Z-009581/2014/1070/KMC

NAJVYŠŠÍ KONTROLNÝ ÚRAD SLOVENSKEJ REPUBLIKY

Číslo poverenia: 1050/01
Zo dňa: 19.11.2014

Počet výtlačkov: 2
Výtlačok číslo: 1
Počet strán: 13
Počet príloh: 0

P R O T O K O L

o výsledku kontroly
hospodárenia a ochrany aktív v oblasti informačno-komunikačných technológií
vo vybraných nemocniciach SR

Detská fakultná nemocnica s poliklinikou Banská Bystrica

Banská Bystrica december 2014

Zhrnutie:

Najvyšší kontrolný úrad Slovenskej republiky vykonal v spolupráci so Švajčiarskym federálnym kontrolným úradom v marci 2013 rizikovú analýzu informačno-komunikačného prostredia vo vybraných nemocniciach Slovenskej republiky. Riziková analýza ukázala nedostatky v oblasti činnosti organizácie, informačných technológií vnútorného kontrolného systému, aplikačného programového vybavenia, prevádzky informačných technológií a v iných oblastiach. Identifikované boli nedostatky predovšetkým v oblasti implementácie informačných systémov, procesoch vnútorného kontrolného systému, povedomia o informačnej bezpečnosti, stanovenie zodpovednosti a nezlučiteľnosti rolí, kľúčových aplikácií a databázových systémov. Z tohto dôvodu zahrnul Najvyšší kontrolný úrad Slovenskej republiky do plánu kontrolnej činnosti na rok 2014 kontrolu hospodárenia a ochrany aktív v oblasti informačno-komunikačných technológií vo vybraných nemocniciach.

Kontrola bola vykonaná v súlade so zákonom o Najvyššom kontrolnom úrade Slovenskej republiky a boli uplatňované medzinárodné štandardy najvyšších kontrolných inštitúcií.

Predmetom kontroly bola správa majetku štátu, hospodárenie a nakladanie s majetkom štátu v oblasti informačno-komunikačných technológií, dodržiavanie všeobecne záväzných právnych predpisov pri hospodárení s finančnými prostriedkami v oblasti informačno-komunikačných technológií, dodržiavanie všeobecne záväzných predpisov pre oblasť informačných systémov verejnej správy, prevádzka informačných systémov verejnej správy a kontrola bezpečnosti informačných systémov verejnej správy.

Hodnotiacimi kritériami bola relevantná legislatíva Slovenskej republiky, vrátane súvisiacich právnych predpisov, týkajúcich sa jednotlivých oblastí predmetu kontroly a platných v kontrolovanom období.

Základom pre výber kontrolovaných údajov boli účtovné a finančné výkazy, dokumentácia k vedeniu a nakladaniu s majetkom štátu a výstupy z informačných systémov. Z dôvodu rozsiahlej údajovej základne bol výber vzorky realizovaný neštatistickou metódou na základe kvalifikovaného úsudku kontrolóra.

Kontrolou bolo preverené zaraďovanie a evidencia dlhodobého nehmotného a dlhodobého hmotného majetku za oblasť informačno-komunikačných technológií, ako aj evidovanie vybraného drobného dlhodobého nehmotného a hmotného majetku za uvedenú oblasť. Kontrolou uvedenej oblasti nebol zistený rozdiel medzi skutočným a požadovaným stavom.

Súlad dodržiavania všeobecne záväzných právnych predpisov pri hospodárení s finančnými prostriedkami v oblasti informačno-komunikačných technológií bol preverený na vybraných verejných obstarávaniach týkajúcich sa uvedenej oblasti a tiež preverením vybraných faktúr súvisiacich s vynakladaním finančných prostriedkov na oblasť informačno-komunikačných technológií. Kontrolou nebol zistený nesúlad medzi požadovaným a skutočným stavom.

V oblasti dodržiavania všeobecne záväzných právnych predpisov nadväzujúcich na ustanovenia zákona o informačných systémov verejnej správy a zákona o ochrane osobných údajov bolo zistených niekoľko nedostatkov týkajúcich sa neúplnej implementácie týchto predpisov pri prevádzke informačných systémov a pri vypracovaní dvoch základných interných predpisov Detskej fakultne nemocnice s poliklinikou Banská Bystrica pre oblasť informačno-komunikačných technológií – bezpečnostnú politiku a bezpečnostný projekt.

Kontrolou prevádzky a bezpečnosti informačných systémov kontrolovaného subjektu zameranou hlavne na zálohovanie a obnovu informačných systémov, politiky hesiel a fyzickej bezpečnosti informačných systémov nebol zistený nesúlad medzi skutočným a požadovaným stavom.

Súčasťou kontroly bolo aj preverenie vybraných rizík zistených rizikovou analýzou najmä v riadení procesov v oblasti informačných technológií, implementácie informačných systémov a vnútorného kontrolného systému. Najvyšší kontrolný úrad Slovenskej republiky konštatoval zlepšenie v niektorých rizikových oblastiach v dôsledku činnosti kontrolovaného subjektu počas roku 2014.

Odporúčania na riešenie zistených nedostatkov:

- aktualizovať koncepciu rozvoja informačných systémov s ohľadom na platné legislatívne predpisy v oblasti informačno-komunikačných technológii,
- prijať také opatrenia, aby bola zabezpečená bezpečnosť informácií a aktív Detskej fakultnej nemocnice s poliklinikou Banská Bystrica, ktoré sú spravované tretími stranami,
- dopracovať poučenie oprávnenej osoby o rozsah oprávnení, popis povolených činností a podmienky spracúvania osobných údajov,
- upraviť poučenia oprávnených osôb v zmysle platnej legislatívy, ktorá nepozná pojem oboznámená osoba a vnímať ako oprávnenú osobu každého, kto prichádza do styku s osobnými údajmi,
- vypracovať evidenčný list ku každému používanému informačnému systému, v ktorom sa spracovávajú osobné údaje.

Protokol
o výsledku kontroly

Podľa poverenia predsedu NKÚ SR č. **1050/01** z 19.11.2014 vykonali:

Ing. Marián Koreň, vedúci kontrolnej skupiny
Ing. Martina Gallasová, členka kontrolnej skupiny
Ing. Ján Kúdola, člen kontrolnej skupiny
Ing. František Žabka, člen kontrolnej skupiny

kontrolu hospodárenia a ochrany aktív v oblasti informačno-komunikačných technológií vo vybraných nemocniciach SR, ktorej účelom bolo preveriť stav dodržiavania všeobecne záväzných právnych predpisov, hospodárnosti a správy a ochrany aktív v oblasti informačno-komunikačných technológií vo vzťahu k zabezpečeniu a ochrany aktív informačno-komunikačných technológií na základe výsledkov rizikovej analýzy.

Kontrola bola vykonaná v čase od 21.11.2014 do 08.12.2014 v

Detskej fakultnej nemocnici s poliklinikou Banská Bystrica,
Námestie L. Svobodu 4, 974 01 Banská Bystrica, IČO 37957937

za kontrolované obdobie rokov 2012-2014, v prípade potreby objektívneho zhodnotenia kontrolovanej skutočnosti aj predchádzajúce obdobie.

Kontrola bola vykonaná v súlade so zákonom č. 39/1993 Z. z. o Najvyššom kontrolnom úrade Slovenskej republiky v znení neskorších predpisov a so štandardami, ktoré vychádzajú zo základných princípov kontroly (ISSAI 100 – 999) v rámci medzinárodných štandardov najvyšších kontrolných inštitúcií.

Predmetom kontroly bolo:

- správa majetku štátu, hospodárenie a nakladanie s majetkom štátu v oblasti informačno-komunikačných technológií,
- dodržiavanie všeobecne záväzných právnych predpisov pri hospodárení s finančnými prostriedkami v oblasti informačno-komunikačných technológií,
- dodržiavanie všeobecne záväzných predpisov pre oblasť informačných systémov verejnej správy,
- prevádzka informačných systémov verejnej správy,
- bezpečnosť informačných systémov verejnej správy.

Počas výkonu kontroly bolo zistené:

Detská fakultná nemocnica s poliklinikou Banská Bystrica (ďalej len „DFNsP BB“ alebo „kontrolovaný subjekt“) bola zriadená dňa 28.12.2004 zriaďovacou listinou č. 14192-6/2004-OPP, ktorá bola vydaná Ministerstvom zdravotníctva Slovenskej republiky (ďalej aj „MZ SR“) dňa 24.11.2004.

Kontrolovaný subjekt je štátna príspevková zdravotnícka organizácia.

Organizačná štruktúra kontrolovaného subjektu má tri úrovne rozhodovania. Štatutárnym orgánom je riaditeľ nemocnice, ďalej sú to námestníci a vedúci jednotlivých oddelení. DFNsP BB je napojená na systém Štátnej pokladnice. Činnosť organizácie je zabezpečovaná verejnými zdrojmi, ktorými sú verejné prostriedky zo zdravotných poisťovní, prostriedky získané z vlastnej činnosti, darované prostriedky a prostriedky zo štátneho rozpočtu SR z kapitoly MZ SR.

Predmetom činnosti DFNsP BB je poskytovanie špecializovanej ambulantnej a ústavnej zdravotnej starostlivosti pacientom detského veku od narodenia do 18 rokov veku vrátane, najmä diagnostika, liečba a dispenzarizácia pacientov v odbore pediatria a jeho špecializáciách.

DFNsP BB sa tiež podieľa na vedecko - výskumnej činnosti. Spolupracuje so vzdelávacími ustanovizňami, ktoré poskytujú stredoškolské, vysokoškolské a ďalšie vzdelávanie zdravotníckych pracovníkov a v spolupráci s príslušnými odbornými spoločnosťami a stavovskými organizáciami v zdravotníctve organizuje sústavné vzdelávanie zdravotníckych pracovníkov.

1. Správa majetku štátu, hospodárenie a nakladanie s majetkom štátu v oblasti informačno-komunikačných technológií

Správu majetku štátu upravoval v kontrolovanom období zákon č. 278/1993 Z. z. o správe majetku štátu v znení neskorších predpisov. V zmysle § 3 ods. 2 uvedeného zákona bola DFNsP BB oprávnená a povinná tento majetok užívať na plnenie úloh v rámci predmetu činnosti alebo v súvislosti s ním, nakladať s ním podľa tohto zákona, udržiavať ho v riadnom stave, využívať všetky právne prostriedky na jeho ochranu a dbať, aby nedošlo najmä k jeho poškodeniu, strate, zneužitiu alebo zmenšeniu. Podľa ustanovenia § 3 ods. 9 uvedeného zákona bola DFNsP BB povinná viesť o majetku štátu účtovníctvo v rozsahu a spôsobom ustanoveným zákonom č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov.

Obstaranie majetku, vedenie evidencie a účtovanie o ňom v podmienkach DFNsP BB upravoval najmä organizačný poriadok a smernica č. 06/2007 - Dlhodobý majetok (ďalej len „smernica o dlhodobom majetku“).

Podľa organizačného poriadku zabezpečovalo nakladanie s majetkom DFNsP BB od 01.03.2012 oddelenie nákupu v členení na referát nákupu liekov a zdravotníckych pomôcok a referát nákupu ostatných tovarov a služieb, ktoré okrem iného zodpovedalo za vyhotovovanie objednávok, kontrolu dodacích listov a faktúr, vykonanie inventarizácie, zaradenie majetku a pod.

V zmysle smernice o dlhodobom majetku neúčtovala DFNsP BB o drobnom dlhodobom nehmotnom a hmotnom majetku. Dlhodobý nehmotný majetok pod stanovené sumy bol považovaný za služby, vedený na operatívnej evidencii a jeho hodnota bola účtovaná na podsúvahových účtoch. Dlhodobý hmotný majetok s obstarávacou cenou nižšou ako 1 700,00 eur a s dobou použiteľnosti dlhšou ako jeden rok bol považovaný za zásoby, vedený v operatívnej evidencii a jeho hodnota bola účtovaná na podsúvahových účtoch.

Evidencia majetku bola vedená programovým vybavením.

Prehľad o stave celkového majetku DFNsP BB a za vybrané účty, na ktorých bol počas kontrolovaného obdobia účtovaný aj majetok týkajúci sa informačno-komunikačných technológii (ďalej len „IKT“), je uvedený v nasledovnej tabuľke.

v eur

Druh majetku	Rok 2012			Rok 2013		Rok 2014	
	stav k 01.01.2012	stav k 31.12.2012	prírastok /úbytok	stav k 31.12.2013	prírastok /úbytok	stav k 30.09.2014	prírastok /úbytok
MAJETOK celkom	**11 917 457,37**	**16 429 254,66**	**4 511 797,29**	**16 957 359,57**	**528 104,91**	**x**	**x**
DNM	**142 294,25**	**182 695,01**	**40 400,76**	**182 695,01**	**0,00**	**182 695,01**	**0,00**
softvér	142 294,25	182 695,01	40 400,76	182 695,01	0,00	182 695,01	0,00
obstaranie DNM	0,00	0,00	0,00	0,00	0,00	0,00	0,00
DHM	**13 964 402,88**	**14 257 038,49**	**292 635,61**	**14 544 863,45**	**287 824,96**	**x**	**x**
samost. hnuteľné veci a súbory	4 589 496,89	4 812 724,93	223 228,04	5 087 301,98	274 577,05	5 166 688,42	79 386,44
obstaranie DHM	13 504,47	69 255,20	55 750,73	15 249,50	-54 005,70	35 261,25	20 011,75

*zdroj: súvaha a hlavná kniha k 31.12.2012, 31.12.2013 a k 30.09.2014
DNM – dlhodobý nehmotný majetok, DHM – dlhodobý hmotný majetok

Dlhodobý nehmotný majetok zaznamenal prírastok len v roku 2012, kedy DFNsP BB obstarala softvér v rámci projektu Manažment centrálneho katalógu liekov v sume 40 400,76 eur. V roku 2013 a k 30.09.2014 nebol obstaraný žiadny dlhodobý nehmotný majetok.

Dlhodobý hmotný majetok za vybrané účty vzrástol v každom z rokov kontrolovaného obdobia, okrem účtu obstarania, ktorý k 31.12.2013 poklesol. Prírastok majetku za oblasť IKT bol evidovaný na účte 022 120 - samostatné hnuteľné veci nasledovne:

- v roku 2012 technologická časť manažmentu centrálneho katalógu liekov v sume 8 226,00 eur,
- v roku 2013 výpočtová technika, najmä servery, v celkovej sume 26 540,82 eur,
- v roku 2014 nebol obstaraný žiadny dlhodobý hmotný majetok za oblasť IKT.

Kontrolou bolo preverené zaraďovanie a evidencia dlhodobého nehmotného a dlhodobého hmotného majetku za oblasť IKT v celkovej sume 75 167,58 eur. Ďalej bolo preverené evidovanie vybraného drobného dlhodobého nehmotného a hmotného majetku s najvyššími hodnotami za oblasť IKT v celkovej sume 13 537,50 eur, obstaraného počas kontrolovaného obdobia.

Kontrolou nebol zistený nesúlad medzi požadovaným a skutočným stavom.

DFNsP BB po obstaraní majetku evidovala majetok nad stanovené sumy na príslušných majetkových účtoch a inventárnych kartách. Súčasťou evidencie boli aj faktúry, likvidačné listy k faktúram, dodacie listy, resp. akceptačné protokoly a zaraďovacie protokoly. Inventárne karty zaradeného majetku obsahovali aj osobu zodpovednú za príslušný majetok. Hodnota majetku pod stanovené hodnoty bola evidovaná na podsúvahových účtoch.

Smernica o dlhodobom majetku upravovala aj vyraďovanie a likvidáciu majetku v podmienkach DFNsP BB, podľa ktorej návrh na vyradenie podávala zodpovedná osoba za majetok vyraďovacej komisii s dôvodom na vyradenie a dokladom o neopraviteľnosti. Podkladom pre zaúčtovanie vyradenia majetku z evidencie a jeho fyzickej likvidácie bolo vydané rozhodnutie riaditeľa DFNsP BB o neupotrebiteľnosti majetku štátu, ktoré vydal na základe návrhu vyraďovacej komisie. Súčasťou evidencie k vyradeniu majetku bol vyraďovací protokol a doklad o uskutočnení likvidácie.

V roku 2012 bol za oblasť IKT vyradený majetok v celkovej sume 14 730,18 eur. Kontrolou vyraďovania a likvidácie uvedeného majetku neboli zistené nedostatky.

Vyraďovanie a likvidácia majetku za rok 2013 bola predmetom kontroly NKÚ SR zmluvných vzťahov a úhrad za poskytovanie zdravotnej starostlivosti vykonanou v roku 2014. Uvedenou kontrolou neboli zistené nedostatky.

Inventarizácia majetku, záväzkov a rozdielu majetku a záväzkov DFNsP BB k 31.12.2012 bola vykonaná na základe príkazu riaditeľa DFNsP BB č. 6/2012 z 01.10.2012. V zmysle uvedeného príkazu nebol predmetom inventarizácie dlhodobý hmotný a drobný dlhodobý hmotný majetok.

Preverením inventarizácie majetku súvisiaceho s IKT k 31.12.2012 nebol zistený nesúlad medzi požadovaným a skutočným stavom. Stav zistený inventarizáciu súhlasil s účtovným stavom.

Inventarizácia k 31.12.2013 bola predmetom kontroly NKÚ SR zmluvných vzťahov a úhrad za poskytovanie zdravotnej starostlivosti vykonanou v roku 2014. Uvedenou kontrolou neboli zistené nedostatky.

2. Dodržiavanie všeobecne záväzných právnych predpisov pri hospodárení s finančnými prostriedkami v oblasti IKT

DFNsP BB vykonala v kontrolovanom období 13 verejných obstarávaní v celkovej hodnote 127 137,34 eur. Len jedno z verejných obstarávaní v sume 35 876,30 eur bez DPH bolo realizované formou podprahovej zákazky rokovacím konaním bez zverejnenia. Táto zákazka sa týkala zmeny a rozšírenia funkcionality jedného z informačných systémov (ďalej len „IS“) v rámci projektu Manažment centrálneho katalógu liekov (ďalej len „MCKL“). Ostatné zákazky boli obstarávané ako zákazky s nízkou hodnotou.

Manažment centrálneho katalógu liekov

Kontrolovaný subjekt sa v roku 2012 zapojil do projektu MCKL na základe projektového zámeru MZ SR. Projekt mal nadviazať na aktuálny stav používaných IS DFNsP BB a doplniť ich nevyhnutným hardvérovým a softvérovým vybavením pre účely projektu.

Technologickú časť projektu - server, MS Windows Server 2008, MS SQL Server 2008, záložný zdroj, VPN, zariadenie na archiváciu údajov DFNsP BB obstarala ako zákazku s nízkou hodnotou formou prieskumu trhu. Z ponúk troch záujemcov bola vybraná a zrealizovaná najnižšia ponuka v sume 11 959,20 eur.

Softvérovú časť zabezpečila DFNsP BB prostredníctvom podprahovej zákazky rokovacím konaním bez zverejnenia. Postup verejného obstarávania odôvodnila s nadväznosťou na aktuálny ekonomický IS s autorským certifikátom, s ktorým mal MCKL komunikovať ako jeho nový modul. DFNsP BB podpísala dňa 27.02.2012 zmluvu o dielo s finančným plnením v celkovej hodnote 35 867,30 eur bez DPH. Predmetom zákazky bolo vybudovanie dátového skladu údajov lekárenského charakteru a ich následné spracovanie s komunikáciou s dátovým centrom v Národnom centre zdravotníckych informácií. Podľa vyjadrenia DFNsP BB výška nákladov na vyvolané programátorské úpravy v existujúcom ekonomickým IS bola nižšia ako nákup samostatne fungujúceho lekárnického IS od špecializovaných dodávateľov s nadväznými programátorskými úpravami v tomto IS.

Kontrolou bolo preverené aj plnenie zmluvy z finančného a účtovného hľadiska. DFNsP BB z prijatej sumy 55 000,00 eur kapitálovým transferom financovala technologickú

časť sumou 11 959,20 eur a softvérovú časť sumou 40 400,76 eur. Zmluvne dohodnuté prostriedky na softvérovú časť v sume 2 640,00 eur DFNsP BB nevyčerpala a pri zúčtovaní transferu vrátila uvedenú sumu na účet MZ SR. Vrátené prostriedky vecne predstavovali sumu za nezrealizovanú implementáciu rozhraní na centrálny kontrakt manažment. Podľa vysvetlenia DFNsP BB systém MCKL bol v prevádzke a jeho ukončenie bolo vyvolané zastavením činnosti systému u iniciátora projektu, tzn. MZ SR.

V čase kontroly sa centrálny katalóg liekov nevyužíval, resp. neplnil účel, na ktorý bol projekt orientovaný. Daný stav však nie je výsledkom nesprávnej realizácie projektu zo strany DFNsP BB, ale pozastavením aktivít súvisiacich s projektom zo strany MZ SR ako iniciátora projektu. V súčasnosti je technologická časť obstarávaná v rámci tohto projektu po odsúhlasení zo strany MZ SR využívaná DFNsP BB na iné účely potrebné pre výkon svojich činností.

Niektoré zákazky obstarávané v kontrolovanom období formou zákazky s nízkou hodnotou sa týkali len predĺženia produktovej a metodickej podpory zo strany externých dodávateľov vyplývajúcich zo zmlúv, ktoré DFNsP BB uzavrela pred kontrolovaným obdobím.

Jedinou zmenou v aplikačnom programovom vybavení bolo rozšírenie využívaného ekonomického IS o modul týkajúci sa ľudských zdrojov vrátane dochádzkovej karty a dvoch aktívnych a pasívnych používateľských licencií v sume 2 016,00 eur s DPH na základe dodatku č. 1 k zmluve o nájme aplikačného vybavenia zo dňa 27.12.2012.

Nezmenené podmienky o nájme aplikačného programového vybavenia boli znovu predĺžené na ďalších 24 mesiacov zmluvou z 31.10.2013.

Na vzorke 18 dodávateľských faktúr v celkovej sume 43 023,74 eur bolo preverené aj dodržiavanie všeobecne záväzných právnych predpisov pri hospodárení s finančnými prostriedkami v oblasti IKT. Preverená suma predstavovala 16,7 % z hodnoty všetkých výdavkov týkajúcich sa oblasti IKT v kontrolovanom období.

Kontrolou nebol zistený nesúlad medzi požadovaným a skutočným stavom.

3. Dodržiavanie všeobecne záväzných predpisov pre oblasť IS verejnej správy

DFNsP BB je v zmysle § 3 ods. 3 písm. e) zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 275/2006 Z. z.“) povinnou osobou, ktorá je povinná vypracovať a aktualizovať Koncepciu rozvoja informačných systémov verejnej správy.

DFNsP BB mala vypracovanú Koncepciu rozvoja informačných systémov zo dňa 16.11.2011. Ako povinná osoba spravovala a prevádzkovala IS verejnej správy a podľa § 3 ods. 4 písm. i) zákona č. 275/2006 Z. z. bola povinná zabezpečiť, aby bol IS v súlade s výnosom Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy (ďalej len „výnos MF SR č. 55/2014 Z. z.“),

V oblasti prevádzky a správy IKT mala DFNsP BB prijaté dva interné predpisy, a to smernicu č. 2/2014 – „Bezpečnostná politika Detskej fakultnej nemocnice s poliklinikou Banská Bystrica“ (ďalej len „bezpečnostná politika“) a smernicu č. 1/2014 - Bezpečnostný projekt s účinnosťou od 01.04.2014 (ďalej len „bezpečnostný projekt“). Uvedené interné

predpisy nezohľadňovali niektoré ustanovenia výnosu MF SR č. 55/2014 Z. z., avšak zohľadňovali odporúčacie štandardy a dobrú prax v oblasti prevádzky IS.

Kontrolou bolo zistené porušenie výnosu MF SR č. 55/2014 Z. z. najmä tým, že DFNsP BB nepostupovala v súlade s:

- § 15 najmä písm. c) a f), keď obsah jej webového sídla nebol v súlade s uvedeným ustanovením,
- § 26 písm. b), nakoľko nepoužívala e-mailové adresy používateľov bez diakritiky pred deliacim znakom @ v tvare „meno.priezvisko“,
- § 29 písm. a), bodu 10, nakoľko nemala určený rozsah a periodicitu auditu informačnej bezpečnosti,
- § 29 písm. f), nakoľko nemala určenú konkrétnu zodpovednosť za jednotlivé aktíva,
- § 29 písm. g), nakoľko nemala určené privilegované roly, bezpečnostné požiadavky na jednotlivé privilegované roly a určené, ktoré používateľské roly nie je možné navzájom zlúčiť (privilegovanými používateľskými rolami sú najmä správca systému, operátor, používateľ, audítor a programátor),
- § 41 písm. a), nakoľko v niekoľkých vstupoch do IS DFNsP BB nebola zavedená identifikácia používateľa a následná autentizácia.

Kontrolovaný subjekt mal v súlade so zákonom č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 122/2013 Z. z.) vypracovaný bezpečnostný projekt.

V kapitole B - Informačné systémy bola uvedená len informácia, kto vedie evidenciu IS a prílohu č. 1 tvorili jednotlivé evidenčné listy IS, ale nebol uvedený názov IS, na ktorý sa bezpečnostný projekt vťahuje.

Kontrolovaný subjekt tým nepostupoval v súlade s § 5 ods. 1 písm. a) vyhlášky Úradu na ochranu osobných údajov SR č. 164/2013 Z. z. zo dňa 13.05.2013, podľa ktorého by mal bezpečnostný projekt obsahovať názov IS, na ktorý sa vzťahuje.

V zmysle § 21 ods. 1 zákona č. 122/2013 Z. z. sa fyzická osoba stáva oprávnenou osobou dňom jej poučenia. V zmysle § 4 ods. 2 písm. e) uvedeného zákona je oprávnenou osobou každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení podľa § 21 uvedeného zákona.

Poučení musia byť všetci zamestnanci vrátane sanitára, pomocného pracovníka v zdravotníctve, upratovačky, zamestnanca práčovne aj údržbára, ak prichádzajú do styku s osobnými údajmi.

V interných smerniciach kontrolovaného subjektu sa objavoval aj výraz „oboznámená osoba“, pričom v zákone č. 122/2013 Z. z. taký pojem zavedený nie je. Niektoré osoby boli preto poučené ako oboznámené osoby, nie ako oprávnené osoby.

Poučenie neobsahovalo dostatočne rozpracovaný rozsah oprávnení, popis povolených činností a podmienky spracúvania.

4. Prevádzka IS verejnej správy

DFNsP BB v kontrolovanom období využívala pre svoju činnosť najmä nemocničný IS (ďalej len „NIS“), ktorý bol z hľadiska činnosti kontrolovaného subjektu kľúčový. Tento systém bol prepojený s röntgenovým IS (ďalej len „PACS“) súvisiacim s vytváraním digitálnych röntgenových snímok. Obidva systémy využívala v kontrolovanom období DFNsP BB na základe zmlúv o poskytovaní služieb podpory pre aplikačné programové vybavenie uzavretými s rovnakým dodávateľom.

Na činnosti súvisiace s ekonomikou kontrolovaného subjektu bol využívaný ekonomický IS a mzdový IS.

Zamestnanci DFNsP BB disponovali v kontrolovanom období čipovou kartou, prostredníctvom ktorej mali pridelené práva v rámci prístupového IS zabezpečujúceho vstup do jednotlivých miestností DFNsP BB v rozsahu pre nich potrebnom. Karta bola využívaná aj v súvislosti s dochádzkovým IS, ktorý monitoroval pohyb zamestnancov a výstupy z neho boli podkladom pre mzdový IS.

Oblasť IKT mala DFNsP BB od 01.04.2014 upravenú v dvoch základných interných predpisoch, povinnosť vypracovania týchto dokumentov vychádzala z platnej legislatívy.

Podľa výnosu MF SR č. 55/2014 Z. z. je štandardom pre riadenie informačnej bezpečnosti vypracovanie a schválenie bezpečnostnej politiky povinnej osoby, ktorou je podľa zákona 275/2006 Z. z. aj kontrolovaný subjekt. V uvedenom výnose je vymedzený obsah tejto bezpečnostnej politiky a povinnosť jej vypracovania bola platná pre celé kontrolované obdobie.

DFNsP BB vypracovalo bezpečnostnú politiku dňa 31.03.2014 s účinnosťou od 01.04.2014. Bezpečnostná politika obsahovala hlavne základné bezpečnostné ciele, osoby zodpovedné za podporu bezpečnostnej politiky v organizácii, manažment rizík pre oblasť informačnej bezpečnosti a spôsob ochrany IS. Bezpečnostná politika obsahovala aj popis opatrení, ako aj kontrolu a postup pri zlyhaní týchto opatrení.

Tým, že DFNsP BB vypracovala bezpečnostnú politiku až dňa 31.03.2014, nepostupovala v súlade s § 28 písm. a) výnosu MF SR č. 312/2010 Z. z. o štandardoch informačných systémov verejnej správy účinného do 14.03.2014, podľa ktorého mal mať kontrolovaný subjekt ako povinná osoba vypracovanú bezpečnostnú politiku počas celého kontrolovaného obdobia.

Súlad uvedených interných smerníc kontrolovaného subjektu bol detailne preverený v rámci bodu č. 3 tohto protokolu.

Väčšina oblastí upravených v bezpečnostnej politike odkazovala na druhý nosný dokument týkajúci sa oblasti informačných technológií (ďalej len „IT“), zameraný na bezpečnosť IS z hľadiska ochrany osobných údajov – bezpečnostný projekt.

Bezpečnostný projekt upravoval najmä základné bezpečnostné ciele, špecifikáciu technických, organizačných a personálnych opatrení a definovanie možných rizík.

Súčasťou bezpečnostného projektu bola aj analýza bezpečnosti IS z hľadiska jeho zabezpečenia pred možnými hrozbami, ako aj definovanie oprávnení konkrétnych zamestnancov, spôsob, forma a periodicita kontrolných činností zameraných na bezpečnostné opatrenia, ale aj definovanie havarijného stavu a postup pri vzniku takéhoto stavu, vrátane preventívnych opatrení.

Prílohami bezpečnostného projektu boli evidenčné listy jednotlivých IS a harmonogram zálohovania údajov z nich, postupy pri reinštalácii serverov, vzor poučenia oprávnenej osoby a tiež zoznam prístupov do počítačovej siete DFNsP BB.

Zálohovanie údajov z IS DFNsP BB sa v kontrolovanom období vykonávalo na troch úrovniach, a to na serveri, na virtuálnom serveri a na páskových jednotkách.

Prevádzkové zálohy na server sa ukladali na každodennej báze vždy v nočných hodinách. Zálohovanie transakčných logov NIS prebiehalo každých 30 minút.

Vytvorené zálohy sa priebežne ukladali na páskové jednotky, ktoré boli každý týždeň fyzicky ukladané vedúcim oddelenia IT do trezoru v pokladni DFNsP BB. Funkčnosť týchto páskových jednotiek bola priebežne testovaná.

V priebehu kontrolovaného obdobia nedošlo k havarijnému stavu, ktorý by si vyžiadal obnovu údajov v dôsledku ich straty. Testy obnovy údajov boli vykonávané priebežne vedúcim oddelenia IT na virtuálnych serveroch.

DFNsP BB v kontrolovanom období nezavádzala do produkčného prostredia žiadny nový IS s výnimkou nového modulu týkajúceho sa ľudských zdrojov. Vzhľadom na dôležitosť tohto modulu prebiehali v januári 2013 všetky procesy súbežne v novom aj pôvodnom IS. Nový modul bol zavedený do ostrej prevádzky až po porovnaní a vyhodnotení výsledkov z obidvoch modulov. V súvislosti so zavádzaním nového modulu do prevádzky bola vypracovaná dokumentácia o príprave testovania, ako aj o vyhodnotení jeho bezproblémového priebehu.

Za zástupcu zodpovedného za bezpečnosť IS a zavádzanie postupov pri ich aktualizácii bol menovaný na základe menovacieho dekrétu vedúci oddelenia IT.

Kontrola bola zameraná aj na rizikové oblasti špecifikované pri rizikovej analýze vykonanej formou samohodnotenia DFNsP BB v roku 2013. Analýzou súčasného stavu bolo zistené, že koncepcia, riadenie procesov a organizácia v oblasti IT už v súčasnosti zohľadňuje implementáciu niektorých štandardných metodík.

Oblasť riadenia rizík bola formalizovaná a rovnako boli jasne definované opatrenia na elimináciu týchto rizík. Na úrovni celej organizácie existoval formalizovaný vnútorný kontrolný systém, ktorý bol pravidelne dokumentovaný. Zamestnanci organizácie boli vyškolení v oblasti informačnej bezpečnosti a boli o nej pravidelne informovaní.

V oblasti aplikácií IS DFNsP BB používala štandardný softvér, ktorý bol počas kontrolovaného obdobia modifikovaný len minimálne. Dôležité aplikácie mali svoje testovacie prostredie, ktoré bolo oddelené od produkčnej prevádzky.

Oblasť prístupu k údajom a definovanie prístupových práv, ako aj oblasť zálohovania údajov z IS, bola tiež v kontrolovanom období formalizovaná.

5. Bezpečnosť IS verejnej správy

Bezpečnosť IS je ochrana IKT a všetkého, čo s nimi súvisí pred akýmkoľvek neštandardným zásahom zvonku alebo zvnútra systému. Je definovaná ako schopnosť siete alebo IS ako celku odolať s určitou úrovňou spoľahlivosti náhodným udalostiam, alebo nezákonnému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov a súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a systémov.

Do IS využívaných DFNsP BB sa zamestnanci, ktorí mali pridelené právo vstupu do príslušného IS, prihlasovali pod svojim menom a zadaním hesla, ktorého štruktúra a periodicita jeho zmien bola štandardizovaná. Prístup do konkrétneho IS vyžadoval pri prihlásení zamestnanca aj ďalšie heslo.

Každý zamestnanec mal prostredníctvom doménového radiča pridelené do systému len také práva, aké súviseli s náplňou jeho pracovnej činnosti. Kontrola prístupov bola vykonaná preverením záznamov na jednom z modulov za vybrané obdobie.

Kontrolou bola preverená aj dokumentácia týkajúca sa pridelenia a zrušenia prístupových práv pri vzniku a ukončení pracovného pomeru vybraných zamestnancov v kontrolovanom období. Prístupové práva boli novým zamestnancom prideľované spolu s e-mailovým kontom na základe žiadanky o ich zriadenie a týkali sa len vstupu do IS súvisiacich s pracovnou náplňou zamestnanca. Odoberanie prístupových práv sa realizovalo v rámci vyrovnania záväzku zamestnanca a bolo formalizované v rámci výstupného listu.

Zamestnanci s presne definovanými prístupovými právami boli v kontrolovanom období zaškolení a informovaní o práci s IT z hľadiska bezpečnosti ich využívania. V kontrolovanom období boli povinní riadiť sa bezpečnostnými zásadami vyplývajúcimi zo súvisiacich interných predpisov a ich prístup v rámci využívania IT bol obmedzený.

Do IS DFNsP BB mali v kontrolovanom období s výnimkou zamestnancov nemocnice prístup aj tretie osoby, ktorých účasť upravoval výnos MF SR č. 55/2014 Z. z.

Riziká súvisiace so vstupom tretích strán do IS boli upravené v bezpečnostnej politike, v ktorej bola definovaná povinnosť pridelenia len takých prístupových práv, ktoré tretia strana potrebuje na plnenie práv a povinností vyplývajúcich zo zmluvného vzťahu a ich odobratie v prípade ukončenia zmluvné vzťahu. Súčasťou sprístupnenia údajov z IS bola aj zmluvná povinnosť poučenia zamestnancov, ktorí prichádzajú do styku s osobnými údajmi.

Prístup v rozsahu potrebnom pre činnosti vyplývajúce zo zmlúv uzatvorených s každým dodávateľom bol v kontrolovanom období pridelený v súvislosti so servisom IS využívaných na základe nájmu aplikačného programového vybavenia, ale aj v súvislosti s poskytovaním služieb podpory pre NIS a systém PACS. Práva a povinnosti týkajúce sa ochrany osobných údajov a bezpečnosti IS súvisiace s prístupom dodávateľov boli upravené v zmluvách s každým z týchto dodávateľov.

Rovnako boli upravené aj mandátne zmluvy s dvomi fyzickými osobami, v ktorých bol upravený ich prístup do IS súvisiaci s vykonávaním konziliárnych činností a klinickej logopédie pre DFNsP BB ako mandanta.

Údaje z IS DFNsP BB boli umiestnené v dvoch serverových miestnostiach. Prvá miestnosť sa nachádzala na prvom poschodí a nachádzali sa v nej servery IS PACS. Druhá miestnosť, ktorá bola vytvorená v dôsledku nepostačujúcich kapacít pôvodnej miestnosti len za účelom zálohovania údajov z IS, sa nachádzala na štvrtom poschodí a nachádzali sa v nej servery ostatných IS.

Obidve miestnosti sa nachádzali nad povrchom zeme a nebol do nich možný prístup z exteriéru budovy. Z tohto dôvodu neboli na oknách týchto miestností namontované mreže. Ani jedna z miestností, rovnako ako aj samotný vstup do budovy, nebola zabezpečená recepciou, prípadne bezpečnostnou službou. Jediným bezpečnostným prvkom zamedzenia vstupu neoprávnených osôb bolo zamykanie dverí na štvrtom poschodí a zablokovanie prístupu výťahom po pracovnom čase.

Vstup do miestností bol zabezpečený požiarnymi dverami so zámkom. Kľúče od tejto miestnosti mali len traja zamestnanci oddelenia IT. Vstup do miestností nebol žiadnym spôsobom zaznamenávaný a nebol ani monitorovaný kamerovým systémom.

V obidvoch miestnostiach bola nainštalovaná klimatizačná jednotka, v prípade jej výpadku boli všetky skrine, v ktorých boli servery umiestnené, vybavené ventilátormi. Miestnosti boli ďalej vybavené dymovým senzorom, hasiacimi prístrojmi a v prípade výpadku elektrickej energie aj záložným zdrojom energie.

V kontrolovanom období nenastala situácia, ktorá by ohrozila bezpečnosť IS DFNsP BB alebo nepretržitý chod ich prevádzky.

Protokol o výsledku kontroly vypracovali dňa 09.12.2014

Ing. Marián Koreň
vedúci kontrolnej skupiny

Ing. Martina Gallasová
členka kontrolnej skupiny

Ing. Ján Kúdola
člen kontrolnej skupiny

Ing. František Žabka
člen kontrolnej skupiny

S obsahom protokolu o výsledku kontroly bola oboznámená dňa 12.12.2014

Ing. Marianna Hoghová
riaditeľka DFNsP BB