

## **Vyhodnotenie úloh vyplývajúcich z Pokynu rektora č.1/2014 (čl.4 CIS) a návrh opatrení na odstránenie zistených nedostatkov pri napĺňaní cieľov vnútorného systému kvality**

*(Správa za rok 2015)*

### **I. Prevádzka, bezpečnosť, dostupnosť a rozvoj univerzitnej dátovej siete**

#### **Dokumentácia:**

- a) Smernica rektora č.13/2012 Pravidlá používania a správy dátovej a hlasovej siete TU
- b) Politika informačnej bezpečnosti
- c) Bezpečnostné smernice

#### **Cieľ:**

Univerzitná dátová sieť, pozostávajúca z lokálnych dátových sietí a aktívnych sieťových zaradení, patrí k strategickým aktívam, ktoré zabezpečujú funkčnosť riadiacich a hlavných procesov univerzity. Cieľom je zabezpečiť, aby univerzitná dátová sieť efektívne fungovala a poskytovala nepretržité služby pre manažment, pedagógov, študentov a za-mestnancov pri dodržaní všetkých zásad bezpečnosti.

#### **Úlohy:**

- 1) Zabezpečiť podmienky pre nepretržitú prevádzku a správnu funkčnosť strategických sieťových komponentov univerzitnej siete (Firewall, centrálny prepínač, DNS).

##### **Vyhodnotenie:**

- a) Centrálna správa a servisná podpora strategických sieťových komponentov univerzitnej siete (Firewall, centrálny prepínač, DNS) bola zabezpečená zmluvne, finančne i technicky.
- b) Zvýšila sa fyzická bezpečnosť dvoch centrálnych serverovní inštaláciou protipožiarnych dverí a doplnením monitorovacieho systému do novej serverovne študentského domova.

##### **Sledované indikátory:**

- 5 900 používateľov univerzitnej dátovej siete (zamestnanci a študenti TU) – zaznamenaný pokles o cca 890 v dôsledku poklesu počtu študentov.

##### **Návrh opatrení:**

- a) Udržať kvalitu centralizovanej správy jednotlivých uzlov a zabezpečiť servisnú podporu strategických sieťových komponentov. Realizácia: riaditeľ CIS TU.
- b) Pokračovať v realizácii fyzickej bezpečnosti serverovní TU. Realizácia: riaditeľ CIS TU.

- 2) Monitorovať všetky neoprávnené aktivity a snahy o prienik do univerzitnej siete.

##### **Vyhodnotenie:**

- a) Monitorovací systém bezpečnosti univerzitnej siete bol funkčný a zaznamenával neoprávnené snahy o prieniky do siete TU.
- b) V decembri 2015 bol inštalovaný sieťový hardvérový systém CheckPoint na externý prístup do univerzitnej siete cez Gateway č. 2.

##### **Sledované indikátory:**

- 14 interných neoprávnených aktivít – zaznamenané sťahovanie torrentov (obsahy chránené ako autorské diela) v sieti PdF a študentského domova - vyriešené napomenutím, resp. krátkodobým zablokovaním prístupu k dátovej sieti;
- 64 958 externých neoprávnených aktivít zachytených na úrovni hardvérových zariadení – pokles o 402 prípadov;

- 2 neoprávnené aktivity vyriešené zásahom administrátora siete.

**Návrh opatrení:**

- a) Zabezpečiť prevádzku implementovaného monitorovacieho systému bezpečnosti celej univerzitnej siete udržaním jeho supportu (čerpanie položky Fondu IŠaS). Realizácia: riaditeľ CIS TU.
- b) V súlade s dostupnými finančnými a technickými možnosťami zabezpečiť efektívnu konfiguráciu systému CheckPoint FW. Realizácia: vedúci oddelenia komunikačných sietí CIS TU.

- 3) Realizovať opatrenia na ochranu univerzitnej dátovej siete pred identifikovanými hrozbami.

**Vyhodnotenie:**

- a) Na základe analýzy identifikovaných bezpečnostných hrozieb bola vykonaná revízia spôsobu pripojení externých používateľov (dodávateľa, poskytovateľa supportu) a boli povolené prístupy do univerzitnej siete iba cez bezpečné pripojenie VPN.
- b) Prístup k sieti wifi pre externých používateľov bol vyriešený vytvorením nového SSID pripojenia.

**Sledované indikátory:**

- Počet realizovaných opatrení na ochranu dátovej siete: 3

**Návrh opatrení:**

- a) Realizovať analýzu SSID pripojenia pre bezpečnú autentifikáciu do univerzitnej wifi siete bez nutnosti zverejňovať prístupové heslo. Realizácia: vedúci oddelenia komunikačných sietí CIS TU.

- 4) Monitorovať výpadky hlavných komponentov a nefunkčnosť univerzitnej dátovej siete.

**Vyhodnotenie:**

- b) V roku 2015 nebola zaznamenaná potreba využiť redundantné strategické sieťové komponenty;
- c) Disková úložná kapacita pri zlyhaniach sieťových diskov bola zabezpečená v plnej miere.

**Sledované indikátory:**

1 výpadok metropolitnej siete SANET – nefunkčnosť univerzitnej siete cca 32 hodín;

2 ohlásené prerušenia funkčnosti univerzitnej siete – údržba;

**Návrh opatrení:**

- a) Udržať redundantnosť (duplicitu pre prípad hardvérového výpadku) strategických sieťových komponentov udržaním súčasného zmluvne dohodnutého supportu. Fond IŠaS má v roku 2016 garantovanú položku na supporty strategických sieťových komponentov. Realizácia: riaditeľ CIS TU.
- b) Zabezpečiť dostatočnú úložnú kapacitu na rýchle presmerovanie a dostupnosť všetkých sieťových služieb. V r.2016 je v rozpočte Fondu IŠaS nové diskové pole, ktoré zabezpečí rýchle presmerovanie služieb v prípade hardvérovej chyby na pevnom disku. Realizácia: riaditeľ CIS TU.

- 5) Rozširovať počet trás a posilňovať prenosovú kapacitu dátovej siete.

**Vyhodnotenie:**

- a) Univerzitná sieť TU mala dosiaľ jedno nezálohované pripojenie do siete SANET (rektorát TU - MtF STU na Paulínskej ulici). V roku 2015 bolo realizované záložné pripojenie k sieti SANET (Študentský domov Petra Pázmaňa – budova MtF STU

na Hajdóczyho ulici). Prepojenie rektorát – študentský domov sa stalo majetkom TU.

- b) Podpora a údržba prevádzky komponentov IKT bola organizačne zabezpečená zamestnancami CIS TU.

**Sledovaný indikátor:**

2 nové optické trasy univerzitnej dátovej siete.

**Návrh opatrení:**

- a) V novom komunikačnom uzle dokončiť všetky potrebné sieťové inštalácie (FireWall, aktívne prepínače, prístupové body wifi, UPS) na bezpečnú prevádzku lokálnej dátovej siete a prístup k sieti internet. Financovanie opatrenia je zabezpečené z prostriedkov ŠD. Realizácia: vedúci oddelenia komunikačných sietí CIS TU.

- 6) Zabezpečiť realizáciu opatrení na ochranu univerzitnej siete pred výpadkami elektrickej energie.

**Vyhodnotenie:**

- a) V serverovni Adalbertinum A202 boli doplnené 2 záložné zdroje UPS;
- b) Riešenie reklamačných konaní s distribútorom elektrickej energie Západoslvenská distribučná, a.s.

**Sledované indikátory:**

1 ohlásený výpadok elektrickej energie – bez zistených problémov;

1 neohlásený výpadok elektrickej energie – zničenie 3 ks HDD z diskových polí a pamäťového segmentu FireWall Cisco ASA.

**Návrh opatrení:**

- a) Spracovať plány obnovy činností centrálnych serverovní TU po neplánovaných výpadkoch elektrickej energie Realizácia: riaditeľ a vedúci oddelení CIS TU.

## **II. Prevádzka, dostupnosť webových, e-mailových služieb, univerzitných IS a ochrana osobných údajov**

**Dokumentácia:**

- a) Smernica rektora č.13/2012 Pravidlá používania a správy dátovej a hlasovej siete TU
- b) Bezpečnostný projekt na ochranu osobných údajov
- c) Metodický pokyn CIS č.1/2012 (vrátane Dodatku č.1)

**Cieľ:**

Webové služby, služby elektronickej pošty a univerzitné informačné systémy (UIS) sú nevyhnutnou súčasťou riadiacich procesov (SAP-SOFIA, ISSM, Novell IDM) a hlavných procesov univerzity (MAIS, NetDimensions Suite, EZP, LCMS, DAWINCI, Virtuálna univerzita). Cieľom je zabezpečiť, aby univerzitné informačné systémy mali vysokú mieru dostupnosti z rôznych prostredí s primeranou ochranou osobných údajov v súlade s legislatívou SR a EÚ.

**Úlohy:**

- 1) Zabezpečiť podmienky pre bezpečnú prevádzku a dostupnosť webových služieb a IS univerzity.

**Vyhodnotenie:**

- a) Centrálne UIS boli aktualizované v súlade s legislatívnymi potrebami a schválenými požiadavkami používateľov TU.
- b) Zabezpečená podpora používateľov UIS formou e-mailového Help Desk. Bola spracovaná analýza požiadaviek na informačný systém univerzitného HelpDesk.
- c) Dokončené integračné rozhrania Novell IDM – ESS portál a Novell IDM – LMS.

V sledovanom období bola zabezpečená dostatočná serverová a úložná kapacita na prevádzku 10 univerzitných informačných systémov (UIS), 42 databáz, 45 univerzitných webstránok a množstva webových služieb. Databázy a aplikačné konfigurácie serverov boli pravidelne zálohované. Nebol zaznamenaný žiadny prípad nevratnej straty údajov z UIS.

**Sledované indikátory:**

Počet zmlúv o zabezpečení servisných služieb na UIS: 10 (zvýšenie o 1)

**Návrh opatrení:**

- a) Priebežne zabezpečovať aktualizáciu, údržbu a podporu UIS v spolupráci s externými poskytovateľmi služieb v súlade so supportnými zmluvami. Realizácia: riaditeľ CIS TU.
- b) Otestovať a zaviesť do skúšobnej prevádzky komerčný systém Help Desk. Realizácia: vedúca oddelenia IS CIS TU.
- c) Zabezpečiť spoľahlivú prevádzku všetkých integračných rozhraní a ochranu interných dát. Realizácia: vedúca oddelenia IS CIS TU.

- 2) Zabezpečiť nepretržitosť prevádzky a dostupnosť webových služieb, služieb elektronickej pošty a univerzitných IS z prostredia univerzity i mimo nej.

**Vyhodnotenie:**

- a) Všetky centrálné UIS (aplikačné servery a dátové úložiská) boli premigrované na virtualizovanú infraštruktúru VMware, čím sa zvýšila nepretržitosť ich prevádzky.
- b) Boli spracované postupy na zálohovanie aplikačných serverov metódou snapshot a tiež vytváranie záloh na magnetopáskovú knižnicu systémom NetBackup.

Okrem prípadov výpadkov všetkých UIS v dôsledku prerušenia dodávok elektrickej energie bolo spolu zaznamenaných 11 výpadkov UIS vplyvom zlyhania hardvéru alebo softvérovej poruchy: EVOB (1), EZP (2), BRISK (2), CardPay (2), ASPI (2), NetBackup (2). Najneskoršie obnovenie prevádzky po uvedených výpadkoch nastalo do 18 hodín.

**Sledované indikátory:**

11 vážnych nepredpokladaných výpadkov UIS (nezávisle od výpadkov elektrickej energie)

**Návrh opatrení:**

- a) Dôsledné vyhodnocovanie notifikácií o stave prevádzky centrálnych UIS za účelom včasného zistenia chybných funkcií IS alebo nedostupnosti IS. Realizácia: správcovia UIS CIS TU.
- b) Dodržiavanie metodiky zálohovania aplikačných a dátových serverov na automatizovanej magnetopáskovej knižnici. Realizácia: správca databázy CIS TU.

- 3) Monitorovať všetky neoprávnené aktivity v súvislosti s bezpečnosťou webových služieb, služieb elektronickej pošty a integritou IS.

**Vyhodnotenie:**

- a) Všetci zamestnanci a študenti boli správcami e-mailového servera opakovane informovaní o phishingových útokoch a nebezpečenstve podozrivých príloh obsahujúcich škodlivý kód.
- b) Za neoprávnený prístup k e-mailovej schránke bolo udelené jedno napomenutie externej študentke TU.

Prístup k UIS z externého prostredia rozľahlých internetových sietí (WAN) je obmedzený na pripojenie prostredníctvom bezpečného VPN kanála, kde je zabezpečená jednotná autentifikácia riadená systémom IDM. Neboli zaznamenané žiadne neoprávnené prístupy do UIS integrovaných s IDM. Systém elektronickej pošty Zimbra je dostupný z WAN cez štandardné protokoly a tie umožňujú doručenie rôznych správ, ktoré v mnohých prípadoch môžu byť phishingovými útokmi (podvodné správy zamerané na zistenie používateľských prístupových údajov). Okrem toho priložené skomprimované súbory môžu obsahovať škodlivý kód, ktorý môže zničiť, resp. zakódovať dáta používateľa PC. Správca systému elektronickej pošty niekoľkokrát upozornil všetkých používateľov, aby nikdy nezasielali e-mailom svoje meno a heslo a dôsledne dodržiavali Smernicu rektora TU č.13/2012 a Metodický pokyn CIS č.1/2014.

**Sledované indikátory:**

- a) Počet zaznamenaných phishingových útokov: 12 080 (nárast o 11935)
- b) Počet úspešných phishingových útokov: 55 (nárast o 39)
- c) Počet zachytených nebezpečných príloh: 2610 (nárast o 514 príloh)
- d) Počet úspešne napadnutých (hacknutých) webstránok fakúlt: 5

**Návrh opatrení:**

- a) Dôsledne zabezpečiť informovanosť všetkých zamestnancov a študentov o povinnostiach vyplývajúcich zo Smernice rektora TU č.13/2012 a Metodického pokynu CIS č.1/2014. Realizácia: manažéri jednotlivých súčastí TU.
- b) Zabezpečiť pripojenie všetkých PC do univerzitnej domény a uplatňovať schválenú Smernicu rektora TU č.8/2015. Realizácia: odborní zamestnanci IT na fakultách, hardvérový špecialista CIS TU.

- 4) Zabezpečiť prístup k webovým službám, službám elektronickej pošty a IS univerzity všetkým oprávneným používateľom.

**Vyhodnotenie:**

Všetci používatelia UIS mali zabezpečené osobné prístupové údaje k univerzitným systémom a službám. Prístup oprávnených používateľov k vybraným UIS (MAIS, EZP, ESS portál, DaWinci), k sieťovým službám (VPN, SunRay, PC v učebniach) a k systému elektronickej pošty (Zimbra) je riadený systémom na správu identít Novell IDM. Na prístup k uvedeným systémom má každý oprávnený používateľ univerzity jednotné meno a heslo, ktoré si dokáže spravovať prostredníctvom autentifikačného portálu TU. Prístup k ostatným UIS (BRISK, CardPay, ASPI) je pridelený príslušným správcam systému. V súlade s bezpečnostnými smernicami nesmie používateľ odovzdať svoje prihlasovacie údaje inej osobe.

**Sledované indikátory:**

Počet používateľov jednotlivých UIS:

- a) Systém správy identít Novell IDM – 5 900 (nárast o 100)
- b) Akademický systém MAIS – 5 700 (nárast o 200)
- c) Finančný informačný systém SAP-SOFIA – 65 (zvýšenie o 3)
- d) Zamestnanecký portál VŠ ESS portál – 550 (nárast o 195)
- e) Systém EZP – 4200
- f) E-mailový systém Zimbra1 (zamestnanci) – 500 (pokles o 74)  
Zimbra2 (študenti) – 5 200 (pokles o 77)
- g) Systém spisovej služby BRISK – 60 (pokles o 40)
- h) Knižničný systém DAWINCI – 7 000 (pokles o 200)
- i) Stravovací systém CardPay – 4 253 (nárast o 280)
- j) Systém právnych informácií ASPI – 11 používateľov (nárast o 7)
- k) Webstránky fakúlt – 5 900

**Návrh opatrení:**

Zabezpečiť dodržiavanie Smernice rektora TU č.13/2012 a uznesenia KR TU všetkými zamestnancami a študentami. Realizácia: manažéri jednotlivých súčastí TU.

- 5) Zaznamenávať bezpečnostné incidenty súvisiace s ochranou osobných údajov v IS.

**Vyhodnotenie:**

V súlade so schválenými bezpečnostnými smernicami na ochranu osobných údajov pôsobí na univerzite Rada na ochranu osobných údajov. Jej kompetenciou je riadiť organizačné, technické a personálne procesy súvisiace s ochranou osobných údajov na všetkých súčastiach univerzity. V roku 2015 bolo zriadené Grémium informačnej bezpečnosti (GIB). Ustanovenie Pracovného poriadku o povinnom školení novoprijatých zamestnancov o zásadách práce v UIS a o informačnej bezpečnosti dodržiavali iba univerzitné pracoviská a rektorát TU.

**Sledovaný indikátor:**

Počet zaznamenaných bezpečnostných incidentov súvisiacich s ochranou osobných údajov v IS: 1

**Návrh opatrení:**

- a) Dodržiavať ustanovenia Pracovného poriadku (čl.4 ods.18 a čl.11 ods.5 písm. e) o oboznámení novoprijímaných zamestnancov o informačnej bezpečnosti a oprávnené osoby o zásadách ochrany osobných údajov. Realizácia: personalistky, študijné referentky, školitelia CIS.
- b) Pokračovať v realizácii školení novoprijatých študentov o zásadách práce v UIS a o informačnej bezpečnosti. Realizácia: dekaní fakúlt v spolupráci s CIS TU.

### **III. Služby používateľom systému automatizovanej identifikácie osôb (SAIO)**

**Dokumentácia:**

- a) Smernica rektora č.13/2012 Pravidlá používania a správy dátovej a hlasovej siete TU
- b) Vyhláška rektora č.3/2004 Organizačný a prevádzkový poriadok systému automatizovanej identifikácie osôb (SAIO)

**Cieľ:**

CIS TU poskytuje servisné služby pre držiteľov preukazov TU na svojom stredisku čipových kariet. Cieľom je zabezpečiť komplexné vybavenie požiadaviek študentov a zamestnancov univerzity, ktoré súvisia s podpornými procesmi - využívaním služieb SAIO (preukaz študenta, preukaz zamestnanca, stravovací systém, prístupový systém).

**Úlohy:**

- 1) Vytvoriť materiálne a organizačné podmienky pre prevádzku Strediska čipových kariet (SČK) univerzity.

**Vyhodnotenie:**

SČK má zabezpečené technické a materiálne vybavenie na zabezpečenie služieb, ktoré súvisia s vydávaním a spravovaním identifikačných preukazov všetkých študentov a zamestnancov TU v Trnave. V roku 2015 bolo implementované integračné rozhranie Novell IDM-EMStudent, ktoré umožňuje prenos dát potrebných pre výrobu preukazov ISIC a vydávanie prolongačných známok. V roku 2015 sa nepodarilo realizovať navrhnuté

opatrenie – kontrolu zameranú na overenie správnej prolongácie preukazov študenta na fakultách TU.

**Sledovaný indikátor:**

5 900 používateľov služieb SAIO, z toho 3 739 používateľov systému CKM Online

**Návrh opatrení:**

- a) Zabezpečiť na jednotlivých fakultách TU dôsledné dodržiavanie Pokynov správcu SČK o vydávaní prolongačných známok. Realizácia: dekaní fakúlt.
  - b) Aspoň raz v priebehu akademického roka kontrolovať platnosť preukazov študentov a zistené nedostatky disciplinárne riešiť. Realizácia: dekaní fakúlt.
- 2) Poskytovať komplexné služby SAIO pre oprávnených používateľov v súlade s vnútornými predpismi.

**Vyhodnotenie:**

SČK poskytuje držiteľom preukazov TU komplexné služby:

- a) zhotovenie preukazu a jeho zaslanie na študijné oddelenie,
- b) zhotovenie duplikátu preukazu v prípade mimoriadnej udalosti,
- c) zabezpečenie objednanej prolongačnej známky,
- d) aktualizáciu dát na univerzitnom terminály,
- e) aktiváciu prihlasovacích údajov do stravovacieho systému CardPay,
- f) aktiváciu prístupu na parkovisko TU,
- g) riešenie reklamácií nefunkčných kariet.

**Sledované indikátory:**

Počet zaznamenaných prípadov nedostupnosti služieb SČK - 0

Počet uznaných reklamácií na chybné údaje na preukaze študenta - 3.

**Návrh opatrení:**

- a) Udržať úroveň poskytovaných služieb a realizovať integráciu systému správy preukazov EMStudent so systémom na správu identít, čím sa zabezpečí vyššia úroveň automatizácie procesu zhotovenia preukazov, resp. ich prolongácie. Realizácia: riaditeľ CIS TU.
- b) Zabezpečiť vyššiu úroveň súčinnosti s dodávateľom technológie a systémov EMStudent a VSprint na promptné odstránenie ich výpadku alebo nesprávnej funkčnosti. Realizácia: správca SČK CIS TU.

V Trnave, dňa 20.4.2016

Spracoval: Ing. Jozef Koricina  
*riaditeľ CIS TU*