Úřad vlády České republiky
Odbor Rady pro výzkum, vývoj a inovace

Politika bezpečnosti informací IS VaVaI

Politika bezpečnosti informací IS VaVaI – informačního systému pro výzkum, vývoj a inovace – stanovuje základní požadavky a pravidla k zajištění bezpečnosti aktiv tohoto informačního systému. Vychází z požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a dále též z normy ČSN ISO/IEC 27001:2014.

Zpracoval: kolektiv RELSIE
Schválil: Marek Jan
Verze: 1.0
Datum: 16. ledna 2019

Obsah

1. Systém řízení bezpečnosti informací

K zajištění systematického přístupu k řešení bezpečnosti informací, resp. kybernetické bezpečnosti, informačního systému pro vědu, výzkum a inovace (IS VaVaI), je zaveden systém řízení bezpečnosti informací (ISMS) v souladu s požadavky zákona o kybernetické bezpečnosti a normy ČSN ISO/IEC 27001:2014.

Rozsah řízení bezpečnosti ISMS musí být definován tak, aby byly jednoznačně vymezeny hranice, ve kterých je uplatňováno řízení bezpečnosti. V rámci definovaného rozsahu ISMS musí být „začleněna" všechna aktiva IS VaVaI.

V rámci ISMS IS VaVaI jsou stanoveny bezpečnostní cíle, postupy a pravidla pro zajištění bezpečnosti aktiv IS VaVaI, které jsou dokumentovány v Příručce ISMS.

Bezpečnost IS VaVaI musí být založena na základě řízení rizik bezpečnosti informací. K zajištění této zásady musí být přijata opatření a periodicky prováděno hodnocení rizik a na tomto základě stanovovány bezpečnostní cíle a opatření o ošetření rizik bezpečnosti IS VaVaI.

Pravidla, postupy a kompetence při provozování ISMS jsou stanoveny v Příručce ISMS IS VaVaI.

2. Řízení aktiv a klasifikace informací

2.1. Řízení aktiv

Řízení aktiv IS VaVaI musí probíhat dle následujících pravidel:

1) Všechna aktiva (primární/podpůrná), související se zpracováním informací v IS VaVaI, jsou identifikována a evidována způsobem umožňující:
   - jejich rozdělení na primární a podpůrná aktiva,
   - hodnocení primárních aktiv z hlediska důvěrnosti, dostupnosti a integrity,
   - určení vazeb mezi primárními a podpůrnými aktivy a hodnocení závislostí mezi nimi,
   - hodnocení podpůrných aktiv na základě identifikovaných závislostí,
   - udržování evidence aktiv v aktuálním a přesném stavu, v návaznosti na další procesy v IS VaVaI.
2) K identifikaci a hodnocení aktiva dle výše uvedených požadavků musí být stanovena metodika naplňující požadavky ZKB a normy ISO27001
3) Hodnocení aktiv je prováděno dle schválené metodiky nejméně jednou za 3 roky nebo při provedení významné změny v IS VaVaI.
4) Pro každé aktivum je určen „Garant aktiva", (= pracovník RVVI), který má odpovědnost za toto aktivum a podílí se stanoveným způsobem na zajištění jeho rozvoje a bezpečnosti.
5) Na základě hodnocení aktiv jsou stanovena:
   - pravidla ochrany jednotlivých úrovní aktiv (viz klasifikace informací),
   - přípustné způsoby používání aktiv a pravidla pro manipulaci s těmito aktivy,
   - jsou určeny způsoby spolehlivého mazání a likvidace dat (dle typu jejich nosičů).

6) Způsob a postupy identifikace a hodnocení aktiv jsou stanoveny v rámci metodiky hodnocení rizik bezpečnosti informací. Přípustné způsoby používání a manipulace s aktivy dle jednotlivých úrovní aktiv, včetně určení způsobu likvidace dat a datových nosičů, jsou stanovena v interním předpisu.

2.2. Klasifikace informačních aktiv

Klasifikace informačních aktiv v IS VaVaI musí zohlednit jejich hodnotu, kritičnost a citlivost v IS VaVaI.

Klasifikační schéma informačních aktiv, spadající do kategorie „neutajované informace“[1], je následující:

- **Veřejné** – informace a data přístupná všem zaměstnancům RVVI, externím subjektům a v případě potřeby i veřejnosti bez omezení;
- **Interní** – informace a data přístupná všem zaměstnancům RVVI, určitým externích subjektů (v rámci rolí v IS VaVaI, s povinností ochrany informací). Data nejsou přístupná veřejnosti;
- **Citlivé** – informace a data přístupná pouze určeným osobám; informační aktiva podléhají zvláštnímu režimu zabezpečení a nakládání s nimi.

Pravidla klasifikace informačních aktiv jsou stanovena jednotně v rámci Úřadu vlády ČR, ve **směrnici vedoucího Úřadu vlády ČR č. 09/2017, o zásadách ochrany informací.**

3. Organizace bezpečnosti informací

Pro potřeby řízení a zajištění bezpečnosti musí být zavedena vhodná organizační struktura bezpečnostních rolí, příp. dalších rolí, která:

- zahrnuje bezpečnostní role mandatorně vyžadované legislativou ČR a EU, dále
- zahrnuje role a funkční místa, které jsou potřebné pro efektivní řízení a zajištění bezpečnosti IS VaVaI.

Pro všechna funkční místa a role musí být stanoveny povinnosti a odpovědnosti v celém životním cyklu zajištění bezpečnosti informací.

Struktura rolí a funkčních míst, včetně jejich působnosti, musí vytvářet předpoklady pro zajištění potřebné podpory procesům bezpečnosti informací a dosahování cílů bezpečnosti informací.

Výkon stanovených rolí musí být zajištěn pracovníky s potřebou kvalifikací; pro vybrané role dle potřeb IS VaVaI musí být zajištěna zastupitelnost pracovníků vykonávající danou roli.

4. Bezpečnost ve vztazích s dodavateli a externími subjekty

4.1. Řízení dodavatelů

Požadavky bezpečnosti informací na snížení rizik spojených s přístupem dodavatelů k aktivům organizace musí být projednány s dodavateli a dokumentovány. Obecná pravidla stanoví Rozhodnutí vedoucího Úřadu vlády ČR č. 8/2017, kterým se vydává Bezpečnostní politika ochrany informačních systémů v Úřadu vlády ČR.

[1] Viz Směrnice vedoucího Úřadu vlády ČR č. 09/2017, o zásadách ochrany informací.

Bezpečnostní cíle stanovené pro oblast řízení dodavatelů zahrnují:

- zajištění ochrany aktiv organizace, ke kterým mají dodavatelé přístup,
- udržování dohodnuté úrovně bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami.

Pro řízení dodavatelů IS VaVaI jsou stanoveny následující bezpečnostní zásady:

a) požadavky bezpečnosti (ve vztahu k dodavateli) jsou stanovovány na základě výsledků hodnocení rizik,
b) každý dodavatel, který může přistupovat k informacím, zpracovávat je, ukládat, komunikovat nebo je zajišťovat prvky IT infrastruktury, je zavázán k dodržování všech relevantních požadavků bezpečnosti informací,
c) dohody s dodavateli zahrnují požadavky na řízení rizik bezpečnosti informací spojených s dodavatelským řetězcem služeb a produktů informačních a komunikačních technologií,

4.2. Pravidla pro výběr dodavatelů

Při výběru dodavatelů zařízení a služeb vztahující se k aktivům IS VaVaI musí být zohledněno:

- bezpečnostní potřeby IS VaVaI související s předmětem zakázky/dodávky,
- rizika vyplývající z předmětu dodávky a konkrétního dodavatele produktu nebo služby.

Výběrem dodavatele musí být minimalizována případná nebo identifikovaná rizika, která by mohla nastat výběrem dodavatele, který není způsobilý splnit předmět zakázky/dodávky. Omezující požadavky (tj. požadavky na bezpečnostní postupy a opatření) při výběru dodavatelů musí být začleněny do zadávacích podmínek výběru dodavatele zakázky.

Hodnocení dodavatelů z bezpečnostního hlediska musí být součástí každého zadávacího řízení, kde předmětem je dodávka služeb nebo zařízení využívané v IS VaVaI.

4.3. Hodnocení rizik související s dodavateli

Hodnocení rizik spojená s dodavateli je prováděno:

- při výběru vhodného dodavatele v rámci výběrového řízení před uzavřením smlouvy,
- v průběhu trvání dodavatelského smluvního vztahu v rámci pravidelného hodnocení rizik.

4.4. Bezpečnostní požadavky v dohodách s dodavateli/externími subjekty

Podmínky, za kterých externí subjekt (dodavatel, třetí strana) může přistupovat k aktivům IS VaVaI, musí být stanoveny ve smlouvě, která musí obsahovat veškeré požadavky vedoucí k naplnění politiky bezpečnosti IS VaVaI v daném smluvním vztahu.

V rámci smluvního vztahu s externím subjektem musí být zajištěno:

a) Ujednání o zajištění bezpečnosti aktiv IS VaVaI v požadovaném rozsahu, tzn. zejména povinnost zachovávat mlčenlivosti, dodržovat zásady bezpečnosti informací dle požadavků IS-VaVaI, poskytovat součinnost při zajišťování bezpečnosti informací dle požadavku právních předpisů ČR.
b) Že externí subjekt (dodavatel) bude schopen dodržovat veškerá bezpečnostní opatření dle požadavků IS VaVaI.

c) Ujednání o kontrolním (auditním) režimu, v rámci, kterého je externí subjekt povinen podrobit se kontrole za účelem kontroly dodržování bezpečnostních opatření.

Pro řešení smluvních vztahů a uzavírání smluv s externími subjekty s přístupem k aktivům IS VaVaI je využíván metodický postup platná v rámci úřadu vlády.

4.5. Bezpečnostní požadavky ve smlouvách o outsourcingu

Smluvní vztah s externím subjektem (dodavatelem) zajišťující outsourcing určitých činností pro IS VaVaI, musí (kromě obecných požadavků pro smlouvy s dodavateli), též stanovovat podrobnější požadavky na pokrytí rizik vyplývající z této činnosti, zejména se jedná o stanovení:

a) jak budou splněny právní požadavky na provoz těchto systémů, tj. požadavky platné legislativy ČR a EU na ochranu osobních údajů,
b) jak bude zajištěno, aby si všechny smluvní strany, včetně subdodavatelů poskytovatele outsourcingu, byly vědomy své odpovědnosti za bezpečnost dat,
c) jak bude udržována a testována integrita a důvěrnost aktiv,
d) jaká logická a fyzická opatření budou použita pro zajištění přístupu oprávněných uživatelů k informacím IS VaVaI,
e) jak bude v případě havárie zajištěna dostupnost služeb.

5. Politika bezpečnosti lidských zdrojů

Cílem politiky bezpečnosti lidských zdrojů zajištění výběru vhodných osob pro výkon zamýšlených činností v IS VaVaI; aby všichni zaměstnanci chápali své povinnosti při zajištění bezpečnosti informací a udržování bezpečnostního povědomí uživatelů IS VaVaI. Účelem procesu řízení bezpečnosti lidských zdrojů je snížení rizika lidské chyby a zneužití prostředků IS VaVaI.

Bezpečnostní cíle v oblasti lidských zdrojů jsou zajišťovány:

a) postupy v rámci přijímacího řízení zaměstnanců,
b) udržování bezpečnostního povědomí uživatelů IS VaVaI,
c) vhodnými postupy při obsazování pracovních pozici, včetně změny pracovní pozice,
d) vhodnými postupy při ukončení pracovního poměru zaměstnance.

Pro oblast personální bezpečnosti jsou v rámci IS VaVaI stanoveny následující bezpečnostní zásady:

Podmínky pracovního poměru:

a) Je veden přehled funkčních míst, kde ke každému pracovnímu místu jsou přiřazeny požadavky na odbornou kvalifikaci a další specifické požadavky na dané místo.

Před vznikem pracovního vztahu:

b) posuzování uchazečů o zaměstnání z hlediska personální bezpečnosti je součástí výkonu personálních činností dle Pracovního řádu a v souladu s obsahem pracovněprávních dokumentů v personálních šablonách,
c) seznámení zaměstnanců s Politikou bezpečnosti informací IS VaVaI v rámci vstupního školení a dalších periodických školení bezpečnosti informací,

Během pracovního vztahu:

d) zaměstnanci podepisují prohlášení o mlčenlivosti formou závazku zaměstnance ve smyslu zákonem uložené povinnosti,
e) zaměstnanci jsou povinni zachovávat mlčenlivost o skutečnostech, se kterými se seznámili při plnění svých pracovních úkolů nebo v přímé souvislosti s nimi a tato povinnost trvá i po skončení pracovního vztahu, pokud zvláštní právní předpis nestanoví jinak,
f) v případě změny pracovního stavu jsou přístupová práva modifikována dle potřeb nově přidělené pracovní pozice,
g) nedodržení bezpečnostních zásad může být kvalifikováno jako porušení povinností zaměstnance příp. porušení pracovní kázně s příslušnými důsledky pro zaměstnance, ve smyslu zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů nebo trestný čin podle § 178 zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů,

Ukončení pracovního vztahu:

h) Pro ukončení pracovního stavu jsou stanoveny příslušné postupy, které mimo jiné zahrnují navrácení zapůjčených prostředků zpracování informací a zrušení přístupových práv.

Bezpečnostní povědomí

V RVVI je formulován Plán rozvoje bezpečnostního povědomí“ v té míře, jehož realizací bude zajištěno odpovídající vzdělávání a zlepšování znalostí zaměstnanců RVVI a osob vykonávající stanovené role v IS VaVaI.

Školení je realizováno v rámci:

- školení nových zaměstnanců,
- všeobecného vzdělávání zaměstnanců RVVI dle ročního plánu,
- dalších specializovaných školení pro bezpečnostní role.

Disciplinární řízení

Porušení zásad bezpečnosti informací se považuje za porušení pracovních povinností zaměstnance. Disciplinární řízení těch, kteří porušili pravidla bezpečnosti informací, jsou řešena v Pracovním řádu, Zákonu o státní službě a dle Zákoníku práce.

6. Řízení přístupu

Řízení přístupu k informačním aktivům a prostředkům pro jejich zpracování v IS VaVaI musí zabezpečit využívání těchto aktiv a prostředků pouze oprávněnými uživateli. Pro přístup k informacím a prostředkům IS VaVaI jsou stanovena pravidla, určují postupy pro autorizaci, zřizování, změny a odebírání přístupových práv. Systém správy přístupu IS VaVaI zajišťuje definovaný postup přidělování, změny a odebírání přístupu, správu hesel a kontrolu přístupových oprávnění.

6.1. Přístupová oprávnění k IS VaVaI

V rámci IS VaVaI jsou využívány následující uživatelské role, pro které jsou nastavena speciální aplikační oprávnění:

Role[2]	Rozsah činností a oprávnění
Administrátor – Úřad vlády	Přihlášení do rozhraní IS VaVaI pro Administrátory, správa všech číselníků, administrace a správa uživatelů všech úrovní, správa definic oprávnění, zálohování databáze, správa webu a verzí SW, správa všech oblastí IS VaVaI (CEP, CEA, RIV, VES).
Administrátor – Správce rady	Přihlášení do rozhraní IS VaVaI pro Administrátory, správa všech oblastí IS VaVaI (CEP, CEA, RIV, VES), schvalování nových a editovaných veřejných soutěží, schvalování nových a editovaných aktivit.
Uživatel – Poskytovatel	Přihlášení do rozhraní IS VaVaI pro Poskytovatele, založení a editace záznamů vlastní organizace, změna přístupového hesla
Uživatel – Příjemce	Přihlášení do rozhraní VaVER pro vytváření XML souborů pro předávání dat v požadované a předepsané struktuře. Nicméně funkcionalita je udělaná tak, že ti lidé jsou administrátorem spravování a mají účty s přístupem na provozní server IS VaVaI.
Anonymní uživatel	Prohlížení záznamů ve veřejné části IS VaVaI

Zakládání účtů **Uživatel – Poskytovatel** a přidělování oprávnění provádí **Administrátor – Úřad vlády** na základě písemné žádosti schválené vedoucím Oddělení informačních systémů Odboru Rady pro výzkum, vývoj a inovace.

Uživatelská oprávnění pro správu virtualizační platformy, operačních systémů, databází a aplikačních serverů jsou omezena na definované pracovníky Úřadu vlády ČR, kteří dané úkony vykonávají jako:

Role	Rozsah činností a oprávnění
Systémový administrátor	Administrátorská oprávnění ke správě virtualizační platformy a operačního systému serverů, k nástrojům pro zálohování a dalším technologickým SW
Databázový administrátor	Administrátorská oprávnění k databázovému systému
Administrátor aplikace	Administrátorská oprávnění k aplikačnímu serveru, správa kódu aplikace, správa verzí a release management

Zakládání uživatelů a přidělování oprávnění provádí vedoucí Oddělení informačních systémů Odboru Rady pro výzkum, vývoj a inovace nebo jím pověřený administrátor.

[2] Administrátorem je v kontextu tohoto přehledu myšlena uživatelská role s rozšířenou sadou oprávnění v rámci aplikace IS VaVaI, nikoliv osoba s oprávněními nutnými pro administraci technických systémů zajišťujících provoz IS VaVaI

6.2. Bezpečné postupy přihlášení

Přístup k informačním službám IS VaVaI musí být zajištěn prostřednictvím bezpečného přihlašovacího postupu, který musí minimalizovat možnost neoprávněného přístupu, „prozrazuje“ minimum informací a který musí:

a) Nezobrazovat identifikátory systému nebo aplikace, dokud není přihlašovací proces dokončen,
b) Zobrazovat obecné varování, že počítač smí používat pouze oprávnění uživatelé.
c) Neposkytovat nápovědu během přihlašovacího postupu, která může pomoci neoprávněnému uživateli.
d) Zkontrolovat platnost přihlašovacích informací jen v případě, že jsou vstupní data kompletní. Pokud se vyskytne chyba, systém neindikuje, která část přihlašovacích dat je správná, nebo chybná.
e) Stanovit maximální počet povolených neúspěšných přihlašovacích pokusů. Při jejich překročení:
    - účet uživatele musí být uzamčen a blokován na určitou dobu a zařízení uživatele odpojena od všech připojení,
    - dalšího pokusy o přihlášení povolit po uplynutí stanovené doby, minimálně po 60 minutách.
f) Omezí minimální a maximální dobu povolenou pro přihlášení; pokud je překročena, systém by měl přihlašovací postup ukončit.
g) Při dokončení úspěšného přihlášení zobrazí následující informace:
    - datum a čas předchozího úspěšného přihlášení,
    - informace o všech neúspěšných pokusech o přihlášení od posledního úspěšného přihlášení.

6.3. Správa a ověřování identit

K ověřování identity uživatelů je využíván autentizační mechanismus založený na ověření identity uživatele na základě ID uživatele a hesla vydané k účtu uživatele. Přidělování autentizačních faktorů (identifikátor účtu a hesla) je zajištěno formálním postupem, zajišťující bezpečnost vydaných autentizačních informací.

Pro správu a použití hesel PIN platí následující pravidla:

a) všechna hesla (včetně jednorázových) musí být bezpečná a musí splňovat podmínky stanovené touto politikou,
b) při prvním přihlášení nově vydaným heslem musí být vynucena změna tohoto hesla uživatelem,
c) heslo nesmí být v počítači uloženo v otevřené podobě,
d) ověření identity musí být provedeno před zahájením aktivit v IS,
e) uživatel je poučen o pravidlech nakládání s hesly a jeho povinnosti udržovat autentizační údaje v tajnosti,
f) hesla jsou ukládána v zašifrované podobě s použitím jednosměrného šifrovacího algoritmu odděleně od dat aplikací.

Nástroj pro správu a pro ověřování identity v IS musí splňovat následující pravidla:

a) Je řízen počet neúspěšných pokusů o přihlášení, dle následujícího:
   - maximální počet povolených neúspěšných pokusů je 5,
   - při překročení tohoto počtu neúspěšných pokusů je účet uživatele zablokován na 60 minut.

b) Jsou nastavena pravidla řízení a používání hesel dle následujícího:
   - minimální délka hesla je:
     - běžný uživatel = 12 znaků,
     - uživatel s privilegovaným přístupem = 17 znaků,
   - maximální doba platnosti = 18 měsíců,
   - minimální doba platnosti hesla = nesmí být kratší než 30 minut,
   - opětovně použití dříve použitých hesel = minimálně 12 předchozích hesel,
   - nelze použít mnohonásobně opakující se znaky, uživatelské jméno, …

c) je povinná změna hesla v intervalu maximální doby platnosti hesla.

d) po určité době nečinnosti účtu uživatele je vynuceno opětovné ověření identity uživatele.

e) „prvotní“ heslo sloužící ke zřízení nebo obnovení přístupu k IS, po jeho prvním použití, musí být bezodkladně zneplatněno.

Přístupová oprávnění uživatelů jsou kontrolována v pravidelných intervalech, max. interval 12 měsíců.

6.4. Vzdálený přístup pracovníků provádějící správu IS VaVaI

Vzdálený přístup je povolen pouze určeným pracovníkům správy IS VaVaI. Připojení je možné pouze přes VPN vytvářenou pracovištěm OIT.

7. Bezpečné chování uživatelů

Problematika způsobů využívání výpočetní techniky a dalších prostředků pro zpracování informací je definována jednotně pro všechna pracoviště v rámci Úřadu vlády ČR.

Zásady používání výpočetní techniky jsou stanoveny ve **Směrnici vedoucího Úřadu vlády ČR č. 2/2017, o zásadách užívání výpočetní techniky a kancelářské techniky**.

Za využívání výpočetní techniky na straně „Poskytovatelů“ odpovídá příslušný „Poskytovatel“ informací do IS VaVaI.

Odpovědnost uživatele IS VaVaI

Uživatel IS VaVaI je odpovědný za ochranu autentizačních informací (identifikátor uživatele a heslo), při tom se řídí následujícími pravidly:

- heslo se udržuje v tajnosti, tzn. že nesmí být zapisováno, s výjimkou míst, kdy jsou bezpečně uložena,
- změna hesla se provádí v případě jakéhokoliv náznaku jeho možného kompromitování (tj. porušení důvěrnosti hesla),
- heslo se vytváří v souladu s politikou pro tvorbu hesel tak, aby:

  - splňovalo minimální počet znaků pro heslo,
  - nebylo založeno na informacích vztahujících se k uživateli, které by mohl kdokoliv další lehce uhodnout nebo získat, např. jména, telefonní čísla, data narození apod.,
  - neobsahovalo po sobě jdoucí stejné znaky a neobsahovalo pouze číselné nebo pouze písmenné skupiny,
- měnit heslo v pravidelných intervalech,
- nepoužívat opakovaně dřívějších hesla,
- změnit dočasně vydaná hesla při prvním přihlášení,
- nezahrnovat hesla do žádného automatizovaného přihlašovacího procesu, např. uložení do makra nebo funkční klávesy, výjimkou jsou systémy pro šifrované uložení dat (např. tokeny, šifrované databáze atd.),
- nesdílet osobní uživatelská hesla s jinou osobou.

8. Bezpečnost provozu ICT

8.1. Řízení provozu a komunikací

Řízení provozu IS VaVaI musí: zajistit správný a bezpečný provoz systémů a všech jeho součástí při zpracování informací, minimalizovat riziko selhání systému, minimalizovat negativní dopady havárie systému, chránit integritu a dostupnost programů, dat a informačních systémů, chránit důvěrnost informací a zajistit ochranu počítačových sítí.

Při řízení provozu IS VaVaI jsou využívány následující bezpečnostní zásady, prvky a činnosti:

a) je využívána ochrana proti škodlivým a automaticky spouštěným programům a škodlivému kódu,
b) je prováděno zálohování, které umožní obnovu dat a systémů ve vazbě na zachování základních funkcí IS VaVaI,
c) jsou zpracovány postupy obnovy po selhání nebo výpadku IS VaVaI,
d) je prováděno zajišťování bezpečnosti komunikační infrastruktury,
e) je zajištěna dostupnost informací a služeb dle definované požadované úrovně dostupnosti stanovené v rámci klasifikace aktiv,
f) je zajištěna důvěrnost informací při jejich přenosu pomocí kryptografické ochrany,
g) je zajištěna ochrana před neautorizovanými zásahy dodržováním principu oddělení povinností a odpovědností při přidělování uživatelských práv,
h) je prováděno monitorování provozu a zaznamenávání událostí,
i) jsou přijata opatření pro zajištění bezpečnosti elektronické pošty,
j) je vymáháno dodržování bezpečnosti při zacházení s paměťovými médii.

Bezpečnost provozu IS VaVaI zajišťuje odbor informatiky ÚV ČR.

8.2. Politika zálohování a obnovy

Zálohování dat musí ochránit data v informačním systému IS VaVaI před jejich ztrátou, přičemž režim pořizování záloh (tj. četnost a rozsah) musí být nastaven v souladu s mírou rizika ztráty dat a odrážet požadavky IS VaVaI na kritičnost informací z hlediska zajištění kontinuity činnosti IS VaVaI.

Režim a opatření při zálohování musí zajistit obnovu všech důležitých informací a software IS VaVaI v případě havárie.

Pravidla a postupy pro zálohování a obnovu dat stanoveny v provozní dokumentaci IS VaVaI dle v následujícím rámci:

- zálohování celého systému se provádí denně, tyto denní zálohy se uchovávají měsíc,
- vytváření je měsíční a roční zálohy (kopie), případně dle potřeby.
- Jsou dokumentovány a testovány postupy obnovy chodu systému.

8.3. Přenos/výměna informací

V rámci komunikační sítě využívané IS VaVaI jsou využívány prostředky a postupy zajišťující bezpečnost, funkčnost a spolehlivost přenosů informací v míře vyplývající z výsledků hodnocení rizik.

Pro zajištění spolehlivost a důvěrnosti přenosů musí být aplikováno (dle potřeby):

- užití dedikovaných nebo nesdílených komunikačních cest,
- kryptografická ochrana přenášených informací na úrovni přenosové cesty, spojení nebo transakce,
- řízení kapacity datových toků pomocí omezení nebo stanovením priorit.

Konkrétní způsob zajištění provozu a bezpečnosti přenosu informací stanovuje Odbor informatiky ÚV ČR.

Pravidla používání kryptografické ochrany při přenosu zpráv

Pro použití prostředků kryptografické ochrany musí být definována pravidla – tj. způsob používání šifrování, elektronického podpisu.

8.4. Správa technických zranitelností

Cílem bezpečnostních opatření je zabránění využívání technických zranitelností zařízení v rámci infrastruktury ICT využívané IS VaVaI. Musí být definován proces správy a kontroly technických zranitelností, který zahrnuje:

a) stanovení odpovědností pro správu zranitelností (v rámci ICT),
b) určení důvěryhodných zdrojů informací o zranitelnostech,
c) určení činností (posouzení rizika, priorit, postupů) při reakci na zjištěné zranitelnosti,
d) určení způsobu otestování záplaty a vyhodnocení jejich účinku / vedlejších účinků,
e) Vyhodnocování účinnosti a efektivity správy zranitelností.

Omezení instalace software

Instalaci SW na zařízení ICT mohou provádět pouze stanovení pracovníci (administrátoři), pro uživatele musí být zakázáno provádět instalaci software, resp. musí být stanoveno, jaké typy instalací jsou povoleny (např. aktualizace systému, záplaty, …) a jaké jsou zakázány,

Instalace software musí splňovat licenční podmínky a jsou vedeny záznamy o instalaci jednotlivých software na prostředcích ICT.

9. Bezpečné používání mobilních zařízení

Pravidla pro využívání mobilních zařízení v IS VaVaI vychází ze zásad bezpečnosti stanovených v rámci Úřadu vlády ČR, viz. Směrnice vedoucího Úřadu vlády ČR č. 2/2017, o zásadách využívání výpočetní a kancelářské techniky.

10.Akvizice, vývoj a údržba IS VaVaI

Cílem v oblasti vývoje a údržby je prosazení bezpečnosti informací do celého životního cyklu IS VaVaI, jak ve fázi vývoje, tak při jeho provozování a údržbě. Zajištění bezpečnosti informací musí být zajištěno především prostřednictvím opatření:

a) analýzou a specifikací bezpečnostních požadavků – tzn. určení bezpečnostních požadavků v jednotlivých fázích životního cyklu IS, jejich definování a případně dokumentování v rámci plánované akvizice,
b) k zajištění přesnosti a spolehlivosti zpracování dat v aplikacích a kryptografická opatření – validace a kontrola dat má spolu s kryptografickými opatřeními za cíl předcházet ztrátě, neoprávněné modifikaci nebo zneužití dat v aplikacích,
c) bezpečnost systémových souborů a procesu vývoje a podpory – je nutné zabezpečit systémové soubory a zdrojový kód a kontrolovat postupy vývoje a podpory, včetně formalizovaného postupu řízení změn,
d) správa zranitelností – je nutné vhodnými opatřeními omezit rizika vyplývající ze zneužití publikovaných zranitelností,
e) při akvizici/vývoji představující „významnou změnu“, vždy musí být využito vývojové a testovací prostředí, včetně vytvoření testovacích dat.

Obecně pro akvizice v IS VaVaI platí, že nově zaváděné aplikace a komponenty systému musí splňovat požadavky bezpečnosti informací vyplývající z platné legislativy ČR a EU a politiky bezpečnosti informací ÚV ČR.

Licenční politika

V oblasti nabývání licencí programového vybavení IS VaVaI musí být dodržována pravidla a postupy vyplývající z licenční politiky ÚV ČR.

11. Ochrana osobních údajů

Zpracování osobních údajů (OÚ) vyplývá z nařízení 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).; ve které je rovněž stanoven povinný rozsah zpracovávaných OÚ a povolené způsoby jejich zpracování, resp. zveřejňování.

Zpracování OÚ v IS VaVaI musí naplňovat požadavky obecně platných zákonných předpisů ČR a EU pro tuto oblast. Bezpečnost zpracovávaných OÚ je zajišťována opatřeními kybernetické bezpečnosti.

12. Fyzická a objektová bezpečnost

Účelem fyzické bezpečnosti je zabránění fyzickému přístupu nepovolaných osob, poškození a narušování i informačních a technických aktiv IS VaVaI. Pro zajištění fyzické bezpečnosti aktiva IS VaVaI platí následující pravidla.

Zabezpečené oblasti

Všechna aktiva IS VaVaI musí být umístěna v zabezpečených oblastech, ve kterých jsou aplikována adekvátní bezpečnostní opatření k zamezení působení hrozeb, fyzikálním vlivům a neautorizovanému přístupu.

Pro zabezpečené oblasti:

- je definován a dokumentován bezpečnostní perimetr a provozní řád,
- na základě posouzení rizik jsou aplikována potřebná bezpečnostní opatření fyzické bezpečnosti k eliminaci zjištěných rizik,
- je aplikováno řízení přístupu do zabezpečených oblastí k zamezení neoprávněného vstupu, příp. poškození umístěných technických aktiv či neoprávněným zásahům.

Objektová bezpečnost

Přístup do objektů s aktivy IS VaVaI, včetně zabezpečených oblastí IS VaVaI, je chráněn přiměřenými kontrolami vstupu v rámci režimových opatření objektu. Opatření objektové bezpečnosti zajišťuje správce daného objektu.

Pro ochranu kanceláří v objektu jsou zavedena vhodná opatření dle bezpečnostních požadavků stanovených na základě posouzení rizik. Minimálním bezpečnostním požadavkem je – kanceláře musí být uzamykatelné a musí být vybaveny uzamykatelnými skříněmi.

Bezpečnost zařízení

K zajištění bezpečnosti zařízení související se zpracováním informačních aktiv IS VaVaI musí být uplatněny níže uvedená pravidla:

a) **Umístění zařízení a jeho ochrana** – zařízení pro zpracování informací IS VaVaI a související infrastruktura prostředků ICT musí být umístěna a chráněna tak, aby:
   - se snížila rizika působení vnějších hrozeb (oheň, voda, kouř, prach, …),
   - bylo sníženo nebezpečí zásahu nepovolných osob a úniku informací postranními kanály.

b) **Podpůrná zařízení a služby –** důležitá technická aktiva musí být chráněna proti výpadkům napájení a proti dalším poruchám způsobených výpadky podpůrných služeb a musí být zajištěno vhodné prostředí pro jejich provoz (například teplota, vlhkost, …). Správná funkčnost podpůrných zařízení a služeb musí být periodicky kontrolována a testována.

c) **Údržba zařízení** – technická aktiva IS VaVaI musí být udržována a provozována v souladu s doporučeními dodavatele a výrobce. Pro údržbu a opravy zařízení platí následující pravidla:
   - opravy a servis musí provádět pouze oprávněný personál,
   - o všech závadách, preventivních prohlídkách a opravách musejí být pořízeny záznamy,
   - před provedením údržby zařízení mimo bezpečnostní perimetr IS VaVaI, musí být odstraněna veškerá klasifikovaná data se stupněm Interní a Diskrétní,

- při servisní činnosti prováděné externími pracovníky na pracovišti RVVI, musejí být tito pracovníci po celou dobu pobytu doprovázeni odpovědnými pracovníky RVVI s oprávněným přístupem k danému zařízení.

d) **Bezpečnost zařízení mimo prostory organizace** – pro technická zařízení trvale (nebo i dočasně) umístěná mimo perimetr fyzické ochrany IS VaVaI musí být zajištěna fyzická ochrana těchto zařízení v souladu s předpokládanými riziky.

Opatření fyzické/objektové jsou zajišťována správci objektů, jsou pravidelně kontrolována, aktualizována a revidována na základě periodicky prováděné analýzy rizik a auditu bezpečnostních opatření.

13. Bezpečnosti komunikační sítě

Zajištění bezpečnosti komunikační sítě ÚV ČR, které využívá IS VaVaI, spadá do kompetence Odboru informatiky ÚV ČR.

14. Ochrany před škodlivým kódem

Ochrana proti škodlivým kódům v IS VaVaI musí být založena především na detekci škodlivých kódů, dále též na bezpečnostním povědomí uživatelů, na opatřeních řízení změn v IS VaVaI.

Ochrana před škodlivými kódy v IS VaVaI:

a) koncových stanic uživatelů – je zajišťována postupy a prostředky příslušných provozovatelů této výpočetní techniky – tzn. v rámci ÚV ČR (pro uživatele z řad RVVI) a dále v rámci jednotlivých poskytovatelů informací do IS VaVaI.

b) Serverů, datových úložišť a komunikačních prvků – je zajišťovány v rámci zabezpečení ICT Úřadu vlády ČR.

V případě písm. b) musí být ochrana zajištěna instalací vhodného nástroje pro ochranu proti škodlivým kódům, který je pravidelně aktualizován.

15. Nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

Vzhledem ke skutečnosti, že IS VaVaI je provozován v rámci sítě ÚV ČR, potom problematika detekce a vyhodnocení kybernetických událostí, včetně nasazení příslušného nástroje pro detekci a vyhodnocování událostí, je plněn v kompetenci Odboru informatiky ÚV ČR.

16. Používání kryptografické ochrany

K zajištění správného a efektivního využívání kryptografické ochrany v rámci IS VaVaI musí být naplněny následující zásady:

- při aplikování prostředků kryptografické ochrany musí být využívány aktuálně odolné kryptografické algoritmy a klíče,
- opatření kryptografické ochrany jsou dokumentována v provozní dokumentaci IS VaVaI,
- opodstatněnost využití opatření kryptografické ochrany, včetně úroveň ochrany, musí vyplývat z výsledků hodnocení rizik bezpečnosti informací a z ohodnocení informačních aktiv,
- použití kryptografické ochrany v IS VaVaI nesmí být v rozporu s platnou legislativou ČR a EU.

Použití prostředků kryptografické ochrany IS VaVaI schvaluje Manažer KB IS VaVaI.

17. Řízení změn

Změny související s provozem IS VaVaI musí být řízeny s využitím formálních postupů a musí být provedeno posouzení možných dopadů plánované změny. V případě, že plánovaná změna představuje „významnou změnu“[3] z hlediska bezpečnosti informací, potom řízení plánované změny musí zahrnovat:

- stanovení postupu plánování, schvalování a realizace změny,
- posouzení rizik vyplývající z plánované změny a přijetí opatření za účelem snížení nepříznivých dopadů se změnami,
- aktualizaci relevantní dokumentace,
- otestování, zda provedená změna nemá dopady na bezpečnost informací,
- nouzové postupy za přerušení změn a obnovení původního stavu.

Všechny změny musí být schváleny a dokumentovány v IS VaVaI.

18. Zvládání kybernetických bezpečnostních incidentů

Vzhledem ke skutečnosti, že IS VaVaI je provozován v rámci sítě ÚV ČR, potom problematika detekce a vyhodnocení kybernetických událostí nebo incidentů je zajišťována prostředky této sítě ÚV ČR a je plněn v kompetenci Odboru informatiky ÚV ČR.

19. Řízení kontinuity činností

Cílem je zajistit připravenost na řešení krizových situací a zachování základních provozních a bezpečnostních funkcí IS VaVaI v rozsahu definovaných zákonem o RVVI.

V rámci ÚV ČR pro řízení kontinuity činností, ve vztahu k IS VaVaI, jsou definovány následující bezpečnostní zásady:

a) rozhodnutí o zablokování komunikace IS VaVaI anebo o realizaci dalších opatření (mající vliv na rozsah služeb IS VaVaI) z důvodů detekované bezpečnostní události I, spadá do kompetence **Manažera KB IS VaVaI**. Ten je oprávněn tuto kompetenci v definovaných případech delegovat na **Manažera KB Úřadu vlády**.

[3] Viz Vyhláška č.82/2018 Sb., §2 písm. o) – významná změna – změna, která má nebo může mít vliv na kybernetickou bezpečnost IS a představuje vysoké riziko.

b) realizace přechodu na krizové řízení spadá do kompetence **Manažera KB Úřadu vlády.**
c) realizace opatření k zachování základních funkcí spadá do kompetence **Manažera KB IS VaVaI.**

Cíle řízení kontinuity IS VaVaI

Cíle řízení kontinuity IS VaVaI jsou definovány následujícím způsobem:

1. minimální úrovně poskytovaných služeb, která je přijatelná pro zajištění funkcionalit IS VaVaI.
2. doba obnovení chodu IS VaVaI, během které bude obnoven provoz IS VaVaI na definované minimální úrovni,
3. stanovení doby obnovy dat IS VaVaI, během které musí být zpětně obnovena data IS VaVaI po incidentu nebo selhání prostředků systému.

Cíle řízení kontinuity IS VaVaI jsou stanoveny na základě vyhodnocení výsledků hodnocení rizik, analýzy dopadů možných incidentů a požadavků stanovených provozním řádem IS VaVaI.

Havarijní plány IS VaVaI

Jsou definovány plány kontinuity činnosti (havarijní plány) IS VaVaI, které obsahují postupy odezvy na nežádoucí („možné“) situace, postupy na udržení bezpečnosti informací IS VaVaI a odpovědnosti jednotlivých rolí.