Správa o výsledku kontroly informačných systémov v Trnavskom samosprávnom kraji a vo vybranej organizácii v jeho zriaďovateľskej pôsobnosti

Kontrola informačných systémov v Trnavskom samosprávnom kraji a vo vybranej organizácii v jeho zriaďovateľskej pôsobnosti bola vykonaná v súlade s plánom kontrolnej činnosti NKÚ SR na rok 2009 a v súlade so stratégiou úradu.

Účelom kontrolnej akcie bolo preverenie informačných systémov (ďalej len „IS"), ich bezpečnosť, spoľahlivosť a korektnosť. Preverenie údajov v týchto systémoch so zreteľom na spoľahlivosť, úplnosť a dostatočnosť ich zabezpečenia.

Predmetom kontrolnej akcie bolo:

A. Všeobecná časť

1. Prevádzka informačných systémov
2. Bezpečnosť IS
3. Operačné systémy a siete

B. Aplikačná časť

1. Aplikačná kontrola

Kontrola bola vykonaná v termíne od 29.06.2009 do 31.07.2009 v subjektoch:

- Trnavský samosprávny kraj, Starohájska 10, 917 01 Trnava,
- Správa a údržba ciest Trnavského samosprávneho kraja, Bulharská 39, 918 53, Trnava

za obdobie roku 2009.

Počas výkonu kontroly bolo zistené:

1. Prevádzka informačných systémov

V podmienkach Trnavského samosprávneho kraja (ďalej len „TTSK") správu a riadenie informačných a komunikačných technológií a informačných systémov (ďalej len „IS") zabezpečuje Úrad Trnavského samosprávneho kraja (ďalej len „ÚTTSK") prostredníctvom oddelenia informatiky, ktoré je organizačne začlenené pod odbor vnútornej správy Sekcie riadenia ÚTTSK.

V oblasti kontroly súladu s platnou legislatívou SR pre informačné systémy verejnej správy (ďalej len „ISVS") kontrolná skupina NKÚ SR v intenciách s ustanoveniami Európskych vykonávacích smerníc pre kontrolné štandardy INTOSAI akceptovala výsledky práce externých kontrolórov v oblasti kontroly dodržiavania bezpečnostných štandardov pre ISVS. Táto kontrola bola vykonaná Ministerstvom financií SR v súlade so zákonom o ISVS v období jún 2009, pričom výsledok kontroly preukázal drobné nedostatky.

Ďalej bola preverená oblasť prijatých vnútroorganizačných smerníc a nariadení pre prevádzku IS v podmienkach TTSK. Kontrolou bolo zistené nedostatočné formálne upravenie dôležitých oblastí týkajúcich sa zabezpečenia nepretržitej prevádzky a obnovy IS po havárii systému.

Nezabezpečenie zásad nepretržitej prevádzky a obnovy systému môže viesť k strate a poškodeniu údajov a k prípadnému znefunkčneniu prevádzky IS, čo v konečnom dôsledku môže mať značné finančné následky na verejné financie.

Vykonaná kontrola taktiež preukázala nedostatočné zmluvné upravenie prístupu do IS kontrolovaného subjektu externými poskytovateľmi služieb. Vo viacerých prípadoch bolo zistené nedostatočné formálne upravenie podmienok prístupu do IS TTSK tretími stranami, prípadne tieto podmienky prístupu neboli vzhľadom k skutočnosti aktualizované.

2. Bezpečnosť IS

Kontrolou bezpečnosti IS TTSK boli zistené viaceré nedostatky v uvedenej oblasti. Taktiež bolo zistené nedôsledné uplatňovanie prijatých vnútropodnikových smerníc pre oblasť bezpečnosti a správy IS v TTSK.

Špecifikácia konkrétnych nedostatkov bola z dôvodu zachovania dôvernosti informácií oznámená iba kompetentným osobám kontrolovaného subjektu.

3. Operačné systémy a siete

Údržba a monitorovanie operačných systémov a aplikačného programového vybavenia (ďalej len „APV“) v rámci IS TTSK sú vykonávané povereným zamestnancom oddelenia informatiky kontrolovaného subjektu. V niektorých prípadoch je aktualizácia APV vykonávaná dodávateľom konkrétnej aplikácie.

Kontrolou bolo zistené, že v čase kontroly kontrolovaný subjekt nemal v oblasti IS prijatý žiadny vnútroorganizačný predpis, ktorý by formálne upravoval proces aktualizácie operačných systémov a APV v podmienkach IS TTSK. Taktiež bola zistená absencia formálne zavedených postupov pre testovanie aktualizácií APV pred nasadením do produkčného prostredia IS a v prípade tretích strán táto skutočnosť nebola právne upravená v zmluvnom vzťahu s externými poskytovateľmi služieb.

4. Aplikačná kontrola

Aplikačná kontrola bola vykonaná v subjekte Správa a údržba ciest Trnavského samosprávneho kraja (ďalej len „SaÚC TTSK“), ktorého zriaďovateľom je TTSK. Predmetom kontroly bol ekonomický informačný systém (ďalej len „EIS“) využívaný SaÚC TTSK.

Na kontrolovanom subjekte SaÚC TTSK boli implementované jednotlivé moduly EIS a ich komponenty pre spracovanie ekonomických činností, logistiky, evidencie majetku a sumarizácie údajov pre potreby ÚTTSK. Správu EIS vykonáva pracovník oddelenia informatiky ÚTTSK zodpovedný za túto oblasť.

Kontrolou bolo zistené, že neboli v dostatočnej miere vymedzené povinnosti poskytovateľa EIS v oblasti administrácie uvedeného EIS.

Zhrnutie

Vykonanou kontrolou boli zistené viaceré nedostatky v oblasti prevádzky a bezpečnosti informačných systémov TTSK a taktiež v oblasti operačných systémov a sietí.

Návrh odporúčaní na riešenie zistených nedostatkov:

V oblasti prevádzky IS:

- Prijať vnútroorganizačné predpisy, podrobne upravujúce proces vytvárania, uchovávania a testovania záložných kópií údajov a programového vybavenia IS.

- Prijať vnútroorganizačné dokumenty, podrobne upravujúce plán obnovy IS pre kľúčové informačné systémy organizácie pre prípad nepredvídaných okolností a zaviesť postupy obnovy a reštartovania, vrátane rýchlej obnovy poškodených alebo stratených súborov a tieto pravidelne testovať. Kópie plánov obnovy pre prípad nepredvídaných okolností uchovávať na vzdialenom mieste.

V oblasti bezpečnosti:

- Korektne nastaviť a dôsledne uplatňovať bezpečnostnú politiku v rámci organizácie ako i vo vzťahu k tretím osobám.

- Zmluvne upraviť prístup tretích strán do aplikácií obsahujúcich citlivé informácie organizácie.

V oblasti operačných systémov a sietí:

- Prijať zásady schvaľovania a implementácie aktualizácií operačných systémov a aplikačného vybavenia IS.

Výsledky vykonanej kontroly boli prerokované so štatutárnymi zástupcami kontrolovaných subjektov, ktorí prijali celkovo 7 komplexných opatrení na kontrolou zistených nedostatkov. Plnenie prijatých opatrení bude NKÚ SR v rámci svojej činnosti sledovať a kontrolovať.