

# NAJVYŠŠÍ KONTROLNÝ ÚRAD SLOVENSKEJ REPUBLIKY

Číslo poverenia: 1048/01  
Zo dňa: 23.09.2014

Počet výtlačkov: 2  
Výtlačok číslo: 1  
Počet strán: 18  
Počet príloh: 0



## PROTOKOL

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

**Univerzitná nemocnica L. Pasteura Košice**

Košice november 2014

Zhrnutie:

Najvyšší kontrolný úrad Slovenskej republiky v spolupráci so Švajčiarskym federálnym kontrolným úradom vykonal v marci 2013 rizikovú analýzu informačno-komunikačného prostredia vo vybraných nemocniciach SR. 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 NKÚ SR do plánu kontrolnej činnosti na rok 2014 zahrnul kontrolu hospodárenia a ochrany aktív v oblasti informačno-komunikačných technológií vo vybraných nemocniciach.

Kontrola bola vykonaná v súlade so zákonom o NKÚ SR a boli uplatňované medzinárodné štandardy najvyšších kontrolných inštitúcií ISSAI.

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.

Pri kontrole sa používala najmä technika preverovania účtovných dokladov, výstupov z informačných systémov a dokumentácia k evidencii a nakladaniu s majetkom štátu. Výber vzorky bol realizovaný neštatistickou metódou úsudku kontrolóra.

Preverením prírastkov a úbytkov dlhodobého hmotného a dlhodobého nehmotného majetku Univerzitnej nemocnice L. Pasteura Košice v oblasti informačno-komunikačných technológií v kontrolovanom období nebol zistený rozdiel medzi požadovaným a skutočným stavom. Nadobudnutý majetok bol zaradený do evidencie majetku nemocnice. V oblasti informačno-komunikačných technológií bol vyradený iba morálne a funkčne zastaraný majetok.

UNLP Košice bola v zmysle zákona č. 275/2006 Z.z. o informačných systémoch verejnej správy povinnou osobou a bola povinná vypracovať koncepciu rozvoja informačného systému verejnej správy. Nemocnica tým, že nevypracovala koncepcie rozvoja informačného systému verejnej správy nekonala v súlade uvedeným zákonom.

Preverením vybraných štandardov pre informačné systémy verejnej správy bolo zistené, že nemocnica mala v interných materiáloch vypracované základné pravidlá pre zálohovanie údajov. Taktiež nemocnica nezabezpečila vypracovanie plánov na zachovanie kontinuity pozostávajúcich z havarijných plánov a plánov na obnovu činnosti. V rozpore so štandardami pre informačné systémy verejnej správy nemocnica nemala menované osoby zodpovedné za informačnú bezpečnosť a správu jednotlivých aktív nemocnice. Dodávatelia, ktorí vykonávali pre nemocnicu činnosti vyplývajúce zo zmluvných vzťahov, boli poučení o schválenej bezpečnostnej politike nemocnice. Povinnosti zamestnancov nemocnice vyplývajúce z bezpečnostnej politiky neboli uvedené v pracovných zmluvách. Nebol dodržaný štandard pre tvar e-mailových adries používateľov informačného systému verejnej správy.

Nedodržaním vyššie uvedených štandardov pre informačné systémy verejnej správy nemocnica porušila zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy.

Komplexný nemocničný informačný systém aj personálno-mzdový systém bol tvorený z jednotlivých modulov podľa špecializácie, technickú prevádzku zabezpečoval odbor informatiky. Prístup tretích strán do informačných systémov bol realizovaný na základe dvoch zmlúv o podpore a servise. V zmluvách boli dohodnuté základné bezpečnostné požiadavky pre poskytovanie služieb vyplývajúcich z uvedených zmlúv.

Kľúčové komponenty nemocničného informačného systému (servery, digitálne archívy, aktívne sieťové komponenty,...) mala nemocnica umiestnené vo vyhradených priestoroch troch serverovní s primerane zabezpečeným vstupom. Rizikom fyzického zabezpečenia boli technické rozvody vody v priestoroch serverovní.

Odporúčania na riešenie zistených nedostatkov:

1. Sprehľadniť evidenciu informačno-komunikačných prostriedkov zavedením štandardizovaného označenia v analytickom členení.
2. Dôsledne dodržiavať interné predpisy.

Podľa poverenia predsedu NKÚ SR č. **1048/01** z 23.09.2014 vykonali:

RNDr. Marcel Kudláč, vedúci kontrolnej skupiny

Ing. Ján Kúdola, člen kontrolnej skupiny

Ing. Ivan Valent, 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, správy a ochrany aktív v oblasti informačno-komunikačných technológií vo vzťahu k zabezpečeniu a ochrany aktív IKT na základe výsledkov rizikovej analýzy.

Kontrola bola vykonaná v čase od 07.10.2014 do 26.11.2014 v

**Univerzitnej nemocnici L. Pasteura Košice,  
Rastislavova 43, 041 90 Košice-Juh, IČO 00606707**

(ďalej len „UNLP Košice“, „nemocnica“ alebo „kontrolovaný subjekt“) za kontrolované obdobie rokov 2012-2014, v prípade potreby 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:

Informačný systém (ďalej len „IS“) je funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov, ktoré sú súčasťou IS alebo ktoré informačnému systému poskytuje iný IS.

Informačným systémom verejnej správy (ďalej len „ISVS“) je IS v pôsobnosti povinnej osoby ako správcu podporujúci služby verejnej správy, služby vo verejnom záujme a verejné služby.

Informačná činnosť je získavanie, zhromažďovanie, spracúvanie, prístupňovanie, poskytovanie, prenos, ukladanie, archivácia a likvidácia údajov.

Informačno-komunikačná technológia/ technika (ďalej len „IKT“) sú technológie, ktoré umožňujú elektronicky zaznamenávať, uchovávať, vyhľadávať, spracovávať, prenášať a šíriť informácie. Podľa Európskeho strediska pre rozvoj odborného vzdelávania ide teda o druh informačnej a komunikačnej technológie a techniky používanej v rôznych odvetviach a činnostiach.

Vzhľadom k technologickému pokroku, aktuálnej situácii a implementácii najnovších technických prostriedkov, prístrojov a technológií do oblasti zdravotníctva, sa kontrolná skupina zaoberala tými prostriedkami IKT, ktoré bezprostredne súvisia so spracovaním, prenosom, ukladáním a archiváciou už získaných zdravotníckych informácií a ich následným používaním. Z uvedeného je vyčlenená tzv. zdravotnícka technika, ktorej primárnym cieľom je informácie elektronickým spôsobom získať.

UNLP Košice bola zriadená v roku 1990 a od 01.01.1991 sa stala štátnou rozpočtovou organizáciou s názvom „Fakultná nemocnica Košice“ so sídlom v Košiciach. Od svojho vzniku prešla nemocnica viacerými zmenami. S účinnosťou od 01.01.1992 sa zmenilo financovanie z rozpočtovej na príspevkovú organizáciu a od 06.07.1993 došlo k zmene názvu na „Fakultná nemocnica L. Pasteura“.

Rozhodnutím Ministerstva zdravotníctva SR (ďalej len „MZ SR“) zanikla 31.12.2004 štátna príspevková organizácia Fakultná nemocnica s poliklinikou, Trieda SNP 1, Košice zlúčením s Fakultnou nemocnicou L. Pasteura. K 01.01.2005 prešiel všetok hnutel'ný a nehnuteľný majetok a finančné prostriedky v správe Fakultnej nemocnice s poliklinikou v rozsahu účtovnej závierky so stavom k 31.12.2004 a delimitačných protokolov do správy Fakultnej nemocnice L. Pasteura.

Rozhodnutím MZ SR zo 17.06.2010 bol zmenený názov kontrolovaného subjektu na „Univerzitná nemocnica L. Pasteura Košice“ s účinnosťou od 01.07.2010.

UNLP Košice je druhou najväčšou slovenskou nemocnicou a poskytuje vysokokvalitnú zdravotnú starostlivosť nielen pre pacientov z Košického kraja, ale v špecifických odboroch pre celý východoslovenský región. Nemocnica má dve pracoviská – Rastislavova 43 a Trieda SNP 1. Jej pracoviská tvoria centrá, ústavy, kliniky, oddelenia a ambulantné pracoviská. Poskytuje široké spektrum zdravotníckych výkonov hradených z verejného zdravotného poistenia a tiež služby nad rámec verejného zdravotného poistenia. Je výučbovou základňou pre Lekársku fakultu Univerzity Pavla Jozefa Šafárika v Košiciach.

UNLP Košice vykonáva predmet svojej činnosti v zmysle zákona č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, na základe platného rozhodnutia Košického samosprávneho kraja o povolení prevádzkovať zdravotnícke zariadenie a lekáreň, a živnosti. Svoju činnosť UNLP Košice vykonáva na základe zákona č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a v súlade s príslušnými právnymi predpismi.

UNLP Košice hospodári podľa rozpočtu nákladov, výnosov a výsledku hospodárenia. Zároveň realizuje v súlade so živnostenskými listami podnikateľskú činnosť, ktorej finančné efekty využíva predovšetkým na podporu skvalitnenia poskytovanej zdravotnej činnosti.

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

### **1.1 Evidencia, prírastky a úbytky dlhodobého hmotného a nehmotného majetku.**

Evidencia dlhodobého hmotného a nehmotného majetku bola vedená na oddelení správy majetku UNLP Košice. UNLP Košice mala spracovaný interný predpis „IN-13 Evidencia, oceňovanie, odpisovanie, vyradovanie, likvidácia majetku a nakladanie s hnutel'ným majetkom štátu“.

Kontrolou bolo zistené, že v kontrolovanom období boli v oblasti IKT zaevidované prírastky majetku, ktoré tvoril predovšetkým novoobstaraný dlhodobý hmotný majetok (sieťové komponenty, servery a pracovné stanice) a dlhodobý nehmotný majetok (aplikačné programové vybavenie - predovšetkým moduly komplexného nemocničného informačného systému (ďalej len „KNIS“).

Novoobstaraný majetok bol po obstaraní a prevzatí do užívania zaradený do evidencie majetku v primeraných lehotách.

Hmotný majetok bol odpisovaný metódou rovnomerného odpisovania v IS Navision pričom účtovné odpisy sa rovnali daňovým. V uvedenej oblasti neboli na vybranej vzorke kontrolou zistené nedostatky.

## **1.2 Inventarizácia majetku, záväzkov a rozdielu majetku a záväzkov**

Inventarizácia majetku, záväzkov a rozdielu majetku a záväzkov bola vykonaná k 31.12.2012 na základe príkazu riaditeľa UNLP Košice č. 82/2012 vydaného 10.10.2012.

V zmysle zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov (ďalej len „zákon o účtovníctve“) v znení neskorších predpisov a internej normy IN-08 Inventarizácia majetku a záväzkov bola inventúra inventúra vykonaná po jednotlivých úsekoch v období od 01.11.2012 do 31.12.2012.

Inventarizácia majetku, záväzkov a rozdielu majetku a záväzkov v oblasti IKT za rok 2013 bola vykonaná na jednotlivých strediskách kontrolovaného subjektu k 31.12.2013 na základe príkazu riaditeľa UNLP Košice č. 28/2013 z 02.10.2013. Výsledky inventarizácie majetku, záväzkov a rozdielu majetku a záväzkov k 31.12.2013 boli prerokované na zasadnutí Ústrednej inventarizačnej komisie 21.01.2014. Inventúrou zistené prebytky, ktoré získala UNLP Košice darom, boli zaevidované do účtovnej evidencie majetku.

Vzhľadom k termínu kontroly bola inventúra za rok 2014 v priebehu výkonu.

Kontrolou dokumentácie z inventarizácie majetku a záväzkov v oblasti IKT neboli zistené nedostatky.

## **1.3 Správa aktív IKT**

Súčasťou aktív sú v zmysle bezpečnostnej politiky IKT zahrnuté:

- Hardvér (servery, digitálne archívy, pracovné stanice, PC a notebooky, tlačiarne a multifunkčné zariadenia, ďalšie sieťové komponenty), dátové nosiče, komunikačné prostriedky,
- softvér (informačné systémy, aplikačné programy, operačné systémy),
- optické a metalické siete,
- informácie/ dáta - dokumenty, databázy, zálohy, nastavenia, záznamy,
- budovy a ich vybavenia,
- osoby (osoby zodpovedné za správu majetku IKT, vlastníci údajov a aplikácií).

V zmysle § 3 ods.1 písm. e) zákona č. 122/2013 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov bola UNLP Košice povinnou osobou, ktorá prevádzkovala a spravovala ISVS.

Za účelom spracovania personálnej a mzdovej agendy zamestnancov UNLP Košice prevádzkovala aj personálny a mzdový informačný systém.

Za správu prostriedkov IKT bolo v UNLP Košice zodpovedné oddelenie informatiky. Jednotliví zamestnanci oddelenia mali stanovený popis pracovnej činnosti a pridelené úlohy. Okrem technickej podpory a servisu sa podieľali na nepretržitej informatickej službe, ktorou bola zabezpečená 24 hod. podpora činnosti IKT. Zodpovední zamestnanci oddelenia informatiky boli zároveň zodpovední za systémové IKT prostriedky (sieťové prvky, servery, operačné systémy,...) a aplikačné programové vybavenie na sieťových prvkoch, serveroch.

Za pridelený majetok, ktorý mali zamestnanci evidovaný na svojich evidenčných kartách, boli zodpovední samotní zamestnanci. Pridelený hardvér bol doplnený predinštalovaným operačným systémom (obyčajne vo verzii OEM, Original Equipment Manufacturer) a ďalším programovým vybavením.

## **2 Dodržiavanie všeobecne záväzných právnych predpisov pri hospodárení s finančnými prostriedkami v oblasti informačno-komunikačných technológií**

Finančné prostriedky investované v oblasti IKT boli rozdelené do troch oblastí. Za kontrolované obdobie od 01.01.2012 do 30.09.2014 kontrolovaný subjekt nakúpil, resp. investoval do zhodnotenia operačného a aplikačného programového vybavenia celkom 490 454,71 eur. Z toho najväčšiu položku tvorila položka za KNIS a jeho jednotlivé moduly vo výške 360 322,84 Eur. Súčasne bol odpísaný a vyradený softvér v celkovej sume 32 651,89 eur, ktorý sa už nepoužíval a bol nahradený funkčnými modulmi KNIS-u.

Kontrolovaný subjekt v kontrolovanom období obstaral hardvér a technické vybavenie v celkovej hodnote 1 127 558,20 eur. Najväčšou položkou bol obstaraný súbor PACS digitálny archív a 30 ks PACS pracovnej stanice v celkovej hodnote 1 056 000,00 eur. Sumu 13 067,15 eur kontrolovaný subjekt investoval do dobudovania a technického zhodnotenia optickej a metalickej siete a sieťových komponentov.

Obstarané prístroje a zariadenia boli zaevidované do evidencie majetku aj účtovníctva. Po preskúšaní boli uvedené do prevádzky a k dátumu kontroly boli funkčné.

### **2.1 Dodržiavania hospodárnosti pri vynakladaní finančných prostriedkov na obstaranie a využívanie DHM a DNM**

#### **Obstaranie PACS staníc**

Picture Archiving and Communication System, (ďalej len „PACS“) je systém pracujúci na štandarde DICOM (Digital Imaging and Communications in Medicine), určenom pre manipuláciu, skladovanie, tlač a prenos medicínskych zobrazení/ obrazov. Obsahuje definovaný formát súborov a komunikačného protokolu. Systém umožňuje zdieľanie a archiváciu digitálne spracovanej zdravotníckej dokumentácie - odborných vyšetrení v obrazovej a videosekvenčnej podobe (RTG snímky, vyšetrenie MR, CT, USG, intratelovými kamerami,...). Obrazové informácie sú digitalizované buď priamo použitou zdravotníckou technikou (priama digitalizácia) alebo nepriamo (napr. staršie klasické RTG snímky sa použitím transskriptora digitalizujú do elektronickej podoby). PACS je bezprostredne prepojený a používaný s aplikáciou T3 Centrum (ďalej len „T3C“) pomocou ktorej je možný prenos medicínskych informácií zdravotníckej dokumentácie PACS nielen v rámci UNLP Košice, ale medzi všetkými organizáciami pripojenými na T3C

(v kryptologicky šifrovanej a konverzovanej podobe). Vzhľadom na nutnosť rozlíšenia detailov pri diagnostike boli jednotlivé pracoviská UNLP Košice postupne vybavované PACS pracovnými stanicami s diagnostickými monitormi.

UNLP Košice realizovala v kontrolovanom období investičnú akciu „Urgentný príjem Univerzitnej nemocnice L. Pasteura Košice“ v rámci operačného programu Zdravotníctvo na základe výzvy č. OPZ 2009/1.2/01 Ministerstva zdravotníctva SR, (riadiaci orgán pre Operačný program Zdravotníctvo) na predkladanie žiadostí o nenávratný finančný príspevok „Zabezpečenie rekonštrukcie a modernizácie zdravotníckej infraštruktúry všeobecných nemocníc s prednostným zameraním na liečbu ochorení skupiny 5“ z 29.10.2009. Maximálna výška nenávratného finančného príspevku bola stanovená na 27 000 000,00 eur. V článku 7 písm. d) výzvy bolo stanovené, že

„Žiadateľ/Prijímateľ realizuje maximálne 2 verejné obstarávania, a to jedno verejné obstarávanie na stavebný dozor projektu pri obstarávaní stavebných prác (pokiaľ je zabezpečený ako externá služba) a druhé verejné obstarávanie na všetky ostatné aktivity projektu (hlavné aj podporné), to znamená, že nie je možné rozdeliť predmet obstarávania na stavebné práce, dodávku tovarov (prístrojov, zariadení) alebo poskytovanie služieb.“

Dôsledkom takto pripravenej výzvy bolo, že dodávateľom vysokošpecializovanej zdravotníckej aj nezdravotníckej techniky bol dodávateľ, ktorého primárna oblasť pôsobenia bola stavebná činnosť. Už pri príprave zmluvy bolo zrejmé, že dodanie vysúťážených zariadení bude realizovať prostredníctvom subdodávateľov.

Ako výsledok zadávania nadlimitnej zákazky vo verejnej súťaži vyhlásenej UNLP Košice ako verejným obstarávateľom v Publikačnom vestníku EÚ 2010/S 109-165145 z 08.06.2010 a vo Vestníku verejného obstarávania SR č. 110/2010, z 05.06.2010, pod značkou 03760-MUP, na predmet zákazky: „Urgentný príjem Univerzitnej nemocnice L. Pasteura Košice“ uzavrel kontrolovaný subjekt 05.01.2012 rámcovú kúpnu zmluvu RKZ č. 55/2012 (ďalej len „RKZ“) na 5 790 168,00 eur s DPH so skupinou dvoch dodávateľov. Zmluva bola uzavretá na 24 mesiacov odo dňa účinnosti (deň zverejnenia RKZ v centrálnom registri zmlúv bol 27.01.2012).

Podľa článku III Predmet zmluvy (dodanie tovaru), bod 2. Dodávka tovaru - zdravotnícka technika a vybavenie, položka 3.32 bol predmetom dodania, okrem iného majetku, „PACS digitálny archív 30 prehliadacích staníc pre KÚCH (1 položka)“. V prílohe č. 1 tejto zmluvy bol jednoznačne určený aj typ syngo.plaza, výrobca Siemens AG a cena za PACS súbor vo výške 1 056 000,00 eur s DPH (1x PACS archív + 30x PACS stanica). RKZ bola výsledkom dohodnutej opcie pri investičnej akcii na vybudovanie urgentného príjmu UNLP Košice. Prílohou RKZ bola aj Dohoda o budúcej spolupráci medzi dodávateľom č.1 a subdodávateľom.

Na základe objednávky UNLP Košice č. ZT1400055 z 15.01.2014 boli PACS archív a pracovné stanice PACS (ďalej len „PACS stanice“) fakturované dodávateľom č. 2, faktúrou č. 3287014001 z 27.05.2014. Dodávka bola zaúčtovaná účtovným dokladom č. 1140570004, interné číslo faktúry 20140520315, položka č. 5, CPV33162100-4 ako jeden obstarávaný súbor. Celková fakturovaná suma bola 4 181 568,00 eur s DPH/ 3 484 640,00 eur bez DPH, fakturovaná suma pod položkou č.5 bola 1 056 000,00 eur s DPH (1x PACS archív + 30x PACS stanica). Vo faktúre nebola špecifikovaná jednotková cena jednotlivých pracovných staníc.

PACS stanice boli dodané 23.03.2014 spolu s PACS archívom ako jeden súhrnný balík. Do účtovnej evidencie bol obstaraný majetok zaevidovaný ako samostatný PACS archív a 30 samostatných pracovných dvojmonitorových PACS staníc. V 26 prípadoch boli súčasťou pracovnej stanice PACS monitory MultiSync E231W a MDView 232W. V dvoch prípadoch išlo o kombináciu monitorov MultiSync E231W a MD211C2 a v ďalších dvoch prípadoch o kombináciu MultiSync E231W a NEC MD211C3. Monitory MD211C2 a MD211C3 sú špecializované zobrazovacie zariadenia s certifikátom pre použitie v oblasti medicínskej diagnostiky a zobrazovania.

Pretože vo faktúre č.3287014001 z 27.05.2014, interné číslo faktúry 20140520315, pod položkou č. 5 CPV33162100-4 na dodávku PACS archívu nebola špecifikovaná jednotková cena, pri evidencii obstarávaného majetku bola obstarávacia cena položiek majetku určená na základe emailovej komunikácie z 26.06.2014 medzi zástupcom z odboru nákupu UNLP Košice a oblasťným riaditeľom dodávateľa č. 2 pre Košický a Prešovský kraj. V elektronickej správe oblasťný riaditeľ dodávateľa č. 2 informoval zástupcu nemocnice, že po porade so zástupcom subdodávateľa možno obstarávaciu cenu 1 056 000,00 eur rozdeliť v pomere :

- PACS archív ... 23%, t.j. 242 880,00 eur
  - PACS pracovné stanice (30 ks) ... 77%, t.j. 812 120,00 eur
- t.j. 27 104,00 eur (1/30) pre 1 PACS stanicu

Vzhľadom k tomu, že PACS stanice boli v troch rôznych konfiguráciách, líšili sa kombináciou a typom monitorov v zostave. Pri určení obstarávacej ceny jednotlivých PACS staníc s rozdielnou konfiguráciou UNLP Košice postupovala tak, že percentuálne určený podiel z ceny faktúry získaný od dodávateľa emailovou komunikáciou, predelil počtom všetkých pracovných staníc (30 ks).

Podľa vyjadrenia UNLP Košice č.746/2014-TPÚ z 27.11.2014 nevedel kontrolovaný subjekt doložiť cenu jednotlivých PACS staníc „...pretože celý PACS bol vysúťážený a obstaraný ako celok vrátane servera, SW, pripojenia jednotlivých modalít, PACS staníc a inštalácie“. Zároveň sa UNLP Košice zaviazala vyžiadať od dodávateľa „úplný súpis tovaru a vykonaných prác predmetného PACS-u aj s ich ocenením a na základe toho prehodnotí pomer medzi serverom, SW a jednotlivými stanicami, pretože určenie ceny pracovnej stanice nebolo správne“.

Kontrolovaný subjekt tým, že pri ocenení PACS pracovných staníc nezohľadnil rôznu konfiguráciu staníc, ani iné ďalšie možné náklady súvisiace s jeho obstaraním, a vychádzal iba z percentuálneho podielu z ceny faktúry predeleného počtom staníc, nepostupoval v súlade s § 25 ods.1 písm. a) zákona o účtovníctve.

Takto stanovená cena pre zaradenie uvedeného majetku do účtovnej evidencie sa javí ako cena nie obvyklá, za ktorú by sa obstaral rovnaký alebo porovnateľný majetok.

Preberacie konanie na jednotlivých pracoviskách prebehlo podľa zápisov o zaradení do dlhodobého hmotného majetku v dňoch 07.-11.07.2014.

# Najvyšší kontrolný úrad Slovenskej republiky

**Tabuľka 1: Inventárne a výrobné čísla komponentov PACS staníc**

| <b>Položka DHM</b>    | <b>inv.<br/>č. HP<br/>Z420<br/>WS</b> | <b>výr.č. HP<br/>Z420 WS</b> | <b>inv. č.<br/>monitor<br/>MultiSync<br/>E231W</b> | <b>výr.č.<br/>monitor<br/>MultiSync<br/>E231W</b> | <b>inv. č.<br/>monitor<br/>MDView<br/>232W</b> | <b>výr.č.<br/>monitor<br/>MDView<br/>232W</b> | <b>Obstarávacia<br/>cena<br/>v evidencii<br/>DHM (eur)</b> |
|-----------------------|---------------------------------------|------------------------------|----------------------------------------------------|---------------------------------------------------|------------------------------------------------|-----------------------------------------------|------------------------------------------------------------|
| archív digitálny PACS | 8401                                  | 78AK970                      |                                                    |                                                   |                                                |                                               | 242 880,00                                                 |
| stanica pracovná PACS | 8402                                  | CZC4151RXJ                   | PMR01565                                           | 43323973NB                                        | PMR01566                                       | 43300570TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8403                                  | CZC4151RXF                   | PMR01569                                           | 43324004NB                                        | PMR01570                                       | 43300460TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8404                                  | CZC4151RY1                   | PMR01543                                           | 43324015NB                                        | PMR01544                                       | 3Y300237TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8405                                  | CZC4151RXK                   | PMR01602                                           | 43324022NB                                        | PMR01603                                       | 43300418TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8406                                  | CZC4151RXB                   | PMR01606                                           | 43323995NB                                        | PMR01607                                       | 43300539TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8407                                  | CZC4151RXX                   | PMR01639                                           | 43324172NB                                        | PMR01640                                       | 43300508TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8408                                  | CZC4151RXL                   | PMR01643                                           | 43324031NB                                        | PMR01644                                       | 3Y300238TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8409                                  | CZC4151RXV                   | PMR01647                                           | 43324020NB                                        | PMR01649                                       | 43300536TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8410                                  | CZC4151RXM                   | PMR01651                                           | 43324016NB                                        | PMR01652                                       | 43300544TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8411                                  | CZC4151RY3                   | PMR01655                                           | 43324069NB                                        | PMR01656                                       | 43300537TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8412                                  | CZC4151RXH                   | PMR01659                                           | 43324160NB                                        | PMR01660                                       | 43300540TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8413                                  | CZC4151RY0                   | PMR01663                                           | monitor MD<br>View 232W<br>43300487TW             | PMR01664                                       | 43300500TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8414                                  | CZC4151RXG                   | PMR01667                                           | 43324036NB                                        | PMR01669                                       | 43300490TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8415                                  | CZC4151RX8                   | PMR01671                                           | 43323982NB                                        | PMR01672                                       | 43300505TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8416                                  | CZC4151RY6                   | PMR01675                                           | 43323970NB                                        | PMR01676                                       | 43300457TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8417                                  | CZC4151RXR                   | PMR01679                                           | 43324039NB                                        | PMR01680                                       | 39000511TW<br>monitor<br>MD211C2              | 27 104,00                                                  |
| stanica pracovná PACS | 8418                                  | CZC4151RX9                   | PMR01683                                           | 43324021NB                                        | PMR01684                                       | 43324219NB                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8419                                  | CZC4151RXS                   | PMR01687                                           | 43324010NB                                        | PMR01688                                       | 41001486TW<br>monitor<br>MD211C3              | 27 104,00                                                  |
| stanica pracovná PACS | 8420                                  | CZC4151RXD                   | PMR01691                                           | 43323974NB                                        | PMR01692                                       | 43001590TW<br>monitor<br>MD211C3              | 27 104,00                                                  |
| stanica pracovná PACS | 8421                                  | CZC4151RXT                   | PMR01695                                           | 43323985NB                                        | PMR01696                                       | 39000539TW<br>monitor<br>MD211C2              | 27 104,00                                                  |
| stanica pracovná PACS | 8422                                  | CZC4151RXW                   | PMR01699                                           | 43324268NB                                        | PMR01700                                       | 43300488TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 8423                                  | CZC4151RY5                   | PMR01703                                           | 43324026NB                                        | PMR01705                                       | 43300507TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 11784                                 | CZC4151RXY                   | PMS00548                                           | 43324225NB                                        | PMS00549                                       | 43300541TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 11785                                 | CZC4151RXC                   | PMS00588                                           | 43324035NB                                        | PMS00589                                       | 43300456TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 11786                                 | CZC4151RXZ                   | PMS00612                                           | 43324027NB                                        | PMS00825                                       | 43300489TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 11787                                 | CZC4151RY2                   | PMS00826                                           | 43324030NB                                        | PMS00827                                       | 3Y300231TW                                    | 27 104,00                                                  |
| stanica pracovná PACS | 11788                                 | CZC4151RY4                   | PMS00828                                           | 43324023NB                                        | PMS00829                                       | 43300506TW                                    | 27 104,00                                                  |

## Najvyšší kontrolný úrad Slovenskej republiky

|                                   |       |            |          |            |          |            |                     |
|-----------------------------------|-------|------------|----------|------------|----------|------------|---------------------|
| stanica pracovná PACS             | 11789 | CZC4151RXN | PMS00830 | 43324024NB | PMS00831 | 43300491TW | 27 104,00           |
| stanica pracovná PACS             | 11790 | CZC4151RXQ | PMS00832 | 43324019NB | PMS00833 | 43300571TW | 27 104,00           |
| stanica pracovná PACS             | 11791 | CZC4151RXP | PMS00834 | 43323971NB | PMS00835 | 3Y300244TW | 27 104,00           |
| <b>Stanice PACS spolu</b>         |       |            |          |            |          |            | <b>813 120,00</b>   |
| <b>PACS archív + stanice PACS</b> |       |            |          |            |          |            | <b>1 056 000,00</b> |

Kontrolovaný subjekt nepredložil žiadny iný doklad ku špecifikácii PACS archívu, pretože kompletná dokumentácia k verejnému obstarávaniu tohto majetku bola UNLP Košice 23.10.2013 odovzdaná Úradu pre verejné obstarávanie a do dňa vypracovania protokolu o výsledku kontroly nebol známy výsledok preverenia.

### **3 Dodržiavanie všeobecne záväzných predpisov pre oblasť informačných systémov verejnej správy**

#### **3.1 Preverenie vybraných ustanovení zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy**

UNLP Košice bola v zmysle zákona č. 275/2006 Z.z. o informačných systémoch verejnej správy (ďalej len „zákon o ISVS“) od 1. februára 2010 povinnou osobou, ktorá bola povinná vypracovať a aktualizovať koncepciu rozvoja ISVS. Koncepciu nemala povinnosť predkladať na schválenie Ministerstvu financií SR. Kontrolovaný subjekt na základe vyžiadania nepredložil koncepciu s odôvodnením, že v čase výkonu kontroly bola rozpracovaná. Kontrolovaný subjekt tým, že nevypracoval Koncepciu rozvoja ISVS, porušil § 3a zákona uvedeného zákona.

#### **3.2 Preverenie súladu s výnosom MF SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy**

Kontrolovaný subjekt v niektorých prípadoch nepoužíval štandardizovaný tvar e-mailovej adresy [meno.priezvisko@unlp.sk](mailto:meno.priezvisko@unlp.sk) používateľa pri názvoch osobných e-mailových adries používateľov ISVS. E-mailové adresy v tvare [priezvisko@unlp.sk](mailto:priezvisko@unlp.sk) používajú služobne starší zamestnanci UNLP Košice. Každá takáto adresa má v aplikácii poštového servera vytvorený alias v štandardizovanom tvare.

UNLP Košice nemala dostupnú e-mailovú adresu [info@unlp.sk](mailto:info@unlp.sk) na poskytovanie informácií osobám podľa zákona č. 211/2000 Z.z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov čím porušila § 27 výnosu o ISVS.

Nemocnica tým, že nemala určenú osobu zodpovednú za informačnú bezpečnosť - bezpečnostného správcu, postupovala v rozpore s § 29 písm. c) výnosu o ISVS.

#### **3.3 Preverenie vybraných ustanovení zákona č. 122/2013 Z. z. o ochrane osobných údajov**

Kontrolnej skupine bolo predložené poverenie na výkon dohľadu na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov, podľa ktorého v čase od 10.10.2007 mala nemocnica poverenú zodpovednú osobu.

UNLP Košice mala vypracovaný Bezpečnostný projekt z 03.06.2014. V zmysle § 76 ods. 7 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ochrane osobných údajov“) bol prevádzkovateľ povinný zosúladiť bezpečnostné opatrenia so zákonom o ochrane osobných údajov do deviatich mesiacov odo dňa účinnosti, t.j. do 31.03.2014. Tým, že kontrolovaný subjekt vypracoval Bezpečnostný projekt až 03.06.2014, postupoval v rozpore s § 76 ods.7 zákona o ochrane osobných údajov.

Ďalej bolo kontrolou zistené, že v dokumente Bezpečnostný projekt boli nesprávne definované pojmy, ktoré nekorešpondujú s ustanoveniami zákona o ochrane osobných údajov.

V kontrolovanom období boli v oblasti IKT na kontrolovanom subjekte vykonané dve externé kontroly Úradu na ochranu osobných údajov SR (ďalej len „ÚOOÚ“).

V apríli 2014 vykonal ÚOOÚ kontrolu uchovávaní obrazovej zdravotnej dokumentácie v priestoroch voľne prístupných pacientom a nezabezpečeného prístupu tretích osôb k zdravotnej dokumentácii. Na základe výsledku kontroly UNLP Košice prijala opatrenia na odstránenie zistených nedostatkov, vypracovala bezpečnostný projekt a bezpečnostné smernice podľa zákona o ochrane osobných údajov a realizovala opatrenia, ktorými zabezpečila v predmetnej veci súlad s týmto zákonom.

ÚOOÚ vykonal v júli 2014 kontrolu spracovania osobných údajov pacientov v IS UNLP Košice. Predmetom kontroly bolo preverenie konkrétneho prípadu neoprávneného sprístupnenia osobných údajov zo zdravotnej dokumentácie. Kontrolou nebolo preukázané, že UNLP Košice svojim postupom porušila niektorú z povinností bezpečnosti spracovania osobných údajov.

#### **4 Prevádzka informačných systémov verejnej správy**

V rámci realizácie programových služieb spojených s implementáciou IS pre riadenie ekonomiky UNLP Košice používala organizácia aplikačný program Microsoft Dynamics NAV od dodávateľa č. 3. Jednotlivé moduly IS boli vzájomne prepojené.

KNIS je produkt spoločnosti dodávateľa č. 4 zostavený z vybraných podsystémov integrujúci všetky organizačné zložky nemocnice, t.j. riadenie poskytovania zdravotnej starostlivosti, systém medicínskych informácií a administratívne riadenie nemocnice. Podsystémy KNIS-u môžu pracovať aj samostatne (napr. laboratória, ambulancie) a nezávisle na sebe a klient komunikuje s jednotnou dátovou základňou udržiavanou na serveri prostredníctvom SQL liniek. Spracovanie informácií prebieha v reálnom čase, čo dovoľuje spoľahlivé a rýchle rozhodnutia v ktoromkoľvek okamihu riadenia. Každý podsystém umožňuje zadávať informácie v čase ich vzniku, a tieto sú okamžite prístupné pre ďalších používateľov bez zbytočných medzioperácií. Všetky informácie sú aktuálne v čase a sú k dispozícii iba používateľom s príslušným stupňom oprávnenia, ktorí majú právo s nimi pracovať.

##### **4.1 Organizácia a riadenie prevádzky IKT**

UNLP Košice vykonávala svoju činnosť na dvoch pracoviskách - pracovisko Rastislavova 43 a Trieda SNP 1. Za prevádzku prostriedkov IKT bolo v UNLP Košice zodpovedné oddelenie informatiky. Predmetom činnosti oddelenia bolo predovšetkým

zabezpečenie nepretržitej prevádzky komplexného nemocničného informačného systému a ďalších zdravotníckych informačných systémov, zabezpečenie prevádzky ekonomických a kancelárskych informačných systémov, prevádzka optickej siete a metalických sietí, serverov UNLP Košice, výstavba počítačových sietí, servis PC a tlačiarňí, správa webu unlp.sk a školenie zamestnancov UNLP Košice v oblasti informačných technológií.

Pre oblasť IKT mal kontrolovaný subjekt spracovaných niekoľko interných predpisov, ktoré bezprostredne súviseli s charakterom a povahou činností vykonávaných zamestnancami subjektu.

UNLP Košice mala platnú a účinnú Bezpečnostnú politiku informačno-komunikačných technológií. V nej boli spresnené zásady, kompetencie, zodpovednosti, povinnosti a opatrenia na implementáciu a využívanie bezpečnostnej politiky IKT pre pracovníkov Oddelenia informatiky UNLP Košice spravujúcich informačné systémy UNLP Košice. Bezpečnostná politika IKT sa vzťahovala na celý informačný systém organizácie, vrátane všetkých aplikácií, dát, elektronických služieb a komunikačnej infraštruktúry a mala jasne definované ciele.

V bezpečnostnej politike IKT boli spracované aj základné pravidlá pre personálnu bezpečnosť, fyzickú a objektovú bezpečnosť, komunikačný a prevádzkový manažment, riadenie prístupu a bezpečnostné incidenty (prístup do IS subjektu a postupy v prípade vzniku bezpečnostného incidentu), manažment nepretržitosti činnosti (správca – vedúci OI – zabezpečoval nepretržitosť redundanciou dôležitých aktív (nadbytočná záloha), zálohovanie informácií, vzájomnú zastupiteľnosť správcov, znižovanie rizika výpadku služieb, monitoring bezpečnostných incidentov a včasné varovanie pred nimi, pripravenosť na obnovenie činnosti po havárii IT). UNLP Košice mala ďalej vypracované usmernenie Pravidlá správy elektronickej pošty a zriadenú nepretržitú Informatickú službu.

Na zaistenie primeranej úrovne bezpečnosti aktív UNLP Košice sa využíval manažment rizík. Išlo o sústavnú činnosť riadenú správcom a pozostávajúcu z analýzy a riadenia rizík, ktoré vychádzali najmä z možných dopadov, sily a pravdepodobnosti výskytu hrozieb a ich dopad na aktíva UNLP Košice.

Bezpečnostné smernice predpisovali súbor opatrení slúžiacich na zvýšenie bezpečnostnej úrovne informačného systému. Vychádzali z analýzy bezpečnosti informačného systému a riadili sa vypracovaným bezpečnostným zámerom. Bezpečnostné smernice boli povinní dodržiavať všetci zamestnanci zariadenia UNLP Košice vrátane pracovníkov iných organizácií vykonávajúcich činnosti súvisiace s informačným systémom, k čomu ich zaviazal písomný právny úkon.

#### **4.2 Nepretržitá prevádzka a obnova informačných systémov**

UNLP Košice vytvárala archivačné zálohy a prevádzkové zálohy základných informačných systémov s rôznou periodicitou podľa náročnosti a dôležitosti aplikácie. Údaje IS KNIS boli zálohované nepretržite zrkadlením archívov. Po krátkodobej archivácii na rýchlych diskoch a údaje presunú na disky s pomalším prístupom. Po uplynutí nastaveného časového intervalu od posledného použitia dát sa zálohy dát presúvali na pásku s neobmedzenou dobou archivácie. Za vykonávanie archivácie dát informačného systému bolo zodpovedné oddelenie informatiky.

Pravidelná doba archivácie bola stanovená v bezpečnostnej politike. Zhotovené prevádzkové záložné kópie, kópie archivačnej zálohy a dátové nosiče s licencovaným softvérom na dátových nosičoch boli uložené v uzamykateľnej skrini, ktorá sa nachádzala v serverovni. Druhá kópia archivačnej zálohy bola uložená v inom objekte ako sa nachádzajú technické prostriedky ISVS.

Testy obnovy informačného systému zo zálohy sa realizovali minimálne 1x ročne.

UNLP Košice mala pevne zavedené postupy s počiatočným stanovením a zahrnutím bezpečnostných požiadaviek a schvaľovacieho procesu pre zmenu konfigurácie, zavádzanie nových alebo aktualizáciu a rozširovanie funkcionality IS alebo ich častí. Uvedené podmienky boli zahrnuté v zmluvách na dodávku IS, resp. čiastočných zmluvách pre jednotlivé etapy alebo servisných zmluvách o podpore. V kontrolovanom období sa zmeny bezprostredne dotýkali aplikačného programového vybavenia (doplnenie, upgrade modulov a funkcionalít informačných systémov KNIS a NAV).

Dokumentácia týkajúca sa používania informačných systémov (návod na použitie, manuály, užívateľská príručka) bola zverejnená na intranetových stránkach, administrátorská dokumentácia (návod na správu a prevádzku IS) a prevádzková dokumentácia, ktorou je dokumentácia o architektúre IS alebo jeho časti, jeho konfigurácii a väzbách na existujúce informačné systémy verejnej správy bola k dispozícii na oddelení informatiky.

Na zabezpečenie nepretržitej činnosti a funkčnosti prevádzkovanvej IKT používala UNLP Košice ako pomocnú aplikáciu Nagios. Ide o aplikačný program, ktorý v pravidelných intervaloch overoval dostupnosť jednotlivých základných uzlových bodov prevádzkovanvej siete - sieťový status a v prípade vzniku incidentu, resp. poruchy a následnej nefunkčnosti deklarovaného uzlového bodu automaticky informoval emailom zodpovedného zamestnanca. O incidentoch, poruchách systém Nagios automaticky generoval protokol incidentov, ktorý zároveň aj archivoval.

#### **4.3 Preverenie vybraných rizík zistených rizikovou analýzou najmä v oblastiach riadenie procesov v oblasti IT, implementácie informačných systémov a vnútorného kontrolného systému**

Na základe výsledkov rizikovej analýzy kontrolná skupina vyhodnotila možné riziká v nasledovných oblastiach:

Nemocnica uviedla, že stratégia činnosti organizácie závisí na nových technológiách iba v malej miere, ale dôležité procesy organizácie už používajú tieto technológie. Nutné podotknúť, že nemocnica je priamo závislá na bezprostrednom používaní prostriedkov IKT. Pritom nejde iba o samotnú prevádzku nemocnice, ale predovšetkým o IKT využívané pre prácu s patientskou dokumentáciou (snaha o úplný prechod na elektronickú formu a integrovanie do e-health) a hlavne novinky implementované do zdravotníckej techniky. V ďalšom období možno predpokladať ďalší nárast možností a rozsahu prostriedkov IKT v oblasti zdravotníctva a medicíny.

Koncepcia a riadenie procesov a organizácie v oblasti IT boli vypracované vo vlastnej réžii bez ohľadu na štandardy, s prihliadnutím na potreby a technicko-prevádzkové možnosti kontrolovaného subjektu. V súčasnej dobe bolo možno pozorovať štandardizáciu implementovaných riešení a unifikáciu postupov, ktoré sa postupne zavádzajú. Dostupnosť

zdrojov IKT bola dôležitá pre prevádzku a činnosti podľa zamerania kontrolovaného subjektu. Akceptovateľná dĺžka nefunkčnosti IS/ poruchy závisela od jej charakteru, rozsahu a miesta poruchy. Vzhľadom k spojeniu dvoch pracovísk bola UNLP Košice schopná vzniknutý problém v relatívne krátkom čase vyriešiť a prípadný výpadok funkčne nahradiť alternatívnym riešením.

UNLP Košice mala aktuálny prehľad hlavných komponentov celkovej infraštruktúry. Výhodou bolo používanie monitorovacej aplikácie Nagios. Procesy obstarávania, inštalácie a zmeny v evidencii viedli k aktualizácii prehľadu o infraštruktúre IKT. Istým rizikom bola operatívna evidencia drobného majetku s obstarávacou cenou do 1700,00 eur (kategória drobný majetok do 1700,00 eur), do ktorej spadajú takmer všetky prostriedky IKT (pracovné stanice, PC, notebooky, tlačiarne a multifunkčné zariadenia,...). UNLP Košice nemala v evidencii majetku jednoznačne určenú skupinu do ktorej by všetky takéto prostriedky boli zaradené (napr. zvlášť je v evidencii majetok za pracovisko Rastislavova 43, zvlášť za pracovisko Trieda SNP 1).

Riadenie rizík zameraných na aplikácie bolo čiastočne zdokumentované, ale formalizované riadenie rizík nezahrňovalo celú nemocnicu. Opatrenia na zníženie súvisiacich rizík neboli vždy a jednoznačne formálne definované a identifikovateľné.

Nemocnica mala nastavený vnútorný kontrolný systém pre špecifické oblasti. Ten však nepokrýval každú činnosť nemocnice, ale len parciálne oblasti. Nemocnica mala vypracovaný interný predpis „Systém vnútornej kontroly“ a definovaný trojstupňový systém kontroly (riaditeľ UNLP Košice, oddelenie kontroly a sťažností, odborné referáty podľa organizačného poriadku).

Zamestnanci boli poučení o svojej zodpovednosti za dodržiavanie vnútornej a vonkajšej bezpečnosti informácií. Zamestnanci boli opakovane informovaní o svojich povinnostiach a sú primerane vyškolení. Dodržiavanie povinností týkajúce sa bezpečnosti informácií nebolo pravidelne kontrolované.

Pre účtovníctvo sa používal konfigurovateľný softvér so štandardnými alebo individuálnymi možnosťami programovania. Softvér mal len niekoľko možností nastavenia a obmedzenú možnosť individuálnej úpravy používateľmi prostredníctvom programovania. Zmeny v programovej aplikácii sa realizovali treťou stranou (dodávateľsky) na základe požiadaviek odoslaných prostredníctvom Helpdesk-u. Chyby a nedostatky boli zdokumentované, ich vyriešenie a prípadná aktualizácia bola realizovaná operatívne bez zbytočného zdržania na základe podmienok stanovených v servisnej zmluve.

Prostriedky IKT mali malý počet porúch a výpadkov. Systémy boli často zdvojené a zálohované, prípadné výpadky môžu byť efektívne pokryté ďalšími dostupnými prostriedkami. Normálna prevádzka IT bola zabezpečená oddelením informatiky bez vonkajšej pomoci.

UNLP Košice pri používaných IS nemala možnosť využívať žiadne testovacie prostredie. Aplikácie boli vyvinuté a integrované priamo do produkčného prostredia. Prípadné chyby a požiadavky boli priebežne zapracovávané. Do vývojového prostredia mali prístup iba dvaja zamestnanci oddelenia informatiky. Vývoj a samotné úpravy v programe však nerealizovali, tie boli realizované dodávateľom.

Nemocnica má základnú koncepciu prístupu k údajom, ktorá klasifikuje údaje a definuje prístupové práva užívateľov. O možnostiach prístupov boli jednotliví používatelia informovaní. Pridelovanie prístupových práv bolo formalizované, viackrokové. Uvedený fakt sa podieľal na prvotnom zvýšení stupňa zabezpečenia ochrany osobných údajov zamestnancov a pacientov. Rizikovým faktorom bolo zlyhanie ľudského faktora a sprístupňovanie údajov zamestnancami navzájom.

UNLP Košice mala čiastočne spracované formálne pravidlá pre zálohovanie údajov, ale nie všetky v písomnej podobe. V niektorých prípadoch nebolo špecifikované, ktorý dátový súbor bol zálohovaný, v akom časovom intervale a do akej miery. Externý audit IKT nebol v posledných piatich rokoch vykonaný.

## **5 Bezpečnosť informačných systémov verejnej správy**

Bezpečnosť informačných systémov, alebo aj informačná bezpečnosť, je ochrana IKT a všetkého čo s nimi súvisí pred akýmkoľvek neštandardným zásahom zvonku alebo zvnútra systému. Bezpečnosť IS je definovaná ako schopnosť siete alebo informačného systému ako celku odolať s určitou úrovňou spoľahlivosti náhodným udalostiam, alebo nezákonnému, alebo zákernému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov a súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a systémov. Narušenie bezpečnosti zahŕňa všetky činnosti a zásahy, ktoré zasiahnu systém IKT tak, že je nejakým spôsobom narušená funkčnosť celého systému alebo len niektorých jeho prvkov.

### **5.1 Podmienky logického prístupu do informačných systémov**

Kontrolou bolo preverené riadenie logického prístupu do IS prevádzkovaných UNLP Košice, zabezpečenie identifikácie a autentifikácie užívateľov. Oblasť logického prístupu do IS bola pre používateľov formálne stanovená iba okrajovo a vyplývala z jednotlivých pracovných pozícií zamestnancov. Kontrolovaný subjekt mal formálne stanovené postupy zabezpečujúce logický prístup do IS počnúc pridelením prístupových práv až po ich zablokovanie.

Kontrolou bola preverená správa užívateľských účtov v IS Microsoft Dynamics NAV a IS KNIS, evidencie používateľských účtov a nastavenia prístupových práv. Na základe vykonanej kontroly možno konštatovať, že procesne logický prístup do prevádzkovaných systémov zo strany správcu bol zabezpečený v dostatočnej miere.

V IS KNIS sa spracovávali osobné údaje pacientov. Vstup používateľa a vkladanie akýchkoľvek nových údajov do systému bol automaticky zaznamenávaný. Systém nedovoľoval údaje upravovať, ani vymazať. Takýmto spôsobom systém zabráňoval pozmeňovaniu, resp. úprave zdravotnej dokumentácie pacienta. Každý oprávnený zdravotnícky pracovník mohol do KNIS-u vkladať iba tie údaje, na ktoré mal oprávnenie. Podľa nastavených prístupových práv mali jednotliví zamestnanci prístup k adekvátnej časti patientskej dokumentácie. Podobne, ako pri logovaní zamestnancov, KNIS umožňoval odsledovať pre každého pacienta jednotlivé kroky od zaregistrovania pacienta do systému až do aktuálneho stavu.

Riziko spojené s logickým prístupom do systému bolo z tohto pohľadu orientované skôr na zlyhanie ľudského faktora pri neautorizovanom vstupe používateľa IS (zdieľanie hesla medzi zamestnancami).

## **5.2 Správa administrátorských a užívateľských oprávnení**

Správu administrátorských a užívateľských oprávnení mali primárne v kompetencii a pracovnej náplni dvaja zamestnanci oddelenia informatiky s právami superadministrátora. V oboch IS bola správcovská agenda riešená v dvoch úrovniach prostredníctvom prístupových účtov na SQL serveri príslušného IS a až následného zavedenia oprávneného používateľa niektorých modulov IS a prístupových práv.

Prihlasovanie (logovanie) do systému bolo viazané na používateľské meno a prihlasovacie heslo. História výpisu prihlásení (logovací súbor) nebola v grafickom zobrazení priamo explicitne podporovaná, existovala ale možnosť výpisu logovania pomocou SQL servera.

## **5.3 Prístup tretích strán do informačných systémov**

Kontrolou oblasti prístupu tretích strán do IS prevádzkovaných kontrolovaným subjektom bolo zistené, že do IS Microsoft Dynamics NAV mala tretia strana (dodávateľ č. 3) prístup na základe zmluvy o poskytovaní servisných služieb a podpory. Na základe zmluvy a dodatkov k zmluve mali poverení zamestnanci dodávateľa č. 3 prístup do IS za účelom aktualizácie, dopracovania a doplnenia požadovaných funkcionalít.

Podobne, na základe Zmluvy o dielo mala tretia strana (dodávateľ č.4) prístup do IS KNIS na poskytovanie servisu, dodávky upgradov, updatov a hot-line „Informačného systému FNŠP v napojení na zdravotné poisťovne“ a servis operačného systému SCO Unix, databázy INFORMIX, NFS Vision, textového editora AVI a národnej podpory systému. Vzhľadom k tomu, že dodávateľ č. 4 vyvíjal jednotlivé moduly IS na základe požiadaviek kontrolovaného subjektu, bolo poskytnutie prístupu nevyhnutnou podmienkou funkčnosti celého IS.

Na základe zmluvy bolo nastavené zaistenie takých technických, organizačných a právnych podmienok pre činnosť tretích strán v IS, aby nebola narušená bezpečnosť IS. Prístup tretích strán ku všetkým aktívam IS, alebo umožnenie prístupu tretích strán k takýmto údajom bol zmluvne nastavený tak, aby nebola narušená bezpečnosť IS a bezpečnostná politika povinnej osoby. Prístup do IS mali iba oprávnení zamestnanci dodávateľa. Plnenie bezpečnostných požiadaviek bolo realizované prostredníctvom zmluvne dohodnutých zodpovedných zamestnancov a od podpisu zmluvy doteraz nebol zaznamenaný žiaden incident, alebo podozrenie z neoprávneného prístupu k aktívam IS zo strany dodávateľa.

## **5.4 Fyzická bezpečnosť IKT**

Pracovisko Rastislavova 43 bolo tvorené sústavou samostatných pavilónov čiastočne monitorovaných kamerovým systémom. V areáli pracoviska mal kontrolovaný subjekt dve serverovne s kľúčovými prvkami IKT. Pracovisko Trieda SNP 1 bolo tvorené tzv. monoblokom, v ktorom boli koncentrované všetky lôžkové oddelenia. Monoblok bol chodbami prepojený s budovou polikliniky a Detskej fakultnej nemocnice. V priestoroch pracoviska bola umiestnená jedna serverovňa.

Jednotlivé kľúčové prvky IKT boli štandardne umiestnené v zabezpečených priestoroch, v ktorých je obmedzený voľný pohyb osôb. Priestory serverovni a ďalších dôležitých technických miestností boli zabezpečené viacnásobným zámkom a boli prístupné

iba povolanému obslužnému personálu. Rizikovým faktorom bolo umiestnenie heliportu na streche urgentného príjmu a technické rozvody vody (voda, ústredné kúrenie, kanalizácia) v priestoroch serverovni.

Hlavné prostriedky IKT a dôležité zariadenia zdravotníckej techniky boli zabezpečené pred výpadkom zdroja elektrickej energie náhradnými záložnými zdrojmi. Existujúce záložné kapacity používaných prostriedkov IKT boli vzájomne zálohované na oboch pracoviskách. Prístup do priestorov serverovni a samotný prístup k serverom IS bol okrem fyzického zabezpečenia chránený aj sekundárne, administráciou prístupových práv k jednotlivým prostriedkom IS.

Protokol o výsledku kontroly vypracovali dňa 26.11.2014

RNDr. Marcel Kudláč  
vedúci kontrolnej skupiny

Ing. Ján Kúdola  
člen kontrolnej skupiny

Ing. Ivan Valent  
člen kontrolnej skupiny

Ing. František Žabka  
člen kontrolnej skupiny

S obsahom protokolu o výsledku kontroly bol oboznámený dňa 08.12.2014

MUDr. Ladislav Rosocha, MPH  
riaditeľ Univerzitnej nemocnice L. Pasteura Košice