. 2021 ukončená.**

O uvedenej skutočnosti boli používatelia informovaní na hlavnej stránke ITMS Portál ([www.itms.sk](http://www.itms.sk)), ako aj zo strany príslušného riadiaceho, resp. sprostredkovateľského orgánu (RO/SORO).

Dňa 17. 10. 2022 bola uzavretá zmluva o spoločnom postupe v súvislosti s používaním IT monitorovacieho systému pre štrukturálne fondy a Kohézny fond pre programové obdobie 2007 - 2013 a IT monitorovacieho systému pre štrukturálne a investičné fondy pre programové obdobie 2014 - 2020 (číslo MIRRI SR: 670/2021, číslo MF SR: 2022/128, číslo DataCentrum: DC/17/2022), ktorej predmetom je zabezpečenie správy a prevádzky informačného systému ITMS na spracovanie dát za programové obdobie 2004 - 2006 a 2007 - 2013 a zabezpečenie správy a prevádzky informačného systému ITMS2014+ na spracovanie dát za programové obdobie 2014 - 2020.

V decembri 2023 bol uzatvorený „Dodatok č. 1 k zmluve o spoločnom postupe v súvislosti s používaním IT monitorovacieho systému pre štrukturálne fondy a Kohézny fond pre programové obdobie 2007 - 2013 a IT monitorovacieho systému pre štrukturálne a investičné

fondy pre programové obdobie 2014 - 2020“ s účinnosťou od 15. 12. 2023, ktorým sa predlžuje platnosť predmetnej zmluvy do 31. 12. 2028.

Počas roku 2025 DataCentrum realizovalo činnosti vedúce ku skvalitneniu poskytovaných služieb pre všetky prevádzkované informačné systémy vrátane systému ITMS II, ako aj na odstránenie nedostatkov zistených vládnymi auditmi systému ITMS II:

- realizácia nákupu podpory licencií mailového systému,
- realizácia nákupu podpory CITRIX licencie,
- realizácia nákupu podpory na Symantec licencie,
- realizácia nákupu podpory pre bezpečnostné prvky,
- realizácia nákupu Microsoft licencií,
- príprava migrácie na záložný hardvéroch.

### 1. Správa a prevádzka systému

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

Aplikácia ITMS Core 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 DataCentra (KTI). K 31. 12. 2025 bola v produkčnej prevádzke ITMS Core verzia 2.17.1.

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

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

Pomocou nástroja CyberArk boli monitorované aktivity/logy pracovníkov s pridelenými administrátorskými oprávneniami pre ITMS II.

Zamestnanci DataCentra vykonávali v hodnotenom období administráciu časti produkčného a cvičného systému ITMS Core - modulu Administrátorské nástroje - Správa orgánov a užívateľov, Správa priradenia používateľských rolí, Správa rolí orgánu, Správa používateľských 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 systému ITMS II boli dodržiavané všetky bezpečnostné opatrenia vyplývajúce z požiadaviek na bezpečnosť systému.

Systém ITMS Core je začlenený do centrálného monitoringu prevádzky v DataCentre, v rámci ktorého je nad ním uskutočňovaný základný monitoring, ktorý sa zrealizuje pomocou nástroja BAC, a to prihlásením sa do aplikácie pre ITMS Core. V roku 2025 neboli centrálnym monitoringom prevádzky zaznamenané nedostupnosti systému ITMS II, okrem nedostupnosti

počas pravidelnej údržby systému ITMS II. Dostupnosť produkčného systému ITMS II bola v hodnotenom období 100 %.

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

Cieľom úlohy je zabezpečiť pomoc užívateľom pri práci s aplikáciou ITMS Core. DataCentrum počas roku 2025 poskytovalo 1. úroveň podpory a 2. úroveň podpory (aplikačná, technická a technologická) bola poskytovaná v spolupráci s prevádzkovým tímom ITMS.

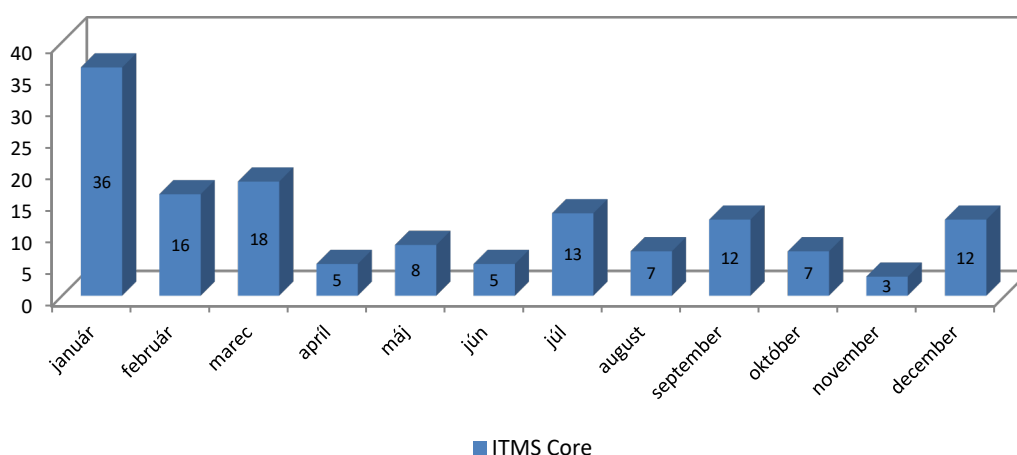
Všetky problémy užívateľov pri práci so systémom ITMS Core, hlásené prostredníctvom telefónu, e-mailu alebo web rozhraním boli zaznamenané v aplikácii Service Manager a riešené pracovníkmi 2. úrovne podpory, prípadne garantmi zo strany vlastníka systému.

Hlásenia zaznamenané v aplikácii Service Manager pre ITMS Core boli kvalifikované ako nekritický problém a boli vyriešené v stanovenom termíne podľa SLA, do 8 pracovných dní - v sledovanom období bolo vyriešených 142 hlásení používateľov pre ITMS Core. Prevažná časť hlásení sa týkala problémov s prihlásením sa do systému ITMS Core (odblokovanie používateľov) a modulu Nezrovnalosti a vrátenia.

### **Doba na vyriešenie incidentu podľa SLA**

Klasifikácia	Reakcia
Kategória A (Kritický problém)	1 pracovný deň
Kategória B (Závažný problém)	3 pracovné dni
Kategória C (Nekritický problém)	8 pracovných dní

Aplikačná podpora pre ITMS II bola poskytovaná permanentne počas pracovných dní v čase od 8.00 hod. do 17.00 hod. a v prípade mimoriadnych situácií aj mimo uvedených hodín.



Graf 1: Počet zaznamenaných a vyriešených hlásení používateľov systému ITMS Core počas roku 2025

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

V priebehu roku 2025 nebolo potrebné túto úlohu realizovať, pre ITMS II neprišla požiadavka na zabezpečenie pripojenia nových koncových bodov do KTI.

### 4. Zabezpečovanie prístupov pre užívateľov systému

Úlohou DataCentra bol zber, registrácia, kontrola písomnej formy žiadosti o prístup (ďalej len „ŽoPR“) pre užívateľov ITMS Core s elektronickou formou a archivácia ŽoPR. 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 **814** aktívnych užívateľov, z toho za sledované obdobie bolo spracovaných **10** nových ŽoPR do ITMS Core, **4** užívateľské prístupy boli aktualizované a **456** užívateľských účtov bolo zrušených/zablokovaných.

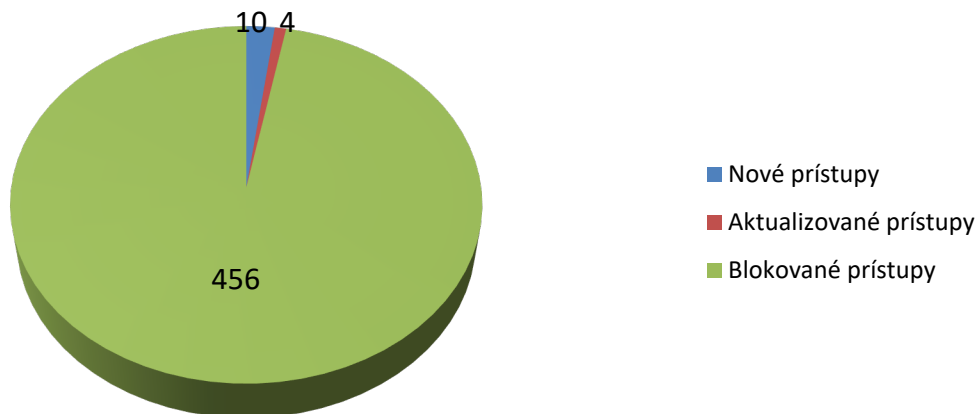
Zároveň boli vytvárané potrebné prístupy na základe poverenia pre administrátora na rezorte a ich zástupcov.

DataCentrum v rámci vytvárania prístupov pre užívateľov systému zabezpečovalo:

- centralizáciu ŽoPR do ITMS Core,
- kontrolu písomnej formy ŽoPR s elektronickou formou,
- vytvorenie, aktualizáciu alebo zrušenie prístupov pre používateľov systému,
- zakladanie a archiváciu ŽoPR do ITMS Core,
- zabezpečenie distribúcie prístupov používateľom 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 je podľa Manuálu pre prístupové práva do ITMS Core a interného Pracovného postupu č. 07 päť pracovných dní.

Proces spracovania všetkých doručených žiadostí do ITMS Core za rok 2025 (od doručenia ŽoPR do ITMS Core do DataCentra po vytvorenie prístupového mena a hesla do ITMS Core a informovanie ŽoPR do ITMS Core/aktualizáciu/zrušenie prístupu) bol realizovaný v lehote kratšej ako päť pracovných dní.



Graf 3: Počet spracovaných ŽoPR do ITMS Core v roku 2025

V mesiacoch máj 2025 a december 2025 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.

#### 5. Zabezpečenie bezpečnosti systému ITMS II

Implementácia navrhovaných riešení z bezpečnostného projektu pre bezpečnosť ITMS II bola zrealizovaná. Všetky bezpečnostné opatrenia boli dodržiavané v spolupráci s odborom prevádzky IS a útvaram bezpečnosti DataCentra a za účasti garantov projektu ITMS II počas celej doby prevádzky systému ITMS II.

#### 6. Udržiavanie havarijných plánov a plánov obnovy činnosti ITMS II v aktuálnom stave

Počas roku 2025 bol aktualizovaný plán zálohovania pre systém ITMS II.

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

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.

Dňa 17. 10. 2022 bola uzavretá zmluva o spoločnom postupe v súvislosti s používaním IT monitorovacieho systému pre štrukturálne fondy a Kohézny fond pre programové obdobie 2007 - 2013 a IT monitorovacieho systému pre štrukturálne a investičné fondy pre programové obdobie 2014 - 2020 (číslo MIRRI SR: 670/2021, číslo MF SR: 2022/128, číslo DataCentrum: DC/17/2022), ktorej predmetom je zabezpečenie správy a prevádzky informačného systému ITMS na spracovanie dát za programové obdobie 2004 - 2006 a 2007 - 2013 a zabezpečenie správy a prevádzky informačného systému ITMS2014+ na spracovanie dát za programové obdobie 2014 - 2020.

V decembri 2023 bol uzatvorený „Dodatok č. 1 k zmluve o spoločnom postupe v súvislosti s používaním IT monitorovacieho systému pre štrukturálne fondy a Kohézny fond pre programové obdobie 2007 - 2013 a IT monitorovacieho systému pre štrukturálne a investičné fondy pre programové obdobie 2014 - 2020“ s účinnosťou od 15. 12. 2023, ktorým sa predlžuje platnosť predmetnej zmluvy do 31. 12. 2028.

Prostredníctvom informačného systému ITMS2014+ bola do 12. 06. 2024 technicky zabezpečovaná, aj úvodná fáza implementácie programového obdobia 2021 - 2027. ITMS2014+ (pôvodne využívaný iba pre implementáciu programového obdobia 2014 - 2020) bol v nevyhnutnej miere upravený a doplnený tak, aby zabezpečil potreby implementácie programového obdobia 2021 - 2027 dočasne, do nasadenia ITMS21+ do prevádzky.

Migrácia údajov z ITMS2014+ bola úspešne ukončená dňa 12. 06. 2024 a od tohto dátumu bola v systéme ITMS2014+ ukončená editácia a práca v evidenciách programového obdobia 2021 - 2027, okrem používateľov s pracovnou pozíciou Kontrolór, ktorí v systéme ITMS2014+, pod orgánmi 21\_RO\_PSK\_MIRRI SR a 21\_SO\_PSK\_ÚV SR, zabezpečovali kontrolu vykonávania úloh zo strany sprostredkovateľského orgánu podľa zmluvy o vykonávaní časti úloh riadiaceho orgánu sprostredkovateľským orgánom.

Funkcionalita výkonu kontroly sprostredkovateľského orgánu podľa zmluvy o vykonávaní časti úloh riadiaceho orgánu sprostredkovateľským orgánom v systéme ITMS21+ zatiaľ nebola implementovaná, preto bolo potrebné počas roku 2025 vytvoriť prístupy pre vybraných používateľov v systéme ITMS2014+, pod orgánmi 21\_RO\_PSK\_MIRRI SR a 21\_SO\_PSK\_ÚV SR.

V roku 2025 DataCentrum realizovalo činnosti súvisiace so zabezpečením produkčnej prevádzky ITMS2014+ a súčasne vedúce ku skvalitneniu poskytovaných služieb pre ITMS2014+, ako aj činnosti na odstránenie nedostatkov zistených vládny auditom ITMS2014+:

- nákup podpory licencií mailového systému,
- nákup podpory CITRIX licencie,
- nákup podpory na Symantec licencie,
- nákup licencií ESET,
- nákup podpory pre bezpečnostné prvky,
- nákup Microsoft licencií,
- realizácia rozšírenia riešenia pre antivírusovú kontrolu príloh,
- integrácia ITMS2014+ na ISLH a ISP.

V priebehu hodnoteného obdobia boli v prevádzke integrácie ITMS2014+ s nasledovnými informačnými systémami:

- ISUF (MF SR),
- Register fyzických osôb (RFO - MV SR),
- Register adries fyzických osôb (RA - MV SR),
- IS CSRÚ - Register právnických osôb (RPO),
- Elektronický kontrakčný systém (EKS - MV SR),
- Vestník ÚVO (ÚVO),
- IS CSRÚ - daňové nedoplatky (MF SR; finančná správa),
- Register úpadcov (MS SR),
- Obchodný register SR (MS SR),
- RÚZ (MF SR; finančná správa),
- 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,
- IS CSRÚ - Sociálna poisťovňa (MPSVR SR) – 4 rôzne integrácie,
- IS CSRÚ - všetky tri zdravotné poisťovne (MF SR),
- Register trestov (GP SR),
- Ústredný portál verejnej správy (ÚPVS),
- IS CSRÚ - kataster nehnuteľností (ESKN),
- IS JRŽ - Jednotný register žiadateľov (PPA),
- IS AGIS - Agrárny informačný systém, PPA (PPA),
- RPVS – register partnerov verejného sektora,
- API (na účely nahrávania účastníkov projektov),
- IS DKS - integrácia s registratúrными systémami subjektov (ako prvý subjekt MIRRI SR),
- Evidencia personálnych výdavkov,
- Register trestov právnických osôb (PPA),
- Centrálny manažment dát ISLH a ISP (PPA).

## 1. Správa a prevádzka systému

DataCentrum, v spolupráci s dodávateľom ITMS2014+, zabezpečovalo prevádzkovanie a spravovanie produkčného, predprodukčného, školiaceho, testovacieho a záložného systému ITMS2014+ neverejná časť a ITMS2014+ verejná časť (inštalácia servisných buildov, administrácia, manažment, zálohovanie...), zabezpečovalo technickú podporu pre systém a bežnú údržbu aplikačných systémov. V priebehu roku 2025 bolo, so súhlasom vlastníka systému, školiace prostredie zrušené.

Serverové komponenty architektúry aplikácie ITMS2014+ neverejná časť a ITMS2014+ verejná časť 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 DataCentra (KTI).

V rámci prevádzky ITMS2014+ sa spravuje produkčné, predprodukčné, testovacie a záložné prostredie, čo predstavuje ku koncu sledovaného obdobia celkom 125 serverov (v priebehu roku 2025 bolo so súhlasom vlastníka systému školiace prostredie zrušené). Záložné prostredie sa vytvára obnovou z Virtuálnej páskovej knižnice na servery v ZVS, ktoré sú prevádzkované DataCentrom. Zoznam serverov, potrebných k testovaniu obnovy ITMS2014+ zo zálohy, dodáva vlastník systému MIRRI SR.

V rámci sledovaného obdobia bolo zrealizovaných **154** požiadaviek vlastníka systému (požiadavky na nasadenie nových verzií aplikácie ITMS2014+ a EPV, požiadavky na spustenie skriptov na modifikáciu dát, generovanie exportov pre MIRRI SR, MF SR a PPA a úlohy na upload excel exportov).

K 31. 12. 2025 bol v prevádzke produkčný systém ITMS2014+ neverejná časť a ITMS2014+ verejná časť verzie 17.3.36.

V priebehu roku 2025 boli pravidelne dopĺňané údaje týkajúce sa ITMS2014+ do konfiguračnej databázy a pravidelne sa vykonávala aj aktualizácia (patchovanie) operačného systému pre ITMS2014+.

Zamestnanci DataCentra vykonávali administráciu časti produkčného, testovacieho a cvičného systému ITMS2014+ neverejná časť a ITMS2014+ verejná časť pre PO 2014 - 2020 a pre PO 2021 - 2027 (používatelia s pracovnou pozíciou Kontrolór) - modulu Orgány a používatelia - Orgány, Pracovné pozície, Používatelia, ŽoAK konta, ŽoPR 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 súlade s Bezpečnostným projektom pre ITMS2014+, Bezpečnostným manuálom pre koncových používateľov a manažérov ITMS2014+ a Katalógom rizík pre systém ITMS2014+.

V priebehu roku 2025 sa pravidelne realizovalo zálohovanie celého VMware vybavenia (virtuálnych serverov) produkčného prostredia VTL (Virtual Tape Library). Zálohovanie ITMS2014+ je systémovou podporou vykonávané formou replikácie z produkčného systému na záložný systém. Inkrementálna záloha je vykonávaná denne, plná záloha sa vykonáva 2x do týždňa.

ITMS2014+ neverejná časť a ITMS2014+ verejná časť sú začlenené do centrálného 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 (ďalej len „ŽoAK“) 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 ITMS2014+ a počas nasadzovania nových verzií a opravných buildov pre systém ITMS2014+, ktoré boli spravidla vykonávané mimo štandardnej doby pre poskytovanie podpory pre ITMS2014+, to znamená po 17-tej hodine.

Dostupnosť produkčného systému ITMS2014+ neverejná časť a ITMS2014+ verejná časť bola v hodnotenom období 99,90 %.

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

Cieľom úlohy je zabezpečiť pomoc používateľom pri práci s aplikáciou ITMS2014+ neverejná časť a ITMS2014+ verejná časť. DataCentrum počas celého roka 2025 poskytovalo 1. úroveň podpory, 2. úroveň podpory (aplikačná, technická a technologická) bola poskytovaná v spolupráci s dodávateľom na základe zmluvy o zabezpečení prevádzky 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 Service Manager a riešené pracovníkmi 2. úrovne podpory, metodické otázky boli riešené na 3. úrovni podpory (odborní garanti z CKO – MIRRI SR a CO – MF SR).

V priebehu roka 2025 bolo v aplikácii HP Service Manager zaznamenaných a vyriešených **4 999** hlásení, z toho bolo **4 996** hlásení bolo vyriešených v stanovenom termíne podľa SLA, pri **3** hláseniach, riešených odbornými garantmi, bola prekročená doba na vyriešenie. Hlásenia, pri ktorých nebola dodržaná SLA, sa týkali problémov, ktoré si vyžadovali spoluprácu viacerých útvarov DataCentra/MIRRI SR/MF SR, čo predĺžilo čas na vyriešenie hlásenia.

### **Doba na vyriešenie incidentu podľa SLA**

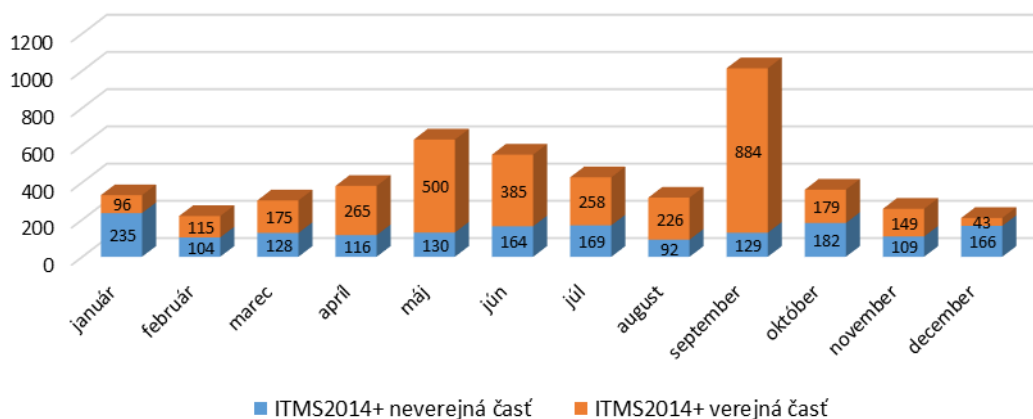
<b>Klasifikácia</b>	<b>Reakcia</b>
Kategória A (Kritický problém)	1 pracovný deň
Kategória B (Závažný problém)	3 pracovné dni
Kategória C (Nekritický problém)	8 pracovných dní

V roku 2025 bolo vyriešených **1 724** hlásení používateľov pre ITMS2014+ neverejná časť a **3 275** hlásení používateľov ITMS2014+ verejná časť. Prevažná časť hlásení sa týkala problémov s prihlásením sa do systému ITMS2014+ verejná časť, problémov používateľov pri vytváraní ŽoPR, problémov pri elektronickom podpisovaní a odosielaní dokumentov, problémov pri práci s užívateľskými účtami, pri vytváraní ŽoP a tiež metodických usmernení používateľov neverejnej časti ITMS2014+.

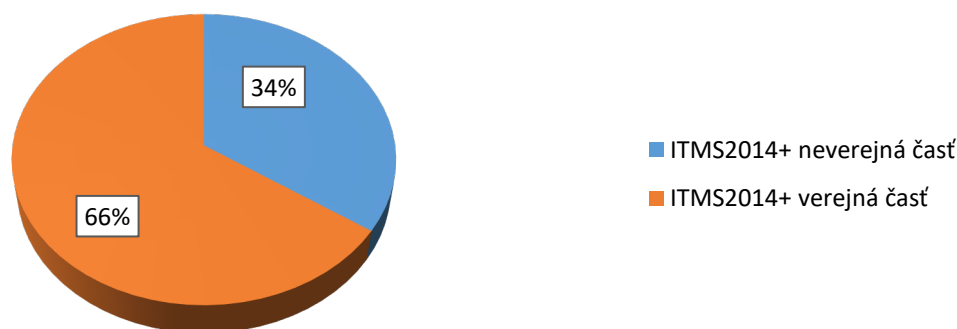
V termíne od 10. 04. 2025 do 09. 05. 2025 bola Pôdohospodárskou platobnou agentúrou vyhlásená „Výzva na predkladanie žiadostí o poskytnutie dotácie na marketingovú podporu

v potravinárstve“, v termíne od 21. 05. 2025 do 21. 07. 2025 bola Pôdohospodárskou platobnou agentúrou vyhlásená „Výzva na predkladanie žiadostí o poskytnutie dotácie na plnenie mimoprodukčných funkcií lesov“ a v termíne od 26. 08. 2025 do 26. 09. 2025 bola Pôdohospodárskou platobnou agentúrou vyhlásená „Výzva na predkladanie žiadostí o poskytnutie štátnej pomoci vo forme úľav na environmentálnych daniach – Zelená nafta 2025“, rámci ktorých DataCentrum zaznamenalo v mesiacoch máj, jún a september 2025 zvýšený počet ŽoPR a hlásení v SM v súvislosti s používaním systému ITMS2014+.

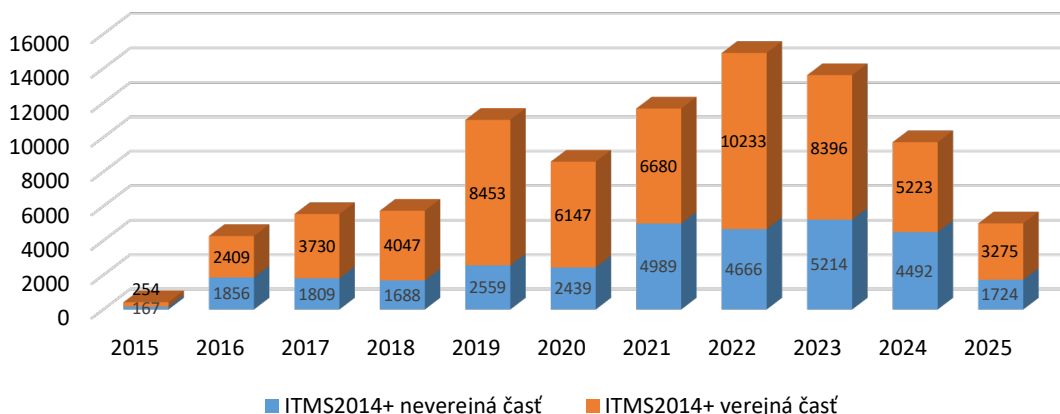
Aplikačná podpora pre ITMS2014+ bola poskytovaná permanentne počas pracovných dní v čase od 8.00 hod do 17.00 hod. a v prípade mimoriadnych situácií aj mimo uvedených hodín.



Graf 1: Počet zaznamenaných a vyriešených hlásení používateľov systému ITMS2014+ v roku 2025



Graf 2: Percentuálne zobrazenie vyriešených hlásení používateľov systému ITMS2014+ v roku 2025



Graf 3: Počty uzatvorených hlásení za ITMS2014+ verejná a neverejná časť v rokoch 2015 - 2025

### 3. Zabezpečovanie prístupov pre používateľov systému

#### **ITMS2014+ neverejná časť:**

V rámci realizácie úlohy procesu spracovania žiadostí pre orgány a ŽoPR do ITMS2014+ neverejná časť sú v systéme ITMS2014+ vytvárané nové orgány a na základe doručených ŽoPR boli vytvárané, aktualizované alebo blokovévané užívateľské kontá.

Úlohou DataCentra bolo zabezpečiť zber, registráciu a kontrolu písomnej formy ŽoPR do ITMS2014+ neverejná časť a po schválení žiadosti v systéme ITMS2014+ archivácia originálu doručenej ŽoPR. DataCentrum na základe schválených ŽoPR zriaďovalo, aktualizovalo alebo blokovalo používateľom prístup do produkčného systému ITMS2014+ neverejná časť a pre manažérov ITMS2014+ aj do testovacieho systému ITMS2014+ neverejná časť. Za sledované obdobie bolo v systéme ITMS2014+ spracovaných 797 ŽoPR pre PO 2014 - 2020 a 10 ŽoPR pre PO 2021 - 2027.

K 31. 12. 2025 bolo v ITMS2014+ 2971 aktívnych používateľov neverejnej časti systému. Zároveň bolo ku koncu sledovaného obdobia aktívnych 755 používateľov s duálnym prístupom. Za sledované obdobie bolo vytvorených 190 nových prístupov do ITMS2014+ neverejná časť, 173 prístupov do ITMS2014+ neverejná časť bolo aktualizovaných a 430 používateľských účtov bolo zablokovaných na základe schválených ŽoPR s predmetom Zneplatnenie prístupu. Štrnásť ŽoPR bolo zamietnutých. Dôvodom zamietnutia ŽoPR do neverejnej časti ITMS2014+ bola nesprávne vyplnená ŽoPR alebo nesplnenie podmienok na schválenie ŽoPR (chýbajúce podpisy). V systéme ITMS2014+ bolo schválených 7 ŽoPR pre používateľov orgánu 21\_RO\_PSK\_MIRRI SR a 3 žiadosti za orgán 21\_SO\_PSK\_UVSR.

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

DataCentrum v rámci vytvárania prístupov pre používateľov systému zabezpečovalo:

- centralizáciu písomnej formy ŽoPR do ITMS2014+ neverejná časť pre PO 2014 - 2020 a PO 2021 - 2027 (vybraní používatelia),

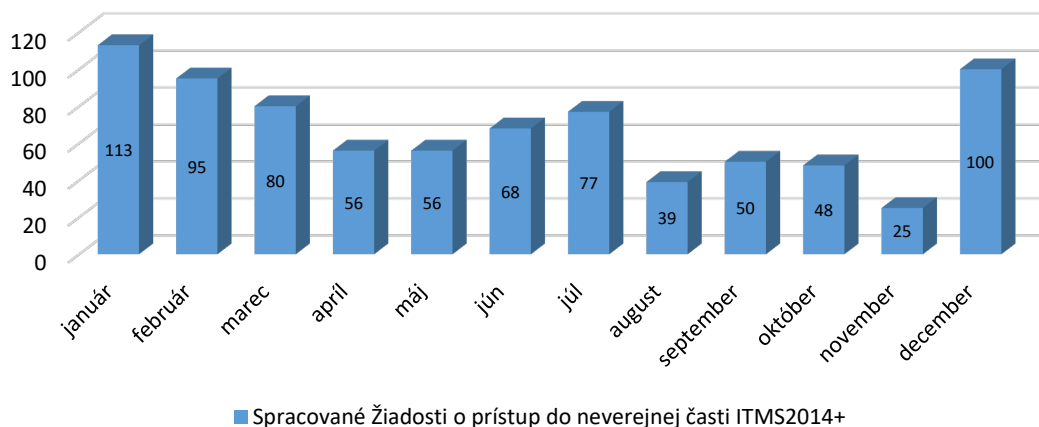
- vytvorenie, aktualizáciu alebo zrušenie prístupov pre používateľov neverejnej časti ITMS2014+, resp. duálnych prístupov schválením ŽoPR pre PO 2014 - 2020 a PO 2021 - 2027 (vybraní používatelia),
- zakladanie a archiváciu ŽoPR do ITMS2014+ neverejná časť pre PO 2014 - 2020 a PO 2021 - 2027 (vybraní používatelia),
- zabezpečenie distribúcie všetkých relevantných dokumentov Manažérom ITMS2014+ na rezortoch,
- vykonávanie pravidelnej previerky prístupov do systému a spracovanie záznamov z previerok prístupov.

Doba na spracovanie žiadostí do neverejnej časti systému ITMS2014+ pre používateľa a doba aktualizácie orgánových a používateľských rolí v systéme ITMS2014+ neverejná časť je podľa Manuálu pre prístupové práva do ITMS2014+ a interného Pracovného postupu č. 62 päť pracovných dní.

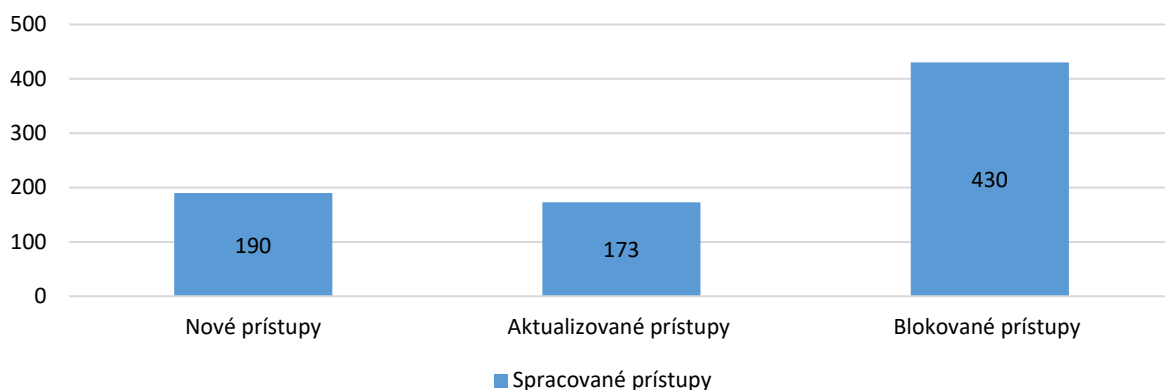
Proces spracovania všetkých doručených žiadostí do neverejnej časti ITMS2014+ za rok 2025 (od doručenia ŽoPR do ITMS2014+ do DataCentra až po schválenie žiadosti a následné vytvorenie, aktualizáciu alebo zrušenie prístupu do ITMS2014+) prebiehal v súlade s Manuálom pre prístupové práva do ITMS2014+ a interným Pracovným postupom č. 62.

Z celkového počtu 807 doručených ŽoPR do ITMS2014+ za rok 2025 bolo 778 žiadostí spracovaných do jedného pracovného dňa; 29 ŽoPR do ITMS2014+ bolo z dôvodu identifikovaných nedostatkov vrátených na doplnenie, čím došlo k predĺženiu lehoty na ich schválenie a vytvorenie prístupu do neverejnej časti ITMS2014+.

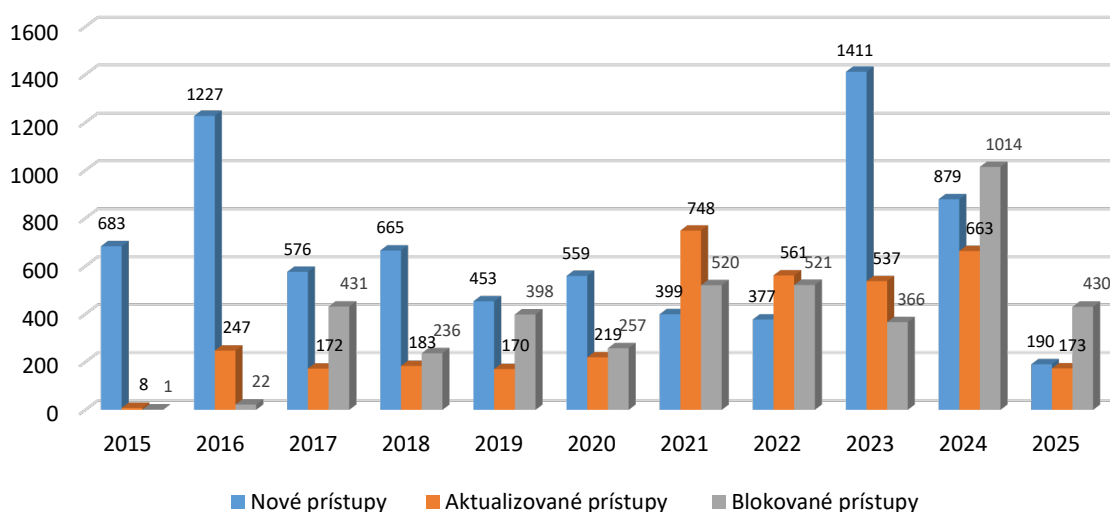
V dňoch 12. 06. 2025 a 06. 11. 2025 boli vykonané previerky prístupov do neverejnej časti systému ITMS2014+. Na kontrolovaných vzorkách prístupov do neverejnej časti systému ITMS2014+ neboli zistené žiadne nedostatky. Z previerok boli vypracované záznamy.



Graf 4: Počet spracovaných ŽoPR do ITMS2014+ neverejná časť počas roku 2025



Graf 5: Počty spracovaných prístupov do ITMS2014+ neverejná časť v roku 2025



Graf 6: Počty spracovaných prístupov do ITMS2014+ neverejná časť v rokoch 2015 - 2025

### ITMS2014+ verejná časť:

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

V ITMS2014+ bolo k 31. 12. 2025 aktívnych 31 526 používateľov verejnej časti, z toho za sledované obdobie bolo schválených 766 ŽoAK a aktivovaných 825 používateľských účtov, 18 ŽoAK konta do ITMS2014+ verejná časť bolo zamietnutých. Najčastejším dôvodom zamietnutia žiadosti bolo doručenie žiadostí s chýbajúcim úradným overením podpisu štatutára, doručenie žiadosti do elektronickej schránky podpísanej s neplatným KEP, prípadne doručenie žiadostí po uplynutí 60 dňovej lehoty od registrácie.

V termíne od 10. 04. 2025 do 09. 05. 2025 bola Pôdohospodárskou platobnou agentúrou vyhlásená „Výzva na predkladanie žiadostí o poskytnutie dotácie na marketingovú podporu v potravinárstve, v termíne od 21. 05. 2025 do 21. 07. 2025 bola Pôdohospodárskou platobnou agentúrou vyhlásená „Výzva na predkladanie žiadostí o poskytnutie dotácie na plnenie mimo produkčných funkcií lesov“ a v termíne od 26. 08. 2025 do 26. 09. 2025 bola Pôdohospodárskou platobnou agentúrou vyhlásená „Výzva na predkladanie žiadostí

o poskytnutie štátnej pomoci vo forme úľav na environmentálnych daniach - Zelená nafta 2025“, v rámci ktorých DataCentrum zaznamenalo v mesiacoch máj, jún a september 2025 zvýšený počet doručených ŽoPR používateľov do verejnej časti ITMS2014+.

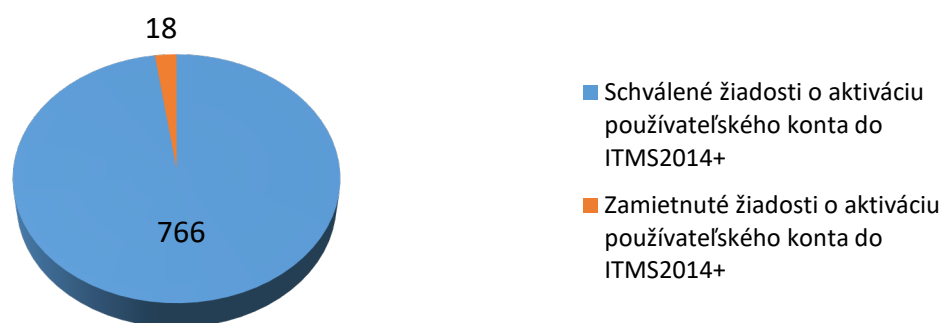
DataCentrum v rámci vytvárania prístupov pre používateľov systému ITMS2014+ verejná časť zabezpečovalo:

- centralizáciu ŽoAK používateľského konta do ITMS2014+ verejná časť,
- kontrolu písomnej formy ŽoAK používateľského konta do ITMS2014+ verejná časť s elektronickou formou,
- schválenie ŽoAK (aktivovanie používateľského konta do ITMS2014+ verejná časť) do 1 pracovného dňa v prípade, že doručená žiadosť bola úplná a spĺňala všetky náležitosti,
- zakladanie a archiváciu ŽoAK používateľského konta do ITMS2014+.

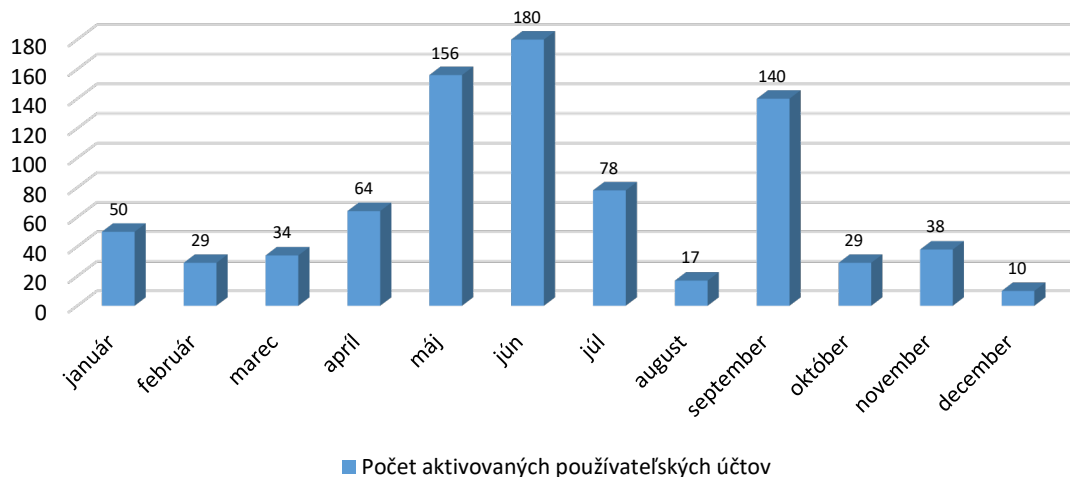
Proces spracovania všetkých doručených žiadostí do verejnej časti ITMS2014+ za rok 2025 (od doručenia ŽoAK používateľského konta do ITMS2014+ do DataCentra až po schválenie žiadosti a následné vytvorenie prístupu do verejnej časti ITMS2014+) prebiehal v súlade s interným Pracovným postupom č. 63.

Z celkového počtu 784 doručených ŽoAK používateľského konta do ITMS2014+ za rok 2025 bolo 689 žiadostí spracovaných do jedného pracovného dňa; 95 ŽoAK používateľského konta do ITMS2014+ bolo z dôvodu identifikovaných nedostatkov vrátených na doplnenie, čím došlo k predĺženiu lehoty na ich schválenie a vytvorenie prístupu do verejnej časti ITMS2014+.

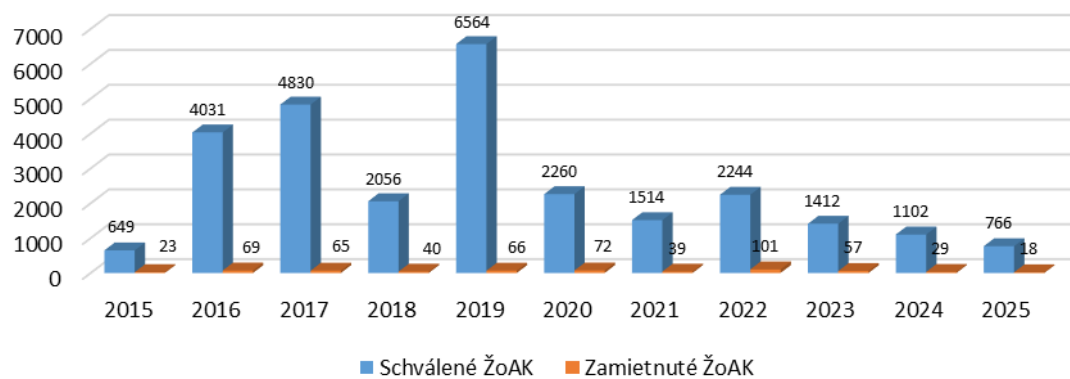
V rámci funkcionality Technický užívateľ (TP) neboli počas roka 2025 vytvorené nové prístupy. V systéme ITMS2014+ k 31. 12. 2025 existuje 13 aktívnych kont Technický užívateľ a 1 konto je zablokované.



Graf 7: Počet ŽoAK používateľského konta do ITMS2014+ verejná časť za rok 2025



Graf 8: Počet aktivovaných používateľských účtov do ITMS2014+ verejná časť počas roku 2025



Graf 9: Celkový počet spracovaných ŽoAK používateľského konta v rokoch 2015 - 2025

#### 4. Zabezpečenie bezpečnosti systému

V roku 2015 bol zo strany vlastníka systému ITMS2014+ vypracovaný a schválený Bezpečnostný projekt pre ITMS2014+, Bezpečnostný manuál pre koncových používateľov a manažerov ITMS2014+ a Katalóg rizík pre systém ITMS2014+.

Všetky bezpečnostné opatrenia sú dodržiavané v spolupráci s útvarom bezpečnosti DataCentra a za účasti garantov projektu ITMS2014+ počas celej doby prevádzky systému ITMS2014+.

#### 5. Realizácia záložného systému ITMS2014+

Záložné prostredie pre ITMS2014+ je vytvorené a v prípade potreby je možná jeho aktivácia podľa platnej SLA. Počas roku 2025 bol aktualizovaný plán zálohovania ITMS2014+ a plán obnovy ITMS2014+, ktorého obsahom je inštaččný postup, popis architektúry aplikácie ITMS2014+ a podrobný zoznam činností potrebných pre úspešnú obnovu ITMS2014+ zo zálohy v ZVS.

Dňa 19. 11. 2025 sa uskutočnilo teoretické testovanie plánov obnovy systému ITMS2014+. Testovania sa zúčastnili zodpovední zamestnanci MIRRI SR, MF SR, DataCentra a dodávateľov zapojených do obnovy systému ITMS2014+. Z testovania bola vypracovaná

zápisnica a aktualizované dokumenty - plán zálohovania ITMS2014+ a plán obnovy ITMS2014+.

<b>213</b>	<b>IT monitorovací systém pre programové obdobie 2021 - 2027 (ITMS21+)</b>
------------	--

**IT monitorovací systém pre programové obdobie 2021 - 2027 (ITMS21+) je v produkčnej prevádzke od 12. 06. 2024.**

V priebehu hodnoteného obdobia DataCentrum vykonávalo činnosti na zabezpečenie prevádzky systému, činnosti potrebné na ďalší rozvoj a zabezpečenie bezpečnosti systému ITMS21+, schvaľovalo prístupy pre používateľov a poskytovalo aplikačnú podporu používateľom systému ITMS21+.

Dňa 22. 09. 2023 bola uzavretá zmluva o spoločnom postupe v súvislosti s používaním informačného monitorovacieho systému pre Fondy EÚ pre programové obdobie 2021 - 2027 (CEZ MIRRI SR: 2334/2023, CEZ MF SR: 2023/285, CEZ DataCentrum: DC/48/2023), ktorej predmetom je zabezpečenie správy a prevádzky informačného systému ITMS21+ na spracovanie dát za programové obdobie 2021 - 2027, stanovenie podmienok spoločného postupu pri zabezpečovaní činností zmluvy a rámcové vymedzenie postupov súvisiacich s dosiahnutím účelu tejto zmluvy.

Počas roku 2025 sa pravidelne uskutočňovali stretnutia pracovnej skupiny pre ITMS21+, na ktorých bol odpočítovaný aktuálny stav úloh a boli zadané úlohy do najbližšieho stretnutia. Pracovná skupina pre ITMS21+ je tvorená zástupcami vlastníka systému MIRRI SR, MF SR, DataCentra a dodávateľov (JumpSoft, HPE, Eviden).

Počas hodnoteného obdobia bolo v prevádzke predprodukčné, produkčné, testovacie, školiace a záložné prostredie ITMS21+.

V sledovanom období naďalej prebiehalo testovanie verejnej aj neverejnej časti ITMS21+, postupné spúšťanie a testovanie integrácií a aplikácií tretích strán.

Aktuálne funkčné integrácie voči ITMS21+ :

- Integrácia na Register fyzických osôb,
- Integrácia na Register adries,
- Integrácia na Register partnerov verejného sektora,
- Integrácia na Národný inšpektorát práce,
- Integrácia na Register predinsolvenčných, likvidačných a insolvenčných konaní,
- Integrácia na IS finančnej správy,
- Integrácia na IS RÚZ,
- Integrácia na Register právnických osôb,
- Integrácia na IS pre evidenciu a monitorovanie pomoci,
- Integrácia na zdravotné poisťovne,
- Integrácia na Sociálnu poisťovňu,
- Integrácia na Informačný systém účtovníctva fondov,
- Integrácia na Ústredný portál verejnej správy,
- Integrácia so systémom IS CSRÚ

- Údaje o daňových nedoplatkoch;
- Údaje o nedoplatkoch na sociálnom poistení;
- Údaje o nedoplatkoch na zdravotnom poistení;
- Údaje o právnickej osobe;
- Údaje o daňových nedoplatkoch;
- Údaje z registra príjemcov štátnej pomoci a minimálnej pomoci;
- Údaje o vedených konkurzných a reštrukturalizačných konaniach;
- Údaje o fyzickej osobe;
- Údaje o adresnom bode fyzickej osoby;
- Overenie existencie zamestnanca;
- Priebeh registrácií fyzickej osoby;
- Počet zamestnancov zamestnávateľa;
- Automatizované získanie schém pomoci a príslušných číselníkov.

V priebehu roku 2025 DataCentrum realizovalo činnosti súvisiace so zabezpečením produkčnej prevádzky a bezpečnosti ITMS21+:

- nákup podpory licencií mailového systému,
- nákup podpory CITRIX licencie,
- nákup podpory na Symantec licencie,
- nákup licencií ESET,
- nákup podpory pre bezpečnostné prvky,
- nákup Microsoft licencií,
- realizácia rozšírenia riešenia na antivírusovú kontrolu príloh,
- práce na vytvorení záložného prostredia ITMS21+,
- migrácia riešenia do samostatného sieťového segmentu,
- participácia na teste bezpečnosti systému ITMS21+,
- úprava prepojenia ITMS21+ na ÚPVS,
- prístup dodávateľa na prostredia ITMS21+,
- príprava replikácie záložného prostredia ITMS21+,
- konfigurácia sieťových povolení,
- riešenie prevádzkových problémov – OpenSearch, Gitlab, Jenkins, integrácia na AntiVirovúGateWay (AVGW),
- realizácia updateov Opensearch, LDAP, Gitlab a Jenkins,
- oprava Kubernetes prod a test clustrov.

## 1. Správa a prevádzka systému

DataCentrum v spolupráci s dodávateľom ITMS21+ a dodávateľom rezortného privátneho cloudu DataCentra (RPC) zabezpečovalo prevádzkovanie a spravovanie predprodukčného (STG), testovacieho (TST), produkčného, školiaceho a záložného systému ITMS21+, jeho neverejnej aj verejnej časti (inštalácia servisných buildov, administrácia, manažment, zálohovanie, monitorovanie...), zabezpečovalo technickú podporu pre systém a pravidelný upgrade všetkých potrebných súčastí platformy.

Aplikácia ITMS21+ pracuje nad zjednotenou databázou pre verejnú aj neverejnú časť ITMS21+, ktorá je umiestnená v rámci rezortného privátneho cloudu DataCentra (RPC). Systém ITMS21+ je prevádzkovaný na virtualizačnej platforme Kubernetes.

K 31. 12. 2025 bol v prevádzke produkčný systém ITMS21+ verzia 3.2.9.

V rámci sledovaného obdobia bolo zrealizovaných 248 požiadaviek vlastníka systému (požiadavky na nasadenie nových verzií aplikácie ITMS21+, požiadavky na spustenie skriptov na modifikáciu dát a úlohy na upload excel exportov).

Zamestnanci DataCentra vykonávali administráciu časti predprodukčného, produkčného a testovacieho systému ITMS21+ neverejná a verejná časť - modulu Orgány a používatelia - Orgány, Pracovné pozície, Používatelia, ŽoAK konta, ŽoPR a na základe žiadostí zo strany používateľov sa vykonávali aj úpravy v časti Subjekty a osoby.

Počas celej doby prevádzky ITMS21+ boli dodržiavané všetky bezpečnostné opatrenia vyplývajúce z požiadaviek na bezpečnosť systému v súlade s Bezpečnostným projektom ITMS21+, Bezpečnostným manuálom ITMS21+ a Manuálom ITMS21+.

V súvislosti so zvýšením bezpečnosti systému ITMS21+ bola dňa 01. 12. 2025 v systéme ITMS21+ (na neverejnej aj verejnej časti) zapnutá dvojfaktorová autentifikácia.

Jedným z hlavných cieľov od samotného začiatku budovania systému ITMS21+ bolo maximálne využiť potenciál otvoreného softvéru, a to nielen v rámci samotného informačného systému, ale aj v rámci fáz a procesov jeho vývoja. ITMS21+ aktuálne reprezentuje informačný systém výlučne postavený na otvorenom softvéri a technológiách, tzv. Open Source.

Navrhnutá architektúra a vybrané technológie umožňujú vlastníčkovi ITMS21+ flexibilne a transparentne reagovať na vznikajúce požiadavky a realizovať efektívne zmeny komponentov/technológií počas životného cyklu ITMS21+. V sledovanom období v rámci prevádzky ITMS21+ neboli zistené výkonové alebo bezpečnostné problémy, ktoré by boli spôsobené priamo ITMS21+.

Zálohovanie ITMS21+ je vykonávané denne na pásky.

Monitorovanie všetkých dôležitých komponentov systému ITMS21+ je zabezpečované prostredníctvom monitorovacieho nástroja.

Počas roka 2025 neboli na infraštruktúrnej úrovni zaznamenané žiadne hardvérové výpadky. Jediný výpadok bol vopred komunikovaný, a to v súvislosti s migráciou ITMS21+ do DMZ.

Dostupnosť produkčného systému ITMS21+ bola v hodnotenom období 99,9 %.

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

Cieľom úlohy je zabezpečiť pomoc používateľom pri práci s aplikáciou ITMS21+ neverejná časť a verejná časť. DataCentrum počas celého roka 2025 poskytovalo 1. úroveň podpory, 2. úroveň podpory (aplikačná, technická a technologická) bola poskytovaná v spolupráci s dodávateľom na základe Objednávky služieb systémovej, databázovej a aplikačnej podpory pre ITMS21+ podľa článku 4 bodu 4.7 zmluvy o zabezpečení prevádzky ITMS2014+.

Všetky problémy používateľov pri práci so systémom ITMS21+ neverejná časť alebo ITMS21+ verejná časť, hlásené prostredníctvom telefónu, e-mailu alebo web rozhraním, boli zaznamenané v aplikácii HP Service Manager a riešené pracovníkmi 2. úrovne podpory, metodické otázky boli riešené na 3. úrovni podpory (odborní garanti z MIRRI SR a MF SR).

V priebehu roka 2025 bolo v aplikácii HP Service Manager zaznamenaných a vyriešených **13 635** hlásení, z toho bolo **13 606** hlásení bolo vyriešených v stanovenom termíne podľa SLA,

pri 29 hláseniach riešených odbornými garantmi bola prekročená doba na vyriešenie. Hlásenia, pri ktorých nebola dodržaná SLA, sa týkali problémov, ktoré si vyžadovali spoluprácu viacerých útvarov DataCentra/MIRRI SR/MF SR, čo predĺžilo čas na vyriešenie hlásenia.

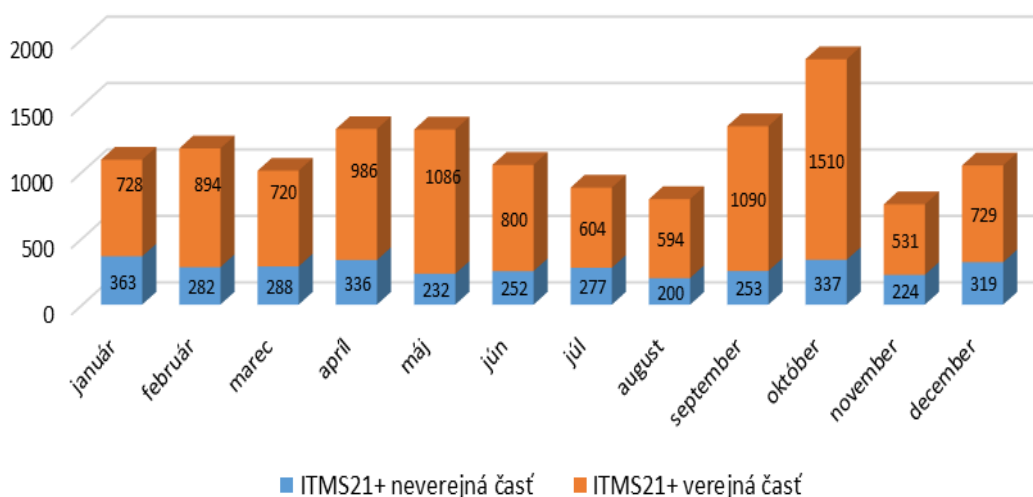
### Doba na vyriešenie incidentu podľa SLA

Klasifikácia	Reakcia
Kategória A (Kritický problém)	1 pracovný deň
Kategória B (Závažný problém)	3 pracovné dni
Kategória C (Nekritický problém)	8 pracovných dní

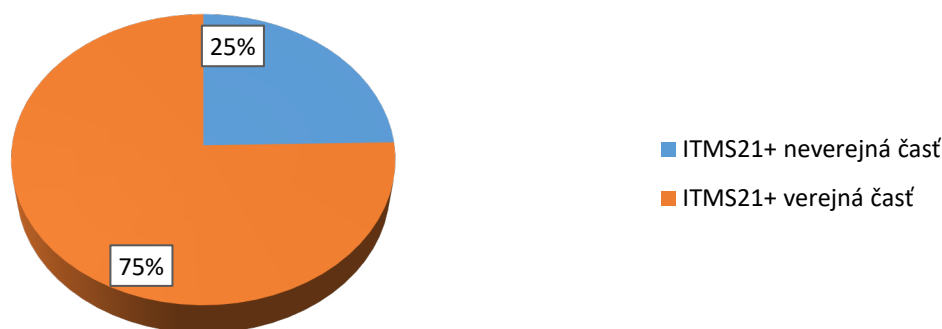
V roku 2025 bolo vyriešených **3 363** hlásení používateľov pre ITMS21+ neverejná časť a **10 272** hlásení používateľov ITMS21+ verejná časť. Prevažná časť hlásení sa týkala problémov s prihlásením sa do systému ITMS21+, problémov používateľov pri vytváraní ŽoAK, problémov pri práci s užívateľskými účtami, pri vytváraní ŽoNFP a tiež metodických usmernení používateľov neverejnej časti ITMS21+.

V mesiaci október 2025 bol v systéme ITMS21+ zaznamenaný zvýšený počet hlásení používateľov v porovnaní s predchádzajúcimi obdobiami, čo bolo spôsobené ukončovaním štyroch výziev Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky a jednej výzvy Ministerstva školstva, výskumu, vývoja a mládeže Slovenskej republiky.

Aplikačná podpora pre ITMS21+ bola poskytovaná permanentne počas pracovných dní v čase od 8.00 hod. do 17.00 hod. a v prípade mimoriadnych situácií aj mimo uvedených hodín.



Graf 1: Počet zaznamenaných a vyriešených hlásení používateľov systému ITMS21+ v roku 2025



Graf 2: Percentuálne zobrazenie vyriešených hlásení používateľov systému ITMS21+ v roku 2025

### 3. Zabezpečovanie prístupov pre používateľov systému

#### **ITMS21+ neverejná časť:**

V rámci realizácie úlohy procesu spracovania ŽoPR do ITMS21+ neverejná časť boli v systéme ITMS21+ na základe doručených ŽoPR vytvárané, aktualizované alebo blokovévané užívateľské kontá.

Úlohou DataCentra bolo zabezpečiť zber, registráciu a kontrolu písomnej formy ŽoPR do ITMS21+ neverejná časť a po schválení žiadosti v systéme ITMS21+ archiváciu originálu doručenej ŽoPR. DataCentrum na základe schválených ŽoPR zriaďovalo, aktualizovalo alebo blokovalo používateľom prístup do produkčného systému ITMS21+ neverejná časť a pre manažérov ITMS21+ aj do predprodukčného systému ITMS21+ neverejná časť. Za sledované obdobie bolo spracovaných **1 377** ŽoPR do neverejnej časti ITMS21+.

K 31. 12. 2025 bolo v ITMS21+ **2 097** aktívnych používateľov neverejnej časti systému. Z tohto počtu bolo ku koncu sledovaného obdobia aktívnych **125** používateľov s duálnym prístupom. Za sledované obdobie bolo vytvorených **457** nových prístupov do neverejnej časti ITMS21+, **560** prístupov do neverejnej časti ITMS21+ bolo aktualizovaných a **345** používateľských účtov bolo zablokovaných na základe schválených ŽoPR s predmetom Zneplatnenie prístupu. **15** ŽoPR bolo zamietnutých. Dôvodom zamietnutia ŽoPR do neverejnej časti ITMS21+ bola nesprávne vyplnená ŽoPR alebo nesplnenie podmienok na schválenie ŽoPR.

Pre Manažérov ITMS21+ bol na požiadanie zriaďovaný aj prístup do neverejnej časti ITMS21+ STG (predprodukčné prostredie ITMS21+ neverejná časť).

DataCentrum v rámci vytvárania prístupov pre používateľov systému zabezpečovalo:

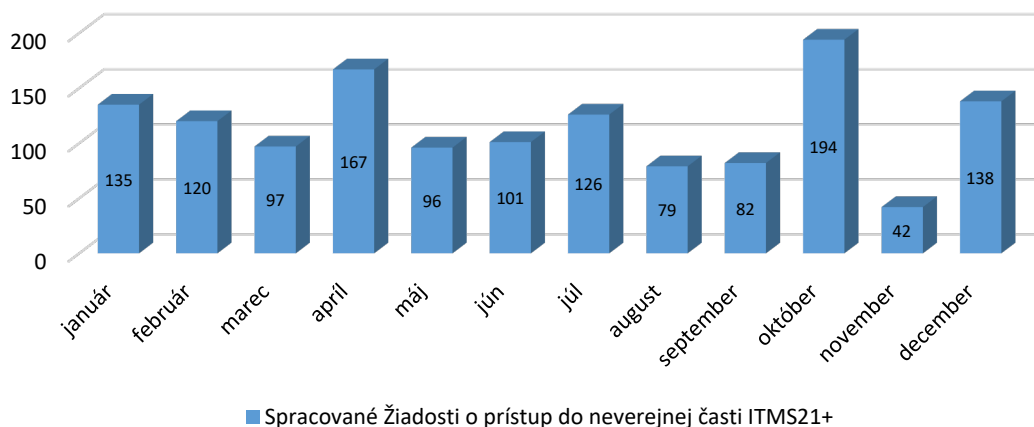
- centralizáciu písomnej formy ŽoPR do ITMS21+ neverejná časť (ŽoPR),
- vytvorenie, aktualizáciu alebo zrušenie prístupov pre používateľov neverejnej časti ITMS21+, resp. duálnych prístupov schválením ŽoPR,
- zakladanie a archiváciu ŽoPR do ITMS21+ neverejná časť,
- zabezpečenie distribúcie všetkých relevantných dokumentov Manažérom ITMS21+ na rezortoch,
- vykonávanie pravidelnej previerky prístupov do systému a spracovanie záznamov z previerok prístupov.

Doba vytvorenia prístupu a aktualizácie používateľských rolí do neverejnej časti systému ITMS21+ je podľa Manuálu ITMS21+ a interného Pracovného postupu č. 78 päť pracovných dní.

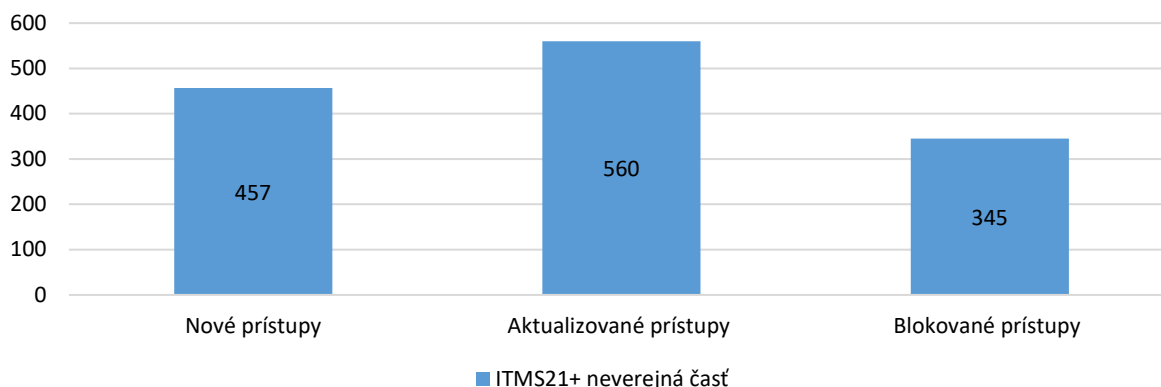
Proces spracovania všetkých doručených žiadostí do neverejnej časti ITMS21+ za rok 2025 (od doručenia ŽoPR do ITMS21+ do DataCentra až po schválenie žiadosti a následné vytvorenie, aktualizáciu alebo zrušenie prístupu do ITMS21+) prebiehal v súlade s Manuálom ITMS21+ a interným Pracovným postupom č. 78.

Z celkového počtu 1 377 doručených ŽoPR do ITMS21+ za rok 2025 bolo 1 367 žiadostí spracovaných do jedného pracovného dňa; 10 ŽoPR do ITMS21+ bolo z dôvodu identifikovaných nedostatkov vrátených na doplnenie, čím došlo k predĺženiu lehoty na ich schválenie a vytvorenie prístupu do neverejnej časti ITMS21+.

V dňoch 06. 08. 2025 a 31. 12. 2025 boli vykonané preverky prístupov do neverejnej časti systému ITMS21+. Na kontrolovaných vzorkách prístupov do neverejnej časti systému ITMS21+ neboli zistené žiadne nedostatky. Z preverky prístupov bol vypracovaný záznam.



Graf 4: Počet spracovaných ŽoPR do neverejnej časti ITMS21+ počas roku 2025



Graf 5: Počty spracovaných prístupov do neverejnej časti ITMS21+ v roku 2025

## ITMS21+ verejná časť:

V rámci realizácie procesu spracovania ŽoAK používateľského konta do verejnej časti ITMS21+ boli DataCentrom vykonávané činnosti - zber, registrácia, kontrola písomnej formy žiadosti s elektronickou a archivácia ŽoAK používateľského konta do ITMS2014+ verejná časť (ŽoAK). Následne, po úspešnej kontrole žiadosti, DataCentrum schválilo ŽoAK a týmto bolo v systéme ITMS21+ vytvorené žiadané užívateľské konto.

V ITMS21+ bolo k 31. 12. 2025 aktívnych **19 091** používateľov verejnej časti, z toho za sledované obdobie bolo schválených **2 061** ŽoAK konta do verejnej časti ITMS21+ a aktivovaných **2 310** používateľských účtov, **15** ŽoAK konta do verejnej časti ITMS21+ bolo zamietnutých. Najčastejším dôvodom zamietnutia žiadosti bolo doručenie žiadosti s chýbajúcim úradným overením podpisu štatutára, prípadne doručenie žiadosti do elektronickej schránky podpísanej s neplatným KEP.

V mesiaci október 2025 bol zaznamenaný zvýšený počet doručených ŽoAK konta do verejnej časti ITMS21+ v porovnaní s predchádzajúcimi obdobiami, čo bolo spôsobené ukončovaním štyroch výziev Ministerstva práce, sociálnych vecí a rodiny Slovenskej republiky a jednej výzvy Ministerstva školstva, výskumu, vývoja a mládeže Slovenskej republiky.

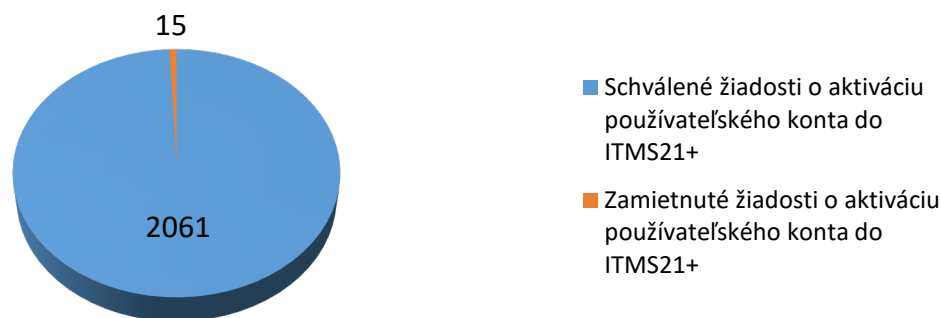
DataCentrum v rámci vytvárania prístupov pre používateľov verejnej časti systému ITMS2014+ zabezpečovalo:

- centralizáciu ŽoAK používateľského konta do ITMS21+ verejná časť,
- kontrolu písomnej formy ŽoAK používateľského konta do ITMS21+ verejná časť s elektronickou formou,
- schválenie ŽoAK (aktivovanie používateľského konta do ITMS21+ verejná časť) do 1 pracovného dňa v prípade, že doručená žiadosť bola úplná a spĺňala všetky náležitosti,
- zakladanie a archiváciu ŽoAK používateľského konta do ITMS21+.

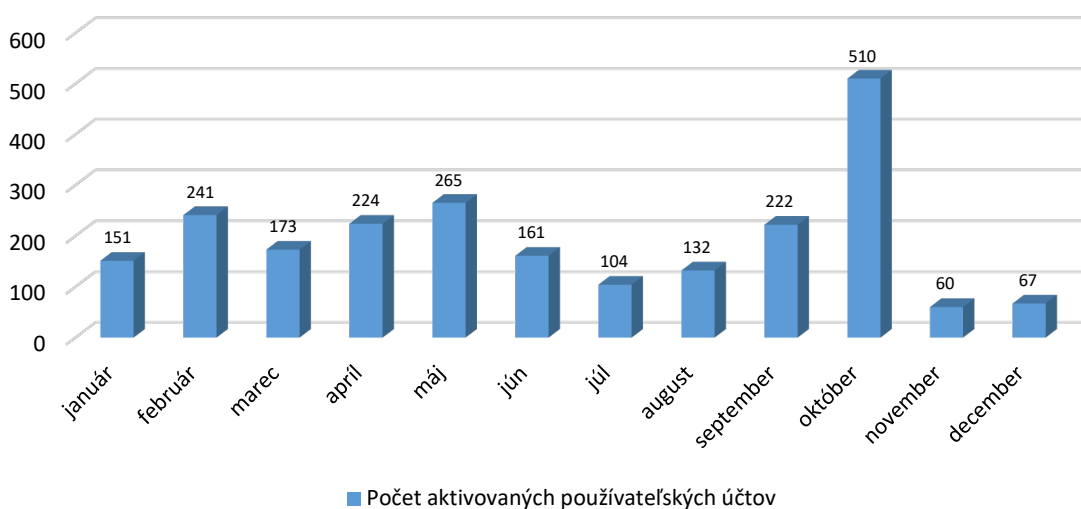
Proces spracovania všetkých doručených žiadostí do verejnej časti ITMS21+ za rok 2025 (od doručenia ŽoAK používateľského konta do ITMS21+ do DataCentra až po schválenie žiadosti a následné vytvorenie prístupu do verejnej časti ITMS21+) prebiehal v súlade s interným Pracovným postupom č. 79.

Z celkového počtu 2 076 doručených ŽoAK používateľského konta do ITMS21+ za rok 2025 bolo 1 972 žiadostí spracovaných do jedného pracovného dňa. 104 ŽoAK používateľského konta do ITMS21+ bolo z dôvodu identifikovaných nedostatkov vrátených na doplnenie, čím došlo k predĺženiu lehoty na ich schválenie a vytvorenie prístupu do verejnej časti ITMS21+.

V rámci funkcionality Technický užívateľ (TP) bolo počas roka 2025 vytvorených **5** nových prístupov. V systéme ITMS21+ je k 31. 12. 2025 **6** aktívnych kont Technický užívateľ.



Graf 7: Počet ŽoAK používateľského konta do ITMS21+ verejná časť za rok 2025



Graf 8: Počet aktivovaných používateľských účtov do ITMS21+ verejná časť počas roku 2025

#### 4. Zabezpečenie bezpečnosti systému

V priebehu roku 2025 sa naďalej vykonávali činnosti vedúce k zabezpečeniu bezpečnosti systému ITMS21+.

V roku 2023 bola vypracovaná, podpísaná a zverejnená zmluva o spracúvaní údajov sprostredkovateľom. Dňa 26. 08. 2024 bola podpísaná zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností medzi DataCentrom a MIRRI SR na účely špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v nadväznosti na zmluvu o spoločnom postupe v súvislosti s používaním Informačného monitorovacieho systému pre Fondy EÚ pre programové obdobie 2021 - 2027. Účelom uvedenej zmluvy je predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby pri plnení zmluvy o spoločnom postupe.

Všetky bezpečnostné opatrenia pre systém ITMS21+ boli navrhované v spolupráci s útvorom bezpečnosti DataCentra a za účasti garantov projektu ITMS21+.

## 5. Realizácia záložného systému ITMS21+

Počas roka 2025 naďalej prebiehali práce na vytvorení záložného prostredia pre ITMS21+. Zároveň bol v roku 2025 aktualizovaný plán zálohovania ITMS21+ a plán obnovy ITMS21.

Dňa 05. 11. 2025 sa uskutočnilo teoretické testovanie plánov obnovy systému ITMS21+. Testovania sa zúčastnili zodpovední zamestnanci MIRRI SR, MF SR, DataCentra a dodávateľov zapojených do obnovy systému ITMS21+. Z testovania bola vypracovaná zápisnica a aktualizované dokumenty - plán zálohovania ITMS21+ a plán obnovy ITMS21+.

<b>221</b>	<b>Komunikačno-technologická infraštruktúra (KTI)</b>
------------	---

Hlavným cieľom úlohy je zabezpečiť nepretržitú správu činnosti celého komunikačného systému, ktorý zabezpečuje spojenia a komunikáciu používateľov IS štátnej pokladnice, informačného systému pre štrukturálne fondy a Kohézny fond a tiež rezortnú počítačovú sieť.

Súčasťou starostlivosti o komunikačné spojenia je aj neustále dopĺňanie systému monitoringu aktívnych liniek v DataCentre, ktoré slúži na sledovanie aktuálnej činnosti liniek a ich potenciálnych poruchových stavov. Počas roka 2025 bolo spravovaných 4 741 liniek, priemerný čas realizácie zriadenia liniek bol 14 dní.

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 2025 IP telefónia DataCentra pracovala bez problémov a v súlade s požiadavkami. Boli vykonávané potrebné zmeny v parametroch klapiek a priebežne boli odstraňované vzniknuté problémy.

Naďalej pokračovalo skvalitňovanie monitorovania chodu počítačovej sály a zvýšil sa počet monitorovaných 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 roka 2025 boli zrealizované pripojenia ďalších rack-ov na systém distribúcie elektrickej energie. Do napájacích vetiev boli inštalované merače prúdu a príkonu. Sústavne boli sledované odbery elektrickej energie v technologických priestoroch. Pravidelne bol 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 používateľov MF SR a finančnej správy prebiehala spolupráca pri nasadzovaní nových aplikácií a pri riešení problémov v prevádzkovaných aplikáciách. Spolu s partnermi v CCN/TC v Bruseli a partnermi ITMS boli pre nové aplikácie k nim vytvárané heslá, pridávané, odoberané, upravované a odblokované kontá podľa požiadaviek vrátane konta pre fronty na bráne a priebežne bola udržiavaná aj potrebná dokumentácia. Dvakrát v roku, v marci a v septembri, bola vykonaná validácia všetkých kont, rovnako ako validácia kontaktných údajov za slovenskú stranu. Nepretržite prebiehalo aj monitorovanie činnosti národného uzla CCN/CSI, pričom boli podľa potreby uskutočňované príslušné zásahy. DataCentrum poskytlo potrebnú súčinnosť pri CCN Conformance migrácii.

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

### **Pre finančnú správu projektu ISVS bolo v roku 2025 zrealizované**

- analýza súčasného stavu zálohovania,
- ISVS backup - modernizácia systému pre zálohovanie a obnovu dát,
- odpojenie starých 3Parov - nasadenie nových zálohovacích serverov a zálohovacích cieľov,
- migrácia SAN direktorov - analýza zón a príprava na migráciu.

Odborní garanti DataCentra kontinuálne zabezpečovali spoľahlivú a bezpečnú prevádzku KTI pre MF SR, Štátnu pokladnicu, Agentúru pre riadenie dlhu a likvidity a finančnú správu.

Pre potreby finančnej správy zabezpečilo DataCentrum technologický upgrade hlavných uzlov WAN (CPE, LAN, FW) a spoľahlivú a bezpečnú prevádzku KTI. Do CMPDC je implementovaný systém sledovania štatistík vyťaženia jednotlivých dátových okruhov finančnej správy s cieľom aktívne monitorovať prevádzku počas implementácie nových aplikácií finančnej správy. Týmto spôsobom bola KTI priebežne nastavovaná podľa aktuálnych záťaží jednotlivých liniek. DataCentrum zabezpečilo zjednotenie WAN sietí finančnej správy 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.

Aj v roku 2025:

- bola naďalej poskytovaná súčinnosť pri realizácii projektu sprísnenej prístupovej a heslovej bezpečnostnej politiky,
- bola poskytovaná súčinnosť pri výmene zastaraných čipových kariet za USB tokeny,
- boli realizované nové prepojenia informačných systémov prevádzkovaných v prostredí KTI s informačnými systémami organizácií štátnej správy.

Počas roku 2025 bola prevádzka aplikačných a infraštruktúrnych systémov KTI realizovaná na požadovanej úrovni, t. j. boli dodržané všetky zmluvne definované SLA. Prevádzka KTI v uplynulom roku bola plynulá, jediný incident nastal dňa 26. 02. 2025, kedy od 8.30 hod. nebolo možné prihlásenie do KTI. Investigáciou problému bola zistená nedostupnosť DHCP servera z nového hardvérového prostredia. Táto nedostupnosť bola zapríčinená sprísňovaním bezpečnostných nastavení v rámci KTI prostredia na základe vykonaných auditov bezpečnosti. Po identifikácii problému boli prijaté operatívne opatrenia na sfunkčnenie DHCP služby, vďaka čomu bolo umožnené prihlasovanie používateľov o cca 11.30 hod. Nedostupnosť KTI trvala 3 hodiny, čo je zároveň aj hodnota celkovej nedostupnosti KTI za rok 2025. Následne po incidente boli prijaté opatrenia na zamedzenie jeho opakovania sa.

V oblasti prevádzky KTI boli v roku 2025 zrealizované aktivity, ktoré spočívali najmä v ukončení prevádzky starej farmy terminálových serverov, ktorá bola v minulom roku v plnom rozsahu nahradená novou farmou s najnovšími verziami všetkých využívaných technológií.

V rámci pokračovania migrácie KTI služieb do prostredia RPC bola zrealizovaná príprava viacerých nových služieb RPC, konkrétne sa jednalo o:

- zvýšenie bezpečnosti prevádzky RPC vypracovaním metodiky centrálnej správy bezpečnostných prostriedkov antivírusového systému v prostredí RPC tenanta a návrh riešenia s vytvorením PoC pre túto službu v prostredí rezortného privátneho cloudu. Služba má za úlohu zabezpečiť priebežné sledovanie bezpečnostných udalostí, identifikáciu potenciálnych hrozieb a podporu pri reakcii na incidenty,
- optimalizáciu existujúcich služieb pred ich transformáciou do RPC; v rámci tejto oblasti bola vypracovaná analýza a návrh riešenia pre presun neterminálových služieb KTI aktuálne prevádzkovaných v prostredí KTI do RPC, súčasťou bolo taktiež vypracovanie návrhu riešenia pre licenčné služby KTI a ďalej návrh riešenia pre oddelenie závislosti IS RIS na službách KTI,
- analýzu adaptácie tenantov aktuálne prevádzkovaných v prostredí KTI na štandardné služby RPC s podrobným popisom služieb tenantov aktuálne prevádzkovaných v prostredí KTI a návrhom ich transformácie na štandardné RPC služby.

<b>222</b>	<b>Komunikačno-technologická infraštruktúra 2 (KTI2)</b>
------------	--

KTI2 je prístupová vrstva na 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 budúcnosti možné využiť aj pre prístup k ďalším aplikáciám.

Prostredie KTI2 bolo vybudované predovšetkým na 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 Multiklientského platobného portálu poskytované ďalšie portálové aplikácie ako EPE (Elektronická portálová evidencia), CKS (Centrálny konsolidačný systém), SEMP (Systém pre evidenciu a monitorovanie pomoci), ďalej boli uvedené do prevádzky portály CEM a CRPŠ (Centrálne evidencie majetku, Centrálne registre pohľadávok štátu), AZÚ (asynchrónny zber údajov, testovací aj ostrý, v záložnom prostredí nie je), reportovací systém BOBJ a DNS služba, CES (Centrálny ekonomický systém), RVO (Register vylúčených osôb), systém Track and trace tabak (TTTSK) a projekt CRÚ (Centrálne registre účtov) a projekt CIS (Cenový informačný systém).

V roku 2025 prebiehalo poskytovanie aplikácií používateľom v stabilnom režime bez zaznamenania závažných neplánovaných výpadkov alebo incidentov, ktoré by mali negatívny vplyv na ich dostupnosť, nedostupnosť KTI2 počas roka 2025 bola na úrovni 0 hodín. Prevádzkové procesy a technická infraštruktúra zabezpečovali spoľahlivú a kontinuálnu prevádzku systémov. Súčasťou bežnej prevádzky boli aj pravidelné kontroly bezpečnostných mechanizmov vrátane priebežného vyhodnocovania a úprav nastavení WAF zabezpečenia s cieľom posilniť ochranu proti bezpečnostným hrozbám.

Súbežne s tým v roku 2025 prebiehali prípravné práce na spustenie ďalšej fázy projektu CES zameranej na samosprávy (CES-VÚC). Hlavný dôraz bol kladený na technickú a procesnú prípravu, definovanie integračných postupov a aktualizáciu súvisiacej dokumentácie s cieľom zabezpečiť hladké a bezproblémové nasadenie projektu pre Košický samosprávny kraj a jeho OvZP. V roku 2025 projekt CRÚ (Centrálny register účtov) pokračoval v stabilnej prevádzke a fungoval bez výpadkov či závažných incidentov. Systém naďalej umožňuje bankám bezpečne zasielať informácie o klientoch cez internet pomocou VPN a oprávneným silovým zložkám pristupovať cez privátne linky, pričom pre používateľov je prístupný prostredníctvom KTI2 prístupovej infraštruktúry. Prevádzka systému prebiehala plynulo a efektívne, čo zabezpečilo spoľahlivú dostupnosť služieb pre všetkých používateľov. V uplynulom období bola taktiež zabezpečená prevádzka záložného prostredia KTI2 v záložnom výpočtovom stredisku, ktorého úlohou je zabezpečiť dostupnosť aplikácií poskytovaných prostredníctvom primárneho prostredia KTI2 v prípade jeho výpadku.

Aj v roku 2025 bol taktiež zakúpený vlastný hardvér na migráciu firewallu v záložnom prostredí. Tento krok zabezpečí vyššiu spoľahlivosť, kontrolu nad infraštruktúrou a dlhodobú udržateľnosť riešenia. 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 sa v prípade potreby uskutočnili rekonfigurácie zariadení, siete alebo systémov.

### **Rozšírenie autentifikačných metód pre dvojfaktorovú autentifikáciu v rámci autentifikačných a autorizačných služieb KTI2 RRP**

V roku 2025 sa podarilo uskutočniť návrh a implementáciu rozvoja služieb prístupovej vrstvy KTI2 vrátane architektúry a implementačného postupu. Bola spracovaná koncepcia centrálného Identity providera (Identity Provider, IdP) a federácie identít podľa SAML/OAuth, ktorá umožní jednotnú autentifikáciu a SSO medzi aplikáciami KTI2 (single sign-on). Definovali sa opatrenia na zvýšenie využívania dvojfaktorovej autentifikácie (two-factor authentication, 2FA) a návrhy úprav pre naplnenie legislatívnych a normatívnych požiadaviek v oblasti riadenia prístupov. Zároveň sa navrhlo a implementovalo riešenie integrácie IS PAGM a správy používateľov RPC do jednotných procesov správy identít.

### **Rozšírenie a optimalizácia poskytovaných služieb pre správu a riadenie prístupov používateľov Centrálného ekonomického systému (CES).**

V rámci tretej vlny rozšírenia CES pre definovaný okruh nových organizácií sa realizovalo rozšírenie a optimalizácia integračných rozhraní RRP, zavedenie riešenia so službami dvojfaktorovej autentifikácie s definovanými procesmi manažmentu autentifikačných prostriedkov a optimalizácia procesu iniciálneho sprístupnenia CES pre cca 20 000 používateľov.

### **Rozšírenie KTI2 RRP – Integrácia SAP Workzone.**

Bol vypracovaný návrh integrácie CES SAP WorkZone do KTI2 RRP vrátane replikácie používateľov a skupín z RRP do SAP. Taktiež bol navrhnutý provisioning prostredníctvom custom adaptera a vývoj WorkZone RRP Proxy pre bezpečnú komunikáciu smerom von z internej siete. Ďalej bola zabezpečená autentifikácia a SSO (single sign-on) s F5 ako Identity Provider (IdP) a SAP WorkZone ako Service Provider (SP).

### **Rozšírenie KTI2 RRP (RRP 2.0)**

V roku 2025 sa podarilo pripraviť analýzu súčasného stavu riešenia KTI2–RRP vrátane procesov, architektúry, integrovaných systémov a integrácií. Bola vypracovaná GAP analýza

voči legislatíve a interným predpisom v oblasti správy identít a prístupov (identity and access management). Na základe analýzy bol navrhnutý cieľový koncept rozšírenia a modernizácie KTI2–RRP s dôrazom na unifikáciu služieb správy identít, elektronizáciu procesov a rozšírenie integračných rozhraní. Vypracovali sa viaceré alternatívy riešenia (existujúce technológie, komerčné alternatívy, open-source) a rámcový návrh architektúry, procesov, UX a reportingu vrátane orientačnej pracovnosti a nákladov.

### **Aplikácia pre zber údajov**

V roku 2025 bola zabezpečovaná aj prevádzka Aplikácie pre zber údajov MS SR (AZÚ) ako nástroja na zber štatistických údajov MS SR. Priebežne boli riešené prevádzkové problémy, pravidelne boli patchované operačné systémy, databázy i aplikácia. Aplikácia i systémové komponenty boli monitorované, na základe zistení z monitoringu prebiehalo proaktívne riešenie vzniknutých problémov. Boli riešené evidované hlásenia od používateľov AZÚ, najmä problémy s prístupmi NS SR cez KTI a taktiež hlásenia ku nastaveniu web-aplikačného firewallu.

<b>223</b>	<b>Poskytovanie služieb riadenia bezpečnosti vo vzťahu MF SR a DataCentra v súčinnosti s tretími stranami</b>
------------	---

Segmentácia siete na zabezpečenie bezpečnosti a dátovej priepustnosti bola nastavovaná podľa požiadaviek nových a aktualizovaných informačných systémov v priebehu celého roka 2025 tak, aby bola v súlade s bezpečnostnými štandardmi a osvedčenými postupmi informačnej bezpečnosti sieťovej prevádzky. V rámci segmentácie siete bolo v roku 2025 vytvorených 32 nových segmentov v sieti LAN a 7 segmentov v sieti DMZ. Pričom celkový počet segmentov v sieti LAN je 367 a 35 v sieti DMZ.

Evidencia a dokumentácia prevádzkových zásahov je evidovaná v elektronickej a papierovej forme (zakladajú sa do zakladača). Požiadavky sa evidujú elektronicke do lokálneho systému SCSM (System Center Service Manager 2022) prevádzkovaného na MF SR. Prístup do helpdesk systému SCSM majú aj zamestnanci odboru informačných technológií - majú tak aktuálny prehľad o požiadavkách, stave ich riešenia a možnosti tlače aktuálnych reportov zo systému.

Incidenty sa nahlasovali telefonicky alebo e-mailom do systému HP Service Manager prevádzkovaného v DataCentre. Na mesačnej báze sa odosielali reporty o stave požiadaviek a incidentov na adresu helpdesk@mfsr.sk.

<b>počet incidentov nahlásených telefonicky do systému HP Service Manager za jednotlivé mesiace</b>												
1	2	3	4	5	6	7	8	9	10	11	12	<b>spolu</b>
114	112	82	69	79	72	70	80	96	94	82	70	<b>1 020</b>

V rámci prevádzkovej podpory pre výpočtovú techniku a informačné systémy boli zaznamenávané požiadavky a incidenty od zamestnancov aj dodávateľov MF SR. Požiadavky od zamestnancov boli zaznamenané cez e-požiadavky prostredníctvom intranetu do systému System center 2022. Celkovo ich bolo 3 151. Z toho bolo 120 s'ahovaní výpočtovej techniky, 166 nástupov nových používateľov a 121 výstupov.

počet e-požiadiaviek nahlásených cez intranet do systému System Center 2022												
za jednotlivé mesiace												
1	2	3	4	5	6	7	8	9	10	11	12	spolu
357	237	283	326	295	272	276	251	194	257	237	166	3 151

Okrem vyššie uvedených incidentov a e-požiadiaviek, bola spracovaná aj e-mailová agenda doručovaná na adresu helpdesk@mfsr.sk, na ktorú bolo doručených za rok 2025 približne 1013 e-mailov.

<b>303</b>	<b>Časové rady v prostredí Lotus Notes</b>
------------	--

V roku 2025 boli v rámci tejto úlohy priebežne prenášané vhodne štrukturované údaje do aplikácie Časové rady v prostredí Lotus Notes na MF SR k používateľom.

Peňažníctvo a menový vývoj – kvartálne údaje za 4. štvrťrok 2024 až 3. štvrťrok 2025 a mesačné údaje za november 2024 až október 2025.

Platobná bilancia SR – kvartálne údaje za 1. štvrťrok 2008 až 2. štvrťrok 2025 a mesačné údaje za január 2008 až september 2025.

<b>311</b>	<b>Podpora používateľov pri práci s aplikáciami rozpočtového informačného systému (RIS)</b>
------------	---

DataCentrum prostredníctvom CPU zabezpečovalo v roku 2025 pre správu a prevádzku informačného systému RIS pomoc používateľom pri používaní jednotlivých modulov, odhaľovanie nekorektnej funkcionality, zbieranie a odovzdávanie námietok na ďalší rozvoj RIS. Pracovisko aplikačnej podpory RIS sa podieľalo na riadiacich a koordinačných činnostiach.

Oddelenie aplikačnej podpory RIS:

- poskytovalo aplikačnú podporu používateľom pri práci s modulmi RIS:
  - RIS.ZoRo - Zostavenie rozpočtu,
  - RIS.MPR - Modul programové rozpočtovanie,
  - RIS.RI - Register investícií,
  - RIS.MÚR - Modul úprav rozpočtu,
  - RIS.NU - Nefinančné ukazovatele,
  - RIS.MaH - Monitorovanie a hodnotenie programovej štruktúry,
  - RIS.KaA - Kontrola a audit,
  - RIS.RKR - Riadenie korupčných rizík,
  - RIS.RR - Riadenie rizík,
- a pri práci s modulmi RIS-SAM - Rozpočtový informačný systém pre samosprávu:
  - RIS.SAM RZP - rozpočet,
  - RIS.SAM VYK - výkazy, konsolidované účtovné závierky,
  - RIS.SAM DOT - dotácie,
  - RIS.SAM DZN - daň z nehnuteľností,
- oddelenie CPU RIS priebežne sprostredkúvalo metodické a organizačné usmernenia medzi vlastníkom procesu, resp. metodickým garantom a používateľmi,

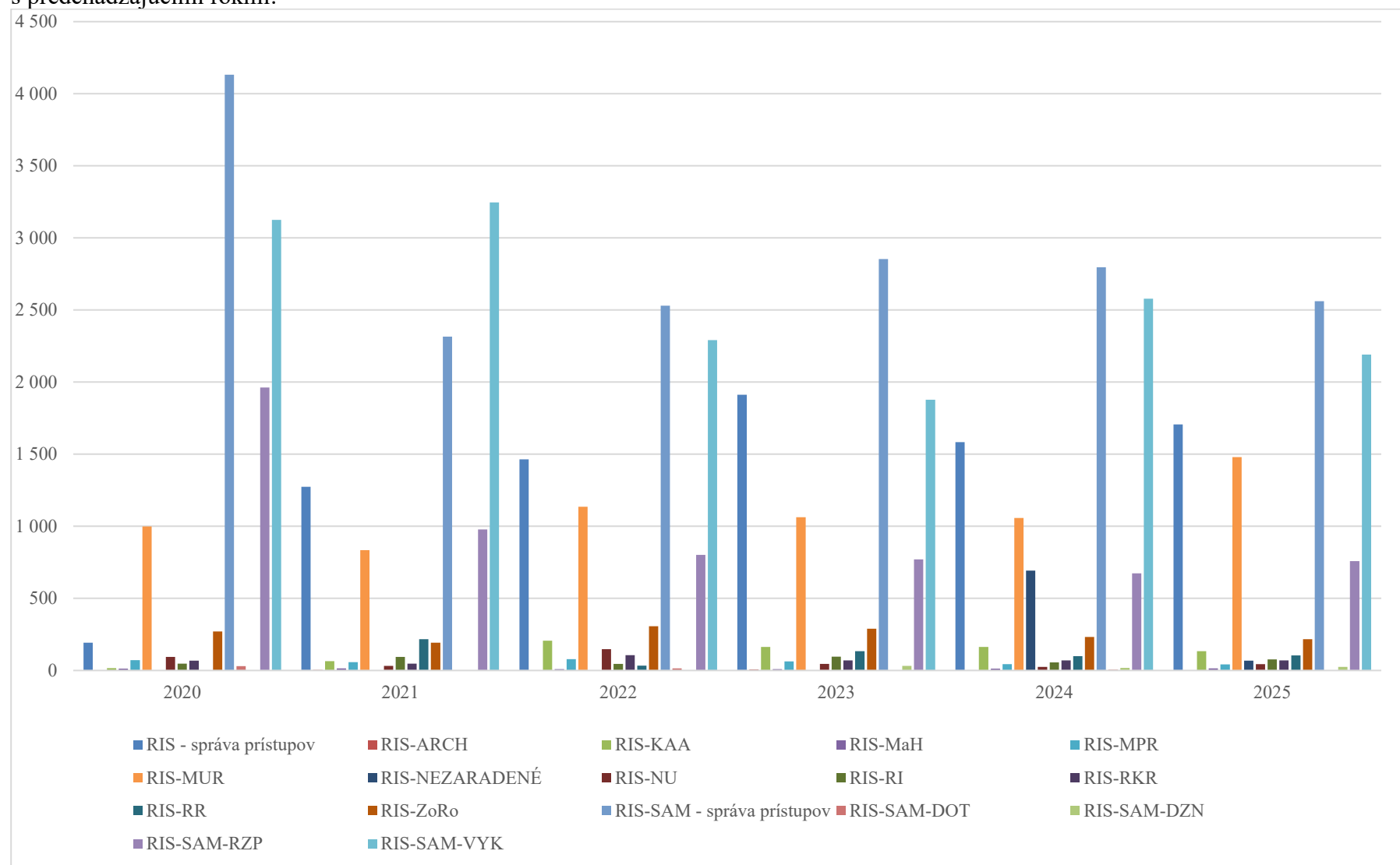
- zaznamenávalo problémy používateľov, ich požiadavky a poskytovalo tieto informácie tretej úrovni podpory, metodickému garantovi a dodávateľovi RIS na účely analýzy najčastejšie sa vyskytujúcich požiadaviek, problémov a navrhovania úprav v jednotlivých moduloch. Pri poskytovaní podpory a služieb spolupracovalo s ostatnými pracoviskami a úrovňami CPU.

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

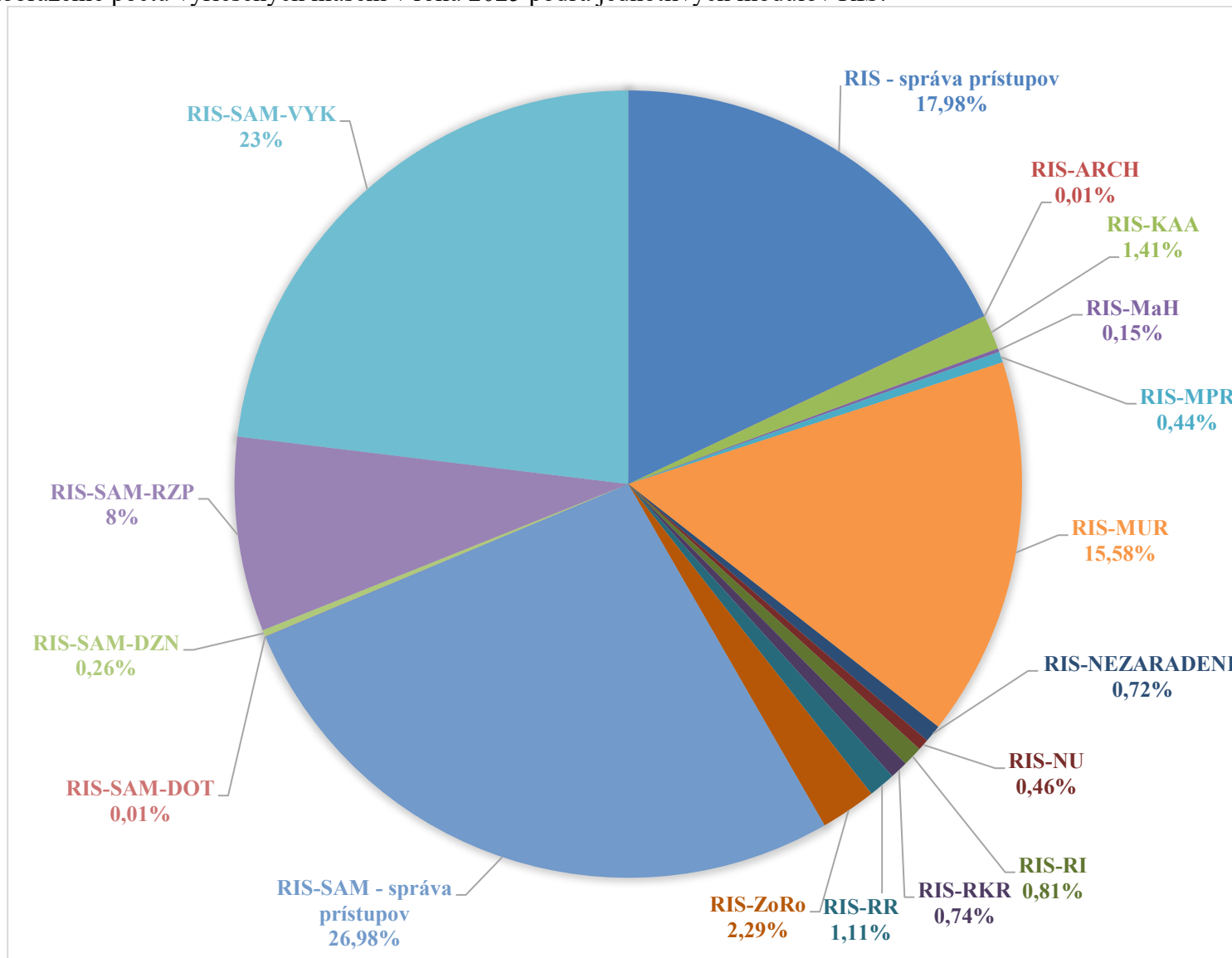
	2020	2021	2022	2023	2024	2025
RIS - správa prístupov	193	1 274	1 465	1 912	1 584	1 707
RIS.ARCH	1	4	0	7	2	1
RIS.KAA	17	64	207	164	163	134
RIS.MaH	13	14	9	9	12	14
RIS.MPR	71	58	78	63	44	42
RIS.MUR	999	834	1 135	1 062	1 057	1 479
RIS.NEZARADENÉ	*	*	*	*	693	68
RIS.NU	94	31	147	45	24	44
RIS.RI	47	94	46	96	56	77
RIS.RKR	68	48	107	69	69	70
RIS.RR	*	217	33	134	100	105
RIS.ZoRo	270	193	307	289	233	217
<b>RIS spolu</b>	<b>1 773</b>	<b>2 831</b>	<b>3 534</b>	<b>3 850</b>	<b>4 037</b>	<b>3 958</b>
RIS.SAM - správa prístupov	4 132	2 316	2 530	2 853	2 797	2 561
RIS.SAM-DOT	30	0	14	1	6	1
RIS.SAM-DZN	1	0	0	32	18	25
RIS.SAM-RZP	1 963	978	801	770	673	758
RIS.SAM-VYK	3 125	3 247	2 292	1 878	2 578	2 190
<b>RIS.SAM spolu</b>	<b>9 251</b>	<b>6 541</b>	<b>5 637</b>	<b>5 534</b>	<b>6 072</b>	<b>5 535</b>
<b>Spolu RIS a RIS.SAM</b>	<b>11 024</b>	<b>9 372</b>	<b>9 171</b>	<b>9 384</b>	<b>10 109</b>	<b>9 493</b>

\* údaje nie sú k dispozícii

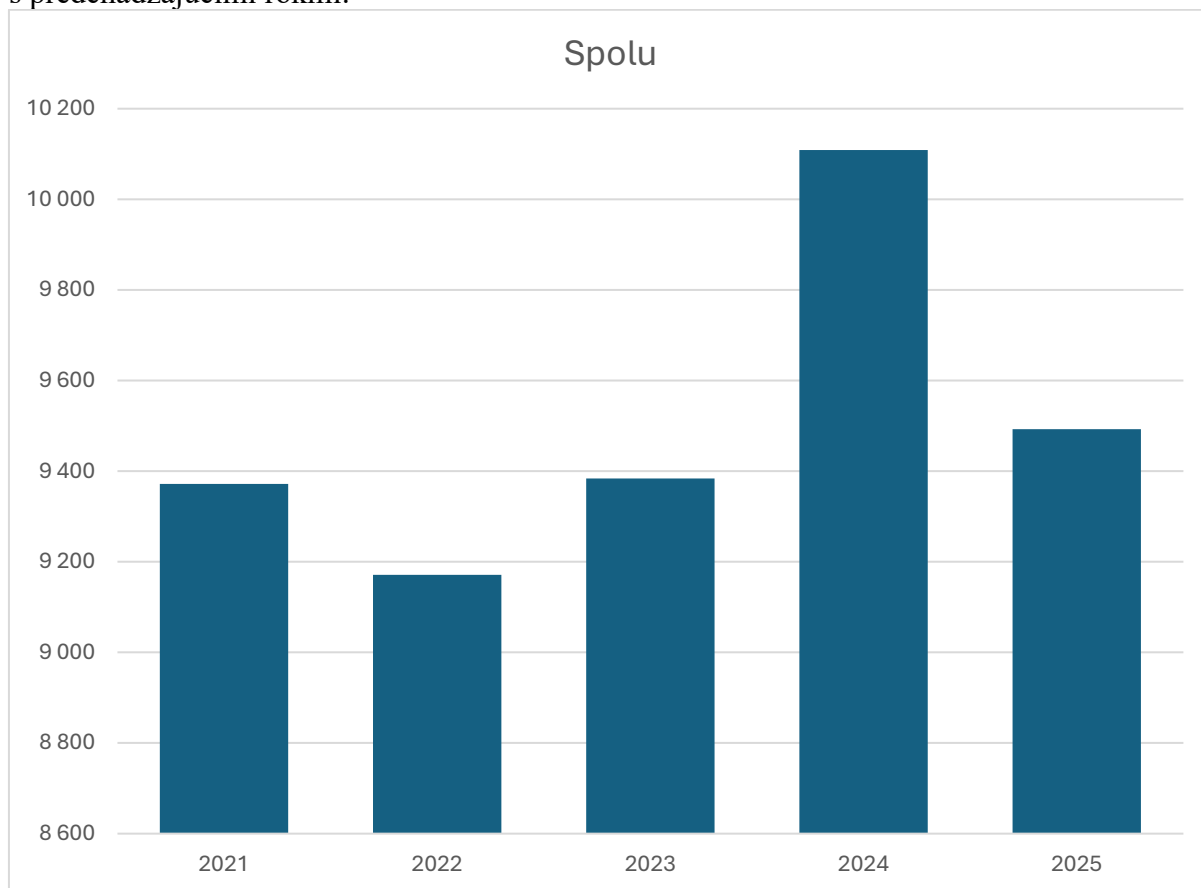
Grafické znázornenie celkového počtu vyriešených hlásení týkajúcich sa aplikačnej podpory RIS po jednotlivých moduloch v porovnaní s predchádzajúcimi rokmi:



Percentuálne zobrazenie počtu vyriešených hlásení v roku 2025 podľa jednotlivých modulov RIS:



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



Vyhodnotenie hodnotiacich kritérií

Hodnotiace kritérium	2025	%	splnené
vyriešených do 24 hod.	8 069	85 %	A
vyriešených do 48 hod.	1 139	12 %	A
nad 48 hod.	285	3 %	A
reklamácie a sťažnosti	0	0 %	A
<b>spolu</b>	<b>9 493</b>	<b>100 %</b>	<b>A</b>

Hodnotiace kritérium je v súčasnosti vyhodnocované na základe kvalifikovaného odborného odhadu, keďže aktuálne používaný systém neumožňuje automatizované sledovanie a jednoznačné vyčíslenie daného SLA parametra. Po nasadení nového systému, ktorý bude poskytovať presné a merateľné údaje o plnení SLA ukazovateľov, bude toto hodnotiace kritérium vyhodnocované priamo na základe týchto exaktných dát.

<b>313</b>	<b>Účtovný informačný systém miestnej samosprávy</b>
------------	--

V roku 2025 boli v rámci tejto úlohy vykonané nasledovné činnosti: úprava programovej aplikácie na uloženie a výber údajov v DataCentre v súvislosti so zmenami vo finančných výkazoch a účtovných závierok pre rok 2024 a pre rok 2025 na 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, aktualizácia klasifikácie výdavkov verejnej správy podľa funkcie – COFOG, aktualizácia ekonomickej klasifikácie a aktualizácia číselníka zdrojov.

Spracovanie finančných výkazov a účtovných závierok obcí k 31. 12. 2024 (9 druhov výkazov), Poznámok k individuálnej účtovnej závierke (štruktúrovanej časti Poznámok – 15 tabuliek) a Poznámok ku konsolidovanej účtovnej závierke (štruktúrovanej časti Poznámok – 24 tabuliek) za rok 2024 a spracovanie finančných výkazov obcí k 31. 03. 2025, k 30. 06. 2025 a 30. 09. 2025 (6 druhov výkazov) za 2 926 obcí, 2 190 rozpočtových organizácií v pôsobnosti obcí, 245 príspevkových organizácií v pôsobnosti obcí a ostatných subjektov verejnej správy, ktoré majú povinnosť predložiť výkazy v zmysle platnej legislatívy, spracovanie účtovných závierok k 31. 12. 2024 (3 druhy výkazov) za 723 ostatných subjektov verejnej správy 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 2024, mesačne a za 1. až 3. štvrťrok 2025 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 2024 a 1. až 3. štvrťrok 2025 a mesačné spracovanie finančného výkazu FIN 1-12.

Okrem štandardných zostáv pre MF SR bolo odovzdaných 43 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. Ďalej výber a prenos individuálnych údajov za obce, rozpočtové a príspevkové organizácie v ich pôsobnosti a ostatné subjekty verejnej správy do CKS za 4. štvrťrok 2024. Vytvorenie a odovzdanie požadovaných výstupov Centru vedecko-technických informácií SR, MD SR, Najvyššiemu kontrolnému úradu SR a subjektom ŠÚ SR, Národnej banke Slovenska, Rade pre rozpočtovú zodpovednosť, Ministerstvu cestovného ruchu a športu SR, Republikovej únii zamestnávateľov a iným podnikateľským subjektom, s ktorými MF SR uzatvorilo zmluvu o poskytovaní údajov. Bol aktualizovaný obsah prílohy č. 1 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. 2025. 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 2025 bola poskytnutá užívateľská podpora pri práci so systémom RIS.SAM v súčinnosti s CPU DataCentra.

## 314 Správa zberov v RIS.SAM

V roku 2025 v rámci tejto úlohy v systéme RIS.SAM bola vykonávaná správa zberov – zber Finančné výkazy (2024 Finančné výkazy IV. kvartál, 2025 Finančné výkazy I. kvartál, 2025 Finančné výkazy II. kvartál, 2025 Finančné výkazy III. kvartál), Finančné výkazy Ostatné SVS (2024 Finančné výkazy December - Ostatné SVS, 2025 Finančné výkazy Január - Ostatné SVS, 2025 Finančné výkazy November - Ostatné SVS), Individuálna ÚZ (2024 Individuálna ÚZ Obce, RO, PO, 2024 Individuálna ÚZ Ostatné SVS), Formulár vzájomných vzťahov (2024 Formulár vzájomných vzťahov), Konsolidovaná ÚZ (2024 Konsolidovaná ÚZ Obce, RO, PO, 2024 Konsolidovaná ÚZ Ostatné SVS), Mimoriadna IÚZ (2025 Mimoriadna IÚZ Obce, RO, PO, 2025 Mimoriadna IÚZ Ostatné SVS), Finančné výkazy k 31. 12. podľa schválenej ÚZ (2024 Finančné výkazy k 31.12. podľa schválenej ÚZ) a zber Konsolidačný balík, 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 a ďalšie činnosti vyplývajúce z roly administrátora a importéra.

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 ÚZ, Formulár vzájomných vzťahov a Konsolidovaná ÚZ 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 na účely spracovania Súhrnnej účtovnej závierky MF SR.

V roku 2025 bola poskytnutá užívateľská podpora pri práci so systémom RIS.SAM v súčinnosti s CPU DataCentra.

## 316 Informačný systém pre centrálnu evidenciu zmlúv o hypotekárnych úveroch

Centrálna evidencia zmlúv o hypotekárnych úveroch s nárokovaným štátnym príspevkom a štátnym príspevkom pre mladých je vedená v zmysle zákona č. 483/2001 Z. z. o bankách v znení neskorších predpisov a Dohody uzavretej medzi MF SR a príslušnou bankou poskytujúcou úvery so štátnym príspevkom.

Za hodnotené obdobie roka 2025 bolo v januári uzatvorené spracovanie údajov za rok 2024. Boli archivované údaje databázy centrálnej evidencie k 31. 12. 2024, vstupné súbory predložené bankami, výstupné súbory, písomnosti a zostavy vytvorené v DataCentre za jednotlivé mesiace spracovania príslušného kalendárneho roka.

Údaje, ktoré patria do kategórie osobných údajov, boli spracované v súlade so ZOOÚ a všeobecným nariadením o ochrane údajov GDPR. Ochrana predkladaných údajov bola zabezpečená šifrovaním predmetných súborov prostriedkom Symantec Encryption Desktop (ďalej len „PGP“).

Verejné kľúče platné pre kalendárny rok 2025 na operáciu šifrovania a overovania elektronických podpisov boli poskytnuté oprávneným osobám bánk a MF SR. Oprávnené osoby potvrdili prevzatie kľúčov písomným protokolom.

Banky, ktoré evidujú hypotekárne úvery s nárokovaným štátnym príspevkom, predkladali údaje do centrálnej evidencie v šifrovaných súboroch prostredníctvom elektronickej pošty do e-mail schránky oprávnených osôb DataCentra. Nezrovnalosti v štruktúre, formáte a nedostatky vo vecnej správnosti predložených údajov zistené pri ich kontrole boli oznámené oprávnenej osobe príslušnej banky. Po oprave a opätovnom predložení súboru korektných údajov zo strany bánk prebehlo spracovanie údajov v zmysle požiadaviek MF SR. Súbory, ktoré obsahovali chybné údaje, boli bezpečne mazané pomocou PGP.

Cieľom mesačného spracovania údajov v centrálnej evidencii zmlúv bolo vyhodnotiť nárok poberateľa úveru na poskytnutie štátneho príspevku z pohľadu viacnásobného uplatnenia nároku v jednom kalendárnom roku. Súčasťou spracovania bola mesačne vypočítavaná celková suma nárokovaného štátneho príspevku v eurách za jednotlivé banky a typ úveru. K vzniknutým rozdielom v celkovej výške nárokovaného štátneho príspevku vypočítaného z údajov centrálnej evidencie a skutočne nárokovaného štátneho príspevku jednotlivými bankami prebehli konzultácie s oprávnenými osobami bánk. Následne došlo k zosúladieniu sumy nárokov na štátny príspevok za príslušné obdobie spracovania.

Výstupom spracovania boli zostavy predkladané na MF SR a hypotekárnym bankám opäť formou šifrovaných elektronických súborov. Priebežne boli spracovávané požiadavky zo strany bánk na opravu údajov v databáze údajov a mimoriadne požiadavky zo strany MF SR.

Pre sekciu auditu a kontroly MF SR, odbor vládneho auditu vlastných zdrojov boli z centrálnej evidencie poskytnuté podklady pre výkon štátneho dozoru pri čerpaní prostriedkov zo štátneho rozpočtu určených na štátny príspevok k hypotekárnym úverom. Analýza údajov sa týkala zmlúv evidovaných za Všeobecnú úverovú banku, a.s., Slovenskú sporiteľňu, a.s., Tatra banku, a.s., Československú obchodnú banku, a.s., UniCredit Bank Slovakia, a.s., a obdobie špecifikované v príslušnej požiadavke sekcie auditu a kontroly.

**317**

**Podpora používateľov pri práci s aplikáciou CKS, časť Výkazníctvo**

DataCentrum aj v roku 2025 plnilo úlohu zabezpečenia pomoci koncovým používateľom pri používaní informačného systému CKS, časť Výkazníctvo. Zabezpečovalo aplikačnú podporu v module Výkazníctvo pre koncových používateľov, odhaľovanie nekorektností a disfunkcionalít v aplikácii, zber a odovzdávanie námietok pre ďalší rozvoj tohto informačného systému.

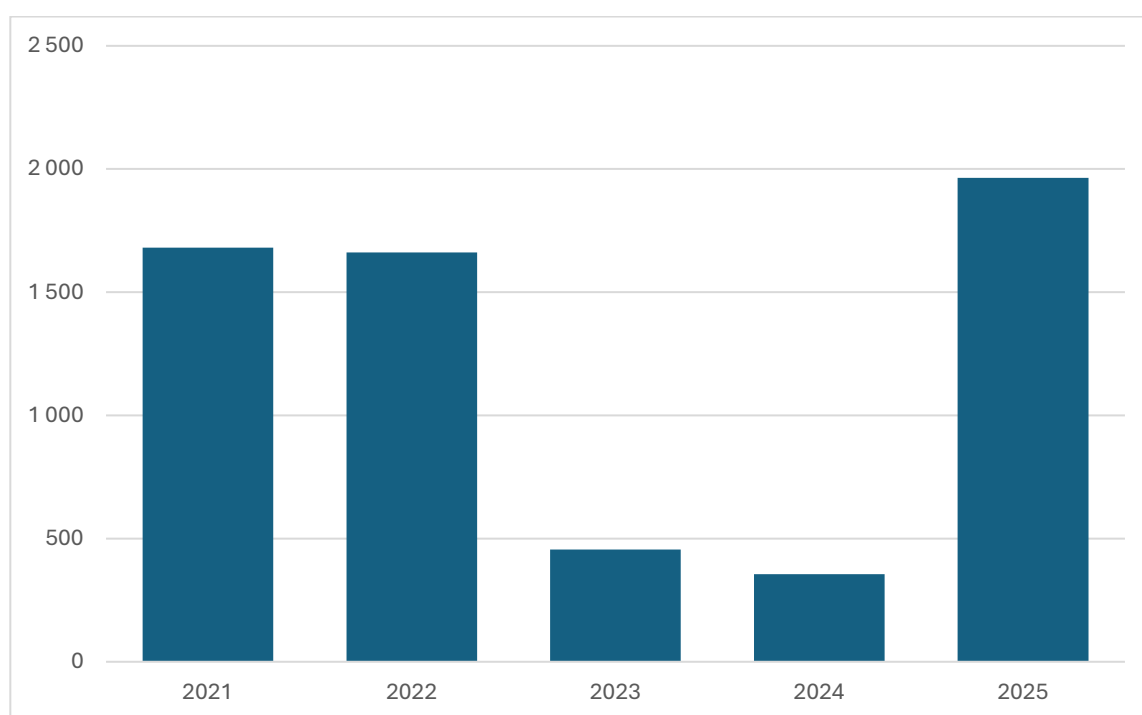
Pomoc používateľom modulu CKS časť Výkazníctvo bola zabezpečovaná prostredníctvom metodického a organizačného usmernenia a komunikáciou s riešiteľmi na tretej úrovni podpory na účely vyriešenia používateľského problému. Zaznamenávané boli aj užívateľské pripomienky a požiadavky ako námety na analýzy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

Celkový počet hlásení týkajúcich sa aplikačnej podpory modulu CKS časť Výkazníctvo je v porovnaní s ostatnými rokmi nasledovný:

Modul	2021	2022	2023	2024	2025
Výkazníctvo	1 681	1 662	455	356	1 964

Nárast hlásení vznikol z dôvodu, že podpora prešla z IS ŠP pod CKS a používatelia nás kontaktovali z dôvodu navigácie a prvotnej orientácie v aplikácií, následne sa počet hlásení stabilizoval. Identifikačný list sa zmenil už pre rok 2025, a to v názve, keďže úloha ostala rovnaká, len prešla pod inú pracovnú skupinu (oddelenie).

V grafickom vyjadrení počet uzatvorených hlásení k výkazníctvu v porovnaní s predchádzajúcimi rokmi:



Vyhodnotenie hodnotiacich kritérií:

Hodnotiace kritérium	2025	%	splnené
vyriešených do 24 hod.	1 590	81 %	A
vyriešených do 48 hod.	235	12 %	A
nad 48 hod.	139	7 %	A
reklamácie a sťažnosti	0	0 %	A
<b>spolu</b>	<b>1 964</b>	<b>100 %</b>	<b>A</b>

Hodnotiace kritérium je v súčasnosti vyhodnocované na základe kvalifikovaného odborného odhadu, keďže aktuálne používaný systém neumožňuje automatizované sledovanie a jednoznačné vyčíslenie daného SLA parametra. Po nasadení nového systému, ktorý bude poskytovať presné a merateľné údaje o plnení SLA ukazovateľov, bude toto hodnotiace kritérium vyhodnocované priamo na základe týchto exaktných dát.

V hodnotenom období plnilo DataCentrum úlohu podpory používateľov zabezpečením pomoci koncovým používateľom pri používaní Informačného systému 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 námietov pre ďalší rozvoj tohto IS a participovalo tiež na spolupráci riešiteľov systémov RIS a IS ŠP.

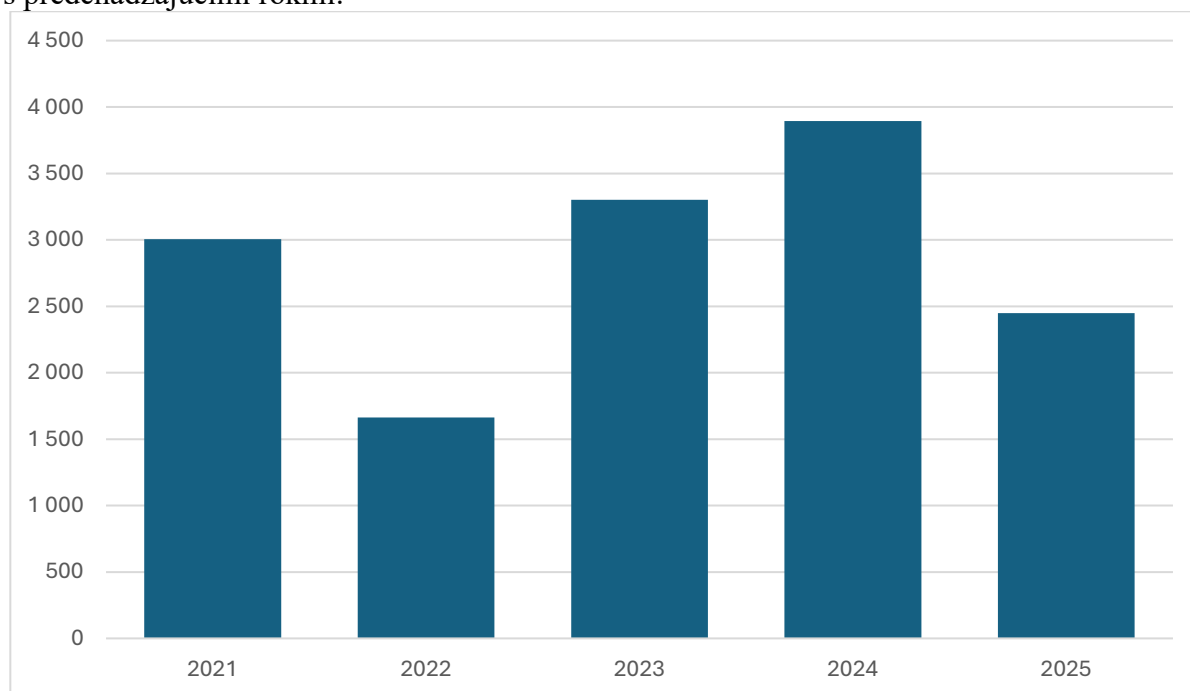
Pomoc používateľom modulu IS ŠP pre riadenie výdavkov (ManEx) bola realizovaná prostredníctvom telefonického komunikácie a priamou navigáciou na obrazovke. Používateľom boli sprostredkované metodické a organizačné usmernenia a komunikácia s riešiteľmi na tretej úrovni podpory na účely vyriešenia používateľského problému. Okrem toho boli zaznamenávané užívateľské pripomienky a požiadavky ako námety na 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 pracovnými skupinami CPU.

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

Modul	2021	2022	2023	2024	2025
Riadenie výdavkov	3 006	1 662	3302	3 894	2 449

V grafickom vyjadrení počet hlásení súvisiacich s riadením výdavkov v porovnaní s predchádzajúcimi rokmi:



Vyhodnotenie hodnotiacich kritérií:

Hodnotiace kritérium	2025	%	splnené
vyriešených do 24 hod.	2 204	90 %	A
vyriešených do 48 hod.	196	8 %	A
nad 48 hod.	49	2 %	A
reklamácie a sťažnosti	0	0 %	A
<b>spolu</b>	<b>2 449</b>	<b>100 %</b>	<b>A</b>

Hodnotiace kritérium je v súčasnosti vyhodnocované na základe kvalifikovaného odborného odhadu, keďže aktuálne používaný systém neumožňuje automatizované sledovanie a jednoznačné vyčíslenie daného SLA parametra. Po nasadení nového systému, ktorý bude poskytovať presné a merateľné údaje o plnení SLA ukazovateľov, bude toto hodnotiace kritérium vyhodnocované priamo na základe týchto exaktných dát.

### 321 Spracovanie údajov o dani z nehnuteľnosti

V rámci úlohy boli zapracované zmeny do programového vybavenia úlohy na spracovanie údajov z Výkazov o dani z nehnuteľností za rok 2024 v prostredí RIS.SAM v súlade s opatrením Ministerstva financií Slovenskej republiky 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 2 827 výkazov, ktoré boli skontrolované a spracované podľa požiadaviek MF SR.

K 09. 07. 2025 boli vytvorené výstupy v papierovej forme. Tabuľková časť obsahovala spracované údaje za Slovenskú republiku, kraje a okresy SR za rok 2024 a grafická časť obsahovala prehľad vývoja jednotlivých ukazovateľov za Slovenskú republiku a kraje za roky 2016-2024. Taktiež boli vytvorené výstupy v elektronickej forme v podobe súboru \*.pdf. Súbor v \*.pdf formáte obsahoval presne to, čo výstupy v papierovej forme.

### 323 Informačný systém pre centrálnu evidenciu zmlúv o stavebnom sporení

V rámci úlohy boli na zabezpečenie ochrany osobných údajov začiatkom roka vygenerované, vymenené a archivované verejné PGP kľúče oprávnených osôb na MF SR, v DataCentre a za stavebné sporiteľne zapojené do prevádzky IS pre centrálnu evidenciu zmlúv o stavebnom sporení v roku 2025.

Mesačne boli vytvárané štandardné výstupy z prémiovo zvýhodnených zmlúv fyzických osôb a štandardné výstupy z prémiovo zvýhodnených zmlúv právnických osôb za obdobie 12/2024 - 11/2025 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.

Mesačne boli vytvárané výstupné súbory o poskytnutých medziúveroch pre fyzické osoby za obdobie 12/2024 - 11/2025 pre MF SR, na základe ktorého strácajú fyzické osoby nárok na

prémiovo zvýhodnené zmluvy vo všetkých stavebných sporiteľniach počas obdobia trvania medziúveru.

Tiež boli mesačne vytvárané štandardné výstupy z prémiovo zvýhodnených zmlúv fyzických osôb a štandardné výstupy z prémiovo zvýhodnených zmlúv právnických osôb za obdobie 12/2024 - 11/2025 pre stavebné sporiteľne, ako aj výstupné súbory o poskytnutých medziúveroch pre fyzické osoby za obdobie 12/2024 - 11/2025.

Bol vypracovaný výstup zo spracovania oprávnených finančných nárokov fyzických osôb a výstup zo spracovania oprávnených finančných nárokov právnických osôb za rok 2024 pre MF SR. Prebehla aktualizácia existujúceho programového vybavenia informačného systému platného od 01. 02. 2025.

Bola prevedená archivácia centrálnej databázy stavebných sporiteľov za rok 2024, vstupných a výstupných súborov a programového vybavenia úlohy za rok 2024.

341

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

V rámci úlohy boli v roku 2025 priebežne importované údaje z RÚZ vo forme \*.csv súborov z riadnych účtovných závierok podnikateľov (Úč POD 1-01, Úč POD 2-01) a mikro účtovných jednotiek (Úč MÚJ 1-01, Úč MÚJ 2-01) za roky 2023 a 2024.

Bolo ukončené štandardné spracovanie údajov za rok 2023 v celkovom objeme 292 096 súvah a výkazov ziskov a strát. Konečný počet údajov v databáze je 286 721 dvojíc výkazov, z toho 78 071 Úč POD a 208 650 Úč MÚJ.

Na spracovanie nového účtovného obdobia prebehla aktualizácia existujúceho programového vybavenia informačného systému.

Spracovanie údajov účtovných výkazov predstavovalo: importovanie údajov z RÚZ, nahrávanie údajov do rezortnej databázy Oracle, formálne a logické kontroly údajov, identifikáciu a zaznamenanie zistených chýb, rozdelenie údajov na správne, chybné a vylúčené zo spracovania, doplnenie chýbajúcich identifikačných kódov IČO, DIČ, právnej formy a iné. Tvorba registra účtovných jednotiek so správnymi údajmi a priradenie štatistických klasifikácií týmto účtovným jednotkám.

Boli vytvorené nové a aktualizované existujúce programové aplikácie pre tvorbu výstupov agregovaných a individuálnych údajov a individuálnych anonymizovaných údajov v zmysle požiadaviek odberateľov za roky 2019 až 2024. Vo viacerých etapách boli vytvárané a poskytované výstupy vo forme súborov pre:

- MF SR: generálny tajomník služobného úradu (pre externých odberateľov, s ktorými MF SR uzatvorilo zmluvu o poskytovaní údajov), inštitút finančnej politiky;
- ŠÚ SR v zmysle zmluvy;
- Slovak Business Agency v zmysle zmluvy a poverenia MF SR;
- MPRV SR v zmysle objednávok.

Bolo zabezpečené sťahovanie naskenovaných výkazov 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 (IFRS) určených na typovanie, distribúciu a ich spätné importovanie do RÚZ pre zobrazenie výkazov v štruktúrovanej forme.

Z výkazov IFRS boli stiahnuté údaje VÚ-P 1-04 za rok 2023 v počte 30 ks. Za rok 2024 boli stiahnuté údaje v celkovom objeme v počte 160 ks, z toho 114 ks výkazov VÚ POD 1-01, 46 ks výkazov VÚ-B 1-01.

Údaje z výkazov VÚ POD 1-01 boli z RÚZ exportované, spracované a poskytnuté ŠÚ SR v zmysle zmluvy a na MF SR (inštitút finančnej politiky) v počte 99 ks.

<b>342</b>	<b>Účtovný informačný systém účtovných výkazov podnikateľskej sféry fyzických osôb účtujúcich v systave jednoduchého účtovníctva.</b>
------------	---

V prvom polroku 2025 boli preberané údaje prostredníctvom exportu dát z RÚZ. Spracovanie týkajúce sa nahrávania, kontroly a korekcie určitého typu chýb prebehlo pre účtovné závierky roku 2023. Na záver spracovania účtovného obdobia roku 2023 bola uskutočnená archivácia údajov, ako aj registra účtovných jednotiek so štatistickými klasifikáciami do prezentačnej vrstvy v konečnom rozsahu 53 617 dvojíc výkazov.

Pre Slovak Business Agency a MH SR boli zrealizované v marci finálne výstupy z individuálnych anonymizovaných údajov výkazov Úč FO za rok 2023 na základe poverenia MF SR.

Odberateľom zo ŠÚ SR boli poskytnuté výstupné zostavy vytvorené z údajov ÚIS FO za rok 2023 vo forme definitívnych výstupov.

V júni bola realizovaná požiadavka Ministerstva pôdohospodárstva a rozvoja vidieka SR na agregované výstupy subjektov podľa SK NACE za roky 2023 a 2024 pre odbor politiky lesného hospodárstva a spracovania dreva.

Na konci prvého polroka boli prevzaté údaje z RÚZ za účtovné výkazy Úč FO 2024. Z týchto dát v objeme cca 38 500 tisíc subjektov boli vytvorené individuálne výstupy pre ŠÚ SR v zmysle Dohody o vzájomnej spolupráci v oblasti štatistiky.

V 2. polovici roka pokračovalo priebežné preberanie údajov z výkazov za sledované účtovné obdobie 2024 umiestnených v RÚZ. Prevzaté údaje sa pre potreby našej databázy aktualizovali pravidelne prostredníctvom údajov z registrov dodávaných ŠÚ SR. Štandardné spracovanie sa ku koncu roka týkalo približne 49 tisíc dvojíc výkazov.

V auguste prebehli konzultácie s Ministerstvom pôdohospodárstva a rozvoja vidieka SR ohľadom ich požiadaviek na výber údajov, následne sa pripravili pre inštitút pôdohospodárskej politiky požadované výstupy z individuálnych údajov.

Pre odberateľov zo ŠÚ SR z odboru metodiky registrov boli v 2. polroku vo dvoch dávkach vytvorené výstupy individuálnych údajov Úč FO 1-01 a Úč FO 2-01 zvlášť z údajov bezchybných a z údajov chybových.

Pre spoločnosť CRIF – Slovak Credit Bureau sme pripravili v druhom polroku dva typy výstupov – podľa kategorizácie živnostníkov, ako aj z anonymizovaných individuálnych údajov z dát ÚZ FO 2024.

Pre Slovak Business Agency a Ministerstvo hospodárstva SR bola v novembri odovzdaná v zmysle poverenia MF SR prvá dávka predbežných anonymizovaných individuálnych údajov FO za rok 2024 na základe nimi stanovených výberových kritérií.

<b>343</b>	<b>Účtovný informačný systém neziskových organizácií účtujúcich v sústave podvojného účtovníctva</b>
------------	--

V rámci tejto úlohy boli zaktualizované metadátové tabuľky parametrov a príprava skriptov pre vytvorenie výstupných súborov typu \*.csv a vypracované výstupné súbory k 31. 03. 2025 pre ŠÚ SR podľa zadaných požiadaviek – finálne údaje za rok 2023. Konečný počet údajov v databáze za rok 2023 je 10 070 dvojíc výkazov. Priebežne pokračovalo sťahovanie dávok výkazov z RÚZ a následné nahrávanie do tabuliek centrálného databázového systému v prostredí IT Oracle. V databáze bolo potrebné urobiť korekcie kvôli duplicitám a chybným identifikáciám. Boli vypracované výstupné súbory pre ŠÚ SR: údaje za rok 2024 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, individuálne údaje z účtovných výkazov Súvaha Úč NUJ 1-01, 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 13. 08. 2025 a k 30. 11. 2025.

<b>344</b>	<b>Účtovný informačný systém účtovných výkazov neziskovej sféry – jednoduché účtovníctvo</b>
------------	--

V rámci tejto úlohy boli v roku 2025 odovzdané finálne zostavy za rok 2023 za individuálne údaje a vykonaná archivácia výkazov a údajov v databáze za výkazy Úč NO 1-01 a Úč NO 2-01 k 31. 12. 2023. Konečný počet údajov v databáze za rok 2023 je 12 331 dvojíc výkazov. Zároveň boli zaktualizované metadátové tabuľky parametrov a príprava skriptov pre vytvorenie výstupných zostáv typu \*.csv podľa zadaných požiadaviek. Pre potreby ŠÚ SR boli údajmi z RÚZ naplnené databázové tabuľky v prostredí Oracle. Priebežne pokračovalo sťahovanie dávok výkazov z RÚZ a následné nahrávanie do tabuliek centrálného databázového systému v prostredí IT Oracle. Po doplnení dodatočne predložených výkazov bola uskutočnená aktualizácia databázových tabuliek, oprava chybných identifikácií výkazov v súlade s Registrom ŠÚ SR a Daňovým registrom, korekcia duplicit a oprava opraviteľných chýb vo výkazoch. Boli vypracované výstupné súbory pre ŠÚ SR: údaje za rok 2025 z účtovných výkazov Úč NO 1-01 (Príjmy a výdavky) a Úč NO 2-01 (Majetky a záväzky), zoznam spravodajských jednotiek, ktoré predložili výkazy za dobré a chybové údaje, individuálne údaje z účtovných výkazov za dobré a chybové údaje a zoznam spravodajských jednotiek, ktoré sa nenachádzajú v registri ŠÚ SR rozdelený na dva MS Excel súbory za dobré a chybné účtovné jednotky. Výstupné zostavy boli odovzdané ŠÚ SR v termínoch: k 13. 08. 2025 a k 30. 11. 2025.

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

V priebehu prvého polroka 2025 bolo uskutočnené prevzatie a spracovanie údajov registra priestorových jednotiek, registra ekonomických subjektov zo ŠÚ SR za rok 2024, ako aj číselníkov prislúchajúcich k tomuto registru a nahrané do prostredia Oracle.

V priebehu roka bol dopĺňaný a aktualizovaný register ekonomických subjektov podľa požiadaviek používateľov.

**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. Prebehla 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 (ide 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 2025 sa uskutočnilo spracovanie údajov za 4. štvrťrok 2024, 1. štvrťrok, 2. štvrťrok a 3. štvrťrok 2025, pričom boli vypracované a odovzdané súhrnné tabuľky na MF SR vrátane zoznamov subjektov, ktorých údaje boli do nich zahrnuté.

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

**401****Technologická infraštruktúra dátovej sály MF SR**

DataCentrum v roku 2025 zabezpečilo nepretržitú prevádzku technologickej infraštruktúry dátovej sály na MF SR bez neplánovaných výpadkov, aj vďaka neustálemu monitoringu zariadení a požadovaných parametrov pre dátovú sálu. Zabezpečovali sa pravidelné servisné kontroly, opravy, zákonom stanovené revízie a odborné skúšky na jednotlivých zariadeniach.

V prípade zmien bola aktualizovaná relevantná prevádzková dokumentácia. Všetky činnosti súvisiace so zabezpečením nepretržitej prevádzky boli konzultované a vykonávané v súčinnosti zamestnancov DataCentra, MF SR a dodávateľa služieb. Plánované odstávky boli vopred nahlásené a schválené MF SR. Vďaka nášmu úsiliu a súčinnosti MF SR bola garantovaná dostupnosť poskytovaných služieb v režime 24/7/365.

**402****Technická, komunikačná a systémová podpora projektov**

Popri štandardnej každodennej administrácii, ako je kontrola logov, diskových subsystémov, používateľských účtov, zálohovania, riešenie incidentov prevádzky, riešenie hardvérových

problémov atď. boli v roku 2025 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, doménové radiče, súborový server, tlačové služby, poštový server, intranet, certifikačná autorita, server pre riadenie prístupu Network Policy Server (NPS), servery pre aktualizáciu (WSUS), servery pre správu antivírusovej ochrany, servery s rolou kolektora, zbierajúcich a zasielajúcich bezpečnostné logy z doménových radičov, serverov a pracovných staníc do bezpečnostného monitoringu, servery pre monitoring prevádzky, zálohovanie, dochádzkový server,
- priebežne boli vykonávané bežné administrátorské činnosti zamerané na predchádzanie výpadkov, ako je kontrola logov, diskových subsystémov, kontrola používateľských a počítačových účtov,
- boli aplikované skupinové politiky podľa prevádzkových a bezpečnostných požiadaviek,
- ďalej bolo vykonávané:
  - vytvorenie a zrušenie doménových používateľských účtov, riadené príslušnými formulármi,
  - zálohovanie,
  - riadenie prístupových oprávnení k jednotlivým priečinkom sieťových diskov súborového servera,
  - administrácia používateľských certifikátov, podpisovanie požadovaných webových certifikátov,
  - riešenie hardvérových a softvérových problémov,
  - antivírusová ochrana serverov a pracovných staníc,
  - podpora používateľov interných zamestnancov, externých správcov serverov, externých konzultantov,
  - kontrola a spravovanie pracovných staníc prostredníctvom Microsoft Enterprise Configuration Manager, ktorý bol pravidelne aktualizovaný na vyššiu verziu, aktualizácia operačných systémov serverov a pracovných staníc prostredníctvom Windows Server Update Services,
  - príprava pracovných notebookov na bezpečnú prácu z domu pre vybraných a nových používateľov a spravovanie používateľských certifikátov pre vzdialené pripojenie,
  - prevádzkovanie serverov s rolou kolektora, zasielajúcich bezpečnostné logy na servery bezpečnostného monitoringu, zber logov z doménových radičov, súborového servera, poštového, zálohovacieho, antivírusového servera, Network Policy servera a servera na správu pracovných staníc, certifikačnej autority, doménových pracovných staníc a notebookov, úprava politík a pravidiel logovania.

Podľa bezpečnostných varovaní z NASES, Národného bezpečnostného úradu a vládnej jednotky CSIRT.SK boli priebežne preverované a odstraňované zraniteľnosti systémov.

V roku 2025 bol v doméne uvedený do prevádzky druhý server s rolou kolektora, zasielajúceho bezpečnostné logy z doménových radičov, serverov a pracovných staníc v druhej doméne a boli nakonfigurované potrebné doménové politiky.

Po overení funkčnosti nového dochádzkového servera bol predchádzajúci dochádzkový server v roku 2025 vyradený z prevádzky.

### **Správa domény (Active Directory)**

V roku 2025 boli spravované dve domény - jedna pre interných zamestnancov, druhá pre externých spolupracovníkov.

V rámci úlohy sa vytvárali účty novým zamestnancom, doplnila sa štruktúra Active Directory podľa zmien v organizačnej štruktúre, deaktivovali sa účty zamestnancom, ktorí ukončili pracovný pomer, 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. Vykonávala sa kontrola aktívnych a neaktívnych používateľských účtov a ich aktualizácia.

V priebehu roka bola poskytovaná podpora doménovým používateľom a cez doménové politiky sa riešili prístupové práva používateľských účtov na zdroje v doméne, či už pri vytváraní účtu, preradení 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. S cieľom zvýšiť bezpečnosť boli zavedené pravidlá pre prihlasovanie administrátorov.

V prípade potreby boli implementované doménové politiky podľa požiadaviek útvaru bezpečnosti.

V doméne bola pre pracovné stanice s operačným systémom Windows 11 zavedená automatizovaná správa a pravidelná zmena hesla lokálneho účtu administrátora.

Zavedená bola politika, ktorá definuje používanie USB kľúčov.

V roku 2025 sa nevyskytol žiadny výpadok doménových radičov.

### **Správa operačných systémov Linux**

V priebehu roku 2025 prebiehala potrebná aktualizácia operačných systémov Linux.

Okrem toho:

- boli upravované a pridávané nové zónové konfigurácie na DNS serveroch podľa požiadaviek a potrieb používateľov a boli zrušené už neaktuálne DNS záznamy,
- logy do bezpečnostného monitoringu boli presmerované aj z ďalších systémov,
- inštalovali sa agenti nového bezpečnostného monitoringu na ďalšie servery,
- prebiehala komunikácia s podporou Red Hat pri riešení prevádzkových problémov,
- bol zabezpečovaný monitoring v Konzole 2,
- boli na systémoch pridávané nové účty a odoberané staré podľa potreby,
- prebehol čiastočný audit používateľských účtov - kontrola povolených privilegovaných oprávnení, na základe čoho boli niektoré účty odobraté alebo vytvorené,
- boli povolené e-mailové služby zo serverov, kde to bolo potrebné,

- boli vy publikované nové DNS záznamy do Govnetu,
- boli riešené problémy so zaplňaním miesta na webe DataCentra,
- portál web www.informatizacia.sk bol zmigrovaný do NASES/MIRRI SR, v DataCentre bol webserver vypnutý,
- boli vymenené niektoré servery v RRP,
- antivírusové riešenie pre vonkajšie služby bolo rozšírené kvôli škálovateľnosti a HA dostupnosti, zároveň bolo rozšírené aj jeho testovacie prostredie,
- testovacie prostredie IS RVO bolo zmigrované na nové servery,
- bola realizovaná úprava chybových hlásení v monitoringu pre KTI podľa potreby,
- prebehol upgrade ďalších serverov na podporované verzie OS,
- boli vytvorené nové infraštruktúrne servery pre RPC-DMZ,
- bola zmigrovaná služba SFTP pre IS RVO na nový server, následne boli odstraňované problémy s nekompatibilitou so staršími protokolmi,
- prebehlo havarijné testovanie pre jednotlivé IS,
- bol pripravovaný novší hardvér na prostredie pre VAP a LAN v ZVS.

## **Správa VMware**

V priebehu roku 2025 prebiehali potrebné aktualizácie virtualizačných prostredí vrátane FW ILO rozhraní a BIOS.

Okrem toho boli vykonané aj nasledujúce činnosti:

- vykonal sa audit používateľských účtov - kontrola povolených privilegovaných oprávnení, na základe čoho boli niektoré účty odobraté alebo vytvorené,
- v DataCentre Kopčianska bolo sprevádzkované nové virtualizačné prostredie,
- bolo pripojené diskové pole pre monitoring DK,
- bolo pripojené diskové pole pre DK-RPC-DMZ,
- bolo sprístupnené NTP pre nové siete,
- boli riešené problémy so zálohovaním v ZVS,
- boli vymenené pokazené hardvérové komponenty, vymenené batérie na diskovom poli,
- uskutočnila sa výmena chybného zdroja v BLCHS v ITMS3/ISUF v ZAL,
- vykonal sa upgrade FW diskových polí,
- boli navýšené hodnoty RAM, CPU a diskových priestorov jednotlivých VM, kde si to situácia vyžadovala, prebehla optimalizácia a revízia virtuálnych serverov, odstránenie nepotrebných VM,
- boli vytvorené nové virtuálne servery pre rôzne projekty i potreby DataCentra, ako SIEM, monitoring DC-K, IS TABAK, nahrávanie hovorov, antivírusové riešenie pre GW, RRP, SFTP RVO,
- bol vykonaný upgrade konzoly DataCentra v Bratislave na novú verziu.

## **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 v roku 2025 vykonávali nasledujúce činnosti:

- vytvárali sa pravidelne riadne zálohy databáz a kontrolovali sa logy priebehu zálohovania. Záložovali sa príslušné archívne redology, vytvárali sa mimoriadne zálohy vybraných používateľských objektov a ich obnova,
- priebežne boli inštalované patche pre databázový server a vykonával sa plánovaný reštart databáz,

- bola vykonaná archivácia údajov a pripravené prostredie na 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 operácií a obsah alertlogov,
- bol vykonaný upgrade Weblogic forms aplikačného servera a jeho aplikácií,
- boli inštalované patche Weblogic aplikačného servera a JAVA prostredia,
- bol vykonaný upgrade Enterprise Manager-a a je pravidelne patchovaný. Centralizuje a zefektívňuje monitoring a administráciu databázových serverov a aplikačného servera z jedného rozhrania,
- podľa požiadaviek používateľov bolo modifikované produkčné a testovacie prostredie, bola poskytnutá podpora na používanie aplikačného programového vybavenia účtovného IS, podpora pri spracovaní údajov, boli preverené prístupové práva používateľov podľa ich kompetencií,
- na používateľských notebookoch bol inštalovaný softvér: Oracle databázový klient, softvér na prístup do operačného systému servera, vývojové prostredie PL SQL developer, vývojové prostredie Forms Builder a Reports Builder,
- operatívne bola používateľom databáz poskytovaná technická podpora.

### **Administrácia LAN, WAN a redakčných systémov**

V priebehu roka 2025 boli vykonávané profylaktické práce na bezpečnostných prvkoch ako WAF a firewall v pravidelných intervaloch. Priebežne boli vykonávané konfigurácie pravidiel na týchto bezpečnostných prvkoch podľa požiadaviek.

Na základe požiadaviek systémov prevádzkovaných v DataCentre bola na počítačovej sále rozšírená optická a metalická dátová kabeľáž v potrebnom množstve. Priebežne boli vykonávané nové metalické a optické prepoje podľa požiadaviek jednotlivých správcov systémov.

Na počítačovej sále bola vymenená kabeľáž v jednej stavebnej jednotke (POD), keďže bola prevádzkovaná na starom type kabeľáže, ktorá pre dané rýchlosti už nevyhovovala.

Bol vybudovaný nový rack pre testovacie prostredie RPC so všetkou potrebnou metalickou a optickou kabeľážou a napájaním.

Priebežne počas roka 2025 boli vykonávané konfigurácie prístupových prepínačov podľa požiadaviek jednotlivých odborov pri obmene a presune zamestnancov.

Taktiež boli priebežne vykonávané úpravy databáz PCCE, a to najmä z dôvodu potreby ďalších parametrov pre štatistické spracovanie kontaktného centra a na základe požiadavky supervízora boli upravované štatistické reporty pre agentov kontaktného centra.

V priebehu roka boli vykonávané profylaktické práce (inštalácia Windows updatov, opravných balíčkov samotného kontaktného centra a antivírusového programu) na zabezpečenie plynulého chodu PCCE.

Priebežne boli vykonávané konfiguračné zmeny používateľov telefónov a ich klapiek a konfigurácie agentov KC.

V roku 2025 sa začala postupná výmena a doplnenie prepínačov, ktorá umožní výrazné zvýšenie priepustnosti siete, čím sa zabezpečí vyššia efektívnosť a pripravenosť infraštruktúry na budúce požiadavky.

Taktiež začali prípravné práce na konsolidácii rackov jedného z operátorov, keďže už svojimi parametrami nezohľadňuje súčasné priestorové a manipulačné požiadavky.

V roku 2025 tiež začali prípravné práce na výmenu hlavných SAN prepínačov, ktoré pozostávali z prípravy dokumentácie pre prepojenie, keďže bolo potrebné zosúladiť dokumentáciu od viacerých zúčastnených subjektov.

V rámci rekonštrukcie 4. poschodia boli demontované uskladnené všetky sieťové zariadenia.

Z dôvodu rekonštrukcie fasády bola po návrate pracovníkov L2 podpory natáhaná nová prepojujúca kabeláž v niektorých kanceláriách na 1. poschodí.

### **Správa systémov IPS**

Počas roka 2025 sa na bezpečnostných intrusion prevention zariadeniach v infraštruktúre DataCentra vykonávali rutinné a štandardné činnosti súvisiace s administráciou týchto systémov.

Každodenne bol monitorovaný stav jednotlivých bezpečnostných sond a bola vykonávaná aktualizácia reputačných databáz. Každých 24 hod. boli automatizovane vykonávané aktualizácie bezpečnostných signatúr.

Kontrola udalostí, ktoré boli zaznamenané do centrálnej konzoly a preposielané do bezpečnostného monitoringu, nezistila žiaden úspešný útok na monitorované súčasti infraštruktúry DataCentra, keďže u väčšiny bolo zistené, že ide 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.

### **Správa SIEM riešenia a bezpečnostný monitoring**

V priebehu roka 2025 bola zabezpečovaná prevádzka a rozvoj SIEM riešenia nasadeného v roku 2019. Boli odstraňované nedostatky v zbere udalostí, parsovaní udalostí v existujúcich korelačných pravidlách a taktiež boli vytvorené nové korelačné pravidlá. Na zvýšenie viditeľnosti v infraštruktúre sa pokračovalo v implementácii zberu udalostí z ďalších zariadení, IS a bezpečnostných prvkov. Pokračovali práce na uprade SIEM riešenia.

Od roku 2021 sa používa systém, ktorý slúži na uchovávanie indikátorov kompromitácie (IOC) známej škodlivej aktivity z verejných zdrojov a hlásení od partnerov. Tieto informácie sú automatizovane importované do SIEM, čo umožňuje efektívne vyhľadávanie potenciálnej škodlivej aktivity. Systém tiež podporuje automatizovanú integráciu s bezpečnostnými prvkami na rýchle blokovanie známych hrozieb. V roku 2025 bol tento systém naďalej prevádzkovaný a pravidelne aktualizovaný na základe prijatých upozornení od partnerov, ako aj indikátorov zistených vlastným bezpečnostným monitoringom.

Od roku 2022 sa používa riešenie pre monitorovanie bezpečnosti siete. Projekt súvisí s realizáciou bezpečnostného opatrenia pre oblasť riadenia bezpečnosti sietí a informačných

systémov, ako je uvedené v § 10 písm. l) vyhlášky č. 362/2018 Z. z.: „prostredníctvom systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete“. Primárny cieľ je podpora analýzy podozrivej komunikácie a bezpečnostných incidentov. V roku 2025 bol tento systém rozšírený o ďalší preposielací uzol pre zber dát z ďalších zdrojov. Taktiež boli vykonané konfiguračné zmeny s cieľom obohatiť logy a optimalizovať pravidlá. Systém bol počas celého roka 2025 prevádzkovaný a pravidelne aktualizovaný.

V rámci bezpečnostného monitoringu boli denne kontrolované bezpečnostné udalosti a v prípade podozrenia na bezpečnostný incident bola aktivita analyzovaná. Taktiež bol kontrolovaný výskyt IOC na základe hlásení od CSIRT.SK a SK-CERT. Okrem udalostí zo SIEM riešenia boli vykonané viaceré analýzy na základe žiadostí od útvaru bezpečnosti. V priebehu roka 2025 bolo preverovaných viacero bezpečnostných udalostí a incidentov, avšak nebol potvrdený žiadny prípad narušenia bezpečnosti. Väčšina zachytených udalostí bola typu „false positive“.

### **Prevádzka prostredia na manažment zraniteľností a penetračné testovanie**

Prostredie na manažment zraniteľností a penetračné testovanie je prevádzkované od roku 2020. V priebehu roka 2025 boli vykonávané pravidelné skeny zraniteľností vybraných systémov v infraštruktúre DataCentra a pokračovali práce na rozšírení pravidelného skenovania na ďalšie systémy. Bol vykonaný audit MS AD domény automatizovanými nástrojmi. Boli vykonané externé skeny zraniteľností - penetračné testy nasledovných webových stránok/aplikácií:

- www.datacentrum.sk,
- cpu.datacentrum.sk,
- itms.datacentrum.sk,
- akc.integritydata.sk,
- akcl.integritydata.sk.

### **Správa Lotus Domino serverov**

V roku 2025 sa priebežne vykonávala štandardná údržba Lotus Domino servera, prebiehala administrácia poštových schránok a webových služieb. Poštový server bol upgradovaný na najnovšiu verziu.

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

### **Správa webových a aplikačných služieb servera Lotus Domino**

Web server je nakonfigurovaný vo virtuálnom prostredí, ktoré efektívne využíva systémové zdroje a následne aj úsporu hardvéru. Na serveroch sa aj v roku 2025 priebežne vykonávala štandardná správa a údržba a taktiež administrácia webových služieb. Bolo zavedené dvojfaktorové overenie používateľa pri prihlasovaní sa do webmailu a mobilnej aplikácie HCL Verse.

### **Správa pracovných staníc**

V roku 2025 prebiehala štandardná inštalácia, aktualizácia a administrácia pracovných staníc. Vykonávala sa bežná denná údržba výpočtovej techniky vrátane hardvérových a softvérových

riešení problémov, ktoré sa vyskytli na pracovných staniciach zamestnancov. Priebežne sa vymieňali zastarané zostavy za nové. Ďalej sa podľa potreby nasadzovalo riešenie: dokovacia stanica - notebook (+ SD-WAN), súčasne vyhovujúce aj aktuálnym kritériám pre prácu z domu (HO). Na požadovaných pracovných staniciach bola nainštalovaná najnovšia verzia softvéru, potrebného pre pripojenie cez zjednotený prístupový bod a prihlasovanie do KTI DataCentra.

### **Antivírusová, antispyverová a antispamová ochrana serverov, pracovných staníc a e-mailov**

Antivírusová, antispyverová a antispamová ochrana serverov a pracovných staníc vo vnútornej sieti bola aj v roku 2025 zabezpečovaná prostredníctvom manažovacieho servera. Na všetkých doménových serveroch je nastavená konfigurácia zvýšenej ochrany internetového prehliadača. V prípade zachytenia malvéru v karanténe, následného zalogovania a zaslania reportu administrátorom a útvaru bezpečnosti boli vykonané všetky potrebné kontroly logov, poučenie používateľov a následné opatrenia v záujme zvýšenia bezpečnosti. V roku 2025 nebol infikovaný žiadny server ani pracovná stanica.

Ochrana internetovej a e-mailovej komunikácie bola zabezpečovaná prostredníctvom antivírusového a antispamového riešenia ešte pred vstupom do vnútornej siete. Konfigurácia tohto riešenia sa neustále upravuje podľa aktuálnych potrieb a vyskytujúcich sa nových hrozieb. V roku 2025 boli všetky zariadenia - webové, e-mailové brány a ich management upgrade na aktuálne verzie. Prebiehalo tiež pravidelné dohľadávanie internetovej komunikácie v rámci bezpečnostných incidentov. Na vnútornom poštovom serveri bolo prevádzkované ďalšie antimalvérové riešenie. Antivírusové a antispamové servery boli pravidelne aktualizované a boli upravené nastavenia politik a pravidiel podľa potrieb a požiadaviek. Aktualizované boli blacklisty aj e-mailové filtre. Bola vykonávaná pravidelná kontrola karantén na oboch riešeniach e-mailovej antimalvérovej ochrany. Ak boli napriek zavedeným pravidlám zachytené legitímne e-maily označené ako spam, boli ďalej preposielané používateľom. Nadalej sa pravidelne kontrolovala fronta došlej a odchádzajúcej pošty. Na podnet bezpečnostných varovaní z NASES boli došlé e-maily a karantény preverované na prítomnosť podozrivých alebo infikovaných e-mailov a boli k tomu prijaté špeciálne bezpečnostné opatrenia. Ostatné podozrivé e-maily, na ktoré upozornil NASES, skončili zachytené v karanténe alebo neboli adresované do e-mailových schránok DataCentra. Taktiež boli pre potreby DataCentra povolené niektoré potrebné domény na proxy vo whitelistoch, či z bezpečnostných dôvodov boli iné zablokované. Na e-mailové riešenie sa pripojilo aj ďalšie prostredie RPC v ZVS. Bolo sprevádzkované zasielanie notifikácií z monitoringu v RPC. Zaviedlo sa bezpečné riešenie pre posielanie MS Teams pozvánok z DataCentra. V roku 2025 bola vykonaná aj kontrola pravidiel poštového systému. Prešlo sa na nový licenčný model pri webmailových bránach aj s manažmentom. Pri problémoch s upgradom z dôvodu známej chyby v kóde od výrobcu bol tento riešený v spolupráci s podporou. Tiež sa riešili problémy s posielaním e-mailov na gov.sk. Kontrolovali sa a prípadne urobili úpravy mailových TXT záznamov, aby spĺňali najnovšie bezpečnostné požiadavky.

Väčšina v karanténe zachytených e-mailov bolo typu spam.

### **Správa čipových kariet a USB tokenov IS ŠP**

V roku 2025 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. V uplynulom roku prebiehala výmena zastaraných čipových kariet za USB tokeny. Aktuálne prebiehajú výmeny prvých USB čipových tokenov za najnovšie verzie a prechádzame na vyššie podporované modely.

## **Zabezpečenie činnosti záložného pracoviska**

V roku 2025 prevádzka ZVS zabezpečovala správu, monitoring, údržbu a činnosť systémov, zariadení a aplikácií SAP, QP0, USP, BSP, ESO, RIS, KTI, ARDAL, Reuters.

Pokračovala rekonštrukcia infraštruktúry a vybudovanie vysunutého pracoviska ARDAL.

Tiež bola inštalovaná nová technika v novej sále, kde prebieha príprava konektivity a príprava migrácie systémov.

Priebežne sa v ZVS realizovali aktualizácie softvéru, inštalácie nového hardvéru a bežné servisné zásahy. 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. V starej sále bola vymenená klimatizačná technika za novú.

O všetkých zmenách a udalostiach bol vykonaný záznam.

## **Správa Service Managera**

V Service Manager-i boli vykonávané bežné administrátorské činnosti ako správa používateľských účtov, pracovných skupín a služieb, správa konfiguračnej databázy a väzieb na služby, nastavovanie oprávnení, monitoring dostupnosti, monitoring integrácií, riešenie problémov a požiadaviek používateľov, hromadné aktualizácie, ad hoc exporty podľa požiadaviek, nové notifikácie atď.

Boli definované nové globálne pohľady podľa požiadaviek používateľov.

Vykonala sa konsolidácia pracovných skupín, boli deaktivované skupiny, ktoré patrili pod už nepodporované služby, následne sa vykonal audit riešiteľov.

Na základe žiadosti vlastníkov procesov boli vytvorené neštandardné reporty z tabuľky „activity“.

Začala sa analýza na zavedenie príkazov na prácu. Vzhľadom na zložitosť problematiky, ako aj na plánovaný prechod Service Manager-a na vyššiu verziu, sa zavedenie procesu odkladá na obdobie, keď bude aplikácia zmigrovaná na novú verziu.

V rámci starostlivosti o konfiguračnú databázu boli vykonané audity vybraných informačných systémov (KTI, SM) a zaviedli sa položky informačného systému pre vysledovateľnosť tabakových výrobkov.

Do produkčnej prevádzky bola zavedená nová funkcionálna na výmaz klientskych aj riešiteľských účtov, zablokovaných dlhšie ako 10 rokov (požiadavka GDPR). Kvôli odstráneniu účtov bolo potrebné vyriešiť aj odstránenie naviazaných záznamov, napr. interakcie, incidenty atď.

## **Optimalizácia a upgrade Service Manager-a**

V septembri 2025 sa začala príprava na upgrade Service Manager-a. Bola uskutočnená analýza, návrh a implementácia optimalizácie a upgradu Service Manager-a v prostredí DataCentra. Optimalizácia sa týkala nielen samotného prostredia a upgradu SM, ale aj procesov manažmentu zmien, konfiguračného manažmentu, incident manažmentu a interakcií, SLM

manažmentu, manažmentu bezpečnostných incidentov integrácií externých systémov vrátane antivírusovej brány, formulára pre neregistrovaných používateľov a iné. V súčasnosti je k dispozícii testovacie prostredie. V ďalšom období budú práce pokračovať na účely nasadenia nových zmien do produkcie.

Service Manager bol v roku 2025 nedostupný mimo prevádzkovú dobu poskytovania služby len v rámci pravidelnej profylaktiky.

### **Správa produktov SAP**

Plnenie úlohy v roku 2025 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 v roku 2025 prebiehalo v cykloch, ktoré sa opakovali každé štyri týždne. Počas víkendov sa robili plné zálohy pre 90 serverov a cez pracovný týždeň sa robili inkrementálne zálohy pre 9 serverov. Zároveň sa vykonáva archivačná záloha 1x ročne. Okrem toho sa ešte podľa potreby, resp. požiadavky vlastníka systému, robili mimoriadne zálohy a obnovy požadovaných dát.

V uplynulom období bol aktualizovaný zálohovací softvér na vyššiu verziu.

### **Ostatné činnosti**

V roku 2025 bol v prostredí KTI prevádzkovaný nástroj na centralizovanú správu privilegovaných používateľských účtov a bol prevádzkovaný systém pre podporu prevádzky informačných technológií, v rámci ktorého boli patchované operačné systémy aj aplikačný softvér.

### **IS SEMP**

V roku 2025 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.

Vykonávala sa úprava existujúcich a vytvorenie nových reportov na základe požiadaviek Protimonopolného úradu Slovenskej republiky. Rovnako sa realizovala aj úprava ďalšej funkčnosti IS SEMP (v nastavených výpočtoch a kontrolách).

Boli zabezpečované opatrenia na základe výstupov z monitoringu IS SEMP, najmä riešenie nedostatku diskového priestoru.

### **Reporting**

V roku 2025 bol realizovaný upgrade reportingového riešenia DataCentra na novšiu verziu. Pre realizáciu upgradu bolo pripravené nové prostredie so zabezpečeným licencovaním SAP produktov pre nové verzie komponentov. Súčasťou upgradu bola aj migrácia používateľov a oprávnení z existujúceho reportingu do nového. Zároveň sa migrovali aj samotné reporty. Migrácia bola vykonaná najskôr v testovacom prostredí, kde bola otestovaná funkčnosť reportov.

V rámci reportingu boli v roku 2025 realizované nasledovné aktivity:

- nový report hlásení DKS pre CPU do ročenky,
- nový report pre CPU „Počet používateľov v jednotlivých IS“ - komunikácia so zadávateľom, úpravy v zobrazovanom IS v reporte (spojenie alebo rozdelenie vybraných),
- nový report incidentov pre ITMS, ak aspoň raz vykonal nejakú akciu niektorý zo zafinovaných riešiteľov,
- nový report uzatvorených hlásení pre CPU podľa riešiteľov a dĺžky riešenia,
- kontrola ELT jobov a publikácií, nový prehľad incidentov podľa riešiteľov pre CPU.

### **Centrálna evidencia majetku (CEM) a Centrálny register pohľadávok štátu (CRPŠ)**

V rámci prevádzky týchto systémov boli v uplynulom roku, okrem štandardných prevádzkových činností, realizované nasledovné aktivity:

- podpora nábehu a migrácie údajov do CES
  - CEM - príprava a export dát pre organizácie migrujúce do CES,
  - Podpora CES pri exporte kmeňových údajov obchodných partnerov z CEM,
  - Podpora CES RE-FX tímu,
- zabezpečenie pripojenia nových správcov cez B2B, metodická podpora a nastavenie B2B používateľa, testovanie B2B a kontrola dát,
- príprava a export dát z CEM pre organizácie migrujúce do CES.

V roku 2025 DataCentrum poskytovalo podporu externým dodávateľom a spolupracovalo pri konfigurácii serverov a riešilo požiadavku na rozšírenie diskových priestorov.

### **Prevádzka internetových domén**

Priebežne bola zabezpečovaná registrácia nových a prevádzka registrovaných .sk, .eu, .cloud, .info, .net a .org domén. Pribudlo 5 nových registrovaných domén, domény mfsr.sk a kverkom.sk boli na žiadosť preregistrované pod registrátora DataCentrum. V správe DataCentra je aktuálne 112 domén. V roku 2025 ukončilo DataCentrum prevod .eu, .info .net a \*.org domén od registrátora Webglobe do Forpsi (INTERNET CZ) z dôvodu ceny. Správa domén je tak jednoduchšia, domény sú registrované len u dvoch registrátorov. Zrealizovali sa aj aktualizácie publikovaných údajov na základe požiadavky.

### **Návrh a implementácia jednotného AV riešenia**

V uplynulom období bolo vytvorené univerzálne riešenie antivírusovej kontroly súborov. V rámci implementácie bol vytvorený systém, ktorý poskytuje rozhranie pre ostatné informačné systémy (klientov) pomocou REST/SOAP API, kde je možné nahráť súbory, na ktorých má byť vykonaná analýza obsahu súboru s cieľom preskúmať a identifikovať

prítomnosť škodlivého kódu. V priebehu roka 2025 bolo do tohto systému integrovaných 17 klientskych IS. Z dôvodu plánovaného rozširovania zapojených IS a zabezpečenia ich spoľahlivej prevádzky bola navrhnutá škálovateľná architektúra a boli začaté práce na jej nasadení.

## **Rezortný Privátny Cloud (RPC)**

V roku 2025 bol v RPC projekte realizovaný kompletný návrh redizajnu realizácie zálohovania (s využitím obidvoch vysúťážených zálohovacích softvérových platforiem), ktorý spĺňa všetky požiadavky na zálohovanie infraštruktúrnych častí RPC, ako aj požiadavky na zálohovanie jednotlivých IS v RPC z pohľadu bezpečnosti, nezávislosti a izolovanosti zálohovania každého IS v RPC.

V RPC sa začalo s implementáciou monitoringu všetkých infraštruktúrnych služieb ponúkaných v RPC.

V rámci realizácie prepojení na lokalitách DC-C a DC-K boli zrealizované nasledovné práce:

- Pripojenie lokality DC-K do privátnych sietí Finnet a Govnet a pripojenie do siete Orange.
- Boli doladené a otestované VPN pripojenia.
- Bolo zrealizované poskytovanie infraštruktúrnych služieb: HTTP(S) PROXY, SMTP GW, DNS, NTP v aktívnej podobe na oboch lokalitách.
- Bola implementovaná integrácia RPC LDAP na RRP v KTI vo všetkých troch lokalitách RPC na účely manažmentu privilegovaných používateľov do portálovej časti RPC.
- V rámci zabezpečenia prepojenia lokalít DC-C a DC-K v móde Active-Active boli zrealizované viacnásobné globálne failover testy na rôznych úrovniach sieťových prvkov.
- Z lokality DC-K do lokality DC-C bol zrealizovaný simulovaný workload a fail over test.

## **Cenový informačný systém (CIS)**

- V rámci projektu CIS bol v 1. štvrtroku 2025 vysúťážený VO dodávateľ pre frontend CIS.
- Na základe požiadaviek od dodávateľov pre frontend a backend bolo vytvorené testovacie, predprodukčné a produkčné prostredie s požadovanými parametrami a OS, súčasne boli nakonfigurované siete a zrealizované potrebné bezpečnostné sieťové konfigurácie na FW.
- V rámci backend časti CIS bolo pre obchodné reťazce vy publikované API rozhranie. API rozhranie je zabezpečené prostredníctvom web-aplikačného firewallu (WAF). Konzumenti sa pripájajú na API rozhranie zabezpečené WAF na základe povolených IP adries definovaných v Infraštruktúrnej matici prepojenia. Pre potreby pripojenia bolo zrealizované prihlasovanie voči WAF serveru certifikátom, ktorý podpísala CA v DataCentre.
- Pre obchodné reťazce bolo pripravené zabezpečené úložisko na nahrávanie obrázkov jednotlivých tovarov.
- Na backend časti CIS bolo pre potreby administrátora systému (biznis vlastník systému) pripravené grafické rozhranie.

- Jednotlivé prostredia Frontendu boli vypublikované podľa požiadaviek biznis vlastníka do privátnej alebo verejnej siete.
- V rámci pilotnej prevádzky v júli boli zrealizované penetračné a performance testy a následne boli upravované parametre niektorých VM.
- Bolo zrealizované zálohovanie CIS.

## DCOM

V súvislosti s prípravou migrácie IS DCOM do RPC bolo v roku 2025 zrealizovaných viacero analytických, technických a sieťových pracovných stretnutí s DEUS a dodávateľom DCOM a následne bola pripomenovaná pracovná verzia rozsiahleho dokumentu Migrácia IS DCOM do RPC.

## TOSCA

Pre potreby testovania CES bol vytvorený v RPC tenant Tosca. Prostredie a sieťové konfigurácie a zálohovanie boli zrealizované podľa požiadaviek zadávateľa tak, aby bol umiestnený v tom istom PODE a navrhnutom sieťovom segmente, aby pri testoch nebola v žiadnom prípade ovplyvnená prevádzka CES, ako aj iných IS v RPC.

## SIEM CSIRT pre MF SR

Pre potreby SIEM CSIRT MF SR bol v RPC vytvorený tenant CSIRT - Prostredie. Sieťové konfigurácie boli v prvej fáze zrealizované podľa požiadaviek zadávateľa.

<b>404</b>	<b>Prevádzkovanie Registra ponúkaného majetku štátu</b>
------------	---

V rámci úlohy boli v roku 2025 zabezpečené:

- plánované odstávky a bezproblémový nábeh po odstávkach,
- bežné administrátorské činnosti, ako sú aktualizácie, kontrola logov a riešenie prevádzkových problémov,
- prevádzka bezpečnostných systémov a zariadení, ktoré chránia a zároveň kontrolujú prístupy k registru a jeho službám,
- pravidelné zálohovanie servera, jeho operačného systému a súborového systému a tiež monitoring a dohľad servera i aplikácie,
- riešenie problémov v databáze, resp. v administračnom rozhraní.

Na základe hlásení na CPU boli riešené požiadavky používateľov všetkých častí aplikácie (Osobitné ponukové konania, Ponukové konania, Elektronické aukcie, Nájom, Nevymedzený hnutelný majetok) bolo v roku 2025 prijatých 183 hlásení, vyriešených 173 hlásení, 4 boli zrušené používateľom, 4 boli duplicitné, 1 nevyriešené – používateľa nebolo možné kontaktovať, 1 zamietnuté . Bol vytvorený prístup do aplikácie pre 5 nových správcov, pre 29 zamestnancov existujúceho správcu, 9 zamestnancom bol prístup deaktivovaný a 1 bol zmenený typ používateľa z návštevníka na zamestnanca. Údaje 1 správcu boli zmenené.

V súlade s požiadavkami GDPR boli priebežne vymazávané osobné údaje zamestnancov správcov majetku a záujemcov o majetok štátu.

Dňa 5. februára 2025 bol v NR SR schválený vládny návrh zákona o zmene a doplnení niektorých zákonov v súvislosti so zmenami vyvolanými Stavebným zákonom (tlač 701), súčasťou ktorého je aj novela zákona NR SR č. 278/1993 Z. z. o správe majetku štátu v znení neskorších predpisov (ďalej len „novela zákona“). V súvislosti s prijatou novelou zákona boli k 1. aprílu 2025 upravené príslušné formuláre Registra ponúkaného majetku štátu.

Okrem toho bolo v roku 2025 v registri vykonaných niekoľko menších úprav na základe požiadaviek vlastníka a používateľov.

<b>406</b>	<b>Prevádzka dátovej sály MF SR</b>
------------	-------------------------------------

V priebehu roka 2025 bola zabezpečená nepretržitá prevádzka dátovej sály a boli garantované poskytované IT služby. V rámci prevádzkovej podpory rezortu MF SR sa vykonávali komplexné činnosti v prospech používateľov informačných systémov. Požiadavky a incidenty od zamestnancov, súvisiace s IT prevádzkou, boli zaznamenané a neodkladne riešené.

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

Okrem iného boli v požadovaných parametroch zabezpečované nasledovné služby:

- dostupnosť služieb AD, CA, DHCP, DNS, LAN, SAN, VMware virtualizácia,
- dostupnosť hardvérovej infraštruktúry, zálohovania,
- dostupnosť elektronickej pošty,
- dostupnosť VPN služieb pre vzdialený prístup, videokonferencií,
- dostupnosť tlačového servera, dátového úložiska, prístup do internetu,
- import dát zo SAP-u a následné zavedenie personálnych zmien,
- dostupnosť dochádzkového systému.

## **O365**

V roku 2025 pokračovala integrácia pracovných staníc MF SR do Microsoft tenantu formou hybrid AD join. Počas tejto integrácie boli navrhnuté nastavenia APP protection policies pre zariadenia prístupujúce do tenantu MF SR.

Upravené boli nastavenia Azure AD, Exchange Online, SharePoint, prístupu k dátam, auditovania a logovania, mobile device management-u.

## **Pomoc seniorom**

Počas roku 2025 bola technicky zabezpečovaná správa informačného systému na vyplácanie pomoci seniorom. Aktivity pozostávali zo spracovávaní dát o očkovaní seniorov z NCZI, detekcie a oprave chybných dát z NCZI, vytvorenia očkovanej osoby, vyhodnotenia zákonných podmienok pre vyplatenie pomoci, vytvorenia dátovej dávky pre Slovenskú poštu, a.s., na tlač poukazov, spracovávaní dávky z pošty o vyplatených/nevyplatených poukazoch, aktualizácii

údajov o senioroch a opätovnom odosielaní nevyplatených poukazov, dohľadávaní adries v RFO a následnej aktualizácii dát u seniorov, spracovaní a vyplácaní poukazov v dedičských konaniach.

### **LAN – Obnova core časti LAN siete na dátovej sále**

Koncom roka 2025 bola zahájená obmena centrálnych prvkov LAN infraštruktúry na dátovej sále, konkrétne centrálnych firewallov, centrálnych switchov, DMZ firewallov a DMZ switchov. Súčasťou úlohy je aj konfigurácia týchto zariadení s cieľom zabezpečiť georedundanciu infraštruktúry v prípade výpadku jednej dátovej sály. Kým doteraz bola prevádzkovaná len jedna dátová sála, po dokončení úlohy budú k dispozícii dve geograficky redundantné dátové sály. Nové zariadenia prešli úvodnou konfiguráciou, aktualizáciou softvéru, boli zapojené oddelene od existujúcej infraštruktúry a v súčasnosti prebieha migrácia konfigurácie.

### **Aktualizácia virtualizačnej platformy**

V roku 2025 bola priebežne aktualizovaná serverová farma novej generácie, na ktorej je prevádzkovaná aktuálna verzia virtualizačnej platformy VMWare.

### **Rozšírenie kapacity diskového poľa**

Kapacita nového diskového poľa bola v priebehu roka postupne dopĺňaná tak, aby sa vyrovnala staršiemu diskovému poľu. Taktiež boli migrované dáta z diskového poľa, ktorého životný cyklus bol už výrobcom ukončený.

Požiadavky dodávateľov a konfiguračné práce na informačných systémoch MF SR boli vykonávané podľa požiadaviek a po schválení útvaru informačnej a kybernetickej bezpečnosti. Na dennej báze boli vykonávané zálohy s denným reportom a sú k nahliadnutiu v zálohovacom systéme Veeam. Požiadavky na obnovu zmazaných súborov alebo e-mailu boli realizované na týždennej báze.

<b>407</b>	<b>Informačný systém účtovníctva fondov (ISUF)</b>
------------	--

V roku 2025 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.

DataCentrum aj v roku 2025 koordinovalo práce v procese zabezpečenia pripájania nových koncových používateľov do KTI v spolupráci s CPU pri realizácii pripojenia. Na základe doručených formulárov na pridelenie/odobratie oprávnení zabezpečovalo DataCentrum aj zakladanie, zmeny a výmazy používateľských účtov.

Prostredníctvom CPU bolo v roku 2025 zaevidovaných 182 používateľov a zaznamenaných 510 hlásení, ktoré boli následne vyriešené a uzatvorené jednotlivými pracovnými skupinami riešiteľov.

Pravidelne na mesačnej báze bola spracovávaná správa z HP Service Manager-a o vyhodnotení riešenia incidentov a problémov ISUF, ktorá bola poskytovaná aj vlastníčkovi informačného systému - MF SR.

Dostupnosť serverov ISUF (ostrého, školiaceho a testovacieho) bola zabezpečená bez zásadnejších problémov a bol prevádzkovaný aj funkčný záložný systém ISUF, čo predstavuje splnenie požiadavky MF SR.

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

V rámci zabezpečenia prevádzky a funkčnosti informačného systému bol zabezpečovaný súlad bezpečnostnej politiky a analýzy rizík s GDPR a zákona o kybernetickej bezpečnosti.

Všetky úlohy vyplývajúce z kontraktu na rok 2025 boli splnené a vykonané v súlade s identifikačným listom úlohy a schváleným projektovým zámerom ISUF.

Vyhodnotenie hodnotiacich kritérií:

Hodnotiace kritérium	2025	%	splnené
97 % vyriešených do 24 hod.	495	97,01	A
Menej ako 3 % nad 24 hod.	15	2,99	A

#### 408 Ekonomické informačné systémy (EIS) a systémy VÚC

V roku 2025 DataCentrum zabezpečovalo štandardné prevádzkové služby pre produkčné, testovacie, vývojové a prípadne aj záložné prostredia nasledovných EIS (Ekonomických informačných systémov) a VÚC systémov:

MZP/100	Envirofond
MZP/100	OÚŽP (Obvodný úrad životného prostredia)
TDM/100	TDMS (GDPR, Test Data Migration Server)
ESO/001	Štátny dlh
ESO/001	Všeobecná pokladničná správa
B1P/001	PPA - Pôdohospodárska platobná agentúra
BUT/BUD	NBÚ - Národný bezpečnostný úrad (len vývojové a testovacie prostredia)
JEP, JAP, JPP, JJP, JBP, BJP	CKS - Centrálny konsolidačný systém
BSP, BBP, JVP	BBSK - Banskobystrický samosprávny kraj
MKPP	Multi-klientsky platobný portál pre VÚC

Okrem vyššie spomenutých systémov stále prebieha údržba nižšie uvedených systémov pre organizácie, ktoré boli premigrované do nového EIS systému CES.

SRP/100	Ministerstvo spravodlivosti SR (vrátane SCP a SPP)
SRP/100	Kancelária Najvyššieho súdu SR (vrátane SCP a SPP)
MZP/100	Ministerstvo životného prostredia SR
PE3/100	Ministerstvo hospodárstva SR (vrátane EPP a ECP)
PE3/200	Ministerstvo školstva, výskumu, vývoja a mládeže SR
PE3/200	APVV - Agentúra na podporu výskumu a vývoja
PE3/200	ŠIOV - Štátny inštitút odborného vzdelávania
PE3/200	8 ÚO RÚŠS - Účtovné okruhy Regionálny úrad školskej správy
PE3/300	Ministerstvo zahraničných vecí a európskych záležitostí SR
PE3/300	SAMRS - Slovenská agentúra pre medzinárodnú rozvojovú spoluprácu
PE3/300	SÚZA - Správa účelových zariadení
EPP	Portál - MZVEZ SR
PHP/100	Ministerstvo pôdohospodárstva a rozvoja vidieka SR
PHP/100	Pôdohospodárska platobná agentúra
PHP/400	Úrad vlády SR
PHP/600	Kancelária Národnej rady SR
ESO/001	MIRRI SR
ESO/001	Najvyšší kontrolný úrad SR
ESO/001	MF SR
ESO/001	Úrad jadrového dozoru SR
ESO/001	Vzdelávacie a doškoloňovacie zariadenie VS - Financie Tatranská Lomnica
ESO/002	Úrad pre normalizáciu, metrológiu a skúšobníctvo SR
PHP/500	ŠÚKL - Štátny ústav pre kontrolu liečiv
MDP/100	Slovakia Travel
MDP/100	MD SR
HRP/100	Správa štátnych hmotných rezerv SR (vrátane HCP)

Okrem spomínaných systémov bola zabezpečovaná systémová podpora pre SolMan, VPS reporting a relevantné SAP PI systémy. Ďalej okrem štandardných prevádzkových služieb bola zo strany DataCentra poskytovaná súčinnosť pri implementácii zmien, ich prvotnom testovaní, ako aj ich samotné nasadzovanie v rámci testovacích a produkčných systémov. Taktiež bola zabezpečovaná súčinnosť pri migrácii klientov zo súčasných EIS/NES systémov do systému CES.

Priebežne boli zo strany DataCentra zabezpečované činnosti spojené so správou, údržbou a vytváraním prístupov pre existujúcich a nových používateľov EIS a VÚC systémov na prístupovej platforme KTI. Taktiež boli oddelením CPU zabezpečované služby spojené s nahlasovaním požiadaviek a problémov koncových používateľov od ich evidencie, postúpenia na príslušné riešiteľské skupiny, monitoringu ich riešenia v nasledovných počtoch hlásení v jednotlivých systémoch:

	2025	2025	2025	2025	2025	2025	2025	2025	2025	2025	2025	2025	Spolu
	1	2	3	4	5	6	7	8	9	10	11	12	
EIS SAP-ESO				2				2	3	2			9
EIS SAP-MD SR				1					1				2
EIS SAP-MH SR					1								1
MKPP	53	53	41	52	42	52	41	75	108	74	66	87	744
<b>Spolu</b>	53	53	41	55	43	52	41	77	112	76	66	87	756

V roku 2025 nebola na žiadnom z uvedených systémov zaregistrovaná neplánovaná nedostupnosť v pracovných dňoch v čase od 7.00 hod. do 19.00 hod. Nedostupnosť v iných časoch bola vopred komunikovaná a bola len v prípade plánovaných odstávok spojených s update a upgrade systémov a aplikácií.

Okrem vyššie uvedených štandardných činností bolo v roku 2025 zabezpečené aj nasledovné:

- Podpora a súčinnosť pri upgrade všetkých Unix systémov na najvyššiu verziu,
- upgrade OS na Linux aplikačných serveroch, patchovanie OS,
- upgrade SAP Kernel,
- SAP SOLMAN patchovanie,
- implementácia SAP Security Notes,
- podpora a súčinnosť pri konfigurovaní a príprave infraštruktúry pre nové systémy CES,
- podpora a súčinnosť pri konfigurovaní a príprave infraštruktúry CES ZVS,
- prípravné činnosti a POC pre migráciu systémov z OS Unix na Linux.

<b>409</b>	<b>Riešenie požiadaviek a hlásení pre zamestnancov MF SR</b>
------------	--

V roku 2025 boli v súčinnosti s odborom informačných technológií pripravované technické podklady potrebné na začatie verejného obstarávania na hardvérové a softvérové 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.

V rámci prevádzkovej podpory pre výpočtovú techniku a informačné systémy boli zaznamenávané požiadavky a incidenty od zamestnancov aj dodávateľov MF SR, ktoré boli nahlásované e-mailom na helpdesk@mfsr.sk (2 013 správ), cez MF SR SCSM systém (3 151 požiadaviek) a tiež telefonicky alebo e-mailom na CPU DataCentra (1 020) 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. Zamestnancom pracujúcim v režime Home office, bola poskytovaná identická podpora s využitím technických prostriedkov pre vzdialený prístup.

Pri vyradovaní zastaranej alebo nefunkčnej techniky bolo vyradených 5 tlačiarň. Neboli nasadené žiadne nové tlačiarne. 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 roku 2025 bolo v rámci prípravy výpočtovej techniky pre zamestnancov pripravených 169 pracovných staníc pre nových zamestnancov MF SR a zamestnancom, ktorí ukončili pracovný pomer, bolo odobraných 126 pracovných staníc. Boli realizované konfiguračné a inštaláčnne práce na novej výpočtovej technike, tlačiarňach a periférnych zariadeniach, aby spĺňali požiadavky zapojenia do počítačovej siete LAN. Pri výmene či obnove techniky boli doladované automatizačné procesy ktoré dopomohli k zníženiu časového prestoja pri odobratí starej techniky a výdaji novej.

Priebežne bolo reinštalovaných 112 pracovných staníc. Reinštalácia lokálnych pracovných staníc bola automatizovaná pomocou systémových nástrojov SCCM2022 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 softvérové vybavenie na MF SR. Pred nasadením image súborov do prevádzky boli všetky verzie otestované. Pracovné stanice na MF SR boli centrálné spravované a pravidelne sa na nich inštalovali bezpečnostné záplaty pre operačný systém, programové vybavenie a udržiavala sa aktuálna antivírusová databáza. Centrálné boli definované bezpečnostné politiky na zabezpečenie vyššej bezpečnosti v súlade s bezpečnostnými odporúčaniami. Počas roka 2025 pokračoval výdaj výpočtovej techniky na platforme Windows 11 (aktuálne na 924 staniciach); 200 notebookov bolo vymenených za nové.

Pre potreby konferenčných a video konferenčných hovorov sa v roku 2025 pokračovalo v používaní prostredia MS Teams.

Evidencia a dokumentácia prevádzkových zásahov je evidovaná v elektronickej a papierovej forme (zakladajú sa do zakladača). Požiadavky sa evidujú elektronicky do lokálneho systému SCSM (System Center Service Manager) prevádzkovaného na MF SR. Prístup do helpdesk systému SCSM majú aj 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.

Incidenty sa nahlásujú 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.

Pri zabezpečovaní technologickej platformy a používateľskej podpory boli realizované aj školenia zamestnancov MF SR o obsahu interného riadiaceho aktu, o prevádzke a bezpečnosti LAN, ktoré sa uskutočňujú 1 - 2x za mesiac, prípadne podľa požiadaviek MF SR. Termíny školení sa určovali na podnet osobného úradu. V reakcii na zvýšený počet pracujúcich z domu boli vytvorené príručky a manuály na rýchle zaškolenie zamestnancov. Aj vďaka proaktívnemu prístupu sa v maximálnej miere zabezpečoval pracovný komfort pre všetkých zamestnancov.

<b>410</b>	<b>Systém vysledovateľnosti tabakových výrobkov</b>
------------	---

V roku 2025 bol Systém vysledovateľnosti tabakových výrobkov prevádzkovaný v režime 24/7/365 s dostupnosťou na úrovni 100 % počas celého roka.

Počet registrovaných hospodárskych subjektov bol 13 129, počet registrovaných prevádzok hospodárskych subjektov bol 24 501. Celkový počet registrovaných používateľov predstavoval 12 394.

Systémom pre vytváranie a vydávanie jedinečných identifikátorov na účely systému vysledovateľnosti tabakových výrobkov bolo v priebehu uplynulého roka vydaných celkom 359 909 934 jedinečných identifikátorov (jedinečné identifikátory jednotkového balenia a jedinečné identifikátory agregovaného balenia).

Počet interakcií s používateľmi za uplynulý rok bol na úrovni 16 606. Používatelia vo vysokej miere využívali zverejnené FAQ, ktoré boli neustále dopĺňané v zmysle postupov „Best practice“. Aj z tohto dôvodu počet jednotlivých nových požiadaviek zo strany hospodárskych subjektov a iných zúčastnených subjektov v porovnaní s predchádzajúcim rokom mierne klesol.

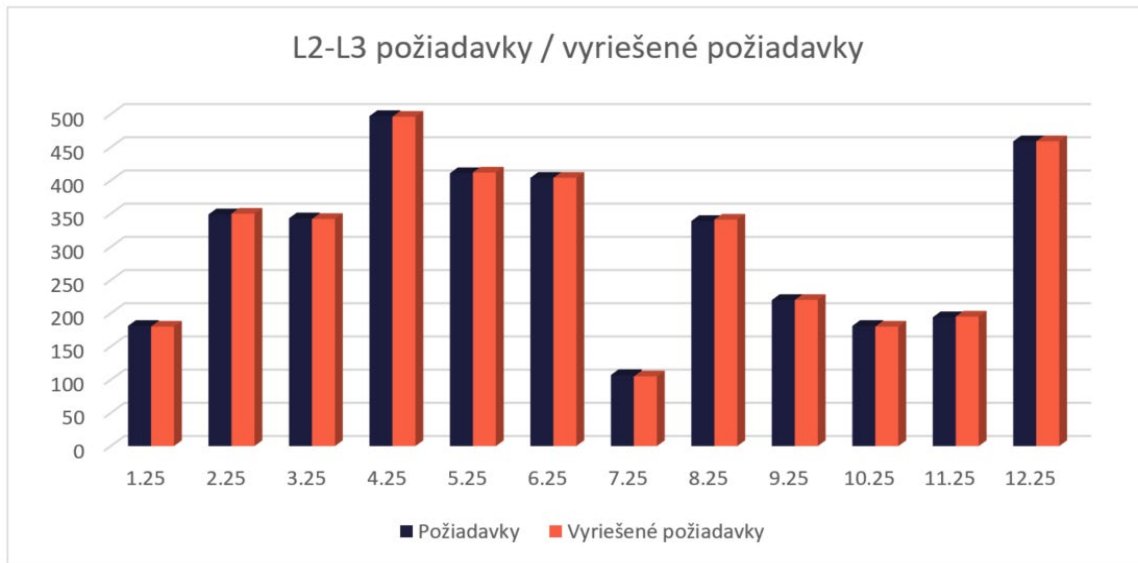
Na vyššie úrovne podpory bolo eskalovaných celkom 3 685 interakcií.

Obdobie	1	2	3	4	5	6	7	8	9	10	11	12	SPOLU
Úroveň L1	762	1 501	1 463	2 237	2 101	1 520	1 120	1 618	801	878	893	1 610	<b>16 606</b>
Úroveň L2/L3	181	349	343	497	411	404	107	339	220	181	194	459	<b>3 685</b>

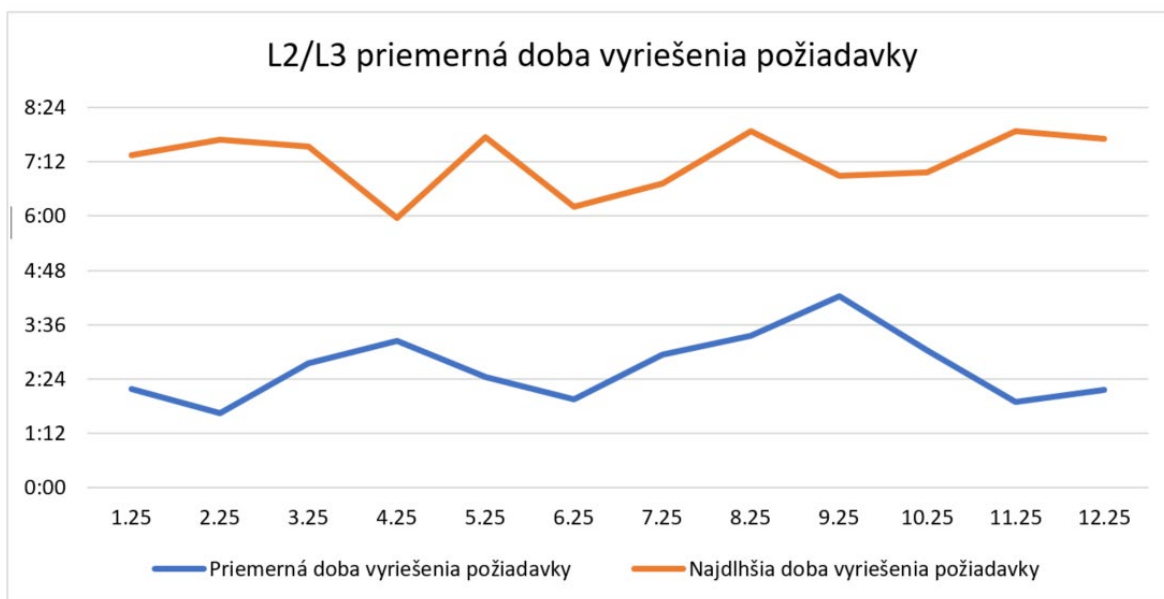
Z požiadaviek eskalovaných na podporu L2/L3 boli následne vytvorené a registrované hlásenia a sledované ich riešenie počas celého hodnoteného obdobia.

Obdobie	1	2	3	4	5	6	7	8	9	10	11	12	SPOLU
Hlásenia	181	349	343	497	411	404	107	339	220	181	194	459	<b>3 685</b>
Vyriešené	180	350	342	496	412	404	105	341	220	180	195	459	<b>3 684</b>

Úspešnosť vyriešenia registrovaných hlásení postúpených na L2/L3 úroveň podpory bola za rok 2025 na úrovni 99,94 %.



Doba vyriešenia všetkých požiadaviek eskalovaných na L2/L3 podporu bola v sledovanom období roku 2025 konzistentne pod úrovňou ôsmich hodín. Priemerné hodnoty za jednotlivé mesiace sú uvedené v grafe nižšie.



Priemerná doba vyriešenia požiadavky za celé sledované obdobie roku 2025 bola na úrovni 02:39 hod., priemerná najdlhšia doba vyriešenia požiadavky za celé sledované obdobie roku 2025 bola na úrovni 07:12 hod.

V roku 2025 bolo realizované množstvo aktualizácií, zmien a vylepšení v rámci jednotlivých modulov a častí systému.

Na základe interných kontrol vykonaných Českým dozorným orgánom bola predložená formálna požiadavka na zavedenie automatizovaného kontrolného mechanizmu v procese generovania jedinečných identifikátorov. Cieľom tohto kontrolného mechanizmu je zabrániť

objednávaníu identifikátorov určených pre iné ako domáce trhy v rámci Európskej únie, pričom systém bude naďalej umožňovať generovanie identifikátorov pre trhy mimo Európskej únie.

V roku 2025 bolo navrhnuté technické riešenie potrebné na implementáciu tohto automatizovaného kontrolného mechanizmu. Po schválení je implementácia tohto vylepšenia plánovaná na nasadenie v roku 2026.

V sledovanom období taktiež prebehla migrácia systému TTTSK na novú serverovú platformu. V rámci tejto migrácie bolo navrhnuté, implementované a otestované plne automatizované riešenie pre preklopenie do záložného dátového centra, ktoré zabezpečuje kontinuitu služieb bez potreby manuálneho zásahu.

V rámci sledovaného obdobia boli vykonávané pravidelné bezpečnostné audity a nasadenia opatrení voči potenciálnym hrozbám a zneužitiam, pravidelne bola vykonávaná inštalácia nových verzií jednotlivých komponent informačného systému.

<b>411</b>	<b>Informačný systém štátnej pokladnice</b>
------------	---

V roku 2025 DataCentrum zabezpečovalo štandardné prevádzkové služby pre produkčné, testovacie, vývojové a prípadne aj záložné prostredia nasledovných systémov Štátnej pokladnice:

- IS ŠP – Informačný systém štátnej pokladnice pozostávajúci z nasledovných samostatných modulov/aplikácií:
  - ManEx – Riadenie výdavkov,
  - AccoMan/PayEx – Vedenie účtov a platobný styk,
  - PlarEx – Finančné plánovanie,
  - FlexMan – Flexibilné analytické zostavy,
  - UseMan – Správa používateľov,
  - ArchMan – Archivačný systém,
  - ArchUseMan – Správa používateľov pre archivačný systém,
  - QxHUB – Moduly pre TIPS,
  - TxDA – Integrácia core-banking s KZ,
  - BPM – Business Proces Management,
  - SAP-PI/MPDR – Integrované platformy,
  - PBŠP – Platobná brána ŠP,
  - SAP R3 – Systém účtovníctva,
  - SAP BW – Systém výkazníctva,
  - KZ – Klientska zóna ŠP,
  - Úhrady/Platby štátu.

V roku 2025 medzi prevádzkované systémy pribudol modul QxHUB a Úhrady/Platby štátu v produkčnej prevádzke.

Ďalej okrem štandardných prevádzkových služieb bola zo strany DataCentra poskytovaná súčinnosť pri implementácii zmien, ich prvotnom testovaní, ako aj ich samotné nasadzovanie v rámci testovacích a produkčných systémov. Medzi najväčšie zmeny, pri ktorých bola poskytovaná súčinnosť, bola implementácia okamžitých platieb (TIPS2 platieb), kde boli implementované nové moduly a bolo potrebné riešiť vzájomnú integráciu a prepojenie aj na sieťovej úrovni medzi samotnými modulmi TIPS2 prevádzkovanými Štátnou pokladnicou

a backendovým modulom systému ŠP prevádzkovaným DataCentrom. Nová funkcionálna okamžitých platieb TIPS1 (prijímanie) bola do produkčnej prevádzky úspešne spustená 06. 01. 2025 a rozšírená funkcionálna okamžitých platieb TIPS2 (odosielanie) bola do produkčnej prevádzky uvedená 03. 10. 2025.

Priebežne boli zo strany DataCentra zabezpečované činnosti spojené so správou, údržbou a vytváraním prístupov pre existujúcich a nových používateľov IS ŠP systémov na prístupovej platforme KTI.

Taktiež boli oddelením CPU zabezpečované služby spojené s nahlasovaním požiadaviek a problémov koncových používateľov od ich evidencie, postúpenia na príslušné riešiteľské skupiny, monitoringu ich riešenia v nasledovných počtoch hlásení v jednotlivých systémoch:

	2025	2025	2025	2025	2025	2025	2025	2025	2025	2025	2025	2025	Spolu
	1	2	3	4	5	6	7	8	9	10	11	12	
AccoMan		18	2	1	3		3	2		5	2	2	38
ISŠP APLIKÁCIE	7	12	6	2	3	4	13	8	6	12	6	4	83
ManEx		42		3				1	10		1	22	79
Portál	216	128	122	109	112	124	124	76	108	124	165	395	1 803
ISŠP SAP PI	31	45	45	17	33	45	36	38	31	41	35	41	438
SAP Účtovníctvo ŠP		3	1		1	1			1			1	8
SAP Výkazníctvo ŠP									1	1		1	3
<b>Spolu</b>	<b>254</b>	<b>248</b>	<b>176</b>	<b>132</b>	<b>152</b>	<b>174</b>	<b>176</b>	<b>125</b>	<b>157</b>	<b>183</b>	<b>209</b>	<b>466</b>	<b>2 452</b>

V roku 2025 bola na uvedených systémoch zaregistrovaná v pracovných dňoch v čase od 7.00 hod. do 19.00 hod. krátka neplánovaná nedostupnosť v trvaní 30 minút na systéme BPM spôsobená výpadkom hardvéru a následným zlyhaním failoveru. Nedostupnosť v iných časoch bola vopred komunikovaná a bola len v prípade plánovaných odstávok spojených s update a upgrade systémov a aplikácií.

Okrem vyššie uvedených štandardných činností bolo v roku 2025 zabezpečené aj nasledovné:

- RÚZ 2025 – podpora a koordinácia prípravnej a ostrej ročnej účtovnej závierky,
- podpora a súčinnosť pri uprade všetkých Unix systémov na najnovšiu verziu,
- patchovanie komponentov modulov TxDA,
- upgrade OS na Linux aplikačných serveroch, patchovanie OS,
- upgrade SAP Kernel,
- príprava novej infraštruktúry a serverov pre rozšírenie modulu Klientskej zóny Štátnej pokladnice (SmartPOS, Úhrady),
- príprava novej infraštruktúry a serverov pre novú integráciu pre výmenu správ pre nové TIPS1/TIPS2 moduly,
- zabezpečenie integrácie na REST služby pre TIPS/VOP,
- prípravné činnosti a POC pre migráciu systémov z OS Unix na Linux.

<b>412</b>	<b>Register vylúčených osôb (RVO)</b>
------------	---------------------------------------

V priebehu roka 2025 bolo pri prevádzke Registra vylúčených osôb riešených 108 hlásení používateľov. Vo veľkej miere sa tieto hlásenia týkali problémov s prevádzkami, pridelenými tokenmi, či prístupov cez API rozhranie.

V uplynulom roku prebiehalo pravidelné importovanie zoznamov osôb vylúčených z hrania hazardných hier prostredníctvom Centrálného systému referenčných údajov a z dát poskytnutých z ďalších organizácií, ktoré sú zdrojom pre systém RVO.

Import nových prevádzok do systému RVO je od roku 2024 plne v kompetencii ÚRHH.

Z dôvodu neustáleho pribúdania údajov a zapájania diskových priestorov v architektúre IS RVO, bola vykonaná konsolidácia hardvérových zdrojov.

Na konci kalendárneho roka 2025 boli začaté práce na publikovaní novej RVO aplikácie. Aplikácia je momentálne v testovacej fáze a bude primárne určená pre zamestnancov ÚRHH.

Taktiež prebehla príprava nového produkčného prostredia s aktualizovanou verziou operačných systémov. Samotná migrácia prebehne začiatkom roka 2026.

Za celý rok 2025 DataCentrum evidovalo nedostupnosť systému v trvaní celkovo 28 minút. Celková dostupnosť systému bola na úrovni 99,99 %.

<b>413</b>	<b>Rozpočtový informačný systém (RIS)</b>
------------	---

V rámci prevádzky Rozpočtového informačného systému bola zabezpečovaná prevádzka operačných systémov, aplikačných a databázových serverov a serverov pre automatizačné a orchestračné služby, ďalej RIS middleware vrstvy a všetkých modulov a aplikácií RIS vrátane integrácií, taktiež bola zabezpečovaná prevádzka virtualizačnej platformy Oracle VM.

Počas celého roka bol sledovaný monitoring, dashboardy a e-mail alerty, následne na základe identifikácie a klasifikácie problémových stavov základných služieb boli zakladané incidenty, ktoré boli posúvané na jednotlivé úrovne podpory na vyriešenie problému, opravu problémového zariadenia, príp. eskaláciu riešenia na vlastníka.

Pravidelne prebiehalo zálohovanie RIS databáz a virtuálnych serverov v súlade s internými predpismi. Rovnako v pravidelných intervaloch boli aktualizované všetky komponenty RIS, od operačných systémov cez aplikačnú a databázovú vrstvu až po sieťové a bezpečnostné technológie. Zároveň prebiehal deployment aplikácií RIS a inštalácia nových verzií a updatov.

V uvedenom období boli vytvárané prístupy pre nových používateľov do jednotlivých aplikácií RIS.

V roku 2025 bola prevádzka aplikačných a infraštruktúrnych systémov RIS realizovaná na požadovanej úrovni, t. j. boli dodržané všetky zmluvne definované SLA. Prevádzka bola stabilná, bez vážnych incidentov, ktoré by znamenali celkový výpadok služieb.

V roku 2025 boli v rámci Rozpočtového informačného systému (RIS) realizované projekty, ktoré sa týkali činností súvisiacich s migráciou RIS do rezortného privátneho cloudu (RPC).

Išlo najmä o činnosti v oblasti optimalizácie prevádzky RIS v RPC. Tento projekt spočíval najmä v príprave a otestovaní pilotného PoC prostredia pre realizáciu plánovanej zmeny publikovania aplikácií a modulov Rozpočtového informačného systému z aktuálne využívaného spôsobu v KTI DataCentra na štandardnú platformu použitú v prostredí RPC. Po dokončení PoC fázy boli vytvorené najprv v ZVS a následne v DC-C testovacie a produkčné prostredia s aplikačnými a webovými virtuálnymi servermi. S tým súviselo viacnásobné konfigurovanie sieťových pravidiel, zároveň boli začaté práce na realizácii backup riešenia pre RIS v RPC. Ďalším projektom bola realizácia integrácie databázových prostredí IS RIS do prevádzky RPC.

<b>414</b>	<b>Centrálny register účtov (CRÚ)</b>
------------	---------------------------------------

V rámci projektu CRÚ boli ešte v roku 2022 vytvorené serverové systémy pre jednotlivé prostredia IS CRÚ, v roku 2023 boli následne povolené potrebné sieťové prepojenia pre testovacie a predprodukčné prostredia a zabezpečené ďalšie potrebné nastavenia pre sfunkčnenie týchto prostredí. Následne v roku 2024 boli sfunkčnené produkčné a záložné prostredia. V uplynulom roku bola zabezpečovaná štandardná prevádzka systémov CRÚ na účely bezproblémovej funkčnosti a dostupnosti tohto informačného systému.

V priebehu roka 2025 boli realizované migrácie pripojenia niekoľkých finančných inštitúcií, a to z dôvodu potreby odstavenia VPN zariadení, prostredníctvom ktorých bolo pripojenie realizované.

Používateľom systému CRÚ bola poskytovaná podpora prostredníctvom Centra podpory používateľov DataCentra a ďalších riešiteľských skupín z MF SR a dodávateľa systému.

Vďaka prepojeniu na e-mailovú infraštruktúru DataCentra boli zasielané e-mailové notifikácie používateľom systému, ktoré sú podľa požiadavky vlastníka IS súčasťou workflow IS CRÚ.

V uplynulom roku v súvislosti s nábehom produkčnej prevádzky boli vlastníkov systému vytvorené a poskytnuté prehľady o počtoch používateľov, o inicializácii hesla a prihlásení pomocou OTP tokenu. Taktiež bol vytvorený prehľad neaktívnych používateľov.

V závere roka prebehli na tomto IS testy bezpečnosti, pri konaní ktorých DataCentrum poskytlo potrebnú súčinnosť.

<b>415</b>	<b>Centrálny ekonomický systém (CES)</b>
------------	--

Počas roka 2025 prebiehali štandardné prevádzkové činnosti, v rámci nich bolo potrebné realizovať úpravu prevádzkových parametrov a navyšovanie zdrojov serverov CES, ako sú veľkosť diskového priestoru či operačnej pamäte.

V hodnotenom období bolo realizované prepojenie CES modulu M28\_1 na Národný katalóg otvorených dát (data.slovensko.sk), pilotne pre potreby reportingu ÚVO na účely zberu otvorených dát. Taktiež prebehlo aj rozšírenie existujúceho prístupu cez KTI2 na ďalšie systémy CES podľa aktuálne schválenej detailnej špecifikácie riešenia.

V roku 2025 sa v testovacom prostredí KTI2 RRP pracovalo na príprave služby overenia dvojfaktorovej autentifikácie s využitím jednorazového hesla založeného na tzv. softvér tokene

na účely zabezpečenia silnej autentifikácie používateľského prístupu. V roku 2025 bola táto služba nasadená v produkčnom prostredí CES, čím bola dosiahnutá vyššia úroveň bezpečnosti pri prihlasovaní používateľov.

V súvislosti s prípravou tretej vlny rozšírenia CES pre definovaný okruh nových organizácií, medzi ktorými je aj Košický samosprávny kraj a organizácie v jeho zriaďovateľskej pôsobnosti, prebehla analýza a príprava používateľov pre migráciu dát do CES a RRP, taktiež prebehlo modelovanie a mapovanie architektúry CES pre potreby nahratia údajov do konfiguračnej databázy. Pre potreby projektu CES bol pripravený návrh úprav Service Manager-a. Taktiež prebehla integrácia na systém RRP so službami dvojfaktorovej autentifikácie s definovanými procesmi manažmentu autentifikačných prostriedkov pre nových používateľov. V rámci tohto prepojenia bol kladený dôraz na zabezpečenie prístupu prostredníctvom Single Sign-On, t. j. aby koncoví používatelia pri prístupe na webové aplikácie CES SAP Fiori iba raz zadali meno a heslo.

Ďalej bola poskytnutá súčinnosť pri príprave a realizácii pripájania organizácií zapojených do tretej vlny rozšírenia systému CES.

Pre potreby performance testov pred realizáciou tretej vlny bolo na základe požiadaviek dodávateľa CES potrebné na QE1 prostredí robiť úpravy na existujúcich databázových VM a zároveň pripraviť potrebný výpočtový výkon na realizáciu požadovanej záťaže, to nevyhnutne vyžadovalo aj potrebné sieťové konfigurácie v lokalite DC-C a DC-K.

V rámci prevádzky CES bolo pred nábehom tretej vlny zrealizované navýšenie výpočtových kapacít VM (navýšenie RAM).

V roku 2025 boli integrované nové moduly CES na AV riešenie na účely kontroly súborov na prítomnosť škodlivého kódu.

V rámci Portálovej aplikácie grant management (PAGM) boli v uplynulom roku realizované:

- zálohovanie,
- umiestnenie do DMZ siete,
- konfigurácia web-aplikačného firewallu,
- konfigurácia sieťových a bezpečnostných prvkov na umožnenie funkčnosti celého prostredia PAGM,
- súčinnosť pri realizácii performance a penetračných testov.

V rámci Portálovej aplikácie grant management (PAGM) bolo realizované prepojenie so systémom RRP. Cieľom tejto integrácie je v rámci PAGM zabezpečiť správu a riadenie prístupov zamestnancov OVM pod jednotnou identitou zamestnanca, ktorá sa viaže na evidenciu a priame prepojenie na CES. Prístup používateľov je vďaka tomu riadený rolami SAP M15 CES.

Všetky prostredia PAGM boli pripravené na odovzdanie prevádzkovateľovi CES.

V roku 2025 bol nasadený systém na nahrávanie hovorov agentov CES v kontaktnom centre IPCC. Systém poskytuje komplexné riešenie záznamu a analýzy interakcií so zákazníkmi, vylepšuje efektivitu prevádzky a zabezpečuje zhodu s pravidlami. Pre supervízorov systém umožňuje webový prístup na vyhľadávanie, prehrávanie a export nahrávok s jedinečnými ID hovorov.

## **CES - DR prostredie v ZVS**

V roku 2025 v rámci projektu CES sa realizovalo vytvorenie DR prostredia v ZVS. Boli vytvorené nezávislé jump servre v ZVS. Skompletizovala sa architektúra vrátane všetkých integrácií a potvrdil sa aj zoznam nevyhnutných integrácií v ZVS. Implementoval sa NiFi - centrálny synchronizačný systém na synchronizáciu aplikačnej vrstvy. Urobilo sa komplexné riešenie DNS resolvingu v ZVS. Bol potvrdený zoznam replikovaných služieb v ZVS. Bola nakonfigurovaná replikácia SAP HANA DB (QEH) node1 (DC-C)-> node3 (ZVS), súčasne bola vykonaná kontrola aplikačných aj DB VM inšancií - z čoho vyplynula potreba upraviť niektoré parametre aplikačných VM inšancií. Následne bol zrealizovaný test failover medzi HANA DB QEH DC-C vs ZVS - node1 vs node3. Bola nakonfigurovaná aj lokálna replikácia v ZVS HANA DB QEH v ZVS - node3 na node4 a zrealizovaný test failover medzi HANA DB QEH v ZVS - node3 vs node4. V ďalších krokoch bolo potrebné zrealizovať replikáciu Content servera QC1 SAP MaxDB a v tejto časti bolo potrebné vytvoriť unikátny kód. Na aplikačnej vrstve bolo tiež potrebné spojzduť Content Server PC1, replikáciu ADS aplikačnej vrstvy a tiež replikáciu transportného adresára. Medzi lokalitami DC-C a ZVS bolo potrebné zistiť celkovú potrebnú prenosovú kapacitu pre CES replikačné mechanizmy počas bežnej dlhodobej prevádzky. Musela sa aj doriešiť problematika patchovania MAX DB. Boli vypracované detailné testovacie scenáre. Finálny test so spoluúčasťou MF SR trval 4 hodiny.

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. Kapacitne sú v tejto úlohe obsiahnuté aj všetky ostatné činnosti prevádzkového charakteru. Ide o činnosti súvisiace so zabezpečením bezproblémového plnenia všetkých úloh vyplývajúcich pre DataCentrum z jeho štatútu, podpísaného kontraktu na príslušný rok, činnosti potrebné na zabezpečenie aj rozvojových úloh, prípadne neplánovaných alebo mimoriadnych úloh a činnosti súvisiace s vytvorením a podporou pracovných podmienok k tomu potrebných.

Úlohy boli riešené a organizačne zabezpečované a koordinované v súlade s internými pracovnými postupmi a relevantnou legislatívou tak, aby bol zabezpečený bezproblémový chod DataCentra, ako aj prevádzka spravovaných informačných systémov a plnenie kontrahovaných úloh.

Tieto činnosti a ani čerpané kapacity neboli predmetom žiadnej inej úlohy špecifikovanej v kontrahovanom identifikačnom liste.