METODIKA CERTIFIKACE

informačního systému určeného pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené

(verze 1.1)

Obsah

Čl. 1

Úvodní ustanovení

(1) Metodika certifikace informačního systému malého rozsahu určeného pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené (dále jen „Metodika certifikace“) je dokument, který stanovuje a sjednocuje postup certifikace informačních systémů malého rozsahu určených pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené.

(2) Metodika certifikace je tvořena souborem pravidel a postupů určující způsob provádění certifikace informačního systému malého rozsahu určeného pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené (dále jen „informační systém“).

Čl. 2

Vymezení pojmů

(1) Pro účely tohoto dokumentu se rozumí:

a) pracovištěm informačního systému jeden samostatný stacionární případně přenosný počítač, jeho programové vybavení, k tomu patřící periferní zařízení nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací, který je umístěn v ohraničeném prostoru a není propojen s jiným informačním případně komunikačním systémem (dále jen „pracoviště“),

b) informačním systémem jedno nebo několik samostatných vzájemně nepropojených pracovišť,

c) žadatelem právnická osoba nebo podnikající fyzická osoba (dále jen „podnikatel“), nebo organizační složka státu, která zažádala o provedení certifikace informačního systému,

d) provozovatelem podnikatel, nebo organizační složka státu, která je držitelem certifikátu informačního systému.

Čl. 3

Předpoklady

(1) Podnikatel, který potřebuje provozovat informační systém musí splňovat podmínky k přístupu k utajované informaci podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon 412/2005 Sb.“).

(2) Podmínky k přístupu k utajované informaci jsou splněny, pokud podnikatel:

a) je držitelem osvědčení podnikatele pro stupeň utajení Důvěrné nebo vyšší pro přístup k utajované informaci, která u něho vzniká, nebo je mu poskytnuta,

b) vydá prohlášení podnikatele podle § 15a zákona č. 412/2005 Sb., pro přístup k utajované informaci stupně utajení Vyhrazené, která u něho vzniká, nebo je mu poskytnuta.

(3) V případě splnění podmínky k přístupu k utajované informaci formou vydání prohlášení podnikatele, podnikatel tímto prohlášením stvrzuje, že má vytvořeny podmínky

pro ochranu utajovaných informací stupně utajení Vyhrazené v oblasti personální, fyzické a administrativní bezpečnosti.

(4) Pro splnění podmínek uvedených v odstavci 3 musí podnikatel vytvořit a vést bezpečnostní dokumentaci podnikatele podle § 68a zákona č. 412/2005 Sb. Navíc k této povinnosti musí podnikatel disponovat dokumentem „Projekt fyzické bezpečnosti“ minimálně v rozsahu tabulky bodového hodnocení zabezpečené oblasti v níž bude informační systém provozován. Tato problematika věcně spadá pod Národní bezpečnostní úřad. Případné informace o tvorbě bezpečnostní dokumentace podnikatele včetně telefonických kontaktů lze nalézt na webových stránkách Národního bezpečnostního úřadu na adrese https://www.nbu.cz/cs/ochrana-utajovanych-informaci-rozcestnik/ pod jednotlivými částmi (personální, průmyslová, fyzická a administrativní bezpečnost).

Čl. 4

Postup certifikace

(1) Certifikace informačního systému je zahájena doručením žádosti o certifikaci na NÚKIB.

(2) Žádost o certifikaci může být podána samostatně nebo spolu s bezpečnostní dokumentací a dalšími vyžadovanými podklady.

(3) Vzor žádosti o certifikaci, typovou bezpečnostní dokumentaci a vzory požadovaných podkladů poskytuje NÚKIB na svém webovém portálu.

(4) Názvy poskytovaných dokumentů začínají číselným údajem, který identifikuje určení dokumentu.

(5) Dokumenty jejichž název začíná označením 0x (kde x je číslo mezi 0 a 9) jsou pomocné nebo informativní dokumenty, které žadateli poskytují informace a návody potřebné pro zvládnutí certifikačního procesu.

(6) Dokumenty jejichž název začíná označením 1x (kde x je číslo mezi 0 a 9) jsou dokumenty, které vyžadují od žadatele pouze minimální úpravy (většinou doplnění podpisové doložky). Tyto dokumenty žadatel uchovává v tištěné podobě a na NÚKIB je poskytuje v elektronické podobě.

(7) Dokumenty jejichž název začíná označením 2x (kde x je číslo mezi 0 a 9) jsou dokumenty, které vyžadují od žadatele výraznější zásahy. Jedná se o dokumenty, které musí žadatel upravit a doplnit do nich aktuálně platné informace. Tyto dokumenty žadatel uchovává v tištěné podobě a na NÚKIB je poskytuje v elektronické podobě.

(8) Dokumenty jejichž název začíná označením 3x (kde x je číslo mezi 0 a 9) jsou dokumenty, které jsou určeny pro provoz informačního systému. Tyto dokumenty vyžadují od žadatele pouze minimální úpravy (většinou doplnění podpisové doložky). Dokumenty „34_Evidence_uzivatelu.docx“, „35_Evidence_nosicu_informaci.docx“, „36_Kniha_manipulace_s_nosici.docx“ a „37_Provozni_denik_pracoviste.docx“ žadatel vytiskne, sešije nebo sváže a nechá prokazatelně schválit (podepsat) odpovědnou osobou uvedenou v podpisové doložce. Tyto dokumenty se až na výjimky uvedené dále nezasílají na NÚKIB.

Čl. 5

Žádost o certifikaci informačního systému

(1) Certifikace informačního systému podle zákona č. 412/2005 Sb., probíhá formou správního řízení.

(2) Příslušným správním úřadem pro certifikaci informačních systémů podle zákona č. 412/2005 Sb., je Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“).

(3) Žadatel o certifikaci informačního systému musí splňovat předpoklady uvedené v článku 3.

(4) Žádost o certifikaci informačního systému podává žadatel nejlépe elektronickou formou prostřednictvím systému datových schránek ISDS.

(5) Náležitosti žádosti o certifikaci informačního systému jsou uvedeny v § 45 vyhlášky č. 479/2024 Sb., o informační bezpečnosti (dále jen „vyhláška č. 479/2024 Sb.“).

(6) Žádost o certifikaci informačního systému musí obsahovat následující údaje:

a) jednoznačnou identifikaci žadatele,

b) kontaktní osobu včetně kontaktu na ni,

c) stručný popis účelu a rozsahu informačního systému,

d) stupeň utajení utajovaných informací, se kterými bude informační systém nakládat,

e) bezpečnostní provozní mód informačního systému a

f) identifikaci případného dodavatele informačního systému.

(7) Jako žádost o certifikaci informačního systému lze využít typový vzor žádosti, který je dostupný na webovém portálu NÚKIB.

(8) Jednoznačnou identifikací žadatele rozumíme:

a) úplný název podnikatele,

b) adresu sídla podnikatele a

c) identifikační číslo podnikatele.

(9) Uvedené údaje musí odpovídat údajům uvedeným v administrativním registru ekonomických subjektů.

(10) Kontaktní osobou včetně kontaktu na ni rozumíme:

a) titul, jméno a příjmení kontaktní osoby,

b) pracovní telefonní spojení na kontaktní osobu a

c) pracovní e-mail kontaktní osoby.

(11) Stručný popis účelu a rozsahu informačního systému může být v případě informačního systému malého rozsahu uveden následovně: „Jedná se o informační systém malého rozsahu, který je vytvářen především z důvodu možnosti účasti na zakázkách v jejichž požadavcích je uvedena podmínka provozování certifikovaného informačního systému pro nakládání s utajovanými informacemi do a včetně stupně utajení Vyhrazené“.

(12) V části stupeň utajení utajovaných informací, se kterými bude informační systém nakládat uveďte „Informační systém bude nakládat se stupněm utajení utajovaných informací Vyhrazené“.

(13) Bezpečnostní provozní mód vychází z §§ 6 a 7 vyhlášky č. 479/2024 Sb. V současné době a vzhledem k rozsahu informačního systému přichází v úvahu bezpečnostní provozní mód „Dedikovaný“ nebo „S nejvyšší úrovní“.

(14) Vzhledem k faktu, že bezpečnostní provozní mód „Dedikovaný“ existuje především z historických důvodů (u starších operačních systémů nebylo možné řídit přístupy k uloženým informacím), tak je jeho použití Úřadem spíše nedoporučováno. Dalším důvodem pro jeho nepoužití je i to, že při použití tohoto bezpečnostního provozního módu musí být provozovatel informačního systému schopen doložit, že všichni pověření uživatelé informačního systému jsou pověření a splňují „need to know“ princip přístupu ke všem zpracovávaným informacím v informačním systému, a to i bez ohledu na to, že je přístup k těmto informacím řízen a nastaven prostředky použitých moderních operačních systémů.

(15) Jako použitý bezpečnostní provozní mód pro informační systémy malého rozsahu proto Úřad doporučuje bezpečnostní provozní mód „S nejvyšší úrovní“.

(16) Identifikace dodavatele je na žádosti o certifikaci informačního systému uváděna pouze v případě, kdy je informační systém budován třetí stranou (dodavatelem).

(17) V případě, kdy informační systém vzniká vlastními silami podnikatele, je v žádosti o certifikaci informačního systému uvedeno „informační systém je budován vlastními silami žadatele“.

(18) Pro podání žádosti o certifikaci informačního systému lze použít vzorovou typovou žádost obsaženou v dokumentu „20_Zadost_Certifikace_V.docx“.

Čl. 6

Bezpečnostní dokumentace

(1) Pro potřeby certifikace informačního systému musí žadatel předložit na NÚKIB příslušnou bezpečnostní dokumentaci.

(2) Pro certifikaci informačních systémů malého rozsahu NÚKIB vytvořil a poskytuje žadatelům vzorovou typovou bezpečnostní dokumentaci, která je obsažena v dokumentu „10_Bezpecnostni_dokumentace_V.docx“.

(3) Dokument „10_Bezpecnostni_dokumentace_V.docx“ obsahuje základní bezpečnostní dokumentaci informačního systému (Bezpečnostní politiku, Analýzu rizik, Návrh bezpečnosti, Bezpečnostní nastavení operačního systému a Bezpečnostní směrnice pro jednotlivé role). Tento dokument vyžaduje od žadatele provedení pouze minimálních úprav, které spočívají v nahrazení údajů na titulní straně dokumentu uvedených červenou kurzívou skutečně platnými údaji. Jedná se o následující údaje:

a) *místo a datum* (např. Praha 12.3.2018),

b) *titul jméno a příjmení* (např. Ing. Petr Novák),

c) *odpovědná osoba/bezpečnostní ředitel* (např. jednatel společnosti, nebo bezpečnostní ředitel).

(4) Tento dokument, po výše uváděných úpravách, žadatel vytiskne, sešije nebo sváže a nechá prokazatelně schválit (podepsat) odpovědnou osobou uvedenou v podpisové doložce.

(5) Vytištěný dokument zůstává uložen u bezpečnostního správce informačního systému a na NÚKIB je odeslána, prostřednictvím systému datových schránek ISDS, jeho elektronická verze.

Čl. 7

Splnění bezpečnostních předpokladů

(1) Žadatel musí NÚKIB prokázat, že splňuje předpoklady z oblasti průmyslové, personální, fyzické a administrativní bezpečnosti.

(2) Žadatel prokazuje splnění těchto předpokladů tím, že vyplní a zašle, prostřednictvím systému datových schránek ISDS, na NÚKIB soubor „21_Splneni_predpokladu_V.docx“.

(3) Vyplnění příslušných údajů v dokumentu probíhá formou nahrazení částí psaných červenou kurzívou skutečnými údaji nebo jejich nahrazení příslušným skenem, fotokopií nebo fotografií.

Čl. 8

Nastavení BIOS/UEFI

(1) Základním nastavením z oblasti informační bezpečnosti je nastavení BIOS/UEFI pracovní stanice nebo notebooku.

(2) Požadavky na natavení BIOS/UEFI spolu s požadavky na informace, které je žadatel povinen dodat na NÚKIB, jsou uvedeny v dokumentu „22_Bezp_nastaveni_BIOS_V.docx“.

(3) Vyplnění příslušných údajů v dokumentu probíhá formou nahrazení částí psaných červenou kurzívou skutečnými údaji nebo jejich nahrazení příslušným snímkem obrazovky.

Čl. 9

Nastavení operačního systému

(1) Nastavení bezpečnostních parametrů operačního systému musí být nastaveny v souladu s doporučením NÚKIB.

(2) Pro snadné a bezchybné zajištění nastavení bezpečnostních atributů poskytuje NÚKIB automatizovaný nástroj pro bezpečnostní nastavení AuTo4SeSe (**Au**tomated **To**ol for **Se**curity **Se**ttings).

(3) Nástroj umožňuje:

a) nastavit bezpečnostní atributy operačního systému,

b) vybrat jednu z nabízených politik hesel (9 znaků – 90 dní / 12 znaků – 720 dní),

c) nastavit možnost používání CD/DVD zařízení,

d) nastavit možnost používání USM Mass Storage zařízení,

e) povolení konkrétního zařízení USM Mass Storage,

f) kontrolu nastavení bezpečnostních atributů operačního systému

(4) Nástroj je distribuován v archivu „skript.7z“ a je chráněn heslem: nukib. Důvodem je fakt, že nástroj je ve formátu „.bat“ a v případě jeho distribuce pomocí emailových serverů, z nichž některé kontrolují obsah archivů, by nebyl doručen.

(5) Archiv „skript.7z“ je nutné rozbalit do předem vytvořené složky „C:\nukib“, neboť z jiného umístění by skript nebyl funkční. Archiv obsahuje dva soubory:

a) „prislo-od-nukib“ – obsahuje pomocné soubory pro běh skriptu,

b) „prave-tlacitko-spustit-jako-spravce.bat“ – příslušný skript (nástroj AuTo4SeSe).

(6) Název skriptu je volen tak, aby přímo napověděl, že je nutné ho spouštět s oprávněním správce (administrátora), tj. pod účtem správce, a ještě zvolit možnost Spustit jako správce.

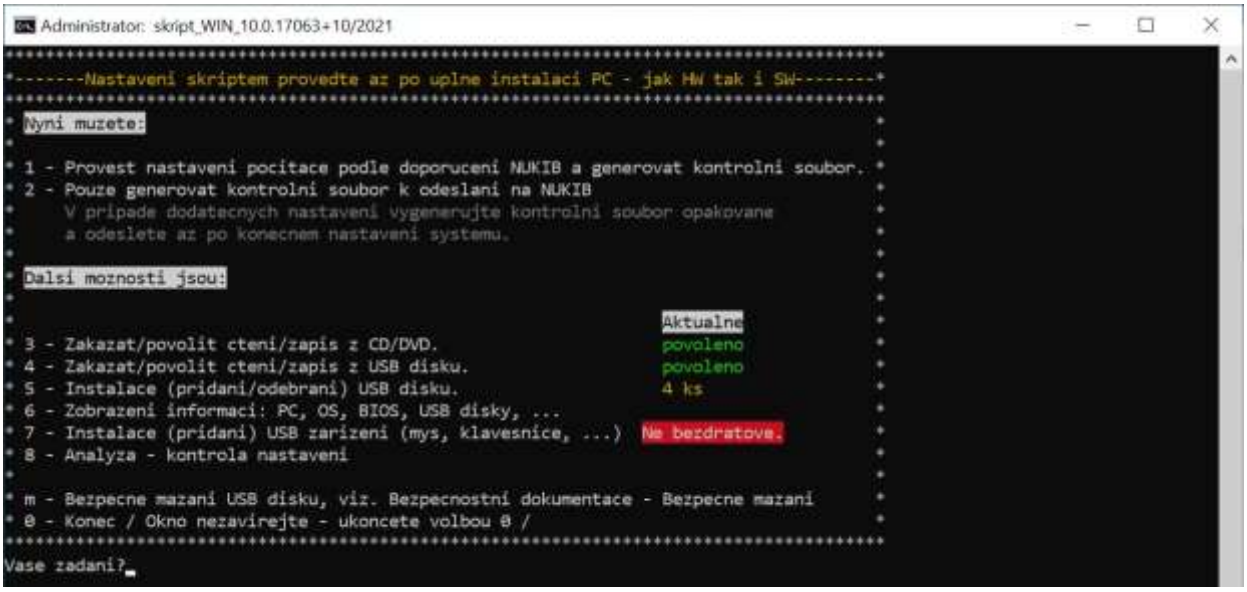
(7) Skript je určen pro nastavení operačního sytému Windows 10 Pro, Enterprise nebo Education (64 bit) 21H1, build 19043. Minimálním předpokladem pro funkci skriptu je build operačního systému 17063. Skriptem je možno nastavovat i operační systém Windows 11 Pro, Enterprise nebo Education (64 bit).

(8) Možnosti skriptu lze rozdělit na tři základní úrovně:

a) Nastavení systému podle doporučení NÚKIB,

b) Dodatečné nastavení – umožňuje úpravu některých vybraných nastavení,

c) Kontrola a generování souboru pro NÚKIB.



(9) Nastavení systému provádějte až po kompletní instalaci systému, HW příslušenství i uživatelského SW.

(10) Nastavení systému se provádí volbou 1. Po zvolení volby 1 následují tyto akce:

a) informace o zálohování nastavení služeb systému,

b) smazání nepotřebných aplikací integrovaných do systému,

c) **dotaz** na volbu politiky hesel (lze volit ze dvou možností),

d) informace o tom, že všichni uživatelé budou muset při dalším přihlášení změnit heslo,

e) **dotaz** na povolení nebo zakázání v systému vestavěného účtu správce (admin_root). Pro malé systémy se sloučenou funkcí provozního a bezpečnostního správce doporučuje NÚKIB tento účet povolit. Při povolení účtu je vygenerováno silné heslo, které si spolu s názvem účtu zapište a uložte v zalepené obálce v úschovném objektu (trezoru). Heslo není utajovanou informací ve smyslu zákona č. 412/2005 Sb., ale musí být chráněno jako utajovaná informace stupně utajení Vyhrazené,

f) **dotaz** na povolení čtení a zápisu z CD/DVD,

g) **dotaz** na povolení čtení a zápisu z USB disku,

h) při povolení zápisu a čtení z USB – **dotaz** na okamžité nebo odložené přidání USB disků do systému. Skript ze systému odebral všechny dříve vložené USB disky a nyní nebo později musíte pomocí skriptu disky opět přidat (nainstalovat). Jinak žádný USB disk nebude funkční. Nyní se předpokládá, že používáte k přenosu skriptu do nastavovaného počítače USB disk, který budete následně využívat, a proto ho do systému můžete přidat,

i) **dotaz** na přidání dalšího USB disku. Držte se pokynů skriptu a přidejte nyní nebo později všechny používané USB disky. Veškeré USB disky, které budou do systému přidány, musí být evidovány. Pro instalace a aktualizace SW a aktualizaci virových definic zaevidujte a používejte výlučně neutajovaný USB disk.

j) informace o generování kontrolního souboru.

(11) Ve složce „C:\nukib“ je vygenerován soubor „odeslat-na-nukib“. Tento soubor odešlete, prostřednictvím emailu na NUKIB. Pokud budete provádět dodatečně některá další nastavení (např. povolovat čtení zápis CD/DVD/USB, přidávat USB disky nebo USB zařízení), tak je nutné před odesláním souboru vygenerovat pomocí volby 2 tento soubor znovu, tak aby obsahoval aktuální verzi nastavení.

(12) Skript umožňuje některé dodatečné nastavení:

a) Volba 3 – umožňuje zakázat/povolit čtení/zápis z CD/DVD. Toto nastavení je trvalé (do další změny) a musí se shodovat s dokumentací k vašemu systému.

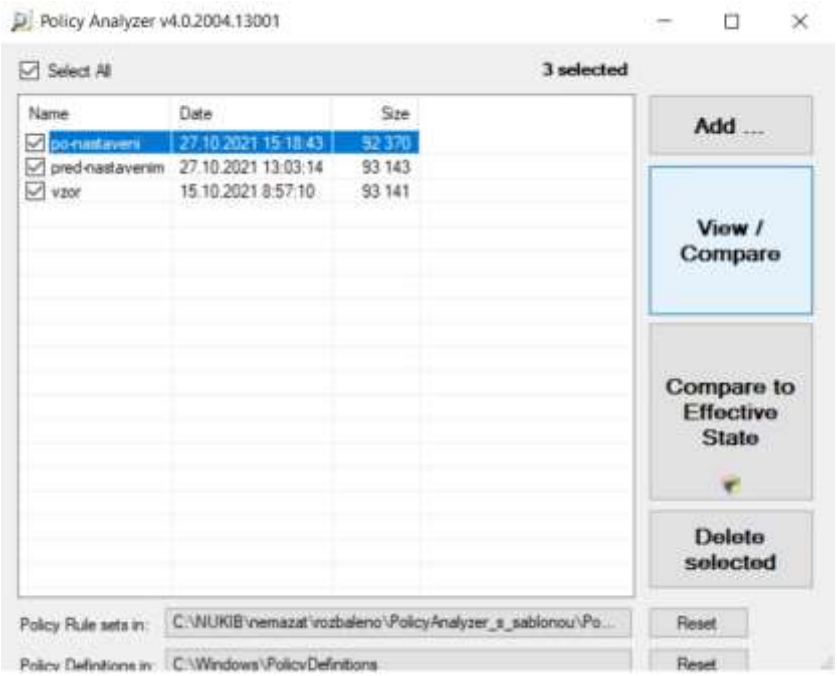
b) Volba 4 – umožňuje zakázat/povolit čtení/zápis z USB disku – toto nastavení je trvalé (do další změny) a musí se shodovat s dokumentací k vašemu systému. V některých případech, ale v souladu s dokumentací umožněno správci systému povolit čtení/zápis jen dočasně, například pro účely aktualizace SW.

c) Volba 5 – umožňuje instalaci (přidání) dalšího / dalších USB disků nebo odstranění všech USB disků, které byly do systému přidány. V průběhu této volby dojde dočasně k povolení instalace (přidání) dalších USB disků. Skript umožňuje přidávat jednotlivé USB disky, ale v případě odstraňování umožňuje pouze odstranění všech USB disků najednou. Pokud provedete odstranění USB disků, je následně potřeba ty USB disky, které chcete v systému i nadále používat opětovně přidat do systému.

d) Volba 7 – umožňuje instalaci (přidání) dalšího, dalších USB zařízení, které budete v systému využívat (zařízení HID např. klávesnice nebo myš). V průběhu této volby dojde dočasně k povolení instalace (přidání) dalších USB zařízení. Po skončení této volby dojde opět k zablokování možnosti přidání dalších USB zařízení. Pokud chcete do systému přidat další USB zařízení, které není uvedené ve schválené dokumentaci

(seznam HW na specifikačním listu pracoviště), tak je potřeba si nejprve vyžádat souhlas NÚKIB.

e) Volba 8 – umožňuje provedení kontroly nastavení systému. Volba spustí „Policy Analyzer“, v němž je možno provést porovnání aktuálního a doporučeného bezpečnostního nastavení systému. Za předpokladu, že byl systém nastaven volbou 1 je možné porovnat celkem 3 bezpečnostní nastavení systému („po-nastaveni“, „pred-nastavenim“ a „vzor“).



(13) Po ukončení všech nastavení, kdy je systém ve stavu, ve kterém bude provozován, vygenerujte kontrolní soubory pomocí volby 2 v menu skriptu („odeslat-na-nukib“ a „odeslat-datovou-schrankou.txt“). Soubor „odeslat-na-nukib“ odešlete na e-mail příslušného zaměstnance NÚKIB (viz kontaktní pracovník uvedený v odpovědi na žádost o certifikaci) a soubor „odeslat-datovou-schrankou.txt“ odešlete na NÚKIB datovou schránkou (ISDS: zzfnkp3) spolu s ostatními požadovanými dokumenty pro certifikaci informačního systému.

(14) Volba m – umožňuje bezpečné mazání vyjímatelných disků připojitelných prostřednictvím USB rozhraní, a to tak, jak je popsáno v části Bezpečné mazání tohoto dokumentu.

Čl. 10

Označení a evidence

(1) Každá HW a SW komponenta informačního systému (včetně operačního systému) být evidována na specifikačním listu pracoviště.

(2) Dokument „23_Specifikacni_list_pracoviste.docx“ je potřeba před jeho odesláním na NÚKIB vyplnit příslušnými údaji. Vyplnění příslušných údajů v dokumentu probíhá formou nahrazení částí psaných červenou kurzívou skutečnými údaji. Jedná se o následující údaje:

a) *název pracoviště* (např. PV-01),

b) *Firma a.s.* (např. První stavební s.r.o.),

c) *město / obec, část obce, PSČ, ulice a číslo* (údaje o adrese organizace provozující IS uváděné v obchodním rejstříku),

d) *poschodí* (např. 5NP, nebo 2PP),

e) *označení* (např. místnost č. 245, nebo místnost č. 45A2),

f) *kategorie objektu* (např. Vyhrazené),

g) *kategorie zabezpečené oblasti* (např. Vyhrazené),

h) *parametr S1* (např. 5 bodů),

i) *X* u položky „Politika hesel“ slouží pro vyznačení zvolené politiky hesel, je nutné ponechat pouze u vybrané varianty,

j) *titul jméno a příjmení* (např. Ing. Petr Novák).

k) V částích označených jako „Seznam HW“ a „Seznam SW“ je nutné vyplnit skutečné údaje o HW a SW konfiguraci pracoviště informačního systému (včetně operačního systému).

(3) Vytištěný dokument zůstává uložen u bezpečnostního správce informačního systému a na NÚKIB je odeslána, prostřednictvím systému datových schránek ISDS, jeho elektronická verze.

(4) Základní jednotka počítače nebo notebook musí být na viditelném místě označena štítkem obsahujícím údaje o stupni maximálním utajení zpracovávaných utajovaných informací a názvem provozovatele informačního systému.

(5) Příklad štítku pro označení základní jednotky počítačové sestavy:

IS pro zpracování
utajovaných informací:

VYHRAZENÉ

Otisk razítka nebo název provozovatele

(6) HW komponenty pracoviště obsahující alespoň jeden nevyjímatelný nosič informací, který nepotřebuje pro uchování informace trvalé připojení k elektrické energii musí být opatřeny jedním nebo několika ochranným prvky.

(7) Ochranné prvky musí být na HW komponentě umístěny tak, aby při pokusu o vniknutí do HW komponenty došlo k jejich poškození a zároveň tak, aby byla možná jejich snadná vizuální kontrola uživatelem.

(8) Ochranný prvek musí být číslovaný a obsahovat reziduální vrstvu, která zajistí znehodnocení ochranného prvku při pokusu o jeho sejmutí (odstranění z HW komponenty). Příklad ochranného prvku:

(9) Všechny nosiče informací používané v informačním systému musí být evidované v evidenční pomůcce. Vzor evidenční pomůcky je uveden v dokumentu „35_Evidence_nosicu_informaci.docx“.

(10) Nosiče informací, které jsou používány jako pomůcka uživatele k ukládání utajovaných informací (záloha uživatelských dat apod.) musí být označeny štítkem nebo visačkou obsahujícím název provozovatele, evidenční číslo a stupeň utajení nosiče. Příklad štítku utajovaného nosiče:

Provozovatel: ……..
……
Ev.č.: ……...
stupeň utajení: **V Y H R A Z E N É**

(11) Nosiče informací, které jsou používány jako pomůcka uživatele k ukládání neutajovaných informací (vkládání aktualizací virových řetězců, záloha auditních záznamů apod.) musí být opatřeny štítkem obsahujícím název provozovatele a evidenční číslo nosiče. Příklad štítku neutajovaného nosiče:

Provozovatel: ……..
……
Ev.č.: ……...

(12) V případě pevného disku, který je pevně zabudován v pracovní stanici nebo notebooku je pracovní stanice nebo notebook opatřen štítkem, který informuje o zabudovaném nosiči informací. Příklad štítku:

Zařízení obsahuje zabudovaný nosič informací:

ev.č.: ……...

stupeň utajení: **VYHRAZENÉ**

Čl. 11

Test bezpečnosti

(1) Dokument „24_Test_bezpecnosti.docx“ je potřeba před jeho odesláním na NÚKIB vyplnit příslušnými údaji. Vyplnění příslušných údajů v dokumentu probíhá formou doplnění výsledků jednotlivých testů do sloupečku „Výsledek“, doplnění jmen a podpisů příslušníků kontrolní komise a nahrazení částí psaných červenou kurzívou skutečnými údaji. Jedná se o následující údaje:

a) *název pracoviště* (např. PV-01).

b) *datum* (např. 24. ledna 2019).

(2) Komise musí mít minimálně dva členy a jedním z nich je vždy bezpečnostní správce informačního systému.

(3) Vytištěný dokument zůstává uložen u bezpečnostního správce informačního systému a na NÚKIB je odeslána, prostřednictvím systému datových schránek ISDS, jeho elektronická verze.

Čl. 12

Provozní dokumentace

(1) Základní provozní dokumentace vedená k informačnímu systému je:

a) „31_Povereni_k_cinnosti.docx“ – pověření k výkonu role v informačním systému pro jednotlivé zaměstnance.

b) „32_Ukonceni_povereni.docx“ – ukončení pověření k výkonu role v informačním systému pro jednotlivé zaměstnance.

c) „33_Evidence_skoleni_uzivatelu.docx“ – výkaz každoročních pravidelných školení uživatelů informačního systému.

d) „34_Evidence_uzivatelu.docx“ – slouží k evidenci uživatelů informačního systému.

e) „35_Evidence_nosicu_informaci.docx“ – slouží k evidenci provozních nosičů utajovaných i neutajovaných informací. Provozní nosiče informací se evidují způsobem uvedeným v § 13 odst. 2 vyhlášky č. 479/2024 Sb., kde se nosič opatřuje označením obsahujícím evidenční číslo a identifikaci provozovatele informačního systému. Evidenční číslo provozního nosiče obsahuje informace podle § 42 odst. 4 písm. c) vyhlášky č. 479/2024 Sb., zkratka stupně utajení, je-li nosič informací utajovaný, nebo zkratka informace o tom, že nosič informací je neutajovaný, pořadové číslo, rok zavedení do evidence a identifikaci provozovatele informačního systému. Jednotlivé části evidenčního

čísla se od sebe oddělují obvykle lomítkem nebo spojovníkem. Příklad evidenčního čísla: N/1/2021-ELT (N-neutajovaný nosič, 1-první v evidenční pomůcce, 2021-rok zaevidování, ELT-zkratka provozovatele informačního systému). V případě, kdy je evidence nosičů prováděna v jiné evidenční pomůcce, tak tento dokument nemusí existovat, nicméně povinnost evidence provozních nosičů tím není nijak dotčena.

f) „36_Kniha_manipulace_s_nosici.docx“ – slouží k záznamům o předávání utajovaného nosiče informací nebo notebooku. Tento dokument může být společný pro celý informační systém, nebo v případě, kdy jsou jednotlivá pracoviště umístěná v různých zabezpečených oblastech, existuje vždy jeden pro každé pracoviště.

g) „37_Provozni_denik_pracoviste.docx“ – slouží k zaznamenávání událostí prováděných pracovníky správy (provozní a bezpečnostní správce) v rámci provozu informačního systému (aktualizace, stahování a archivace auditních záznamů, instalace SW apod.). Tento dokument musí existovat pro každé pracoviště informačního systému. V případě, že je více pracovišť informačního systému provozováno v jedné zabezpečené oblasti, tak lze provádět zápisy do jednoho deníku pracoviště, ale u každého zápisu musí být uvedeno pro které pracoviště informačního systému platí.

h) „23_Specifikacni_list_pracoviste.docx“ – slouží k základnímu popisu pracoviště informačního systému (název, umístění, fyzické zabezpečení a politika hesel) a k evidenci HW a SW komponent.

i) „24_Test_bezpecnosti.docx“ – dokument o provedeném testu bezpečnosti pracoviště informačního systému. Test bezpečnosti se provádí vždy před začleněním pracoviště do informačního systému, nebo při podstatných změnách provedených na pracovišti (přeinstalace operačního systému). Elektronická kopie testu bezpečnosti se zasílá na NÚKIB.

Čl. 13

Kontrolní obhlídka

(1) Na základě doručené bezpečnostní dokumentace a výsledků z nastavení operačního systému provede NÚKIB vyhodnocení a rozhodne o provedení kontrolní obhlídky.

(2) Kontrolní obhlídka se provádí v místě instalace informačního systému a dochází při ní k ověření opatření z oblasti administrativní, fyzické, personální, průmyslové a informační bezpečnosti.

Čl. 14

Ukončení správního řízení

(1) Na základě podkladů a případných zjištění při prováděné kontrolní obhlídce je správní řízení o certifikaci informačního systému ukončeno:

a) vydáním certifikátu a certifikační zprávy informačního systému,

b) rozhodnutím o nevydání certifikátu informačního systému.