

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

INFORMAČNÍ KONCEPCE
Kraj Vysočina



INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Obsah

1.	Identifikace informační koncepce	3
1.1	Identifikační údaje informační koncepce	3
1.2	Verze informační koncepce	4
1.2.1	Verze 3.0	4
1.2.2	Verze 2.0 a subverze 2.1, 2.2, 2.3, 2.4, 2.5	5
1.2.3	Verze 1.0 a subverze 1.1, 1.2, 1.3, 1.4, 1.5	6
2.	Kontext informační koncepce	8
3.	Informační systémy	9
4.	Management informačních systémů	13
4.1	Rozvoj informačních systémů	13
4.2	Kvalita informačních systémů	16
4.2.1	Dlouhodobé cíle kvality	16
4.2.2	Požadavky na kvalitu	16
4.2.3	Plán řízení kvality	19
4.3	Bezpečnost informačních systémů	22
4.3.1	Dlouhodobé cíle bezpečnosti	22
4.3.2	Požadavky na bezpečnost	22
4.3.3	Plán řízení bezpečnosti	22
4.4	Správa informačních systémů	27
4.4.1	Životní cyklus informačních systémů	27
4.4.2	Pořízení informačního systému	28
4.4.3	Role správy informačních systémů	29
4.4.4	Procesy správy informačních systémů	31
4.5	Financování informačních systémů	34
4.5.1	Zdroje financování informačních systémů	34
4.5.2	Plán financování informačních systémů	34
4.5.3	Základní poměrové finanční ukazatele	34
4.5.4	Procesy financování informačních systémů	34
4.5.5	Rozpočet informačních technologií	35
4.5.6	Rozpočtový výhled informačních technologií	36
4.5.7	Rozpočet informačních projektů	36
5.	Implementace informační koncepce	37
5.1	Realizace informační koncepce	37
5.2	Vyhodnocení informační koncepce	39
6.	Přílohy informační koncepce	40

1. Identifikace informační koncepce

1.1 Identifikační údaje informační koncepce

Tabulka č. 1: Základní identifikační údaje Informační koncepce Kraje Vysočina

Název dokumentu	Informační koncepce Kraje Vysočina
Název a sídlo orgánu veřejné správy	Kraj Vysočina Žižkova 57 587 33 Jihlava
Identifikační číslo	70890749
Typ orgánu veřejné správy	Kraj
Zpracovatel	Ing. Václav Jáchim Úředník Odboru informatiky na úseku koncepce IT 04 +420 564 602 346 jachim.v@kr-vysocina.cz Ing. Petr Pavlinec Vedoucí Odboru informatiky +420 564 602 114 pavlinec.p@kr-vysocina.cz
Schvalovatel	Mgr. Ing. Zdeněk Kadlec, dr. h. c. Ředitel Krajského úřadu Kraje Vysočina +420 564 602 250 kadlec.z@kr-vysocina.cz Rada Kraje Vysočina (číslo usnesení ...)
Datum zpracování	dd. mm. 2019
Datum schválení	dd. mm. 2019
Datum platnosti	dd. mm. 2019
Datum ukončení platnosti	dd. mm. 2024
Počáteční verze	1.0
Aktuální verze	3.0
Soubor	2019-Informacni-koncepce-Vysocina-kraj.docx
Uložení	Intranet
Počet stran	40
Počet příloh	1
Důvěrnost	Střední stupeň (přístup k informacím je vázán na splnění specifických podmínek).

1.2 Verze informační koncepce

Verze dokumentu jsou chronologicky řazené od nejnovější k nejstarší.

Verze dokumentu jsou označeny dvěma čísly, oddělenými tečkou:

- hlavní číslo verze, které odlišuje verze s významnými změnami,
- vedlejší číslo verze, které odlišuje drobnější změny.

Verze dokumentu obsahuje popis a odůvodnění změn oproti předchozí verzi a identifikaci příslušných částí, které byly změněny.

1.2.1 Verze 3.0

Tabulka č. 2: Základní identifikační údaje Informační koncepce Kraje Vysočina, verze 3.0

Název dokumentu	Informační koncepce Kraje Vysočina
Verze	3.0
Zpracovatel	Ing. Václav Jáchim Úředník Odboru informatiky na úseku koncepce IT 04 +420 564 602 346 jachim.v@kr-vysocina.cz Ing. Petr Pavlinec Vedoucí Odboru informatiky +420 564 602 114 pavlinec.p@kr-vysocina.cz
Schvalovatel	Mgr. Ing. Zdeněk Kadlec, dr. h. c. Ředitel Krajského úřadu Kraje Vysočina +420 564 602 250 kadlec.z@kr-vysocina.cz Rada Kraje Vysočina (číslo usnesení ...)
Datum zpracování	dd. mm. 2019
Datum schválení	dd. mm. 2019
Datum platnosti	dd. mm. 2019
Soubor	2019-Informacni-koncepce-Vysocina-kraj.docx
Počet stran	40
Počet příloh	1

Tabulka č. 3: Historie změn informační koncepce mezi verzemi 3.0 a 2.0 (2.1, 2.2, 2.3, 2.4, 2.5)

Změněná část	Popis a odůvodnění změny
Celý dokument	Nová forma, struktura, obsah

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

1.2.2 Verze 2.0 a subverze 2.1, 2.2, 2.3, 2.4, 2.5

Tabulka č. 4: Základní identifikační údaje Informační koncepce Krajského úřadu Kraje Vysočina, verze 2.0

Název dokumentu	Informační koncepce Krajského úřadu Kraje Vysočina
Verze	2.0
Zpracovatel	Odbor informatiky
Schvalovatel	Rada Kraje Vysočina
Datum zpracování	30. 3. 2014
Datum schválení	31. 3. 2014 (verze 2.5 schválena 24. 3. 2015)
Datum platnosti	1. 4. 2014
Soubor	2014-Informacni-koncepce-Vysocina-kraj.docx
Počet stran	35
Počet příloh	2

Tabulka č. 5: Historie změn informační koncepce mezi verzemi 2.0 (2.1, 2.2, 2.3, 2.4, 2.5) a 1.0 (1.1, 1.2, 1.3, 1.4, 1.5)

Změněná část	Popis a odůvodnění změny
Kap. 2.2.	Aktualizace legislativního rámce
Kap. 3	Aktualizace přehledu provozovaných ISVS a provozních agend s vazbou na ISVS

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

1.2.3 Verze 1.0 a subverze 1.1, 1.2, 1.3, 1.4, 1.5

Tabulka č. 6: Základní identifikační údaje Informační koncepce Krajského úřadu Kraje Vysočina, verze 1.0

Název dokumentu	Informační koncepce Krajského úřadu Kraje Vysočina
Verze	1.0
Zpracovatel	Odbor informatiky
Schvalovatel	Rada Kraje Vysočina (číslo usnesení 0539/13/2009/RK)
Datum zpracování	8. 8. 2008
Datum schválení	14. 4. 2009
Datum platnosti	1. 5. 2009
Soubor	2009-Informacni-koncepce-Vysocina-kraj.docx
Počet stran	30
Počet příloh	1

Tabulka č. 7: Historie změn informační koncepce ve verzích 1.1, 1.2, 1.3, 1.4, 1.5

Změněná část – dílčí verze	Popis a odůvodnění změny
Verze 1.1	Byly vyřazeny ISVS Civilní služba, PUKNi. Dále se již aktivně nevyužívaly. Naopak se začaly využívat systémy EVI – Evidence odpadů, EDA – evidence dopravních agend, EMY – Evidence myslivosti, GORVYK/UCR – sběr ek. dat. Do plánovaných ISVS byly přidány tyto informační systémy: Twist ENZZ, KS Program
Verze 1.2	Byl vyřazen provozní systém napojený na ISVS FLUX Mzdy. Tento systém byl nahrazen systémem KS Program. Dále se začaly využívat Twist ENZZ (plánovaný viz rok 2010, verze IK 1.1). Do plánovaných ISVS byly přidány tyto informační systémy: Ovzduší, Tagra Tachografy, eDotace, Proxy ISZR
Verze 1.3	Začaly se využívat systémy Ovzduší, eDotace. Tagra tachografy, Proxy ISZR (plánované viz rok 2011, verze IK 1.2). Do plánovaných ISVS byly přidány tyto informační systémy: IDM Identity management, KDS krajská digitální spisovna, Cityware spisová služba
Verze 1.4	Začaly se využívat systémy IDM Identity management, KDS krajská digitální spisovna, Cityware spisová služba (plánované viz rok 2012, verze IK 1.3).

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

	<p>Došlo:</p> <p>Ke sloučení dvou IS (Ginis EKO a Ginis SSL) do nového IS Ginis ERP.</p> <p>K úpravě názvu IS Dotace na Dotace – zemědělství</p> <p>K úpravě IS Topol Heletax na Heletax – lesní hosp. plány.</p>
Verze 1.5	<p>Byl vyřazen ISVS Webové stránky Kraje Vysočina, protože došlo k přehodnocení jejich zařazení do systémů ISVS.</p>

2. Kontext informační koncepce

Kraj Vysočina je podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy, v rámci tzv. dlouhodobého řízení informačních systémů veřejné správy povinnou vytvářet a vydávat informační koncepci, uplatňovat ji v praxi a vyhodnocovat její dodržování. V informační koncepci kraj stanoví své dlouhodobé cíle v oblasti řízení kvality a bezpečnosti spravovaných informačních systémů a vymezí obecné principy jejich pořizování, vytváření a provozování. Na základě vydané informační koncepce kraj vytváří a vydává provozní dokumentaci k jednotlivým informačním systémům, uplatňuje ji v praxi a vyhodnocuje její dodržování.

Při zpracování informační koncepce bylo metodicky postupováno dle vyhlášky č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy. Všechny povinné náležitosti, které vyhláška stanovuje, jsou v informační koncepci obsaženy.

Vrcholové vedení Kraje Vysočina si uvědomuje důležitost koncepčního řízení informačních systémů veřejné správy, resp. celé oblasti IS/IT, a prostřednictvím Odboru informatiky svou činností vytváří podmínky pro naplňování této informační koncepce.

Pro koncepční řízení IS/IT Kraje Vysočina jsou více či méně využívány následující zdroje, nástroje, a prostředky:

- relevantní legislativní normy,
- procesní a projektové řízení,
- řízení služeb informačních technologií (ITSM¹) – rámec ITIL² 2011 Edition,
- IT Governance³ – metodologie CobiT⁴ 4.1, resp. CobiT 5,
- systém správy IT služeb (norma ČSN ISO/IEC 20000),
- systém řízení bezpečnosti informací (zákon č. 181/2014 Sb., o kybernetické bezpečnosti, norma ISO27001),
- systém řízení kvality (norma ČSN ISO/IEC 9001).

Koncepční řízení IS/IT Kraje Vysočina je v souladu s příslušnými právními předpisy o ochraně osobních údajů a s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

¹ ITSM – IT Service Management - oblast řízení služeb informačních technologií, která upřednostňuje vztahy se zákazníky orgánu veřejné správy a s odběrateli IT služeb namísto technologií samotných.

² ITIL – rámec pro návrh, implementaci, provozování IT služeb, včetně neustálého měření jejich kvality a jejich zlepšování; vztahuje se na IT služby jak z pohledu jejich dodavatele, tak z pohledu zákazníka.

³ IT Governance – zajišťuje soulad cílů orgánu veřejné správy s cíli IT strategie (informační koncepce), efektivní využití IT a řízení rizik informačních systémů a technologií.

⁴ CobiT – rámec pro řídicí a kontrolní systém fungující nad IT prostředím; poskytuje kompletní sadu ověřených postupů pro propojení cílů orgánu veřejné správy s pravidly, která jsou uplatňována v IT prostředí (není určen pro každodenní řízení IT útvarů, ale slouží primárně pro vedení orgánu veřejné správy).

3. Informační systémy

Informační systém je systém technologických a programových prostředků, informací, dat a lidí, jehož cílem je efektivní podpora informačních, rozhodovacích a řídicích procesů na všech úrovních řízení kraje.

Informační systémy Kraje Vysočina tvoří následující typy IS:

- informační systémy veřejné správy (ISVS)⁵ – zajišťují informační služby pro výkon agend veřejné správy; specifické ISVS⁶:
 - významné informační systémy (VIS)⁷,
 - informační systémy kritické informační infrastruktury (IS KII)⁸,
- provozní informační systémy (PIS)⁹ – zajišťují informační služby nutné pro vnitřní provoz kraje,
- suportivní informační systémy (SIS) – zajišťují podpůrné služby a informační činnosti nutné pro provoz ISVS a PIS.

Seznam IS kraje tvoří tzv. portfolio informačních systémů, jež je obsahem tab. č. 8.

Informační systémy, a především informační systémy veřejné správy a provozní informační systémy podléhající režimu zákona č. 365/2000 Sb., o informačních systémech veřejné správy, jsou blíže specifikovány těmito charakteristikami:

- ID informačního systému,
- název informačního systému,
- účel informačního systému,
- typ informačního systému,
- uživatelé informačního systému,
- vazby na jiné informační systémy (služby jiným informačním systémům),
- legislativní základ,
- dodavatel informačního systému.

Kraj Vysočina se v rámci pořízování nových informačních systémů zaměřuje na hledání synergických efektů a koordinaci s rozvojem informačních systémů stávajících. Záměry na pořízení nebo vytvoření nových informačních systémů kraje jsou obsahem tabulky č. 9.

⁵ Pro jednoznačnou terminologii platí, že informační systém se považuje za ISVS, i když pouze některá jeho část (subsystém/modul) slouží pro výkon agend veřejné správy.

⁶ V praxi mohou nastat případy, kdy systém je významným informačním systémem, a přitom není informačním systémem veřejné správy.

⁷ VIS – významným informačním systémem je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého jsou naplněna dopadová anebo oblastní určující kritéria dle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

⁸ IS KII – kritickou informační infrastrukturou se rozumí prvek nebo systém prvků kritické infrastruktury v oblasti komunikační a informační systémy v oblasti kybernetické bezpečnosti.

⁹ Podle novely zákona č. 365/2000 Sb., o informačních systémech veřejné správy, se nejrozšířenější provozní informační systémy podřizují režimu zákona č. 365/2000 Sb., o informačních systémech veřejné správy - nově zákonu podléhají informační systémy pro řízení a rozvoj lidských zdrojů, pro odměňování, elektronické systémy spisové služby, informační systémy pro vedení účetnictví nebo systémy elektronické pošty.

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Tabulka č. 8: Portfolio informačních systémů Kraje Vysočina

ID	Název	Účel	Typ ¹⁰	Uživatelé	Vazby na jiné IS	Legislativa	Dodavatel
IS 1	CityWare spisová služba - GEOVAP	Spisová služba	ISVS	Príspevkové organizace zřízované Krajem Vysočina	ISDS, evidence veřejných zakázek	499/2004 Sb.	Geovap
IS 2	Dotace - zemědělství	Evidence dotací v zemědělství	ISVS	Zaměstnanci KrÚ	Ginis	129/2000 Sb.	Foresta SG
IS 3	eDotace	Dotace Fondu Vysočiny	PIS	Zaměstnanci KrÚ, žadatelé o dotaci	Ginis, de minimis, evidence smluv	129/2000 Sb.	Kraj Vysočina
IS 4	EVI - Evidence odpadů	Evidence odpadů	ISVS	Zaměstnanci KrÚ	RES, ISPO, ISOH	185/2001 Sb.	Inisoft
IS 5	EDA - Evidence dopravních agend	Evidence dopravních agend	ISVS	Zaměstnanci KrÚ	Registr dopravců	361/2000 Sb.	Yamaco
IS 6	EMY - Evidence myslivosti	Evidence myslivosti	ISVS	Zaměstnanci KrÚ	ISRS	449/2001 Sb.	Yamaco
IS 7	GINIS ERP a SSL	Erp systém s spisová služba KrÚ	VIS	Zaměstnanci KrÚ	Ares, IS státní pokladny, ISZR, ISRS, insolvenční rejstřík, Národní digitální archiv	129/2000 Sb.	Gordic

¹⁰ ISVS, ISVS–VIS, ISVS–IS KII, VIS, PIS, SIS.

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

ID	Název	Účel	Typ ¹⁰	Uživatelé	Vazby na jiné IS	Legislativa	Dodavatel
IS 8	GORVYK/UCR - sběr dat	Sběr , kontrola, předání výkazů	ISVS	Zaměstnanci KrÚ	IISSP	Usnesení vlády č. 169-2005	Gordic
IS 9	Heletax	Podpora LHP, LHK, mapové podklady	ISVS	Zaměstnanci KrÚ	UHÚL	289/1995 Sb.	Topol pro
IS 10	IDM	Identity Management	PIS	Zaměstnanci KrÚ,PO, dodavatelé	Významné systémy KrÚ	129/2000 Sb.	Autocont
IS 11	Proxy - ISZR	Přístup k základním registrům	ISVS	Zaměstnanci KrÚ	Ginis, IDM	111/2009 Sb.	Marbes Consulting
IS 12	Tagra - tachografy	Čtení a zpracování dat z tachografů	ISVS	Zaměstnanci KrÚ		505/1990 Sb.	Truck Data Technology
IS 13	Twist (ENZZ)	Evidence nestátních zdravotních zařízení	ISVS	Zaměstnanci KrÚ	Registr NZZ, zákl. reg.	372/2011 Sb.	Tmapy
IS 14	Evidence náhradní rodinné péče - Kraj Vysočina	Náhradní rodinná péče	ISVS	Zaměstnanci KrÚ		94/1963 Sb.	Kraj Vysočina
IS 15	Evidence smluv	Evidence smluv	PIS	Zaměstnanci KrÚ	ISRS	499/2004 Sb. Zákon o registru smluv	Kraj Vysočina

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Tabulka č. 9: Záměry na pořízení nebo vytvoření nových informačních systémů Kraje Vysočina

ID ¹¹	Název	Účel	Typ ¹²	Uživatelé	Vazby na jiné IS	Legislativa	Dodavatel
ZIS 1	UtilityReport	Online vyjádření k existenci sítí	ISVS	Občané Kraje Vysočina	NIA, Portál občana	Stavební zákon	Hrdlička s.r.o.
ZIS 2	NCPeH	Národní kontaktní místo pro eHealth	ISVS	Pacienty poskytovatelů zdravotních služeb, poskytovatelé zdravotních služeb	NIA, Portál občana, NRZP, NRZPZS, ISZR, eMeDoCS, Transmise, CEUeR	372/2011 Sb. o zdravotních službách; zákona o léčivech č. 378/2007 Sb.	Kraj Vysočina, EC, ScaleSoft, SUKL

¹¹ ZIS – Záměr informačního systému.

¹² ISVS, ISVS–VIS, ISVS–IS KII, VIS, PIS, SIS.

4. Management informačních systémů

4.1 Rozvoj informačních systémů

Rozvoj informačních systémů Kraje Vysočina probíhá v souladu se změnami legislativy, rozvojem informačních a komunikačních technologií a požadavky klíčových uživatelů. Informační systémy jsou upravovány dle nové a novelizované legislativy, jsou průběžně zapracovávány změny a nové metodické postupy.

Procesy kraje jsou vysoce podporovány informačními a komunikačními technologiemi a tato skutečnost tedy přináší tlak na Odbor informatiky v oblasti realizace nových projektů a realizace změn stávajících informačních systémů.

Rozvoj informačních systémů Kraje Vysočina je realizován prostřednictvím informačních projektů realizujících cíle a požadavky rozvoje informačních systémů. Seznam všech současných aktivně řízených a také plánovaných budoucích informačních projektů kraje tvoří tzv. portfolio informačních projektů¹³, jež je obsahem tabulky č. 10.

Informační projekty jsou blíže specifikovány těmito charakteristikami:

- ID informačního projektu,
- název informačního projektu,
- navrhovatel informačního projektu,
- specifikace informačního projektu,
- typ informačního projektu,
- předpokládaný termín realizace,
- předpokládaná finanční náročnost,
- priorita informačního projektu.

Projekt je řízenou skupinou činností (aktivit) vyvolaných za účelem dosažení předem určených cílů v daných termínech, ceně a s přidělenými zdroji. Informační projekt je projekt vyvolaný za účelem porizení nebo adaptace (změny) informačních technologií, směřující k dosažení předem určených cílů. Komplexnost informačních projektů je dána skutečností, že projekty směřují k realizaci svých cílů ve vyvíjejícím se světě uživatelských cílů, požadavků, průběžně zlepšovaných věcných procesů, rychle se vyvíjejících technologií a integrujících se systémů.

Informační projekty mohou být následujících typů:

- aplikační informační projekty (AIP),
- technologické informační projekty (TIP),
- datové informační projekty (DIP),
- organizační informační projekty (OIP),
- kombinované informační projekty (KIP),
- jiné (ostatní) informační projekty (JIP).

Logická topologie počítačové sítě Krajského úřadu Vysočina je znázorněna na obrázku č. 1.

¹³ Portfoliem informačních projektů se rozumí kolekce informačních projektů, které sdílí stejné strategické cíle a využívají stejné zdroje, které jsou jednotlivým projektům alokovány.

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

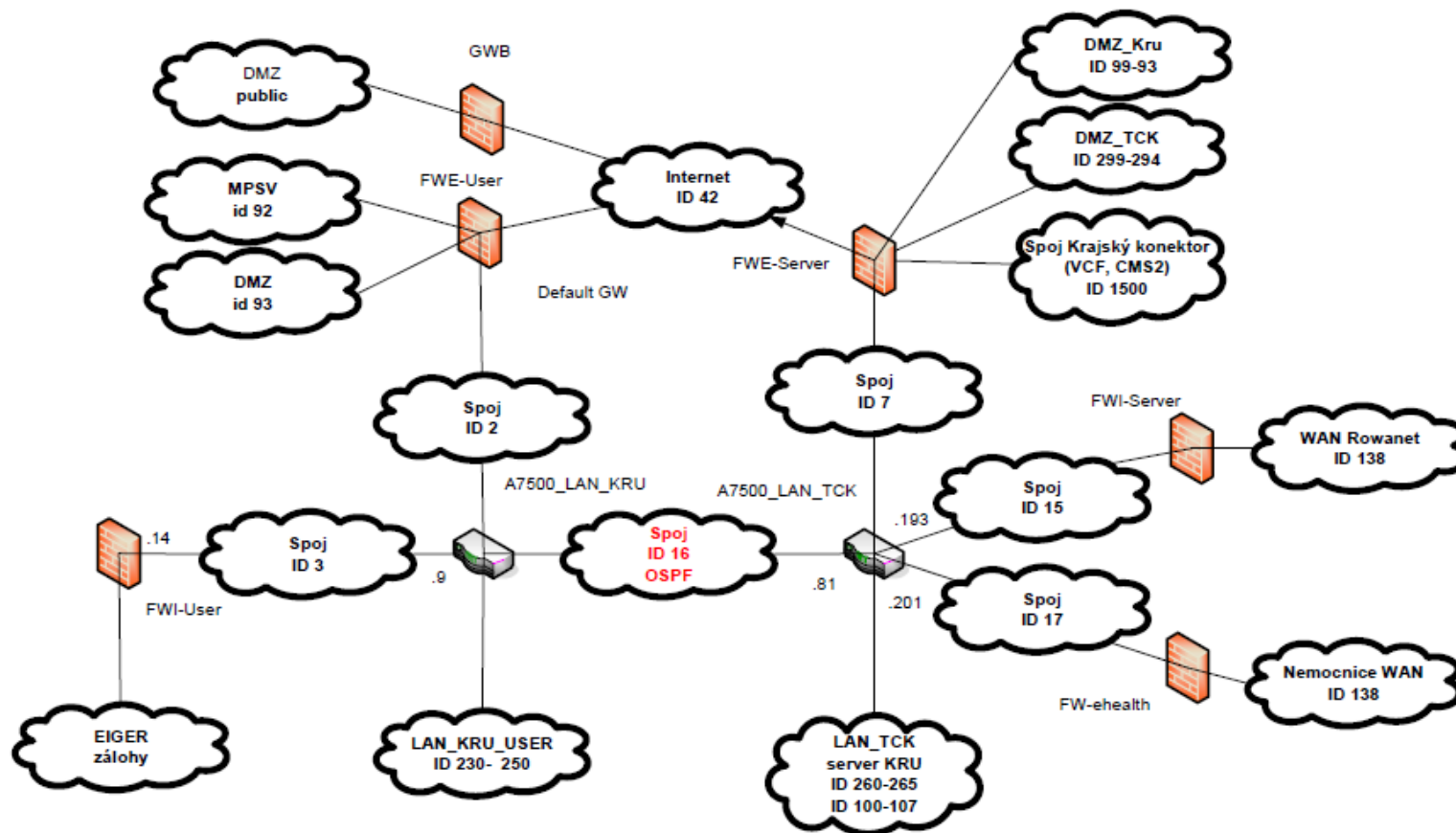
Tabulka č. 10: Portfolio informačních projektů Kraje Vysočina

ID	Název	Navrhovatel	Specifikace	Typ ¹⁴	Termín	Finance (Kč) bez DPH	Priorita ¹⁵
IP 1	Digitální technická mapa	OI	Mapa všech technických sítí na území kraje	AIP	2021	15 000 000	1
IP 2	NIS	OI	Společný nemocniční informační systém pro krajské nemocnice	AIP	2022	50 000 000	1
IP 3	IOT systém pro energetický management	OI	Společná platforma pro energetický management – elektřina, voda, plyn, teplo...	AIP	2020	2 000 000	1
IP 4	Rozvoj páteří sítě ROWANet	OI	Zakruhování sítě optických tras	TIP	2021	10 000 000	1
IP 5	Přeshraniční eRecept, elektronická identita v eHeath	OI	Technické řešení pro přeshraniční výměnu zdravotnických dat	DIP	2024	15 000 000	1
IP 6	Technická infrastruktura pro veřejnou dopravu kraje	OI	Technologické zabezpečení jednotného dopravního systému kraje	TIP	2022	20 000 000	1
IP 7	Rozvoj autentizovaných veřejných wifi hotspotů	OI	Rozvoj sítě veřejně přístupných míst k internetu	TIP	2024	1 000 000	2
IP 8	Rozvoj systému kyberbezpečnosti kraje	OI	Neustálá modernizace systému zabezpečení ICT infrastruktury a systémů kraje	TIP	2019 - 24	5 000 000	1
IP 9	Znalostní cesty do zahraničí pro úspěšné studenty technických středních škol	OI	Praktické ukázky implementací nejnovějších ICT inovací	OIP	2019 - 24	2 000 000	2
IP 10	Vnitřní konektivita škol	OI	Rozvoj technické infrastruktury ICT škol	TIP	2022	10 000 000	1
...							

¹⁴ AIP, TIP, DIP, OIP, KIP, JIP.

¹⁵ 1 - velmi důležitý, 2 - středně důležitý, 3 - méně důležitý.

KrU logická topologie



Obrázek č. 1: Logická topologie počítačové sítě Krajského úřadu Vysočina

4.2 Kvalita informačních systémů

4.2.1 Dlouhodobé cíle kvality

Základními dlouhodobými cíli, kterých chce Kraj Vysočina v oblasti řízení kvality informačních systémů dosáhnout, jsou:

- Zajištění kvality dat, která jsou v informačních systémech zpracovávána
- Zajištění kvality technických a programových prostředků
- Zajištění kvality služeb, které jsou prostřednictvím informačních systémů poskytovány

4.2.2 Požadavky na kvalitu

Požadavky na kvalitu jsou definovány z pohledu primárních aktiv, tedy dat informačních systémů, přičemž technické a programové prostředky a služby jsou (ve smyslu podpůrných a technických aktiv) nutnou podmínkou pro jejich zajištění. Požadavky na kvalitu informačních systémů Kraje Vysočina jsou stanoveny v tabulce č. 11.

Tabulka č. 11: Požadavky na kvalitu informačních systémů Kraje Vysočina

Požadavek na kvalitu	Kvalita			Specifikace
	dat	TPP	služeb	
Bezvadnost (E)	✓	✓	✓	IS nemají vady, nedostatky či nedodělky, které ztěžují či přímo zabraňují užívání systému ze strany uživatelů či způsobují poškození dat.
Kvalitativní parametry (Q)	✓	✓	✓	Znaky či vlastnosti aktiv informačních systémů, které jsou pro uživatele důležité (z pohledu dostupnosti, odezvy atp.). Čím mají informační systémy lepší vlastnosti, tím jsou považovány za kvalitnější.
Stabilita (S)	✓	✓	✓	Zajištění stability (kvality) informačních systémů v čase, a to prostřednictvím systému řízení kvality informačních systémů (mnoho změn v IT prostředí vede k nespokojenosti uživatelů a zvýšení rizika nefunkčnosti jednotlivých systémů)

Přehled základních kvalitativních parametrů technologických a programových prostředků informačních systémů je obsahem tabulky č. 12.

Přehled základních kvalitativních parametrů dat informačních systémů je obsahem tabulky č. 13. Přehled základních nástrojů řízení kvality dat informačních systémů je obsahem tabulky č. 14.

Přehled základních kvalitativních parametrů služeb informačních systémů je obsahem tabulky č. 15.

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Tabulka č. 12: Základní kvalitativní parametry technologických a programových prostředků informačních systémů

Kvalitativní parametr	Specifikace
Funkčnost	IS poskytuje funkce, které uspokojují stanovené a předpokládané potřeby.
Interoperabilita	IS je schopen interakce s dalšími IS.
Použitelnost	IS je pro své uživatele srozumitelný, zvládnutelný a atraktivní.
Efektivita	IS poskytuje odpovídající výkon při odpovídajícím využití systémových zdrojů.
Bezporuchovost	IS poskytuje bezporuchový provoz.
Udržitelnost	IS je způsobilý k úpravám a implementaci nových funkcí dle nových legislativních a dalších požadavků.
Přenositelnost	IS je způsobilý k převodu na odlišnou platformu při zachování své kvality.
Dostupnost	IS je dostupný pro všechny oprávněné uživatele.
Certifikace	Technologické prostředky IS mají platnou certifikaci pro zamýšlené programové prostředky.
Odolnost	Technologické prostředky IS jsou odolné vůči poruchám.
Úroveň služeb síťové infrastruktury	Síťová infrastruktura nezbytná pro provoz IS je na odpovídající úrovni.
Úroveň internetové konektivity	Konektivita do internetu nezbytná pro provoz IS je na odpovídající úrovni.

Tabulka č. 13: Základní kvalitativní parametry dat informačních systémů

Kvalitativní parametr	Specifikace
Přesnost	Reprezentace skutečné hodnoty v IS je v kontextu jejího použití dostatečně přesná.
Úplnost	V IS jsou vedeny hodnoty, pokud možno pro všechny atributy entity, a také všechny ostatní relevantní entity.
Konzistence	Různé údaje ke stejné entitě v IS nejsou ve zřejmém logickém rozporu.
Aktuálnost	IS využívá a poskytuje aktuální data a informace.
Důvěryhodnost	Data a informace, poskytované IS, jsou pravdivé a důvěryhodné.
Přístupnost	Data a informace v IS jsou vedené v takové formě, aby byly přístupné, a to zejména pro osoby, které vyžadují podpůrné technologie.
Dostupnost	Data a informace vedené v IS jsou vždy dostupné všem uživatelům s oprávněním k přístupu.
Utajitelnost	Data a informace vedené v IS jsou přístupné pouze oprávněným uživatelům.
Srozumitelnost	Data a informace vedené v IS jsou snadno interpretovatelné uživatelem a vyjádřené ve vhodném jazyce a jednotkách.
Efektivita	Při zpracování dat a informací v IS je zajištěn odpovídající výkon systému a je využito odpovídající množství systémových zdrojů.
Přenositelnost	Data a informace vedené v IS umožňují převod na odlišnou platformu při zachování své kvality.

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Kvalitativní parametr	Specifikace
Sledovatelnost	Při přístupu k datům a informacím, jejich vkládání nebo změně v IS probíhá sledování, kdo a kdy k datům přistupuje a kdo a kdy vložení nebo změny provádí.
Soulad s právními předpisy	Data a informace jsou v IS uloženy v souladu s platnými obecně závaznými právními předpisy a podle veřejně dostupných standardů a datových formátů.

Tabulka č. 14: Nástroje řízení kvality dat informačních systémů

Nástroj	Specifikace
Monitorování dat	Upozorňují uživatele v reálném čase na základě stanovených pravidel a postupů a zabraňují tak opětovnému vzniku nedostatků (uživatelé jsou upozorňováni, pokud byly zadány hodnoty mimo stanovený rámec, pokud nebyla splněna stanovená pravidla, nebo když je vývoj a postup procesu v rozporu s jeho definicí).
Čištění dat	Čištění dat používající složitější a sofistikovanější metody, které mají vestavěné různé vzory a předdefinované operace.
Verifikace dat	Data a informace se povinně ověřují vůči daným interním či externím číselníkům.
Obohacování dat	Data a informace se doplňují za využití externích, volně přístupných zdrojů informací.

Tabulka č. 15: Základní kvalitativní parametry služeb informačních systémů

Kvalitativní parametr	Specifikace
Dostupnost	Služby IS jsou dostupné za předem určených podmínek (místo, formát, čas).
Přehlednost	Služby IS, zejména ty, které využívají grafického uživatelského rozhraní, jsou přehledné.
Srozumitelnost	Služby IS, zejména ty, které využívají grafického uživatelského rozhraní, jsou srozumitelné.
Přístupnost	Služby IS, zejména ty, které využívají grafického uživatelského rozhraní, jsou přístupné i uživatelům, kteří pro přístup vyžadují speciální technologie.
Interoperabilita	Služby IS jsou způsobilé ke komunikaci s jinými informačními systémy.
Dohledatelnost	Služby IS jsou dohledatelné za pomoci běžných nástrojů.

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

4.2.3 Plán řízení kvality

Plán řízení kvality informačních systémů Kraje Vysočina sestává ze třech typů vykonávaných činností:

- Provozní činnosti – tab. č. 16
- Rozvojové činnosti – tab. č. 17
- Systémové kontrolní činnosti – tab. č. 18

Tabulka č. 16: Provozní činnosti vykonávané v rámci řízení kvality informačních systémů

Činnost	Požadavek	Specifikace	Termín
Management konfigurace	E, Q, S	Dokumentování, aktualizace a správa komponent služeb a TPP, zajištění dostupnosti konfigurační matice relevantním rolím.	průběžně
Management incidentů a problémů	E, Q, S	Systematické řešení výpadků kvality IS (dodávky služeb apod.). Příjem a řešení chybových hlášení, identifikace příčin, přiřazení řešitele a řešení hlášení. Systematická identifikace problémů a jejich řešení.	průběžně
Management změn	E, Q, S	Systematické řešení změnových požadavků, návrh řešení, realizace, analýzy dopadů a implementace do provozního prostředí.	průběžně
Management nasazení	E, Q, S	Řízení plánování a nasazení releasů IS, řízení vývoje, testování a konečného vyhodnocování.	průběžně
Management úrovně služeb	E, Q	Řízení specifikace požadavků koncového zákazníka, jejich ukotvení a nastavení jejich parametrů.	průběžně
Management kapacit	E, Q, S	Řízení zdrojů pro zajištění služeb a infrastruktury, zejm. kapacit infrastruktury (vč. monitoringu apod.), ale i kapacit lidských zdrojů a dalších.	průběžně
Management kontinuity a dostupnosti služeb	E, S	Průběžná analýza dopadů výpadků kritických služeb IT, stanovení a aktualizace plánů obnovy, vyhodnocování jejich efektivity a jejich další aktualizace.	průběžně
Management vztahů s odběrateli	E, Q, S	Evidence koncových zákazníků jednotlivých služeb, řízení evidence jejich požadavků na změny i chybových hlášení, identifikace zákaznických potřeb a kontrola jejich spokojenosti.	průběžně
Řízení dodavatelů	E, Q, S	Evidence externích dodavatelů, jejich vazeb na dodávky služeb a komponent, monitorování jejich výkonnosti, identifikace slabých míst smluvních vztahů a jejich vylepšování a případné řízení změny dodavatelů služeb a komponent.	průběžně
Reportování služeb	Q	Systematické měření kvalitativních parametrů služeb a TPP a jejich vyhodnocování.	průběžně

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Činnost	Požadavek	Specifikace	Termín
Řízení kvality dat	E, Q	Monitorování dat, tj. kontrola zadávaných hodnot, notifikace uživatele v reálném čase na základě stanovených pravidel a postupů, čištění dat dle složitějších a sofistikovanějších metod, ověřování dat vůči daným interním či externím číselníkům, doplňování dat za využití externích, volně přístupných zdrojů informací.	průběžně

Tabulka č. 17: Rozvojové činnosti vykonávané v rámci řízení kvality informačních systémů

Činnost	Požadavek	Specifikace	Termín
Naplnění základních požadavků na kvalitu zpracovávaných dat	Q	<ul style="list-style-type: none"> - školení uživatelů o povědomí kvality dat - důslednost zadávání všech povinných údajů - zamezení zpracovávání duplicitních dat v různých systémech - přítomnost automatických kontrolních mechanismů při zadávání dat - homogenizace datové základny - integrace a ověřování údajů s ISZR, využívání referenčních dat z ISZR (Informační systém základních registrů) - využívání definovaných rozhraní pro sdílení dat mezi různými systémy - sledování identity uživatele - účtovatelnost přístupů - kvalitní systém ukládání a zálohování dat - unifikované kódování textů - sledování a naplňování požadavků relevantní legislativy (zákon č. 101/2000 Sb., o ochraně osobních údajů, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, vyhláška č. 442/2006 Sb., kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup, vyhláška č. 64/2008 Sb. o přístupnosti) 	průběžně
Naplnění základních požadavků na kvalitu poskytovaných služeb	Q	<ul style="list-style-type: none"> - katalog poskytovaných služeb - garantovaná doba dostupnosti služeb v pracovní dny (informační služby nepřetržitě) - nepřetržitý dohled nad provozem systémů a jejich služeb - definovaná úroveň poskytovaných služeb (SLA) ze strany dodavatelů IS - jednotná terminologie - provoz systémů ve virtuálním prostředí - kvalitní webová prezentace – rozhraní poskytovaných služeb občanovi 	průběžně

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Činnost	Požadavek	Specifikace	Termín
Naplnění základních požadavků na kvalitu používaných technologických a programových prostředků	Q	<ul style="list-style-type: none"> - definovaná úroveň poskytovaných služeb (SLA) ze strany dodavatelů SW a HW - virtualizovaný přístup k aplikacím - použití rozhraní webových služeb systémů - definovaná doba odezvy systému - pravidelný upgrade serverů a diskového pole - modulární (rozšiřitelné) systémy - jednotné přihlašování k systémům a doménovým prostředkům (Active Directory) 	průběžně
...			

Tabulka č. 18: Systémové kontrolní činnosti vykonávané v rámci řízení kvality informačních systémů

Činnost	Požadavek	Specifikace	Termín
Stanovení dlouhodobých cílů kvality informačních systémů	E, Q, S	Vymezení dlouhodobých cílů kvality informačních systémů a jejich transformace přes požadavky na kvalitu do informačních projektů a jejich začlenění do portfolia informačních projektů.	1x ročně
Implementace dlouhodobých cílů kvality informačních systémů	E, Q, S	Realizace dlouhodobých cílů kvality informačních systémů v rámci řízení portfolia informačních projektů.	průběžně
Vyhodnocení dlouhodobých cílů kvality informačních systémů	E, Q, S	Vyhodnocení dlouhodobých cílů kvality informačních systémů v rámci vyhodnocení informační koncepce.	1x ročně
Revize dlouhodobých cílů kvality informačních systémů	E, Q, S	Revize dlouhodobých cílů kvality informačních systémů (vyřazení naplněných cílů, příp. aktualizace stávajících cílů a stanovení nových cílů).	1x ročně

4.3 Bezpečnost informačních systémů

4.3.1 Dlouhodobé cíle bezpečnosti

Základními dlouhodobými cíli, kterých chce Kraj Vysočina v oblasti řízení bezpečnosti informačních systémů dosáhnout, jsou:

- Zajištění bezpečnosti dat, která jsou v informačních systémech zpracovávána
- Zajištění bezpečnosti technických a programových prostředků
- Zajištění bezpečnosti služeb, které jsou prostřednictvím informačních systémů poskytovány

4.3.2 Požadavky na bezpečnost

Požadavky na bezpečnost jsou definovány z pohledu primárních aktiv, tedy dat informačních systémů, přičemž technické a programové prostředky a služby jsou (ve smyslu podpůrných a technických aktiv) nutnou podmínkou pro jejich zajištění. Požadavky na bezpečnost informačních systémů Kraje Vysočina jsou stanoveny v tabulce č. 19.

Tabulka č. 19: Požadavky na bezpečnost informačních systémů Kraje Vysočina

Požadavek na bezpečnost	Bezpečnost			Specifikace
	dat	TPP	služeb	
Dostupnost (A)	✓	✓	✓	Data a informace jsou dostupné v okamžiku jejich potřeby v požadovaném rozsahu a kvalitě.
Důvěrnost (C)	✓	✓	✓	K datům a informacím mají přístup pouze oprávněné osoby, jsou chráněné před neoprávněným užitím.
Integrita (I)	✓	✓	✓	U dat a informací je zajištěna jejich správnost a úplnost a jsou stanovena práva pro jejich změnu.
Auditovatelnost (L)	✓	✓	✓	Dohledatelnost aktivit ve vztahu k datům a informacím (logy aktivit uživatelů).

4.3.3 Plán řízení bezpečnosti

Plán řízení bezpečnosti informačních systémů Kraje Vysočina sestává ze třech typů vykonávaných činností:

- Provozní činnosti – tab. č. 20
- Rozvojové činnosti – tab. č. 21
- Systémové kontrolní činnosti – tab. č. 22

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Tabulka č. 20: Provozní činnosti vykonávané v rámci řízení bezpečnosti informačních systémů

Činnost	Požadavek	Specifikace	Termín
Údržba systému řízení bezpečnosti dat	A, C, I, L	Postupné zavedení systému řízení bezpečnosti dat a informací (ISMS) a následná certifikace ISMS. Vyhodnocování a údržba systému ISMS.	průběžně
Řízení aktiv informačních systémů	A, C, I, L	Identifikování a ohodnocení primárních aktiv, určení garantů aktiv. Stanovení a prosazení pravidel pro ochranu aktiv podle jejich klasifikace. Spolehlivé mazání a likvidace aktiv.	průběžně
Řízení rizik aktiv informačních systémů	A, C, I, L	Identifikace a hodnocení rizik primárních aktiv (významných) informačních systémů. Určení a schválení zbytkových rizik, vytvoření zprávy o hodnocení rizik a jejich pravidelná aktualizace. Zpracování prohlášení o aplikovatelnosti. Zpracování a zavedení plánu zvládnání rizik.	průběžně
Hodnocení a aktualizace bezpečnostní politiky informačních systémů	A, C, I, L	Stanovení pravidel pro 10 základních oblastí kybernetické bezpečnosti (ISMS, aktiva, rizika, ...). Hodnocení účinnosti politik a jejich aktualizace.	průběžně
Zajištění organizační bezpečnosti	C, I, L	Zpracování dokumentace o bezpečnostních rolích, nastavení systému a jeho kontrola. Ochrana autorizačních údajů ze strany všech uživatelů.	průběžně
Řízení bezpečnosti dodavatelů	A, C, I, L	Využití dodavatelů při rozvoji, provozu ICT nebo zajištění bezpečnosti podmíněno smlouvou včetně ujednání o bezpečnosti informací	průběžně
Zajištění bezpečnosti lidských zdrojů	C, I, L	Poučení lidských zdrojů o bezpečnosti informací. Kontrola dodržování pravidel. Vrácení svěřených prostředků při ukončení pracovního poměru. Zpracování a zavedení plánu rozvoje bezpečnostního povědomí.	průběžně
Řízení provozu a komunikace informačních systémů	A, C, I, L	Detekce kybernetických bezpečnostních událostí a jejich vyhodnocení. Zajištění bezpečného provozu, stanovení provozních pravidel a postupů.	průběžně
Řízení přístupu k informačním systémům	C, I, L	Nastavení, řízení a kontrola systému řízení přístupu k informačním systémům a datům.	průběžně
Řízení akvizice, vývoje a údržby informačních systémů	A, C, I, L	Stanovení bezpečnostních požadavků na informační systémy, koordinace nastavení v rámci systému IT, vlastní řízení.	průběžně
Řešení kybernetických bezpečnostních událostí a incidentů	A, C, I, L	Příprava prostředí pro vyhodnocení kybernetických bezpečnostních událostí. Neprodlené hlášení každého kybernetického bezpečnostního incidentu. Dokumentace systému zvládnání kybernetických bezpečnostních incidentů.	průběžně

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Činnost	Požadavek	Specifikace	Termín
Zajištění kontinuity činností informacích systémů	A, C, I, L	Dokumentace strategie a cílů řízení kontinuity. Stanovení postupů pro provedení protipatření.	průběžně
Provádění kontrol a auditů	L	Dokumentace požadavků relevantních právních a regulatorních předpisů a smluvních závazků. Provádění a dokumentování kontrol dodržování stanovených pravidel.	průběžně
Zajištění fyzické bezpečnosti	A, C, I, L	Ochrana neoprávněného vstupu, poškození, kompromitace aktiv. Zavedení prostředků fyzické bezpečnosti – mechanické zábranné, EZS, vstupní systémy, kamerové systémy, UPS, klimatizace, ...	průběžně
Využívání požadovaných bezpečnostních SW nástrojů	A, C, I, L	Ochrana integrity komunikačních sítí (rozhraní vnější a vnitřní sítě) prostřednictvím SW nástroje. Ověřování identity uživatelů prostřednictvím SW nástroje. Řízení přístupových oprávnění prostřednictvím SW nástroje. Ochrana před škodlivým kódem prostřednictvím SW nástroje. Zaznamenávání činností informačních systémů, jejich uživatelů a správců prostřednictvím SW nástroje. Detekce kybernetických bezpečnostních událostí prostřednictvím SW nástroje.	průběžně
Zajištění aplikační bezpečnosti	A, C, I, L	Realizace bezpečnostních testů aplikací přístupných z vnější sítě před uvedením do provozu.	průběžně
Využívání kryptografických prostředků	C	Stanovení politiky kryptografické ochrany (typ a síla kryptografického algoritmu). Ochrana přenosu po komunikačních sítích, uložení na mobilní zařízení nebo vyměnitelná média.	průběžně
Údržba požadované bezpečnostní dokumentace	A, C, I, L	Údržba, vyhodnocování a aktualizace dokumentů: Bezpečnostní politika, Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik, Zpráva o hodnocení rizik, Prohlášení o aplikovatelnosti, Plán zvládnutí rizik, Plán rozvoje bezpečnostního povědomí, Zvládnutí kybernetických bezpečnostních incidentů, Strategie řízení kontinuity činností.	průběžně

Tabulka č. 21: Rozvojové činnosti vykonávané v rámci řízení bezpečnosti informačních systémů

Činnost	Požadavek	Specifikace	Termín
ISO 27001	A, C, I, L	Udržení certifikace ISO 27001.	průběžně
Zavedení kryptografických prostředků	A, C, I, L	Stanovení politiky kryptografické ochrany (typ a síla kryptografického algoritmu). Ochrana přenosu po komunikačních sítích, uložení na mobilní zařízení nebo vyměnitelná média.	průběžně

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Činnost	Požadavek	Specifikace	Termín
Řízení informačních aktiv	A, C, I, L	Identifikace informačních aktiv Analýza rizik Režim práce s osobními údaji Režim práce s utajovanými skutečnostmi	průběžně
Bezpečnost lidských zdrojů	A, C, I, L	Školení bezpečnosti informací	průběžně
Fyzická bezpečnost	A, C, I, L	Identifikace zabezpečených oblastí a bezpečnostních perimetrů Režim přístupu do zabezpečených oblastí a režim jejich ochrany	průběžně
Řízení přístupu	A, C, I, L	Dokument „Přístupová práva uživatele IS“ Registr přístupových práv všech kategorií uživatelů	průběžně
Řízení bezpečnostních incidentů	A, C, I, L	Řízení incidentů – identifikace, evidence, řešení Znalostní databáze incidentů	průběžně
Řízení kontinuity činností informačních systémů	A, C, I, L	Identifikace reálných mimořádných událostí Stanovení minimálního požadovaného rozsahu funkcionality informačních systémů Plány kontinuity činnosti informačních systémů	průběžně
Soulad s požadavky	A, C, I, L	Audit bezpečnosti informačních systémů.	průběžně
...			

Tabulka č. 22: Systémové kontrolní činnosti vykonávané v rámci řízení bezpečnosti informačních systémů

Činnost	Požadavek	Specifikace	Termín
Stanovení dlouhodobých cílů bezpečnosti informačních systémů	A, C, I, L	Vymezení dlouhodobých cílů bezpečnosti informačních systémů a jejich transformace přes požadavky na bezpečnost do informačních projektů a jejich začlenění do portfolia informačních projektů.	1x ročně
Implementace dlouhodobých cílů bezpečnosti informačních systémů	A, C, I, L	Realizace dlouhodobých cílů bezpečnosti informačních systémů v rámci řízení portfolia informačních projektů.	průběžně
Vyhodnocení dlouhodobých cílů bezpečnosti informačních systémů	A, C, I, L	Vyhodnocení dlouhodobých cílů bezpečnosti informačních systémů v rámci vyhodnocení informační koncepce.	1x ročně

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Činnost	Požadavek	Specifikace	Termín
Revize dlouhodobých cílů bezpečnosti informačních systémů	A, C, I, L	Revize dlouhodobých cílů bezpečnosti informačních systémů (vyřazení naplněných cílů, příp. aktualizace stávajících cílů a stanovení nových cílů).	1x ročně

4.4 Správa informačních systémů

Správa informačních systémů Kraje Vysočina je prakticky realizována prostřednictvím praktického výkonu nastavených procesů, zásad a postupů správy těchto informačních systémů ve všech fázích jejich životního cyklu.

4.4.1 Životní cyklus informačních systémů

Životní cyklus informačního systému je tvořen fázemi popisujícími jeho „život“, tzn. od okamžiku, kdy pro něj padne rozhodnutí až do okamžiku, kdy se přestane používat. Celý životní cyklus informačního systému je podřízen principům procesního a projektového řízení. Základní fáze životního cyklu informačních systémů jsou obsahem následující tabulky č. 23.

Tabulka č. 23: Základní fáze životního cyklu informačních systémů

ID	Fáze (4P)	Dílčí fáze	Specifikace
F 1 ¹⁶	Plánování	Předběžná analýza	Dokument, obsahující základní rámec cílů, požadavků a funkcí informačního systému.
		Detailní analýza	Dokument, obsahující detailní rozbor předběžné analýzy – návrh řešení informačního systému.
		Návrh	Dokument, obsahující detailní návrh informačního systému, který je podkladem pro obsah smlouvy s vybranou externí dodavatelskou firmou o návrhu a realizaci informačního systému.
F 2	Pořízení	Implementace	Vlastní realizace návrhu - programování, kterého se účastní vybraní experti v programování a analytik nesoucí zodpovědnost za správnost řešení.
		Testování	Realizace připravených testů na hotovém informačním systému v testovacím prostředí zpravidla odděleném od produkčního (vyzkoušení veškerých možných reakcí informačního systému na zadávaná data) a opravení zjištěných nedostatků. Testování prokazuje, že informační systém vyhovuje zadaným specifikacím a je připraven pro použití v cílovém prostředí.
		Zavádění	Instalace a zavedení informačního systému do (zkušebního) provozu, zpřístupnění (původní) datové základny pro nový informační systém, poskytnutí manuálů a školení uživatelům.
		Zkušební provoz	Nasazení informačního systému do zkušebního provozu, v jehož rámci dodavatel poskytuje okamžitý servis, odstraňuje zjištěné chyby a řeší dodatečné požadavky uživatelů.
F 3	Provoz	Rutinní provoz	Nasazení informačního systému do rutinního provozu a užívání a zajištění provozu.
		Údržba	Běžná údržba a řízení změn informačního systému vedoucích k naplnění nových požadavků uživatelů.
F 4	Přehodnocení	Přehodnocení požadavků	Radikální přehodnocení požadavků na informační systém. S ohledem na stáří použitých technologií může být další provoz a údržba informačního systému nevhodná a výhodnější je náhrada současného řešení novým.

¹⁶ F – Fáze (životního cyklu informačního systému) - analogicky s cyklem PDCA.

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

ID	Fáze (4P)	Dílčí fáze	Specifikace
		Ukončení provozu a činnosti	Eliminace (vyřazení) informačního systému z provozu a činnosti v případě nereálnosti naplnění přehodnocených požadavků na informační systém v rámci dílčí fáze údržby. Zakonzervování informačního systému, který již není nadále rozvíjen ani rutinně využíván, leč pro občasný přístup k historickým datům je udržován jako dostupný.
		Předběžná analýza	Návrat na počátek životního cyklu informačního systému.

4.4.2 Pořízení informačního systému

Pořízení informačního systému je možno dvěma základními způsoby, které mají svá specifická pravidla a postupy.

A. Pořízení IS dodavatelským způsobem

Základní realizované postupy:

- výběr vhodných a odpovídajících principů a postupů projektového řízení,
- customizace (individuální úprava hotového IS, např. typového dodavatelského řešení, a jeho přizpůsobení specifickým požadavkům) a implementace IS (proces přizpůsobení IS konkrétní informační a komunikační infrastruktuře) za součinnosti systémového správce,
- testování IS, které prokazuje, že IS vyhovuje požadovaným specifikacím a je připraven pro použití v daném prostředí (u dodávaného IS v rozsahu a způsobem stanoveným ve smlouvě),
- vyžádání dodavatelské provozní dokumentace (především bezpečnostní směrnice pro bezpečnostního správce, systémové příručky pro systémového správce a uživatelské příručky pro uživatele IS a další dle platné legislativy (např. bezpečnostní dokumentace),
- převzetí provozní a instalační dokumentace od dodavatele IS (uživatelské příručky musí obsahovat i popis bezpečnostních funkcí IS),
- akceptační řízení - vyhodnocení splnění akceptačních kritérií (akceptování je možné v jednotlivých etapách dílčího plnění),
- akceptace a převzetí IS systémovým a bezpečnostním správcem a klíčovým uživatelem oproti podpisu akceptačního a předávacího protokolu,
- akceptace je odmítnuta v případě, že předávaná část díla vykazuje na základě vyhodnocení akceptačních kritérií natolik vážné vady, že nemůže sloužit svému účelu vůbec nebo s výraznými omezeními,
- v případě méně vážných vad se použije akceptace s výhradami (postup při jejich odstranění se stanoví na základě vzájemné dohody).

B. Vývoj (vytvoření) IS vlastními zdroji

Základní realizované postupy:

- výběr vhodných a odpovídajících principů a postupů projektového řízení,
- výběr vhodných frameworků a platform, definice způsobů a principů konkrétních analytických a programátorských prací,

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

- vývoj IS – proces tvorby, customizace, testování, instalace a implementace IS včetně právního, organizačního a technického zajištění IS,
- testování IS, které prokazuje, že IS vyhovuje požadovaným specifikacím a je připraven pro použití v daném prostředí (u vlastního IS podle platných interních pravidel),
- vypracování provozní dokumentace (především bezpečnostní směrnice pro bezpečnostního správce, systémové příručky pro systémového správce a uživatelské příručky pro uživatele IS) a další dle platné legislativy (např. bezpečnostní dokumentace) tvůrci IS,
- převzetí provozní a instalační dokumentace od tvůrců IS (uživatelské příručky musí obsahovat i popis bezpečnostních funkcí IS),
- akceptační řízení - vyhodnocení splnění akceptačních kritérií (akceptování je možné v jednotlivých etapách dílčího plnění),
- akceptace a převzetí IS systémovým a bezpečnostním správcem a klíčovým uživatelem oproti podpisu akceptačního a předávacího protokolu,
- akceptace je odmítnuta v případě, že předávaná část díla vykazuje na základě vyhodnocení akceptačních kritérií natolik vážné vady, že nemůže sloužit svému účelu vůbec nebo s výraznými omezeními,
- v případě méně vážných vad se použije akceptace s výhradami (postup při jejich odstranění se stanoví na základě vzájemné dohody).

4.4.3 Role správy informačních systémů

Každému informačnímu systému veřejné správy jsou dle zákona o informačních systémech veřejné správy přiděleny následující role jeho správy:

- Systémový správce (Správce systému) – odborný zaměstnanec Odboru informatiky pověřený správou kvality informačního systému.
- Bezpečnostní správce (Bezpečnostní správce systému) – odborný zaměstnanec Odboru informatiky pověřený správou bezpečnosti informačního systému.
- Klíčový uživatel (Odborný garant) - představitel uživatelů informačního systému, zpravidla vedoucí organizační jednotky, která informační systém používá pro podporu výkonu své agendy.

Specifikace základních aktivit vykonávaných rolemi správy informačních systémů dle zákona o informačních systémech veřejné správy je obsahem následující tabulky č. 24.

Podle zákona o kybernetické bezpečnosti jsou přiděleny následující bezpečnostní role:

- Manažer kybernetické bezpečnosti – osoba odpovědná za systém řízení bezpečnosti informací, která je pro tuto činnost vyškolená a prokáže odbornou způsobilost praxí s řízením bezpečnosti informací po dobu nejméně tří let.
- Architekt kybernetické bezpečnosti - osoba zajišťující návrh a implementaci bezpečnostních opatření, která je pro tuto činnost vyškolená a prokáže odbornou způsobilost praxí s navrhováním bezpečnostní architektury po dobu nejméně tří let.
- Auditor kybernetické bezpečnosti - osoba provádějící audit kybernetické bezpečnosti, která je pro tuto činnost vyškolená a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let; auditor

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

kybernetické bezpečnosti vykonává svoji roli nestranně a výkon jeho role je oddělen od výkonu výše a níže uvedených rolí.

- Garant aktiva – osoba zajišťující rozvoj a použití aktiva a spolupodílející se na zajištění bezpečnosti aktiva¹⁷.

Tabulka č. 24: Základní aktivity rolí správy informačních systémů dle zákona o ISVS

Role správy	Specifikace aktivit
Systémový správce	<ul style="list-style-type: none"> - zajišťuje plynulý a bezproblémový průběh celého životního cyklu informačního systému, především rutinního provozu informačního systému, - poskytuje bezprostřední součinnost bezpečnostnímu správci a klíčovému uživateli informačního systému v rámci celého životního cyklu informačního systému; řídí všechny 4P fáze informačního systému, - řídí kvalitu aktiv informačního systému, především kvalitu technologických a programových prostředků a kvalitu služeb; spoluřídí kvalitu dat a informací vedených a zpracovávaných v informačním systému, - shromažďuje a řídí veškeré požadavky, náměty a připomínky k informačnímu systému, - řídí změny informačního systému, - předkládá požadavky a návrhy na finanční krytí informačního systému, - předkládá požadavky na počet licencí a garantuje majetková, licenční a užívací práva k informačnímu systému, - zajišťuje existenci systémové dokumentace (především systémové příručky) a uživatelské dokumentace (především uživatelské příručky), - zajišťuje přípravu a realizaci uživatelských školení uživatelů.
Bezpečnostní správce	<ul style="list-style-type: none"> - zajišťuje bezpečný průběh celého životního cyklu informačního systému, především rutinního provozu informačního systému, - řídí bezpečnost aktiv informačního systému, především bezpečnost technologických a programových prostředků a bezpečnost služeb; spoluřídí bezpečnost dat a informací vedených a zpracovávaných v informačním systému, - provádí uplatňování a kontrolu funkčnosti bezpečnostních opatření a mechanismů, - předkládá požadavky a návrhy na finanční krytí bezpečnostních opatření a mechanismů, - poskytuje bezprostřední součinnost systémovému správci a klíčovému uživateli informačního systému v rámci celého životního cyklu informačního systému, - řídí bezpečnostní rizika, bezpečnostní incidenty a spravuje související znalostní databázi, - zajišťuje roli manažera a architekta kybernetické bezpečnosti, - zajišťuje existenci bezpečnostní dokumentace (především bezpečnostní směrnice), - zajišťuje přípravu a realizaci bezpečnostních školení uživatelů.
Klíčový uživatel	<ul style="list-style-type: none"> - používá informační systém v rozsahu svých uživatelských oprávnění jako prostředek k automatizovanému provádění konkrétních činností v rámci pracovního pověření a jako zdroj nezbytných informací; po uživatelské stránce informačnímu systému nejlépe rozumí, - poskytuje bezprostřední součinnost správcům informačního systému v rámci celého životního cyklu informačního systému, - posuzuje relevantnost požadavků, námětů a připomínek uživatelů informačního systému a zprostředkovává je správcům informačního systému,

¹⁷ Bezpečnost aktiva (informačního systému) primárně zajišťuje bezpečnostní správce.

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Role správy	Specifikace aktivit
	<ul style="list-style-type: none"> - spoluřídí kvalitu a bezpečnost dat a informací vedených a zpracovávaných v informačním systému, - spolupodílí se na zajištění existence uživatelské dokumentace (především uživatelské příručky), - spolupodílí se na zajištění přípravy a realizace uživatelských a bezpečnostních školení uživatelů.

4.4.4 Procesy správy informačních systémů

Rámcová specifikace základních procesů správy informačních systémů v rámci jednotlivých fází jejich životního cyklu je obsahem tabulky č. 25.

Tabulka č. 25: Základní procesy správy informačních systémů

Dílčí fáze	Specifikace procesů
Předběžná analýza	<ul style="list-style-type: none"> - shromáždění podnětů a požadavků z různých míst a od různých subjektů, posouzení jejich relevantnosti a prvotní eliminace (schválení nebo zamítnutí), a jejich předání ke schválení, - analýza rizik pořízení informačního systému a jeho uvedení do provozu, - rozpočet informačního systému - předložení požadavků na finanční krytí z investičních nebo provozních prostředků, a jejich předání ke schválení, - předběžná analýza - má-li být provedena externím subjektem, musí k tomu dojít na základě smluvního vztahu, který vzejde z jiné veřejné zakázky, - vypracování zadávací dokumentace (poptávkový dokument) tak, aby vyhovovala konkrétním a schváleným požadavkům a byla v souladu s právními předpisy a vnitřními směrnici, a její předání ke schválení; součástí zadávací dokumentace je také návrh smluvního ujednání a řešení autorskoprávní ochrany, - samotné zadávací řízení - předání zadávací dokumentace uchazečům (externím dodavatelům), vše v souladu se zákonem o zadávání veřejných zakázek¹⁸.
Detailní analýza	<ul style="list-style-type: none"> - detailní analýza a vypracování návrhu řešení (nabídkový dokument), doloženého mj. cenovou kalkulací, - předání nabídkového dokumentu zadavateli k posouzení, - v případě jednacího řízení s uveřejněním případné předání všech připomínek a námětů vybraným uchazečům k doplnění nabídky, - posouzení předložených nabídek a výběr nabídky nejvhodnější.
Návrh	<ul style="list-style-type: none"> - vypracování detailního návrhu informačního systému dodavatelem, - uzavření smluvního vztahu mezi krajem a dodavatelem.
Implementace	<ul style="list-style-type: none"> - realizace návrhu dodavatelem – konkrétní analytické a programátorské práce, - definice vstupů a výstupů jednotlivých operací, - naprogramování a ověření veškerých funkcí a jejich vzájemného propojení, - příprava testovacích dat, obsahujících maximum dat reálných, - příp. customizace nebo parametrizace.
Testování	<ul style="list-style-type: none"> - příprava testovacího prostředí odděleného od prostředí produkčního, - realizace připravených testů na hotovém informačním systému - vyzkoušení veškerých možných reakcí informačního systému na zadávaná data, testování požadovaných funkcí a zátěžových vlastností informačního systému,

¹⁸ Zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů.

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Dílčí fáze	Specifikace procesů
	- opravení zjištěných nedostatků.
Zavádění	- kompletace prekvizit ¹⁹ instalace informačního systému, - instalace (dle instalační dokumentace) a zavedení informačního systému do provozu ²⁰ , - zpřístupnění datové základny, - zajištění (vypracování) provozní dokumentace (min. systémová příručka, bezpečnostní směrnice, uživatelská příručka), - školení uživatelů, prioritně klíčového uživatele.
Zkušební provoz	- okamžitý servis dodavatele (odstraňování zjištěných chyb a řešení dodatečných požadavků uživatelů), - uzavření smluvního vztahu mezi krajem a dodavatelem – servisní smlouva (smlouva o podpoře), - akceptační řízení - vyhodnocení splnění akceptačních kritérií, akceptace informačního systému a podpis akceptačního protokolu, - předávací řízení - vyhodnocení splnění předávacích kritérií, převzetí informačního systému do rutinního provozu a podpis předávacího protokolu.
Rutinní provoz	- ostrá migrace dat, - autorský dozor dodavatele do doby stabilizace rutinního provozu informačního systému, - uživatelská práce s daty - ukládání, shromažďování, vyhodnocování a poskytování dat a informací prostřednictvím provozovaného informačního systému, - řízení kvality informačního systému, zajištění systémových činností a opatření, - řízení bezpečnosti informačního systému, zajištění bezpečnostních činností a opatření, - podpora uživatelů.
Údržba	- běžná údržba informačního systému, - řízení změn informačního systému, - údržba a update ²¹ informačního systému – modifikace informačního systému na základě zjištěných problémů, potřeby zdokonalení nebo adaptace na změnu, sloužící k zajištění bezporuchového provozu, - upgrade ²² informačního systému – úpravy, opravy a rozšíření obsahu a rozsahu řešení na základě změny zákonných předpisů, inovace procesů a naléhavých uživatelských požadavků, - opětovné školení uživatelů.
Přehodnocení požadavků	- radikální přehodnocení požadavků na informační systém, které vede k rozhodnutí o ukončení provozu a činnosti informačního systému, pokud nelze tyto požadavky naplnit v rámci dílčí fáze údržby informačního systému, - s ohledem na stáří použitých technologií může být další provoz a údržba informačního systému nevhodná a výhodnější je náhrada současného řešení

¹⁹ Konkrétní podmínky, které jsou kladeny na infrastrukturu nebo zdroje za účelem jejich přípravy, zajištění a ověření ještě před zahájením instalace z důvodu minimalizace rizika selhání instalačního procesu.

²⁰ Dle zvolené strategie zavedení (souběžná, postupná, pilotní, nárazová).

²¹ Drobné opravy informačního systému, které zásadně nemění jeho funkčnost nebo datové rozhraní, a které jsou řešeny v rámci provozních činností/výdajů informačního systému.

²² Zahrnuje kvalitativní změny informačního systému vždy spojené se změnami funkčnosti nebo datového rozhraní, které jsou řešeny v rámci investičních činností/výdajů informačního systému.

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Dílčí fáze	Specifikace procesů
	novým.
Ukončení provozu a činnosti	<ul style="list-style-type: none"> - protokolární projednání, naplánování a rozhodnutí o ukončení provozu a činnosti informačního systému, - zajištění kontinuity služeb eliminovaného (vyřazovaného) informačního systému, - bezpečné naložení (uložení, archivace) s provozní dokumentací informačního systému, - bezpečné naložení s daty (uchování, převedení, zničení) informačního systému.

4.5 Financování informačních systémů

4.5.1 Zdroje financování informačních systémů

Financování informačních systémů, resp. celé oblasti informačních technologií, je primárně realizováno z celkového rozpočtu Kraje Vysočina dle každoročního návrhu rozpočtu informačních technologií, který je jeho dílčí částí. Po konečném schválení rozpočtu zastupitelstvem lze finance čerpat v souladu s rozpočtovými pravidly a hospodařit s nimi dle schváleného rozpočtu.

Financování informačních technologií může probíhat také s finančním příspěvkem Evropské unie (využití operačních programů strukturálních fondů určených pro podporu modernizace veřejné správy a rozvoj informační společnosti ve veřejné správě). V případě použití finančního příspěvku EU postupuje kraj v souladu s pravidly a povinnostmi příslušného dotačního titulu.

4.5.2 Plán financování informačních systémů

Plán financování informačních systémů sestává z následujících rozpočtových plánů:

1. Plán rozpočtu informačních technologií.
2. Rozpočtový výhled informačních technologií.
3. Plán rozpočtu informačních projektů.

4.5.3 Základní poměrové finanční ukazatele

Základními sledovanými poměrovými finančními ukazateli informačních technologií jsou:

- roční výdaje na informační technologie jako procento celkových výdajů kraje,
- roční procento investic na informační technologie jako procento z celkových výdajů na investice kraje.

4.5.4 Procesy financování informačních systémů

Základní procesy probíhající v rámci plánování a řízení financování informačních systémů jsou uvedeny v tab. č. 26.

Tabulka č. 26: Základní procesy financování informačních systémů

Dílčí plán	Proces
Rozpočet informačních technologií	Získání podkladů pro rozpočet.
	Analýza jednotlivých požadavků, stanovení jejich priorit a finanční ohodnocení.
	Stanovení nákladových středisek.
	Vytvoření podkladů pro rozpočet na základě predikce nákladů a výnosů podle vývoje v minulých obdobích a na základě diskuse s ostatními organizačními jednotkami, kterým jsou poskytovány informační služby.
	Celková kompletace podkladů pro rozpočet.
	Úprava rozpočtu vzhledem k disponibilním finančním zdrojům, možnostem financování jednotlivých projektů a akcí.
	Stanovení jednotlivých dílčích položek rozpočtu podle stanovené rozpočtové skladby.
	Schválení rozpočtu.
	Řízení (kontrola) rozpočtu a jeho změn.

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Dílčí plán	Proces
	Sledování poměrových ukazatelů (min. roční výdaje na IT jako procento celkových výdajů a roční procento investic na IT jako procento z celkových výdajů na investice).
Rozpočtový výhled informačních technologií	Stanovení období rozpočtového výhledu.
	Rozpočtový výhled příjmů.
	Rozpočtový výhled investičních nákladů.
	Rozpočtový výhled provozních nákladů.
	Aktualizace (zpřesnění) rozpočtového výhledu.
Rozpočet informačních projektů	Stanovení předběžného portfolia informačních projektů.
	Hrubý odhad nákladů projektů.
	Výběr projektů určených k realizaci – finální portfolio informačních projektů.
	Rozpočtový odhad nákladů projektů.
	Vytvoření rozpočtu projektů.
	Konečný odhad nákladů projektů.
	Vytvoření směrného plánu nákladů projektů.
	Řízení (kontrola) směrného plánu nákladů projektů a jeho změn.
	Řízení financování portfolia informačních projektů.

4.5.5 Rozpočet informačních technologií

Účelem rozpočtu informačních technologií (IT rozpočet) je zachytit finanční potřeby Odboru informatiky na dané období v kontextu celkových finančních potřeb (rozpočtu) kraje. Rozpočet informačních technologií se zpracovává na období jednoho roku a obsahuje položky jednotlivých nákladových a výnosových účtů (v celkové výši za dané období a je-li to relevantní, tak i v podrobnějším časovém rozlišení).

Odbor informatiky neposkytuje ostatním organizačním jednotkám informační služby definované prostřednictvím SLA²³, tzn. kromě rozpočtu celkových nákladů a výnosů nejsou zpracovávány detailní rozpočty na jednotlivé dílčí služby.

V rámci Odboru informatiky prakticky nedochází až na malé výjimky k realizaci výnosových položek v peněžních jednotkách, ale jedná se spíše o subjektivní přínosy²⁴.

Plánování rozpočtu informačních technologií se obvykle dělí na plánování skupiny výnosů a dvou základních skupin nákladů (z hlediska účelu jejich vynaložení):

- INCOMES – příjmy (výnosy),
- CAPEX – kapitálové či investiční náklady,
- OPEX – neinvestiční, provozní či běžné náklady.

Základní rozpočtová skladba Odboru informatiky je uvedena v tab. č. 27.

²³ SLA - Service Level Agreement - dohoda o úrovni poskytovaných služeb.

²⁴ Může se např. jednat o výnosy dosažené jeho prostřednictvím (např. poplatek za výpis), úspora nákladů generovaných jinými subsystemy kraje, či úspora lidské práce.

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Tabulka č. 27: Základní rozpočtová skladba Odboru informatiky

ID	Rozpočtová položka - specifikace	Typ
6111	Programové vybavení (nad 60.000,- Kč)	CAPEX
6119	Ostatní nákup dlouhodobého nehmotného majetku	
6121	Budovy, haly a stavby	
6125	Výpočetní technika (nad 40.000,- Kč)	
5136	Knihy, učební pomůcky a tisk	OPEX
5137	Drobný hmotný dlouhodobý majetek (do 40.000,- Kč)	
5139	Nákup materiálu jinde nezařazený	
5162	Služby telekomunikací a radiokomunikací	
5164	Nájemné	
5167	Služby školení a vzdělávání	
5168	Zpracování dat a služby související s informačními a komunikačními technologiemi	
5169	Nákup ostatních služeb	
5171	Opravy a udržování	
5172	Programové vybavení (do 60.000,- Kč)	
5173	Cestovné (tuzemské i zahraniční)	
5175	Pohoštění	

4.5.6 Rozpočtový výhled informačních technologií

Povinnost vypracovat rozpočtový výhled ukládá zákon č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů, ve znění pozdějších předpisů. Rozpočtový výhled se sestavuje zpravidla na dobu 2-5 let následujících po roce, na který se sestavuje rozpočet.

4.5.7 Rozpočet informačních projektů

Účelem rozpočtu informačních projektů je zachytit finanční potřeby informačních projektů na dané období v kontextu celkových finančních potřeb (rozpočtu) kraje.

Mezi informační projekty patří veškeré rozvojové informační projekty, projekty řízení kvality a bezpečnosti informačních systémů s vazbou na naplňování dlouhodobých cílů kvality a bezpečnosti informačních systémů, stejně jako informační projekty s vazbou na správu životního cyklu informačních systémů.

5. Implementace informační koncepce

5.1 Realizace informační koncepce

Vlastníkem informační koncepce je Kraj Vysočina. Vedoucí Odboru informatiky je z titulu své pozice vrcholově odpovědný za vytváření, aktualizaci, údržbu, naplňování, realizaci a dohlížení nad dodržováním informační koncepce.

Realizace informační koncepce je uskutečňována prostřednictvím souboru činností a aktivit vedoucích k naplnění této informační koncepce. Minimálně se jedná o činnosti:

- praktické naplňování informační koncepce a jejích příloh,
- udržování informační koncepce a jejích příloh v aktuálním stavu.

Na realizaci informační koncepce se podílí všechny organizační jednotky:

- Odbor informatiky – především po stránce odborné a realizační,
- Ostatní organizační jednotky – především po stránce uživatelské,
- Ředitel krajského úřadu – především po stránce řídicí, kontrolní a schvalovací,
- Rada kraje – především po stránce řídicí a schvalovací,
- Zastupitelstvo kraje - především po stránce schvalovací.

Dílčí odpovědnosti za jednotlivé oblasti realizace informační koncepce a jednotlivé oblasti splnění zákonných povinností jsou obsahem tabulek č. 28 a 29.

Tabulka č. 28: Dílčí odpovědnosti za jednotlivé oblasti realizace Informační koncepce Kraje Vysočina

Oblast odpovědnosti	Odpovídá
vytváření záměrů na pořízení nebo vytvoření nových IS	Vedoucí Odboru informatiky
schvalování záměrů na pořízení nebo vytvoření nových IS	Grémium ředitele krajského úřadu Rada kraje, Zastupitelstvo kraje
řízení kvality IS	Vedoucí Odboru informatiky
řízení bezpečnosti IS	Vedoucí Odboru informatiky, bezpečnostní analytik KrÚ
řízení postupů pro pořizování a vytváření IS	Vedoucí Odboru informatiky
koordinace činností v oblasti rozvoje IS	Vedoucí Odboru informatiky
příprava informačních projektů (plánu rozvoje IS)	Vedoucí Odboru informatiky
schvalování informačních projektů (plánu rozvoje IS)	Grémium ředitele krajského úřadu Rada kraje
zajištění provozu a údržby IS	Vedoucí Odboru informatiky
vyhodnocování dodržování souladu provozování IS	Vedoucí Odboru informatiky
koordinace a vyhodnocování řízení změn	Vedoucí Odboru informatiky
řízení ukončování provozu IS	Vedoucí Odboru informatiky
vytváření a údržba plánu financování IS	Vedoucí Odboru informatiky
schvalování plánu financování IS	Grémium ředitele krajského úřadu Rada kraje
příprava změn a tvorba nových verzí IK	Vedoucí Odboru informatiky

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Oblast odpovědnosti	Odpovídá
schvalování změn IK a jejich nových verzí	Grémium ředitele krajského úřadu Rada kraje
příprava nové IK před ukončením platnosti stávající	Vedoucí Odboru informatiky
provádění vyhodnocování dodržování IK a vyhotovení zápisu o něm	Nezávislá osoba Vedoucí Odboru informatiky
návrh opatření na základě zjištění při vyhodnocování	Vedoucí Odboru informatiky
schvalování opatření na základě zjištění při vyhodnocování	Grémium ředitele krajského úřadu
schválení zápisu z vyhodnocení	Grémium ředitele krajského úřadu

Tabulka č. 29: Dílčí odpovědnosti za jednotlivé oblasti splnění zákonných povinností

Zákonná povinnost	Odpovídá
spolupracovat s Ministerstvem vnitra při plnění jeho úkolů	Ředitel krajského úřadu Vedoucí Odboru informatiky
spolupracovat s Ministerstvem vnitra při provádění kontroly na místě dle zákona o státní kontrole	Ředitel krajského úřadu Vedoucí Odboru informatiky
předložit Ministerstvu vnitra k vyjádření návrhy dokumentací programů obsahující pořízení, obnovu a provozování informačních a komunikačních technologií	Ředitel krajského úřadu Vedoucí Odboru informatiky
předložit Ministerstvu vnitra k vyjádření investiční záměry akcí pořízení, obnovy a provozování informačních a komunikačních technologií - přesné podmínky viz zákon	Ředitel krajského úřadu Vedoucí Odboru informatiky
uveřejňovat číselníky, pokud jsou jejich správci a není zákonem stanoveno jinak, a to i způsobem umožňujícím dálkový přístup	Ředitel krajského úřadu Vedoucí Odboru informatiky
předávat Ministerstvu vnitra údaje do informačního systému o datových prvcích v elektronické podobě, ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem	Ředitel krajského úřadu Vedoucí Odboru informatiky
zajistit, aby vazby jimi provozovaného informačního systému na informační systémy jiného provozovatele byly uskutečňovány prostřednictvím referenčního rozhraní s využitím datových prvků vyhlášených ministerstvem a vedených v informačním systému o datových prvcích	Ředitel krajského úřadu Vedoucí Odboru informatiky
prokázat atestem způsobilost informačního systému k realizaci výše uvedených vazeb	Ředitel krajského úřadu Vedoucí Odboru informatiky
zpřístupňovat ministerstvu v elektronické podobě, ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem, bez zbytečného odkladu informace o jimi provozovaném informačním systému a jím poskytovaných službách a používaných datových prvcích, a to za účelem uveřejnění v IS o ISVS a IS o DP	Ředitel krajského úřadu Vedoucí Odboru informatiky
odstranit zjištěné nedostatky ve lhůtě stanovené Ministerstvem vnitra	Ředitel krajského úřadu

INFORMAČNÍ KONCEPCE KRAJE VYSOČINA

Zákonná povinnost	Odpovídá
	Vedoucí Odboru informatiky
vytvářet a vydávat informační koncepci, uplatňovat ji v praxi a vyhodnocovat její dodržování	Ředitel krajského úřadu Vedoucí Odboru informatiky
vytvářet a vydávat provozní dokumentaci k jednotlivým ISVS, uplatňovat ji v praxi a vyhodnocovat její dodržování	Ředitel krajského úřadu Vedoucí Odboru informatiky
zajistit si atest dlouhodobého řízení ISVS	Ředitel krajského úřadu Vedoucí Odboru informatiky
zajišťovat bezpečnost ISVS v rozsahu odpovídajícím alespoň minimálním bezpečnostním požadavkům k zajištění důvěrnosti, integrity a dostupnosti zpracovávaných informací dle prováděcího předpisu	Ředitel krajského úřadu Vedoucí Odboru informatiky

5.2 Vyhodnocení informační koncepce

Vyhodnocení informační koncepce je základním kontrolním mechanismem zajišťujícím zpětnou vazbu o realizaci (aktuálnosti, efektivnosti, účinnosti, míře naplnění) informační koncepce.

Vyhodnocení informační koncepce probíhá metodou dekompozice informační koncepce na hlavní oblasti (a tyto dále na dílčí oblasti), kterým je přiřazena odpovědnost jednotlivých rolí v rámci organizační struktury Kraje Vysočina za jejich realizaci, a jejich následnou expertní analýzou. Těmito hlavními oblastmi informační koncepce jsou:

- informační systémy,
- rozvoj informačních systémů,
- kvalita informačních systémů,
- bezpečnost informačních systémů,
- správa informačních systémů,
- financování informačních systémů,
- implementace informační koncepce.

Vyhodnocení informační koncepce provádí osoba (resp. organizační jednotka) nezávislá na realizaci informační koncepce, a to za odborné asistence zpracovatele informační koncepce.

Výstupy vyhodnocení informační koncepce jsou:

- report analyzovaných nedostatků,
- report navrhovaných opatření,
- report schválených opatření.

Každé realizované vyhodnocení informační koncepce je blíže specifikováno v příloze č. 1 - dokumentu „Zápis z vyhodnocení informační koncepce“. Příloha č. 1 se aktualizuje minimálně 1x ročně, tzn., že také vyhodnocení, revize a aktualizace informační koncepce probíhá minimálně 1x ročně.

Vypracování nové informační koncepce probíhá 1 x za 5 roků, přičemž ze strany vedení kraje může dojít ke strategickému rozhodnutí o předčasném vypracování nové informační koncepce.

6. Přílohy informační koncepce

Nedílnou součástí informační koncepce jsou přílohy specifikované v následující tabulce č. 30.

Tabulka č. 30: Přílohy Informační koncepce Kraje Vysočina

ID	Název přílohy	Specifikace	Soubor
Příloha č. 1	Zápis z vyhodnocení informační koncepce	Obsahuje expertní analýzu informační koncepce, popis analyzovaných nedostatků a popis navrhovaných opatření.	Zapis_vyhodnoceni_IK_Vysocina.pdf