METODICKÝ MANUÁL č. 4

Metodický manuál pre zabezpečenie informačnej bezpečnosti

Verzia 2.0

Riadenie dokumentu:

Dokument	**Názov**	Metodický manuál pre zabezpečenie informačnej bezpečnosti		
	Verzia:	2.0	**ID:**	0
	Číslo:	1	**Stav:**	Finálny
	Vydanie:		**Vytvorený:**	21. 06. 2009
	Dostupný v:		**Posledná úprava:**	16. 09. 2009
	Kľúčové slová:		**Celkom strán:**	92
Autor	**Pripravený kým:**		**Celkový čas prípravy:**	-
	Prispievatelia:			

Odovzdal:	**Oponoval:**	**Prevzal:**
[.....]	[.....]	[.....]
Alena Kulíková **microform, s.r.o**. Zhotoviteľ	RNDr. Anna Levčíková **MK SR** Odborný garant	Václav Šuplata **Národné osvetové centrum** Objednávateľ

Zoznam stavov dokumentu:

Verzia	Dátum	Dôvod zmeny, dodatku	Autor
1.0	12. 06. 2009	Vytvorenie dokumentu	
1.5	30. 07. 2009	Doplnenie dokumentu	
2.0	16.09.2009	Finálna verzia	

História verzií

Verzia	Zoznam menených častí
1.0	Priebežná verzia
2.0	Finálna verzia

OBSAH

1 ÚVOD

Cieľom tohto metodického manuálu je vymedziť a popísať princípy a postupy riešenia informačnej bezpečnosti v kontexte prípravy a realizácie projektov OPIS prioritná os 2 (ďalej len „OPIS2“). Dokument vysvetľuje a interpretuje formálne požiadavky platných právnych predpisov Slovenskej republiky, noriem, vnútorných riadiacich aktov platných v rezorte Ministerstva kultúry Slovenskej republiky (ďalej len „MK SR“) a ďalších dokumentov súvisiacich s informačnou bezpečnosťou a konkretizuje princípy a spôsoby ich napĺňania.

Pri napĺňaní formálnych bezpečnostných požiadaviek je dôležite zohľadniť potrebu praktických a vecne opodstatnených opatrení vyplývajúcich z činností vykonávaných v rámci projektov OPIS2. V dokumente sú navrhované metodické postupy a bezpečnostné opatrenia, ktorých naplnenie a dodržiavanie prispeje k spoľahlivému, bezpečnému a riadenému výkonu analytických aj realizačných činností a k celkovej efektivite celého priebehu realizácie jednotlivých projektov OPIS2.

Kľúčovým materiálom určujúcim bezpečnostné princípy tohto metodického manuálu je Bezpečnostná politika informačných systémov v rezorte Ministerstva kultúry Slovenskej republiky. Táto bola pri spracovaní metodického manuálu v plnej miere zohľadnená.

Pri tvorbe dokumentu sa kládol dôraz aj na Výnos Ministerstva financií Slovenskej republiky z 8. Septembra 2008 č. F/013261/2008-132 o štandardoch pre informačné systémy verejnej správy (ďalej len „Výnos“), podľa ktorého všetky informačné systémy verejnej správy musia mať vo svojich IS aplikované prvky bezpečnostných štandardov (§ 27 - § 41 Výnosu).

Praktické opatrenia sú postavené na východiskách vyplývajúcich z normy STN ISO/IEC 27002:2005 Informačné technológie. Zabezpečovacie techniky. Pravidlá dobrej praxe manažérstva informačnej bezpečnosti.

Manuál popisuje zabezpečenie informačnej bezpečnosti najmä z technicko-realizačného pohľadu vo vzťahu Žiadateľ o nenávratný finančný príspevok (ďalej len „NFP“) / Pamäťová a fondová inštitúcia (ďalej len „PFI“) / digitalizačné pracovisko – partneri projektu a dodávatelia.

Metodický manuál je určený trom okruhom zúčastnených subjektov:

- PFI (v závislosti od konkrétneho projektu OPIS2 sem môžu byť zaradení aj potenciálni partneri digitalizácie, napr. MV SR),
- digitalizačné pracoviská,
- tretie strany (dodávatelia digitalizácie a čiastočne aj potenciálni partneri digitalizácie) zúčastňujúce sa na príprave a realizácii projektov OPIS2.

2 INFORMÁCIE O POUŽÍVANÍ METODICKÉHO MANUÁLU

2.1 Využitie metodiky

Tento metodický manuál predstavuje základný rámec pre zabezpečenie informačnej bezpečnosti v projektoch OPIS2. Pozostáva z návrhu preverených a funkčných postupov, krokov a návodov použiteľných v praxi

V závislosti od požiadaviek na riešenie konkrétnej oblasti informačnej bezpečnosti je túto metodiku potrebné dávať do súladu s miestnymi podmienkami a možnosťami (napríklad zohľadniť existujúce riadiace akty, ktoré upravujú prístup k implementácii informačnej bezpečnosti, vyhodnotiť možnosti využitia existujúcich prvkov riadenia informačnej bezpečnosti, prispôsobiť rozsah zabezpečovanie jednotlivých činností personálnym kapacitám a ich súčasným kvalifikačným predpokladom).

2.2 Členenie Metodického manuálu a práca s dokumentom

Členenie dokumentu rešpektuje v zásade jednotnú štruktúru všetkých Metodických manuálov pre OPIS2. V prípade tohto manuálu však boli vypustené niektoré technologicky orientované kapitoly, ktoré nie sú relevantné pre oblasť informačnej bezpečnosti.

V časti 3 Metodiky sú uvedené hlavné ciele, princípy a postupy riešenia informačnej bezpečnosti v kontexte prípravy a realizácie projektov OPIS2 a zakotvenie týchto cieľov v širšom kontexte strategických plánov a dokumentov.

V časti 4 je všeobecná oblasť informačnej bezpečnosti rozdelená do 11-tich konkrétnych oblastí, ktoré sú predmetom implementácie v projektoch OPIS2 podľa tohto metodického manuálu.

Časť 5 vysvetľuje základné princípy a východiská v jednotlivých oblastiach informačnej bezpečnosti a uvádza relevantnú legislatívu a súvisiace kľúčové dokumenty.

Časť 6 predstavuje ťažisko tohto metodického manuálu a popisuje konkrétne metodické postupy pre jednotlivé oblasti bezpečnosti samostatne vo vzťahu k žiadateľovi o NFP a vo vzťahu k dodávateľovi projektu OPIS2.

Metodický manuál pre zabezpečenie informačnej bezpečnosti súvisí s viacerými ostatnými metodickými manuálmi, pretože má prierezový charakter a predstavuje komplexný riadiaci, analytický a výkonný rámec pre identifikáciu a napĺňanie bezpečnostných požiadaviek v rámci prípravy a realizácie projektov OPIS2.

3 HLAVNÉ CIELE

3.1 Hlavné ciele

Hlavným cieľom tohto metodického manuálu je určiť a popísať princípy a postupy riešenia informačnej bezpečnosti v kontexte prípravy a realizácie projektov OPIS2. Dokument vysvetľuje formálne požiadavky platných právnych predpisov Slovenskej republiky, noriem a ďalších dokumentov súvisiacich s informačnou bezpečnosťou a konkretizuje spôsoby ich napĺňania.

Pri napĺňaní formálnych bezpečnostných požiadaviek je dôležite zohľadniť potrebu praktických a vecne opodstatnených opatrení vyplývajúcich z činností vykonávaných v rámci projektov OPIS2. V dokumente sú konkretizované bezpečnostné opatrenia a odporúčania, ktorých naplnenie a dodržiavanie prispeje k spoľahlivému, bezpečnému a riadenému výkonu digitalizácie a celkovej efektivite prípravy a výkonu činností.

3.2 Nadstavbové ciele

Operačný program informatizácia spoločnosti implementuje špecifickú prioritu *2.1 Informatizácia spoločnosti* v rámci strategickej priority NSRR[1] *2. Vedomostná ekonomika.*

Nadstavbovým prínosom adekvátneho zabezpečenia informačnej bezpečnosti je hladká realizácia programovej osi OPIS2 *„Rozvoj pamäťových a fondových inštitúcií a obnova ich národnej infraštruktúry“* a relevantného Opatrenia 2.2[2]. Špecifický cieľ prioritnej osi 2 OPIS sa opiera o požiadavky EK na členské štáty v oblasti integrácie národných systémov do Europeany[3] a kritériá pre jej budovanie. Implementácia národných projektov v rámci OPIS2 tak predstavuje hlavnú národnú iniciatívu a nástroj praktického zapojenia inštitúcií SR do Europeany. Cieľom osi 2 je

„Skvalitnenie systémov získavania, spracovania, ochrany a využitia poznatkov a digitálneho obsahu, modernizácia a dobudovanie infraštruktúry pamäťových a fondových inštitúcií na národnej úrovni“

Prostredníctvom projektov v Opatreniu 2.2 „*Digitalizácia obsahu pamäťových a fondových inštitúcií, archivovanie a sprístupňovanie digitálnych dát“* bude adresované špecifické potreby sektoru vyjadrené v zdôvodneniu prioritnej osi:

---

1 http://www.strukturalnefondy.sk/download.php?FNAME=1209486396.upl&ANAME=NSRR290607.zip

2 *zdroj: OPIS programový dokument http://informatizacia.sk/operacny-program-informatizacia-spolocnosti/1884s*

3 *Europeana je Tematická sieť financovaná Európskou komisiou v rámci programu eContentplus, súčasti politiky i2010. Pôvodne známe ako sieť Európskej digitálnej knižnice– EDLnet – partnerstvo zahŕňa 100 zástupcov z organizácií zameraných na dedičstvo a znalosti a IT expertov z celej Európy.*

„…je potrebné dosiahnuť vysokú mieru prepojenia a sprístupňovania dát a informácií (vo fyzickej alebo digitálnej forme), dlhodobé a bezpečné uloženie dát na rôznych nosičoch a podporiť ich čo najširšiu aplikáciu v oblasti výskumu, vývoja, inovácie, miestneho a regionálneho rozvoja a strategického plánovania na národnej úrovni alebo regionálnej úrovni“.

4 ZÁKLADNÉ INFORMÁCIE O SPRACOVÁVANEJ OBLASTI

Z hľadiska určovania špecifických bezpečnostných cieľov a spôsobov ich dosahovania je všeobecná oblasť informačnej bezpečnosti rozdelená do 11-tich konkrétnych oblastí. Pre každú z oblastí sú v tomto metodickom manuáli určené jednotlivé princípy, legislatívne a normatívne východiská a metodické postupy pre jednotlivé cieľové skupiny.

4.1 Základná charakteristika oblasti

V súlade s normou STN ISO/IEC 27002:2005 ako aj z hľadiska praktických a v praxi očakávateľných potrieb tento metodický manuál upravuje nasledovné oblasti informačnej bezpečnosti:

- Politika bezpečnosti
- Organizácia bezpečnosti
- Klasifikácia a riadenie aktív
- Personálna bezpečnosť
- Fyzická bezpečnosť a bezpečnosť prostredia
- Riadenie komunikácií a prevádzky
- Riadenie prístupov
- Vývoj, nasadzovanie a údržba informačných systémov
- Monitorovanie a manažment bezpečnostných incidentov
- Riadenie kontinuity procesov závislých od IS
- Súlad s požiadavkami
- Manažment rizík pre oblasť informačnej bezpečnosti

Súčasťou úpravy je aj vysvetlenie hodnotenia a zvládania bezpečnostných rizík, ktoré budú identifkované v jednotlivých projektoch OPIS2. Táto oblasť je vzhľadom na rozsah projektov veľmi dôležitá, a preto je jej venovaná samostatná metodická časť (podkapitoly 5.3.12, 6.1.13 a 6.2.13).

Celková architektúra oblastí a procesov, ktoré si vyžadujú riešenie informačnej bezpečnosti podľa tohto metodického manuálu je detailne popísaná v ďalších metodických manuáloch:

- Metodický manuál pre zabezpečenie projektového manažmentu,
- Metodický manuál pre zabezpečenie centrálneho prepojenia konverzie, evidencie, spracovania a prezentácie objektov a následného spracovania obsahu,
- Metodický manuál pre zabezpečenie dlhodobej archivácie konvertovaných objektov,
- Metodický manuál pre zabezpečenie národných autorít, centrálnych slovníkov a tezaurov,
- Metodický manuál pre zabezpečenie spracovania správy a prezentácie konvertovaných objektov.

4.2 Stručná história vývoja konkrétnej oblasti

Prostredie potenciálnych žiadateľov o NFP bolo v čase spracovania tohto metodického manuálu predmetom rozvoja informačnej bezpečnosti, najmä z dôvodu implementácie bezpečnostných štandardov podľa požiadaviek Výnosu Ministerstva financií Slovenskej republiky z 8. Septembra 2008 č. F/013261/2008-132 o štandardoch pre informačné systémy verejnej správy. Praktická implementácia informačnej bezpečnosti v jednotlivých organizáciách je konzistentná s postupmi odporúčanými týmto metodickým manuálom.

5 VÝCHODISKÁ A PRINCÍPY

5.1 Východiská

Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, ktorá bola schválená vládou SR uznesením č.570/2008, vytyčuje konkrétne priority informačnej bezpečnosti. Pre podmienky prípravy a realizácie projektov OPIS2 sú aktuálne najmä nasledovné:

- budovanie povedomia a kompetentnosti v informačnej bezpečnosti,
- vytváranie bezpečného prostredia,
- zefektívnenie riadenia informačnej bezpečnosti.

MK SR má vypracovanú a schválenú Bezpečnostnú politiku informačných systémov v rezorte Ministerstva kultúry Slovenskej republiky (ďalej len „Bezpečnostná politika IS rezortu MK SR“), ktorá bola schválená na porade vedenia Ministerstva kultúry Slovenskej republiky ako súčasť materiálu „Návrh riešenia bezpečnosti informačných systémov v rezorte MK SR na roky 2008“ dňa 15.júla 2008. Bezpečnostná politika IS rezortu MK SR je priebežne implementovaná do praxe v časovom období rokov 2008 – 2010. Požiadavky z nej vyplývajúce je nutné zohľadniť aj v kontexte projektov OPIS2 realizovaných v rezorte MK SR.

Pri implementácii praktických bezpečnostných opatrení sa musia zohľadňovať požiadavky Výnosu Ministerstva financií Slovenskej republiky z 8. Septembra 2008 č. MF/013261/2008-132 o štandardoch pre informačné systémy verejnej správy[4], podľa ktorého všetky informačné systémy verejnej správy musia mať vo svojich informačných systémoch aplikované prvky bezpečnostných štandardov (§ 27 - § 41 Výnosu[5]). Pre Výnos je kľúčovou vyššou právnou normou zákon č.275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. V zmysle § 3 ods. 2) písm. b) a písm. c) tohto zákona povinné osoby:

- zabezpečujú plynulú, bezpečnú a spoľahlivú prevádzku informačných systémov verejnej správy,
- zodpovedajú za zabezpečenie informačného systému proti zneužitiu.

V zmysle § 3 ods. 3) písm. a) správca informačného systému verejnej správy:

- je povinný zabezpečiť, aby informačný systém verejnej správy vyhovoval štandardom.

Okrem štandardu STN ISO/IEC 27002:2005 bol základným metodickým východiskom pre spracovanie tohto metodického manuálu najmä Výnos – jeho časť „Bezpečnostné štandardy“ (§ 27 - § 41 Výnosu). Výnos definuje dve základné kategórie bezpečnostných štandardov:

- štandardy pre architektúru riadenia,
- štandardy minimálneho technického zabezpečenia.

[4] S účinnosťou od 1.10.2008.

[5] Bezpečnostné štandardy musia byť implementované v súlade s účinnosťou Výnosu, okrem § 27 písm. a) druhého, tretieho, šiesteho, siedmeho, deviateho a štrnásteho bodu a písm. e) až g), § 28, § 29 písm. b) až f), § 30 písm. b), § 31 písm. c) až f), § 32 písm. b) a c), § 33, § 35 písm. a) až c) a písm. e), § 37 písm. d), § 39 písm. b) až j), § 40 ktoré nadobúdajú účinnosť 1.októbra 2009.

Štandardy pre architektúru riadenia Výnosu pokrývajú nasledovné oblasti:

- § 27 Riadenie informačnej bezpečnosti,
- § 28 Personálna bezpečnosť,
- § 29 Manažment rizík pre oblasť informačnej bezpečnosti,
- § 30 Kontrolný mechanizmus riadenia informačnej bezpečnosti.

Štandardy minimálneho technického zabezpečenia Výnosu pokrývajú nasledovné oblasti:

- § 31 Ochrana proti škodlivému kódu,
- § 32 Sieťová bezpečnosť,
- § 33 Fyzická bezpečnosť a bezpečnosť prostredia,
- § 34 Aktualizácia softvéru,
- § 35 Monitorovanie a manažment bezpečnostných incidentov,
- § 36 Periodické hodnotenie zraniteľnosti,
- § 37 Zálohovanie,
- § 38 Fyzické ukladanie záloh,
- § 39 Riadenie prístupu,
- § 40 Aktualizácia informačno-komunikačných technológií,
- § 41 Účasť tretej strany.

Bezpečnostné štandardy musia byť implementované v súlade s účinnosťou Výnosu (t.j. od 1.10.2008), okrem § 27 písm. a) druhého, tretieho, šiesteho, siedmeho, deviateho a štrnásteho bodu a písm. e) až g), § 28, § 29 písm. b) až f), § 30 písm. b), § 31 písm. c) až f), § 32 písm. b) a c), § 33, § 35 písm. a) až c) a písm. e), § 37 písm. d), § 39 písm. b) až j), § 40 ktoré nadobúdajú účinnosť 1.októbra 2009.

Princípy a postupy riešenia jednotlivých oblastí bezpečnosti v tomto dokumente zohľadňujú vyššie uvedené požiadavky Výnosu a interpretujú ich pre potreby pokrytia špecifických bezpečnostných potrieb a požiadaviek digitalizácie.

MK SR malo v čase vypracovania tohto metodického manuálu vydané štyri metodické pokyny s rezortnou platnosťou upravujúce vybrané oblasti informačnej bezpečnosti a samostatnú smernicu:

- Metodický pokyn Ministerstva kultúry Slovenskej republiky č. MK–2349/2009-10/2396 z 20. februára 2009 pre klasifikáciu a riadenie aktív informačných systémov,
- Metodický pokyn Ministerstva kultúry Slovenskej republiky č. MK-2216/2009-10/1992 z 15. februára 2009 pre nákup, vývoj a údržbu informačných systémov,
- Metodický pokyn Ministerstva kultúry Slovenskej republiky č. MK - 2902/2009-10/4659 z 15. apríla 2009 pre organizáciu a riadenie bezpečnosti informačných systémov,
- Metodický pokyn Ministerstva kultúry Slovenskej republiky č. MK-3822/2009-10/8737 z 10. júla 2009 pre analýzu a riadenie rizík informačných systémov.
- Smernica MK SR č. MK-3821/2009-10/8736 o postupoch monitorovania a manažmentu bezpečnostných incidentov informačných systémov Ministerstva kultúry Slovenskej republiky.

V príprave boli aj ďalšie rezortné metodické pokyny pre jednotlivé oblasti bezpečnosti. Uvedené metodické pokyny je v projektoch OPIS2 potrebné aplikovať v súlade s postupmi špecifikovanými v tomto metodickom manuáli.

Sumarizácia základných východísk pre zabezpečenie informačnej bezpečnosti je uvedená v nasledovnej tabuľke:

Základné východiská	
Požiadavky vyplývajúce zo zákonov SR, z uznesení vlády SR a z interných predpisov rezortu kultúry	Národná stratégia pre informačnú bezpečnosť v Slovenskej republike Zákon č.275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov Výnos MF SR z 8. Septembra 2008 č. MF/013261/2008-132 o štandardoch pre informačné systémy verejnej správy Bezpečnostná politika IS rezortu MK SR
Princípy, normy, štandardy a metódy metodiky	STN ISO/IEC 27002:2005 Informačné technológie.Zabezpečovacie techniky. Pravidlá dobrej praxe manažérstva informačnej bezpečnosti.

5.2 Požiadavky na riadenie informačnej bezpečnosti

Základné roviny riadenia informačnej bezpečnosti v projektoch OPIS2 sa odvíjajú od nasledovných požiadaviek:

- požiadavky vyplývajúce z aplikovateľnej legislatívy SR a medzinárodného i národného štandardizačného rámca súvisiaceho s informačnou bezpečnosťou,
- požiadavky vyplývajúce z vecných a funkčných potrieb prípravy, vývoja a prevádzky predmetov projektov OPIS2.

Legislatívne a štandardizačné prvky obsahujú a agregujú široké spektrum požiadaviek informačnej bezpečnosti a pre potreby realizácie projektov OPIS2 musia byť správne interpretované. Súčasťou každého projektu OPIS2 by teda mala byť aj analýza aplikovateľnej legislatívy majúcej dopad na predmet príslušného projektu OPIS2 a určenie spôsobov jej naplnenia.

Pre druhú rovinu požiadaviek sú určujúce konkrétne prakticky orientované oblasti informačnej bezpečnosti, ktoré musia byť v primeranej miere zohľadnené. Týkajú sa predovšetkým troch základných logických fáz technicko-realizačnej časti projektov OPIS2. Z hľadiska informačnej bezpečnosti sa jedná o bezpečnosť vývoja, implementácie a dodávky systémov IKT, internú bezpečnosť systémov IKT a bezpečnosť prevádzky systémov IKT. Určenie, spresňovanie a napĺňanie týchto požiadaviek musí byť realizované paralelne s projektovými, analytickými a realizačnými aktivitami súvisiacimi s jednotlivými projektmi OPIS2.

5.3 Princípy v jednotlivých oblastiach informačnej bezpečnosti

Všetky základné princípy špecifikované v nasledujúcich oblastiach bezpečnosti vychádzajú z bezpečnostnej politiky IS rezortu MK SR.

5.3.1 Politika bezpečnosti

5.3.1.1 Základné princípy

V súlade s formálnymi a praktickými požiadavkami na riešenie informačnej bezpečnosti je potrebné v procese prípravy a výkonu projektov OPIS2 najmä:

- zaistiť dodržiavanie právnych predpisov a stanovených požiadaviek relevantných pre oblasť informačnej bezpečnosti počas prípravy a realizácie digitalizácie,
- minimalizovať finančné a iné straty súvisiace s narušením výkonu digitalizácie, bezpečnostnými incidentmi počas priebehu projektov OPIS2, nedostatočne alebo nevhodne riadenými digitalizačnými procesmi,
- vytvoriť a prevádzkovať dôveryhodné a spoľahlivé služby a prostredie, v ktorom bude digitalizácia realizovaná,
- minimalizovať riziká ohrozenia digitálnych objektov, digitálnych zbierok, metaúdajov a ďalších informačných aktív zahrnutých a vytváraných počas digitalizácie,
- zaistiť poskytovanie služieb digitalizácie v stanovenej kvalite a rozsahu aj pri neštandardných (havarijných) stavoch IS,
- chrániť dobré meno jednotlivých PFI a partnerov.

Na zaistenie dosahovania vyššie uvedených bezpečnostných cieľov je potrebné implementovať a počas výkonu činností kontinuálne sledovať najmä tieto princípy:

- Na ochranu elektronických informácií vytváraných a spracúvaných počas projektov OPIS2 musia byť vytvorené zodpovedajúce technické a organizačné predpoklady.
- Informácie môžu byť uložené a spracúvané iba v systémoch a aplikáciách, ktoré zodpovedajú štandardom zavedeným a požadovaným v rámci projektov OPIS2.
- Spracúvané informácie musia byť chránené tak, aby sa nenarušila ich dôvernosť, integrita a dostupnosť.
- Účinnosť bezpečnostných opatrení slúžiacich na ochranu by mala byť priebežne vyhodnocovaná.
- Pokrytie formálnych i praktických požiadaviek riešenia informačnej bezpečnosti musí byť súčasťou každého samostatného projektu, realizovaného v rámci OPIS2.
- Úroveň bezpečnostného povedomia všetkých osôb podieľajúcich sa na príprave a realizácii projektov OPIS2 musí byť primeraná okruhu činností, ktoré jednotlivé osoby vykonávajú resp. zabezpečujú.

V praxi je pri implementácii bezpečnostných opatrení potrebné zohľadňovať konkrétne okruhy aktív, ktoré si vyžadujú primeranú úroveň ochrany. Sú to najmä:

- samotné zbierkové predmety, ktoré sú predmetom digitalizácie,
- fyzické komponenty a objekty súvisiace s výkonom digitalizácie (budovy, miestnosti, počítače, komunikačná infraštruktúra, pamäťové média, periférne zariadenia),
- softvér (operačné a aplikačné systémy, systémové súbory),
- údaje (spracovaný obsah, metaúdaje, evidencia, prístupové heslá, dokumentácia),

- iné nehmotné aktíva (služby, ľudské zdroje, ..).

Jednotlivé aktíva sa musia spresniť a konkretizovať v každom projekte OPIS2.

5.3.1.2 Normatívne východiská

Táto oblasť bezpečnosti je východiskovo upravená:

- v štandarde STN ISO/IEC 27002:2005, kapitola Bezpečnostná politika, podkapitola Bezpečnostná politika informácií,
- vo Výnose, § 27 Riadenie informačnej bezpečnosti písm a) a b).

5.3.2 Organizácia bezpečnosti

5.3.2.1 Základné princípy

Hlavným cieľom tejto oblasti bezpečnosti je kontinuálne a efektívne riadiť informačnú bezpečnosť počas prípravy a realizácie projektov OPIS2 vrátane vzťahov k dodávateľským firmám a outsourcingovým partnerom.

Základné princípy v tejto oblasti sú najmä nasledovné:

- za účelom identifikácie a minimalizácie bezpečnostných rizík musí byť v úvodných etapách každého projektu OPIS2 vykonaná analýza rizík,
- jednotlivé roly vo vzťahu k informačnej bezpečnosti v kontexte projektov OPIS2 musia byť definované a musia mať priradené činnosti, zodpovednosti a právomoci,
- zodpovednosti za informačnú bezpečnosť v zmluvných vzťahoch s dodávateľskými firmami a outsourcingovými partnermi sa musia explicitne vymedziť.

Kľúčové role a subjekty súvisiace so zabezpečením a koordináciou plnenia úloh v oblasti riadenia bezpečnosti v kontexte projektov OPIS2 v rezorte MK SR sú nasledovné:

- Rada ministra kultúry SR pre informatizáciu a digitalizáciu,
- predstavený odboru informatizácie MK SR,
- pracovná skupina pre informačnú bezpečnosť zriadená podľa článku 5. odst. 8. Organizačného a rokovacieho poriadku Rady ministra kultúry SR pre informatizáciu a digitalizáciu ako prierezová pracovná skupina na plnenie úloh v oblasti informačnej bezpečnosti rezortu MK SR,
- bezpečnostný manažér IS na odbore informatizácie MK SR,
- bezpečnostní správcovia IS resp. iné osoby poverené zabezpečením informačnej bezpečnosti v procese digitalizácie v jednotlivých PFI a na digitalizačných pracoviskách.

Postavenie a princípy pôsobenia týchto rolí sú detailnejšie rozpracované v samostatnom riadiacom akte MK SR.[6]

Okrem vyššie uvedených môžu byť v rámci projektov OPIS2 zriadené a obsadené ďalšie role, špecifické pre riadenie a riešenie informačnej bezpečnosti. Dôležitou požiadavkou je

[6] Metodický pokyn Ministerstva kultúry Slovenskej republiky č. MK - 2902/2009-10/4659 z 15. apríla 2009 pre organizáciu a riadenie bezpečnosti informačných systémov

najmä menovanie osoby zodpovednej za oblasť informačnej bezpečnosti za každého dodávateľa, podieľajúceho sa príprave a výkone služieb digitalizácie.

5.3.2.2 Normatívne východiská

Táto oblasť bezpečnosti je východiskovo upravená:

- v štandarde STN ISO/IEC 27002:2005, kapitola Organizácia bezpečnosti, podkapitoly Interná organizácia, a Externé subjekty,
- vo Výnose, § 27 Riadenie informačnej bezpečnosti písm. c) až g).

5.3.3 Klasifikácia a riadenie aktív

5.3.3.1 Základné princípy

Ako aktívum z hľadiska digitalizácie sa chápe najmä samotný digitalizovaný objekt, ale aj každá ďalšia dôležitá informácia a dokumentácia (najmä metaúdaje), zmluva, programové vybavenie, technické zariadenie, poskytovaná služba, kvalifikovaní používatelia, dobré meno a ďalšie skutočnosti, sú v rámci prípravy a realizácie projektov OPIS2 považované za dôležité. Výsledkom klasifikácie a riadenia aktív je vytvorenie úplného a aktuálneho prehľadu o okruhu aktív spracúvaného v projekte.

Prevažujúcim bezpečnostným cieľom pre túto oblasť v kontexte digitalizácie je podpora zabezpečenia dostupnosti a integrity elektronických informácií a dostupnosti poskytovaných služieb ako aj zabezpečenie evidencie vytváraných a využívaných aktív a ochrany s nimi súvisiacich elektronických informácií.

Základné princípy v tejto oblasti sú najmä nasledovné:

- postupy evidencie aktív musia byť jasne stanovené, nositelia zodpovednosti za aktíva musia byť určení,
- pravidlá klasifikácie a označovania aktív musia byť stanovené tak, aby boli v praxe použiteľné, plnili svoj účel a zodpovedali potrebám vyplývajúcim z projektov OPIS2,
- pre vybrané typy aktív (najmä pre elektronické informácie priamo súvisiace s digitalizáciou, napríklad pre digitalizované objekty) musí byť explicitne určený ich životný cyklus,
- v prípade, že digitalizovaný objekt bude klasifikovaný ako utajovaná skutočnosť v zmysle zákona č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov, podliehajú všetky činnosti spojené s týmto objektom osobitnému režimu. Podmienky osobitného režimu určia oprávnené osoby – nositelia zodpovednosti za dané aktíva resp. vlastníci aktív.

Presná špecifikácia uvedených princípov je v samostatnom metodickom manuáli (Metodický manuál pre zabezpečenie jednoznačnej a trvalej identifikácie konvertovaných objektov).

Postupy evidencie aktív zahŕňajú nasledovné typy aktív:

- zariadenia IKT, využívané na účely digitalizácie (vo vlastníctve PFI resp. digitalizačného pracoviska),
- cudzie zariadenia IKT (používané v PFI alebo na digitalizačnom pracovisku),
- dôležité dátové médiá,
- aplikačné a programové vybavenie.

Klasifikačná schéma digitalizačných aktív by mala zodpovedať aj životnému cyklu digitalizácie jednotlivých objektov, ich finalizácii a archivácii (stavom, v ktorých sa digitalizovaný objekt môže nachádzať) a zohľadňovať princíp vlastníctva v každom jednotlivom stave. Evidencia stavov a s nimi spojených informácií bude podporená centralizovanými aplikáciami. Podrobnosti sú uvedené v samostatnom metodickom manuáli (Metodický manuál pre zabezpečenie národných autorít, centrálnych slovníkov a tezaurov).

5.3.3.2 Normatívne východiská

Táto oblasť bezpečnosti je východiskovo upravená:

- v štandarde STN ISO/IEC 27002:2005, kapitola Klasifikácia a riadenie aktív, podkapitoly Zodpovednosť za aktíva a Klasifikácia informácií,
- vo Výnose, § 27 Riadenie informačnej bezpečnosti písm. a) bod 1., písm. f), § 29 Manažment rizík pre oblasť informačnej bezpečnosti písm. c), § 41 Účasť tretej strany písm. c).

5.3.4 Personálna bezpečnosť

5.3.4.1 Základné princípy

Hlavným cieľom tejto oblasti bezpečnosti je redukovať riziká súvisiace s ľudskými chybami, zlyhaniami, zneužitím práv, vedomým alebo nevedomým porušovaním bezpečnostných zásad. Za účelom dosahovania tohto cieľu je potrebné primerane aplikovať nasledovné princípy:

- zvyšovať bezpečnostné povedomie u osôb podieľajúcich sa na príprave a realizácii projektov OPIS2 formou školení a praktických inštruktáží,
- zahrnúť do pracovných zmlúv alebo iných právnych dokumentov upravujúcich vzťah osoby a PFI alebo digitalizačného pracoviska konkrétne bezpečnostné zodpovednosti,
- pri výbere nových zamestnancov a obsadzovaní pracovných miest zohľadňovať kvalifikačné a osobnostné predpoklady.

Každá osoba podieľajúca sa na príprave a výkone digitalizácie musí byť poučená o zodpovednosti za bezpečnosť aktív, s ktorými bude prichádzať do styku, ktoré jej budú zverené resp. za ktoré bude niesť zodpovednosť. Rovnako musí byť oboznámená so spôsobom používania jednotlivých aplikácií, ich bezpečnostných mechanizmov ako aj o povolených spôsoboch prenosu digitalizovaných objektov v rozsahu svojej pracovnej náplne. Z dôvodu minimalizácie rizika straty, porušenia alebo zneužitia digitalizovaných objektov musia byť osoby zapojené do procesu digitalizácie poučené tak, aby vedeli identifikovať bezpečnostný incident a zvládnuť postup v prípade jeho výskytu (napríklad podozrenie na neoprávnenú modifikáciu digitalizovaného subjektu).

Riadenie informačnej bezpečnosti v rámci projektov OPIS2 vyžaduje určenie konkrétnych osôb resp. projektových pozícií, ktoré v sa v rámci svojich kompetencií podieľajú na riešení jednotlivých oblastí bezpečnosti a napĺňaní praktických bezpečnostných požiadaviek. Je dôležité, aby každá osoba podieľajúca sa na príprave a výkone digitalizácie bola informovaná o kontaktnej osobe, na ktorú sa môže obracať s otázkami a nejasnosťami v rámci konkrétnych aktivít (v rámci informačnej bezpečnosti).

Pri školeniach jednotlivých pracovníkov je dôležité klásť dôraz na vysvetlenie ich zodpovednosti za upozorňovanie na bezpečnostné riziká a nahlasovanie bezpečnostných incidentov. Podrobnosti preškoľovania a ich náplň je vhodné stanoviť v rámci celkového školiaceho plánu, ktorý by mal byť v rámci projektov OPIS2 vytvorený a implementovaný.

Pri uzatváraní zmlúv s tretími stranami (externými subjektmi) musia byť zmluvne stanovené primerané opatrenia pre tak, aby nedošlo k narušeniu jednak bezpečnostnej politiky IS rezortu MK SR ako aj iných právnych predpisov, ktoré súvisia s informačnou bezpečnosťou a majú vzťah s digitalizáciou (napr. Zákon č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom). Cieľom tejto požiadavky je jednak vymedziť a upraviť zodpovednosť za dodržiavanie týchto predpisov v externom subjekte ako aj umožniť PFI alebo digitalizačnému pracovisku a úložisku možnosť sledovania dodržiavania týchto opatrení.

5.3.4.2 Normatívne východiská

Táto oblasť bezpečnosti je východiskovo upravená:

- v štandarde STN ISO/IEC 27002:2005, kapitola Bezpečnosť ľudských zdrojov, podkapitoly Pred vznikom pracovného vzťahu , Počas pracovného vzťahu, Ukončenie alebo zmena pracovného vzťahu,
- vo Výnose, § 28 Personálna bezpečnosť.

5.3.5 Fyzická bezpečnosť a bezpečnosť prostredia

5.3.5.1 Základné princípy

Hlavným cieľom tejto oblasti je minimalizovať riziká neoprávneného fyzického prístupu k aktívam (zbierkové predmety, digitalizované objekty), ich krádeže, zneužitia, ohrozenia vyššou mocou (prírodný živel). Pri implementácii opatrení je potrebné prihliadať najmä na nasledovné hrozby:

- havárie vodného a vykurovacieho prostredia budov,
- zlyhanie napájacej sústavy alebo dodávky elektrickej energie,
- zlyhanie podporných prostriedkov ochrany prostredia (klimatizácia);
- krádeže zvnútra alebo zvonku,
- personálne zlyhanie (nelegálna manipulácia s aktívami),
- cieľavedomá sabotáž zvnútra alebo zvonku,
- prírodné katastrofy a priemyselné alebo dopravné havárie v blízkosti priestorov s digitalizačnými aktívami.

Zníženie hrozieb je možné v praxi dosiahnuť aplikovaním nasledovných postupov:

- používanie mechanických a technických bezpečnostných opatrení (mreže, klimatizácia, EPS/EZS) vo všetkých priestoroch, kde to je potrebné a opodstatnené,
- pravidelná kontrola funkčnosti ochrany objektov, v ktorých dochádza k uskladneniu (trvalému alebo dočasnému) aktív,
- vytvorenie bezpečnostných zón (priestorov s riadeným fyzickým prístupom osôb a evidenciou ich prístupov),
- organizačné opatrenia (najmä so zameraním na obmedzenie pohybu cudzích osôb).

Okrem vplyvov prostredia (napr. zvýšená teplota) predstavujú najčastejšie riziko pre fyzickú bezpečnosť aktív cudzie osoby v priestoroch organizácie.

Pracoviská plánované na zabezpečenie a realizáciu procesov digitalizácie musia byť umiestnené v budovách primerane vybavenými opatreniami fyzickej bezpečnosti. Táto požiadavka sa týka aj prenajatých priestorov. Primerané opatrenia fyzickej bezpečnosti sú najmä:

- ochrana mechanickými a technickými opatreniami (bezpečnostné dvere, mreže, zabezpečovacia signalizácia a pod.),
- ochrana pred vplyvmi prostredia (teplota, prašnosť, vlhkosť),
- centralizovaný vstup so strážnou službou resp. informátorom.

Kľúčové komponenty IKT využívané pri digitalizačných činnostiach (servery, centrálne sieťové prvky, skenery a pod.) musia byť umiestnené v priestoroch, ktoré spĺňajú špeciálne požiadavky na opatrenia fyzickej bezpečnosti (priestory so zvláštnym určením). Tieto priestory musia byť chránené pred nadmernou teplotou, prašnosťou, vlhkosťou a svojimi parametrami musia zodpovedať požiadavkám na ochranu jednotlivých druhov zbierkových predmetov. V týchto priestoroch sa smie upratovať a vykonávať servisné služby len v prítomnosti určenej osoby.

5.3.5.2 Normatívne východiská

Táto oblasť bezpečnosti je východiskovo upravená:

- v štandarde STN ISO/IEC 27002:2005, kapitola Fyzická bezpečnosť a bezpečnosť prostredia, podkapitoly Zabezpečené oblasti a Bezpečnosť zariadení,
- vo Výnose, § 33 Fyzická bezpečnosť a bezpečnosť prostredia.

5.3.6 Riadenie komunikácií a prevádzky

5.3.6.1 Základné princípy

Táto oblasť bezpečnosti upravuje zásady pre zabezpečenie spoľahlivej a bezpečnej prevádzky infraštruktúry a prvkov IKT, ktoré sú alebo budú využívané ako podporné prostriedky realizácie projektov OPIS2. Cieľom je predchádzať narušeniam bezpečnosti pri práci s médiami obsahujúcimi digitalizované objekty a súvisiace informácie ako aj predchádzať strate, neoprávnenej modifikácii alebo zneužitiu elektronických informácií pri ich prenose medzi subjektmi zúčastnenými na projektoch OPIS2.

Bezpečnostné ciele v oblasti riadenia komunikácií a prevádzky sa dosahujú aplikovaním nasledovných princípov:

- štandardizácia pracovných postupov súvisiacich s výkonom digitalizačných činnosti a s nimi spojených podporných procesov,
- minimalizácia rizika zníženia bezpečnosti alebo narušenia prevádzky pri zmenách v prevádzkovom prostredí (hardvér, aplikačné programové vybavenie, operačné systémy a iné),
- predchádzanie únikom a strate informácií prostredníctvom médií,
- používanie prenosných médií (USB kľúče, externé pevné disky) iba na prenos digitalizovaných objektov a iných informácií, nie na ich trvalé uskladňovanie,

- zohľadnenie platných právnych predpisov, pokiaľ sa tieto na prenos alebo sprístupnenie informácií vzťahujú,
- zaručenie integrity pri prenose údajov (aplikovanie bezpečnostných mechanizmov, ktoré zaručia celistvosť a úplnosť prenášaných údajov)
- úroveň bezpečnosti komunikačných trás a počítačových sietí využívaných v projektoch OPIS2 musí zodpovedať bezpečnostným požiadavkám na ochranu aktív využívajúcich služby týchto sietí.

Na zaistenie správneho využívanie bezpečnostných mechanizmov implementovaných v súlade s vyššie uvedenými princípmi sa musí spôsob ich použitia zdokumentovať. Pre každú významnú aplikáciu IS podporujúcu realizáciu projektov OPIS2, vytvorenú v rámci projektu alebo existujúcu a súvisiacu s digitalizovanými objektmi musí existovať:

- používateľská dokumentácia,
- administrátorská dokumentácia,
- prevádzková dokumentácia.

Používateľská dokumentácia obsahuje popis všetkých bezpečnostných mechanizmov, ktoré musí používateľ rutinne využívať. Ďalej obsahuje popis správneho používania aplikácie a popis zakázaného používania aplikácie.

Administrátorská dokumentácia obsahuje najmä popis správy bezpečnostných mechanizmov aplikácie, správy používateľov aplikácie, správy údajov v aplikácii a vysvetlenie spôsobu konfigurácie aplikácie.

Prevádzková dokumentácia obsahuje najmä:

- popisy konfigurácie a zapojenia,
- operátorský denník,
- popis spôsobov riadenia a plánovania zmien a implementácie nových verzií a rozšírení,
- popis spôsobov zálohovania údajov,
- popis spôsobov monitorovania prevádzky (z hľadiska záťaže, kapacít, konfigurácie, chýb).

Prostredie v ktorom budú prebiehať digitalizačné procesy musí byť pripravené na implementáciu zmien a vylepšení. Zmeny v prevádzkovom prostredí sa musia vykonávať riadeným spôsobom pokrývajúcim:

- zmeny aplikácií a databáz,
- zmeny v operačných systémoch, ich konfigurácii a technologickej infraštruktúre IS,
- zmeny prevádzkových postupov.

Zmeny aplikácií a databáz musia byť odôvodnené, schválené a otestované mimo produkčného prostredia. Všetky zmeny musia byť zdokumentované.

Na ochranu pred stratou alebo poškodením sa musia všetky dôležité údajové databázy chrániť zálohovaním. Zálohovanie musí byť pravidelné a nenarúšajúce bežnú prevádzku IS. Pre médiá obsahujúce záložné kópie sa musí zaistiť rovnaký stupeň bezpečnosti, ako je požadovaný pre údaje, ktoré sú na nich uložené. Tieto médiá sa musia zároveň uchovávať mimo priestorov s centrálnymi komponentmi IS tak, aby sa minimalizovalo riziko súčasného poškodenia originálnych aj záložných údajov.

Ako prevencia zlyhaní IS sa musí využívať monitorovanie v týchto oblastiach:

- záťaž kľúčových komponentov IS a komunikačnej infraštruktúry,

- kapacitné rezervy kľúčových komponentov IS (napr. voľné miesto na systémovom disku),
- výskyt chýb v IS (z hľadiska technického aj aplikačného).

Možnosti prieniku škodlivého kódu (napr. počítačové vírusy) sa musia minimalizovať, rovnako ako aj následky takéhoto prieniku. S týmto cieľom sa musia implementovať adekvátne bezpečnostné mechanizmy a pracovné postupy; pre všetky zúčastnené strany platí striktný zákaz ich obchádzania.

Výmeny informácií medzi PFI, digitalizačnými pracoviskami, úložiskami, partnermi a dodávateľmi digitalizácie sa môžu realizovať iba na základe zmlúv alebo písomných poverení. Zoznam informácií poskytnutých externej firme sa musí evidovať. Pre prenos informácií prostredníctvom elektronickej pošty a iných elektronických služieb sa musia stanoviť pravidlá. Na zverejňovanie elektronických informácií musia byť stanovené postupy pre odsúhlasenie zverejnenia.

Na zaistenie ochrany pred možnými hrozbami, zaručenie bezpečnosti systémov a aplikácií využívajúcich počítačové siete a na zaistenie bezpečnosti informácií pri prenose cez počítačové siete, majú byť tieto siete adekvátne spravované a kontrolované. Bezpečnostné prvky, úroveň poskytovaných služieb a požiadavky na riadenie všetkých sieťových služieb musia byť identifikované a zahrnuté do zmlúv o poskytovaní týchto služieb. Spôsobilosť poskytovateľa sieťových služieb na bezpečné zaistenie ich správy je potrebné preveriť a priebežne monitorovať. Rovnako by malo byť odsúhlasené právo na vykonanie kontroly sieťovej komunikácie (napr. pri podozrení na bezpečnostný incident).

Ďalšie podrobnosti o sieťovom modeli, na ktorý je potrebné aplikovať vyššie uvedené princípy riešenia bezpečnosti sú uvedené v Metodickom manuáli pre zabezpečenie centrálneho prepojenia konverzie, evidencie, archivácie, spracovania a prezentácie objektov a následného spracovania obsahu.

5.3.6.2 Normatívne východiská

Táto oblasť bezpečnosti je východiskovo upravená:

- v štandarde STN ISO/IEC 27002:2005, kapitola Riadenie komunikácií a riadenie prevádzky, podkapitoly Prevádzkové postupy a zodpovednosti, Riadenie dodávok tretích strán, Ochrana proti škodlivým programom a mobilným kódom, Zálohovanie, Správa siete, Bezpečnosť pri zaobchádzaní s médiami, Výmeny informácií, Monitorovanie,
- vo Výnose § 32 Sieťová bezpečnosť ako aj v časti Štandardy minimálneho technického zabezpečenia.

5.3.7 Riadenie prístupov

5.3.7.1 Základné princípy

Cieľom tejto oblasti bezpečnosti je predchádzať neoprávnenému prístupu k údajom a službám súvisiacim s digitalizáciou a neoprávnenému použitiu prvkov IKT, aplikácií a zariadení používaných na výkon digitalizácie a narábanie s digitalizovanými objektmi.

Pri napĺňaní tohto cieľa je potrebné aplikovať nasledovné základné princípy:

- LAN siete subjektov podieľajúcich sa na digitalizácii musia byť chránené tak, aby mohli byť považované za dôveryhodné prostredie.
- Prideľovanie prístupov je explicitné a rešpektuje filozofiu „všetko, čo nie je povolené, je zakázané“.
- Interné LAN siete PFI, centrálneho archívu, úložísk a digitalizačných pracovísk a externé dátové siete / LAN siete dodávateľov digitalizácie musia byť vzájomne logicky oddelené tak, aby sa mohol efektívne riadiť a monitorovať tok dát medzi sieťami.
- Prístupy dodávateľov k informáciám spracúvaným v prostredí PFI, centralizovaných registrov alebo digitalizačných pracovísk musia byť jasne zdôvodnené a evidované. Udeleniu prístupu musí predchádzať schválenie oprávnenou osobou v organizácii, ktorá prístup plánuje umožniť.
- Prideľovanie prístupov k službám a informáciám spracúvaným v prostredí centralizovaných aplikácií súvisiacich s projektmi OPIS2 musí prebiehať riadeným procesom. Tento proces musí mať definované prvky schvaľovania spôsobu a rozsahu prístupu, vedenia evidencia pridelených prístupov a odobrania prístupu.

Pravidlá tvorby používateľských účtov a prideľovania oprávnení musia vychádzať z bezpečnostných požiadaviek súvisiacich s aktívami (služby a spôsob ich využitia, hodnota elektronických informácií a spôsob prístupu k nim), ku ktorým sa prístup udeľuje. Pri voľbe prostriedkov identifikácie a autentifikácie osôb, ktorým sa prístup udeľuje, musia byť vyvážené požiadavky na stupeň dosiahnutej bezpečnosti a miera náročnosti používania týchto prostriedkov.

Pre prácu v prostredí viacužívateľských IS musí mať každý používateľ vytvorený prístupový účet. Pre každú aplikáciu využívanú v realizačných procesoch projektov OPIS2 sa musí definovať bezpečnostná parametrizácia používateľských účtov v závislosti od systémových možností aplikácie (používateľské profily). Pred prístupom do IS sa používateľ musí prihlásiť (autorizovať) jemu prideleným používateľským menom a heslom. Každý používateľ má jedinečnú identitu, skupinové účty (účty, pod ktorými môže pracovať viacero používateľov) nie sú akceptovateľné. Požiadavku na zastupovanie používateľa IS počas jeho neprítomnosti iným používateľom musí uplatniť jeho nadriadený alebo príslušný riadiaci pracovník v projektovom tíme projektu OPIS2.

Všetky činnosti používateľov vykonávané pri práci s aplikáciami sa môžu monitorovať. Pre každú aplikáciu, resp. prvok IKT musia byť definované udalosti, ktoré sa monitorujú trvalo (každá udalosť daného typu je zaznamenaná v žurnálových súboroch). Musí sa tiež zabezpečiť aj priebežné vyhodnocovanie údajov z monitorovania.

Zapájanie ľubovoľných zariadení do počítačových sietí a ostatnej komunikačnej infraštruktúry PFI alebo digitalizačných pracovísk smú vykonávať iba poverení zamestnanci alebo zmluvní externí partneri, ale iba so súhlasom určeného zamestnanca organizácie. Zmeny v komunikačnej infraštruktúre PFI, úložísk alebo digitalizačných pracovísk z pohľadu jej prepojenia s externými sieťami (napríklad s dodávateľmi) musia byť vopred schválené určenou osobou v danej organizácii.

5.3.7.2 Normatívne východiská

Táto oblasť bezpečnosti je východiskovo upravená:

- v štandarde STN ISO/IEC 27002:2005, kapitola Riadenie prístupu, podkapitoly Požiadavky na riadenie prístupu, Riadenie prístupu používateľov, Zodpovednosti používateľov, Riadenie prístupu k sieti, Riadenie prístupu k operačnému systému,

Riadenie prístupu k aplikáciám a k informáciám, Mobilné zariadenia a práca na diaľku,
- vo Výnose v § 39 Riadenie prístupu.

5.3.8 Vývoj, nasadzovanie a údržba informačných systémov

5.3.8.1 Základné princípy

Cieľom tejto oblasti bezpečnosti je zabezpečiť identifikáciu a implementáciu bezpečnostných opatrení počas vývoja a nasadzovania nových prvkov IKT. Z pohľadu informačnej bezpečnostne je tiež dôležité zaistiť, aby projekty OPIS2 prebiehali riadeným a kontrolovateľným spôsobom.

Tieto ciele sa v praxi dosahujú aplikovaním nasledovných kľúčových princípov:
- Pre každý projekt OPIS2 sa musia identifikovať a špecifikovať bezpečnostné požiadavky súvisiace s predmetom tohto projektu, jeho výstupmi a službami, ktoré sa počas projektu budú poskytovať resp. odoberať.
- Súčasťou každého projektu OPIS2 musí byť analýza rizík súvisiacich s vývojom a prevádzkovým prostredím, v ktorom bude výstup projektu prevádzkovaný resp. analýza rizík spojených so službami, ktoré budú v rámci projektu zabezpečované (napríklad digitalizačné alebo prezentačné služby).
- Dodávateľ musí pre každý projekt ktorý zabezpečuje, menovať osobu, ktorá bude zabezpečovať napĺňanie požiadaviek na informačnú bezpečnosť vyplývajúcu tak z platných právnych predpisov ako aj z praktických vecne opodstatnených potrieb.
- V rámci projektu musia byť navrhnuté a vykonané bezpečnostné testy tak, aby po ich ukončení bola potvrdená primeraná úroveň odolnosti výsledku projektu voči identifikovaným bezpečnostným rizikám.
- Súčasťou každého projektu musí byť špecifikácia pozícií na ktorých sa bude vykonávať údržba nových prvkov IKT po ich zavedení do rutinnej prevádzky.
- Súčasťou každého projektu musí byť vypracovanie príslušnej projektovej dokumentácie.

Pri koncipovaní každého projektu OPIS2 musí byť súčasťou projektových prác zistenie a naplnenie požiadaviek na informačnú bezpečnosť.

Požiadavky na bezpečnosť sa v tejto oblasti rozdeľujú do nasledovných okruhov:
- požiadavky na vývoj,
- požiadavky na produkt (hardvér, aplikáciu, ucelený IS alebo poskytovanú službu),
- požiadavky na prevádzku,
- požiadavky na súlad.

Za účelom naplnenia požiadaviek vyššie uvedených okruhov musí byť v každom projekte digitalizácie zriadená a obsadená rola, ktorá bude zodpovedať za integráciu požadovaných bezpečnostných opatrení počas realizácie projektu (za stranu dodávateľa aj za stranu žiadateľa o NFP). Ďalej táto rola musí zabezpečiť:
- zohľadnenie právnych predpisov a technologických požiadaviek na bezpečnosť,
- vykonanie analýzy rizík,
- špecifikovanie bezpečnostných opatrení.

Na zaistenie primeranej úrovne bezpečnosti musí byť v každom projekte OPIS2 vývojové a testovacie prostredie oddelené od produkčného prostredia tak, aby nemohlo dochádzať k ich bezpečnostne neprípustnému prelínaniu. Pri testovaní vyvíjaných komponentov sa nesmú použiť údaje z produkčných databáz, v opačnom prípade musia byť pre testovacie prostredie vytvorené rovnaké bezpečnostné opatrenia ako pre produkčné prostredie.

Súčasťou každého projektu OPIS2 musí byť aj definícia bezpečnostných testov. Tieto testy sa musia vykonať pred spustením predmetu projektu v produkčnom prostredí. Záverečná správa, zahŕňajúca výsledky z týchto testov, musí byť súčasťou projektovej dokumentácie.

V každom projekte OPIS2 sa musia určiť role, ktoré budú vykonávať údržbu predmetu projektu po jeho zavedení do rutinnej prevádzky. Pri definícií týchto rolí a ich následnom personálnom obsadzovaní sa musia špecifikovať a zohľadniť požiadavky na ich nezlučiteľnosť (nemožnosť kumulácie rolí) a vzájomnú zastupiteľnosť.

Sumárne, v rámci riešenia tejto oblasti bezpečnosti je potrebné určiť postupy ako a akým spôsobom sa budú:

- definovať procesy riadenia bezpečnosti počas vývoja (koncept integrovanej bezpečnosti a kontinuity realizovaných činností vrátane požiadaviek na súvisiacu dokumentáciu),
- definovať katalóg bezpečnostných požiadaviek podporujúcich bezpečnosť v nasadzovaných a implementovaných IS a poskytujúcich bezpečné služby používateľom týchto IS,
- definovať požiadavky na priradenie zodpovedností.

5.3.8.2 Normatívne východiská

Táto oblasť bezpečnosti je východiskovo upravená:

- v štandarde STN ISO/IEC 27002:2005, kapitola Nákup, vývoj a údržba informačného systému, podkapitoly Bezpečnostné požiadavky systémov, Správne spracovanie v aplikáciách, Kryptografické opatrenia, Bezpečnosť systémových súborov Bezpečnosť procesov vývoja a podpory, Riadenie technických zraniteľnosti,
- vo Výnose § 40 Aktualizácia informačno-komunikačných technológií.

5.3.9 Monitorovanie a manažment bezpečnostných incidentov

5.3.9.1 Základné princípy

Cieľom tejto oblasti bezpečnosti je zabezpečiť včasnú identifikáciu a úspešné zvládanie bezpečnostných incidentov, ktoré môžu vzniknúť počas realizácie projektov OPIS2. Implementované postupy musia zaistiť bezprostrednú reakciu vedúcu k náprave a k minimalizácii škôd vzniknutých v dôsledku bezpečnostného incidentu.

Pod bezpečnostným incidentom sa v tomto metodickom manuáli chápe jedna alebo viacero neželaných alebo neočakávaných bezpečnostných udalostí, ktoré majú významnú pravdepodobnosť narušenia priebehu projektu OPIS2, narušenia dôležitých služieb/procesov a tým pádom aj priame alebo nepriame finančné straty (napr. v dôsledku narušenia dobrého mena, neoprávneného využívania a rozširovania digitalizovaných objektov, zlyhania poskytovania služieb verejnosti).

Tento cieľ sa v praxi dosahuje uplatňovaním nasledovných základných princípov:

- bezpečnostné incidenty na PFI, digitalizačných pracoviskách ako aj u dodávateľov sa musia nahlasovať definovaným spôsobom okamžite bez zbytočných prieťahov,
- na zvládanie bezpečnostných incidentov je potrebné definovať zaviesť jasné v praxi použiteľné postupy,
- pre bezpečnostné incidenty musí byť definovaný mechanizmus odhadu ich dôsledkov vrátane nákladov na ich zvládanie,
- pre prípady právneho pokračovania riešenia bezpečnostného incidentu sa musí zaistiť zhromažďovanie dôkazov v súlade s pravidlami platných právnych predpisov súvisiacich s predmetným incidentom.

V rámci systému zvládania bezpečnostných incidentov a zvyšovania pripravenosti na ich výskyt v rámci výkonu digitalizácie je potrebné sledovať nasledovné základné okruhy:

- včasná detekcia incidentov,
- určenie konkrétnych postupov zvládania incidentov,
- definovanie rolí a kompetencií pre proces zvládania incidentov,
- rozhodnutie o právnom pokračovaní incidentov,
- evidencia incidentov a vyčíslenie škôd.

Okamžite ako vznikne podozrenie, že došlo k bezpečnostnému incidentu, je potrebné začať zaznamenávať všetky fakty, ktoré s ním môžu súvisieť. Zdokumentovanie udalostí, systémových zmien v súboroch a skutkového stavu bezpečnostnej udalosti uľahčí ďalšie riešenie bezpečnostného incidentu. Každý krok súvisiaci s detekciou a analýzou bezpečnostného incidentu sa musí stručne zaznamenať aj s časom v ktorom sa krok vykonal.

Hlavným dôvodom zbierania dôkazov počas incidentu je zvládnutie incidentu. Tieto dôkazy sú však dôležité aj pre prípadné právne pokračovanie. V takýchto prípadoch je nutné zdokumentovať, ako sa prípadné dôkazy ďalej chránili (napr. systémové logy sa archivovali). Každý dôkaz sa musí priradiť konkrétnej osobe/osobám, ktoré ho získali a zaevidovali.

Po zvládnutí incidentu je potrebné zodpovedať najmä tieto otázky:

- Čo presne sa stalo, v akých časoch to bolo zistené ?
- Ako sa postupovalo pri riešení incidentu ? Bol postup vhodný, bolo treba improvizovať ?
- Čo sa bude robiť inak, pokiaľ sa rovnaký incident vyskytne v budúcnosti ?
- Aké opatrenia sa prijali alebo prijmú, aby sa takýto incident v budúcnosti už nevyskytol ?

5.3.9.2 Normatívne východiská

Táto oblasť bezpečnosti je východiskovo upravená:

- v štandarde STN ISO/IEC 27002:2005, kapitola Zvládanie bezpečnostných incidentov, podkapitoly Hlásenie bezpečnostných udalostí a slabín, Zvládanie bezpečnostných incidentov a kroky k náprave,
- vo Výnose § 35 Monitorovanie a manažment bezpečnostných incidentov.

5.3.10 Riadenie kontinuity procesov závislých od IS

5.3.10.1 Základné princípy

Cieľom tejto oblasti bezpečnosti je zabezpečiť nepretržitú funkčnosť procesov súvisiacich s digitalizáciou závislých od IS aj počas výpadkov IS a včasné zotavenie sa z výpadku IS.

Za týmto účelom je v praxi potrebné aplikovať nasledovné princípy:

- priority obnovy pri globálnom výpadku kľúčových IS alebo služieb súvisiacich s výkonom digitalizácie, spracovaním a prezentáciou jej výsledkov musia byť vopred stanovené,
- pre prípady výpadku týchto IS a služieb je potrebné mať spracované náhradné postupy práce,
- na zaistenie rýchlej a efektívnej obnovy funkčnosti IS a služieb pri ich výpadkoch musia byť vopred spracované základne postupy obnovy.

Maximálne tolerovateľné výpadky významných aplikácií a služieb súvisiacich s digitalizáciou musia byť vopred definované. Pre prípady poruchy majúcej za následok výpadok presahujúci tolerovateľný čas výpadku, sa musia spracovať havarijné plány.

Havarijný plán obsahuje najmä:

- vymedzenie rozsahu, účelu a prípadov využitia,
- popis interných a externých rolí podieľajúcich sa na tvorbe a použití plánu,
- popis činností súvisiacich s inicializáciou plánu a rozhodnutí o aktivácii plánu,
- popis havarijných procedúr – činností slúžiacich na návrat z havarijného stavu do normálového stavu,
- popis spôsobu náhradného výkonu činností počas trvania havarijného stavu,
- zoznam kontaktných osôb/subjektov zúčastňujúcich sa na odstraňovaní havarijného stavu.

5.3.10.2 Normatívne východiská

Táto oblasť bezpečnosti je východiskovo upravená:

- v štandarde STN ISO/IEC 27002:2005, kapitola Riadenie kontinuity činností organizácie, podkapitola Aspekty riadenia kontinuity činností organizácie z hľadiska bezpečnosti informácií,
- vo Výnose § 29 Manažment rizík pre oblasť informačnej bezpečnosti, písm. f), § 33 Fyzická bezpečnosť a bezpečnosť prostredia písm. e) a písm. i).

5.3.11 Súlad s požiadavkami

5.3.11.1 Základné princípy

Digitalizácia môže byť vykonávaná iba v súlade s platnými právnymi predpismi a bezpečnostnými požiadavkami. Pri jej realizácii je veľmi dôležité vyvarovať sa porušení zákonných a zmluvných povinností a požiadaviek na bezpečný a spoľahlivý priebeh. Všetky právne normy a zmluvné požiadavky s dosahom na zbierkové predmety, digitalizované objekty a systém narábania s nimi sa musia priebežne identifikovať a zdokumentovať. S touto oblasťou úzko súvisí ďalší metodický manuál (Metodický manuál pre zabezpečenie

digitálnych práv). Súčasťou tejto oblasti bezpečnosti je aj dohliadanie na dodržiavanie požiadaviek bezpečnostnej politiky IS rezortu MK SR počas prípravy a realizácie projektov OPIS2.

Opatrenia a zodpovednosti za aplikáciu právnych predpisov legislatívnych požiadaviek musia byť zdokumentované a zavedené do praxe tak, aby nevznikali pochybnosti o súlade resp. súlad bolo možné preukázať a potvrdiť.

Pri posudzovaní právnych dosahov na aktíva, ktoré sa treba zamerať najmä na tieto oblasti:

- používanie autorských diel v súlade s autorskými zmluvami a licenčnými ustanoveniami,
- tvorba a využívanie autorských diel zamestnancami PFI a digitalizačných pracovísk,
- ochrana spracúvaných osobných údajov,
- ochrana súkromia používateľov,
- využitie ochrany obchodného tajomstva,
- využitie pracovno-právnych zákonov,
- legislatívne pokračovanie bezpečnostných incidentov v rámci pracovno-právnych predpisov.

Bezpečnú a bezproblémovú realizáciu projektov OPIS2 môže významne podporiť priebežne realizovaný audit bezpečnosti projektov OPIS2, ktorého cieľom by bolo najmä:

- hodnotenie napĺňania identifikovaných bezpečnostných opatrení,
- posudzovanie dostatočnosti, účinnosti a využívania bezpečnostných opatrení,
- iniciovanie návrhov nových bezpečnostných opatrení a reakcií na prípadné havarijné situácie alebo bezpečnostné incidenty,
- poskytovanie podpory výkonu procesov riadenia a implementácie informačnej bezpečnosti v projektoch digitalizácie
- posúdenie naplnenia právnych požiadaviek, ktoré vyplývajú z právnych predpisov súvisiacich s informačnou bezpečnosťou.

Periodicita výkonu auditu bezpečnosti predmetov projektov OPIS2 po ich zavedení do rutinnej prevádzky musí byť stanovená v intervale minimálne raz za kalendárny rok.

5.3.11.2 Normatívne východiská

Táto oblasť bezpečnosti je východiskovo upravená:

- v štandarde STN ISO/IEC 27002:2005, kapitola Súlad s požiadavkami, podkapitoly Súlad s právnymi normami, Súlad bezpečnostnými politikami, normami a technická zhoda, Hľadiská auditu informačných systémov,
- vo Výnose § 30 Kontrolný mechanizmus riadenia informačnej bezpečnosti.

5.3.12 Manažment rizík pre oblasť informačnej bezpečnosti

5.3.12.1 Základné princípy

Požiadavky na riešenie informačnej bezpečnosti v rámci projektov OPIS2 by mali byť definované aj vo väzbe na identifikované a ohodnotené bezpečnostné riziká. Výdavky na bezpečnostné opatrenia musia korešpondovať potenciálnym stratám v dôsledku výskytu rizík (finančne alebo iným spôsobom kvantifikovateľným). Výsledky hodnotenia rizík v projektoch

OPIS2 pomôžu projektovým tímom určiť a vykonať zodpovedajúce kroky k minimalizácii rizík a realizovať opatrenia s cieľom minimalizovať dôsledky v prípade naplnenia niektorého rizika.

V rámci hodnotenia rizík by riziká mali byť identifikované a kvantifikované, určený spôsob ich hodnotenia podľa závažnosti a určené kritériá pre prijatie akceptovateľných rizík. Celý proces hodnotenia rizík môže prebiehať na viacerých úrovniach a v rôznej miere detailu, v závislosti od konkrétneho projektu OPI2.

Hodnotenie rizík by malo byť vykonávané v pravidelných intervaloch (v čase prípravy projektu, počas priebehu projektu), pretože úroveň rizík sa v čase môže meniť (napríklad v dôsledku zmien pracovných postupov, zmien prostredia, nových informácií, ktoré neboli známe v čase úvodného hodnotenia rizík). Pri opakovanom hodnotení by mala byť zachovaná jednotná metodika, aby zmeny jednotlivých hodnôt rizík boli porovnateľné.

Úspešné zvládanie bezpečnostných rizík vyžaduje ich systematické riadenie. Cieľom riadenia rizík je zníženie a udržiavanie závažnosti rizík na prijateľnej úrovni. Na riadení rizík sa podieľajú role zapojené do projektov OPIS2 v rozsahu svojej pôsobnosti. Pre praktické riadenie rizík je dôležité:

- identifikovanie, definovanie a zaznamenávanie informácií o rizikách v zrozumiteľnej a vecnej forme,
- odovzdávanie informácií o rizikách (komunikácia a informačné toky) tak, aby boli informované všetky subjekty a pracovné role dotknuté rizikami.

Sumárne, riadenie rizík má prispieť k tomu, aby:

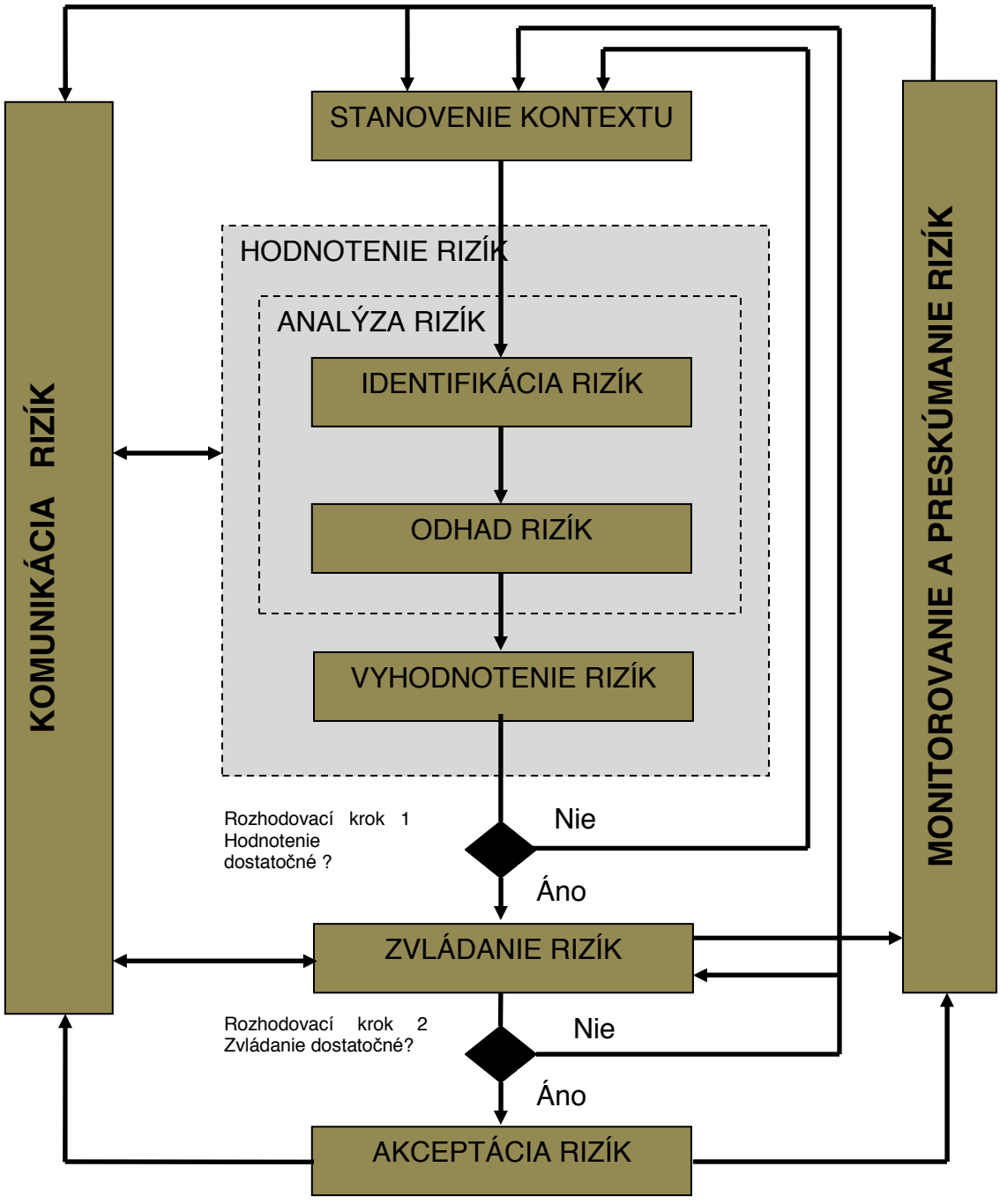
- riziká boli včas identifikované,
- hodnotenie rizík zohľadňovalo ich potenciálne dôsledky v kontexte konkrétneho projektu OPIS2 a pravdepodobnosť ich výskytu,
- pravdepodobnosť a dôsledky týchto rizík boli odkomunikované na úrovni projektových štruktúr a správne pochopené,
- bolo stanovené poradie priorít pri zvládaní rizík,
- bola stanovená priorita výkonu činností smerujúcich k zníženiu výskytu rizík,
- do rozhodovacích procesov o riadení rizík boli zapojené všetky zúčastnené strany (žiadateľ o NFP aj dodávateľ projektu OPIS2),
- bola sledovaná účinnosť zvládania rizík,
- riziká ako aj procesy ich zvládania boli priebežne sledované,
- boli získavané a aplikované informácie slúžiace k zlepšeniu prístupu k riadeniu rizík.

Účinné riadenie rizík vyžaduje štruktúru ohlasovania a vyhodnocovania, ktorá zabezpečí:

- včasnú identifikáciu a hodnotenie rizík,
- zavedenie primeraných bezpečnostných mechanizmov a reakcií na riziká.

Štruktúra ohlasovania a vyhodnocovania rizík musí podľa charakteru rizika zodpovedať tomuto metodickému manuálu a rešpektovať konkrétny charakter rizika (právny, technologický, organizačný, personálny a podobne).

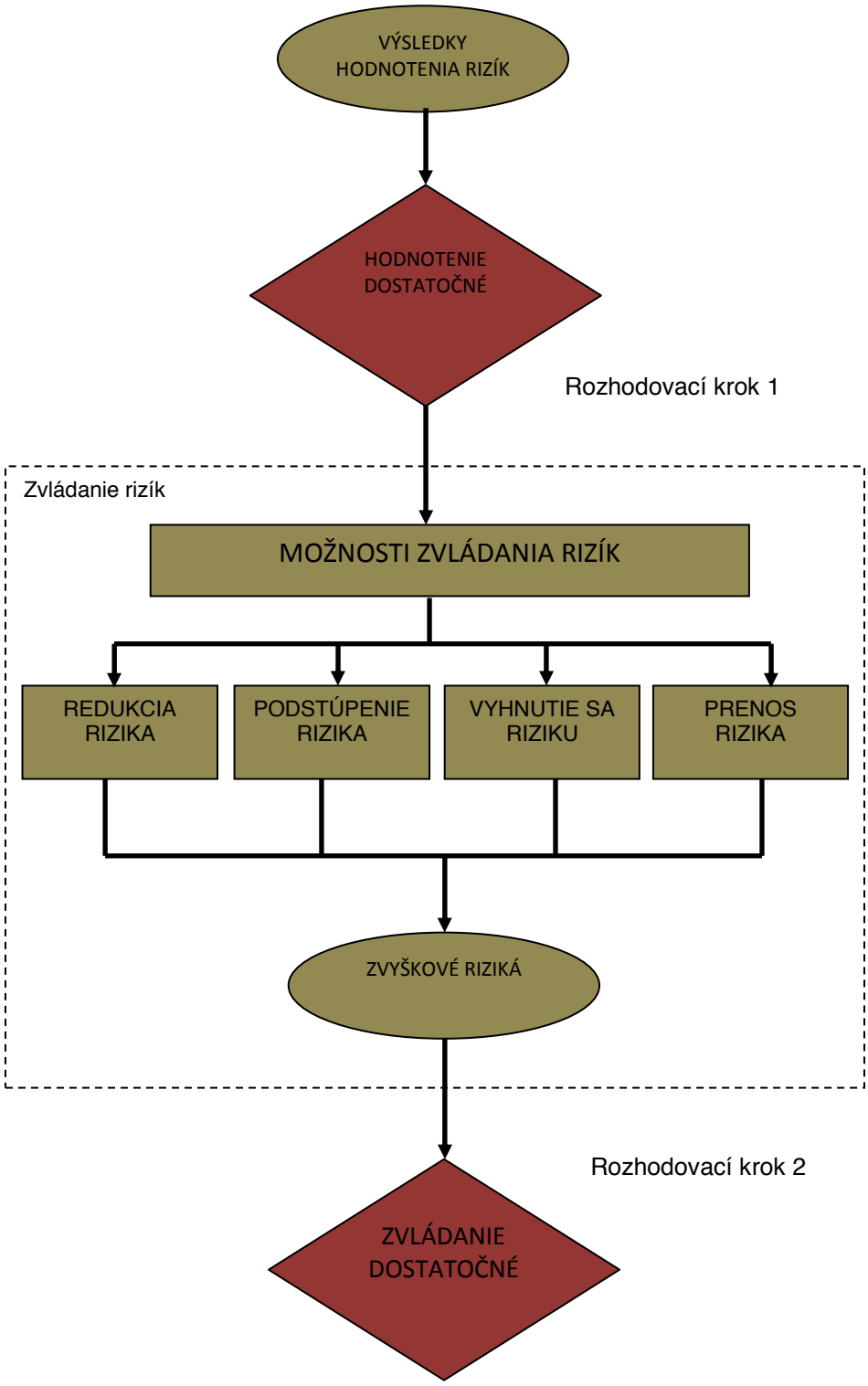
Prehľad procesu manažmentu rizík pre oblasť informačnej bezpečnosti je znázornený na nasledujúcom obrázku.



Obrázok 5.1 Proces manažmentu rizík informačnej bezpečnosti

Ako naznačuje obrázok, celý proces sa môže pri hodnotení rizík ako aj pri zvládaní rizík opakovať. Opakujúci sa prístup môže pri každej iterácii zvyšovať hĺbku a podrobnosť vykonanej činnosti. Takýto prístup zaistí rovnováhu medzi minimalizáciou času a vynaloženým úsilím potrebným na identifikáciu bezpečnostných opatrení, pričom je zaistené náležité ohodnotenie závažných rizík. Jednotlivé činnosti procesu sú podrobnejšie charakterizované a spresnené v podkapitole 6.1.13 resp. 6.2.13.

Proces zvládania rizík ilustruje nasledovný obrázok.



Obrázok 5.2 Zvládanie rizík

Pre všetky identifikované riziká musí byť deklarovaný spôsob ich zvládania alebo kombinácia spôsobov riešenia podľa uvedenej schémy:

- akceptácia (podstúpenie) rizika – rozhodnutie prijať následky potenciálnej realizácie rizika,
- vyhnutie sa riziku – rozhodnutie zmeniť prostredie, v ktorom sa riziko vyskytuje tak, aby toto riziko neprichádzalo do úvahy,
- prenesenie rizika – rozhodnutie preniesť následky realizácie rizika mimo prostredie a subjekty zúčastnené na projekte OPIS2,
- redukcia rizika – rozhodnutie pomocou vhodných opatrení dosiahnuť zníženie následkov realizácie rizika alebo zníženie pravdepodobnosti jeho realizácie.

Cieľom je zníženie rizík na prijateľnú úroveň, ktorá už ďalej nie je efektívne minimalizovateľná (napr. náklady na ďalšie zníženie rizika by prevyšovali potenciálne negatívne dôsledky jeho výskytu). Riziká tejto úrovne označujeme ako zvyškové riziká.

5.3.12.2 Normatívne východiská

Táto oblasť bezpečnosti je východiskovo upravená:

- v štandarde STN ISO/IEC 27002:2005, kapitola Hodnotenie a zvládanie rizík, podkapitoly Hodnotenie bezpečnostných rizík, Zvládanie bezpečnostných rizík, normami a technická zhoda, Hľadiská auditu informačných systémov,
- vo Výnose § 29 Manažment rizík pre oblasť informačnej bezpečnosti.

5.4 Analýza bezpečnosti

V tejto kapitole je uvedená základná analýza rizík pre hlavné aktíva vystupujúce v projektoch OPIS2. Použitá bola metóda analýzy rizík v zmysle série noriem STN ISO/IEC 13335. Cieľom kapitoly je poskytnúť východiskový prehľad o praktickej potrebe riešenia informačnej bezpečnosti v projektoch OPIS2 a spôsoboch prístupu k jej riešeniu.

5.4.1 Aktíva

Aktívum je v najširšom zmysle definície normy STN ISO/IEC 13335-1:2004 čokoľvek, čo má pre jeho vlastníka nejakú hodnotu. V prostredí projektov OPIS2 je za aktívum možné považovať každú informáciu a dokumentáciu, zmluvu, programové vybavenie, technické zariadenie, poskytovanú službu, kvalifikovaných používateľov, dobré meno a ďalšie skutočnosti, ktoré sú dôležité pre plnenie poslania prioritnej osi OPIS2 a súvisia s prevádzkou informačných a komunikačných technológií.

Aktíva, ktoré sú priamym nositeľom hodnoty v rámci projektov OPIS2 (podľa štandardu ISO/IEC 27005 nazývané primárne aktíva) sú nasledovné:

- kultúrne objekty ktoré sú predmetom digitalizácie,
- digitálne údaje o kultúrnych objektoch,
- procesy súvisiace s IKT, pre ktoré:
  - strata možnosti ich vykonávania alebo ich obmedzenie ohrozí plnenie poslania prioritnej osi OPIS2,
  - procesy, ktorých zlyhanie alebo zanedbanie môže poškodiť primárne dátové aktíva - uchovávané digitálne údaje o kultúrnych objektoch,
  - ich zmena môže významne zmeniť spôsob realizácie projektov OPIS2.

V rámci procesov ide najmä o nasledovné:

- postupnosť krokov vytvorenia digitálnych údajov o kultúrnom objekte ich spracovanie a jeho opísanie prostredníctvom atribútov objektu,
- archivácia digitálnych údajov,
- prístup k digitálnym údajom a ich prezentácia,
- možnosť správneho a jednoduchého prepojenia súvisiacich záznamov,
- koordinácia jednotlivých aktivít vykonávaných s digitálnymi údajmi.

Informácie sú najmä:

- digitálne údaje zachytávajúce podobu (vzhľad, zvuk) kultúrneho objektu, alebo sú jeho nosičom (napr. pre film),
- popisné údaje o kultúrnom objekte – klasifikácia, zatriedenie, metadáta,
- identifikačné údaje priradené jednotlivým údajom o kultúrnom objekte,
- údaje o vzťahoch medzi inými typmi informácií.

Podporné aktíva sú také aktíva, ktoré sú potrebné na zabezpečenie prevádzky/používania primárnych aktív. Ide najmä o nasledovné typy aktív:

- hardware – napr. servre, pracovné stanice, špecializovaný HW,
- generický software – napr. operačné systémy, databázové systémy, kancelárske aplikácie,
- špecializované aplikácie – najmä centrálne registre, aplikácia centrálneho archívu a príručných archívov, prezentačné aplikácie,
- riešenia dlhodobého uloženia údajov (storage systémy) – najmä diskové polia, páskové jednotky, sklady archivačných médií,
- počítačová sieť (ako služba) – najmä sieťová infraštruktúra reprezentovaná pasívnymi a aktívnymi prvkami a prevádzkovateľmi sietí,
- budovy a priestory v ktorých sú aktíva uložené,
- komunikácia (ako proces) – najmä komunikácia medzi objednávateľmi digitalizácie, dodávateľmi digitalizácie, pamäťovými a fondovými inštitúciami,
- riadenie projektov (ako proces),
- Používatelia, prevádzkovatelia a správcovia informačných systémov.

5.4.2 Atribúty bezpečnosti

Úroveň bezpečnosti ktorú je potrebné dosiahnuť pre jednotlivé aktíva sa odvíja od ich hodnoty a od požadovaného vzťahu k jednotlivým atribútom bezpečnosti.

Hodnota primárnych aktív je daná najmä nasledovnými faktormi:

- spoločenská a trhová hodnota kultúrneho objektu,
- náklady potrebné na vytvorenie, zhromaždenie a údržbu digitálnych údajov o kultúrnom objekte,
- hodnota získateľná sprístupňovaním digitálnych údajov o kultúrnom objekte na komerčnej báze.

Vyčíslenie konkrétnej (finančnej) hodnoty jednotlivých aktív je mimo rámca tohto metodického manuálu.

Základné atribúty bezpečnosti v zmysle Parkerovej hexády sú nasledovné:

- dôvernosť – stanovuje limity pre autorizovaný prístup k danému aktívu,

- vlastníctvo/kontrola – vlastník aktíva (ten pod koho kontrolou sa aktívum nachádza) rozhoduje o použití aktíva; strata vlastníctva môže znamenať stratu aj ak nie sú iné atribúty (napr. dôvernosť) dotknuté,
- integrita – stanovuje požiadavky na korektnosť a vnútornú konzistentnosť aktíva, zmena aktíva musí viesť od konzistentného stavu k inému konzistentnému stavu,
- autentickosť – určuje požiadavku na správne poznanie a možnosť overenia zdroja aktíva a jeho pravosť,
- dostupnosť – označuje možnosť použiť aktívum v čase keď je to žiadané autorizovaným spôsobom,
- užitočnosť (použiteľnosť/vhodnosť) – vyjadruje vhodnosť aktíva (jeho formy, sprístupnenia) na jednotlivé typy autorizovaného použitia.

Vzťah primárnych aktív k atribútu dôvernosti je možné charakterizovať nasledovne:

- veľká časť kultúrnych predmetov, ktoré sú predmetom digitalizácie je verejne prístupná,
- rovnako má byť prístupná časť digitálnych údajov o kultúrnom predmete,
- pri narušení dôvernosti digitálnych údajov, ktoré nie sú verejne prístupné, sa stráca možnosť ich ekonomického zhodnotenia,
- niektoré kultúrne predmety a ich digitálne reprezentácie môžu mať obmedzený režim sprístupnenia,
- úroveň ochrany dôvernosti z vyššie uvedeného dôvodu závisí na konkrétnom kultúrnom objekte,
- v celom systéme ochrany dôvernosti primárnych aktív je vo všeobecnosti požadované riešenie dôvernosti na najvyššej z úrovní požadovaných pre jednotlivé objekty,
- zaistenie dôvernosti bude v systéme dosahované najmä striktným riadením prístupu k systémom a službám, zvýšenou ochranou centrálnych komponentov a organizačnými opatreniami.

Vzťah primárnych aktív k atribútu vlastníctva/kontroly je možné charakterizovať nasledovne:

- v prípade straty kontroly nad digitálnymi údajmi o kultúrnom predmete, alebo nesprávneho priradenia vlastníctva sa stráca možnosť jeho ekonomického zhodnotenia,
- možnosť vlastníctva (a z neho vyplývajúceho rozhodovania o spôsobe použitia) kultúrneho objektu a z neho odvodených digitálnych údajov je právne upravená,
- v rámci informačných systémov implementovaných v projektoch OPIS2 je preto nevyhnutné vopred analyzovať typy vlastníckych vzťahov medzi subjektmi a aktívami, umožniť tieto vzťahy aplikačne modelovať a technicky vynútiť ich dodržiavanie.

Vzťah primárnych aktív k atribútu integrity je možné charakterizovať nasledovne:

- v prípade narušenia integrity kultúrneho predmetu je nenahraditeľne stratená časť jeho hodnoty (prípadne celá jeho hodnota),
- v prípade narušenia integrity digitálnych údajov o kultúrnom predmete je stratená hodnota vložená do ich vytvorenia a v niektorých prípadoch (ak daný kultúrny predmet už neexistuje, alebo nemá vyjadrenie mimo digitálnej formy) aj hodnota reprezentovaná kultúrnym predmetom,
- požiadavka zachovania integrity je primárnou pre riešenie bezpečnosti v projektoch OPIS2,
- základnými uvažovanými opatreniami na zachovanie integrity sú rigorózne pracovné postupy, viacnásobná záloha digitálnych údajov, evidovanie všetkých vykonávaných zmien, možnosť vykonania zmien iba limitovaným počtom oprávnených používateľov, striktné riadenie prístupu a vykonávanie kontrolných činností.

Vzťah primárnych aktív k atribútu autentickosti je možné charakterizovať nasledovne:

- v rámci projektov OPIS2 je predpokladaný vznik veľkého množstva digitálnych objektov, ktoré sú vzájomne prepojené sieťou vzťahov,
- autentickosť digitálneho objektu v tomto prípade znamená možnosť jeho správneho zaradenia do týchto vzťahov a možnosť spätne určiť pôvodcu tohto začlenenia,
- v prípade straty možnosti prepojenia objektu uvedenými vzťahmi (napr. nemožnosť zistiť ku ktorému kultúrnemu objektu sa dané metadáta vzťahujú) znamená spravidla stratu veľkej časti hodnoty tohto digitálneho objektu (až celú jeho hodnotu),
- autentickosť je z vyššie uvedených dôvodov veľmi dôležitým atribútom v rámci riešenia bezpečnosti v projektoch OPIS2,
- zaistenie autentickosti bude realizované pomocou pridelenia jedinečného identifikátora každému samostatnému digitálnemu objektu, modelovaním a vyhľadávaním a overovaním vzťahov medzi týmito identifikátormi.

Vzťah primárnych aktív k atribútu dostupnosti je možné charakterizovať nasledovne:

- tolerovateľné doby sprístupnenia digitálnych údajov sú v ráde sekúnd/minút, pre niektoré typy údajov (prezentácie) on-line,
- tolerovateľné doby výpadku systémov využívaných v digitalizačných procesoch odhadujeme v ráde hodiny,
- požiadavka na využívanie systémov je primárne počas pracovnej doby,
- v prípade dlhodobej straty dostupnosti systémov sa stráca možnosť ekonomického zhodnotenia digitálnych údajov a nie je možné realizovať niektoré procesy digitalizácie,
- vyššie uvedené parametre nasvedčujú, že dostupnosť systémov v projektoch OPIS2 je dôležitý parameter z dlhodobého hľadiska, voči krátkym výpadkom je značná tolerancia,
- zaistenie dostupnosti bude realizované najmä adekvátnym kapacitným plánovaním (sieťové spojenia, kapacity úložísk) a riadením kontinuity procesov.

Vzťah primárnych aktív ku atribútu užitočnosti je možné charakterizovať nasledovne:

- užitočnosť je v prípade digitálnych údajov o kultúrnych predmetoch determinovaná formátom v ktorom sú dostupné a možnosťou ich vzájomného prepojenia a vyhľadávania v nich,
- narušenie užitočnosti digitálnych objektov znamená sťaženie použitia digitálneho objektu, alebo nemožnosť jeho nájdenia (alebo priradenia ku iným objektom), ktoré má za následok nemožnosť využiť hodnotu ktorú digitálny objekt reprezentuje,
- narušenie užitočnosti bude v prípade projektov OPIS2 systémový problém – t.j. taký, ktorý sa týka celej skupiny objektov,
- v prípade systémového narušenia užitočnosti je náprava problému nákladná (objemom údajov, časovo, zmenou aplikácií, rozhraní, ...),
- z tohto dôvodu je užitočnosť považovaná za dôležitý atribút, ktorého naplnenie v projektoch OPIS2 je potrebné dostatočne naplánovať už vo fáze prípravy projektov,
- zaistenie užitočnosti bude realizované zvolením vhodných formátov pre jednotlivé typy objektov a vytvorením prepojení medzi objektmi, ktoré budú vopred navrhnuté s cieľom pokryť všetky dôležité typy narábania s digitálnymi objektmi.

5.4.3 Hrozby

Pri stanovovaní úrovne závažnosti rizík a návrhu implementácie bezpečnostných opatrení je potrebné vziať do úvahy všetky hrozby relevantné pre daný komponent informačných systémov používaných v rámci procesov digitalizácie.

Hrozby môžeme podľa ich nositeľa rozdeliť do nasledovných tried:

- prírodné sily a vyššia moc,
- organizačné problémy,
- ľudské zlyhania,
- zlyhania techniky,
- zámerné činy.

Príklady hrozieb je možné čerpať z katalógov, napr. z informatívneho zoznamu uvedeného v prílohe normy ISO/IEC 27005.

5.4.4 Riziká

V tejto časti uvádzame na ilustráciu východiskové riziká, ktoré je potrebné zohľadniť a bližšie posúdiť v jednotlivých projektoch OPIS2. Riziká boli identifikované analýzou a vyhodnotením informácií o plánovaných aktivitách projektov OPIS2.

Vo vzťahu k PFI sa jedná najmä o nasledovné riziká:

- strata zdigitalizovaných údajov,
- poškodenie digitalizovaných objektov v úložisku PFI,
- poškodenie médií na ktorých sú digitalizované objekty uložené v PFI,
- strata médií uložených v PFI.

Riziko neautorizovaného prístupu k údajom sa môže vyskytnúť tak na strane žiadateľa o NFP ako aj na strane dodávateľa.

Riziko úniku údajov mimo okruh oprávnených osôb, ktoré môže nastať:

- pri prenose PFI <-> digitalizačné pracovisko <-> dodávateľ (prenos môže byť realizovaný fyzicky prostredníctvom média alebo Internetom)
- priamo v PFI alebo na digitalizačnom pracovisku,
- u dodávateľa.

Riziko skreslenia digitalizovaných objektov (digitalizované údaje nezobrazujú pravdivo daný zbierkový predmet). Toto riziko sa v praxi môže realizovať neúmyselným zavinením, ale aj cielene.

Riziko omeškania výkonu digitalizačných činností spôsobené výpadkami/chybami použitých IKT.

Riziko nedostupnosti prezentácie digitalizovaných objektov v dôsledku výpadku/chyby IKT.

Riziko problematického až nemožného vyhľadania médiá s digitalizovanými údajmi v PFI.

Riziko prepojenia nesprávnych údajov (nesprávne metadáta, digitalizované údaje z iného kultúrneho objektu).

Riziko straty referencie k údajom (nemožnosť identifikovať z ktorého zbierkového predmetu digitalizované údaje vznikli, nemožnosť zistiť ku ktorému predmetu sa vzťahujú metadáta).

Riziko nesprávnej klasifikácie údajov (napríklad nie je identifikované že sú chránené v zmysle platných právnych predpisov, opomenutie ich označenia).

Riziko organizačných problémov (nejasné pravidlá pre komunikáciu zúčastnených strán, zasielanie a výmenu údajov).

Pri všetkých rizikách je potrebné zvážiť pravdepodobnosť/následky ich realizácie v ojedinelom prípade a vo veľkom počte opakovaných výskytov.

5.5 Ohraničenia

Cieľom tohto metodického manuálu nie je komplexná identifikácia a špecifikácia bezpečnostných postupov a požiadaviek pre bezpečnosť nad rámec informačnej bezpečnosti a elektronických informácií (súvisiacich s prípravou a realizáciou projektov OPIS2), prvkov IKT a nimi podporovaných služieb a príslušným projektovým, technologickým a personálnym rámcom. V dokumente nie sú riešené pracovné postupy a bezpečnostné požiadavky súvisiace s nárokmi na fyzickú bezpečnosť zbierkových predmetov počas ich transportu, umiestnenia a výkonu digitalizácie, otázka autorských práv, logistika a právne aspekty procesov výberu, sprístupnenia, odvozu/dovozu zbierkových predmetov a pod.

6 POPIS METODICKÉHO POSTUPU

6.1 Informačná bezpečnosť na strane žiadateľa o NFP

6.1.1 Úvod

V ďalšom teste sú popísané čiastkové metodické postupy pre oblasti bezpečnosti, ktorých princípy boli vysvetlené v predchádzajúcej kapitole. Metodické postupy je potrebné aplikovať v závislosti od konkrétneho predmetu projektu OPIS2 a s ohľadom na existujúci situáciu a prostredie, v ktorom je projekt realizovaný a implementovaný.

6.1.2 Politika bezpečnosti

6.1.2.1 Metodický postup

Pri stanovovaní politiky bezpečnosti pre projekty OPIS2 je potrebné vychádzať zo základných princípov a normatívnych východísk uvedených v časti 5.3.1 Politika bezpečnosti. Politika bezpečnosti sa týka všetkých strán zapojených do realizácie projektov OPIS2 a preto je dôležité pre každý projekt:

- určiť nositeľov kľúčových úloh v oblasti informačnej bezpečnosti v súlade s požiadavkami ostatných oblastí informačnej bezpečnosti popísanými v tomto metodickom manuáli (napríklad ktorá strana zabezpečí výkon analýzy rizík, návrh a vytvorenie havarijných plánov, popis prevádzkových postupov súvisiacej IKT infraštruktúry a podobne),
- stanoviť jasnú deľbu kompetencií a zodpovedností v oblasti informačnej bezpečnosti (ako sa zúčastnené strany budú podieľať na návrhu, výbere a implementácii bezpečnostných opatrení),
- určiť zodpovednosť za naplnenie požiadaviek na informačnú bezpečnosť v projekte OPIS2 vyplývajúcu z platných právnych predpisov.

Vyššie uvedené predstavuje kritické požiadavky, ktoré musia byť naplnené v každom projekte OPIS2. Nestanovenie alebo nejasné stanovenie zodpovedností a kompetencií môže v praxi spôsobiť problematické dosahovanie stanovených bezpečnostných cieľov alebo ich nenaplnenie, komplikácie pri akceptácii čiastkových plnení projektov OPIS2 ako aj neplánované zvyšovanie finančných prostriedkov z dôvodu dodatočnej implementácie bezpečnostných opatrení.

6.1.2.2 Ohraničenia postupu

Metodický postup pre oblasť politiky bezpečnosti nezahŕňa:

- konkretizáciu stratégie deľby kompetencií a zodpovedností spojených s informačnou bezpečnosťou v jednotlivých projektoch OPIS2.

6.1.3 Organizácia bezpečnosti

6.1.3.1 Metodický postup

Vo všetkých projektoch OPIS2 musia byť stanovené a personálne pokryté role súvisiace s:

- riadením informačnej bezpečnosti,
- výkonom činností súvisiacich s informačnou bezpečnosťou,
- kontrolou a vyhodnocovaním dosiahnutej úrovne informačnej bezpečnosti.

Tieto role plnia svoje úlohy v rámci systému riadenie informačnej bezpečnosti, ktorý je založený na cyklickej aplikácii štyroch etáp:

- plánovanie a analýza,
- zavedenie a implementácia,
- monitorovanie a kontrola,
- udržiavanie a zlepšovanie.

Priebeh jednotlivých etáp je potrebné harmonizovať s priebehom prípravných a realizačných činností projektov OPIS2.

V rámci etapy plánovania a analýzy je dôležité najmä:

- implementovať (zaviesť do praktickej aplikácie) jednotlivé metodické manuály tak, aby sa v dostatočnej miere prihliadalo na všetky aspekty informačnej bezpečnosti v nich obsiahnuté,
- navrhnúť konkrétne bezpečnostné opatrenia vo všetkých oblastiach bezpečnosti definovaných týmto metodickým manuálom.

Pri plánovaní bezpečnostných opatrení je potrebné brať do úvahy už existujúce činnosti vykonávané u jednotlivých prijímateľov NFP, ktoré môžu byť opatreniami ovplyvnené a opatrenia logicky zoskupovať podľa čiastkových okruhov bezpečnosti (napríklad opatrenia pre riadenie prístupov do IS, opatrenia pre riadenie komunikácií a prevádzky IS, opatrenia pre personálnu bezpečnosť súvisiacu s IS). Stanovené bezpečnostné opatrenia je potrebné zoradiť podľa priorít na základe parametrov:

- akútnosť potreby bezpečnostného opatrenia,
- rozsah predpokladaného uplatnenia bezpečnostného opatrenia (organizácia, lokalita, okruh bezpečnosti),
- väzby stanovených bezpečnostných opatrení na existujúce alebo pripravované aktivity a projekty (aj na tie, ktoré sa primárne netýkajú informačnej bezpečnosti),
- rešpektovanie požiadaviek platných právnych predpisov súvisiacich so stanovenými opatreniami (napríklad povinnosť dodržiavať zákonné lehoty),
- objem dostupných zdrojov a kapacít (personálnych, finančných) potrebných na implementáciu stanovených opatrení.

Pri plánovaní bezpečnostných opatrení je nutné zohľadniť výsledky analýzy rizík, ktorej závery súvisia s plánovanými opatreniami.

Pre každý riešený okruh informačnej bezpečnosti podľa tohto metodického manuálu sa následne implementujú špecifikované a odsúhlasené opatrenia.

Implementované môžu byť:

- technické opatrenia (napríklad získanie a inštalácia hardvérovej infraštruktúry na výkon archivácie digitalizovaných objektov, inštalácia špecializovanej bezpečnostnej aplikácie, konfigurácia bezpečnostných parametrov prvkov IKT),

- organizačné opatrenia (napríklad určenie a priradenie úloh a zodpovedností jednotlivým pozíciám v projekte OPIS2 v oblasti informačnej bezpečnosti),
- personálne opatrenia a požiadavky na vedomosti a vzdelávanie používateľov IS (napríklad plán školení, školenia používateľov IS, školenia špecialistov IS, školenia kustódov a kurátorov),
- administratívne opatrenia (napríklad vytvorenie prevádzkovej dokumentácie IS, používateľských zásad pre prácu s IS),
- kontrolné a monitorovacie opatrenia (napríklad definovanie kontrolných procesov a cieľov kontrol informačnej bezpečnosti s cieľom hodnotenia dodržiavania platných právnych predpisov, zmluvných ustanovení, bezpečnostnej politiky a ďalších riadiacich aktov, súvisiacich s informačnou bezpečnosťou).

Návrh opatrení ako aj návrh postupu ich implementácie tvorí súčasť realizácie príslušného projektu OPIS2.

Čiastkové výsledky riešenia informačnej bezpečnosti v projektoch OPIS2 a dosahovanie stanovených bezpečnostných cieľov musí byť pravidelne posudzované a vyhodnocované. Pri tomto hodnotení je dôležité zohľadnenie praktických skúseností z riešenia informačnej bezpečnosti v kontexte digitalizácie a prihliadnutie na to:

- či sú identifikované riziká adekvátne pokryté, či a aké škody v dôsledku rizík nastali,
- aké zmeny v jednotlivých oblastiach informačnej bezpečnosti vo vzťahu k projektom OPIS2 nastali a ako sú tieto zmeny z hľadiska informačnej bezpečnosti pokryté,
- či je dosahovaný súlad s požiadavkami a postupmi stanovenými v tomto metodickom manuáli a rozpracovanými v projektovej dokumentácii príslušného projektu OPIS2.

V rámci monitorovania a prehodnocovania postupov riadenia informačnej bezpečnosti a primeranosti implementovaných bezpečnostných opatrení je potrebné sledovať:

- efektívnosť, dostatočnosť a spoľahlivosť opatrení (overiť či zavedené opatrenia sú v praxi zainteresovanými subjektmi vnímané ako dostatočné, odstránili bezpečnostné nedostatky, plnia plánovaný účel),
- mieru akceptácie a využívania opatrení (overiť či sa zavedené opatrenia skutočne využívajú a dodržiavajú),
- problémy s vplyvom na informačnú bezpečnosť a ich následky (napríklad zaznamenané bezpečnostné incidenty).
- zavedenie nových centrálnych aplikácií, outsourcing služieb digitalizácie,
- zmeny v IKT súvisiacich s informačnou bezpečnosťou,
- zmeny v bezpečnostných hrozbách,
- zmeny v oblasti platných právnych predpisov.

V rámci udržiavania a zlepšovania systému riadenia informačnej bezpečnosti sa vytvárajú závery z výsledkov monitorovania, prehodnocovania, posúdení, kontrol a auditov (napríklad na schôdzach tímov projektov OPIS2). Ďalej sa:

- definuje ďalší postup pre oblasti bezpečnosti vyžadujúce si zlepšenie,
- určujú a realizujú dodatočné alebo preventívne bezpečnostné opatrenia.

Realizácia nápravných opatrení a preventívnych činností sa vykonáva priebežne počas priebehu projektu OPIS2 tak, aby bolo dosiahnuté nepretržité zlepšovanie postupov riadenia informačnej bezpečnosti

6.1.3.2 Ohraničenia postupu

Metodický postup pre oblasť organizácie bezpečnosti nezahŕňa:

- konkretizáciu náplne projektových pozícií súvisiacich s informačnou bezpečnosťou a ich obsadenie v jednotlivých projektoch OPIS2,
- spôsob interakcie projektových pozícií s existujúcimi prvkami systému riadenia informačnej bezpečnosti v rezorte MK SR.

6.1.4 Klasifikácia a riadenie aktív

6.1.4.1 Metodický postup

Cieľom riešenia klasifikácie a riadenia aktív v rámci projektu digitalizácie je upraviť spôsob implementácie bezpečnostných opatrení v tejto oblasti v projektoch OPIS2.

Aktíva súvisiace s procesmi digitalizácie je potrebné zahrnúť do evidencie ostatných IT aktív organizácie, ktorá sa na projekte OPIS zúčastňuje. Ide teda o nasledovné typy aktív:

- zariadenia IKT,
- aplikačné a programové vybavenie,
- médiá,
- spracúvané údaje o digitalizácii.

Evidenciu zariadení IKT a aplikácií odporúčame vykonávať štandardným spôsobom ako pre ostatné aktíva tohto typu v organizáciách rezortu.

Všetky médiá, ktoré budú v rámci procesu digitalizácie používané podliehajú evidencii.
Pri evidencii médií rozlišujeme nasledovné základné typy:

- médiá určené na dlhodobé uloženie údajov (archivačné médiá),
- médiá určené na interný prenos údajov pri výkone činností digitalizácie (príručné médiá),
- médiá na ktorých sú odovzdávané výsledky práce objednávateľovi digitalizácie (odovzdávacie médiá) – ide o špecifický typ média určeného na prenos údajov.

Každé médium musí mať pridelený jednoznačný identifikátor a musí ním byť označené. Identifikátory odovzdávacích médií sa vytvoria na základe schémy stanovenej dodávateľom projektu OPIS2. Ďalej musí byť každé médium zverené určitej konkrétnej osobe, ktorá zodpovedá za jeho používanie a ochranu. Údaje z príručných médií je osoba, ktorej boli médiá zverené, povinná priebežne vymazávať. Na médiách je možné mať uložené iba nevyhnutné údaje súvisiace s vykonávanou činnosťou – prenosom, archiváciou. Ukladanie údajov na médiá, ktoré nie sú vo vlastníctve žiadateľa o NFP je považované za poskytnutie údajov mimo priestory organizácie.

V prípade archivácie údajov na médiách odporúčame zriadiť samostatné príručné archívy špecificky na tento účel (t.j. nie spoločne s inými archivovanými údajmi alebo dokumentmi). Pre tieto archívy je potrebné riešiť požiadavky fyzickej bezpečnosti na porovnateľnej úrovni ako pre on-line centrálny archív. Rovnako pri výkone kontroly evidencií aktív odporúčame klásť dôraz na médiá, ich stav, spôsob uloženia a identifikáciu.

Pri procesoch digitalizácie bude vznikať veľké množstvo údajov rôzneho typu. Pre zachovanie kontroly nad prebiehajúcimi procesmi je potrebné tieto údaje a ich tok správne riadiť a klasifikovať. Základom riadenia toku údajov je presná špecifikácia jednotlivých vykonávaných procesov, ich vstupov a výstupov a rozdelenie zodpovedností. Túto

špecifikáciu je potrebné doplniť v čo najširšej miere automatizovanou správu údajov prostredníctvom vhodného aplikačného vybavenia, či už špecifického pre digitalizáciu, alebo generického, napr. pre riadenie projektov alebo riadenie obehu dokumentov.

Ďalej je pre každé aktívum potrebné mať stanoveného jeho vlastníka. Vlastník zodpovedá za zaistenie zodpovedajúcej klasifikácie aktív a vymedzenie požiadaviek na ich bezpečnosť a riadenie prístupu k nim. Stanovenie vlastníkov aktív typu zariadenia a APV odporúčame riešiť štandardným spôsobom napr. ako pre iné centralizované informačné systémy. Zvýšenú pozornosť odporúčame venovať určeniu vlastníctva digitálnych údajov.

Zodpovednosť za používanie a ochranu aktív môže byť vlastníkom ďalej delegovaná, napr. pre zariadenia ktoré sú zverené konkrétnemu zamestnancovi.

Tie aktíva, ktoré sú nevyhnutne potrebné na úspešnú realizáciu procesov digitalizácie, sú považované za kritické aktíva. Týmto aktívam a ich zabezpečeniu je potrebné venovať zvýšenú pozornosť. Za určenie aktív ako kritických zodpovedajú ich vlastníci a sú pre ne prioritne riešené procesy riadenia kontinuity činností (havarijné plánovanie).

Z hľadiska klasifikácie údajov podľa dôvernosti odporúčame vytvoriť a zaviesť klasifikačný stupeň – „digitálne údaje o kultúrnom objekte“, do ktorého patria tak samotné digitálne zobrazenia kultúrnych objektov ako aj pomocné, technické či iné metadáta. Pre tento klasifikačný stupeň by mali platiť nasledovné zásady:

- dokumenty obsahujúce tieto údaje musia byť povinne označené,
- údaje musia jednoznačne identifikované na základe stanovených pravidiel,
- prístup k týmto údajom majú mať iba určené osoby,
- na vysokej úrovni spoľahlivosti je potrebné je potrebné zaistiť ochranu integrity údajov – najmä ochranu pred samovoľným poškodením údajov, stratou a krádežou,
- zakázané je sprístupňovanie, poskytovanie a zverejňovanie týchto údajov (mimo explicitne dohodnuté prípady),
- údaje sú určené na dlhodobú archiváciu.

Pre časť digitálnych údajov o kultúrnom objekte je plánované ich zverejnenie (prezentácia). Tieto údaje odporúčame klasifikovať stupňom „verejné informácie“, ktorý sa bude používať zároveň s označením „digitálne údaje o kultúrnom objekte“. Pre tento typ údajov odporúčame zvážiť možnosť nasadenia technických opatrení s cieľom presadenia autorsko-právnej ochrany údajov, resp. zabrániť nekontrolovanému šíreniu a používaniu údajov – napr. identifikácia autora/vlastníka pomocou „digitálnej vodotlače“, zobrazenie spôsobom sťažujúcim kopírovanie a v neposlednom rade viditeľným uvedením odkazu na pravidlá používania zverejnených materiálov.

Pri klasifikácii z hľadiska spôsobu uloženia je základným východiskom skutočnosť, že primárne uvažované uloženie digitálnych údajov bude v špecializovanom informačnom systéme – centrálnom archíve, príručných archívoch a pod. V rámci tohto systému odporúčame (odhliadnuc od systému riadenia prístupu) implementovať podporu pre rolu vlastníka jednotlivých údajov, ktorý rozhoduje o udelení a zmene oprávnení na prácu s údajmi ďalším používateľom. V používateľskom rozhraní aplikácie odporúčame viditeľne informovať o podmienkach jej používania – napr. pri prihlasovaní používateľa. Pri zobrazovaní údajov v aplikácii odporúčame zobrazovať aj informáciu o ich klasifikácii.

Pri prenose digitálnych údajov o kultúrnom objekte prostredníctvom elektronickej pošty odporúčame postupovať rovnako ako pri prenose údajov klasifikovaných ako „citlivé informácie“. V tele správy je potrebné uviesť klasifikačné stupne informácií ktoré sú

prenášané. Vo všeobecnosti odporúčame elektronickú poštu na prenos týchto údajov nepoužívať, najmä nie pri prenose mimo organizáciu.

Ak sú digitálne údaje o kultúrnom dedičstve súčasťou dokumentov kancelárskeho systému, v záhlaví dokumentu je potrebné tento klasifikačný stupeň uviesť. Zabezpečenie dokumentov odporúčame realizovať v úrovni podobnej ako pre stupeň „citlivé informácie“.

Podrobnejšie informácie o stupňoch klasifikácie aktív sú uvedené v Metodickom pokyne Ministerstva kultúry Slovenskej republiky č. MK–2349/2009-10/2396 z 20. februára 2009 pre klasifikáciu a riadenie aktív informačných systémov.

Podrobnosti o klasifikácii aktív ktoré sú z hľadiska digitalizácie kritické (konvertované objekty), upravuje Metodický manuál pre zabezpečenie jednoznačnej a trvalej identifikácie konvertovaných objektov.

6.1.4.2 Ohraničenia postupu

Metodický postup pre riadenie a klasifikáciu aktív nezahŕňa:

- algoritmus vytvorenia identifikátorov pre jednotlivé typy aktív a spôsob zachovania ich jedinečnosti,
- riešenie evidencie a klasifikácie fyzických objektov, ktoré sú predmetom digitalizácie,
- spôsob práce s digitálnymi údajmi klasifikovanými ako utajované skutočnosti.

6.1.5 Personálna bezpečnosť

6.1.5.1 Metodický postup

Cieľom riešenia personálnej bezpečnosti vo vzťahu k PFI, úložiskám a digitalizačným pracoviskám je ubezpečiť sa, že osoby pokrývajúce pozície pre technickú implementáciu projektov OPIS2 sú dostatočne oboznámené so svojimi povinnosťami a zodpovednosťami. Súčasťou prijímaných opatrení je aj minimalizácia rizika ľudskej chyby, krádeže, podvodu alebo zneužitia oprávnení či prístupu k zbierkovým predmetom a digitalizovaným objektom.

Pre technickú implementáciu projektov OPIS2 bolo identifikovaných viacero nových rolí, napríklad:

- asistenti kurátorov,
- manažér digitalizačného pracoviska,
- operátor digitalizačného pracoviska.

Zodpovednosti zamestnancov pôsobiacich v jednotlivých pracovných pozíciách by mali byť stanovené a zdokumentované. Pri týchto zamestnancov musí byť zaistené:

- naplnenie požiadaviek na ochranu aktív pred neautorizovaným prístupom, modifikáciou, zničením alebo porušením,
- naplnenie požiadaviek na bezpečnosť vykonávania špecifických postupov alebo činností (napríklad vo vzťahu k charakteru zbierkových predmetov, ktoré sú predmetom digitalizácie),
- naplnenie požiadaviek na určenie jednoznačnej zodpovednosti za vykonané činnosti,
- úplné osvojenie postupov pre nahlasovanie neštandardných situácií, havarijných stavov alebo bezpečnostných incidentov.

Súčasťou prijímacieho konania nového zamestnanca alebo zaradenia existujúceho zamestnanca do role súvisiacej s výkonom digitalizácie musí byť vysvetlenie vyššie uvedených požiadaviek a s nimi súvisiacich postupov.

Všetci uchádzači o pracovné pozície súvisiace s technickou implementáciou projektov OPIS2 by mali byť kvalifikačne preverení rovnako by mala byť preverená ich trestná bezúhonnosť. Obsah previerky by mal vychádzať z požiadaviek kladených na konkrétnu rolu, ktorú potenciálny zamestnanec pri výkone digitalizácie bude zastávať. Pri preverovaní je dôležité tiež zohľadniť riziká, ktoré sú spojené s výkonom činností príslušnej role.

Vlastné preverovanie nesmie obmedziť práva prijímaného zamestnanca na dodržanie súkromia, ochranu osobných údajov a nesmie byť v rozpore s platnými právnymi predpismi (napríklad so Zákonníkom práce).

Súčasťou overovania kvalifikačných a etických predpokladov potenciálneho zamestnanca by mali byť:

- kontrola životopisu uchádzača (s ohľadom na vierohodnosť uvedených pracovných skúseností),
- overenie uvádzaného vzdelania a odbornej kvalifikácie,
- overenie totožnosti,
- odpis z registra trestov.

V prípade, že pracovná pozícia prijímaného zamestnanca zahŕňa prístup k aktívam s vysokou hodnotou, je vhodné vykonať aj detailnejšie overenia spoľahlivosti a bezúhonnosti prijímanej osoby.

Podobné previerky by mali byť vykonané aj v prípade externých spolupracovníkov. V prípade, že pracovníka zabezpečí externá špecializovaná agentúra, mala by byť explicitne zmluvne špecifikovaná jej zodpovednosť a povinnosť vo vzťahu k preverovaniu.

Informácie získavané v zmysle vyššie uvedených overovacích postupov majú charakter osobných údajov. Pri ich získavaní a nakladaní s nimi je potrebné riadiť sa zákonom o ochrane osobných údajov a postupovať podľa smerníc MK SR a organizácií v zriaďovacej pôsobnosti MK SR na ochranu osobných údajov v IS.

Pracovné zmluvy zamestnancov zaradených na pozície v rámci technickej implementácie projektov OPIS2 by mali zohľadňovať bezpečnostné požiadavky kladené na výkon pracovných činností. Okrem štandardných klauzúl by mali tiež obsahovať:

- úpravu práv a právnej zodpovednosti zamestnancov (napríklad vo vzťahu k autorskému zákonu, zákonu na ochranu osobných údajov prípadne k iným platným právnym predpisom súvisiacim s činnosťami vykonávanými na danej pozícii),
- stanovenie zodpovednosti za zverené aktíva, napríklad za zbierkové predmety, digitalizované objekty a s nimi súvisiace informácie, s ktorými bude zamestnanec prichádzať do styku,
- stanovenie zodpovednosti za prácu s informáciami prijatými v rámci digitalizácie od dodávateľov digitalizácie,
- rozšírenie zodpovednosti aj mimo bežnej pracovnej doby a mimo sídla resp. priestorov organizácie (napríklad v prípade, že digitalizácia si vyžaduje aktívnu účasť zamestnanca PFI/digitalizačného pracoviska u dodávateľa).

Počas trvania pracovného vzťahu je dôležité, aby si zamestnanci pri výkone činností technickej implementácie projektov OPIS2 boli vedomí bezpečnostných hrozieb, svojich povinností a zodpovedností a boli pripravení podieľať sa na minimalizácii rizík súvisiacich so zlyhaním ľudského faktoru. Zamestnanci by sa mali absolvovať (formálne alebo neformálne) školenia správneho výkonu pracovných postupov. Pre prípady vedomého narušenia bezpečnosti by mali byť vopred stanovené a štatutárnym zástupcom organizácie odsúhlasené zásady pre disciplinárne konania (v pracovnom poriadku organizácie alebo v inej vnútornej smernici).

Vedúci pracovníci (napríklad manažér príslušného projektu OPIS2, manažér digitalizačného pracoviska) podieľajúci sa na zabezpečovaní výkonu prác v rámci projektov OPIS2 by mali:

- oboznámiť zamestnancov s jednotlivými metodickými manuálmi, ktoré súvisia s vykonávanými prácami zamestnancov,
- dostatočne informovať zamestnancov o ich zodpovednostiach ešte pred tým, ako budú zapojení do konkrétnych prác,
- zaistiť, že zamestnanci pri výkone prác budú dodržiavať zmluvné ustanovenia, ktorými sú zmluvné strany projektov OPIS2 viazané.

Pokiaľ zamestnanci nebudú dostatočne informovaní a oboznámení o svojich zodpovednostiach, môžu počas výkonu prác spôsobiť nezanedbateľné škody. O poučení zamestnancov by mala byť vedená písomná evidencia. Podcenenie riadenia zamestnancov môže v extrémnom prípade viesť k vedomému alebo nevedomému zneužitiu aktív zamestnancami.

V prípade preukázateľného porušenia bezpečnosti by voči zamestnancovi malo byť vedené disciplinárne konanie. Toto konanie by malo zodpovedať povahe porušenia bezpečnosti a dôsledkom porušenia. Zohľadniť je tiež potrebné, či narušenie bezpečnosti znamenalo zároveň aj porušenie zmluvných ustanovení s dodávateľom projektu OPIS2 resp. porušenie niektorého zákona. V extrémnom prípade (v závislosti od charakteru narušenia bezpečnosti a jeho dôsledkov) môže byť narušenie oznámené orgánom činným v trestnom konaní.

Ukončenie pracovného vzťahu by malo tiež prebiehať riadeným spôsobom. Ukončenie pôsobenia zamestnanca v niektorej pozícii na technickej implementácii projektu OPIS2 vyžaduje jednoznačné určenie zodpovednosti za priebeh ukončenia pracovného vzťahu, za odovzdanie prideleného vybavenia a agendy za ktorú niesol zamestnanec zodpovednosť. Rozviazanie pracovného pomeru musí rešpektovať podmienky obsiahnuté v pracovnej zmluve ako aj prípadné povinnosti zamestnanca pretrvávajúce i po ukončení pracovného vzťahu.

Celý proces ukončenia pracovného vzťahu by mal zaistiť aj vysporiadanie práv k autorským dielam, ktoré zamestnanec vytvoril počas autorského vzťahu. V prípade, že zamestnanec disponoval špecifickými informáciami alebo know-how, ktorý je dôležitý z hľadiska zachovania kontinuity ním vykonávaných činností, musí byť zaistené ich zdokumentovanie a odovzdanie určenému zamestnancovi (PFI resp. digitalizačného pracoviska).

V rámci ukončenia pracovného vzťahu by mali byť zamestnancovi aj odobrané prístupové práva k jednotlivým aplikáciám, ktoré používal (najmä z hľadiska prístupových práv k centrálnym aplikáciám a registrom). Odobratie zahŕňa aj fyzický prístup (kľúče, identifikačné karty). Konkrétny priebeh procesu ukončenia pracovného vzťahu by mal zohľadniť aj súvisiace rizikové faktory, napríklad:

- skutočnosť, či sa jedná o ukončenie iniciované zamestnávateľom a aké boli dôvody zamestnávateľa,
- mieru zodpovednosti a rozsah kompetencií a oprávnení zamestnanca,

- hodnotu aktív, ku ktorým mal zamestnanec prístup resp. ktoré mu boli zverené.

6.1.5.2 Ohraničenia postupu

Metodický postup pre oblasť personálnej bezpečnosti nezahŕňa:

- spôsob výkonu previerok z hľadiska bezpečnosti prístupu k utajovaným skutočnostiam a práce s nimi.

6.1.6 Fyzická bezpečnosť a bezpečnosť prostredia

6.1.6.1 Metodický postup

Cieľom riešenia fyzickej bezpečnosti a bezpečnosti prostredia vo vzťahu k jednotlivým PFI, centrálnej infraštruktúre a digitalizačným pracoviskám je zníženie rizika neautorizovaného prístupu do priestorov kde sú uložené významné aktíva a rizika poškodenia alebo zásahu do prevádzkovaných systémov a informácií.

Fyzickú bezpečnosť je nevyhnutné riešiť samostatne pre jednotlivé celky zariadení IT / infraštruktúry používanej v rámci procesov digitalizácie. Zaistenie fyzickej bezpečnosti je nevyhnutné riešiť najmä pre:

- jednotlivé lokality centrálneho archívu,
- komunikačnú infraštruktúru potrebnú pre plynulý priebeh procesov digitalizácie (počítačová sieť, telekomunikačná sieť),
- ostatné centrálne aplikačné a databázové servery,
- pracovné stanice z ktorých je realizovaný prístup do centrálnych aplikácií, alebo pomocou ktorých sú spracúvané digitalizované objekty,
- servery umiestnené v rámci jednotlivých PFI (napr. príručné archívy),
- médiá obsahujúce údaje súvisiace s digitalizáciou a sklady médií.

Základným nástrojom na zaistenie fyzickej bezpečnosti je umiestnenie prostriedkov IT spracovávajúcich kritické alebo citlivé informácie do zabezpečenej zóny chránenej definovaných bezpečnostným perimetrom.

Bezpečnostné zóny by mali spĺňať nasledovné opatrenia:

- Na základe vykonania analýzy rizík pre daný typ aktív ktorý bude v zóne uložený je potrebné stanoviť umiestnenie a rozsah bezpečnostného perimetru a jeho základné bezpečnostné charakteristiky.
- V obvode budovy, v ktorej sa nachádza zabezpečená zóna, by nemali existovať slabé miesta, steny by mali mať pevnú konštrukciu, vstupné dvere by mali byť chránené pred neautorizovaným vstupom bezpečnostnými opatreniami (napr. mreže, alarmy, zámky). Pokiaľ sa v budove nikto nenachádza, okná a dvere by mali byť zavreté a zaistené. Ak sa zabezpečená zóna nachádza na prízemí, odporúčame zvážiť možnosť inštalácie mreží na okná, alebo použitie porovnateľných bezpečnostných mechanizmov.
- Vstup do objektu by mal byť umožnený iba cez kontrolovaný bod – vrátnica, recepcia a pod. Vstup môže byť povolený iba oprávneným osobám, prístup verejnosti je zakázaný.
- Tam kde je to možné, je vhodné použiť fyzické bariéry tak, aby chránili zabezpečenú zónu pred neautorizovaným vstupom alebo pôsobením prírodných živlov.

- Zvýšenú pozornosť je potrebné venovať protipožiarnej odolnosti priestorov. Požiarna odolnosť použitých materiálov by mala byť vopred známa a volená dostatočne na realizáciu havarijných plánov.
- Vchodové dvere a dosiahnuteľné okná by mali byť vybavené detekčným systémom. Miestnosti s kľúčovými komponentmi, verejne prístupné priestory, opustené priestory a dosiahnuteľné okná, resp. iné vstupové cesty by mali byť nepretržite monitorované.
- Požiadavky fyzickej bezpečnosti a protipožiarnej bezpečnosti je nutné riešiť v súlade s platnými právnymi predpismi a normami pre túto oblasť bezpečnosti.
- Prostriedky spracovania a ukladania informácií spravované PFI a digitalizačným pracoviskom je potrebné mať umiestnené, alebo uložené oddelene od tých, ktoré sú v správe dodávateľa projektu OPIS2.

Umiestnenie priestorov do bezpečnostných zón je vykonané na základe:
- vyžadovaného stupňa ochrany významných aktív ktoré sú v priestoroch spracúvané,
- určenia osôb ktoré majú do priestorov povolený vstup,
- režimu vstupu a pobytu osôb v priestoroch.

Z pohľadu výkonu digitalizačných procesov je kritickým prvkom fyzickej bezpečnosti prevoz zbierkových predmetov a ich ochrana. Technické a režimové opatrenia súvisiace s týmto prvkom musia zodpovedať hodnote zbierkového objektu, jeho materiálovým charakteristikám a jeho požiadavkám na fyzikálne vlastnosti prostredia, v ktorom je umiestnený.

6.1.6.2 Ohraničenia postupu

Metodický postup pre oblasť fyzickej bezpečnosti a bezpečnosti prostredia nezahŕňa:
- špecifické požiadavky kladené na ochranu zbierkových predmetov počas ich umiestnenia a transportu.

6.1.7 Riadenie komunikácií a prevádzky

6.1.7.1 Metodický postup

Cieľom riešenia bezpečnosti v oblasti riadenia komunikácií a prevádzky je stanoviť taký súbor bezpečnostných opatrení, aby pri prevádzke informačných systémov bola úroveň ich bezpečnosti na požadovanej úrovni.

Základnými doménami riešenými v tejto oblasti bezpečnosti sú:
- prevádzkové postupy a zodpovednosti,
- riadenie dodávok od tretích strán,
- plánovanie a systém preberania IS,
- ochrana pred škodlivým kódom,
- zálohovanie,
- správa siete,
- bezpečnosť práce s médiami,
- výmeny informácií,
- služby elektronického obchodu,
- monitorovanie systémov.

Základným nástrojom riadenia prevádzky informačných systémov je vytvorenie prevádzkovej dokumentácie a jej udržiavanie v aktuálnom stave. V rámci prevádzkovej dokumentácie by mali byť zachytené najmä:

- pravidelne vykonávané činnosti údržby IS,
- parametre konfigurácie IS a ich hodnoty,
- postupy a činnosti riešenia havarijných stavov,
- rozdelenie rolí pri správe a údržbe systému,
- komunikačné rozhrania systému a identifikácia komunikujúcich systémov,
- politika riadenia prístupu k systému (bližšie rozobratá v kapitole 6.1.8 Riadenie prístupov),
- plán výkonu servisu a kontakty na servisných partnerov,
- postupy používania a vyhodnocovania auditných záznamov.

Prevádzková dokumentácia, rovnako ako ďalšia dokumentácia k IS musí byť chránená pred neautorizovaným prístupom, poškodením a stratou.

V prostredí produkčného systému nie je prípustné vykonávať testovanie a ďalší vývoj, jednotlivé prostredia (vývojové/testovacie/produkčné) musia byť vzájomne oddelené tak, aby vývojové a testovacie prostredie nemohlo narušiť prevádzku produkčného prostredia. Rovnako musí byť oddelené riadenie prístupov do jednotlivých prostredí. Pre vývojové a testovacie účely je možné používať iba tie údaje z produkčného prostredia, ktoré sú vopred schválené. Pred prenosom údajov odporúčame vykonať ich anonymizáciu, čiastočné znehodnotenie alebo pozmenenie tak, aby pri ich úniku nedošlo k stratám.

V prostredí produkčného systému je treba všetky zmeny – či už aktualizácie systému, alebo zmeny konfigurácií – vykonávať riadeným spôsobom tak, aby bolo minimalizované riziko výpadku systému, alebo poškodenia údajov.

Prostredie informačných systémov procesov digitalizácie musí byť adekvátne chránené pred vplyvom škodlivých kódov tak na úrovni pracovných staníc ako aj na úrovni centrálnych komponentov – serverov, ich operačného systému a systémových aplikácií. Za týmto účelom je potrebné zaviesť nasledovné opatrenia:

- nasadenie antivírusového nástroja na všetky pracovné stanice a servery, jeho pravidelná a automatická aktualizácia,
- pravidelná kontrola hlavných častí operačného systému a APV na prítomnosť škodlivých kódov antivírusovým nástrojom,
- kontrola prichádzajúcich správ elektronickej pošty,
- na pracovných staniciach automatická aktualizácia operačného systému a aplikácií na prácu s elektronickou poštou a prehliadačom WWW stránok, na serveroch riadené vykonávanie aktualizácie,
- zákaz používania cudzích médií, neautorizovaných aplikácií a prinášania údajov z neautorizovaných zdrojov.

V rámci procesov digitalizácie predpokladáme, že časť údajov bude objednávateľovi digitalizácie odovzdávaná na médiách a vzhľadom na objemnosť týchto údajov tieto médiá budú pravdepodobne aj naďalej používané. Preto by pre prácu s médiami mali byť stanovené formalizované pravidlá[7], ktoré budú zahŕňať:

- ochranu médií pred poškodením, zničením alebo stratou kvality záznamu,
- viacnásobné zálohovanie obsahu archivačných médií (aby pri poškodení jednej kópie nedošlo k strate údajov),

[7] Postupy pri práci s médiami sú čiastočne rozobrané v kapitole 6.1.4 Klasifikácia a riadenie aktív

- pravidelné testovanie čitateľnosti obsahu médií,
- pravidlá identifikácie médií, ich obsahu a miesta uloženia,
- pravidlá manipulácie s médiami,
- ochranu médií pri ich prenose mimo priestory ich vlastníka,
- vymazanie, vyradenie a likvidáciu médií,
- určenie ktoré médiá môžu byť používané v procesoch digitalizácie a akým spôsobom.

Pre výmenu informácií medzi jednotlivými subjektmi v rámci procesov digitalizácie musia byť stanovené formalizované postupy, ktorých cieľom je najmä zaistiť nepopierateľnosť vykonanej operácie a stanovenie presných formátov a protokolov pri výmene. Špecifikácia konkrétnych postupov je mimo rámec tohto metodického manuálu, avšak z hľadiska bezpečnosti je potrebné zohľadniť najmä:

- ochranu pred odpočúvaním, neautorizovaným kopírovaním, modifikáciou, zničením a nesprávnym smerovaním zasielaných informácií,
- označovanie zasielaných informácií,
- špecifikáciu komunikačných kanálov, ktoré je možné použiť (napr. sieť Internet, siete wifi, elektronická pošta) a parametre ich zabezpečenia,
- ochranu autentickosti zasielaných informácií,
- pravidlá archivácie prijatých informácií,
- vykonávanie výmen informácií iba obojstranne odsúhlasenými postupmi a na základe dohody oboch zúčastnených strán,
- bezpečnosť médií pri preprave.

Pod službami elektronického obchodu v zmysle normy ISO/IEC 27002 v rámci projektov OPIS2 rozumieme sprístupňovanie digitálneho obsahu o kultúrnych predmetoch ďalším subjektom (za úhradu). Pre tieto procesy je potrebné vytvoriť bezpečnostný rámec, ktorý zabezpečí minimalizáciu rizík neoprávneného prístupu k údajom, ich zmeny či poškodenia, nedostupnosti a pravosti údajov a riziká plynúce z platobného styku. Zohľadnené musia byť najmä nasledovné aspekty:

- rozdelenie zodpovednosti medzi zúčastnené strany,
- vytvorenie dôveryhodnej identity oboch strán,
- dostatočné mechanizmy autentifikácie a autorizácie,
- ochrana dôvernosti a autentickosti posielaných informácií,
- kontrolné mechanizmy,
- odolnosť systémov pred útokmi vedenými prostredníctvom počítačových sietí,
- transakčné spracovanie požiadaviek,
- spoľahlivý platobný systém,
- ochrana pred neoprávneným použitím údajov (aj zverejnených).

Informačné systémy a aktivity, ktoré v nich používatelia vykonávajú, majú byť monitorované. Monitorovanie musí byť v súlade s právne stanovenými obmedzeniami, najmä požiadavkou na ochranu súkromia používateľov.

V informačných systémoch odporúčame automaticky vytvárať auditné záznamy o aktivitách významných z hľadiska manipulácie s údajmi a o aktivitách dôležitých z hľadiska bezpečnosti systému. Ide najmä o nasledovné typy záznamov:

- úspešný aj neúspešný pokus o autentifikáciu používateľa,
- pridelenie alebo zmena používateľských oprávnení,
- zmeny konfigurácie systému,
- použitie privilegovaných oprávnení,

- odmietnutý pokus o prístup k objektom (v dôsledku nedostatočného oprávnenia používateľa),
- systémové varovania a hlásenia o chybách,
- priebeh automatických činností vykonávaných systémom,
- pre zvlášť citlivé údaje odporúčame zvážiť možnosť monitorovania každého prístupu k údajom,
- pre tie typy údajov kde je to potrebné zaznamenať každú ich zmenu (vytváranie histórie zmien objektov).

Vytváranie auditných záznamov sa zvyčajne vykonáva v jednotlivých systémoch na rôznych úrovniach – napr. na aplikačnej úrovni, na úrovni databázy, na úrovni prístupu k operačnému systému. Pre všetky vznikajúce auditné záznamy je potrebné stanoviť jednotný prístup tak, aby boli ľahko spolu použiteľne, navzájom korelovateľné a chránené na porovnateľnej úrovni. Pre centrálne aplikácie odporúčame zvážiť možnosť nasadenia jednotného systému spracovania auditných záznamov.

Aktivity vykonávané pri správe systému (administrátorom, operátormi, servisnými technikmi) je taktiež potrebné evidovať. Za týmto účelom je potrebné viesť administrátorské denníky, ktoré by mali obsahovať údaje o vykonaných údržbových a servisných činnostiach na systéme a mimoriadnych udalostiach, ktoré sa vyskytnú počas prevádzky aj s uvedením spôsobu ich riešenia.

Administrátorské denníky spolu s prevádzkovou dokumentáciu systému majú vysokú vypovedaciu hodnotu o stave systému a sú významné pri riešení mimoriadnych situácií, vyhodnocovaní fungovania systému a plánovaní jeho ďalšieho rozvoja.

V rámci procesov digitalizácie bude používaných viacero rôznych informačných systémov a ich používatelia budú z rôznych organizácií a v rôznych lokalitách. Zároveň však veľká časť údajov z týchto systémov bude vo vzájomnom vzťahu a musí byť korelovateľná. Preto odporúčame pre všetky centrálne servery a rovnako aj pracovné stanice, ktoré budú používané pri procesoch digitalizácie implementovať systém centrálnej synchronizácie času automatizovaným spôsobom.

Doména riadenia dodávok od tretích strán a plánovanie a systém preberania IS sú riešené v kapitole 6.1.9 Vývoj, nasadzovanie a údržba informačných systémov. Doména správy siete je riešená v kapitole 6.1.8 Riadenie prístupov. Problematika zálohovania je súčasťou kapitoly 6.1.11 Riadenie kontinuity procesov závislých na IS.

6.1.7.2 Ohraničenia postupu

Metodický postup pre riadenie komunikácií a prevádzky nezahŕňa:

- špecifikáciu konkrétnych postupov pri formálnej výmene (odovzdávaní) údajov,
- rozdelenie konkrétnych činností a zodpovedností pri prevádzke a správe informačných systémov.

6.1.8 Riadenie prístupov

6.1.8.1 Metodický postup

Cieľom riešenia bezpečnosti v oblasti riadenia prístupov vo vzťahu k žiadateľom o NFP je navrhnutie a implementácia súboru opatrení, ktorých cieľom je umožniť autorizovaným používateľom prístup k aktívam v čase kedy je to potrebné a naopak, minimalizovať riziko neoprávneného prístupu a nakladania s aktívami.

Z pohľadu riadenia prístupu bude IT infraštruktúra procesov digitalizácie obsahovať nasledovné domény:

- centrálne prevádzkovaná infraštruktúra (centrálny archív, podporné aplikácie, databázy),
- verejné prístupná prezentácia kultúrnych objektov,
- lokálne používané IKT počas digitalizácie (počas samotnej digitalizácie zbierkových predmetom, kancelárske aplikácie, lokálne spracovanie údajov),
- aplikácie na zber a spracovanie údajov, ktoré sú výsledkom procesov digitalizácie (napr. aplikácie správy metadát, centrálnych registrov) – tieto aplikácie budú prevádzkované spravidla centrálne.

Riadenie prístupu v každej z týchto domén sa týka iného okruhu používateľov, rôzne je použité technické zabezpečenie prevádzky v týchto doménach, aj požiadavky na bezpečnosť. Preto odporúčame riadenie prístupu v týchto doménach riešiť samostatne.

Oblasť riadenia prístupu pozostáva z nasledovných komponentov:

- politika riadenia prístupu,
- riadenie prístupu používateľov,
- zodpovednosti používateľov,
- riadenie prístupu v počítačových sieťach,
- riadenie prístupu k operačným systémom,
- riadenie prístupu k aplikáciám a informáciám,
- používanie mobilných zariadení.

Politika riadenia prístupu predstavuje formalizovaným spôsobom stanovené a dokumentované pravidlá týkajúce sa jednotlivých uvedených domén a procesov v nich prebiehajúcich. V politike riadenie prístupu sú zhrnuté zásady stanovené v ostatných komponentoch riadenia prístupu, pri zohľadnení najmä nasledovných hľadísk:

- bezpečnostné požiadavky kladené na jednotlivé aplikácie,
- identifikácia všetkých typov informácií vo vzťahu k aplikáciám a určenie rizík, ktorým sú informácie vystavené,
- pravidlá pre šírenie informácií a pravidlá schvaľovania prístupu, bezpečnostné úrovne a klasifikácia informácií,
- konzistencia prístupových pravidiel a klasifikácie informácií pre rôzne prostredia a počítačové siete,
- zodpovedajúca legislatíva a iné záväzky vo vzťahu k ochrane prístupu k údajom a službám,
- štandardné používateľské role pre výkon bežných činností,
- riadenie prístupových pravidiel v distribuovanom a sieťovom prostredí,
- oddelenie jednotlivých rolí pre riadenie prístupu,
- postupy a požiadavky formálneho schvaľovania žiadostí o prístup,
- požiadavky na výkon pravidelného auditu prístupových oprávnení,
- odobratie prístupových práv.

Riadenie prístupu používateľov zahŕňa nasledovné aspekty:

- proces registrácie používateľa,
- riadenie privilegovaných prístupov,
- správa hesiel,
- audit prístupových oprávnení.

Pre proces registrácie používateľa by mal existovať formalizovaný postup pre získanie prístupu k systému, zmenu oprávnení a zrušenie oprávnení používateľa. Základom pre prístup ku systémom má byť unikátny používateľský identifikátor priradený každému oprávnenému používateľovi. Použitie skupinových identít by malo byť umožnené iba tam, kde je to nevyhnutne potrebné.

Povolenie a rozsah prístupu používateľa by mali vychádzať z rozhodnutia vlastníka systému, alebo informácií ku ktorým sa prístup udeľuje. Rozsah pridelených oprávnení je potrebné stanoviť tak, aby to zodpovedalo zámerom jednotlivých projektov OPIS2. Základným princípom pre riadenie prístupu je pravidlo, že čo nie je explicitne povolené, je zakázané a prístup je povoľovaný iba na základe potreby (need to know). Do praxe je tiež vhodné zaviesť procesy automatického zablokovania prístupu po vypršaní lehoty platnosti udeleného súhlasu.

Súčasťou dokumentácie riadenia prístupu majú byť písomné (alebo obdobné elektronické) žiadosti o udelenie prístupu pre používateľa a súhlas s rešpektovaním stanovených pravidiel prístupu a používania systémov podpísaný používateľom.

Umožnenie privilegovaného prístupu do systémov (administrátorské oprávnenia, oprávnenia modifikovať konfiguráciu systému) by malo byť obmedzené na úzky okruh určených operátorov. Pre každú z privilegovaných rolí by mal byť zdokumentovaný jej účel, rutinne vykonávané operácie (administrátorská príručka), popis privilegovaných oprávnení v systéme. Vhodné je taktiež oddeľovať bežné používateľské prístupové účty od privilegovaných (aj ak sú používané jednou osobou). Pri citlivých operáciách odporúčame vytvoriť oddelené privilegované role tak, aby bola vždy zachovaná možnosť krížovej kontroly jednotlivých používateľov.

Pre autentifikáciu do informačných systémov odporúčame použiť heslá (iné autentifikačné systémy majú pri počte používateľov predpokladanom pre procesy digitalizácie vysoké náklady na údržbu). Používanie hesiel odporúčame realizovať na základe formalizovanej politiky stanovujúcej povinné parametre hesiel (napr. minimálnu dĺžku hesla, použitie kombinácie sád znakov) aj procesy údržby systému hesiel (proces vydania prvotného hesla, postup pri zabudnutí hesla používateľom). Zvolená implementácia autentifikačného systému nesmie nikde ukladať heslá v nechránenej forme. Používatelia majú byť formálne zaviazaní chrániť svoje heslá pre vyzradením, nezaznamenávať (nepísať) ich, nezdieľať pridelený prístup do IS s inými osobami a nahlasovať podozrenia na kompromitáciu používateľskej identity.

Pre privilegované prístupy do systémov so zvýšeným stupňom vyžadovanej bezpečnosti odporúčame zvážiť nasadenie dvojfaktorových autentifikačných mechanizmov – na základe autentifikačného predmetu a hesla/pin-u.

V pravidelných intervaloch je potrebné vykonávať audit existujúcich používateľských účtov a pridelených oprávnení. V rámci tohto auditu je potrebné overiť najmä dodržiavanie politiky riadenia prístupov do systému, opodstatnenosť existencie prístupových oprávnení a súlad

medzi evidenciou o schválených prístupoch a skutočným stavom. Audit odporúčame vykonať minimálne raz ročne, pre privilegované prístupy minimálne raz za 6 mesiacov.

Pre zariadenia, ktoré môžu ostať neobsluhované, je potrebné prijať adekvátne opatrenia na minimalizáciu rizika neautorizovaného prístupu. Rovnako pracovné prostredie používateľov, v ktorom sa môžu nachádzať citlivé údaje má byť udržiavané v súlade so zásadou „prázdneho stola“ a „prázdnej obrazovky“.

V rámci riadenia prístupu k počítačovým sieťam odporúčame implementovať nasledovné opatrenia:

- významné celky infraštruktúry budovať v samostatnej časti siete,
- pre tieto segmenty samostatne riešiť bezpečnosť na úrovni sieťovej vrstvy (firewall, blokovanie portov, IDS/IPS),
- umožnenie prístupu iba k nevyhnutne potrebným sieťovým službám (politika default-deny),
- tam, kde sú citlivé informácie prenášané nedôveryhodnou sieťou (napr. Internet), je potrebné nasadiť ochranu dôvernosti kryptografickými mechanizmy ochrany,
- smerovanie v sieti je potrebné realizovať takým spôsobom, aby bolo minimalizované riziko odpočúvania komunikácie.

Prístup k operačnému systému zariadení používaných v procesoch digitalizácie odporúčame minimalizovať. Používanie systémových nástrojov má byť umožnené iba určeným administrátorom.

Odporúčame časovo limitovať udržiavanie aktívnych sieťových spojení v prípade ak používateľ nie je prítomný (napr. odišiel od počítača).

Informačné systémy budované v rámci projektov OPIS2 budú umožňovať pripojenie a prácu na diaľku (nie sú viazané na určitú lokalitu – fyzické ani sieťové prostredie). Preto treba venovať zvýšenú pozornosť zabezpečeniu komunikácie používateľa s aplikáciou tak, aby bolo minimalizované riziko odpočúvania citlivých alebo údajov (napr. autentifikačné údaje používateľa), riziko narušenia integrity údajov pri prenose, aby bola zaručená nespochybniteľnosť identity a aktivít používateľa. Za týmto účelom odporúčame vypracovať formalizované pravidlá, ktoré budú tiež riešiť podmienky umožnenia prístupu zo zariadení mimo správu prevádzkovateľa informačného systému. Prístup prostredníctvom privilegovaných rolí (napr. administrácia systému) odporúčame z takýchto zariadení vylúčiť.

Pre použitie mobilných výpočtových zariadení musia byť stanovené formalizované pravidlá a opatrenia, ktorých cieľom je minimalizácia rizika odcudzenia/straty mobilného zariadenia a neautorizovanému prístupu k nemu. Tieto pravidlá by mali riešiť najmä opatrenia fyzickej bezpečnosti mobilných zariadení, riadenie prístupu k nim, ochranu dôvernosti použitím kryptografických techník, zálohovanie údajov, antivírovú ochranu, podmienky pripájania sa do počítačových sietí, použitie mobilného zariadenia na verejných priestranstvách.

6.1.8.2 Ohraničenia postupu

Metodický postup pre riadenie prístupov nezahŕňa:

- riadenie prístupu k zbierkovým predmetom ktoré sú predmetom digitalizácie,
- špecifikáciu jednotlivých rolí v informačných systémoch budovaných v rámci projektov OPIS2,

- vzťahy medzi rolami a rozdelenie zodpovednosti pri schvaľovaní prístupových oprávnení.

6.1.9 Vývoj, nasadzovanie a údržba informačných systémov

6.1.9.1 Metodický postup

V rámci všetkých projektov OPIS2 sa musí z technicko-realizačného pohľadu vykonať minimálne:

- analýza rizík súvisiacich s vývojom, plánovaným nasadením, využívaním a prevádzkovým prostredím predmetu projektu
- identifikácia a špecifikácia bezpečnostných požiadaviek,
- návrh bezpečnostných testov a návrh formy overenia bezpečnosti služieb a aplikácií tvoriacich súčasť predmetu projektu OPIS2 pred ich zavedením do rutinnej prevádzky,
- špecifikácia pozícií, ktoré budú zabezpečovať údržbu systémov a aplikácií po ich zavedení do rutinnej prevádzky,
- vypracovanie príslušnej projektovej dokumentácie.

Základné technicko-realizačného požiadavky na informačnú bezpečnosť v oblasti vývoja a dodávky IKT a aplikácií sú rozdelené do nasledovných okruhov:

- požiadavky na bezpečnosť počas vývoja,
- požiadavky na bezpečnosť predmetu projektu OPIS2,
- požiadavky na bezpečnosť počas prevádzky,
- požiadavky na súlad (s platnými právnymi predpismi, s požiadavkami na validáciu výstupov projektu a podobne).

Vyššie uvedené okruhy bezpečnostných požiadaviek sa napĺňajú v rámci nasledovných okruhov činností:

- príprava žiadosti o NFP, verejného obstarávania a zmluvy,
- analýza a špecifikácia požiadaviek na bezpečnostné funkcie a bezpečnostné záruky predmetu projektu OPIS2,
- vývoj a dodávka predmetu projektu OPIS2,
- testovanie a akceptačné konanie,
- zavedenie do produkčnej prevádzky a dokumentácia,
- riadenie zmien a dodávateľská podpora.

Príprava žiadosti o NFP a s ním súvisiaceho verejného obstarávania je predmetom samostatnej dokumentácie k príprave a realizácii projektov OPIS2.

Z hľadiska formálnej úpravy zmluvného vzťahu je však dôležité, aby zmluva s dodávateľom obsahovala:

- meno zástupcu dodávateľa, ktorý zodpovedá za splnenie požiadaviek kladených na bezpečnosť predmetu projektu OPIS2,
- podmienky akceptácie dodávky a spôsoby otestovania predmetu projektu OPIS2,
- vymedzenie obsahu a rozsahu školení poskytnutých dodávateľom,
- určenie spôsobov poskytovania podpory pri prevádzke a rozvoji predmetu projektu OPIS2,

- popis fyzického aj logického oddelenia vývojového, testovacieho a školiaceho prostredia (pokiaľ sú súčasťou predmetného projektu) a popis ich vytvorenia a umiestenia,
- určenie rozsahu a popis obsahu plánovaných testov súvisiacich s vývojom a dodávkou predmetu projektu OPIS2 (cieľom je vyhodnotenie implementovaných bezpečnostných opatrení, ich dostatočnosť a účinnosť),
- špecifikáciu používateľskej, administrátorskej a prevádzkovej dokumentácie,
- licenčné ustanovenia ako aj možnosti prístupu oboch zmluvných strán k zdrojovému kódu po ukončení príslušného projektu,
- záväzok dodávateľa naplniť požiadavky platných právnych predpisov.

Analýza a špecifikácia požiadaviek na bezpečnostné funkcie a bezpečnostné záruky predmetu projektu je dôležitou súčasťou každého projektu OPIS2. Výsledky tejto analýzy tvoria samostatný dokument projektovej dokumentácie Pri výkone analýzy sa prihliada najmä na:

- riadenie prístupov používateľov,
- auditný subsystém (logovanie),
- bezpečnosť prevádzkového prostredia,
- formu a rozsah školení,
- ochranu spracovávaných údajov,
- zálohovanie dôležitých produkčných údajov a žurnálových súborov,
- bezpečnosť sieťovej komunikácie,
- požiadavky vyplývajúce z platných právnych predpisov.

Povinnou súčasťou katalógu požiadaviek je špecifikácia kritických výkonových parametrov a odhad nárokov predmetu projektu OPIS2, najmä:

- predpokladané objemy údajov, počty udalostí určeného typu, komunikačná náročnosť,
- časové odozvy pri práci s aplikáciami počas ich vysokého zaťaženia,
- maximálny možný počet súčasne pracujúcich používateľov.

Napĺňanie požiadaviek informačnej bezpečnosti počas vývoja a dodávky predmetu projektu OPIS2 sa realizuje vo viacerých etapách v súlade s definovanými etapami časového harmonogramu príslušného projektu OPIS2. Každá z etáp sa uzavrie súhrnným dokumentom. Jednotlivé dokumenty spoločne tvoria bezpečnostnú dokumentáciu projektu.

Bezpečnostná dokumentácia projektu obsahuje dokumenty v nasledovnom poradí:

- Koncepcia bezpečnosti,
- Bezpečnostná architektúra,
- Implementácia bezpečnostných mechanizmov,
- Posúdenie súladu.

Koncepcia bezpečnosti:

- určuje strategické ciele bezpečnosti predmetu projektu OPIS2,
- sumarizuje požiadavky na bezpečnostné funkcie predmetu projektu OPIS2,
- sumarizuje požiadavky na úroveň bezpečnosti predmetu projektu OPI2,
- stanovuje základné princípy dosahovania týchto požiadaviek.

Pri vypracúvaní Koncepcie bezpečnosti sa zohľadňujú najmä:

- požiadavky všetkých zúčastnených strán, ktoré budú využívať výsledky projektu,
- všetky predpisy, normy a štandardy súvisiace s predmetom projektu OPIS2,

- riziká ohrozujúce bezpečnosť predmetu projektu OPIS2,
- bezpečnostné mechanizmy implementované v rámci existujúcej infraštruktúry,
- praxou overené bezpečnostné postupy.

Hlavnou časťou Bezpečnostnej architektúry je kvalitatívna analýza rizík[8] a návrh bezpečnostných mechanizmov a funkcií. Bezpečnostná architektúra zaisťuje pokrytie všetkých požiadaviek zadefinovaných v Koncepcii bezpečnosti.

Bezpečnostná architektúra predmetu projektu OPIS2 obsahuje najmä:

- určenie dôležitosti spracúvaných údajov,
- umiestenie kľúčových prvkov,
- systém riadenia prístupov oprávnených používateľov k údajom a službám,
- spôsob zálohovania a archivovania údajov, nastavení a softvérových súčastí,
- ochranu údajov pri komunikácii medzi komponentmi predmetu projektu OPIS2 a pri komunikácii s jeho okolím,
- riešenie havarijných situácií a núdzovej činnosti,
- detekciu neautorizovaného prieniku alebo prístupu k predmetu projektu OPIS2 a monitorovanie využívania jeho služieb,
- riešenie technickej bezpečnosti
- riešenie personálnej bezpečnosti.

Implementácia bezpečnostných mechanizmov zaisťuje praktické zavedenie a používanie bezpečnostných mechanizmov navrhnutých v Bezpečnostnej architektúre. Dokumentácia k tejto etape obsahuje:

- popis režimu činností komponentov,
- popis nastavení a konfigurácií,
- návody pracovných postupov,
- príručky ovládania komponentov, ktoré sú nevyhnutné na správne použitie implementovaných bezpečnostných mechanizmov,
- vysvetlenie všetkých špecifík a obmedzení bezpečnostných opatrení a mechanizmov, ktoré boli navrhnuté v Bezpečnostnej architektúre,
- vysvetlenie vzťahu bezpečnostných opatrení a mechanizmov k rizikám identifikovaným v analýze rizík.

Cieľom Posúdenia súladu je:

- vyhodnotiť súlad implementovaného predmetu projektu OPIS2 so záväzkami, ktoré pre oblasť informačnej bezpečnosti deklaroval dodávateľ,
- overiť dodržanie požadovanej úrovne informačnej bezpečnosti.

Posúdenie súladu sa vykonáva prostredníctvom niektorej z nasledovných možností alebo ich kombináciou:

- testovanie (integračné, bezpečnostné, akceptačné),
- audit informačnej bezpečnosti vykonaný nezávislou spoločnosťou, ktorá sa nepodieľala na vývoji a implementácii predmetu projektu OPIS2.

Výsledky Posúdenia súladu tvoria súčasť bezpečnostnej dokumentácie projektu.

[8] Ako metodické východisko pre výkon analýzy rizík je možné použiť napríklad štandardy STN ISO/IEC 13335, BS 7799-3, ISO/IEC 27005. Prípustná je aj interná metodika dodávateľa, ktorej popis je uvedený v dokumentácii projektu OPIS2

Testovanie a akceptačné konanie prebieha podľa vopred odsúhlaseného plánu. Plán vypracuje zástupca dodávateľa, ktorý zodpovedá za naplnenie požiadaviek na bezpečnosť Súčasťou testovania (podľa charakteru príslušného projektu OPIS2) sú najmä:

- aplikačné testy,
- záťažové a výkonové testy,
- „crash“ testy,
- bezpečnostné testy.

Cieľom aplikačných testov je overenie funkčnosti predmetu projektu OPIS a jeho súladu so špecifikáciou a zmluvnými záväzkami. V testoch sa použijú všetky funkcie a možnosti, ktoré majú byť naplnené podľa špecifikácie. Odchýlky správania sa voči špecifikácii nie sú prípustné.

Otestovaná je aj činnosť pri neštandardnom správaní sa používateľa, pričom sa vykoná najmä:

- test spustenia neštandardných operácií alebo vykonanie operácií v neštandardnom či nesprávnom poradí,
- test zadania chybného alebo neštandardného vstupu zo strany používateľa.

Cieľom záťažových a výkonových testov je otestovanie zvládnutia maximálneho požadovaného alebo projektovaného výkonu aplikácií a otestovanie súčasného výkonu náročných operácií. Požaduje sa, jednotlivé aplikácie splnili takéto testy s dostatočnou rezervou. Predmetom záťažových a výkonových testov je najmä:

- otestovanie súčasného výkonu náročných operácií,
- zistenie kombinácie rutinne vykonávaných činností pri prevádzke a údržbe predmetu projektu, ktoré môžu spôsobiť stav jeho preťaženia[9],
- overenie správania sa predmetu projektu v podmienkach jeho preťaženia (v kritických stavoch).

Cieľom „crash“ testov je overenie funkčnosti predmetu projektu pri zlyhaní niektorých jeho komponentov. Pri havárii ľubovoľného komponentu (hardvéru alebo softvéru) nemôže nastať žiadny z identifikovaných kritických stavov.

Cieľom bezpečnostných testov je overenie dostatočnosti implementácie bezpečnostných požiadaviek, najmä na úrovni:

- overenia autentifikačných mechanizmov, vrátane vyhodnotenia autentifikačných záznamových logov,
- overenia autorizačných mechanizmov,
- zadávania cielene vytvorených špecifických vstupov v neprípustnom formáte alebo rozsahu.

Dôležitým míľnikom implementácie každého projektu OPIS2 bude akceptácia jeho predmetu. Akceptácia musí byť postavená na akceptačných kritériách definovaných v Implementačnom pláne projektu (viď Metodický manuál pre zabezpečenie projektového manažmentu). Akceptačné kritériá sú zoraďované podľa priorít. Tieto kritéria musí finálny predmet projektu splniť pred jeho prijatím (akceptáciou) žiadateľom o NFP, musia však byť vopred písomne schválené oboma zmluvnými stranami.

[9] Ak sa testovaním zistí kombinácia operácií, ktorá spôsobí preťaženie predmetu projektu, je potrebné túto skutočnosť uviesť v dokumentácii k predmetu projektu a stanoviť kroky, ktoré takejto situácii zabránia (napr. určenie poradia alebo výlučnosti niektorých operácií).

Súčasťou zavedenia predmetu projektu do produkčnej prevádzky je dodávka používateľskej, administrátorskej a prevádzkovej dokumentácia k predmetu projektu

Prevádzkovú a administrátorskú dokumentáciu tvorí najmä:

- popis prevádzkových postupov,
- popis bezpečnostných procedúr a ovládanie bezpečnostných mechanizmov vo vzťahu k administrátorovi,
- popis postupov zotavenia sa z bežných chýb,
- rozdelenie a popis funkcií pri prevádzke a administrácii,
- popis konfigurácie predmetu projektu a umiestenia jeho jednotlivých fyzických a aplikačných komponentov,
- politika použitia kryptografických opatrení,
- podrobný popis aktivít vyžadovaných pri systémovej administrácii.

Používateľskú dokumentáciu tvorí najmä:

- popis ovládania aplikácií a využívanie ich služieb,
- scenáre činností pre jednotlivé používateľské funkcie,
- popis bezpečnostných procedúr a ovládanie bezpečnostných mechanizmov vo vzťahu k používateľom,
- popis chybových hlásení.

Súčasťou zavedenia predmetu projektu do prevádzky je realizácia zmluvne dohodnutých školení používateľov a administrátorov. Po skončení príslušného školenia dodávateľ odovzdá dokumentáciu účastníkom školenia.

Nutnou podmienkou zavedenia predmetu projektu OPIS2 do produkčnej prevádzky je zdokumentovanie cieľových prevádzkových podmienok a činnosti (napr. prideľovanie prístupových práv, zálohovanie, rutinná údržba) .

Osobitným okruhom požiadaviek (nie len z pohľadu informačnej bezpečnosti) je validácia kľúčových údajov, ktoré budú súčasťou výkonu digitalizačných činností (digitalizované objekty, metaúdaje). Podrobnosti a metodické postupy pre validáciu upravujú príslušné metodické manuály pre zabezpečenie konverzie jednotlivých typov objektov.

Zmeny vo výstupoch projektu OPIS2 môžu prebiehať výlučne na základe formalizovaného systému riadenia zmien, ktorý určuje najmä:

- postupy zmenového konania,
- proces testovania a nasadzovania zmeny do produkčného prostredia,
- mechanizmy, ktoré zaručia zachovanie bezpečnosti na požadovanej úrovni aj po aplikácii zmeny do produkčného prostredia.

Každá zmena predmetu projektu sa vykonáva riadeným zmenovým konaním pozostávajúcim z nasledovných krokov:

- vyžiadanie zmeny,
- implementácia zmeny,
- otestovanie zmeny,
- zdokumentovanie zmeny.

6.1.9.2 Ohraničenia postupu

Metodický postup pre oblasť Vývoj, nasadzovanie a údržba informačných systémov je aplikovateľný na tie projekty OPIS2, ktorých predmetom je návrh využitia, implementácie a technická realizácia IKT, poskytovanie služieb založených na IKT alebo spracúvanie elektronických informácií.

6.1.10 Monitorovanie a manažment bezpečnostných incidentov

6.1.10.1 Metodický postup

PFI, úložiská a digitalizačné pracoviská v praxi potrebujú byť pripravené zvládať reálne naplnenie dôsledkov niektorého z bezpečnostných rizík. Pri vzniknutých bezpečnostných incidentoch sa všetky kroky súvisiace s reakciou na incident často vykonávajú až po zistení bezpečnostného incidentu (pričom mohol vzniknúť dlhší čas predtým, ako bol vôbec detekovaný). V tejto situácii sa musia potom prijímať rozhodnutia vo veľkom strese, čo môže znížiť schopnosť vykonať nasledovné základné úlohy súvisiace s reakciou na vzniknutý bezpečnostný incident na adekvátnej úrovni:

- správna identifikácia zdroja a rozsahu incidentu,
- ochrana aktív, ktoré sú uložené v IS dotknutom incidentom,
- ochrana aplikácií a sietí, ktoré môžu byť dotknuté incidentom, pri udržaní ich plnej funkčnosti a dostupnosti,
- zhromaždenie informácií na lepšie porozumenie príčinám a dôsledkom bezpečnostného incidentu (bez týchto informácií existuje riziko prijatia mylných rozhodnutí v budúcnosti),
- odvodenie poučenia do budúcnosti.

Je nutné si uvedomiť, že aj v prípade použitia komplexných prvkov ochrany a preventívnych opatrení nie je možné nikdy dosiahnuť absolútnu bezpečnosť. Vždy existuje riziko, že bezpečnostný incident môže nastať. Filozofia zvládania incidentov musí byť tvorená krokmi, ktoré budú nezávislé od typu incidentu, jeho rozsahu, stupňa závažnosti alebo dôvodov jeho vzniku.

Riešenie bezpečnostných incidentov ,ktoré:

- zapríčinili zamestnanci PFI resp. digitalizačného pracoviska,
- boli detekované v priestoroch PFI resp. digitalizačného pracoviska,

musí vychádzať zo zavedených postupov pre zvládanie bezpečnostných incidentov (pokiaľ tieto v príslušnej organizácii existujú). Postupy pre zvládanie bezpečnostných incidentov musia obsahovať minimálne:

- definíciu kontaktného miesta pre ohlasovanie bezpečnostných incidentov,
- vymedzenie udalostí chápaných ako bezpečnostné incidenty s uvedenými príkladmi,
- mechanizmy ohlasovania bezpečnostných incidentov,
- určenie rolí a ich pôsobnosti z hľadiska nahlasovania a riešenia bezpečnostných incidentov (vo vzťahu k pozíciám definovaným v rámci technickej implementácie projektov OPIS2),
- definíciu pravidiel pre úspešné zvládanie bezpečnostných incidentov,
- definíciu pravidiel pre evidenciu bezpečnostných incidentov,
- mechanizmy vyhodnotenia priebehu zvládania bezpečnostného incidentu,
- zásady pre stanovenie opatrení s cieľom zabrániť opakovaného výskytu bezpečnostného incidentu.

Samotné zvládnutie bezpečnostného incidentu v praxi predpokladá postupný výkon nasledovných okruhov činností / fáz (v uvedenom poradí):

- preventívna príprava na riešenie bezpečnostného incidentu (okruh Politika)
- zvládnutie bezpečnostného incidentu (okruhy Analýza, Komunikácia, Zber a ochrana údajov, Izolácia)
- následné činnosti vykonané po zvládnutí bezpečnostného incidentu (okruhy Obnova a Poučenie).

V ďalšom texte sú jednotlivé okruhy činností podrobnejšie vysvetlené.

Všetky pravidlá a postupy vytvárané v rámci okruhu Politika sú na istej úrovni všeobecnosti, majú prípravný a preventívny charakter. Potrebné je:

- Vytvoriť riadiace pravidlá súvisiace s riešením incidentov a zosúladiť ich s projektovým riadením projektov OPIS2, požiadavkami Výnosu, postupmi a procesmi zavedenými v PFI resp. digitalizačnom pracovisku. Na základe týchto pravidiel musí byť jednoznačné, ktorí zamestnanci sú zodpovední za vykonanie ktorých krokov, aká je priorita a poradie vykonávaných činností pri riešení incidentu. Tu je tiež vhodné miesto na určenie role/rolí zodpovedných za riešenie nahlásených bezpečnostných incidentov.
- Navrhnúť konkrétne postupy implementujúce pravidlá riešenia incidentov.
- Všetky navrhnuté pravidlá a postupy posúdiť z právneho hľadiska. Je potrebné posúdiť, či navrhnuté riešenia zodpovedajú platným právnym predpisom. Rovnako sa treba uistiť o dostatočnosti pravidiel na ochranu zamestnancov a prijímateľa NFP pred prípadnými spormi pri zneužití aktív externými osobami (napríklad zamestnancami dodávateľa digitalizácie). Zároveň musí byť jasne stanovené disciplinárne konanie pre prípady vzniku bezpečnostného incidentu v dôsledku nevhodného konania zamestnanca prijímateľa NFP.
- Zaškoliť zodpovedných zamestnancov do problematiky riešenia incidentov. Počas školenia je potrebné objasniť úlohy jednotlivých rolí pri riešení incidentov, vytvoriť kontakty medzi tými zamestnancami, ktorí budú spolupracovať pri riešení incidentu, vysvetliť aké kroky majú byť podniknuté na zdokumentovanie incidentu, komu a za akých okolností môžu byť údaje o incidente poskytnuté (napr. rozsah vyjadrení pre médiá, spôsob kontaktovania polície).

Počas Analýzy je prvoradým cieľom zistiť rozsah bezpečnostného incidentu a vzniknutých škôd a podniknúť kroky na riešenie incidentu. Na základe informácií získaných v tejto fáze budú prijaté kľúčové rozhodnutia a vykonané akcie na zvládnutie a doriešenie bezpečnostného incidentu.

Fáza Komunikácia je dôležitá z hľadiska výmeny informácií a prijímania rozhodnutí počas zvládania bezpečnostného incidentu. Všetky osoby, ktoré sú zapojené do zvládania incidentu, musia byť upovedomené o jeho vzniku a o priebehu riešenia. Okruh dotknutých osôb podľa závažnosti incidentu môže zahŕňať osoby na rôznych pozíciách vrátane riadiacich pracovníkov. Zainteresovanie riadiacich pracovníkov je dôležité, pretože práve oni sú zodpovední za:

- rozhodnutia o rozsahu a charaktere zverejnených informácií o zaznamenanom bezpečnostnom incidente,
- rozhodnutia o upovedomení tretích strán (napríklad partnerov, subdodávateľov) o bezpečnostnom incidente,
- kontaktovanie orgánov činných v trestnom konaní,

- prijatie iných strategických rozhodnutí, ktoré si zvládnutie bezpečnostného incidentu môže vyžadovať.

Vo fáze Komunikácie je potrebné vykonávať najmä nasledovné činnosti:

- vytvoriť, použiť a udržiavať kontaktné údaje osôb zainteresovaných na incidente a informácie o ich úlohe pri riešení incidentu.
- viesť podrobnú evidenciu, kto bol kontaktovaný a aké údaje mu boli poskytnuté.

Ako súčasť pravidiel pre zvládanie bezpečnostných incidentov je nutné vytvoriť politiku poskytovania informácií, v ktorej je potrebné špecifikovať:

- Ktoré osoby a organizácie majú byť informované pri odhalení incidentu a v akom poradí. Množstvo zainteresovaných osôb môže závisieť od rozsahu incidentu.
- Pre každý kontakt vymedziť rolu, ktorú zohráva pri riešení incidentu a rozsah jeho právomocí a zodpovedností.
- Ktoré údaje je možné zdieľať s danými kontaktnými osobami.
- Ktoré komunikačné mechanizmy použiť na posielanie údajov a informáciu o ich bezpečnosti (mail, telefón, fax).
- Kto má oprávnenie rozhodnúť o operatívnych zmenách politiky poskytovania informácií v prípade potreby.

V rámci Zberu a ochrany údajov sú vykonávané najmä nasledovné činnosti:

- Získanie všetkých údajov súvisiacich s incidentom. Zo získaných údajov musí jednoznačne vyplývať odpoveď na otázky kto, čo, kde, kedy, prečo a ako vykonal pri riešení incidentu.
- Zhromažďovanie a uchovanie dôkazov, ktoré môžu napomôcť pri vyšetrovaní incidentu.
- Zaručenie dôveryhodnosti zozbieraných údajov.
- Údržba získaných údajov (je potrebné zaistiť, aby údaje boli aktuálne a každá ich zmena alebo poskytnutie boli zdokumentované).
- Kontakt s kompetentnými orgánmi v prípade rozhodnutia o legislatívnom pokračovaní riešenia incidentu.

Účelom Izolácie je vykonať krátkodobé cielené akcie zamerané na zamedzenie pokračovania/rozširovania dôsledkov incidentu a zabránenie ďalším škodám.

Pri rozhodovaní, ktoré akcie podniknúť, je potrebné zvážiť nasledovné:

- celkové ohodnotenie incidentu (rozsah, dopad, škody),
- všetky výstupy analýzy (napríklad lokalizáciu zdroja incidentu),
- priority a postupy dotknutého subjektu, na základe ktorých sa riadi riešenie incidentu.

V rámci Obnovy je potrebné zaistiť obnovu všetkých pôvodných údajov, činností a služieb do stavu, aký bol pred bezpečnostným incidentom. Tento krok je najlepšie vykonať až po úplnej eliminácii možností zopakovania bezpečnostného incidentu.

Všetky úspešné aj neúspešné aktivity, ktoré prebiehali počas riešenia bezpečnostného incidentu, je potrebné vyhodnotiť a na ich základe upraviť používané postupy a bezpečnostné opatrenia.

Po uzavretí riešenia bezpečnostného incidentu sú dôležité nasledovné činnosti:

- Dorieši sa medializácia incidentu, pokiaľ je to relevantné.

- Vykoná sa záverečná analýza a zhodnotenie postupu pri riešení incidentu. Najvhodnejšou metódou je zorganizovanie stretnutia všetkých pracovníkov zúčastnených na riešení incidentu najneskôr do 3-5 pracovných dní po ukončení riešenia incidentu.
- Vykoná sa revízia adekvátnosti bezpečnostných plánov, smerníc, procedúr a poskytnutých školení zainteresovaným osobám s cieľom zabrániť opakovaniu incidentu.
- V závislosti od závažnosti incidentu je vhodné zvážiť možnosť opätovného vykonania analýzy rizík súvisiacich s aktívami, ktoré boli incidentom dotknuté.
- Ak je to relevantné, zapojiť sa do prebiehajúceho vyšetrovania incidentu.

6.1.10.2 Ohraničenia postupu

Metodický postup pre oblasť zvládania bezpečnostných incidentov nezahŕňa:
- právne riešenie príčin a dôsledkov bezpečnostných incidentov,
- postupy pre kvantifikáciu škôd zapríčinených bezpečnostným incidentom.

6.1.11 Riadenie kontinuity procesov závislých od IS

6.1.11.1 Metodický postup

Túto oblasť bezpečnosti v praxi (v konkrétnom projekte OPIS2) je potrebné riešiť v súlade s jednotlivými analytickými a realizačnými aktivitami príslušného projektu v nasledovných základných etapách:
- stratégia plánovania kontinuity (identifikácia kritických činností a závislosti na tretích stranách, identifikácia a vyhodnotenie rizík a negatívnych dopadov),
- metodika riešenia kontinuity (určenie priorít a stratégie obnovy, určenie a posúdenie možností náhradného výkonu činností, návrh riadiacich procedúr havarijných plánov),
- plány obnovy a havarijné plány (spracovanie konkrétnych plánov, návrh spôsobu údržby a aktualizácie plánov).

K zavedeniu kľúčových prvkov pre adekvátne a efektívne havarijné plánovanie v podmienkach projektov OPIS2 je potrebné zodpovedať nasledovné základné otázky:
- Aké sú kľúčové zámery a ciele projektu a jeho výstupu ?
- Aké výstupy a dosiahnuteľné výsledky sú potrebné, aby boli tieto ciele dosahované ?
- Kedy (v akých časových horizontoch) je potrebné tieto ciele dosahovať ?
- Koho (čo) je potrebné zapojiť (interne/externe), aby tieto ciele boli dosahované ?
- Ako sú/budú tieto ciele dosahované ?

Odpovede na tieto otázky si vyžadujú:
- identifikáciu a parametrizáciu kritických procesov,
- identifikáciu a parametrizáciu zdrojov.

Pri parametrizácii kritických procesov je potrebné sledovať:
- hlavné ciele, ktoré je nevyhnutné naplniť v danom procese,
- tolerovateľné výpadky (charakteristiku typov a trvania výpadkov ktoré ešte neohrozia hlavné ciele procesu, výpadky z ktorých je možné sa zotaviť bez toho aby došlo k narušeniu kľúčových služieb),

- náhradný výkon (či je možné v núdzovom prípade plniť ciele procesu iným ako štandardným spôsobom),
- minulé havárie a spôsob riešenia minulých havárií (pokiaľ sa proces využíval aj pred začiatkom projektu, je vhodné vyhodnotiť najvážnejšie výpadky procesu riešené v minulosti, typ výpadku a jeho rozsah).

Pri zdrojoch využívaných v projekte OPIS2 je potrebné identifikovať a posúdiť najmä nasledovné parametre:

- typ zdroja (interný zdroj ktorý je umiestnený u prijímateľa NFP a je pod jeho úplnou kontrolou alebo externý zdroj, ktorý je v rámci projektu dodávaný zvonka a nie je pod úplnou kontrolou prijímateľa NFP),
- spôsob zaistenia zdroja (akým spôsobom je zaistená dodávka zdroja v prípade externých zdrojov alebo akým spôsobom má prijímateľ NFP riešenú obnovu zdroja v prípade interných zdrojov),
- doba dodávky/obnovy zdroja (záväzne dohodnuté doby a termíny vťahujúce sa na skutočnosti spôsobu zaistenia zdroja),
- kritické obdobia (obdobia, v ktorých vzniká zvýšené riziko výpadku dodávky zdroja, alebo sú kladené zvýšené nároky na dodávku zdroja).

Na základe navrhnutej stratégie plánovania obnovy je v projektoch OPIS2 potrebné:

- určiť priority a stratégiu obnovy (predstavuje určenie základných havarijných stavov a s nimi súvisiacich scenárov a návrh logickej postupnosti základných krokov pri zvládaní týchto scenárov),
- určiť a posúdiť možnosti náhradného výkonu (pokiaľ nastane niektorý z identifikovaných potenciálnych havarijných stavov, je treba mať vyjasnené, aké sú možnosti zabezpečenia dočasného náhradného výkonu, po ako dlhú dobu môže tento náhradný výkon byť poskytovaný, aké dôsledky bude mať pri návrate do normálového stavu),
- navrhnúť riadiace procedúry havarijných plánov a popísať činnosti, role a zodpovednosti pri riešení havarijného stavu. Sem patrí ďalej aj popis pravidiel a procedúr pre tvorbu plánov, ich schvaľovanie, zmenové riadenie a testovanie; popis spôsobu evidencie a distribúcie plánov; návrh systému kategorizácie havárií, spôsoby komunikácie a eskalácie havárie atď.

Stratégia tvorby havarijných procedúr by v sebe mala kombinovať nasledovné hlavné prvky:

- zálohovacie a archivačné postupy ,
- alternatívne priestory na prevádzku IKT a výkon nimi zabezpečovaných procesov,
- spôsob náhrady IKT zariadení resp. ich komponentov a zdrojov potrebných pre výkon kritických procesov,
- role a zodpovednosti.

V ďalšom texte tieto hlavné prvky charakterizujeme podrobnejšie.

Zálohovacie postupy by mali určovať frekvenciu záloh, miesto ukladania záloh, konvencie pre označovanie záloh, spôsob a frekvenciu rotácie médií. V prípade, že sa na ukladanie záloh využíva fyzicky vzdialená lokalita (napr. na zmluvnom základe so špecializovaným subjektom), je potrebné určiť aj spôsob bezpečného transportu médií a spôsob ich vyžiadania a dopravy v prípade akútnej potreby.

Okrem havarijných situácií s dočasným či obmedzeným rozsahom (výpadok servera, výpadok dodávky el. energie, poškodenie diskov a pod.) je potrebné byť pripravený aj na globálne havárie (napr. požiar centrálneho archívu, globálne narušenie činnosti v dôsledku

zatopenia a pod.) s dlhodobejším trvaním a dôsledkami. Pre tieto prípady existujú nasledovné základné preventívne možnosti zaistenia náhradných priestorov/náhradného centra):

- vyhradené centrum (vlastnené a prevádzkované žiadateľom o NFP alebo jeho zriaďovateľom),
- recipročná dohoda s iným subjektom,
- komerčne prenajaté záložné centrum.

Bez ohľadu na konkrétnu možnosť, záložné centrum môže mať rôzne úrovne vybavenosti a pripravenosti na havarijný stav. Jednotlivé typy sú vysvetlené nižšie:

- Cold site predstavuje priestor, ktorý má základné infraštruktúrne vybavenie (rozvody el. energie a počítačovej siete, klimatizáciu, telekomunikačné spojenia). Celý priestor vrátane podlahy je uspôsobený na prevádzku IKT zariadení. Neobsahuje však samotné IKT komponenty ani podporné zariadenia (tlačiarne, faxy a pod.)
- Warm site je čiastočne pripravený priestor, vybavený napr. serverom schopným prevziať kľúčové procesy a podpornou infraštruktúrou (diskové pole, aktívne sieťové prvky). Môže slúžiť aj ako priestor pre čiastočné zabezpečenie bežných prevádzkových činností. V prípade havarijného stavu sa stáva priestorom, ktorý je dovybavený ďalšími IKT prvkami podľa rozsahu havárie v hlavnom centre.
- Hot site predstavuje náhradné centrum, ktoré dokáže plnohodnotne prevziať činnosti hlavného centra. Je vybavené IKT prvkami, ktoré sú predkonfigurované a môžu v krátkom čase prevziať úlohu hlavného výpočtového centra.
- Mirrored site je identická kópia hlavného centra s on-line zrkadlením transakcií. Predstavuje najvyššiu možnú formu záložného centra.

Jednotlivé typy sa od seba odlišujú predovšetkým cenou, časom potrebným na aktiváciu ako aj schopnosťou zastúpiť hlavné centrum. Tieto faktory sú zhrnuté v nasledovnej tabuľke:

Typ centra	Cena	HW vybavenie	Aktivačný čas
Cold site	Nízka	Žiadne	Dlhý
Warm site	Stredná	Čiastočné	Stredný
Hot site	Stredná/vysoká	Čiastočné/Úplné	Krátky
Mirrored site	Vysoká	Úplné	Okamžite

V prípade, že dôjde k poruche alebo poškodení IKT systémov v hlavnom centre, je dôležité mať vopred stanovený spôsob náhrady IKT zariadení. Existujú tri základné stratégie prístupu:

- Dohody s dodávateľmi – súčasťou prípravy postupov pre prípad havarijnej situácie sú aj SLA s dodávateľmi kľúčových IKT komponentov. SLA by mali špecifikovať dobu odozvy dodávateľa po požiadavke na zásah. Súčasťou by malo byť tiež dohodnutie priorít zásahu do strany dodávateľa pre prípad rozsiahlej havarijnej situácie, ktorá si bude vyžadovať aktiváciu záložného centra (v závislosti od typu záložného centra).
- Záložný sklad – potrebné IKT komponenty môžu byť zakúpené resp. zapožičané aj vopred a uložené mimo hlavného centra.
- Existujúce kompatibilné zariadenia – aktuálne používanie zariadenia môžu byť dimenzované tak, aby v prípade potreby dokázali prevziať úlohu vypadnutých zariadení. Príkladom je umiestnenie niektorého kľúčového servera v záložnom centre. V prípade výpadku hlavného centra môže server umiestnený v záložnom

centre pri vhodnom dimenzovaní dočasne prevziať kľúčové činnosti poškodených serverov.

Po výbere zálohovacích postupov, implementácii stratégie obnovy a definícii spôsobu využitia náhradných ITK komponentov a ďalších zdrojov je veľmi dôležité určiť role a zodpovednosti, ktoré súvisia s implementáciou havarijného plánovania v bežnej praxi. Existujú nasledovné hlavné role:

- Osoba s rozhodovacími právomocami na aktiváciu havarijného plánu pri havárii menšieho rozsahu. Mala by mať definovaného zástupcu.
- Osoba s rozhodovacími právomocami na aktiváciu havarijného plánu pri havárii väčšieho rozsahu. Mala by mať definovaného zástupcu (zástupcov) pre jednotlivé okruhy riadenia.
- Administrátor havarijných plánov – zodpovedá za administratívnu údržbu havarijných plánov, sleduje ich aktuálnosť, eviduje ich využitie, testovanie a prípadne revízie. Mal by mať definovaného zástupcu.
- Vedúci havarijného tímu – zodpovedá za vypracovanie, úplnosť, aktuálnosť, praktickú použiteľnosť a testovanie príslušných plánov ako aj za aplikáciu plánu v relevantnej havarijnej situácii. Mal by mať definovaného zástupcu.
- Člen havarijného tímu so zodpovednosťou za obnovu aplikačného prostredia podľa príslušného havarijného plánu
- Člen havarijného tímu so zodpovednosťou za obnovu hardvérového prostredia a operačných systémov podľa príslušného havarijného plánu
- Člen havarijného tímu so zodpovednosťou za obnovu databáz podľa príslušného havarijného plánu
- Člen havarijného tímu so zodpovednosťou za obnovu sieťovej infraštruktúry podľa príslušného havarijného plánu
- Člen havarijného tímu so zodpovednosťou za zachovanie bezpečnosti počas a po havarijnej situácii.

Havarijný plán musí byť udržiavaný tak, aby bol stále aktuálny a zohľadňoval reálnu organizačnú štruktúru, systémové požiadavky, požiadavky na zabezpečenie dostupnosti činností podporujúcich chod kľúčových procesov. Je dôležité procedurálne zabezpečiť, aby jednotlivé havarijné plány boli pravidelne zhodnotené a aktualizované v prípade organizačných, technologických resp. iných zmien. Všeobecným pravidlom je ročná periodicita vyhodnotenia celého plánu, niektoré jeho časti však môžu byť aj častejšie (napr. zoznam kontaktných informácií).

Zhodnotenie plánu by malo zahŕňať:

- operačné požiadavky (požiadavky na zabezpečenie zdrojov, činností a procesov),
- bezpečnostné požiadavky,
- technické procedúry,
- hardvér, softvér a podporné zariadenia (napr. UPS, sieťová kabeláž),
- mená a kontaktné informácie,
- pripravenosť záložného centra (ak súvisí s havarijným plánom),
- iné dôležité záznamy súvisiace plánom (papierové aj elektronické).

Dôležitým prvkom údržby havarijných plánov je ich testovanie. Každý plán by mal byť otestovaný z hľadiska jeho funkčnosti a efektivity. Testy by mali pokrývať nasledovné okruhy:

- obnova údajov zo záložných médií,
- koordinácia osôb podieľajúcich sa na postupoch podľa havarijného plánu,

- aktuálnosť údajov v havarijnom pláne,
- obnova normálového stavu,
- notifikačné procedúry.

6.1.11.2 Ohraničenia postupu

Metodický postup pre oblasť riadenia kontinuity procesov závislých od IS nezahŕňa:

- špecifikáciu technických opatrení slúžiacich k zaisteniu kontinuity kritických procesov,
- konkrétne postupy pre zvládanie havarijných situácií (tieto je potrebné vypracovať ako súčasť príslušného projektu OPIS2).

6.1.12 Súlad s požiadavkami

6.1.12.1 Metodický postup

Základným cieľom tejto oblasti bezpečnosti z pohľadu žiadateľov o NFP je vyvarovať sa porušení zákonných a zmluvných povinností a požiadaviek na bezpečný a spoľahlivý priebeh. Všetky právne normy a zmluvné požiadavky s dosahom na zbierkové predmety, digitalizované objekty a systém narábania s nimi sa musia priebežne identifikovať a zdokumentovať.

Pre všetky informačné systémy a aktíva vytvárané a spracúvané v projektoch OPIS2 musia byť identifikované a zdokumentované zákonné a zmluvné požiadavky a musí byť definovaný spôsob, akým tieto požiadavky žiadateľ o NFP bude napĺňať. Tento špecifický okruh bezpečnosti je metodicky podrobne zdokumentovaný v samostatnom metodickom manuáli (Metodický manuál pre zabezpečenie digitálnych práv).

Dosahovanie súladu z hľadiska autorsko-právnej ochrany vyžaduje implementáciu adekvátnych technologických a organizačných opatrení. Príkladom je riadenie prístupov a správa oprávnení k digitalizovaným objektom. Východiská o dosahovaní tejto formy súladu sú uvedené vo vyššie spomenutom metodickom manuáli.

Z hľadiska realizácie projektov OPIS2 je dôležité, aby všetky informačné aktíva a záznamy o narábaní s nimi (konverzia, vizualizácia, digitalizácia) boli chránené proti strate, zničeniu, sfalšovaniu alebo neoprávnenému použitiu. Informačné aktíva je vhodné z hľadiska informačnej bezpečnosti kategorizovať podľa druhu (databázové záznamy, digitalizované objekty, metaúdaje a podobne) ako aj podľa druhu média na ktorom sú uložené.

Z hľadiska narábania s osobnými údajmi v prostredí projektov OPIS2 sa žiadateľ o NFP riadi svojimi internými predpismi upravujúcimi ochranu osobných údajov. V prípade, že bezpečnostný projekt žiadateľa o NFP nerieši ochranu osobných údajov, ktoré sa v projekte OPIS2 spracúvajú, je potrebné bezpečnostnú dokumentáciu k ochrane osobných údajov aktualizovať.

Všetky IKT zaobstarané a implementované v projektoch OPIS2 by mali byť využívané primárne na účely stanovené týmto projektom. Legitímnosť využívania v prípade potreby aj na iné účely musí byť vopred explicitne stanovená.

Pri nasadzovaní a využívaní IKT v prostredí projektov OPIS2 je potrebné vykonávať aj kontrolu technickej zhody. Primárnym cieľom tejto kontroly je overovanie súladu so

štandardami, politikami a bezpečnostnými smernicami, ktoré sa na tieto IKT a ich využívanie vzťahujú.

Príbuznou aktivitou je aj audit informačnej bezpečnosti. Za účelom minimalizácie narušenia bezpečnosti počas priebehu projektov OPIS2 je potrebné mať v každom projekte vopred vyjasnené požiadavky na:

- zameranie, štruktúru a obsah auditu bezpečnosti,
- spôsoby realizácie systémového auditu kľúčových prvkov IKT a služieb, ktoré tieto IKT poskytujú,
- ochranu záznamov vytváraných auditnými aplikáciami (logov).

Dôležitou súčasťou dosahovania súladu je aj potvrdenie spoľahlivosti a bezpečnosti kritických prvkov digitalizácie (akým je napríklad Centrálny systém pre správu a dlhodobé uchovávanie konvertovaných objektov). Podrobnosti o dosahovaní takéhoto typu súladu formou certifikácie upravuje Metodický manuál pre zabezpečenie dlhodobej archivácie konvertovaných objektov.

6.1.12.2 Ohraničenia postupu

Metodický postup pre oblasť súladu požiadavkami nezahŕňa:

- špecifikáciu podrobných postupov slúžiacich k dosahovaniu právneho súladu v projektoch OPIS,
- spôsob realizácie certifikácie národného archívu.

6.1.13 Manažment rizík pre oblasť informačnej bezpečnosti

6.1.13.1 Metodický postup

Z pohľadu žiadateľa o NFP je dôležité, aby v projektoch OPIS2 boli implementované činnosti procesu riadenia rizík znázornené na obrázku 5.1 v podkapitole 5.3.12.

Základným krokom je stanovenie kontextu manažmentu rizík pre oblasť informačnej bezpečnosti. Kontextom je v tomto prípade obsah príslušného projektu OPIS2. Prístup k riadeniu rizík musí zohľadniť daný kontext ako aj základné kritériá pre:

- vyhodnotenie rizík,
- vyhodnotenie dôsledkov rizík,
- akceptáciu rizík.

Kritériá pre vyhodnotenie rizík musia zohľadňovať najmä:

- kritickosť informačných aktív, ktoré sú vytvárané alebo dotknuté v projekte,
- očakávania a predstavy žiadateľa o NFP o priebehu a výsledkoch projektu,
- negatívne dôsledky straty dôveryhodnosti a narušenia dobrého mena.

Kritériá pre dôsledky výskytu rizík sú určované s ohľadom najmä na:

- narušenie výkonu činností žiadateľa o NFP,
- finančné straty,
- porušenie časových harmonogramov a nedodržanie konečných termínov,
- nedodržanie právnych, regulačných alebo zmluvných požiadaviek.

Kritériá pre akceptáciu rizík závisia na konkrétnych cieľoch príslušného projektu OPIS2 a záujmoch žiadateľa o NFP v danom projekte. Pri určovaní kritérií je potrebné brať do úvahy nasledovné špecifiká:

- Kritéria akceptácie rizík môžu obsahovať určenie oprávnení zodpovedných osôb za určitých okolností dočasne akceptovať aj riziká nad prahovou hodnotou prijateľnosti.
- Pre rôzne triedy rizík môžu platiť rôzne kritériá akceptácie rizík. Riziká, ktoré by mali za následok porušenie platných právnych predpisov nie je v žiadnom prípade možné akceptovať, ale riziká, ktoré by mali za následok porušenie niektorej zmluvnej požiadavky na dodávateľa projektu OPIS2 (napríklad nedodržanie čiastkového časového harmonogramu), je možné dočasne akceptovať.
- Kritériá akceptácie rizík môžu zahŕňať požiadavky na ich zvládanie v budúcnosti (podmienená akceptácia rizík).

Hodnotenie rizík pozostáva z nasledovných činností:

- analýza rizík zahŕňajúca:
  - identifikáciu rizík,
  - odhad rizík,
- vyhodnotenie rizík.

Účelom identifikácie rizík je určiť, čo môže spôsobiť potenciálny negatívny dôsledok. Analýza a odhadovanie rizík sa vykonáva v súlade s vopred určenou konkrétnou metodikou, ktorá je odsúhlasená žiadateľom o NFP aj dodávateľom projektu OPIS2[10].

Všetky identifikované riziká by mali byť kvantifikované alebo kvalitatívne charakterizované a prioritizované v súlade s vyššie uvedenými kritériami a cieľmi príslušného projektu OPIS2.

Po vyhodnotení rizík je potrebné určiť spôsoby, ktoré budú použité na ich zvládnutie (viď obrázok 5.2 v podkapitole 5.3.12). Spôsoby zvládania rizík by sa mali vyberať na základe výstupov z ohodnotenia rizík, predpokladaných nákladov na implementáciu bezpečnostných opatrení a očakávaných prínosov. Ak je možné zaistiť pokrytie väčšieho množstva rizík jednotným finančne nenákladným spôsobom, je potrebné tento spôsob preferovať. Ďalšie spôsoby môžu byť neefektívne a ekonomicky neobhájiteľné.

Z dôvodu potreby určenia rovnováhy medzi nákladmi na prijatie opatrení k identifikovaným rizikám a samotnými rizikami je potrebné definovať v projektovej štruktúre osoby zodpovedné za príslušné rozhodnutia .

Plánované spôsoby zvládania hodnotených rizík musia byť zdokumentované a formálne odsúhlasené. Cieľom je navrhnúť postupy zvládania rizík tak, aby vyhovovali definovaným kritériám pre akceptáciu rizík v kontexte príslušného projektu OPIS2.

Všetky riziká by mali byť predmetom priebežnej komunikácie medzi žiadateľom o NFP a dodávateľom projektu OPIS2. Účinná komunikácia je veľmi dôležitá, pretože môže mať podstatný vplyv na rozhodnutia, ktoré bude potrebné prijímať. Jej cieľom je zaistiť, aby osoby zodpovedné za funkčný manažment rizík a osoby v ktorých záujme je praktické napĺňanie úloh manažmentu rizík dospeli k vzájomnému porozumeniu. Toto porozumenie je kritické najmä pri podkladoch a dokumentoch, ktoré slúžia k zásadným rozhodnutiam. Komunikácia je obojsmerná.

[10] Rámcový postup pre analýzu a riadenia rizík v informačnej bezpečnosti určuje aj Metodický pokyn Ministerstva kultúry Slovenskej republiky č. MK-3822/2009-10/8737 z 10. júla 2009 pre analýzu a riadenie rizík informačných systémov.

Všetky informácie získavané pri manažmente rizík by mali byť priebežne monitorované a preskúmavané (napríklad pravdepodobnosť výskytu rizík, hodnota aktív) s cieľom čo najskôr identifikovať zmeny kontextu projektu OPIS2. Z tohto dôvodu je potrebné zaistiť monitorovanie:

- nových aktív, ktoré neboli zaradené do rozsahu pre manažment rizík,
- zmien v hodnotách aktív,
- nových hrozieb,
- bezpečnostných incidentov (viď podkapitoly 5.3.9, 6.1.10 a 6.2.10)

Cieľom monitorovania je kontinuálny súlad manažmentu rizík s cieľmi príslušného projektu OPIS2, záujmami žiadateľa o NFP a kritériami akceptácie rizík. Proces manažmentu rizík by mal byť trvalou súčasťou každého projektu OPIS2.

6.1.13.2 Ohraničenia postupu

Metodický postup pre oblasť hodnotenia a zvládania rizík nezahŕňa:

- riziká mimo oblasť informačnej bezpečnosti, t.j. finančné riziká, riziká súvisiace s administráciou projektov OPIS2, riziká právneho charakteru (napríklad vysporiadanie autorských práv), riziká súvisiace s technologickými procesmi digitalizácie (napríklad s deacidifikáciou) a ďalšie podobné riziká.

6.1.14 Spôsob implementácie postupu

Postup zabezpečenia informačnej bezpečnosti počas prípravy a realizácie projektu OPIS2 zo strany žiadateľa o NFP, digitalizačného pracoviska a PFI musí byť implementovaný:

- v súlade s celkovým projektovým plánom projektu, do ktorého je riešenie informačnej bezpečnosti začlenené,
- s prihliadnutím na požiadavky platných právnych predpisov súvisiacich s informačnou bezpečnosťou, ktoré korešpondujú s predmetom príslušného projektu OPIS2,
- s ohľadom na existujúce riadiace akty prijímateľa NFP alebo jeho zriaďovateľa.

V závislosti od rozsahu príslušného projektu OPIS2 je na základe tohto metodického manuálu potrebné vypracovať samostatný bezpečnostný projekt, ktorý bude zahrnutý do celkovej projektovej dokumentácie. Obsah, rozsah, zameranie a časti bezpečnostného projektu musia zodpovedať požiadavkám uvedeným v jednotlivých oblastiach bezpečnosti v tomto metodickom manuáli. Vypracovanie bezpečnostného projektu je zodpovednosťou dodávateľa.

6.2 Informačná bezpečnosť vo vzťahu k dodávateľom projektov OPIS2

6.2.1 Úvod

Dodávatelia projektov OPIS2 (externé subjekty) sú z hľadiska bezpečnosti chápané ako tretie strany, na ktoré sa v rámci poskytovania služieb vzťahujú samostatné bezpečnostné požiadavky. Ich identifikácia a záväzok pokrytia zo strany dodávateľa musia byť súčasťou príslušnej zmluvy s dodávateľom. Dodávateľ tieto záväzky prenáša aj na svojich subdodávateľov. Bezpečnostná politika IS rezortu MK SR bude vo všetkých projektoch záväzná pre dodávateľov projektov OPIS2, ako aj pre žiadateľov o NFP.

6.2.2 Politika bezpečnosti

6.2.2.1 Metodický postup

Dodávatelia sa v projektoch OPIS2 riadia aplikovateľnými ustanoveniami politiky bezpečnosti príslušného žiadateľa o NFP. V praxi je dôležité najmä naplnenie požiadaviek uvedených v 6.1.2 Politika bezpečnosti.

6.2.2.2 Ohraničenia postupu

Metodický postup pre oblasť politiky bezpečnosti nezahŕňa:

- konkretizáciu stratégie deľby kompetencií a zodpovedností spojených s informačnou bezpečnosťou v jednotlivých projektoch OPIS2.

6.2.3 Organizácia bezpečnosti

6.2.3.1 Metodický postup

Všetky činnosti súvisiace s riadením informačnej bezpečnosti, návrhom, implementáciou a využívaním bezpečnostných opatrení by mali byť koordinované prostredníctvom určených zástupcov dodávateľa. Títo zástupcovia musia zaisťovať súčinnosť všetkých subdodávateľských skupín, odborníkov na špecifické oblasti (napríklad poistenie) a nimi realizovaných aktivít vrátane projektového riadenia, zaisťovania súladu s platnými právnymi predpismi, rozhodovaním v krízových situáciách (napr. pri zatopení priestorov v ktorých sú umiestnené zbierkové predmety).

Za týmto účelom je v súlade s metodickým manuálom dôležité určiť všetky postupy riadenia bezpečnosti poskytovaných služieb a spracúvaných údajov v súlade s potrebami a prioritami jednotlivých prijímateľov NFP, ako aj s platnými právnymi predpismi.

Pred samotným výkonom činností realizovaných v rámci projektu OPIS2 musí byť vykonaná analýza rizík, súvisiacich s poskytovaním služieb dodávateľským spôsobom. Pri identifikácii rizík je potrebné zobrať do úvahy nasledovné:

- typ prístupu, aký bude mať dodávateľ k jednotlivým aktívam PFI, úložiska alebo digitalizačného pracoviska,
- hodnota a kritickosť jednotlivých aktív,
- identifikácia personálu na strane dodávateľa, ktorý bude mať prístup k jednotlivým aktívam,
- spôsob, akým bude určená a overená identita dodávateľského personálu,
- obmedzenia alebo záväzky vyplývajúce z platných právnych predpisov súvisiacich s predmetom plnenia pripravovaného zmluvného vzťahu.

Dodávateľ pri uzatváraní príslušnej zmluvy v zmluvných podmienkach stanoví konkrétne bezpečnostné záruky tak, aby boli minimalizované identifikované riziká. Potenciálne riziká môžu byť napríklad:

- nekontrolovaný pohyb pracovníkov dodávateľa v priestoroch PFI, úložiska alebo digitalizačného pracoviska počas plnenia zmluvy,
- neoprávnený prístup zamestnancov dodávateľa do IS v priestoroch PFI, úložiska alebo digitalizačného pracoviska,
- nedostatočné personálne a odborné kapacity dodávateľa potrebné pre plnenie zmluvy,
- nedostatočná možnosť kontroly rozsahu a kvality služieb poskytovaných dodávateľom,
- neúmyselné poškodenie zbierkových predmetov aktivitami zamestnancov externého dodávateľa,
- nejasné kritéria pre akceptáciu digitalizovaného objektu.

Za účelom minimalizácie identifikovaných rizík sa v zmluve s dodávateľom musia stanoviť konkrétne zásady najmä pre:

- príchod, odchod a pohyb zamestnancov dodávateľa v priestoroch PFI alebo digitalizačného pracoviska počas plnenia zmluvy,
- prideľovanie oprávnení na prístup do všetkých IS (napríklad centrálny systém pre evidenciu digitalizovaných zbierkových predmetov, centrálne registre), s ktorými zamestnanci dodávateľa prídu do styku počas plnenia zmluvy,
- sprístupňovanie informácií zamestnancom dodávateľa na médiách (DVD, páska, USB kľúč a podobne) a vynášanie týchto médií mimo priestorov PFI alebo digitalizačného pracoviska,
- bezpečný prenos informácií elektronickou poštou prípadne zákaz jej využívania na prenos digitalizovaných objektov,
- výkon zmluvne dohodnutých prác tak, aby nedošlo k poškodeniu alebo zničeniu kľúčových aktív (zbierkové predmety) alebo narušeniu digitalizačných služieb,
- zdokumentovanie poskytnutých prác s cieľom ich evidencie a možnosti spätnej kontroly.

Prístup dodávateľa k riadeniu a implementácii bezpečnostných opatrení súvisiacich s digitalizáciou by mal byť v prípade pochybností zo strany vlastníka zbierkového predmetu preskúmaný (táto možnosť by mala byť zmluvne stanovená).

6.2.3.2 Ohraničenia postupu

Metodický postup pre oblasť organizácie bezpečnosti nezahŕňa:

- organizáciu bezpečnosti v prípade, že digitalizovaný objekt je z kategórie utajovaných skutočností,
- mechanizmy riadenia bezpečnosti a ochrany zbierkových predmetov počas ich transportu a prijatia dodávateľom digitalizácie.

6.2.4 Klasifikácia a riadenie aktív

6.2.4.1 Metodický postup

Cieľom riešenia klasifikácie a riadenia aktív vo vzťahu ku dodávateľovi projektu OPIS2 je vytvorenie a udržiavanie úplného a aktuálneho prehľadu o aktívach zahrnutých do procesu digitalizácie a stanovenie adekvátnych požiadaviek na prácu s nimi a ich bezpečnosť.

V rámci rezortu Ministerstva kultúry SR je táto oblasť upravená v Metodickom pokyne Ministerstva kultúry Slovenskej republiky č. MK–2349/2009-10/2396 z 20. februára 2009 pre klasifikáciu a riadenie aktív informačných systémov, stanovujúcim konkrétne povinnosti v tejto oblasti. Dodávateľ projektu OPIS2 by mal dosiahnuť porovnateľnú úroveň bezpečnosti v tejto oblasti, aká je týmto metodickým pokynom vyžadovaná.

Základným nástrojom v tejto oblasti je vytvorenie evidencie o jednotlivých typoch aktív. Vo vzťahu k dodávateľovi projektu OPIS2 je vyžadované vedenie evidencie pre tie aktíva, ktoré bezprostredne súvisia s výkonom procesov digitalizácie, spracovaním, uložením a transportom údajom vytváraných pri digitalizácii.

Evidenciu je potrebné viesť pre nasledovné typy aktív:

- zariadenia IKT,
- aplikačné a programové vybavenie,
- médiá,
- spracúvané údaje o digitalizácii.

Každé zariadenie používané pri procesoch digitalizácie musí byť jednoznačne označené identifikátorom a informáciou o vlastníkovi zariadenia. O týchto zariadeniach vedie dodávateľ evidenciu, ktorej súčasťou je popis určenia zariadenia, zoznam údajov o inštalovanom APV, popis miesta kde je zariadenie umiestnené, alebo označenie zariadenia ako prenosné, určenie osoby ktorej bolo zariadenie zverené do užívania a informácia o tom, či je zariadenie pripojené do počítačovej siete, alebo k inému zariadeniu.

Ak je digitalizácia vykonávaná s pomocou zariadení ktoré nie sú vo vlastníctve dodávateľa, musí ich použitie odsúhlasené objednávateľom.

Aplikačné a programové vybavenie (systémové, kancelárske alebo špecializované aplikácie) používané na IKT zariadeniach v rámci procesov digitalizácie podlieha evidencii, ktorú vedie dodávateľ projektu OPIS2. Súčasťou tejto evidencie je informácia o počte nainštalovaných kusov (licencií) aplikácie, konkrétnych zariadeniach na ktorých je aplikácia nainštalovaná a dokladoch preukazujúcich legálne nadobudnutie aplikácie (faktúra, licencia).

Všetky médiá, ktoré budú v rámci procesu digitalizácie používané podliehajú evidencii.
Pri evidencii médií rozlišujeme nasledovné základné typy:

- médiá určené na dlhodobé uloženie údajov (archivačné médiá),

- médiá určené na interný prenos údajov pri výkone činností digitalizácie (príručné médiá),
- médiá na ktorých sú odovzdávané výsledky práce žiadateľovi o NFP (odovzdávacie médiá).

Každé médium musí mať pridelený jednoznačný identifikátor a musí ním byť označené. Identifikátory odovzdávacích médií sa vytvoria na základe schémy stanovenej objednávateľom digitalizácie. Ďalej musí byť každé médium zverené určitej konkrétnej osobe, ktorá zodpovedá za jeho používanie a ochranu. Údaje z príručných médií je osoba, ktorej boli médiá zverené, povinná priebežne vymazávať. Na médiách je možné mať uložené iba nevyhnutné údaje súvisiace s vykonávanou činnosťou – prenosom, archiváciou. Ukladanie údajov na médiá, ktoré nie sú vo vlastníctve organizácie je považované za poskytnutie údajov mimo priestory organizácie.

Rozsah a spôsob archivácie údajov na médiách musí byť vopred odsúhlasený žiadateľom o NFP, vo všeobecnosti sa archivácia údajov u dodávateľa nepredpokladá.

Žiadateľ o NFP má mať právo vykonávať kontrolu úplnosti a aktuálnosti evidencie u dodávateľa.

Ďalej je pre každé aktívum potrebné mať stanoveného jeho vlastníka. Vlastník zodpovedá za zaistenie zodpovedajúcej klasifikácie aktív a vymedzenie požiadaviek na ich bezpečnosť a riadenie prístupu k nim.

Zodpovednosť za používanie a ochranu aktív môže byť vlastníkom ďalej delegovaná, napr. pre zariadenia ktoré sú zverené konkrétnemu zamestnancovi.

Pre jednotlivé typy aktív je potrebné formálne stanoviť pravidlá ich prípustného použitia, ktoré sú záväzné pre všetkých kto s týmito aktívami narábajú. Ide najmä o pravidlá nasledovného typu:

- možnosť používania zariadení na iné účely (súkromné použitie, súčasné používanie vo viacerých projektoch),
- možnosť používania APV na iné účely,
- pravidlá pripájania médií do zariadení (vlastných aj cudzích) a pravidlá prenosu médií (napr. mimo priestorov organizácie, medzi jednotlivými lokalitami výkonu digitalizácie),
- spôsob odovzdávania výsledkov digitalizácie na médiách – najmä spôsob ich doručenia, označenia, identifikáciu obsahu, preberanie,
- pravidlá používania systému elektronickej pošty,
- pravidlá používania služieb siete Internet (najmä služba www) zo zariadení používaných na digitalizáciu/spracovanie údajov,

Tie aktíva, ktoré sú nevyhnutne potrebné na úspešnú realizáciu procesov digitalizácie, sú považované za kritické aktíva. Týmto aktívam a ich zabezpečeniu je potrebné venovať zvýšenú pozornosť. Za určenie aktív ako kritických zodpovedajú ich vlastníci a sú pre ne prioritne riešené procesy riadenia kontinuity činností (havarijné plánovanie).

Všetky údaje vytvorené počas digitalizácie sú klasifikované ako citlivé údaje, pre ktoré platia nasledovné zásady:

- prístup k týmto údajom majú mať iba určené osoby,

- je potrebné zaistiť ochranu integrity údajov – najmä ochranu pred samovoľným poškodením údajov, stratou a krádežou,
- všetky údaje musia byť označené a jednoznačne identifikované na základe stanovených pravidiel,
- zakázané je sprístupňovanie, poskytovanie a zverejňovanie týchto údajov (mimo explicitne dohodnuté prípady),
- pre všetky údaje musí byť stanovená lehota ich archivácie alebo vymazanie (u dodávateľa) – napr. po zadanom čase od odovzdania výsledkov prác.

V prípade ak pre niektorý typ údajov vznikne potreba stanovenia špecifických pravidiel, odporúčame tento typ údajov klasifikovať novým stupňom a formálne pre neho stanoviť pravidlá jeho používania.

Podrobnosti o klasifikácii aktív ktoré sú z hľadiska digitalizácie kritické (konvertované objekty), upravuje Metodický manuál pre zabezpečenie jednoznačnej a trvalej identifikácie konvertovaných objektov.

6.2.4.2 Ohraničenia postupu

Metodický postup pre riadenie a klasifikáciu aktív nezahŕňa:

- algoritmus vytvorenia identifikátorov pre jednotlivé typy aktív a spôsob zachovania ich jedinečnosti,
- riešenie evidencie a klasifikácie digitalizovaných predmetov premiestnených počas výkonu digitalizácie k dodávateľovi služieb digitalizácie,
- spôsob preberania výstupov procesu digitalizácie objednávateľom digitalizačných služieb na médiách.

6.2.5 Personálna bezpečnosť

6.2.5.1 Metodický postup

Cieľom riešenia personálnej bezpečnosti vo vzťahu k dodávateľovi digitalizácie je ubezpečiť sa, že dodávateľ, jeho zamestnanci a subdodávatelia sú dostatočne oboznámení so svojimi povinnosťami a zodpovednosťami. Súčasťou prijímaných opatrení je aj minimalizácia rizika ľudskej chyby, krádeže, podvodu alebo zneužitia oprávnení či prístupu k zbierkovým predmetom a digitalizovaným objektom.

Zodpovednosti zamestnancov resp. pracovné role u dodávateľa by mali byť stanovené a zdokumentované. Pri týchto zamestnancov musí byť zaistené:

- naplnenie požiadaviek na ochranu aktív pred neautorizovaným prístupom, modifikáciou, zničením alebo porušením,
- naplnenie požiadaviek na vykonávanie špecifických postupov alebo činností (napríklad vo vzťahu k charakteru zbierkových predmetov, ktoré sú predmetom digitalizácie),
- naplnenie požiadaviek na určenie jednoznačnej zodpovednosti za vykonané činnosti,
- úplné osvojenie postupov pre nahlasovanie neštandardných situácií, havarijných stavov alebo bezpečnostných incidentov.

Súčasťou prijímacieho konania nového zamestnanca alebo zaradenia existujúceho zamestnanca do role súvisiacej s výkonom digitalizácie musí byť vysvetlenie vyššie uvedených požiadaviek a s nimi súvisiacich postupov. Role a zodpovednosti osôb, ktoré nie sú zamestnancami dodávateľa, ale súvisia s výkonom digitalizačných činností zo strany dodávateľa, musia byť vopred identifikované a jasne stanovené.

Všetci uchádzači o pracovné pozície u dodávateľa by mali byť kvalifikačne preverení rovnako by mala byť preverená ich trestná bezúhonnosť. Obsah previerky by mal vychádzať z požiadaviek kladených na konkrétnu rolu, ktorú potenciálny zamestnanec pri výkone digitalizácie bude zastávať. Pri preverovaní je dôležité tiež zohľadniť riziká, ktoré sú spojené s výkonom činností príslušnej role.

Vlastné preverovanie nesmie obmedziť práva prijímaného zamestnanca na dodržanie súkromia, ochranu osobných údajov a nesmie byť v rozpore s platnými právnymi predpismi (napríklad so Zákonníkom práce).

Súčasťou overovania kvalifikačných a etických predpokladov potenciálneho zamestnanca by mali byť:

- kontrola životopisu uchádzača (s ohľadom na vierohodnosť uvedených pracovných skúseností),
- overenie uvádzaného vzdelania a odbornej kvalifikácie,
- overenie totožnosti,
- odpis z registra trestov.

V prípade, že pracovná pozícia prijímaného zamestnanca obnáša prístup k aktívam s vysokou hodnotou, je vhodné vykonať aj detailnejšie overenia spoľahlivosti a bezúhonnosti prijímaného zamestnanca.

Podobné previerky by mali byť vykonané aj v prípade externých spolupracovníkov. V prípade, že pracovníka zabezpečí externá špecializovaná agentúra, mala by byť explicitne zmluvne špecifikovaná jej zodpovednosť a povinnosť vo vzťahu k preverovaniu.

Informácie získavané v zmysle vyššie uvedených overovacích postupov majú charakter osobných údajov. Pri ich získavaní a nakladaní s nimi je potrebné riadiť sa zákonom o ochrane osobných údajov.

Pracovné zmluvy zamestnancov zaradených na pozície v rámci digitalizácie by mali zohľadňovať bezpečnostné požiadavky kladené na výkon pracovných činností. Okrem štandardných klauzúl by mali tiež obsahovať:

- úpravu práv a právnej zodpovednosti zamestnancov (napríklad vo vzťahu k autorskému zákonu, zákonu na ochranu osobných údajov prípadne iné platné právne predpisy súvisiace s činnosťami vykonávanými na danej pozícii),
- stanovenie zodpovednosti za zverené aktíva (samotného dodávateľa ako aj za zbierkové predmety a s nimi súvisiace informácie, s ktorými bude zamestnanec prichádzať do styku),
- stanovenie zodpovednosti za prácu s informáciami obdržanými v rámci digitalizácie (od PFI alebo digitalizačných pracovísk),
- rozšírenie zodpovednosti aj mimo bežnej pracovnej doby a mimo sídla resp. priestorov dodávateľa digitalizácie (napríklad v prípade, že digitalizácia sa vykonáva priamo v niektorej PFI alebo sa vykonáva v neštandardnom čase).

Počas trvania pracovného vzťahu je dôležité, aby si zamestnanci dodávateľa boli vedomí bezpečnostných hrozieb pri výkone digitalizačných činností, svojich povinností a zodpovedností a boli pripravení podieľať sa na minimalizácii rizík súvisiacich so zlyhaním ľudského faktoru. Zamestnanci by sa mali absolvovať (formálne alebo neformálne) školenia správneho výkonu pracovných postupov. Pre prípady vedomého narušenia bezpečnosti by vopred mali byť stanovené zásady pre disciplinárne konania.

Vedúci zamestnanci dodávateľa podieľajúci sa na zabezpečovaní výkonu prác pre digitalizáciu by mali:

- oboznámiť zamestnancov s jednotlivými metodickými manuálmi, ktoré súvisia s vykonávanými prácami zamestnancov,
- dostatočne informovať zamestnancov o ich zodpovednostiach ešte pred tým, ako budú zapojení do konkrétnych prác,
- zaistiť, že zamestnanci pri výkone prác budú dodržiavať zmluvné ustanovenia, ktorými je dodávateľ digitalizácie viazaní.

Pokiaľ zamestnanci nebudú dostatočne informovaní a oboznámení o svojich zodpovednostiach, môžu počas výkonu digitalizácie spôsobiť nezanedbateľné škody. Podcenenie riadenia zamestnancov môže v extrémnom prípade viesť k vedomému alebo nevedomému zneužitiu aktív zamestnancami. Odporúča sa, aby zamestnanci dodávateľa mali platné poistenie zodpovednosti za škodu spôsobenú pri výkone povolania. Poistná suma by mala zodpovedať výške škody, ktorú maximálne môže zamestnávateľ požadovať uhradiť od zamestnanca podľa platných všeobecne záväzných právnych predpisov. Dodávateľ by takisto mal mať platné poistenie zodpovednosti za škodu s primeranou poistnou sumou zodpovedajúcou špecifikám príslušného projektu OPIS2.

V prípade preukázateľného porušenia bezpečnosti by voči zamestnancovi malo byť vedené disciplinárne konanie. Toto konanie by malo zodpovedať povahe porušenia bezpečnosti a dôsledkom porušenia. Zohľadniť je tiež potrebné, či narušenie bezpečnosti znamenalo zároveň aj porušenie zmluvných ustanovení dodávateľa digitalizácie resp. porušenie niektorého zákona. V extrémnom prípade (v závislosti od charakteru narušenia bezpečnosti a jeho dôsledkov) môže byť narušenie oznámené orgánom činným v trestnom konaní.

Ukončenie pracovného vzťahu by malo tiež prebiehať riadeným spôsobom. Dodávateľ digitalizácie by mal mať určené jednoznačné zodpovednosti za priebeh ukončenia pracovného vzťahu, za odovzdanie prideleného vybavenia, agendy zamestnanca súvisiacej s digitalizáciou a zbierkových predmetov, za ktoré zamestnanec niesol zodpovednosť. Rozviazanie pracovného pomeru by malo rešpektovať prípadné zmluvné ustanovenia, ktorými je dodávateľ digitalizácie viazaný, podmienky obsiahnuté v pracovnej zmluve ako aj povinnosti zamestnanca pretrvávajúce i po ukončení pracovného vzťahu.

Celý proces ukončenia pracovného vzťahu by mal zaistiť aj zálohovanie a bezpečné odstránenie informácií uložených na zariadeniach, ktoré zamestnanec pri ukončení vzťahu odkúpil alebo ktoré vytvoril na zariadeniach v jeho vlastníctve. V prípade, že zamestnanec disponoval špecifickými informáciami alebo know-how, ktorý je dôležitý z hľadiska zachovania kontinuity ním vykonávaných činností, musí byť zaistené ich zdokumentovanie a odovzdanie určenému zamestnancovi dodávateľa digitalizácie.

V rámci ukončenia pracovného vzťahu by mali byť zamestnancovi aj odobrané prístupové práva k jednotlivým aplikáciám, ktoré používal (najmä z hľadiska prístupových práv k centrálnym aplikáciám slúžiacim na evidenciu stavov digitalizovaných objektov). Odobratie zahŕňa aj fyzický prístup (kľúče, identifikačné karty). Konkrétny priebeh procesu ukončenia pracovného vzťahu by mal zohľadniť aj súvisiace rizikové faktory, napríklad:

- či sa jedná o ukončenie iniciované zamestnávateľom a aké boli dôvody zamestnávateľa,
- mieru zodpovednosti a rozsah kompetencií a oprávnení zamestnanca,
- hodnota aktív, ku ktorým mal zamestnanec prístup resp. ktoré mu boli zverené.

6.2.5.2 Ohraničenia postupu

Metodický postup pre oblasť personálnej bezpečnosti nezahŕňa:

- vymedzenie kvalifikačných predpokladov na jednotlivé pracovné role súvisiace s digitalizáciou,
- postupy právneho pokračovania pri narušení bezpečnosti.

6.2.6 Fyzická bezpečnosť a bezpečnosť prostredia

6.2.6.1 Metodický postup

Cieľom riešenia fyzickej bezpečnosti a bezpečnosti prostredia vo vzťahu k dodávateľovi projektu OPIS2 je vytvorenie dostatočných záruk, že bezpečnosť v tejto oblasti je dodávateľom riešená na adekvátnej úrovni.

Jednotlivé bezpečnostné opatrenia musia zodpovedať charakteru činností, ktoré dodávateľ v rámci projektu vykonáva. Z pohľadu výkonu digitalizačných procesov je kritickým prvkom fyzickej bezpečnosti prevoz zbierkových predmetov a ich ochrana. Technické a režimové opatrenia súvisiace s týmto prvkom musia zodpovedať hodnote zbierkového objektu, jeho materiálovým charakteristikám a jeho požiadavkám na fyzikálne vlastnosti prostredia, v ktorom je umiestnený. Dodávateľ musí byť viazaný implementovať a používať také bezpečnostné opatrenia, aby sa minimalizovali riziká straty, poškodenia, odcudzenia alebo neoprávneného nakladania so zbierkovými predmetmi počas výkonu ľubovoľnej činnosti realizovanej ním alebo jeho subdodávateľmi.

6.2.6.2 Ohraničenia postupu

Metodický postup pre oblasť fyzickej bezpečnosti a bezpečnosti prostredia nezahŕňa:

- špecifické požiadavky kladené na ochranu zbierkových predmetov počas ich umiestnenia a transportu.

6.2.7 Riadenie komunikácií a prevádzky

6.2.7.1 Metodický postup

Cieľom riešenia bezpečnosti v oblasti riadenia komunikácií a prevádzky vo vzťahu k dodávateľovi projektu OPIS2 je stanoviť taký súbor bezpečnostných opatrení, aby pri prevádzke informačných systémov bola úroveň ich bezpečnosti na požadovanej úrovni.

Z pohľadu dodávateľa digitalizácie sa riadenie komunikácií a prevádzky týka lokálneho prostredia a lokálne používaného IKT počas digitalizácie (systémy v ktorých je vytváraný digitálny obsah, kancelárske aplikácie, lokálne spracovanie údajov).

Riadenie bezpečnosti prevádzky v realizačnom prostredí projektov OPIS2 je zamerané najmä na minimalizáciu rizika neoprávneného prístupu k údajom alebo nepovšimnuté narušenie integrity údajov.

V prípade ak na vytváranie alebo spracovanie údajov v rámci procesov digitalizácie je používaný viacužívateľský distribuovaný systém, je potrebné pre tento vytvoriť a udržiavať aktuálnu prevádzkovú dokumentáciu. V rámci prevádzkovej dokumentácie by mali byť upravené najmä:

- pravidelne vykonávané činnosti údržby IS,
- parametre konfigurácie IS a ich hodnoty,
- postupy riešenia havarijných stavov,
- rozdelenie rolí pri správe a údržbe systému,
- komunikačné rozhrania systému a identifikácia komunikujúcich systémov,
- politika riadenia prístupu k systému (bližšie popísaná v kapitole 6.2.8 Riadenie prístupov),
- plán výkonu servisu a kontakty na servisných partnerov,
- postupy používania a vyhodnotenia auditných záznamov.

Prostredie v ktorom sú realizované procesy digitalizácie musí byť adekvátne chránené pred vplyvom škodlivých kódov. Za týmto účelom je potrebné zaviesť nasledovné opatrenia:

- nasadenie antivírusového nástroja na všetky pracovné stanice a servery, jeho pravidelná a automatická aktualizácia,
- pravidelná kontrola hlavných častí operačného systému a aplikácií na prítomnosť škodlivých kódov antivírusovým nástrojom,
- kontrola prichádzajúcich správ elektronickej pošty,
- na pracovných staniciach automatická aktualizácia operačného systému a aplikácií na prácu s elektronickou poštou a prehliadačom WWW stránok, na serveroch riadené vykonávanie aktualizácie,
- zákaz používania cudzích médií, neautorizovaných aplikácií a prinášania údajov z neautorizovaných zdrojov.

Alternatívne je možné používať izolované systémy (t.j. také, ktoré nekomunikujú priamo s inými sieťami – najmä nie elektronickou poštou, prehliadaním WWW stránok alebo prostredníctvom médií), čím je riziko infiltrácie škodlivým kódom minimalizované.

V rámci procesov digitalizácie predpokladáme, že časť údajov bude objednávateľovi digitalizácie odovzdávaná na médiách. Pri používaní týchto médií, ich označovaní a ochrane sa dodávateľ digitalizácie riadi pravidlami stanovenými objednávateľom digitalizácie, rovnako aj pre ostatné proces výmeny (odovzdávania) údajov.

Zariadenia dodávateľa digitalizácie, ktoré budú komunikovať s centrálnymi aplikáciami používanými v rámci procesov digitalizácie, rovnako aj systémy, ktoré môžu vytvárať údaje typu dátum/čas by mali mať implementovaný systém centrálnej synchronizácie času automatizovaným spôsobom.

6.2.7.2 Ohraničenia postupu

Metodický postup pre riadenie komunikácií a prevádzky nezahŕňa:

- špecifikáciu konkrétnych postupov pri formálnej výmene (odovzdávaní) údajov,
- rozdelenie konkrétnych činností a zodpovedností pri prevádzke a správe informačných systémov,
- využívanie služieb elektronického obchodu dodávateľmi digitalizácie vo väzbe na výkon procesov digitalizácie (nepredpokladá sa).

6.2.8 Riadenie prístupov

6.2.8.1 Metodický postup

Cieľom riešenia bezpečnosti v oblasti riadenia prístupov vo vzťahu k dodávateľom projektov OPIS2 je navrhnutie a implementácia súboru opatrení, ktorých cieľom je umožniť autorizovaným používateľom prístup k aktívam v čase kedy je to potrebné a naopak, minimalizovať riziko neoprávneného prístupu a nakladaniu s aktívami.

Z pohľadu dodávateľa sa riadenie prístupov v rámci procesov digitalizácie týka nasledovných domén:

- lokálne používané IKT počas digitalizácie (systémy kde je vytváraný digitálny obsah, kancelárske aplikácie, lokálne spracovanie údajov),
- prístup k centrálne prevádzkovaným aplikáciám (napr. centrálny archív, aplikácie správy metadát, centrálne registre, aplikácie podpory riadenia projektov OPIS2).

Z hľadiska prístupu k centrálne prevádzkovaným aplikáciám dodávateľ musí spĺňať podmienky bezpečnosti stanovené ich prevádzkovateľom.

Oblasť riadenia prístupu pre lokálne používané IKT počas digitalizácie pozostáva z nasledovných komponentov:

- politika riadenia prístupu,
- riadenie prístupu používateľov,
- zodpovednosť používateľov,
- riadenie prístupu v sieti,
- riadenie prístupu k operačnému systému,
- riadenie prístupu k aplikáciám a informáciám,
- používanie mobilných zariadení.

V nasledovnom texte sú uvedené základné požiadavky riadenia prístupu k údajom vznikajúcim počas procesov digitalizácie a informačným systémom, v ktorých sú tieto údaje uložené u dodávateľa. Tieto pravidlá dodávateľ sumarizuje v dokumente definujúcej politiku riadenia prístupov (súčasť projektovej dokumentácie projektu OPIS2).

Povinné je riadenie prístupu používateľov, ktoré zahŕňa nasledovné aspekty:

- proces registrácie používateľa,
- riadenie privilegovaných prístupov,
- správa hesiel,
- audit prístupových oprávnení.

Pre proces registrácie používateľa by mal existovať formalizovaný postup pre získanie prístupu k systému, zmenu oprávnení a zrušenie oprávnení používateľa. Základom pre prístup ku systémom má byť unikátny používateľský identifikátor priradený každému oprávnenému používateľovi. Použitie skupinových identít by malo byť umožnené iba tam, kde je to nevyhnutne potrebné.

Rozsah pridelených oprávnení je potrebné stanoviť tak, aby to zodpovedalo cieľom a náplni jednotlivých projektov OPIS2. Základným princípom pre riadenie prístupu je pravidlo, že čo nie je explicitne povolené, je zakázané a prístup je povoľovaný iba na základe potreby (need to know). Do praxe je tiež vhodné zaviesť procesy automatického zablokovania prístupu po vypršaní lehoty platnosti udeleného súhlasu.

Prístup je možné udeliť iba určeným používateľom, ktorí sú v priamom pracovnom vzťahu s dodávateľom alebo jeho subdodávateľmi. Súčasťou dokumentácie riadenia prístupu majú byť písomné (alebo obdobné elektronické) žiadosti o udelenie prístupu pre používateľa a súhlas s rešpektovaním stanovených pravidiel prístupu a používania systémov podpísaný používateľom.

Umožnenie privilegovaného prístupu do systémov (administrátorské oprávnenia, oprávnenia modifikovať konfiguráciu systému) by malo byť obmedzené na úzky okruh určených operátorov. Pre každú z privilegovaných rolí by mal byť zdokumentovaný jej účel, rutinne vykonávané operácie (administrátorská príručka), popis privilegovaných oprávnení v systéme. Vhodné je taktiež oddeľovať bežné používateľské prístupové účty od privilegovaných (aj ak sú používané jednou osobou).

Prístup do informačných systémov a k operačnému systému zariadení musí byť podmienený úspešnou autentifikáciou používateľa. Pre zvolenú metódu autentifikácie musí byť vytvorená formalizovaná politika stanovujúca podmienky jej použitia, povinné parametre (napr. minimálnu dĺžku hesla) a procesy údržby systému hesiel (proces vydania prvotného hesla, postup pri zabudnutí hesla používateľom). Zvolená implementácia autentifikačného systému nesmie nikde ukladať autentifikačné údaje v nechránenej forme. Používatelia majú byť formálne zaviazaní chrániť svoje heslá pre vyzradením, nezaznamenávať (nepísať) ich, nezdieľať pridelený prístup do IS s inými osobami a hlásiť podozrenie na kompromitáciu jeho používateľskej identity určenej osobe.

V pravidelných intervaloch je potrebné vykonávať audit existujúcich používateľských účtov a pridelených oprávnení. V rámci tohto auditu je potrebné overiť najmä dodržiavanie politiky riadenia prístupov do systému, opodstatnenosť existencie pridelených prístupových oprávnení a súlad medzi evidenciou o schválených prístupoch a skutočným stavom. Audit odporúčame vykonať minimálne raz ročne, pre privilegované prístupy minimálne raz za 6 mesiacov. Žiadateľ o NFP môže požadovať od dodávateľa projektu OPIS2 predložiť výsledky týchto auditov.

Pre zariadenia ktoré môžu ostať neobsluhované je potrebné prijať adekvátne opatrenia na minimalizáciu rizika neautorizovaného prístupu. Rovnako pracovné prostredie používateľov, v ktorom sa môžu nachádzať citlivé údaje, má byť udržiavané v súlade so zásadou „prázdneho stola“ a „prázdnej obrazovky“.

V rámci riadenia prístupu k sieti odporúčame implementovať nasledovné opatrenia:

- sieťové prostredie dodávateľa budovať ako uzavretý systém (voči iným sieťam, najmä Internetu)
- oddelenie lokálnych zariadení dodávateľa na úrovni sieťovej vrstvy (firewall, blokovanie portov, IDS/IPS),
- zo zariadení ktoré sú používané v rámci procesov digitalizácie umožnenie prístupu iba k nevyhnutne potrebným sieťovým službám (politika default-deny),
- tam, kde sú citlivé informácie prenášané nedôveryhodnou sieťou (napr. Internet), je potrebné nasadiť ochranu dôvernosti kryptografickými mechanizmy ochrany.

Ak je umožnená práca na diaľku, treba venovať zvýšenú pozornosť zabezpečeniu komunikácie používateľa s aplikáciou tak, aby bolo minimalizované riziko odpočúvania citlivých alebo údajov (napr. autentifikačné údaje používateľa), riziko narušenia integrity údajov pri prenose, aby bola zaručená nepopierateľnosť identity a aktivít používateľa. Za týmto účelom odporúčame vypracovať formalizované pravidlá, ktoré budú tiež riešiť podmienky umožnenia prístupu zo zariadení mimo správu prevádzkovateľa informačného

systému. Prístup prostredníctvom privilegovaných rolí (napr. administrácia systému) odporúčame z takýchto zariadení vylúčiť.

Pre využívanie mobilných výpočtových zariadení v digitalizačných procesoch musia byť stanovené formalizované pravidlá stanovujúce opatrenia, ktorých cieľom je minimalizácia rizika odcudzenia/straty mobilného zariadenia a neautorizovanému prístupu k nemu. Tieto pravidlá by mali riešiť najmä opatrenia fyzickej bezpečnosti mobilných zariadení, riadenie prístupu k nim, ochranu dôvernosti použitím kryptografických techník, zálohovanie údajov, antivírovú ochranu, podmienky pripájania sa do počítačových sietí, použitie mobilného zariadenia na verejných priestranstvách.

6.2.8.2 Ohraničenia postupu

Metodický postup pre riadenie prístupov nezahŕňa:

- špecifikáciu jednotlivých rolí v informačných systémoch dodávateľa projektu OPIS2,
- vzťahy medzi rolami a rozdelenie zodpovednosti pri schvaľovaní prístupových oprávnení.

6.2.9 Vývoj, nasadzovanie a údržba informačných systémov

6.2.9.1 Metodický postup

Bezpečnosť počas vývoja a nasadzovania IS zo strany dodávateľa sa riadi prvkami metodického postupu uvedeného v časti 6.1.9 tohto metodického manuálu. Kľúčovou požiadavkou na dodávateľa je menovanie zástupcu zodpovedného za naplnenie požiadaviek kladených na bezpečnosť predmetu projektu OPIS2 a integráciu bezpečnostných opatrení

Dôležité je tiež stanovenie konkrétnych zodpovedností dodávateľa za kľúčové aktivity spojené s bezpečnosťou vývoja a dodávky IS, najmä zodpovednosť za:

- návrh koncepcie riešenia bezpečnosti v príslušnom projekte,
- výkon analýzy rizík,
- návrh bezpečnostnej architektúry,
- implementáciu bezpečnostných opatrení,
- bezpečnostné testovanie,
- naplnenie bezpečnostných štandardov podľa Výnosu.

6.2.9.2 Ohraničenia postupu

Metodický postup pre oblasť Vývoj, nasadzovanie a údržba informačných systémov je aplikovateľný pre tých dodávateľov projektov OPIS2, ktorí zabezpečujú návrh využitia, implementácie a technickú realizáciu IKT, poskytovanie služieb založených na IKT alebo spracúvanie elektronických informácií.

6.2.10 Monitorovanie a manažment bezpečnostných incidentov

6.2.10.1 Metodický postup

V rámci výkonu digitalizácie je potrebné rátať s rizikami tak prírodných živlov ako aj úmyselného zlyhania ľudského faktoru, lúpeže a podobne. Dodávateľ by mal mať stanovené postupy, za akých podmienok a v akej situácii má bezodkladne informovať políciu, hasičov, poisťovňu alebo iný subjekt (v prípade poškodenia zbierkového predmetu v dôsledku požiaru, jeho odcudzenia a podobne).

Riešenie bezpečnostných incidentov, ktoré zapríčinili pracovníci dodávateľa počas realizácie projektu OPIS2, je súčasťou postupov pre zvládanie bezpečnostných incidentov, vysvetlených v 6.1.10 Monitorovanie a manažment bezpečnostných incidentov. Dodávateľ na svojej strane musí mať stanovené nasledovné:

- kontaktné miesto pre ohlasovanie bezpečnostných incidentov,
- udalosti chápané ako bezpečnostné incidenty s uvedenými príkladmi,
- mechanizmy ohlasovania bezpečnostných incidentov,
- pracovné pozície a ich pôsobnosti z hľadiska nahlasovania a riešenia bezpečnostných incidentov (vo vzťahu k pozíciám definovaným v rámci technickej implementácie projektov OPIS2),
- pravidlá pre úspešné zvládanie bezpečnostných incidentov,
- pravidlá pre evidenciu bezpečnostných incidentov,
- mechanizmy vyhodnotenia priebehu zvládania bezpečnostného incidentu,
- zásady pre stanovenie opatrení s cieľom zabrániť opakovaného výskytu bezpečnostného incidentu.

Pri bezpečnostnom incidente zaznamenanom prijímateľom NFP a počas jeho zvládania je dodávateľ povinný poskytnúť potrebnú súčinnosť.

6.2.10.2 Ohraničenia postupu

Metodický postup pre oblasť zvládania bezpečnostných incidentov nezahŕňa:

- právne riešenie zodpovednosti dodávateľa za bezpečnostný incident ním zapríčineným,
- postupy pre kvantifikáciu škôd zapríčinených bezpečnostným incidentom.

6.2.11 Riadenie kontinuity procesov závislých od IS

6.2.11.1 Metodický postup

Dodávateľa sa v tejto oblasti bezpečnosti riadi prvkami metodického postupu uvedeného v časti 6.1.11. V závislosti od predmetu konkrétneho projektu OPIS2 a nárokov na zabezpečenie kontinuity procesov sa odporúča riadiť najmä štandardom BS 25999, ktorý pozostáva z dvoch častí:

- BS 25999-1:2006 A Code of Pratice for Business Continuity,
- BS 25999-2:2006 Specification for Business Continuity Management.

Problematika riadenia kontinuity má osobitnú dôležitosť najmä pri centrálnych prvkoch infraštruktúry a dátových centrách, ako bude napríklad národný digitálny archív, prevádzka

národných registrov, centrálne dátové úložisko. Zaistenie riadenia kontinuity v týchto prípadoch je komplexná problematika do ktorej vstupujú:

- požiadavky na členenie priestorov dátových centier (uskladnenie dát, telekomunikačné miestnosti, transportné trasy, záložné zdroje el. energie/ dieselelektrické generátory, atď.),
- požiadavky na prevádzkové parametre (teplota, vlhkosť, prašnosť, elektrické napájanie, ...),
- požiadavky na bezpečnosť (EPS, EZS, PSN, SKV, kamerové systémy atď.).

Metodický postup implementácie systému riadenia kontinuity je analogický so systémom riadenia informačnej bezpečnosti, ktorého etapy sú popísané v časti 6.1.3.1. Znamená to, že má procesne orientovaný charakter a jeho praktické zavedenie musí zahŕňať:

- základnú politiku riadenia kontinuity,
- procesy na implementáciu politiky riadenia kontinuity,
- určenie pozícií so zodpovednosťami v oblasti riadenia kontinuity
- určenie technologických, priestorových, personálnych a finančných zdrojov potrebných k zaisteniu a riadeniu kontinuity,
- vypracovanie súvisiacej dokumentácie (plánov kontinuity, havarijných plánov).

Zodpovednosť dodávateľa za implementáciu riadenia kontinuity je potrebné explicitne stanoviť v každom projekte OPIS2 formou zodpovedajúcou predmetu projektu (zodpovednosť za vypracovanie plánov kontinuity, SLA, zodpovednosť za návrh a dodávku technickej infraštruktúry atď). Dodávateľ by mal v projektovej dokumentácii stanoviť, akým spôsobom bude túto oblasť bezpečnosti v projekte implementovať (pokiaľ je táto oblasť pre predmet projekte relevantná).

6.2.11.2 Ohraničenia postupu

Metodický postup pre oblasť riadenia kontinuity procesov závislých od IS nezahŕňa:

- špecifikáciu konkrétnych opatrení slúžiacich k zaisteniu kontinuity kritických procesov,
- postupy pre zvládanie havarijných situácií (tieto je potrebné vypracovať ako súčasť príslušného projektu OPIS2).

6.2.12 Súlad s požiadavkami

6.2.12.1 Metodický postup

Digitalizácia môže byť vykonávaná iba v súlade s platnými právnymi predpismi a bezpečnostnými požiadavkami. Pri jej realizácii je veľmi dôležité vyvarovať sa porušení zákonných a zmluvných povinností a požiadaviek na bezpečný a spoľahlivý priebeh. Všetky právne normy a zmluvné požiadavky s dosahom na zbierkové predmety, digitalizované objekty a systém narábania s nimi sa musia priebežne identifikovať a zdokumentovať. S touto oblasťou úzko súvisí ďalší metodický manuál (Metodický manuál pre zabezpečenie digitálnych práv).

Opatrenia a zodpovednosti dodávateľa projektu OPIS2 za aplikáciu právnych predpisov legislatívnych požiadaviek musia byť zdokumentované a zavedené do praxe tak, aby nevznikali pochybnosti o súlade resp. súlad bolo možné preukázať a potvrdiť.
Pri posudzovaní právnych dosahov na aktíva je potrebné zamerať sa najmä na nasledovné oblasti:

- používanie autorských diel v súlade s autorskými zmluvami a licenčnými ustanoveniami,
- ochrana spracúvaných osobných údajov,
- ochrana súkromia používateľov,
- využitie ochrany obchodného tajomstva,
- využitie pracovno-právnych zákonov,
- legislatívne pokračovanie bezpečnostných incidentov v rámci pracovno-právnych predpisov.

Konkrétnom formou dosahovania súladu v priebehu realizácie projektov OPIS sú najmä:

- validácia a kontrola kvality (digitalizovaných objektov, digitalizačných služieb),
- audit / logovanie (prístupov k digitalizačným údajom, objektom, metadátam a pod.),
- synchronizácia s dôrazom na využívanie odsúhlasených štandardov a unifikáciu rozhraní systémov a aplikácii,
- jednotne definované registre.

Bezpečnú a bezproblémovú realizáciu projektov OPIS2 môže významne podporiť priebežne realizovaný audit bezpečnosti projektov OPIS2, ktorého cieľom by bolo najmä:

- hodnotenie napĺňania identifikovaných bezpečnostných opatrení,
- posudzovanie dostatočnosti, účinnosti a využívania bezpečnostných opatrení,
- iniciovanie návrhov nových bezpečnostných opatrení a reakcií na prípadné havarijné situácie alebo bezpečnostné incidenty,
- poskytovanie podpory výkonu procesov riadenia a implementácie informačnej bezpečnosti v projektoch OPIS2,
- posúdenie naplnenia právnych požiadaviek, ktoré vyplývajú z právnych predpisov súvisiacich s informačnou bezpečnosťou.

Audit bezpečnosti musí byť vykonávaný nezávislým špecialistom alebo tímom špecialistov, ktorí sa nepodieľajú na výkone digitalizácie ani nie sú zapojení do riadenia projektu OPIS2.

Dôležitou súčasťou dosahovania súladu je aj potvrdenie spoľahlivosti a bezpečnosti kritických prvkov digitalizácie (akým je napríklad Centrálny systém pre správu a dlhodobé uchovávanie konvertovaných objektov). Podrobnosti o dosahovaní takéhoto typu súladu formou certifikácie upravuje Metodický manuál pre zabezpečenie dlhodobej archivácie konvertovaných objektov.

6.2.12.2 Ohraničenia postupu

Metodický postup pre oblasť súladu požiadavkami nezahŕňa:

- špecifikáciu podrobných postupov slúžiacich k dosahovaniu právneho súladu v projektoch OPIS zo strany dodávateľa,
- spôsob realizácie certifikácie národného archívu.

6.2.13 Manažment rizík pre oblasť informačnej bezpečnosti

6.2.13.1 Metodický postup

Dodávateľ projektu OPIS2 sa pri manažmente rizík pre oblasť informačnej bezpečnosti riadi princípmi uvedenými v podkapitole 5.3.12 a metodickým postupom v podkapitole 6.2.13 Z dôvodu minimalizácie sporov a zaistenia funkčného manažmentu rizík je dôležité

stanovenie kľúčových zodpovedností na strane žiadateľa o NFP ako aj na strane dodávateľa projektu OPIS2 za:

- stanovenie kontextu manažmentu rizík,
- analýzu a vyhodnotenie rizík,
- stanovenie kritérií pre akceptáciu rizík,
- rozhodnutia o akceptácii rizík,
- stanovenie spôsobov zvládania identifikovaných rizík,
- rozhodnutia o znášaní finančných nákladov spojených s prijímaním opatrení na zvládanie rizík,
- monitorovanie manažmentu rizík.

6.2.13.2 Ohraničenia postupu

Metodický postup pre oblasť hodnotenia a zvládania rizík nezahŕňa:

- riziká mimo oblasť informačnej bezpečnosti, t.j. finančné riziká, riziká súvisiace s administráciou projektov OPIS2, riziká právneho charakteru (napríklad vysporiadanie autorských práv), riziká súvisiace s technologickými procesmi pred alebo po digitalizácii (napríklad deacidifikácia, atď.) a ďalšie podobné riziká.

6.2.14 Spôsob implementácie postupu

Postup zabezpečenia informačnej bezpečnosti počas prípravy a realizácie projektu OPIS2 zo strany dodávateľa musí byť implementovaný:

- v súlade s celkovým projektovým plánom projektu, do ktorého je riešenie informačnej bezpečnosti začlenené,
- s prihliadnutím na požiadavky platných právnych predpisov súvisiacich s informačnou bezpečnosťou, ktoré korešpondujú s predmetom príslušného projektu OPIS2,
- s ohľadom na existujúce riadiace akty prijímateľa NFP alebo jeho zriaďovateľa.

V závislosti od rozsahu príslušného projektu OPIS2 je na základe tohto metodického manuálu potrebné vypracovať samostatný bezpečnostný projekt, ktorý bude zahrnutý do celkovej projektovej dokumentácie. Obsah, rozsah, zameranie a časti bezpečnostného projektu musia zodpovedať požiadavkám uvedeným v jednotlivých oblastiach bezpečnosti v tomto metodickom manuáli. Vypracovanie bezpečnostného projektu a jeho implementácia v rámci príslušného projektu OPIS2 je zodpovednosťou dodávateľa.

7 SÚVISLOSTI A PREPOJENIA S INÝMI METODIKAMI

Praktické aplikovanie postupov podľa tohto metodického manuálu súvisí s najmä s konkrétnym projektom OPIS2, v rámci ktorého sa informačné bezpečnosť rieši. Okrem toho je dôležité zohľadniť väzby najmä na:

- Metodický manuál pre zabezpečenie projektového manažmentu
- Metodický manuál na systém správy lokálnych archívov
- Metodický manuál pre zabezpečenie dlhodobej archivácie konvertovaných objektov
- Metodický manuál pre zabezpečenie jednoznačnej a trvalej identifikácie konvertovaných objektov
- Metodický manuál pre zabezpečenie národných autorít, centrálnych slovníkov a tezaurov
- Metodický manuál pre zabezpečenie spracovania správy a prezentácie konvertovaných objektov
- Metodický manuál pre zabezpečenie digitálnych práv
- Metodický manuál pre zabezpečenie centrálneho prepojenia konverzie, evidencie, archivácie, spracovania a prezentácie objektov a následného spracovania obsahu

Kľúčové je najmä zohľadnenie požiadaviek na riešenie informačnej bezpečnosti v celkovom projektovom manažmente projektov OPIS2. Riadenie informačnej bezpečnosti musí tvoriť integrálnu súčasť celkového projektového riadenia. Čiastkové etapy riešenia informačnej bezpečnosti (identifikácia a analýza rizík, implementácia bezpečnostnej architektúry, výkon bezpečnostných testov) musia korešpondovať s priebehom implementačných etáp samotného projektu. Požiadavky na riešenie informačnej bezpečnosti v projekte OPIS2 musia byť stanovené vopred v súlade s celkovou definíciou požiadaviek zo strany žiadateľa o NFP.

8 RIZIKÁ

Oblasť informačnej bezpečnosti má prierezový charakter a priamo súvisí ďalšími okruhmi činností, ktoré sú predmetom ostatných metodických manuálov (napríklad zabezpečenie dlhodobej archivácie konvertovaných objektov, zabezpečenie spracovania správy a prezentácie konvertovaných objektov, zabezpečenie projektového riadenia). Riziká uvedené nižšie boli identifikované vzhľadom na predpokladané použitie tohto metodického manuálu a aktuálny charakter jeho cieľových skupín.

Podľa významnosti rizika sú rizika ohodnotené nasledovne:

- kritické riziká (stupeň A)
- závažné riziká (stupeň B)
- akceptovateľné riziká (stupeň C)

Ohodnotenie rizík vychádza z expertného odhadu na základe analýzy informácií dostupných v čase vytvorenia tohto metodického materiálu.

riziko č.1: nedostatočná praktická implementácia bezpečnostných opatrení odporúčaných týmto metodickým manuálom

stupeň: A

riziko č.2: nerešpektovanie tohto metodického manuálu počas prípravy a realizácie projektov OPIS2

stupeň: A

riziko č.3: nekoordinovaný prístup k riešeniu informačnej bezpečnosti počas prípravy a výkonu digitalizácie

stupeň: B

riziko č.4: nedostatok zdrojov (finančných, personálnych) potrebných na implementáciu potrebných bezpečnostných opatrení

stupeň: B

riziko č.5: nedostatočná konkretizácia bezpečnostných požiadaviek špecifikovaných na základe tohto metodického manuálu

stupeň: B

9 AKTUALIZÁCIA METODIKY

Metodika môže byť v budúcnosti aktualizovaná najmä z nasledovných dôvodov:

- zmena legislatívy SR s dopadom na informačnú bezpečnosť, súvisiaca s výkonom digitalizácie a projektmi OPIS2,
- zavedenie nových alebo aktualizácia existujúcich procesov, služieb alebo IKT prvkov vyžadujúcich si riešenie informačnej bezpečnosti,
- zaznamenanie požiadaviek cieľových skupín na aktualizáciu alebo podrobnejšie rozpracovanie niektorej z oblastí bezpečnosti,
- harmonizáciu obsahu s ďalšími metodickými manuálmi.

10 ZÁVER

Informačná bezpečnosť v prostredí komplexných, vzájomne previazaných a heterogénne orientovaných projektov je prierezová a interdisciplinárna problematika. Projekty OPIS2 predstavujú práve takýto typ projektov. Pri implementácii princípov a metodických postupov uvedených v tomto dokumente je potrebné si uvedomiť, že sa nejedná o izolované aktivity s definovaným začiatkom a ukončením, ale systém vzájomne previazaných a na sebe závislých procesov, ktoré v praxi tvoria hierarchiu riadiacich, výkonných a kontrolných postupov. Trvalé dosahovanie požadovanej úrovne informačnej bezpečnosti v jednotlivých projektoch je možné iba priebežnou implementáciou, rozpracovaním a využívaním postupov uvedených v jednotlivých oblastiach bezpečnosti na strane žiadateľa o NFP ako aj dodávateľa.

11 DEFINÍCIE A SKRATKY

Položka	Typ	Význam
MM	všeobecne odborná	Metodický manuál
MK SR	všeobecne odborná	Ministerstvo kultúry Slovenskej republiky
ISVS	všeobecne odborná	Informačný systém verejnej správy
MF SR	všeobecne odborná	Ministerstvo financií Slovenskej republiky
MV SR	všeobecne odborná	Ministerstvo vnútra Slovenskej republiky
NFP	všeobecne odborná	Nenávratný finančný príspevok
OPIS	všeobecne odborná	Operačný program informatizácia spoločnosti
PFI	všeobecne odborná	Pamäťová a fondová inštitúcia
IS	technická	Informačný systém
HW	technická	Hardware – technické vybavenie
SW	technická	Software – softwarové vybavenie
BP	technická	Bezpečnostný projekt
OS	technická	Operačný systém
IKT	technická	Informačné a komunikačné technológie
STN	technická	Slovenská technická norma
EPS	technická	Elektrická požiarna signalizácia
EZS	technická	Elektronická zabezpečnovacia signalizácia
SKV	technická	Systém na kontrolu vstupov
PSN	technická	Poplachový systém narušenia
APV	technická	Aplikačné programové vybavenie
IDS	technická	Intrusion detection system (systém na detekciu prienikov)
Perimeter	technická	Obvodový ochranný systém
APV	technická	Aplikačné programové vybavenie
SLA	technická	Service level agreement (dohoda o poskytnutí služby)
Analýza rizík	technická	Činnosť, ktorej náplňou je identifikácia a vyhodnocovanie bezpečnostných rizík.
Aplikačné	technická	Zahŕňa všetky programové prostriedky zariadení IKT, najmä

programové vybavenie		systémové aplikácie, serverové aplikácie, kancelárske aplikácie a špecializované aplikácie.
Aktívum	technická	Dôležitá informácia a dokumentácia, digitalizovaný objekt, zmluva, programové vybavenie, technické zariadenie, poskytovaná služba, kvalifikované osoby, dobré meno a ďalšie skutočnosti, ktoré považuje žiadateľ o NFP za citlivé.
Bezpečnostná politika IS rezortu MK SR	všeobecne odborná	Schválený dokument, ktorý určuje základné požiadavky za účelom zaistenia informačnej bezpečnosti v prostredí organizácií rezortu kultúry a súvisiace záväzky jednotlivých subjektov.
Bezpečnostný incident	technická	Úmyselné využitie zraniteľného miesta spôsobujúce škody na aktívach informačného systému alebo neúmyselné vykonanie akcie, ktorej výsledkom je škoda na aktívach.
Informačná bezpečnosť	technická	Súhrn atribútov na stanovenie, určenie, zaistenie a posúdenie úrovne zabezpečenia informácií a súvisiacich prvkov IS. Hlavné atribúty sú dôvernosť, dostupnosť a integrita.
Informačný systém	technická	Funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických a programových prostriedkov, ktoré sú súčasťou IS.
Informačný systém verejnej správy	všeobecne odborná	IS v pôsobnosti povinnej osoby ako správcu, ktorý slúži na výkon správy. Rozoznávame tri časti tohto informačného systému: vecnú (úseky správy – agendy a s nimi súvisiace procesy), inštitucionálnu (kompetencie inštitúcií verejnej správy, resp. povinných osôb vo vzťahu k agendám a procesom) a technologickú (nástroje a metódy; materiálne a technické prostriedky realizácie procesov).
Povinná osoba	všeobecne odborná	Je definovaná zákonom č. 275/2006 Z. z. o informačných systémoch verejnej správy v znení neskorších predpisov.
Prevádzkovateľ ISVS	všeobecne odborná	Povinná osoba určená správcom IS verejnej správy, ktorá vykonáva správcom určené informačné činnosti; prevádzkovateľom IS verejnej správy môže byť aj správca IS verejnej správy.
Riziko	technická	Predstavuje pravdepodobnosť, že zraniteľnosť v systéme negatívne ovplyvní overenie alebo dostupnosť, pravosť, integritu alebo dôvernosť spracovávaných alebo prenesených údajov, ako aj vážnosť následkov úmyselného alebo neúmyselného využitia takejto zraniteľnosti.
Správca ISVS	všeobecne odborná	Povinná osoba, ktorá určuje účel a prostriedky spracovania informácií a ktorá zodpovedá za správu a rozvoj daného ISVS.
Tretia strana	technická	Vo vzťahu k IS označuje externého dodávateľa poskytujúceho služby vývoja, dodávky, údržby, konfigurácie, správy a prevádzky IS a IKT a služby digitalizácie ako aj ďalšie subjekty, ktoré počas projektov OPIS2 môžu prísť do styku s aktívami žiadateľov o NFP.

12 ZOZNAM LITERATÚRY

1. Národná stratégia pre informačnú bezpečnosť v Slovenskej republike schválená vládou SR uznesením č.570/2008
2. Zákon č.275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
3. Zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov
4. Zákon č. 618/2003 Z. z. o autorskom práve a právach súvisiacich s autorským právom
5. Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov
6. Zákon č. 206/2009 Z. z. o múzeách a o galériách a o ochrane predmetov kultúrnej hodnoty a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov v znení neskorších predpisov
7. Zákon č. 343/2007 Z. z. o podmienkach evidencie, verejného šírenia a uchovávania audiovizuálnych diel, multimediálnych diel a zvukových záznamov umeleckých výkonov a o zmene a doplnení niektorých zákonov
8. Zákon č. 516/2008 Z. z. o Audiovizuálnom fonde a o zmene a doplnení niektorých zákonov
9. Zákon č. 183/2000 Z. z. o knižniciach v znení neskorších predpisov
10. Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
11. Zákon č. 49/2002 Z. z. o ochrane pamiatkového fondu
12. Zákon č.215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov
13. Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám v znení neskorších predpisov
14. Zákon o štátnej štatistike č. 540/2001 Z. z.
15. STN ISO/IEC 27001:2005
16. STN ISO/IEC 27002:2005
17. ISO/IEC 27005:2008
18. Výnos MF SR z 8. Septembra 2008 č. MF/013261/2008-132 o štandardoch pre informačné systémy verejnej správy
19. Metodický pokyn MF SR č. MF/014235/2008-132
20. Bezpečnostná politika IS rezortu MK SR
21. Metodický pokyn Ministerstva kultúry Slovenskej republiky č. MK–2349/2009-10/2396 z 20. februára 2009 pre klasifikáciu a riadenie aktív informačných systémov,
22. Metodický pokyn Ministerstva kultúry Slovenskej republiky č. MK-2216/2009-10/1992 z 15. februára 2009 pre nákup, vývoj a údržbu informačných systémov,
23. Metodický pokyn Ministerstva kultúry Slovenskej republiky č. MK - 2902/2009-10/4659 z 15. apríla 2009 pre organizáciu a riadenie bezpečnosti informačných systémov,
24. Metodický pokyn Ministerstva kultúry Slovenskej republiky č. MK-3822/2009-10/8737 z 10. júla 2009 pre analýzu a riadenie rizík informačných systémov.

***