Národní úřad
pro kybernetickou
a informační bezpečnost

P. O. BOX 17
616 00 Brno 16
www.nukib.cz

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Zásady tvorby bezpečnostní dokumentace informačních systémů určených k nakládání s utajovanými informacemi

verze 1.0

Praha, 2017

Obsah

1. Úvodní informace

Následující návod podává základní informace pro tvorbu bezpečnostní dokumentace informačního systému, který je určen k nakládání s utajovanými informacemi a provozovaný v bezpečnostním provozním módu vyhrazeném nebo s nejvyšší úrovní, případně s nejvyšší úrovní s formálním řízením přístupu k informacím. Cílem je zejména usnadnit tvorbu bezpečnostní dokumentace pro účely certifikace informačního systému vlastními silami žadatele.

POZNÁMKA

Pro informační systém založený na použití jednoho nebo více samostatných osobních počítačů se vynechají části týkající se komunikací a jejich zabezpečení.

2. Dokument „Bezpečnostní politika informačního systému“

Dokument „Bezpečnostní politika informačního systému“ je základním dokumentem bezpečnostní dokumentace informačního systému. Vzniká jako první v návaznosti na potřebu provozovat certifikovaný informační systém určený k nakládání s utajovanou informací.

Dokument „Bezpečnostní politika informačního systému“ musí splňovat následující požadavky:

- neobsahuje konkrétní informace (typ HW nebo SW, umístění, nastavení parametrů apod.),
- je tvořen zejména deklaracemi naplnění požadavků právních norem především z oblasti ochrany utajovaných informací,
- je maximálně stručný a v rozsahu maximálně několika stran,
- je autorizován oprávněnou osobou organizace.

2.1. Struktura dokumentu „Bezpečnostní politika informačního systému“

1. Úvodní ustanovení
2. Personální bezpečnost
3. Počítačová bezpečnost
4. Kryptografická ochrana
5. Fyzická bezpečnost
6. Administrativní bezpečnost
7. Řízení a plánování kontinuity
8. Další bezpečnostní dokumentace

2.2. Kapitola „1. Úvodní ustanovení“

Kapitola „Úvodní ustanovení“ slouží k základnímu popisu informačního systému a k vymezení základních bezpečnostních cílů.

Základní popis informačního systému obsahuje:

- základní definici struktury informačního systému (samostatný počítač, skupina samostatných počítačů, malá LAN, rozsáhlá LAN),
- základní určení dislokace informačního systému (neuvádí se konkrétní umístění, ale pouze rozsah umístění informačního systému jedna/několik místností, jedno/několik pater budovy, jedno/několik budov v jednom/několika areálech apod.),
- určení základních typů periferních zařízení (síťové/lokální tiskárny a skenery, aj.),

- nejvyšší stupeň utajení zpracovávaných informací,
- v případě předpokládaného zpracovávání informací cizí moci i nejvyšší stupeň utajení informací cizí moci,
- zvolený bezpečnostní provozní mód,
- základní typ a účel zpracovávaných utajovaných informací (běžné dokumenty, databáze, výkresová dokumentace apod.),
- rozsah utajovaných informací s odkazem na položky Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací,
- základní typ aplikačního SW (kancelářský SW, SW pro kreslení technických výkresů apod.),
- předpokládaný počet uživatelů,
- předpokládaný rozsah zpracování utajovaných informací (časový údaj např. počet hodin za pracovní den),
- použitý operační systém/systémy (neuvádí se konkrétní verze),
- vztah k jiným počítačovým sítím (u samostatných osobních počítačů např. vyjmutí síťové karty, zákaz použití modemu, u LAN zpravidla izolace od jiných počítačových sítí),
- v případě záměru použití kryptografických prostředků uvést účel.

Mezi základní bezpečnostní cíle patří:

- zajištění důvěrnosti a integrity utajované informace všude, kde se vyskytuje,
- zajištění dostupnosti informace a služeb informačního systému a odpovědnosti uživatele informačního systému za jeho činnost v něm,
- zajištění nepopiratelnosti a pravosti informací všude, kde je to aplikovatelné,
- zpracování utajovaných informací bude probíhat v souladu s požadavky zákona č. 412/2005 Sb. a s příslušnými vyhláškami Úřadu v platném znění,
- zpracování utajovaných informací bude probíhat v souladu s požadavky dalších právních předpisů, norem, mezinárodních smluv, nadřízené bezpečnostní politiky, interních předpisů apod. (uvést jejich případný seznam).

2.3. Kapitola „2. Personální bezpečnost“

V kapitole „Personální bezpečnost“ jsou deklarovány základní požadavky na informační systém z hlediska personální bezpečnosti vycházející ze zákona č. 412/2005 Sb. a §§ 16 až 19 vyhlášky č. 523/2005 Sb.

- definice rolí působících v informačním systému (bezpečnostní správce, správce, uživatel apod.) včetně deklarace vytvoření provozních bezpečnostních směrnic pro tyto role, které budou definovat jejich povinnosti,
- deklarace základních požadavků na uživatele informačního systému:
    - splnění podmínek přístupu fyzické osoby k utajované informaci stupně utajení odpovídajícího nejvyššímu stupni utajení informace, která může být v informačním systému zpracovávána (§ 6 nebo § 11 zákona č. 412/2005 Sb.),
    - splnění podmínek přístupu fyzické osoby k utajované informaci cizí moci,
    - pověření do role v informačním systému,
    - proškolení ze znalostí provozních bezpečnostních směrnic (§ 19 odst. 2 vyhlášky č. 523/2005 Sb.),
    - další požadavky podle potřeb organizace (např. odborná způsobilost).

- deklarace zavedení formálních postupů pro udělení oprávnění pro přístup do informačního systému, zavedení uživatele do informačního systému, pro včasné vyřazení uživatele při zániku jeho Osvědčení nebo Oznámení, změně jeho pracovního zařazení, odchodu z organizace apod.,
- deklarace zásady používání jedinečného identifikátoru uživatele pro přístup k informačnímu systému.

2.4. Kapitola „3. Počítačová bezpečnosti“

V kapitole je deklarováno naplnění minimálních požadavků počítačové bezpečnosti podle §§ 7 a 8 vyhlášky č. 523/2005 Sb., požadavků na ochranu proti kompromitujícímu vyzařování podle § 14 vyhlášky č. 523/2005 Sb., požadavků na bezpečnost při instalaci informačního systému podle § 22 vyhlášky č. 523/2005 Sb. a požadavků na bezpečnost provozovaného informačního systému podle § 23 vyhlášky č. 523/2005 Sb.

V rámci požadavků počítačové bezpečnosti je deklarováno zejména naplnění zajištění:

- jednoznačné identifikace a autentizace,
- volitelného řízení k objektům informačního systému,
- nepřetržitého zaznamenávání a možnosti zpětného zkoumání auditních záznamů,
- ošetření paměťových objektů před jejich dalším použitím,
- bezpečnosti vstupně výstupních portů (zejména výměnné nosiče informací),
- naplnění požadavků komunikační bezpečnosti podle §§ 9 a 9a vyhlášky č. 523/2005 Sb.,
- ochrany před škodlivým kódem (zejména antivirová ochrana),
- ochrany proti úniku utajovaných informací prostřednictvím kompromitujícího vyzařování,
- ochrany utajovaných informací při servisní činnosti,
- požadavků na dostupnost informací a služeb informačního systému v čase a místě podle § 10 vyhlášky č. 523/2005 Sb., (jak dlouho smí být služby nedostupné, jaká minimální funkčnost musí být zajištěna i v krizových situacích).

2.5. Kapitola „4. Kryptografická ochrana“

Tato kapitola se zařazuje pouze v případě, že bude v informačním systému provozován kryptografický prostředek certifikovaný podle zákona č. 412/2005 Sb. Je třeba uvést, zda kryptografický prostředek bude použit pro ochranu utajované informace uložené na počítačovém médiu nebo pro ochranu komunikací a deklarovat zajištění souladu se zákonem č. 412/2005 Sb. a vyhláškou č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb.

2.6. Kapitola „5. Fyzická bezpečnost“

V kapitole je deklarováno naplnění požadavků fyzické bezpečnosti v závislosti na tom, zda na daném zařízení se informace pouze zpracovávají a zobrazují nebo i ukládají podle vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011 Sb., a § 20 vyhlášky č. 523/2005 Sb.

2.7. Kapitola „6. Administrativní bezpečnost“

V kapitole je deklarováno naplnění požadavků administrativní bezpečnosti podle vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů.

V rámci administrativní bezpečnosti je deklarováno naplnění požadavků:

- na nosiče utajovaných informací podle § 15 vyhlášky č. 523/2005 Sb.,
- na evidenci a autorizaci administrativních a evidenčních pomůcek a dokumentace.

2.8. Kapitola „7. Řízení a plánování kontinuity“

V kapitole je deklarováno zajištění řízení kontinuity a vypracování plánů kontinuity (havarijní plány a činnosti při krizových situacích a bezpečnostních incidentech).

2.9. Kapitola „8. Další bezpečnostní dokumentace“

V kapitole je deklarováno, že bude provedena analýza rizik v souladu se stanovenými bezpečnostními požadavky a na základě výsledků této analýzy bude vypracován „Návrh bezpečnosti informačního systému“, bezpečnostní směrnice pro jednotlivé role definované v informačním systému a případně další specifikované dokumenty.

3. Dokument „Analýza rizik informačního systému“

Dokument „Analýza rizik informačního systému“ je druhým dokumentem v rámci projektové bezpečnostní dokumentace. Analýza rizik vychází z dokumentu „Bezpečnostní politika informačního systému“ a snaží se nalézt možné hrozby a zranitelnosti působící na hodnocený informační systém a následně stanovit relevantní protiopatření pro zajištění přiměřené ochrany tak, aby byla tato protiopatření dostatečně účinná a současně finančně a organizačně přiměřená povaze chráněné věci.

Analýzu rizik je možno provádět různými metodami viz ČSN ISO/IEC 27005 „Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací“.

Pro informační systémy malého rozsahu Úřad na základě normy ČSN ISO/IEC 27005 vypracoval zjednodušenou metodiku hodnocení rizik, kterou poskytuje na základě písemného vyžádání žadatelům o certifikaci nebo opakovanou certifikaci informačního systému. Zjednodušená analýza rizik jer určena pro malé informační systémy (samostatná pracovní stanice) určené pro nakládání s utajovanými informacemi nejvýše do stupně utajení Vyhrazené.

Při provádění analýzy rizik u informačních systémů určených k nakládání s utajovanými informacemi je nutno brát v úvahu jistá specifika těchto systémů:

- maximální důraz na dodržování legislativních opatření určených právními předpisy z oblasti ochrany utajovaných informací,
- nemožnost stanovení konkrétní finanční hodnoty nejdůležitějšího aktiva – utajované informace.

3.1. Základní analýza rizik

Pro informační systémy malého rozsahu lze obecně konstatovat, že pokud jsou dodržena veškerá legislativní opatření a doporučení Úřadu, pak lze předpokládat, že míry veškerých rizik jsou pod hodnotou akceptovatelné meze a informační systém lze pokládat za bezpečný pro nakládání s utajovanou informací.

V takovémto případě postačuje, aby dokument „Analýza rizik informačního systému“ obsahoval pouze seznam identifikovaných aktiv a aplikovaných protiopatření.

3.1.1. Protiopatření v oblasti personální bezpečnosti a organizačních opatřeních

- Uživatelé informačního systému musí splňovat podmínky pro přístup k utajované informaci v souladu s § 6 nebo § 11 zákona č. 412/2005 Sb. a musí být pro práci v informačním systému prokazatelně pověřeni odpovědnou osobou provozovatele informačního systému nebo jí pověřenou osobou.
- Uživatelé, bezpečnostní správci a správci informačního systému musí splňovat podmínky pro přístup k utajované informaci stupně utajení, stanoveným v souladu s bezpečnostním provozním módem a v závislosti na nejvyšším stupni utajení utajovaných informací se kterými může informační systém nakládat (§ 16 vyhlášky č. 523/2005 Sb.).
- Je-li provozovatelem informačního systému podnikatel, pak musí splňovat podmínky § 15 zákona č. 412/2005 Sb.
- Pro informační systém se zavádí systém bezpečnostní správy s rolí bezpečnostního správce (§ 18 vyhlášky č. 523/2005 Sb.).
- Bezpečnostní správce povede seznam autorizovaných uživatelů informačního systému (§ 19 odst. 1 vyhlášky č. 523/2005 Sb.).
- Provozovatel informačního systému bude zajišťovat úvodní školení uživatelů, bezpečnostních správců a správců v dodržování opatření stanovených v bezpečnostní dokumentaci a správném užívání informačního systému. Další školení bude provozovatelem zajišťováno okamžitě při

podstatných změnách v informačním systému a jinak nejméně jedenkrát ročně (§ 19 odst. 2 vyhlášky č. 523/2005 Sb.).

- V bezpečnostní dokumentaci informačního systému budou pro řešení krizových situací stanovena opatření zaměřená na jeho uvedení do stavu odpovídající bezpečnostní dokumentaci. V bezpečnostní dokumentaci budou uvedeny základní typy krizových situací spolu se specifikovanými činnostmi zaměřenými na minimalizaci škod, likvidaci následků a zajištění informací potřebných pro zjištění příčin a mechanizmu vzniku (§ 23 odst. 10 vyhlášky č. 523/2005 Sb.).
- Servisní činnost v informačním systému bude organizována tak, aby nebyla ohrožena jeho bezpečnost. Údržbu komponent informačního systému zajišťující bezpečnostní funkce nebo přímo ovlivňující jeho bezpečnost musí zajišťovat osoby splňující podmínky zákona pro přístup k utajovaným informacím nejvyššího stupně utajení, pro jehož nakládání je informační systém určen (§ 23 odst. 6 a7 vyhlášky č. 523/2005 Sb.).
- V informačním systému bude používáno pouze SW a HW vybavení odpovídající bezpečnostní dokumentaci schválené Úřadem a podmínkám certifikační zprávy k certifikátu informačního systému (§ 23 odst. 4 vyhlášky č. 523/2005 Sb.).
- Pro informační systém bude existovat bezpečnostní dokumentace schválená Úřadem §4 vyhlášky č. 523/2005 Sb.).
- Bezpečnost informačního systému bude průběžně, s ohledem na jeho skutečný stav, prověřována a vyhodnocována (§ 23 odst. 1 vyhlášky č. 523/2005 Sb.).

3.1.2. Protiopatření v oblasti fyzické bezpečnosti

- Utajovaná informace bude zpracovávána v souladu s §24 odst. 5 zákona č. 412/2005 Sb., v zabezpečené oblasti příslušné kategorie nebo vyšší, nebo v objektu příslušné kategorie nebo vyšší.
- Utajovaná informace bude ukládána v úschovném objektu v zabezpečené oblasti příslušné kategorie nebo vyšší (§24 odst. 6 zákona č. 412/2005 Sb.).
- Opatření fyzické bezpečnosti stanoví odpovědná osoba nebo jí pověřená osoba v projektu fyzické bezpečnosti (§31 odst. 3 zákona č. 412/2005 Sb.).
- Orgán státu, právnická osoba a podnikající fyzická osoba budou zajišťovat a pravidelně ověřovat, zda použitá opatření fyzické bezpečnosti odpovídají projektu fyzické bezpečnosti a právním předpisům v oblasti ochrany utajovaných informací (§31 odst. 5 zákona č. 412/2005 Sb.).
- Aktiva informačního systému budou umístěna do prostoru, ve kterém je zajištěna fyzická ochrana informačního systému před neoprávněným přístupem, poškozením a ovlivněním (§20 odst. 1 vyhlášky č. 523/2005 Sb.).
- Umístění aktiv informačního systému bude provedeno tak, aby zamezovalo nepovolané osobě odezírat utajované informace nebo informace sloužící k identifikaci a autentizaci uživatele (§20 odst. 3 vyhlášky č. 523/2005 Sb.).
- Aktiva informačního systému budou opatřena ochrannými prvky, tak aby je bylo možné otevřít, pouze při současném zničení těchto prvků (§ 20 odst. 2 vyhlášky č. 523/2005 Sb.).

3.1.3. Protiopatření v oblasti počítačové bezpečnosti

- Operační systémy budou nastaveny v souladu s doporučeními Úřadu.
- Každý SW bude před nasazením do informačního systému testován v provozním prostředí s ohledem na požadovanou funkcionalitu a testování bude zadokumentováno.
- Řízení vstupně výstupních portů bude prováděno v souladu s doporučeními Úřadu.

- Ochrana před škodlivým kódem bude prováděna v souladu s doporučeními Úřadu.

3.1.4. Protiopatření v oblasti komunikační bezpečnosti

- Komunikační bezpečnost bude nastavena v souladu s doporučeními Úřadu.
- Ochrana pasivních prvků síťové infrastruktury bude prováděna v souladu s doporučeními Úřadu.
- Ochrana aktivních prvků síťové infrastruktury bude prováděna v souladu s doporučeními Úřadu.

3.1.5. Protiopatření v oblasti administrativní bezpečnosti

- Všechny nosiče utajovaných informací používané při provozu v informačním systému budou evidované a označené (§ 15 odst. 1 a 2 vyhlášky č. 523/2005 Sb.).
- Všechny nosiče utajovaných informací používané pro předávání utajovaných informací jiným subjektům (orgán státu, právnická osoba nebo podnikající fyzická osoba) budou evidované a označené (vyhláška č. 529/2005 Sb.).
- Ničení nosiče utajovaných informací bude provedeno tak, aby se znemožnilo utajovanou informaci z něho opětovně získat (§15 odst. 7 vyhlášky č. 523/2005 Sb.).

3.1.6. Protiopatření v oblasti kompromitujícího vyzařování

- Použitá HW zařízení v informačním systému budou splňovat požadavky na elektrickou bezpečnost a elektromagnetickou kompatibilitu (EMC) podle zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.
- Umístění aktiv informačního systému bude provedeno tak, aby zamezovalo nepovolané osobě odezírat utajované informace nebo informace sloužící k identifikaci a autentizaci uživatele (§20 odst. 3 vyhlášky č. 523/2005 Sb.).
- Použitá HW zařízení v informačním systému budou splňovat požadavky standardu NBÚ-2/2007, verze 2 z roku 2011, Instalace zařízení z hlediska kompromitujícího elektromagnetického vyzařování.

3.2. Doplňková analýza rizik

Pokud nelze splnit některá protiopatření definovaná v předešlých kapitolách, pak je nutné tuto skutečnosti zohlednit a odůvodnit v doplňkové analýze rizik.

Doplňková analýza rizik musí obsahovat:

- stanovení hrozeb a zranitelností na něž neaplikované protiopatření mělo působit,
- stanovení nových náhradních protiopatření,
- ohodnocení vlivu nových protiopatření na hrozby a zranitelnosti a
- odůvodnění dostatečnosti navrhovaných protiopatření.

4. Dokument „Návrh bezpečnosti informačního systému“

Dokument „Návrh bezpečnosti informačního systému“ je stěžejním dokumentem projektové bezpečnostní dokumentace informačního systému.

Návrh bezpečnosti detailně rozpracovává aplikaci protiopatření stanovených v dokumentu „Analýza rizik informačního systému“ pro splnění požadavků definovaných v dokumentu „Bezpečnostní politika informačního systému“.

Dokument „Návrh bezpečnosti informačního systému“ musí splňovat následující požadavky:

- obsahuje konkrétní informace (typ HW nebo SW, umístění, nastavení parametrů apod.),
- je maximálně přesný,
- je autorizován oprávněnou osobou organizace.

4.1. Struktura dokumentu „Návrh bezpečnosti informačního systému“

1. Úvodní ustanovení
    1.1. Popis informačního systému
    1.2. HW konfigurace informačního systému
    1.3. SW konfigurace informačního systému
2. Personální bezpečnost
3. Počítačová bezpečnost
    3.1. Jednoznačná identifikace a autentizace
    3.2. Volitelné řízení přístupu
    3.3. Auditní záznamy
    3.4. Opakované použití objektů
    3.5. Ochrana před škodlivým kódem
    3.6. Instalace, používání a bezpečnostní nastavení SW
    3.7. Komunikační bezpečnost
    3.8. Kompromitující vyzařování
    3.9. Servisní činnost
    3.10. Požadavky na dostupnost
4. Kryptografická ochrana
5. Fyzická bezpečnost
6. Administrativní bezpečnost
7. Řízení a plánování kontinuity

4.2. Kapitola „1. Úvodní ustanovení“

Kapitola detailně rozpracovává základní popis informačního systému uvedený v dokumentu „Bezpečnostní politika“.

4.2.1. Kapitola „1.1. Popis informačního systému“

- úplný a přesný popis informačního systému doplněný schématem,
- přesnou dislokaci informačního systému,

- nejvyšší stupeň utajení zpracovávaných informací,
- v případě zpracovávání informací cizí moci i nejvyšší stupeň utajení informací cizí moci,
- zvolený bezpečnostní provozní mód,
- předpokládaný počet uživatelů,
- předpokládaný rozsah zpracování utajovaných informací (časové vyjádření),
- vztah k jiným počítačovým sítím (u samostatných osobních počítačů např. vyjmutí síťové karty, zákaz použití modemu, u LAN zpravidla izolace od jiných počítačových sítí),
- v případě záměru použití kryptografických prostředků uvést účel a typ.

4.2.2. Kapitola „1.2. HW konfigurace informačního systému“

Úplný a přesný seznam HW komponent včetně sériových čísel.

Informační systém samostatných počítačů (1 a více):

- typ PC s bližšími údaji o jeho komponentách včetně HDD,
- typ monitoru včetně typu připojení k PC (VGA, DVI apod.),
- human interface (klávesnice, myš) včetně typu připojení (PS2, USB apod.),
- HW kryptografické prostředky,
- periferní zařízení (např. zálohování, UPS).

Informační systém typu LAN:

- servery – typ a bližší údaje o jejich komponentách,
- pracovní stanice – typ a bližší údaje o jejich komponentách včetně lokálních periferních zařízeních (např. tiskárny, UPS),
- HW kryptografické prostředky,
- síťové periferní zařízení (např. síťové tiskárny, disková pole, zálohovací zařízení, centrální UPS),
- pasivní prvky síťové infrastruktury (datové rozvody) – typ, způsob vedení apod.,
- aktivní prvky síťové infrastruktury (např. router, switch).

4.2.3. Kapitola „1.3. SW konfigurace informačního systému“

Úplný a přesný seznam SW komponent včetně označení jejich verzí.

Mezi SW komponenty patří zejména:

- operační systémy,
- aplikační SW (komerční i speciální),
- antivirové programy,
- SW kryptografické prostředky,
- zálohovací utility,
- administrátorské utility.

4.3. Kapitola „2. Personální bezpečnost“

- definice rolí působících v informačním systému (podle bezpečnostní politiky),
- seznam konkrétních požadavků na osoby v jednotlivých rolích informačního systému:
    - splnění podmínek přístupu fyzické osoby k utajované informaci konkrétního stupně utajení (případně i utajované informaci cizí moci),

    - pověření do role v informačním systému (kdo a jak),
    - proškolení ze znalostí provozních bezpečnostních směrnic (kdo a jak),
    - další konkrétní požadavky podle potřeb organizace (např. odborná způsobilost).
- popis způsobu pověřování osob vyžadovaných bezpečnostní politikou pro správu informačního systému (bezpečnostního správce, správce, případně jejich zástupci aj.)
    - odkaz na přílohu, v níž jsou uvedeny osoby, aktuálně jmenované do těchto funkcí, s čísly jejich Osvědčení od NBÚ pro přístup k odpovídajícímu stupni utajení, případně s údaji o Oznámení
    - vzory formulářů pro jmenování uvedených osob
    - zajištění zástupnosti,
    - případné sloučení rolí,
- popis postupu pro zařazení/vyřazení uživatele do/z informačního systému (kdo o tom rozhodne, kdo informuje bezpečnostního správce o zrušení oprávnění pro přístup do informačního systému před odchodem dané osoby z organizace, zánikem jejího Osvědčení nebo Oznámení, způsob sdělování této informace bezpečnostnímu správci, vzor formuláře se schválením zařazení/vyřazení uživatele do/z informačního systému),
- určení povinnosti vedení seznamu uživatelů bezpečnostním správcem informačního systému včetně vzoru seznamu uživatelů.

4.4. Kapitola „3. Počítačová bezpečnost“

Uvést pro nasazené operační systémy původ použitého bezpečnostního nastavení (dodané Úřadem, vlastní návrh, dodané třetí stranou apod.).

Bezpečnostní nastavení operačního systému může být obsaženo v jednotlivých podkapitolách kapitoly „Počítačová bezpečnost“, nebo je možné shrnout veškerá nastavení bezpečnostních parametrů do samostatného dokumentu a v dokumentu „Návrhu bezpečnosti informačního systému„ se na něj pouze odkazovat.

4.4.1. Kapitola „3.1. Jednoznačná identifikace a autentizace“

- popis nastavení bezpečnostních parametrů operačního systému,
- popis případných použitých speciálních prostředků pro identifikaci a autentizaci včetně konkrétních údajů a nastavení (smart card, biometrické zařízení, apod.),
- pokud je používána identifikace a autentizace na aplikační úrovni, tak popsat a specifikovat potřebné nastavení,
- definice povinnosti uzamčením pracovní stanice nebo samostatného osobního počítače při krátkodobém opuštění zapnutého počítače a umožněním opětovné práce v systému až po úspěšné identifikaci a autentizaci uživatele,
- definice povinnosti bezpečného ukládání hesel pro speciální účty ve stanoveném úschovném objektu (vestavěné účty administrátorů, účty důležitých služeb, BIOS apod.).

4.4.2. Kapitola „3.2. Volitelné řízení přístupu“

- popis nastavení bezpečnostních parametrů operačního systému,
- pokud je používáno na aplikační úrovni, popsat a specifikovat potřebné nastavení,
- popis řízení přístupu k vstupně výstupním portům zejména k USB (zablokování přístupu všech uživatelů, umožnění přístupu pro konkrétní média konkrétním uživatelům apod.), uvést použité prostředky a příslušná nastavení,

- popis logické struktury pevných disků, pravidla pro řízení přístupu uživatelů k datové části pevného disku,
- matice přístupových práv pro uživatele.

4.4.3. Kapitola „3.3. Auditní záznamy“

- popis nastavení bezpečnostních parametrů operačního systému,
- definice povinnosti bezpečnostního správce:
    - zkoumat pravidelně auditní záznamy,
    - archivovat pravidelně auditní záznamy (kdy, jak a na jak dlouho),
- pokud je používáno vytváření auditních záznamů na aplikační úrovni, popsat a specifikovat potřebné nastavení (např. speciální SW pro řízení přístupu k USB),
- definovat omezení přístupu uživatelů k auditním záznamům,
- uvést a popsat používané nástroje pro analýzu auditních záznamů.

4.4.4. Kapitola „3.4. Opakované použití objektů“

- popis nastavení bezpečnostních parametrů operačního systému,
- v případě používání speciálních prostředků, např. utilit pro bezpečné vymazávání informací z pevných disků, popsat a specifikovat potřebné nastavení,
- definovat možnosti a způsob případné deklasifikace nosičů informací,
- definovat způsob zacházení s HW komponentami informačního systému, které obsahují nosiče informací (paměti typu RAM, HDD apod.), odpojování od napájecího napětí, vyjímání nosičů apod.

4.4.5. Kapitola „3.5. Ochrana před škodlivým kódem“

- uvést typ antivirového prostředku,
- definovat kdo bude zajišťovat jeho aktualizaci,
- definovat jak často bude prováděna jeho aktualizace.

4.4.6. Kapitola „3.6. Instalace, používání a bezpečnostní nastavení SW“

- uvést způsob zajištění správy konfigurace a vedení seznamu SW bezpečnostním správcem, včetně údaje o, případně používaném SW nástroji,
- uvést způsob zajištění údržby SW (aplikace opravných programových balíčků a aktualizací vydávaných výrobci SW).

4.4.7. Kapitola „3.7. Komunikační bezpečnost“ (pouze pro LAN)

Uvést kompletní údaje o LAN:

- typ kabeláže a použité standardy,
- síťové protokoly a pro ně potřebná konfigurace (např. MAC adresy, IP adresy a masky podsítí pro IP protokol),
- topografie LAN (fyzické umístění jednotlivých zařízení - servery, pracovní stanice, aktivní prvky sítě, kryptografické prostředky, kabely),

- topologie LAN (např. sběrnicová, hvězdicová, kruhová, fyzická segmentace na jednotlivých vrstvách OSI modelu a skutečná konfigurace síťových komponent, případně logická segmentace na bázi VLAN a konfigurační soubory), aj.

4.4.8. Kapitola „3.8. Kompromitující vyzařování“

- definovat povinnost používat pouze HW zařízení, která splňují požadavky na elektrickou bezpečnost a elektromagnetickou kompatibilitu (EMC) podle zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů,
- definovat povinnost umístění aktiv informačního systému tak, aby se zamezilo nepovolané osobě odezírat utajované informace nebo informace sloužící k identifikaci a autentizaci uživatele (§20 odst. 3 vyhlášky č. 523/2005 Sb.).
- pro informační systém nakládající s utajovanou informací stupně utajení Důvěrné a vyšší definovat povinnost splnit požadavky standardu NBÚ-2/2007, verze 2 z roku 2011, Instalace zařízení z hlediska kompromitujícího elektromagnetického vyzařování,
- definovat povinnost pracovníků správy systému v oblasti kontroly a dodržování stanovených pravidel.

4.4.9. Kapitola „3.9. Servisní činnost“

- definovat povinnost pracovníků správy systému při provádění nebo zajišťování servisní činnost (kdo, jak a kde může servis provádět),
- definovat podmínky pro náhradní HW komponenty používané při servisu v návaznosti na problematiku kompromitujícího vyzařování,
- definovat podmínky provádění servisu s ohledem na ochranu utajovaných informací (vyjímaní nosičů informací apod.),
- definovat povinnost používat v informačním systému pouze SW a HW vybavení odpovídající bezpečnostní dokumentaci schválené Úřadem a podmínkám certifikační zprávy k certifikátu informačního systému (§ 23 odst. 4 vyhlášky č. 523/2005 Sb.),

4.4.10. Kapitola „3.10. Požadavky na dostupnost“

- uvést požadavky na dostupnost definované v bezpečnostní politice,
- definovat systém zálohování SW i HW prostředků pro zajištění definované dostupnosti,
- definovat a popsat minimální funkčnost systému, která musí být zajištěna,
- definovat a popsat způsob obnovy systému,
- definovat odpovědnosti za zálohování a obnovu systému.

4.5. Kapitola „4. Kryptografická ochrana“

- Uvést jaký kryptografický prostředek bude v informačním systému používán, přesný typ a počty prostředků, jak bude zajišťován klíčový materiál, kde bude umístěn a jak bude zajištěna jeho fyzická bezpečnost, vyškolený personál požadovaný pro jeho provoz, jaké dokumenty pro jeho provoz budou vytvořeny apod.

4.6. Kapitola „5. Fyzická bezpečnost“

- popsat zabezpečení všech prostor, v nichž budou umístěny komponenty informačního systému:
    - identifikace místnosti, které komponenty v ní jsou a aplikovaná opatření fyzické bezpečnosti včetně režimových opatření, pro podrobnější popis je možno provést odkaz na příslušný bezpečnostní projekt nebo směrnici,
    - zvlášť opatření pro servery a pro pracovní stanice,
    - rozmístění jednotlivých zařízení v místnosti, se zohledněním instalačních požadavků (např. formou grafického znázornění).
- definovat povinnost pracovníků správy systému v oblasti kontroly a vedení přehledu umístění všech zařízení a jejich rozmístění v stanovených prostorech,
- popsat, jak bude vedena evidence spjatá se vstupem uživatelů, pokud je vyžadována bezpečnostní politikou, evidenční pomůcky, procedury,
- popsat, jak bude vedena evidence spjatá se vstupem návštěv, pokud jsou povoleny v bezpečnostní politice,
- uvést umístění úschovných objektů pro ukládání výměnných nosičů informací a řešení řízení fyzického přístupu k těmto nosičům,
- definovat způsob použití a typ ochranných prvků pro pečetění krytů HW komponent,
- definovat povinnost pracovníků správy systému a uživatelů v oblasti kontroly ochranných prvků,
- definovat způsob evidence a označováno HW komponent,
- definovat povinnost pracovníků správy systému v oblasti vedení seznamu HW komponent.

4.7. Kapitola „6. Administrativní bezpečnost“

- definovat povinnost dodržovat požadavky vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů,
- definovat povinnost používání pouze evidovaných a označených nosičů informací přičemž:
    - nosiče používané v provozu systému se evidují a označují podle § 15 vyhlášky č. 523/2005 Sb.,
    - nosiče pro předávání informací jiným subjektům se evidují a označují podle vyhlášky č. 529/2005 Sb.,
    - pro evidence a označení nosičů pro neutajované informace se přiměřeně použije § 15 vyhlášky č. 523/2005 Sb.,
- definovat možnosti a způsob ničení nosičů informací (komisionální ničení s učiněním záznamu o zničení, soulad se skartačním řádem organizace, prostředky fyzického ničení a soulad s aktuálními standardy NBÚ, postup pro pevné disky apod.),
- definovat všechny evidence a formuláře vedené v informačním systému, kdo je vede, kdo je autorizuje, kde jsou ukládány během používání, kde a jak dlouho jsou uchovávány, jejich vzory, jejich stupeň utajení, obvykle:
    - seznam uživatelů,
    - evidence školení uživatelů,
    - evidence provozních nosičů informací,
    - u vyjímatelných HDD evidence výdeje/příjmu HDD z úschovného objektu,
    - seznam HW (pokud není uveden v návrhu bezpečnosti),
    - seznam SW (pokud není uveden v návrhu bezpečnosti),

    - provozní deník systému (záznamy o opravách a údržbě, o provedení zálohy, o provedení updatu antivirového programu, o kontrole auditních záznamů a jejich zálohování, o krizových situacích a bezpečnostních incidentech, o dalších bezpečnostně relevantních událostech, charakteru administrativní pomůcky, s uvedením data, času, zúčastněných osob a jejich podpisů),
    - případně další administrativní pomůcky.
- definovat další návaznou bezpečnostní dokumentaci pro informační systém, kdo jí vede, kdo jí autorizuje, její klasifikaci, obvykle:
    - bezpečnostní směrnice pro jednotlivé role,
    - testy bezpečnosti,
    - případně další dokumentace.

4.8. Kapitola „7. Řízení a plánování kontinuity“

- definovat typy a modelové způsoby řešení možných krizových situací,
- definovat typy a modelové způsoby řešení bezpečnostních incidentů,
- definovat typy a modelové způsoby řešení možné kompromitace (v případě použití kryptografické ochrany),
- definovat povinnost pracovníků správy systému při řízení změn v provozovaném a certifikovaném informačním systému (jak změny provádět a jaké změny hlásit Úřadu),
- definovat povinnost pracovníků správy systému při provádění testů bezpečnosti (způsob provádění a vyhodnocování testů).

5. Dokumenty „Bezpečnostní směrnice informačního systému“

Pro zajištění bezpečnosti během provozu informačního systému je vyhláškou č. 523/2005 Sb., vyžadováno oddělené zpracování bezpečnostních směrnic pro bezpečnostního správce informačního systému, správce informačního systému a pro jednotlivé typy uživatelů informačního systému. Obecně se i v malém informačním systému specifikuje role správce informačního systému, v odůvodněných případech je slučována s rolí bezpečnostního správce informačního systému. Provozní bezpečnostní směrnice musí konkretizovat povinnosti osob při manipulaci s informacemi a informačním systémem v ochraně utajovaných informací.

V dalším textu jsou uvedeny obvyklé povinnosti uživatelů a bezpečnostních správců/správců informačního systému malých informačních systémů. Tyto seznamy nepředstavují univerzální a úplný seznam povinností uživatelů a bezpečnostních správců/správců informačních systémů a je třeba k nim přistupovat z hlediska požadavků konkrétního informačního systému. Jednotlivé body vyžadují konkretizaci a rozvedení do potřebných podrobností. Rozdělení povinností mezi správce informačního systému a bezpečnostního správce informačního systému je možno modifikovat, s ohledem na úroveň bezpečnostního prověření správce informačního systému a předpokládané technické znalosti bezpečnostního správce informačního systému.

Pokud je v informačním systému zavedena další role související se zabezpečením informačního systému, je nutno navíc specifikovat povinnosti a procedury s ní spjaté.

Dokumenty „Bezpečnostní směrnice *název role*“ musí být autorizovány oprávněnou osobou organizace.

5.1. Struktura bezpečnostních směrnic

Dokument „Bezpečnostní směrnice *název role*“ musí obsahovat minimálně kapitoly, které popisují:

- povinností dané role,
- práva dané role,
- procedury spojené s povinnostmi a právy dané role.

Dokument „Bezpečnostní směrnice uživatele“ musí navíc obsahovat kapitoly popisující:

- stručný a zjednodušený popis informačního systému včetně jeho rozsahu a umístění,
- definici a rozdělení krizových situací včetně základního popisu toho, jak se uživatel podílí na řešení,
- definici a rozdělení bezpečnostních incidentů včetně základního popisu toho, jak se uživatel podílí na řešení,
- definici kompromitace včetně základního popisu toho, jak se uživatel podílí na řešení (pouze při použití kryptografického prostředku).

V bezpečnostní směrnici bezpečnostního správce/správce informačního systému je možno specifikovat jeho povinnosti a procedury s nimi spojené odkazem na dokument „Návrh bezpečnosti informačního systému“ (pokud jsou v něm řešeny).

V bezpečnostní směrnici uživatele je nutno je nutno uvádět úplnou a přesnou specifikaci jeho povinností a procedur s nimi spojených, neboť uživatel obvykle nemá k jiným dokumentům bezpečnostní dokumentace přístup.

5.2. Typické povinnosti bezpečnostního správce

- udržuje aktuální seznam oprávněných uživatelů,
- zajišťuje, aby fyzický přístup do prostor s HW komponentami informačního systému, k vyjímatelným pevným diskům apod. mohli získat jen oprávnění uživatelé,

- přiděluje uživateli uživatelské jméno a prvotní heslo, vytváří uživatelské účty a spravuje je ve shodě s bezpečnostní dokumentací, v případě potřeby mu v této činnosti poskytuje technickou podporu správce,
- ručí za trvalé dodržování schválené konfigurace HW i SW informačního systému, včetně nastavení bezpečnostních charakteristik operačního systému a aplikačního SW,
- ručí za dodržování umístění informačního systému a instalačních požadavků,
- ve shodě s bezpečnostní dokumentací zkoumá pravidelně auditní záznamy a vytváří jejich archivní kopie takovým způsobem, aby bylo umožněno jejich zpětné zkoumání, obvykle 3 roky nazpět,
- zajišťuje ochranu záložních kopií auditních záznamů před modifikací nebo zničením,
- zkoumá auditní záznamy po bezpečnostním incidentu,
- zkoumá a řeší bezpečnostní incidenty, hlásí je řediteli organizace (nebo jinému příslušnému funkcionáři),
- zajišťuje školení uživatelů v oblasti bezpečnosti informačního systému,
- kontroluje dodržování bezpečnostních směrnic,
- zajišťuje v předepsaném rozsahu bezpečnost nosičů informací, zejména jejich vyřazování a ničení,
- vede potřebné evidence (podle bezpečnostní dokumentace, uvést seznam evidencí),
- provádí správu dokumentace bezpečnosti informačního systému (kde je uložena apod.),
- vydává uživatelům výměnné pevné disky, přenosný počítač (popsat jak, pokud je ovšem tento postup použit),
- zajišťuje dodržování povinnosti při ochraně utajovaných informací v případě servisu,
- spolupracuje se správcem při uvedení informačního systému do stavu odpovídajícího schválené bezpečnostní dokumentaci informačního systému po ostatních bezpečnostních incidentech nebo mimořádných událostech,
- hraje klíčovou úlohu při řešení základních krizových situací,
- je-li oblastí působnosti bezpečnostního správce LAN, musí být veškeré povinnosti rozšířeny do síťového prostředí, musí být zahrnuta kontrola neporušenosti kabeláže, aktivních prvků sítě, konfigurace VLAN apod.

5.3. Typické povinnosti správce

- provádí činnost administrátora operačního systému (správce sítě LAN), stanoveným způsobem zabezpečuje denní provoz informační systém po technické stránce,
- instaluje operační systém, aplikační SW, zajišťuje aktualizaci antivirového SW,
- provádí zálohování systémového programového vybavení, zajišťuje ochranu záložních dat (konkretizovat systém zálohování, kde jsou zálohy ukládány apod.),
- spolupracuje s bezpečnostním správcem informačního systému při nastavení bezpečnostních charakteristik operačního systému a aplikačního SW podle schválené bezpečnostní dokumentace informačního systému,
- spravuje uživatelské účty ve spolupráci s bezpečnostním správcem informačního systému,
- spolupracuje s bezpečnostním správcem informačního systému při vyčištění a zotavení systému po napadení viry,
- spolupracuje s bezpečnostním správcem při uvedení informačního systému do stavu odpovídajícího schválené bezpečnostní dokumentaci informačního systému po ostatních bezpečnostních incidentech nebo mimořádných událostech.

5.4. Typické povinnosti uživatele

Bezpečnostní směrnice pro uživatele vyžaduje přehledné a srozumitelné zpracování. Nesmí obsahovat údaje, které uživatel nepotřebuje znát a které by mu umožnily zneužití informačního systému. Zejména je třeba, aby byl uživatel informován:

- o účelu informačního systému,
- kde smí pracovat s utajovanými informacemi, případně v jakém časovém rozpětí během dne,
- jaké je standardní zahájení práce v informačním systému (přístup, přihlašovací procedura a postup identifikace a autentizace uživatele, jaká jsou omezení v počtu chybných přihlášení, délce hesla a době jeho platnosti, délce PINu čipové karty apod.),
- jakou kontrolu HW (případně kabeláže), prostředí nebo podle okolností i jiných prvků informačního systému má provést před započetím práce,
- jak má zacházet s vyjímatelnými pevnými disky a dalšími nosiči informací používanými v daném informačním systému,
- do jakého úschovného objektu má ukládat klasifikované nosiče informací nebo od koho je před započetím práce v informačním systému získá a komu je po skončení práce vrací k uložení,
- jakým způsobem získá vyjímatelný pevný disk nebo přenosný počítač nebo jiný HW systému před započetím práce, jakým způsobem ho opět vrací, s tím spjaté povinnosti a evidence,
- v jaké oblasti pevného disku může/má ukládat uživatelské soubory, případně že je na lokální pevný disk ukládat nesmí/nemůže apod.,
- jak musí/může zálohovat uživatelská data a na jaký nosič informací, jak musí chránit záložní nosiče informací,
- jak se chovat k návštěvě, jak k pracovníkům úklidu (aby to vyhovovalo bezpečnostní dokumentaci),
- o své povinnosti dodržovat schválenou konfiguraci HW a SW,
- o své povinnosti hlásit poruchy HW i SW, výskyt bezpečnostního incidentu nebo podezření na možnost kompromitace utajovaných informací bezpečnostnímu správci,
- o tom, jaké základní bezpečnostní incidenty se mohou vyskytnout a jak má bezprostředně reagovat, pokud to typ události vyžaduje, před kontaktem s bezpečnostním správcem,
- o zavedené ochraně vstupně výstupních portů, zejména v souvislosti s používáním USB paměťových zařízení,
- o postupu pro export informací z informačního systému na nosič informací, pokud je uživateli povolen,
- o postupu pro import informací do informačního systému prostřednictvím nosiče informací, pokud je uživateli povolen,
- o povinnosti označit tiskové výstupy stupněm utajení a dalšími náležitostmi podle požadavků administrativní bezpečnosti a zajistit neprodleně jejich zaevidování,
- o postupech při ničení a skartaci nosičů informací a příslušných pravidlech administrativní bezpečnosti,
- o předepsaném postupu při nutnosti opustit počítač v běhu, povolená lhůta,
- o proceduře pro standardní bezpečné ukončení práce v informačním systému - veškeré povinnosti týkající se počítače, periférií, místnosti, klíčů, EZS atd.
- o správném používání hesla, jak ho tvořit, že ho nesmí sdílet, prozradit atd.,
- o ochraně, kterou musí poskytovat magnetické nebo čipové kartě (případně jiným pomůckám) využívané pro identifikaci a autentizaci uživatele v informačním systému,

- o způsobu používání klíčů od místnosti, systému elektrické zabezpečovací signalizace, systému elektronické kontroly vstupu, podle konkrétní situace, je možno řešit i odkazem na příslušný bezpečnostní projekt objektové a technické bezpečnosti,
- o tom, jaké základní mimořádné (krizové) situace mohou nastat a jaké jsou jeho povinnosti při jejich řešení,
- o všech svých dalších povinnostech vyplývajících z bezpečnostní dokumentace informačního systému,
- v potřebné míře o okolnostech umožňujících mu pochopení jeho povinností.