Informační systém pro zpracování utajovaných informací

An Information System for Processing Classified Information

Bc. Martin Kuška

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martin KUŠKA**
Osobní číslo:	**A10904**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Informační systém pro zpracování utajovaných informací**

Zásady pro vypracování:

Cíl: Navrhnout projekt informačního systému pro zpracování utajovaných informací.

1. **Vysvětlete zpracovávání a ukládání utajovaných informací.**
2. **Uveďte platnou legislativu v problému.**
3. **Popište zpracování a ukládání utajovaných informací v elektronické podobě.**
4. **Uveďte úkoly NBÚ v problematice.**
5. **Zpracujte návrh projektu informačního systému pro zpracovávání a uchovávání utajovaných informací**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Česká republika. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti. In:Sbírka zákonů České republiky. 2005, částka 143. ISSN 1211-1244. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/**
2. **Česká republika. Vyhláška č. 523 ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor. In:Sbírka zákonů České republiky. 2005, částka 179. ISSN 1211-1244. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/**
3. **Česká republika. Vyhláška č. 528 ze dne 5. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In:Sbírka zákonů České republiky. 2005, částka 179. ISSN 1211-1244. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/**
4. **Národní bezpečnostní úřad [online]. 2012 [cit. 2012-01-13]. Dostupné z: http://www.nbu.cz/**
5. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2004, 64 s. ISBN 80-731-8194-0.**
6. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 1. Ve Zlíně: Univerzita Tomáše Bati, 2004, 122 s. ISBN 80-731-8231-9.**
7. **LAUCKÝ, Vladimír. Speciální bezpečnostní technologie. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009, 223 s. ISBN 978-807-3187-620.**

Vedoucí diplomové práce: **JUDr. Vladimír Laucký**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce si klade za cíl přiblížit a objasnit zpracování a ukládání utajovaných informací, legislativní úpravu pro nakládání s utajovanými informacemi v České republice a podobu návrhu projektu informačního systému pro zpracování a ukládání utajovaných informací, včetně zpracování projektové a provozní dokumentace systému.

Klíčová slova: utajovaná informace, informační systém, projekt informačního systému, bezpečnost, kompromitující vyzařování

ABSTRACT

This thesis introduces and explains the processing and storage of classified information, legislation concerning classified information handling in the Czech Republic and presents the design of an information system project for processing and storage of classified information, including the project and operating documentation of the system.

Keywords: Classified Information, Information System, Project Information System, Security, Compromising Emission

Poděkování:

Chtěl bych touto cestou poděkovat, panu JUDr. Vladimíru Lauckému, za odborné vedení této diplomové práce, věcné připomínky a rady, svým kolegům a především své rodině za velkou podporu během studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

…….

podpis diplomanta

OBSAH

ÚVOD

Jsme svědky skutečně prudkého rozšíření informačních a komunikačních technologií, které do naší každodenní činnosti pronikly takovým způsobem, že si bez nich obyčejný den dokážeme těžko představit. Tyto technologie nám dnes umožňují rychlou, efektivní ale ne vždy zcela bezpečnou výměnu informací. A právě informace se dnes stala mnohdy tím nejdůležitějším co společnost, firma nebo fyzická osoba vlastní. Vynakládáme nemalé úsilí, abychom takovou informaci ochránili, bezpečně uložili, předali nebo přijali.

O to větší důraz je kladen na ochranu informací, které označujeme jako utajované. Problematika ochrany utajovaných informací je poměrně složitou a specifickou oblastí ochrany informací, která je v České republice vymezena a upravena zákonem č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů. V souvislosti s rozvojem technologií a výpočetní techniky, jsou i utajované informace vytvářeny, zpracovávány, ukládány nebo je s nimi jinak nakládáno pomocí informačních technologií a výpočetní techniky. Ve výše uvedeném zákoně a dalších prováděcích právních předpisech jsou vymezeny podmínky a požadavky, které jsou kladeny při nakládání s utajovanými informacemi výpočetní technikou. Jednou ze základních podmínek je nakládání s utajovanou informací v certifikovaném informačním systému.

Dokumentace takového systému je minimálně neveřejná a není možné se běžně s takovou dokumentací seznámit. Cílem této práce je seznámení s projektem takového informačního systému a s podobou projektové a provozní dokumentace.

I. TEORETICKÁ ČÁST

1 UTAJOVANÉ INFORMACE A JEJICH OCHRANA

1.1 Utajovaná informace

Informací, kterou nazýváme nebo označujeme za utajovanou je podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti taková informace, která je označena stupněm utajení, je uvedena v seznamu utajovaných informací a její zneužití nebo vyzrazení může způsobit újmu zájmům České republiky nebo může být pro takový zájem nevýhodné. Jak je informace zaznamenána zde není rozhodující, informace může být zaznamenána v jakékoli podobě a na jakémkoli nosiči. Pojem utajovaná informace je vymezen v §2 zákona č. 412/2005 Sb.

Seznam utajovaných informací tvoří přílohy k nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb. Nařízení vlády má celkem osmnáct příloh, ve kterých jsou uvedeny oblasti informací podléhající některému ze stupňů utajení. Oblasti informací jsou zde uvedeny včetně stupně nebo možného rozsahu stupňů utajení. Samotné přílohy se týkají nejen jednotlivých ministerstev a jejich oblastí působení, ale také dalších složek státního aparátu jako jsou ozbrojené bezpečnostní sbory, zpravodajské služby, telekomunikační úřad, Česká národní banka a další.

1.2 Právní úprava ochrany utajovaných informací v ČR

Ochranou utajovaných informací se v právním řádu České republiky zabývá zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti. Tento zákon byl naposledy novelizován zákonem č. 255/2011 Sb. s účinností od 1. ledna 2012. Zákon je rozdělen na devět částí a celkem obsahuje 161 paragrafů. Níže uvedená tabulka uvádí rozdělení jednotlivých částí zákona a popisuje, čemu se věnují.

Tab. 1: Části zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti

Část číslo	Obsah části
1.	Úvodní ustanovení
2.	Ochrana utajovaných informací

Část číslo	Obsah části
	Hlava I. Ochrana utajovaných informací, klasifikace, stupně utajení, druhy zajištění ochrany, *Hlava II.* personální bezpečnost, podmínky pro přístup k utajovaným informacím fyzických osob *Hlava III.* Průmyslová bezpečnost, podmínky a formy přístupu k utajované informaci podnikatelem *Hlava IV.* Administrativní bezpečnost, označování a evidence utajovaných informací *Hlava V.* Fyzická bezpečnost, kde se utajovaná informace zpracovává, ukládá, projednává, projekt fyzické bezpečnosti *Hlava VI.* Bezpečnost informačních a komunikačních systémů, taktická informace *Hlava VII.* Ochrana utajovaných informací v elektronické podobě při zpracování v zařízeních, které nejsou součástí informačního nebo komunikačního systému jako jsou psací stroje s pamětí, kopírky, apod. *Hlava VIII.* Kryptografická ochrana a její výkon a způsobilost, manipulace s kryptografickým materiálem, kompromitace kryptografického materiálu, kompromitující vyzařování *Hlava IX.* Žádost o certifikaci a certifikace technického prostředku, informačního systému, kryptografického prostředku, pracoviště, stínící komory *Hlava X.* Osvědčení fyzické osoby a podnikatele, zvláštní a jednorázový přístup k utajové informaci, zproštění mlčenlivosti *Hlava XI.* Povinnosti při ochraně utajovaných informací, průmyslového vlastnictví *Hlava XII.* Poskytování utajovaných informací v mezinárodním styku, způsob, podmínky a žádost pro takové poskytování informací, povolení a souhlas
3.	Bezpečnostní způsobilost
4.	Bezpečnostní řízení *Hlava I.* Obecné zásady, vyloučení a účastník řízení

Část číslo	Obsah části
	Hlava II. Zahájení a průběh řízení, úkony v řízení o vydání osvědčení fyzické osoby, podnikatele, přerušení a zastavení řízení, lhůty, doručování
5.	Výkon státní správy
6.	Státní dozor
7.	Kontrola činnosti úřadu
8.	Správní delikty, přestupky, pokuty
9.	Přechodná a závěrečná ustanovení

1.3 Novelizace zákona 412/2005 Sb. s účinností od 1.1.2012

Od 1.1. 2012 je účinná dosud největší novelizace a doplnění zákona o ochraně utajovaných informací a přináší řadu změn. Novelizaci provádí zákon č. 255/2011 Sb., kterým se mění zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti, ve znění pozdějších předpisů, a zákon č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů. Z důvodové zprávy vyplývá, že cílem novelizace je zkrácení doby bezpečnostních řízení pro vydání osvědčeních a dokladů, úspora nákladů a administrativní zátěže všech účastníků bezpečnostního řízení a dále zjednodušení právní úpravy.

Rozsáhlá novelizace zákona se významně dotýká průmyslové bezpečnosti a pravomocí NBÚ v oblasti veřejných zakázek.

Přístup podnikatele k utajované informaci stupně utajení Vyhrazené již nebude udělován na základě bezpečnostního řízení vedené NBÚ, ale bude na základě prohlášení podnikatele, že je schopen zabezpečit ochranu utajovaných informací. Bezpečnostní řízení bude nadále prováděno pro stupně utajení Důvěrné a vyšší.

Prohlášení předá podnikatel tomu, kdo mu utajovanou informaci poskytuje. Učinit takové prohlášení může podnikatel jen za podmínek, že splňuje a má vytvořeny odpovídající podmínky pro přístup k takové informaci a její ochranu. Utajovaná informace může i nemusí u podnikatele vznikat, je mu poskytována nebo mu poskytována není, ale jeho zaměstnanci k ní v souvislosti s výkonem práce mají přístup. Odpovědná osoba podnikatele musí mít osvědčení fyzické osoby nebo doklad nebo být držitelem oznámení.

Kdo podnikateli poskytuje utajovanou informaci je povinen požadovat od podnikatele předložení jeho bezpečnostní dokumentace a poskytovatel se po zvážení rozhodne o zpřístupnění utajované informace.

V případě, že utajovaná informace u podnikatele vzniká, zašle své prohlášení Národnímu bezpečnostnímu úřadu.

Podnikatel, který vydává prohlášení, si musí vést přehled kdy, komu a jaké prohlášení postoupil. V případě změny nebo zániku takového prohlášení, je toto podnikatel povinen neprodleně oznámit tomu, komu takového prohlášení postoupil. Platnost prohlášení je stanovena na pět let.

Novela dále zavádí správní poplatky za podání žádosti podnikatele o vydání osvědčení podnikatele. Smyslem těchto správních poplatků je regulace a snížení počtu podávaných žádostí. V důvodové zprávě se uvádí, že slouží vydané certifikáty mnohdy pouze k prezentaci firmy bez toho, aniž by podnikatel nebo jeho zaměstnanci s utajovanými informacemi nakládali.

Výše správních poplatků za podání žádosti podnikatele je stanovena na 5.000,-Kč pro podnikatele kde utajovaná informace nevzniká, ale jeho zaměstnanci mají k utajované informaci přístup v souvislosti s výkonem zaměstnání. Částku 10.000,-Kč musí uhradit podnikatel, u kterého utajovaná informace vzniká nebo mu je poskytována.

V oblasti veřejných zakázek zavádí novela povinnost právnickým osobám a podnikajícím fyzickým osobám písemně informovat Národní bezpečnostní úřad o zadání veřejné zakázky mimo zákon o veřejných zakázkách nebo záměr uzavřít smlouvu, která by jinak byla smlouvou koncesní, mimo koncesní zákon, v obou případech z důvodu ochrany utajovaných informací. Národní bezpečnostní úřad má pak oprávnění se v 30 denní lhůtě k těmto zakázkám vyjádřit a poskytnout oznámení a vyjádření Úřadu pro ochranu hospodářské soutěže. NBÚ tedy posuzuje zadávací dokumentaci veřejné zakázky, tedy jestli je požadavek zadavatele oprávněný.

1.3.1 Bezpečnostní způsobilost

Novela mění podmínky vydání dokladu o bezpečnostní způsobilosti:

a) pro cizince se prodloužila z 2 na 10 let doba za kterou předkládají doklad podobný výpisu z rejstříku trestů států, v nichž souvisle pobývali déle než 6 měsíců
b) jako negativní okolnost pro vydání dokladu jsou zjevně nepřiměřené majetkové poměry, které kontrastují s přiznanými příjmy fyzické osoby

c) styky s osobou, která vyvíjí nebo vyvíjela činnost proti zájmům republiky, nebo opakované neposkytnutí součinnosti dle zákona, podmíněné zastavení trestního stíhání pro úmyslný trestný čin, podmíněné odložení návrhu na potrestání pro úmyslný trestný čin, u nichž stanovená zkušební doba dosud neuplynula, anebo schválení narovnání pro úmyslný trestný čin

Jsou stanoveny nové důvody zániku platnosti dokladu o bezpečnostní způsobilosti (vrácení držitelem, doručením nového dokladu, čímž zaniká starý doklad). V případě zneplatnění dokladu z důvodu ztráty, odcizení, poškození, změny je stanovena 15ti denní lhůta pro požádání o nový doklad. V případě nepožádání zaniká možnost vykonávat citlivou činnost.

1.3.2 Personální bezpečnost

Novela provádí změny i některých částí personální bezpečnosti. Mezi nejpodstatnější patří zrychlení a zefektivnění přístupu fyzické osoby k utajované informaci stupně utajení Vyhrazené, doplnění dalších způsobů zániku platnosti oznámení, zejména možnost prostého vrácení oznámení vydavateli, popř. NBÚ a zpřesnění základních povinností fyzické osoby.

U pozice bezpečnostního ředitele to je nově schvalování přehledu míst a funkcí, kde je vyžadován přístup k utajované informaci.

Dochází též k doplnění sankčních ustanovení, zejména směrem k podnikatelským subjektům, podnikajícím fyzickým osobám a jejich případným správním deliktům nebo přestupkům.

1.4 Klasifikace a stupně utajení utajovaných informací

Dle ustanovení §4 zákona č. 412/2005 Sb. se utajovaná informace dělí do čtyř stupňů utajení. Tyto stupně utajení jsou Vyhrazené, Důvěrné, Tajné a Přísně tajné.

Jako **Vyhrazené** se klasifikuje taková informace, jejíž vyzrazení neoprávněné osobě nebo zneužití, může být pro zájmy České republiky *nevýhodné*.

Důvěrné jsou označeny informace, které vyzrazením nebo zneužitím můžou způsobit *prostou újmu* zájmům České republiky.

Tajné označujeme informace, které vyzrazením nebo zneužitím můžou způsobit *vážnou újmu* zájmům České republiky.
Přísně tajné označujeme informace, které vyzrazením nebo zneužitím můžou způsobit *mimořádně vážnou újmu* zájmům České republiky.

1.5 Národní bezpečnostní úřad

Nejvyšším správním úřadem v České republice pro oblast ochrany utajovaných informací a bezpečnostní způsobilosti je Národní bezpečnostní úřad (NBÚ). Jako orgán výkonné moci byl k 1.8. 1998 zřízen zákonem č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů.

Hlavní úkoly NBÚ:

- rozhoduje o vydání osvědčení fyzické osoby, osvědčení podnikatele a o vydání dokladu o bezpečnostní způsobilosti fyzické osoby a o zrušení platnosti osvědčení fyzické osoby, osvědčení podnikatele a dokladu
- plní úkoly v oblasti ochrany utajovaných informací v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, Organizaci Severoatlantické smlouvy a z mezinárodních smluv, jimiž je Česká republika vázána
- ve stanovených případech povoluje poskytování utajovaných informací v mezinárodním styku, vede ústřední registr a schvaluje zřízení registrů
- provádí výkon státního dozoru a ukládá sankce za nedodržení povinností stanovených zákonem
- zajišťuje činnost Národního střediska komunikační bezpečnosti, Národního střediska pro distribuci kryptografického materiálu, Národního střediska pro měření kompromitujícího elektromagnetického vyzařování a Národního střediska pro bezpečnost informačních systémů, které jsou jeho součástí
- provádí certifikace technického prostředku, informačního systému, kryptografického prostředku, kryptografického pracoviště a stínicí komory
- zajišťuje výzkum, vývoj a výrobu národních kryptografických prostředků
- vyvíjí a schvaluje národní šifrové algoritmy a vytváří národní politiku kryptografické ochrany.

1.5.1 Certifikace informačního systému

Pro vytváření, zpracování či jiné nakládání s utajovanou informací v rámci informačního systému ukládá zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti povinnost používat výhradně informační systémy, které jsou certifikovány Národním bezpečnostním úřadem. Schválení takového systému provádí NBÚ v souladu s uvedeným zákonem č. 412/2005 Sb. a s vyhláškou č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.

V průběhu certifikačního řízení je NBÚ posuzována vhodnost navržených opatření k dosažení bezpečnosti informačního systému, správnost realizace těchto opatření a dále správnost a úplnost projektové a provozní bezpečnostní dokumentace.

Pokud Národní bezpečnostní úřad shledá informační systém dostatečně způsobilý k ochraně utajovaných informací v rozsahu k jakému byl navržen s ohledem na podmínky v jakých bude provozován, vydá mu certifikát informačního systému. V opačném případě rozhodne o nevydání certifikátu. Proti rozhodnutí o nevydání certifikátu NBÚ není možné žádné odvolání. Doba platnosti certifikátů informačního systému je dána nejvyšším stupněm utajení, se kterými může systém nakládat, viz. tabulka č. 2.

Certifikačnímu řízení předchází žádost ze strany žadatele o certifikaci informačního řízení a předložení podkladů požadovaných NBÚ k provedení certifikace.

Žádost o certifikaci informačního systému musí obsahovat:

a) identifikaci žadatele
b) celé jméno kontaktního pracovníka žadatele včetně kontaktu na něj
c) stručný popis, účel a rozsah informačního systému
d) stupeň utajení utajovaných informací, se kterými bude informační systém nakládat
e) stanovení bezpečnostního provozního módu informačního systému
f) identifikaci dodavatele informačního systému nebo jeho komponent ovlivňujících bezpečnost informačního systému

Doklady předkládané žadatelem k provedení certifikace:

a) bezpečnostní politika informačního systému a výsledky analýzy rizik
b) návrh bezpečnosti informačního systému
c) sadu testů bezpečnosti informačního systému, jejich popis a popis výsledků testování
d) bezpečnostní provozní dokumentace informačního systému

e) popis bezpečnosti vývojového prostředí
f) další podklady nezbytné k certifikaci informačního systému, které vyplývají ze specifikace informačního systému.

Tab. 2: Doba platnosti certifikátu informačního systému v závislosti na stupni utajení

Stupeň utajení IS	**Platnost certifikátu IS**
Vyhrazené	5 let
Důvěrné	3 roky
Tajné	2 roky
Přísně tajné	2 roky

1.6 Ochrana utajované informace, druhy zajištění

1.6.1 Personální bezpečnost

Základním způsobem zajištění ochrany utajované informace je personální bezpečnost. Jedná se o soubor podmínek, které jsou kladeny a požadovány po fyzické osobě, které má mít přístup k utajované informaci. Odpovědnost za řádné plnění podmínek, které jsou požadovány po fyzické osobě seznamující se s utajovanou informací, nese určená odpovědná osoba. Odpovědná osoba také provádí pravidelné proškolení fyzických osob z právních předpisů k ochraně utajovaných informací a vede o nich přehled.

Máme celkem čtyři různé stupně utajení a pro každý stupeň jsou kladeny jiné podmínky, které musí fyzická osoba splňovat.

Tab. 3. Ověřovací podmínky pro fyzické osoby

PODMÍNKY	***VYHRAZENÉ (oznámení)***	***DŮVĚRNÉ, TAJNÉ, PŘÍSNĚ TAJNÉ (osvědčení)***
Způsobilost k právním úkonům	ANO	ANO
Věk minimálně 18 let	ANO	ANO
Bezúhonnost	ANO	ANO
Státní občanství ČR, země EU, NATO	NE	ANO
Osobnostní způsobilost	NE	ANO
Bezpečnostní spolehlivost	NE	ANO

1.6.2 Administrativní bezpečnost

Administrativní bezpečnosti je věnován §21 až §23 zákona č. 412/2005 Sb. ve znění pozdějších předpisů. Doplňujícím dokumentem je vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů .

Obě tyto vyhlášky stanovují správné označování, evidování utajovaných informací, druhy a náležitosti administrativních pomůcek k jejich evidenci, podmínky a detaily přenášení, přepravy, zapůjčování a další manipulace s utajovanými dokumenty. Ve vyhlášce jsou též upraveny opisy, výpisy, kopie a překlady utajovaných dokumentů. Stanovené podmínky a povinnosti se týkají dokumentů v listinné i nelistinné podobě.

Administrativní bezpečnost je tedy souborem opatření uplatňujících se při vytváření, úpravě, evidenci, přepravě, přenášení, odesílání, ukládání, skartaci a případně další jiné manipulaci s utajovaným dokumentem nebo informací obecně.

Přílohou vyhlášky č. 529/2005 Sb. jsou vzory administrativních pomůcek. Celkem je třináct příloh a jsou jimi:

a) příloha č. 1 - jednací protokol, slouží k evidování utajovaných dokumentů
b) příloha č. 2 - pomocný jednací protokol, zaznamenává pohyb utajovaných dokumentů v rámci orgánu státu, právnické osoby nebo podnikající fyzické osoby
c) příloha č. 3 – manipulační kniha, slouží k evidenci utajovaného dokumentu při jeho vytváření, převzetí a předání. Každá osoba mívá svou vlastní manipulační knihu, do které zaznamenává pohyb utajovaných dokumentů, které přes ní prošly nebo u ní vznikly
d) příloha č. 4 - doručovací kniha, k zaznamenání předání utajovaného dokumentu
e) příloha č. 5 – zápůjční kniha, zaznamenává zapůjčení již uložených utajovaných dokumentů
f) příloha č. 6 – kontrolní list utajovaného dokumentu, určeno pro stupně utajení Důvěrné, Tajné a Přísně tajné. Zde se zaznamenávají osoby, které se s obsahem dokumentu seznámily.
g) příloha č. 7 – sběrný arch, rozšiřuje evidenci resp. záznam v jednacím protokole
h) příloha č. 8 – vzor první strany utajovaného dokumentu
i) příloha č. 9 – vzor rozdělovníku a záznamu pro uložení utajovaného dokumentu
j) příloha č. 10 – vzor stvrzenky o převzetí utajovaného dokumentu
k) příloha č. 11 – vzor kurýrního listu

l) příloha č. 12 – vzor evidenčního listu registru
m) příloha č. 13 - vzor zprávy o kontrole utajovaných informací vedených v registru

V odůvodněných případech je možné používat další administrativní pomůcky sloužící k evidenci utajovaných dokumentů, musejí ale obsahovat položky jako jednací protokol s přihlédnutím k účelu pro jaký jsou vedeny. Tyto administrativní pomůcky a pomůcky uvedené v přílohách č. 1-5 musejí být autentizovány, jak uvádí §3 odstavec 2 vyhlášky č. 529/2005 Sb. Autentizace administrativní pomůcky se provádí spočítáním a očíslováním všech listů, na druhé straně uvedením evidenčního označení, počtu listů, data kdy je dána do používání, podepsáním odpovědnou osobou a prošitím autentizační šňůrou (zpravidla v barvě trikolóry)

Obr. 1: Příklad autentizace (prošití) administrativní pomůcky

Na elektronické vedení administrativních pomůcek pamatuje §3 odstavec 4 vyhlášky č. 529/2005 Sb. Předpokladem k vedení v elektronické formě je zabezpečení systému, v němž jsou pomůcky vedeny proti neoprávněnému zásahu a přístupu osob, které k tomu nejsou oprávněny. Dále musí systém prokazatelným způsobem zaznamenávat veškeré prováděné změny a manipulaci s údaji. Používání systému pro elektronickou evidenci pomůcek musí být schváleno odpovědnou osobou. Systém též musí umožňovat převod do listinné podoby nebo export do formátu PDF (Portable Document Format). Při exportování do formátu PDF musí systém umět opatřit PDF dokument uznávaným elektronickým podpisem nebo opatřit elektronickou značkou a kvalifikovaným časovým razítkem.

1.6.3 Průmyslová bezpečnost

Pod průmyslovou bezpečností jsou v zákoně o ochraně utajovaných informací a o bezpečnostní způsobilosti definovány podmínky a formy přístupu podnikatele k utajovaným informacím. Průmyslové bezpečnosti je věnován §15 až §20 zákona č. 412/2005 Sb., vyhláška č. 405/2011 o průmyslové bezpečnosti. K vyhlášce jsou jako přílohy uvedeny vzory žádostí, osvědčení, dotazníků a prohlášení.

V případě, že podnikatel nezbytně potřebuje k výkonu své činnosti přístup k utajované informaci, musí doložit:

- pro stupeň utajení Vyhrazené
  - prohlášení podnikatele, kterým doloží svou schopnost zabezpečit v souladu s platnou vyhláškou ochranu utajovaných informací
  - osvědčení podnikatele pro daný nebo vyšší stupeň utajení
- pro stupeň utajení Důvěrné a vyšší
  - osvědčení podnikatele pro příslušný stupeň utajení nebo vyšší

1.6.4 Fyzická bezpečnost

Soubor opatření fyzické bezpečnosti má za úkol zabránit nebo ztížit případné neoprávněné osobě přístup k utajované informaci, případně úspěšný nebo neúspěšný pokus o přístup zaznamenat. V hlavě V zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, jsou definovány pojmy jako objekt, zabezpečená oblast a jednací oblast, které se určují v rámci zajištění fyzické bezpečnosti utajované informace.

Objektem se rozumí budova nebo jiný ohraničený prostor, ve kterém se zpravidla nachází zabezpečená oblast nebo jednací oblast. Objekt slouží ke zpracovávání a manipulaci s utajovanou informací.

Zabezpečená oblast slouží k ukládání utajované informace. Ta se ukládá do trezoru nebo jiné uzamykatelné schránky, nacházející se v zabezpečené oblasti. Zabezpečené oblasti se zařazují do kategorií Přísně tajné, Tajné, Důvěrné, nebo Vyhrazené a to podle nejvyššího stupně utajení utajované informace, která se v nich ukládá.

Jednací oblast slouží k projednávání utajovaných informací stupně utajení Tajné nebo Přísně tajné. Jinde není dovoleno pravidelně projednávat informace s takovou klasifikací.

Zabezpečení zabezpečené a jednací oblasti a objektu je zajišťováno kombinací opatření fyzické bezpečnosti, které jsou ostraha, režimová opatření a technické prostředky. Výkon ostrahy, rozsah použití opatření fyzické bezpečnosti a rozsah použití technických prostředků se stanoví v závislosti na stupni utajovaných informací a na vyhodnocení rizik v projektu fyzické bezpečnosti. Pro ochranu utajovaných informací se používají certifikované nebo necertifikované technické prostředky v závislosti na kategorii a vyhodnocení rizik.

Certifikaci (posouzení technických parametrů) provádí odborné pracoviště NBÚ a na základě odborného posudku vydává certifikát. NBÚ vydává certifikáty pro mechanické zábranné prostředky, elektrická zámková zařízení a systémy pro kontrolu vstupů, zařízení elektrické zabezpečovací signalizace, tísňové systémy a zařízení fyzického ničení nosičů informací nebo dat.

1.6.5 Bezpečnost informačních systémů

V závislosti na stupni utajení utajovaných informací, se kterými informační systém nakládá, obsahu bezpečnostní dokumentace a na bezpečnostním provozním módu jsou kladeny požadavky na informační systém a stanoveny podmínky jeho bezpečného provozu., které jsou uvedeny ve vyhlášce č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. Nakládat s utajovanými informacemi pomocí informačního systému lze výhradně s informačními takovými systémy, které jsou certifikovány Národním bezpečnostním úřadem a písemně schváleny do provozu a užívání odpovědnou osobou. Odpovědná osoba má pak za povinnost do 30ti dnů schválení takového systému do provozu písemně oznámit NBÚ.

V případě informačních systémů pracujících s utajovanou informací stupňů utajení Důvěrné, Tajné nebo Přísně tajné je povinnost aplikovat opatření na ochranu utajované informace před jejím únikem pomocí kompromitujícího elektromagnetického vyzařování z elektrických a elektronických zařízení. Za účelem eliminace kompromitujícího vyzařování (KV) je možné využít stínící komory. Stínící komora musí být certifikována NBÚ.

Ověření způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajované informace kompromitujícím

elektromagnetickým vyzařováním zajišťuje NBÚ při certifikaci informačního systému nebo kryptografického prostředku, případně na základě písemné žádosti.

1.6.6 Kryptografická ochrana

Kryptografickou ochranu tvoří soubor prostředků, metod a opatření na ochranu utajovaných informací s využitím kryptografického materiálu a kryptografických metod. Kryptografická ochrana je upravena v hlavě VIII zákona č. 412/2005 Sb. a vyhláškou č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací.

Od 1.1. 2012 byla zrušena stará vyhláška č. 524/2005 Sb. o zajištění kryptografické ochrany utajovaných informací.

Za kryptografický materiál je považován kryptografický prostředek, materiál k zajištění jeho funkce a kryptografický dokument. Použitý kryptografický prostředek (hardwarový nebo softwarový produkt určený ke kryptografické ochraně) musí být certifikován Národním bezpečnostní úřadem. Kryptografickým dokumentem je listina nebo jiný nosič informací obsahující utajované informace kryptografické ochrany.

Výkon kryptografické ochrany mohou provádět pracovníci kryptografické ochrany, kteří jsou k této činnosti pověřeni odpovědnou osobou, úspěšně absolvovali odbornou zkoušku na základě které jim bylo vydáno osvědčení o zvláštní odborné způsobilosti a jsou držiteli platného osvědčení fyzické osoby.

Do výkonu kryptografické ochrany zahrnujeme:

a) bezpečnostní správu
b) speciální obsluhu kryptografického prostředku
c) výrobu kryptografického prostředku nebo materiálu k zajištění jeho funkce

S kryptografickou ochranou souvisí také pojem kryptografické pracoviště, což je pracoviště sloužící k výrobě a testování materiálu pro zajištění funkce kryptografického prostředku, k ukládání kryptografického materiálu, jeho distribuci a evidenci nebo k výrobě a testování kryptografického prostředku. Kryptografické pracoviště je schvalováno odpovědnou osobou nebo bezpečnostním ředitelem a musí splňovat bezpečnostní standardy. V případě, že pracoviště slouží k výrobě nebo testování materiálu k zajištění funkce kryptografického prostředku nebo je místem pro centrální distribuci nebo evidenci kryptografického materiálu, musí být před schválením certifikováno Národním bezpečnostním úřadem.

1.6.7 Kompromitující vyzařování

Každé elektrické a elektronické zařízení při svém provozu vyzařuje do svého okolí určitou dávku elektromagnetického záření. U výpočetní a kancelářské techniky tomu není jinak. V souvislosti se zpracováváním a ochranou utajované informace, musíme toto záření brát na vědomí a uvědomit si, že toto neúmyslně vyzářené elektromagnetické záření může být zachytáváno, analyzováno a využito k rekonstrukci nebo obecně k získání utajované informace.

Jako kompromitující vyzařování (KV) tedy označujeme elektromagnetické, optické nebo akustické vyzařování elektronických a elektrických zařízení, které může způsobit únik utajované informace.

Kompromitující vyzařování je nežádoucí zejména ve spojitosti se zobrazováním informace na monitoru, zadávání na klávesnici, využívání tiskáren a ukládání na nosiče dat. V případě pravidelného zpracování utajované informace se riziko zvyšuje, právě z důvodu pravidelnosti činnosti a využití opakování k získání nebo odvození utajované informace. V takových případech se aplikují přísnější požadavky.

S kompromitujícím vyzařováním souvisí také termín ***TEMPEST***. TEMPEST je kódové označení pro zkoumání a analýzu kompromitujícího vyzařování. Termín TEMPEST je často používán pro celou oblast EMSEC (Emission Security), označujících soubor bezpečnostních opatření proti získání informací prostřednictvím nežádoucích emisí energií. Termín TEMPEST byl vytvořen na přelomu 60. a 70. let minulého století jako kódové označení operace NSA, není tedy původně žádnou zkratkou.

Již při návrhu informačního systému je vhodné se touto problematikou zabývat a volit vhodný typ zařízení a jeho vhodné umístění vzhledem ke kontrolovanému prostoru[1]. S vhodně zvoleným umístěním IS je možné dosáhnout lepší zóny a zpravidla pak nejsou kladeny tak přísné požadavky na třídu zařízení, čímž lze docílit finanční úspory.

V České republice se uplatňuje tzv. „zónový princip“. To znamená, že jednotlivé komponenty informačního systému nebo celý informační systém je hodnocen tzv. třídou. Prostoru, kde je informační systém umístěn je přiřazena tzv. zóna

Pro informační systémy a zařízení, které jsou určeny pro zpracování utajovaných informací do stupně utajení Vyhrazené, je požadováno pouze „Prohlášení o shodě“, pokud toto prohlášení mají, jsou hodnocena jako zařízení třídy 2. Další opatření týkající se kompromitujícího vyzařování nejsou požadována.

1 Kontrolovaný prostor dle NBÚ je: „třírozměrný prostor, obklopující IS, ve kterém je zajištěno, že nepovolaná osoba zde nebude provádět nekontrolovatelnou činnost za účelem získání utajovaných informací formou kompromitujícího vyzařování. Velikost kontrolovaného prostoru se udává v metrech.“

U zpracování utajovaných informací stupně utajení Důvěrné a vyšší je požadováno aby napájení zařízení bylo odděleno vysokofrekvenčním filtrem a dále jsou kladeny požadavky na kompromitující vyzařování.

1.6.8 Hodnocení informačních systémů

Hodnocení informačních systémů je prováděno dle standardů NBÚ, které vycházejí z požadavků a dokumentů NATO (SDIP) a z převzaté evropské normy ČSN EN 55022.

NATO SDIP-27

Tento dokument NATO rozděluje zařízení do tříd 0 až 2, z čehož třída 0 je nejpřísnější.

Tab. 4. Třídy dle NATO SDIP-27

Třída	***Popis***
Třída 0	Nejpřísnější norma pro zařízení, předpokládá se, že útočník se může nacházet v téměř bezprostřední blízkosti (asi 1 m, sousední místnost)
Třída 1	Mírnější norma, předpokládá se, že útočník se může dostat blíže než 20 m (nebo stavební materiály zajistí útlum rovnající se této vzdálenosti ve volném prostoru)
Třída 2	Nejmírnější norma, útočník musí překonat útlum odpovídající hodnotě na 100 m ve volném prostoru (nebo jeho ekvivalent zeslabený pomocí stavebních materiálů). Jako zařízení třídy 2 jsou bez měření hodnoceny všechny zařízení s vydaným „Prohlášením o shodě“ s ČSN EN 55022

ČSN EN 55022

ČSN EN 55022 je převzatá evropská norma, podle které by měla být testována všechna elektronická zařízení prodávaná v České republice. Na základě měření a jeho výsledků je výrobcem, případně dovozcem, vydáváno „Prohlášení o shodě“.

Všechna zařízení vyhovující této normě, jsou bez dalšího měření hodnocena jako zařízení třídy 2.

1.6.9 Instalace informačních systémů

Umístění informačního systému se řídí několika dokumenty, především dokumentem NATO SDIP-29. Tímto dokumentem jsou stanoveny především minimální požadované vzdálenosti IS od metalických vedení nebo ostatních elektronických zařízení. Dalším dokumentem upravujícím instalaci IS je Bezpečnostní standard NBÚ-2/2007 „Instalace zařízení z hlediska kompromitujícího elektromagnetického vyzařování“ , který je klasifikován stupněm utajení Důvěrné a šířen zásadně dle zásady „Need To Know[1]“

Umístění IS by mělo být koncipováno ve vhodné místnosti, dle doporučení NBÚ nejlépe v místnostech, které jsou nejdále od veřejného prostoru (ulice, veřejné prostranství, cizí objekt), nejlépe orientovány do nějakého vnitřního traktu či dvora nebo umístění v suterénních podlažích bez oken. V samotné místnosti se hledí na křížení nebo dokonce souběžné vedení kabeláže (včetně napájení) s cizími nekontrolovanými metalickými rozvody (např. telefonní, silnoproudé, topení, klimatizace, voda, atd.), též se hledí na umístění IS vzhledem k oknům (možnost případného odpozorování zobrazovaných informací na monitoru apod.)

1.6.10 Analýza rizik

Součástí projektové bezpečnostní dokumentace informačního systému je i analýza rizik. Při této činnosti stanovujeme, případně hodnotíme aktiva informačního systému a snažíme se co nejlépe předvídat a identifikovat potencionální hrozby a zranitelnosti, které mohou vést k riziku ohrožení stanovených aktiv informačního systému. Vztah mezi jednotlivými pojmy analýzy rizik ilustruje obrázek č. 2. Za aktiva informačního systému jsou považovány všechny hmotné i nehmotné prvky systému, které jsou důležité a mají z pohledu uživatele hodnotu (definovaný hardware, software, dokumentace, data uložená v systému). Posuzují se především hrozby, které mohou ohrozit bezpečnost informačního systému nebo způsobit jeho nefunkčnost. Výsledkem analýzy je pak seznam hrozeb, jejich dopad a k nim odpovídající míra rizika. Na základě analýzy se určují vhodná protiopatření s maximálním využitím implementovaných funkcí, zařízení a služeb taková, která jsou nezbytná pro splnění účelu, pro který je systém zřizován.

1 „Need To Know“ - princip, podle kterého má osoba jen nezbytně nutné informace potřebné k požadované činnosti

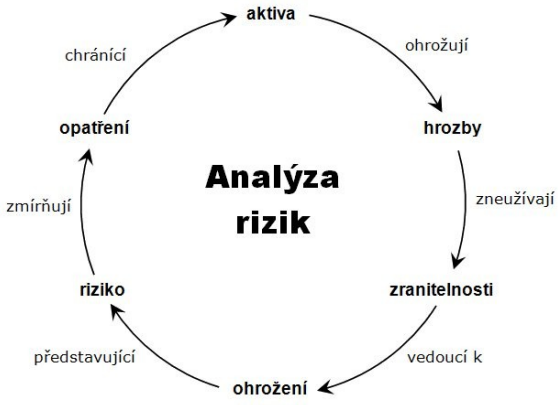
U osobních počítačů je specifickou hrozbou získání fyzického přístupu k počítačové sestavě, kdy neoprávněná osoba může zcizit v něm obsažená paměťová média s utajovanými informacemi nebo HW vybavení nebo tyto poškodit či zničit. Další možnou hrozbou je logický přístup, ke kterému může dojít nastartováním počítačové sestavy z vnějšího paměťového média (CD, USB disk, disketa, apod.) a k získání přístupu k datovému obsahu nebo může dojít k umožnění manipulace se systémovým nebo aplikačním vybavením počítače.

Je několik způsobů a metod, které jsou využívány pro analýzu rizik a jednou z těchto metod je analýza vyhodnocující pravděpodobnost ohrožení (vzniku incidentu) a jeho dopad. Tato metoda využívá dva parametry, a to pravděpodobnost a dopad ohrožení. Pravděpodobnost ohrožení se snižuje působením existujících opatření. Stanovení hodnoty dopadu působení hrozby souvisí s ohodnocením aktiva. Pokud dojde k úplnému zničení aktiva, bude dopad ohodnocen stejně jako aktivum. U částečného poškození aktiva, bude ohodnocení dopadu nižší.

Míru rizika stanovíme podle vztahu $Riziko = Pravděpodobnost\ ohrožení \times Dopad$

Základní kroky analýzy rizik:

1) stanovení a ohodnocení aktiv
2) identifikace možných hrozeb, nalezení zranitelností, které mohou být zneužity
3) určení pravděpodobnosti, že daná hrozba využije či zneužije zranitelnost
4) stanovení dopadu na aktiva (hodnoty dopadu)
5) vypočtení rizika



Obr. 2: Analýza rizik

1.6.11 Zpracování a ukládání utajované informace

Místem, kde lze zpracovávat utajované informace, je zabezpečená oblast příslušné kategorie (zabezpečenou oblastí je myšlen ohraničený prostor v objektu) nebo jeli zajištěno, že k utajované informaci nemá přístup neoprávněná osoba, v objektu příslušné a vyšší kategorie.

Ve výjimečných případech a na základě písemného souhlasu odpovědné osoby nebo bezpečnostního ředitele a kdy je zajištěno, že se k utajované informace nedostane neoprávněná osoba, lze utajovanou informaci zpracovávat mimo objekt nebo v objektu jiné kategorie, než je stupeň utajení zpracovávané utajované informace.

1.7 Utajovaná informace v elektronické podobě

Informace označená v souladu se zákonem jako utajovaná se může vyskytovat v jakékoli podobě na jakémkoliv nosiči. V souvislosti s výpočetní technikou a informačními technologiemi obecně se setkáváme s utajovanými informacemi v elektronické podobě na různých paměťových médiích tedy nosičích informací. Z pohledu zákona a vyhlášky o administrativní bezpečnosti a o registrech utajovaných informací takovéto utajované dokumenty v elektronické formě označujeme jako utajované dokumenty v nelistinné podobě. Obdobně jsou označeny a evidovány nosiče utajovaných informací např. pevné disky, CD-ROM, DVD, USB disky, apod.

Náležitosti, které musí utajovaný dokument nelistinné podoby obsahovat uvádí §17 vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. Pokud je utajovaným dokumentem v nelistinné podobě paměťový nosič informace (např. pevný disk, USB disk, apod.), uvedou se tyto náležitosti přímo na tento nosič v podobě popisného štítku nebo se k němu takový štítek vhodně připevní. Příkladem označení takového paměťového nosiče je obrázek č. 3

Obr. 3: Příklad označení nosiče utajovaných informací

Nakládat s utajovanými informacemi a nosiči utajovaných informací lze na schválených a certifikovaných zařízeních a informačních systémech.

1.7.1 Zpracování utajované informace v elektronické podobě zařízením, které není součástí IS

Novelou zákona platnou od 1.1.2012 jsou v § 36 zákona č.412/2005 Sb. stanoveny povinnosti orgánu státu, právnické osoby a podnikající fyzické osoby při zpracování utajované informace v zařízení, které není součástí žádného informačního systému. Jsou to především kopírky, psací stroje s pamětí, skenery, konvertory do jiných datových formátu apod. U těchto zařízeních musí být vydána bezpečnostní provozní směrnice, ve které musí být uveden způsob bezpečného provozování zařízení, a dále je uvedena provozní směrnice pro uživatele, kteří zařízení používají.

Vyhláškou č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb., jsou v její šesté části upřesněny podmínky bezpečného provozování těchto zařízení. Jedná se zejména o aplikaci personální, fyzické a administrativní bezpečnosti a též o aplikaci ochrany proti úniku utajované informace kompromitujícím vyzařováním. Kladeny jsou i požadavky na fyzické umístění zařízení, aby bylo ochráněno před přístupem neoprávněných osob, před odezíráním utajované informace a aby bylo vhodně umístěno s ohledem na závěry analýzy rizik.

Zařízení, které v sobě obsahuje paměťový nosič, resp. nosič utajovaných informací (např. pevný disk), musí být viditelně označeno informací o stupni utajení uchovávaných informací na tomto nosiči a musí to být také uvedeno v bezpečnostní provozní směrnici. Tyto nosiče musejí být řádně evidovány a označeny, nejpozději po vyjmutí ze zařízení.

2 INFORMAČNÍ SYSTÉMY

V případě zpracování a uchovávání utajovaných informací v elektronické podobě budeme využívat informační systém. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti v § 34 definuje co to informační systém je. Informačním systémem tedy rozumíme jeden nebo více počítačů, včetně jejich programového vybavení, periferních zařízení, procesů nebo prostředků schopných provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací. Pod pojem informační systém patří též správa takového systému.

Informační systém musí být certifikován Národním bezpečnostním úřadem a písemně schválen do provozu odpovědnou osobou nebo osobou jí pověřenou. Odpovědná osoba je pak povinna do 30 dnů oznámit NBÚ schválení takového systému do provozu. Pokud se jedná o informační systém podnikatele, který má přístup k utajované informaci stupně Vyhrazené, může být schválen a provozován jen v době platnosti prohlášení podnikatele.

Zásadním dokumentem je vyhláška č. 523/2005 Sb. o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor, ve znění pozdějších předpisů. Předmětem této vyhlášky je stanovení požadavků, které musí schválený informační systém splňovat aby mohl být certifikován, provozován a mohl nakládat s utajovanými informacemi. Upravuje též podmínky a průběh certifikace informačních systémů, dále se zabývá schvalováním projektů bezpečnosti, ochranou utajovaných informací v elektronické podobě a ochranou utajovaných informací před jejich únikem kompromitujícím elektromagnetickým zářením.

2.1 Bezpečnost informačních systémů

Cílem přijatých opatření pro zajištění bezpečnosti informačního systému je minimalizovat rizika, kterým je informační systém vystaven, na co nejnižší nebo nejnižší přijatelnou úroveň. Soubor těchto opatření je konkrétně popsán v bezpečnostní dokumentaci. Zajištění bezpečnosti informačních systémů se dosahuje několika způsoby a aplikováním opatření z oblastí:

- personální bezpečnosti
- administrativní bezpečnosti a organizačních opatření

- fyzické bezpečnosti informačního systému
- počítačové a komunikační bezpečnosti
- kryptografické ochrany
- ochrany proti úniku kompromitujícího vyzařování

2.2 Hodnocení bezpečnosti informačních systémů

V roce 2004 se Česká republika připojila k dohodě CCRA (Common Criteria Recognition Arrangement) jako účastník využívající certifikáty Common Criteria (CC). Common Criteria je výsledkem posledního společného snažení původně šesti států o vytvoření společného standardu v oblasti hodnocení bezpečnosti informačních technologií. CC je založena na dříve používaných kritériích hodnocení, zejména na amerických TCSEC (Trusted Computer System Evaluation Criteria), evropských ITSEC (Information Technology Security Evaluation Criteria) a kanadských CTCPEC (Canadian Trusted Computer Product Evaluation Criteria).

K provádění hodnocení podle CC byla vytvořena společná metodologie Common Evaluation Metodology (CEM), která zahrnuje hodnocení pro první čtyři stupně záruk EAL1-EAL4 včetně. Poslední oficiální verzí CEM je 2.3, která je zveřejněna jako norma ISO/IEC 18405:2005.

Využívání CC je v souladu se záměry NBÚ, a proto je její využití ze strany NBÚ doporučováno.

CC jsou rozdělena na 3 části:

1. Úvod a všeobecný model (Introduction and general model)
2. Bezpečnostní funkční požadavky (Security functional requirements)
3. Požadavky na záruky bezpečnosti (Security assurance requirements).

V CC jsou odděleně vyjádřeny požadavky pro požadovanou bezpečnostní funkčnost a požadovanou úroveň záruky za správnost, podobné rozdělení je i v evropské ITSEC. CC stanovuje stupnici pro úrovně hodnocení, definuje 7 balíků záruky, jinak známých jako EALs (Evaluation Assurance Levels)

Dnes prováděná hodnocení dle CC jsou prováděna podle některé úrovně EAL, většinou se provádí do úrovně EAL4.

V dokumentu „Informace o hodnocení bezpečnosti informačních technologií“ Národního bezpečnostního úřadu je uveden následující stručný popis jednotlivých úrovní hodnocení. [24]

Tab. 5: Popis úrovní hodnocení EAL Common Criteria

EAL1	je vhodná, pokud je vyžadována určitá základní důvěra ve správnost fungování hodnoceného PP, ST nebo TOE, avšak hrozby nejsou považovány za vážné. Důvěry se dosahuje nezávislým testováním shody hodnoceného PP, ST nebo TOE s neformální funkční specifikací a zkoumáním předložených příruček pro uživatele.
EAL2	již vyžaduje spolupráci vývojáře, který musí v podstatě dodat funkční specifikace, určité informace o návrhu bezpečnostních funkcí (na úrovni globálního návrhu, high-level design) a výsledky testování, avšak vývoj si nevyžaduje více úsilí nežli je potřebné pro dodržování dobré komerční praxe, a v podstatě nepřináší zvýšení nákladů. Poskytuje nízkou až střední nezávisle ověřenou bezpečnost v případě, že není dostupná kompletní informace z fáze vývoje. Důvěry se dosahuje analýzou vyžadované dokumentace, ověřením výsledků některých testů, analýzou síly funkcí a analýzou zřejmých zranitelností. Pro TOE musí být sestaven seznam konfigurace a vypracovány procedura pro bezpečnou instalaci, generování a spouštění.
EAL3	je možno ještě dosáhnout bez podstatných změn základních existujících vývojářských praktik. Je aplikovatelná v případě, že se vyžaduje střední úroveň nezávisle ověřené bezpečnosti a je opřena o důkladné zkoumání TOE (ST, PP). Navíc oproti EAL2 se vyžaduje rozsáhlejší testování, kontroly vývojového prostředí a zajištění správy konfigurace.
EAL4	stále umožňuje pohybovat se v rámci dobré komerční vývojářské praxe. Jakkoliv přísné jsou tyto praktiky, nevyžadují podstatné specializované znalosti, dovednosti a jiné zdroje. EAL4 je nejvyšší úrovní záruk, kterou lze dosáhnout (za rozumné náklady) zpětně pro již existující produkt. Poskytuje střední až vysokou úroveň záruky nezávisle ověřené bezpečnosti pro běžnou komoditu produktů a vyžaduje ze strany vývojáře nebo uživatelů připravenost k pokrytí dodatečných specifických nákladů spjatých s bezpečnostním inženýrstvím. Navíc oproti EAL3 se již vyžaduje také detailní návrh (low-level design) TOE, neformální model bezpečnostní politiky TOE a dodání určité podmnožiny implementace (např. část zdrojového kódu bezpečnostních funkcí). Nezávislá analýza zranitelností musí demonstrovat odolnost vůči průniku útočníků s nízkým potenciálem pro útok. Kontroly vývojového prostředí jsou doplněny modelem životního cyklu, stanovením nástrojů a automatizovanou správou konfigurace.
EAL5	vyžaduje kromě přísného uplatnění dobré komerční vývojářské praxe aplikaci speciálních technik bezpečnostního inženýrství ve středním rozsahu. Dané TOE bude

	pravděpodobně již navrženo a vyvíjeno s cílem dosáhnout úrovně záruk EAL5. Nepředpokládá se nicméně velké zvýšení nákladů oproti EAL4. EAL5 je tak vhodná v případech, kdy se vyžaduje vysoká úroveň záruky nezávisle ověřené bezpečnosti aniž by náklady na specializované techniky byly nerozumně vysoké. Navíc oproti EAL4 je vyžadováno dodání kompletní implementace TOE, formální model bezpečnostní politiky TOE, poloformální presentace funkčních specifikací, poloformální globální návrh (high-level design) a poloformální demonstrace korespondence. Nezávislá analýza zranitelností musí demonstrovat odolnost vůči průniku útočníků se středním potenciálem pro útok. Vyžaduje se také analýza skrytých kanálů a modularita návrhu.
EAL6	vyžaduje aplikaci technik bezpečnostního inženýrství do přísného vývojového prostředí a je určena pro vývoj TOE sloužícího pro ochranu vysoce hodnotných aktiv proti význačným rizikům, kdy lze odůvodnit dodatečné náklady. Navíc oproti EAL5 se vyžaduje poloformální detailní návrh, rozsáhlejší testování, návrh TOE musí být modulární a zvrstvený, prezentace implementace strukturovaná. Nezávislá analýza zranitelností musí demonstrovat odolnost vůči průniku útočníků s vysokým potenciálem pro útok. Analýza skrytých kanálů musí být systematická. Vyšší nároky jsou kladeny na správu konfigurace a kontroly vývojového prostředí.
EAL7	je použitelná pro vývoj produktů určených do extrémně rizikového prostředí a/nebo kde vysoká hodnota aktiv ospravedlňuje vyšší náklady. Praktické použití EAL7 je v současnosti omezeno na TOE a úzce vymezenou bezpečnostní funkčností, kde lze provést formální analýzu v požadované míře. Vyžaduje se plná formalizace, formální model bezpečnostní politiky, formální presentace funkčních specifikací and high-level návrhu, poloformální detailní návrh, formální a poloformální demonstrace korespondence. Testování se vyžaduje na úrovni bílé skříňky (white-box) a musí být dosaženo úplného nezávislého potvrzení výsledků všech předložených testů. Složitost návrhu musí být minimalizována.

2.3 Bezpečnostní dokumentace informačního systému

Každý informační systém musí mít vlastní schválenou bezpečnostní dokumentaci. Co musí taková dokumentace obsahovat a popisovat určuje §4 až §6 vyhlášky č. 523/2005 Sb. Bezpečnostní dokumentace informačního systému je složena z *projektové bezpečnostní dokumentace informačního systému* a *provozní bezpečnostní dokumentace informačního systému*.

Projektová bezpečnostní dokumentace informačního systému obsahuje

a) bezpečnostní politiku informačního systému a výsledky analýzy rizik
b) návrh bezpečnosti informačního systému
c) dokumentace k testům bezpečnosti

Provozní bezpečnostní dokumentace informačního systému obsahuje

a) bezpečnostní směrnice informačního systému pro bezpečnostní správce
b) bezpečnostní směrnice informačního systému pro správce
c) bezpečnostní směrnice informačního systému pro uživatele

2.3.1 Bezpečnostní politika

Je základním dokumentem, který je zpracováván v počáteční fázi vývoje informačního systému a z tohoto dokumentu vycházejí další části celé dokumentace. Bezpečnostní politika definuje pravidla, normy a postupy, jakými je zajišťována bezpečnost, důvěrnost, integrita, dostupnost a případně i nepopiratelnost nebo pravost utajované informace a služeb celého systému. Určuje dále odpovědnost uživatelů, správců a bezpečnostních správců za jejich činnost v systému. Je formulována na základě minimálních bezpečnostních požadavků v oblasti počítačové bezpečnosti, uživatelských požadavků, výsledků provedené analýzy rizik, případně s ohledem na již existující bezpečnostní politiku nadřízeného orgánu a z ní vyplývající bezpečnostní požadavky.

Pro informační systémy nakládajícími s utajovanými informacemi stupně utajení Důvěrné a vyšší platí pro minimální bezpečnostní požadavky podmínky §7 vyhlášky č. 523/2005 Sb. a musí být zajištěna bezpečnostní funkce jako je jednoznačná identifikace uživatele informačního systému, zaznamenávání veškeré činnosti a událostí schopných ovlivnit bezpečnost informačního systému do auditního protokolu, zabezpečení auditního protokolu před neoprávněným přístupem a manipulací, možnost zkoumání auditních záznamů, ochrana důvěrnosti dat během přenosu mezi zdrojem a cílem, schopnost ošetřovat paměťový prostor a jeho další využívání, tak, aby nemohlo dojít ke zjištění předchozího obsahu.

V informačním systému pro utajované informace do stupně utajení Vyhrazené se musejí využívat popsané bezpečnostní funkce v přiměřené míře doplněné o personální, administrativní a fyzickou bezpečnost informačního systému.

Součástí bezpečnostní politiky informačního systému jsou výsledky provedené analýzy rizik.

Bezpečnostní provozní mód

V bezpečnostní politice musí být uveden bezpečnostní provozní mód. Jedná se o typ a především vlastnosti prostředí, ve kterém systém a uživatelé tohoto systému pracují. IS musí být v některém ze čtyř provozních módů provozován.

Bezpečnostní provozní módy:

a) **vyhrazený**

Prostředí umožňující zpracovávání informací různých stupňů utajení, uživatelé systému musejí splňovat veškeré podmínky pro přístup k utajované informaci s nejvyšším stupněm utajení, která se v systému nachází a současně musejí být oprávněni k seznámení, případně k práci se všemi utajovanými informacemi v systému. Název bezpečnostního provozního módu „Vyhrazený“ nesouvisí se stupněm utajení „Vyhrazený“.

Pro lepší představu si můžeme uvést příklad, kdy uživatelé budou používat stejné úložiště dokumentů. Každý uživatel se tedy může seznámit s jakýmkoli dokumentem a v něm obsaženými informacemi.

b) **s nejvyšší úrovní**

V tomto prostředí je možné zpracovávat informace různého stupně utajení, přičemž uživatelé musejí splňovat podmínky pro přístup k informaci s nejvyšším stupněm utajení, která se v systému nachází, ale všichni uživatelé nemusejí být oprávněni se seznamovat nebo pracovat se všemi utajovanými dokumenty v systému.

c) **s nejvyšší úrovní s formálním řízením přístupu k informacím**

Odpovídá bezpečnostnímu provoznímu módu s nejvyšší úrovní, ale navíc se zde předpokládá centrální řízení a kontrola přístupu

d) **víceúrovňový**

Prostředí umožňuje současné zpracování utajovaných informací různých stupňů utajení, všichni uživatelé nemusejí splňovat podmínky pro přístup k utajované informaci s nejvyšším stupněm utajení, která je v systému obsažena, ale nemusejí být všichni uživatelé oprávněni pracovat se všemi utajovanými informacemi v systému. U systému provozovaných v tomto provozním módu je věnována zvláštní pozornost možnosti systému zabezpečit řízení přístupu subjektů k objektům systému na základě jejich oprávnění a pověření. Dále schopnosti jasně a přesně označit vystupující informaci příslušným stupněm utajení a u vstupující informace možnosti jejího označení stupněm utajení. U systému pracující s informacemi klasifikace Přísně tajné musí být provedena analýza skrytých kanálů. Je to

identifikace a analýza možné skryté a závadové komunikace, kterou by bylo možné se neoprávněně dostat k utajované informaci nebo součásti informačního systému.

2.3.2 Návrh bezpečnosti informačního systému

Navazujícím dokumentem na bezpečnostní politiku je návrh bezpečnosti informačního systému. Tento návrh uvádí a upřesňuje prostředky jakými budou dosaženy cíle bezpečnostní politiky. Uvádějí se zde již konkrétní hardwarové specifikace zařízení a sestav, softwarové vybavení, prostředky zajištění jednoznačné identifikace a autentizace uživatelů systému.

Také tu jsou konkretizovány způsoby fyzického zabezpečení informačního systému, umístění systému, jeho zajištění proti neoprávněné manipulaci, zajištění a vedení kabeláže, ochrana proti úniku utajovaných informací v důsledku kompromitujícího vyzařování. Pozornost je věnována i samotnému napájení zařízení, kde jsou kladeny požadavky na vysokofrekvenční filtraci, především u vyšších stupňů utajení.

Dále tu jsou rozvedeny oblasti personální a administrativní bezpečnosti.

Při návrhu jsou zohledňovány závěry a výsledky provedené analýzy rizik. Podrobnosti nastavení samotného operačního systému bývají uvedené v příloze návrhu, v *Nastavení bezpečnostních charakteristik OS*.

II. PRAKTICKÁ ČÁST

3 NÁVRH INFORMAČNÍHO SYSTÉMU

V praktické části diplomové práce se budu zabývat především návrhem projektu informačního systému, který bude určen pro nakládání s utajovanými informacemi stupně utajení Vyhrazené. U systémů, které mají za úkol chránit citlivé informace, je nanejvýš důležité, aby jejich dokumentace nebyla veřejně přístupná a seznamovaly se sní, resp. s jejími částmi jen ty osoby, které jsou oprávněny s takovým systémem pracovat a byly seznámeny s dokumentací jen v nezbytně nutném rozsahu.

Popisovaný návrh informačního systému vychází z veřejných informací, dokumentů a zkušeností a vznikl pro potřeby této práce.

4 PROJEKTOVÁ BEZPEČNOSTNÍ DOKUMENTACE

4.1 Bezpečnostní politika

BEZPEČNOSTNÍ POLITIKA

Informačního systému **V**ÁCLAV

Vypracoval: Bc. Martin Kuška Dne: 26.4.2012

1 POPIS SYSTÉMU

Informační systém (dále jen IS) je navržen pro zpracování a ukládání utajovaných informací do stupně utajení VYHRAZENÉ v malém rozsahu. Základním účelem zpracování utajovaných informací na tomto IS je potřeba zpracovávat utajované části dokumentace zakázek firmy. Informační systém je provozován v bezpečnostním módu s nejvyšším zabezpečením na samostatném, nepřenosném osobním počítači, který je součástí níže upřesněné počítačové sestavy. Informační systém není připojen do žádné počítačové sítě ani jinak propojen s dalším osobním počítačem.

Počítačová sestava se skládá z monitoru, samostatné jednotky počítače, klávesnice a myši. K sestavě je připojena černobílá laserová tiskárna a záložní napájecí zdroj. Napájení celé sestavy je realizováno přes přepěťovou ochranu s odrušovacím vysokofrekvenčním filtrem. Pevný disk počítače je pevně zabudován v počítačové skříni, která je opatřena pečetěmi proti neoprávněnému otevření a manipulaci se zabudovanými komponenty.

Výstup informací ze systému je možný v tištěné formě nebo elektronické podobě na evidovaném paměťovém médiu.

Informační systém je provozován na operačním systému Microsoft Windows XP. Jako aplikační software je použit lokalizovaný standardní kancelářský software pro tvorbu a editaci dokumentů. Operační systém je doplněn softwarem pro antivirovou kontrolu (antivir) a softwarem pro bezpečné mazání.

U informačního systému se předpokládá využití deseti uživateli.

Bezpečnostní cíl informačního systému je zajištění integrity, důvěrnosti, dostupnosti utajované informace, dostupnosti služeb informačního systému a odpovědnosti uživatele za jeho prováděnou činnost v IS.

Zpracovávání utajovaných informací musí probíhat v souladu se zákonem č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti a s vyhláškami NBÚ v platném znění.

2 PERSONÁLNÍ BEZPEČNOST

Základním předpokladem pro zajištění bezpečnosti systému a informací v něm obsažených je oddělení jednotlivých rolí.

2.1. Role v informačním systému

V informačním systému jsou zavedeny celkem tři role:

1. **Bezpečnostní správce**
   - je pověřen pro nejvyšší stupeň utajení informace, jaká se může v systému nacházet
   - povinnosti bezpečnostního správce jsou stanoveny v bezpečnostní dokumentaci IS
   - může vykonávat povinnosti Správce systému
2. **Správce systému**
   - spravuje operační systém, aplikační software, provádí hardwarovou údržbu
   - je pověřen pro nejvyšší stupeň utajení informace, jaká se může v systému nacházet
   - povinnosti správce systému jsou stanoveny v bezpečnostní dokumentaci IS
3. **Uživatel**
   - provádí zpracování informací
   - povinnosti a zakázané činnosti uživatele jsou uvedeny v uživatelské části bezpečnostní dokumentace

Z personálních důvodů a s přihlédnutím k faktu, že tento informační systém slouží ze zpracování utajovaných informací v malém rozsahu, je možné role bezpečnostního správce a správce sloučit a může je vykonávat jedna osoba.

Do informačního systému mají přístup pouze uživatelé kteří:

a) splňují požadavky dle zákona č. 412/2005 Sb. Pro přístup k utajované informaci stupně utajení Vyhrazené nebo vyšší (mají příslušné osvědčení nebo oznámení)
b) jsou písemně pověřeni k práci v tomto IS oprávněným vedoucím pracovníkem
c) jsou prokazatelně poučeni o přístupu k utajovaným informacím podle zákona č. 412/2005 Sb.

d) jsou prokazatelně seznámeni/proškoleni s provozní dokumentací, platnost proškolení je 1 rok, pravidelné proškolení zajišťuje bezpečnostní správce IS

Uživatel je seznámen s nezbytnými informacemi vztahujícími se k IS, dle zásady „Need-To-Know“

Oprávnění uživatelé jsou vedeni v Evidenci uživatelů, obsahující údaje jako číslo jednací pověření kterým jsou do informačního systému zavedeni, datum platnosti Osvědčení nebo Oznámení, datum posledního proškolení. V případě zániku některého z dokumentů nebo lhůty je uživateli znemožněn přístup do IS.

Každý uživatel má v rámci IS jedinečné uživatelské jméno, pod kterým v rámci IS vystupuje. Přihlášení a přístup uživatele do informačního systému probíhá pomocí ověřovacích a řídících mechanismů operačního systému na základě přidělených oprávnění.

3 SPLNĚNÍ MINIMÁLNÍCH POŽADAVKŮ POČÍTAČOVÉ BEZPEČNOSTI

Informační systém využívá bezpečnostní funkce operačního systému. Všem aktivitám uživatele, správce systému a bezpečnostního správce předchází jednoznačná identifikace a autentizace, přihlášení se do IS na základě jednoznačného identifikátoru. Přístup k objektům IS je řízen systémem na základě přidělených přístupových práv.

4 Uživatelské účty

4.1.1. Zásady uživatelských účtů

- název uživatelského účtu je jedinečný
- u uživatele IS je název jeho uživatelského účtu tvořen příjmením, případně přidáním písmene z křestního jména za příjmení, vše bez diakritiky

4.1.2. Zásady hesla uživatelského účtu

- minimální délka 12 znaků

- musí splňovat podmínku komplexnosti, heslo musí obsahovat znaky ze tří z následujících čtyř skupin (malá písmena [a-z], velká písmena [A-Z], čísla [0-9], nečíselné znaky [např. #,!.*])
- nesmí obsahovat uživatelské jméno nebo jeho podstatnou část
- nesmí být lehce odvoditelné dle informací vztahující se k danému uživateli (např. jména dětí, značka auta)
- maximální platnost hesla je 90 dní
- posledních 24 hesel se nesmějí opakovat

4.1.3. Zásady uzamčení účtů

- po 3 neúspěšných pokusech o přihlášení dojde k uzamčení účtu
- po vypršení platnosti účtu (platnosti proškolení, platnosti pověření/prověrky)
- doba uzamčení účtu je neomezená, odemčení může provést pouze bezpečnostní správce

4.2. Přerušení činnosti a nečinnost

Po 30-ti minutové nečinnosti se stanice automaticky uzamkne a odemčení lze provést pouze novou autorizací. Při krátkodobém přerušení činnosti na stanici (do 30-ti minut) je uživatel povinen stanici též uzamknout a prostor zajistit před neoprávněnými osobami. Při delší nečinnosti, tj. nad 30 minut, je povinen řádně ukončit práci na IS.

4.3. Auditní záznamy

Pro monitorování činnosti v IS jsou využívány prostředky operačního systému, které umožňují automatické vytváření auditních záznamů a jsou vhodně nastaveny. Zaznamenávány jsou především úspěšné i neúspěšné pokusy o přihlášení do systému, správa uživatelských účtů a skupin, změny zabezpečení a neúspěšné pokusy o přístup k objektům a souborům, použití přístupových práv.

Zaznamenané auditní záznamy jsou přístupné pouze bezpečnostnímu správci. Bezpečnostní správce má povinnost minimálně 1 krát měsíčně auditní záznamy kontrolovat a zálohovat. Kontrolu auditních záznamů bezpečnostní správce provádí vždy po bezpečnostním incidentu či podezření na něj nebo jiné mimořádné události mající vliv na

bezpečnost systému. Auditní záznamy jsou archivovány po dobu minimálně 5 ti let od doby pořízení.

4.4. Požadavky na dostupnost

Dostupnost dat, především jejich zálohování bude prováděno samotným uživatelem. Uživatel si sám zálohuje svá vlastní data na evidované a označené nosiče utajovaných dat (paměťová média). Nosiče utajovaných informací ukládá v souladu s předpisy.

5 ANALÝZA RIZIK A DALŠÍ BEZPEČNOSTNÍ OPATŘENÍ

Specifickou hrozbou pro osobní počítač je získání fyzického přístupu neoprávněnou osobou, která může odcizit, zničit nebo poškodit paměťové médium s utajovanými informacemi. Dále může následovat získání neoprávněného logického přístupu do systému, toho lze docílit např. nastartováním do jiného operačního systému z cizího paměťového média (disketa, CD-ROM, USB disk) a získání utajované informace nebo jejích fragmentů, zbytkových informací za pomoci specializovaných prostředků.

S provozem výpočetní techniky souvisí nežádoucí elektromagnetické vyzařování obsahující utajovanou informaci jinak nazývané kompromitující vyzařování. Detekcí a analýzou kompromitujícího vyzařování může být neoprávněná osoba schopna rekonstruovat utajovanou informaci.

5.1. Analýza rizik

Tab. 6: Analýza rizik vyhodnocující pravděpodobnost ohrožení

Aktivum	Hodnota	Hrozba	Zranitelnost	Pravděpodobnost incidentu	Dopad	Riziko	Opatření
Počítačová sestava	5	Selhání HW	Prach, vlhkost, přepětí v síti, otřesy	3	5	15	Vyvýšené umístění, přepěťová ochrana
		Selhání SW	Škodlivé kódy, vyměnitelná média	3	4	12	Antivir, administrativní bezpečnost

		Krádež	Nedostatečné fyzické zabezpečení	3	5	15	
		Požár	Kouření na pracovišti, elektrická závada	2	5	10	Nekuřácké pracoviště, pravidelná revize
		Vytopení	Rozvody vody, topení	1	4	4	Vyvýšené umístění
Uživatelská data	5	Neúmyslná modifikace	Nedostatečné proškolení a výcvik	5	5	25	Pravidelné školení, počítačová gramotnost
		Úmyslná modifikace	Nedostatek fyzického zabezpečení, nedostatečné zabezpečení operačního systému	4	5	20	Opatření personální a fyzické bezpečnosti, vhodné zabezpečení OS
		Vyzrazení UI kompromitujícím vyzařováním	Nevhodné umístění zařízení, nedovolené komponenty	3	5	15	Dodržení minimálních vzdáleností
		Vyzrazení UI odpozorováním	Nevhodné situování, přímá viditelnost okny na zařízení	3	5	15	Zneprůhlednění oken

5.2. Ochrana integrity hardware

K zajištění integrity HW jsou použity pečetě, které jsou umístěna na obalu HW tak, aby nebylo možné bez porušení krytu nebo pečetě zařízení otevřít a získat tak přístup k vnitřním komponentám nebo vně uložených paměťových médií. Pečetě jsou takové povahy, že při pokusu o jejich odstranění nebo překonání dojde zaručeně k jejich viditelnému poškození.

5.3. Ochrana integrity operačního systému a software

Pro případ zamezení neoprávněného logického přístupu do operačního systému a případné neoprávněné modifikace nebo vložení škodlivého kódu do operačního systému nebo SW, jsou pro nastartování systému znemožněny všechny ostatní možnosti (disketa, CD-ROM, LAN) kromě systémového pevného disku.

5.4. Kompromitující vyzařování

Nežádoucímu zachycení kompromitujícího vyzařování počítačové sestavy a připojených periferních zařízení se zabraňuje vhodným umístěním informačního systému a volbou vyhovujících zařízení.

Všechna zařízení, která jsou součástí informačního systému, musejí splňovat požadavky na elektrickou bezpečnost a elektromagnetickou kompatibilitu dle zákona[1], zařízení musejí mít tzv. "Prohlášení o shodě".

5.5. Bezpečné používání paměťových médií USB

Pro zajištění uživatelského komfortu je povoleno za dodržení určitých podmínek a postupů použití USB paměťových médií („flash disků“). Možnost používání USB médií je podmíněno:

a) instalací NBÚ schváleného softwaru 3. strany na kontrolu, audit a řízení přístupu USB zařízení, umožňující selektivní přístup k prostředku
b) prováděním auditu užití prostředku
c) zavedení principu „White List“, je primárně nastavena nejvyšší úroveň zabezpečení – všechna zařízení jsou zakázána a do seznamu se přidávají výjimky/povolená zařízení
d) připojit lze jen USB média, která umožňují jednoznačnou identifikaci[2]
e) USB média jsou řádně označena a evidována

6 FYZICKÁ BEZPEČNOST

Informační systém je instalován na režimovém pracovišti v zabezpečené oblasti kategorie VYHRAZENÉ (dále jen „pracoviště systému“).

Samostatně vstupovat do místnosti pracoviště systému jsou pouze bezpečnostní správce a oprávněný uživatel informačního systému (dále jen „oprávněné osoby“). Ostatní osoby mohou do prostoru pracoviště systému vstupovat a zdržovat se v něm pouze za doprovodu oprávněné osoby a jen nezbytně nutnou dobu. Osoby, které nejsou oprávněny

1 Zákon č. 22/1997 Sb. o technických požadavcích na výrobky a o změně a doplnění některých zákonů.
2 USB zařízení obsahuje položku Serial Number (SN), jednoznačnou identitu tvoří trojice Vendor ID (VID), Product ID (PID), Serial Number (SN)

samostatně vstupovat do místnosti, jsou povinny zapsat se do „knihy návštěv“. Povinností oprávněné osoby je zajistit, aby nemohlo dojít k neoprávněnému seznámení s utajovanými informacemi.

V době nepřítomnosti oprávněných osob je pracoviště systému uzamčeno a řádně zajištěno dle příslušného projektu fyzické bezpečnosti.

Klíče od místnosti jsou v souladu s projektem fyzické bezpečnosti řádně označeny, uloženy a vydávány pouze oprávněným osobám proti podpisu ostrahou objektu.

Umístění počítačové sestavy je provedeno tak, aby bylo znemožněno odezírání utajované informace z obrazovky, klávesnice a tiskárny nepovolanými osobami. Jsou učiněna i další opatření proti odezírání jako je instalace tzv. mléčných skel, fólií nebo aplikace přípravku pro zneprůhlednění skleněných tabulí (např. „ledové květy“). Při umisťování sestavy je dodržena minimální vzdálenost 0,5 m od ostatních elektrických spotřebičů a metalického vedení a rozvodů v místnosti, zejména rozvodů elektřiny, telefonu, datových rozvodů, topení, rozvodů vody.

7 ADMINISTRATIVNÍ BEZPEČNOST

7.1. Paměťová média, nosiče utajovaných informací

Veškerá paměťová média využívaná při provozu informačního systému (včetně zabudovaného pevného disku) jsou řádně označena a evidována v administrativní pomůcce vytvořené pro tento účel (Evidence médií).

Pokud je paměťové médium určeno k uložení utajované informace (nosič utajované informace), je takové médium označeno a evidováno jako utajovaná písemnost nelistinného charakteru v souladu s platnou vyhláškou[1].

Nosiče utajovaných informací mohou být použity výhradně v tomto informačním systému.

Nepotřebné a vadné nosiče utajovaných informací jsou fyzicky zničeny v souladu s vyhláškou. O fyzickém zničení je proveden záznam s podpisy nejméně dvou pracovníků, kteří zničení provedli. Snižování stupně utajení nosičů utajovaných informací je zakázáno.

1 Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací

7.2. Ukládání utajovaných informací

Veškeré výstupy utajované informace z informačního systému (tištěné i elektronické) musejí být řádně označeny odpovídajícím stupněm utajení a způsobem dle platných předpisů. Všechny tiskové výstupy jsou bez odkladu řádně evidovány jako utajované písemnosti nebo okamžitě skartovány na certifikovaném zařízení. Výstupy utajované informace jsou ukládány u úschovných objektech k tomuto účelu určených v příslušné zabezpečené oblasti.

8 SERVISNÍ ČINNOST

Servisní činnost musí být prováděna tak, aby nemohlo dojít k neoprávněnému seznámení s utajovanou skutečností, případně nemohlo dojít k narušení integrity hardwaru nebo softwaru vedoucí ke kompromitaci utajované informace.

Před vlastní opravou musejí být z pracovní stanice vyjmuty všechny vyměnitelné nosiče informací (disketa, CD/DVD, paměťová média USB).

Opravy jsou prováděny pokud možno na pracovišti systému správcem IS nebo vlastními pracovníky společnosti za dozoru bezpečnostního správce.

Pokud se oprava týká části osobního počítače obsahující pevný disk a opravu neprovádí správce IS, musí být pevný disk před opravou vyjmut.

Pokud oprava vyžaduje použití pevného disku a není prováděna správcem, musí být:

a) prováděna na pracovišti IS
b) osobou, která má prověrku příslušného stupně utajení
c) za dozoru bezpečnostního správce

Při opravě smějí být použity pouze takové komponenty, které splňují prohlášení o shodě a jsou typově stejné s původními komponenty.

O každém servisním zásahu je proveden záznam. Záznamy jsou uchovávány nejméně 5 let.

9 BEZPEČNOSTNÍ INCIDENTY A KRIZOVÉ SITUACE

9.1. Bezpečnostní incident

Za bezpečnostní incident se považuje:

a) porušení bezpečnostních směrnic
b) porušení ochranného prvku
c) neoprávněná změna hardwarové nebo softwarové konfigurace
d) neoprávněné nakládání s utajovanými informacemi zpracovávanými v systému
e) úmyslné nebo neúmyslné vyzrazení utajované informace neoprávněné osobě
f) projev počítačového viru nebo jiného zlomyslného softwaru
g) ztráta nosiče informací, který je v informačním systému používán
h) neoprávněné nakládání s nosiči informací používanými v informačním systému
i) kompromitace hesla uživatelského účtu
j) ztráta klíčů od místnosti pracoviště informačního systému
k) proniknutí nepovolané osoby do místnosti s IS nebo pokusy o proniknutí
l) jiné události, které mohou mít vliv na důvěrnost, integritu nebo dostupnost utajované informace zpracovávané v informačním systému

O všech bezpečnostních incidentech je neprodleně vyrozuměn bezpečnostní správce informačního systému, který rozhodne o dalším postupu. Do rozhodnutí bezpečnostního správce nesmí být na sestavě pokračováno v práci nebo v práci započato.
O bezpečnostním incidentu musí být proveden záznam. Záznamy jsou uchovávány nejméně 5 let.

9.2. Krizové situace

Krizovou situací se považuje:

- požár na pracovišti informačního systému nebo v budově
- přírodní katastrofa
- sabotáž
- teroristický útok nebo jeho hrozba
- záplava, prosakování tekutin
- další obdobné situace mající vliv na dostupnost IS

V případě vzniku krizové situace musí být bezpečnostním správcem zajištěna taková opatření, aby nedošlo k ohrožení utajovaných informací.
O krizové situaci musí být proveden záznam. Záznamy jsou uchovávány nejméně 5 let.

10 DALŠÍ BEZPEČNOSTNÍ DOKUMENTACE

Na bezpečnostní politiku informačního systému navazuje další dokument z projektové bezpečnostní dokumentace a to Návrh bezpečnosti informačního systému.
Provozní bezpečnostní dokumentaci informačního systému tvoří:

a) Bezpečnostní směrnice bezpečnostního správce
b) Bezpečnostní směrnice správce
c) Bezpečnostní směrnice uživatele

Jednotlivé bezpečnostní směrnice jsou zpracovány odděleně, aby nedocházelo k seznamování se s informacemi, které nejsou k výkonu role v systému nezbytné.

4.2 Návrh bezpečnosti

NÁVRH BEZPEČNOSTI

Informačního systému **V**ÁCLAV

Vypracoval: Bc. Martin Kuška Dne: 26.4.2012

1 POPIS HARDWAROVÉHO A SOFTWAROVÉHO VYBAVENÍ

1.1. Konfigurace HW:

- samostatné PC Autocont OfficePro 1000 (H61, DDR3, mikro)
  - skříň Mikro YY-3606 černo/šedá
  - Zdroj 300W
  - GIGABYTE H61, 1xDVI (1xS, P)
  - CPU Intel® Pentium G620 (int. VGA)
  - paměť RAM 2GB DDR3 1333MHz (2x1GB)
  - HDD SATA2 320GB
  - čtečka karet + USB černá
  - DVDRW/RAM LG černá SATA
  - Klávesnice Microsoft černá, USB
  - Myš Microsoft optická černá, USB
- monitor - 22" LCD iiyama E2208HDS – 16:9,DVI,2ms,Repro
- č/b laserová tiskárna Hewlett-Packard LaserJet P2035
- UPS Back-UPS RS 500VA/300W
- přepěťový a vysokofrekvenční filtr APC Essential SurgeArrest 5 outlets 230V

1.2. Konfigurace SW:

- operační systém Windows XP Professional, SP3 (downgrade z Windows 7 Professional CZ)
- software pro bezpečné používání USB paměťových zařízení OptimAccess
- kancelářský software Microsoft Office nebo OpenOffice.org
- prohlížeč PDF souborů Adobe Acrobat Reader
- antivirový software Microsoft Security Essentials
- software pro bezpečné mazání Blancco – File Shredder

2 POČÍTAČOVÁ BEZPEČNOST

2.1. Identifikace a autentizace uživatele

Jednoznačná identifikace a autentizace uživatele je prováděna prostředky operačního systému. Operační systém má vhodně nastaveny bezpečnostní parametry.

Při krátkodobém opuštění zapnutého počítače dojde k uzamčení pracovní stanice a další používání stanice je umožněno až po opakované identifikaci a autentizaci uživatele. Volitelné řízení přístupu k objektům IS je řízeno prostředky operačního systému.

Auditní záznamy jsou vytvářeny prostředky operačního systému. Jsou zaznamenávány úspěšné i neúspěšné pokusy o přihlášení do systému, správu uživatelských účtů a skupin, změny zabezpečení a neúspěšné pokusy o přístup k souborům a objektům, použití přístupových práv. K auditním záznamům má přístup pouze bezpečnostní správce.

K podpoře auditních záznamů slouží provozní deník, do kterého uživatel zapisuje svou činnost v informačním systému

Kontrola a zálohování auditních záznamů je prováděna minimálně jednou v kalendářním měsíci. Záloha auditních záznamů je uchovávána po dobu 5ti let u bezpečnostního správce.

3 PERSONÁLNÍ BEZPEČNOST

Aktuální seznam uživatelů je veden bezpečnostním správcem. V seznamu jsou uvedeny především tyto údaje: celé jméno, číslo osvědčení, pro jaký stupeň utajení platí, konec platnosti osvědčení

3.1. Pověření osob vyžadované bezpečnostní politikou

Pověření osob vyžadované bezpečnostní dokumentací (bezpečnostní správce, správce) písemně provádí vedoucí pracovník s personální pravomocí.

3.2. Uživatelé, pověření a odvolávání

3.2.1. Pověření

Pověření uživatelů k práci v informačním systému schvaluje vedoucí pracovník s personální pravomocí. Pověření je písemnou formou a je adresováno bezpečnostnímu správci IS.

3.2.2. Odvolání, zamezení přístupu

Odvolání uživatele z IS schvaluje vedoucí pracovník s personální pravomocí. Odvolání v písemné podobě je adresováno bezpečnostnímu správci. Na základě odvolání provede bezpečnostní správce zrušení a smazání účtu uživatele.

V případě zániku Osvědčení nebo Oznámení uživatele nebo při výskytu skutečnosti, která je v rozporu s personální bezpečností, je povinností samotného uživatele nebo jeho přímého nadřízeného oznámit tyto skutečnosti bezpečnostnímu správci.

3.2.3. Bezpečnostní školení

Bezpečnostní školení uživatelů provádí a organizuje bezpečnostní správce. Školení je pravidelně prováděno minimálně 1x ročně a před skutečným zavedením uživatele do systému. Uživatel pochopení a znalost bezpečnostních směrnic stvrzuje svým podpisem.

3.2.4. Uložení identifikátoru a hesla administrátorského účtu

Název administrátorského účtu a platné heslo je pro výjimečné případy uloženo v zapečetěné obálce u vedoucího s personální pravomocí v trezoru určeném pro uchovávání utajovaných informací.

3.3. Požadavky na dostupnost

Zálohování dat provádí každý uživatel samostatně na evidované nosiče informací za dodržování pravidel pro nakládání s nosiči informací a nakládání s utajovanými informacemi.

4 ADMINISTRATIVNÍ BEZPEČNOST

Do informačního systému je možné vkládat pouze evidovaná média typu CD/DVD, USB flash disk.

Z informačního systému může informace vystupovat v tištěné podobě nebo v elektronické podobě zapsáním na CD/DVD nebo USB flash disk. Veškeré výstupy utajované informace ze systému musejí být bez odkladu řádně označeny stupněm utajení a evidovány dle platných předpisů

Veškeré vkládané nosiče informace musejí být řádně evidovány v administrativní pomůcce a označeny dle platné vyhlášky. V případě, že se na médiu nachází uložená utajovaná informace, je s tímto nosičem utajované informace zacházeno jako s utajovanou písemností nelistinného charakteru v souladu s platnou vyhláškou[1].

Vyjímatelné nosiče utajovaných informací (CD/DVD, USB disk) jsou ukládány v úschovném trezoru příslušné kategorie.

4.1. Evidence vedené v IS

a) seznam uživatelů a jejich proškolení – veden a je uložen u bezpečnostního správce
b) seznam osob spravující IS – u bezpečnostního správce
c) evidence médií – vedena a je uložena u bezpečnostního správce
d) provozní deník – uložen u sestavy, záznamy o vadách, incidentech, činnost jednotlivých uživatelů
e) deník bezpečnostního správce – stupeň utajení VYHRAZENÝ, záznamy a činnost bezpečnostního správce IS
f) deník správce – stupeň utajení VYHRAZENÝ, záznamy a činnost správce IS

4.2. Bezpečnostní provozní dokumentace

Provozní bezpečnostní dokumentaci informačního systému tvoří:

a) Bezpečnostní směrnice bezpečnostního správce
b) Bezpečnostní směrnice správce
c) Bezpečnostní směrnice uživatele

Jednotlivé bezpečnostní směrnice jsou zpracovány odděleně, aby nedocházelo k seznamování se s informacemi, které nejsou k výkonu role v systému nezbytné.

1 Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací

5 FYZICKÉ ZABEZPEČENÍ IS

Zabezpečení prostoru, ve kterém se nachází informační systém, je dle projektu fyzické bezpečnosti objektu.

Informační systém je umístěn v suterénní místnosti A.03 podléhající režimovým opatřením. Vstup do místnosti je zaznamenáván do administrativní pomůcky Evidence vstupů. Do této evidence jsou povinny se zapsat a podepsat všechny osoby vstupující do místnosti. Záznam musí obsahovat celé jméno a podpis, čas vstupu a opuštění místnosti a důvod vstupu.

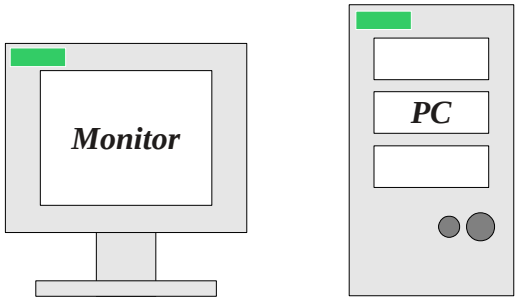
Pro případ uložení vyměnitelných médií s utajovanými informacemi se v místnosti nachází schválený trezor. Otevření trezoru provádí osoba pověřená vedením evidence utajovaných informací. V trezoru má každý oprávněný uživatel svou zapečetěnou schránku, do které ukládá své utajované písemnosti a nosiče utajovaných informací (vyměnitelných médií).

Ochrana integrity hardwarového vybavení je chráněna speciálními holografickými pečetěmi s vlastním pořadovým (evidenčním) číslem. Pečetě jsou umístěny na krytech zařízení tak, aby nemohlo dojít k jeho otevření bez jejich porušení

Obr. 4: Příklad hologramové bezpečnostní plomby s evidenčním číslem

Označení počítačové sestavy informativním štítkem je vyvedeno v zelené barvě. Na štítku je vyznačen název informačního systému a nejvyšší stupeň utajení informací, které je na něm možné zpracovávat.

Obr. 5: Informativní štítek



Obr. 6: Umístění informativních štítků na PC sestavě

Rozmístění zařízení v místnosti je provedeno s ohledem na možnost odezírání utajovaných informací a kompromitující elektromagnetické vyzařování.

5.1. Kompromitující vyzařování

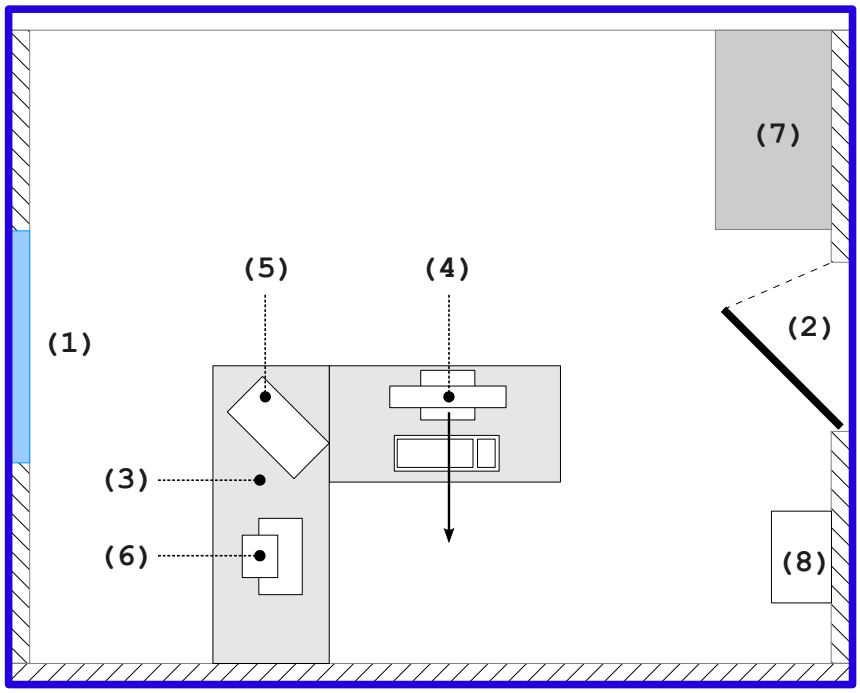
Všechna zařízení, která jsou součástí počítačové sestavy a informačního systému, splňují požadavky na elektrickou bezpečnost a elektromagnetickou kompatibilitu dle zákona a mají prohlášení o shodě a jsou tedy hodnocena jako zařízení třídy 2.

Celá počítačová sestava je napájena přes schválený přepěťový a vysokofrekvenční filtr komerčního typu s minimálním útlumem 20dB v kmitočtovém pásmu 100 kHz až 20 MHz.

U instalace jednotlivých zařízení je dodržena minimální bezpečnostní vzdálenost 0,5 m od cizích elektrických zařízení, metalické kabeláže a rozvodů.

5.2. Nákres pracoviště systému

Místnost A.03



Obr. 7: Nákres pracoviště systému

Legenda:

1. Okno
2. Dveře, vstup do místnosti
3. Pracovní stůl
4. Monitor s vyznačeným směrem natočení
5. Počítač
6. Tiskárna
7. Trezor
8. Skartovací zařízení

Hranice zabezpečené oblasti

4.3 Nastavení bezpečnostních charakteristik OS

Nastavení bezpečnostních charakteristik OS

Informačního systému **V**ÁCLAV

Vypracoval: Bc. Martin Kuška Dne: 26.4.2012

1 NASTAVENÍ BIOS

1.1. Priorita startování systému

Priorita zařízení ze kterých bude systém startován je nastavena na pevný disk (HDD0). Ostatní možné zařízení a způsoby jsou zakázány nebo potlačeny.

1.2. Ochrana heslem

Přístup do BIOS a ochrana nastavení je nastavením hesla pro přístup (*Set Supervisor Password*)

Heslo musí mít maximální možnou délku, které je BIOS schopen.

1.3. Integrovaná síťová karta

V případě integrované síťové karty je tato deaktivována.

2 OPERAČNÍ SYSTÉM

2.1. Instalace

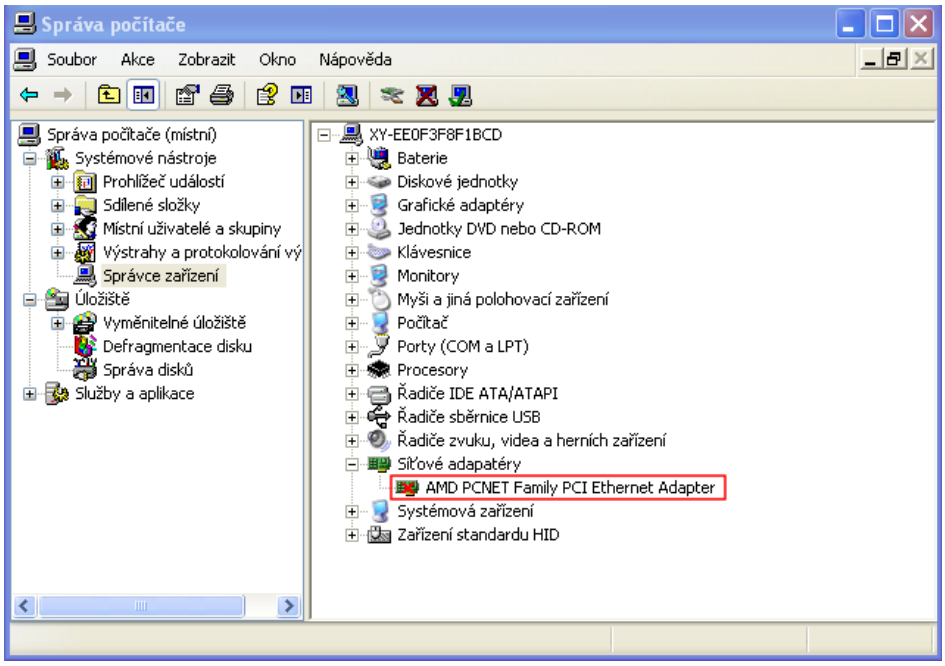
Instalace operačního systému je prováděna výhradně z originálních instalačních médií Microsoft Windows XP s posledním balíkem aktualizací Service Pack 3 na zcela zformátovaný pevný disk počítače. Na pevném disku bude vytvořen jeden oddíl o velikosti 20 GB a zformátován souborovým systémem NTFS.

Samotná instalace je provedena standardní postupem s využitím instalačního průvodce a jsou ponechány všechna výchozí nastavení.

Do operačního systému z dodaných instalačních médií výrobce nahrajte všechny nezbytné ovladače hardwaru.

2.2. Síťové rozhraní

Pokud nelze síťovou kartu zakázat již v BIOS, musí být zakázána ve Správci zařízení. Ve Správci zařízení rozevřete položku „Síťové adaptéry“ a zde přes pravé tlačítko myši všechny adaptéry zakažte.



2.3. Přejmenování výchozích účtů

Ve výchozím stavu je po instalaci vytvořen účet správce s nejvyššími právy na lokálním systému s názvem „administrator“ a účet hosta s názvem „guest“. Tyto účty musejí být přejmenovány. Přejmenování bude provedeno aplikací níže popsanou šablonou zabezpečení, ve které je nutné odkomentovat a doplnit hodnoty položek `NewAdministratorName` a `NewGuestName`. Mezi uvozovky doplňte nové názvy pro tyto účty.

```
NewAdministratorName = "Nove uzivatelske jmeno Administratora"
NewGuestName = "Nove uzivatelske jmeno Guesta"
```

2.4. Šablona zabezpečení

Na operační systém je aplikována šablona zabezpečení vycházející z certifikované šablony zabezpečení dle standardu Common Criteria.

Výpis šablony zabezpečení:

```
; (c) Microsoft Corporation 1997-2007
;
; Security Configuration Template for Security Configuration Editor
;
; Sablona zabezpeceni IS Vaclav, zalozena na certifikvane sablone Common Criteria pro Microsoft
; Windows XP CC_HiSec_XP_Professional_V3.inf
;
;

[Version]
signature="$CHICAGO$"
Revision=1

[Unicode]
Unicode=yes


[System Access]
;-------------------------------------------------------------------------------
;Account Policies - Password Policy.
;-------------------------------------------------------------------------------
MinimumPasswordAge = 2
MaximumPasswordAge = 90
MinimumPasswordLength = 12
PasswordComplexity = 1
PasswordHistorySize = 24
ClearTextPassword = 0

;-------------------------------------------------------------------------------
;Network Access: Allow anonymous SID/Name translation (Disabled)
;-------------------------------------------------------------------------------
LSAAnonymousNameLookup = 0

;-------------------------------------------------------------------------------
;Accounts: Administrator account status (Enabled)
;-------------------------------------------------------------------------------
EnableAdminAccount = 1

;-------------------------------------------------------------------------------
;Accounts: Guest account status (Disabled)
;-------------------------------------------------------------------------------
EnableGuestAccount = 0

;-------------------------------------------------------------------------------
;Account Policies - Lockout Policy.
;-------------------------------------------------------------------------------
LockoutBadCount = 3
ResetLockoutCount = 99999
LockoutDuration = -1

;-------------------------------------------------------------------------------
;Network security - Force logoff when logon hours expire.
;-------------------------------------------------------------------------------
ForceLogoffWhenHourExpire = 1
```

```
;-------------------------------------------------------------------------------
;NewAdministratorName = "Nove uzivatelske jmeno Administratora"
;NewGuestName = "Nove uzivatelske jmeno Guesta"


;-------------------------------------------------------------------------------
;Local Policies - Audit Policy.
;-------------------------------------------------------------------------------
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 3
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 3
AuditDSAccess = 3
AuditAccountLogon = 3

;-------------------------------------------------------------------------------
;Local Policies - User Rights Assignment.
;-------------------------------------------------------------------------------
[Privilege Rights]
seassignprimarytokenprivilege = *S-1-5-20,*S-1-5-19
seauditprivilege = *S-1-5-20,*S-1-5-19
sebackupprivilege = *S-1-5-32-551,*S-1-5-32-544
sebatchlogonright =
secreatepagefileprivilege = *S-1-5-32-544
secreatetokenprivilege =
sedebugprivilege =
seenabledelegationprivilege =
seincreasequotaprivilege = *S-1-5-20,*S-1-5-19,*S-1-5-32-544
seinteractivelogonright = *S-1-5-32-545,*S-1-5-32-547,*S-1-5-32-551,*S-1-5-32-544
semachineaccountprivilege =
semanagevolumeprivilege = *S-1-5-32-544
senetworklogonright = *S-1-5-32-544,*S-1-5-11,*S-1-5-32-551,*S-1-5-32-547,*S-1-5-32-545
seremoteinteractivelogonright =
serestoreprivilege = *S-1-5-32-551,*S-1-5-32-544
sesecurityprivilege = *S-1-5-32-544
sesystemenvironmentprivilege = *S-1-5-32-544
sesystemprofileprivilege = *S-1-5-32-544
sesystemtimeprivilege = *S-1-5-32-547,*S-1-5-32-544
setakeownershipprivilege = *S-1-5-32-544
setcbprivilege =
seloaddriverprivilege = *S-1-5-32-544
SeImpersonatePrivilege = *S-1-5-6,*S-1-5-32-544

;-------------------------------------------------------------------------------
;Local Policies - Security Options.
;-------------------------------------------------------------------------------
;-------------------------------------------------------------------------------
;Registry Values.
;-------------------------------------------------------------------------------
; Registry value name in full path = Type, Value
; REG_SZ                        ( 1 )
; REG_EXPAND_SZ                 ( 2 )  // with environment variables to expand
```

```
; REG_BINARY                  ( 3 )
; REG_DWORD                   ( 4 )
; REG_MULTI_SZ                ( 7 )

[Registry Values]
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLockedUserId=4,3
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=4,0
MACHINE\Software\Policies\Microsoft\Cryptography\ForceKeyProtection=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\ForceGuest=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\NoDefaultAdminOwner=4,1
MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths\Machine=7,
MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\Machine=7,
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes=7,SPOOLSS
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionShares=7,
MACHINE\System\CurrentControlSet\Control\Lsa\DisableDomainCreds=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous=4,0
MACHINE\System\CurrentControlSet\Control\Lsa\LimitBlankPasswordUse=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel=4,4
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinClientSec=4,537395248
MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0\NTLMMinServerSec=4,537395248
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous=4,1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM=4,1
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print
Services\Servers\AddPrinterDrivers=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Kernel\ObCaseInsensitive=4,1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect=4,15
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RestrictNullSessAccess=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\RequireSecuritySignature=4,0
MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\EnablePlainTextPassword=4,0
MACHINE\System\CurrentControlSet\Services\LDAP\LDAPClientIntegrity=4,2
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey=4,1
MACHINE\Software\Microsoft\Driver Signing\Policy=3,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD=4,0
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1


;-------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption=1,"VAROVÁNÍ"
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText=7,POZOR, přihlašujete
se do systému podléhající zákonu č. 412/2005 Sb., o ochraně utajovaných informací, pokud nejste
oprávněná osoba ukončete činnost - vystavuje se postihu!

MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\UndockWithoutLogon=4,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SecurityLevel=4,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\SetCommand=4,0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms=1,"1"
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateDASD=1,"0"
```

```
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies=1,"1"
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount=1,"0"
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\PasswordExpiryWarning=4,14
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScRemoveOption=1,"1"

;-------------------------------------------------------------------------------
;The following Registry value will shut down the system immediately if it is
;unable to log security audits.  While it is a recommended setting, it should
;only be enabled where there is a strict audit management process in place for
;reviewing, archiving, and clearing the audit log on a regular basis.
;-------------------------------------------------------------------------------
;MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1

;-------------------------------------------------------------------------------
;The following Registry values for auditing access of global system objects and
;backup and restore privileges will generate a large amount of audit events.
;While they are recommended settings, they should only be enabled where there is
;a strict audit management process in place for reviewing, archiving, and
;clearing the audit log on a regular basis.  The maximum log size should also be
;edited to support an increase in events being logged.
;-------------------------------------------------------------------------------
;MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects=4,1
;MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing=3,1


;-------------------------------------------------------------------------------
;Disable DirectDraw acceleration.  Also direct frame-buffer access is not permitted
;in order to prevent direct access to the graphics hardware by the application.
;-------------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\GraphicsDrivers\DCI\Timeout=4,0

;-------------------------------------------------------------------------------
;Remove POSIX subsystem.
;-------------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\optional=7,

;-------------------------------------------------------------------------------
;Disable unnecessary services.  These services do not appear in the Services
;interface.
;-------------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\audstub\Start=4,4
MACHINE\System\CurrentControlSet\Services\mnmdd\Start=4,4
MACHINE\System\CurrentControlSet\Services\NDProxy\Start=4,4
MACHINE\System\CurrentControlSet\Services\ParVdm\Start=4,4
MACHINE\System\CurrentControlSet\Services\PptpMiniport\Start=4,4
MACHINE\System\CurrentControlSet\Services\Ptilink\Start=4,4
MACHINE\System\CurrentControlSet\Services\RasAcd\Start=4,4
MACHINE\System\CurrentControlSet\Services\Rasl2tp\Start=4,4
MACHINE\System\CurrentControlSet\Services\Raspti\Start=4,4
MACHINE\System\CurrentControlSet\Services\Wanarp\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisTapi\Start=4,4
MACHINE\System\CurrentControlSet\Services\NdisWan\Start=4,4
MACHINE\System\CurrentControlSet\Services\RDPCDD\Start=4,4
MACHINE\System\CurrentControlSet\Services\rdpdr\Start=4,4
MACHINE\System\CurrentControlSet\Services\TermDD\Start=4,4
MACHINE\System\CurrentControlSet\Services\Atmarpc\Start=4,4
MACHINE\System\CurrentControlSet\Services\IRENUM\Start=4,4
```

```
MACHINE\System\CurrentControlSet\Services\NwlnkFwd\Start=4,4
MACHINE\System\CurrentControlSet\Services\NwlnkFlt\Start=4,4
MACHINE\System\CurrentControlSet\Services\rdpwd\Start=4,4
MACHINE\System\CurrentControlSet\Services\crcdisk\Start=4,4
MACHINE\System\CurrentControlSet\Services\wlbs\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDCOMP\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDFRAME\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDRELI\Start=4,4
MACHINE\System\CurrentControlSet\Services\PDRFRAME\Start=4,4
MACHINE\System\CurrentControlSet\Services\arp1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\nic1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\Ohci1394\Start=4,4
MACHINE\System\CurrentControlSet\Services\secdrv\Start=4,4
MACHINE\System\CurrentControlSet\Services\cdac15ba\Start=4,4
MACHINE\System\CurrentControlSet\Services\cdad10ba\Start=4,4
MACHINE\System\CurrentControlSet\Services\tdtcp\Start=4,4
MACHINE\System\CurrentControlSet\Services\wdica\Start=4,4
MACHINE\System\CurrentControlSet\Services\tdpipe\Start=4,4
MACHINE\System\CurrentControlSet\Services\mssmbios\Start=4,4
MACHINE\System\CurrentControlSet\Services\sacdrv\Start=4,4

;-------------------------------------------------------------------------------
;Ensure that non-Adminstrative users do not have access to raw sockets.  Default
;is no value present or 0.
;-------------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\AllowUserRawAccess=4,0

;-------------------------------------------------------------------------------
;Disable Remote Assistance feature of the Help and Support service.
;-------------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Control\Terminal Server\fEnableSalem=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowToGetHelp=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowUnsolicited=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\fAllowUnsolicitedFullControl=4,0
MACHINE\System\CurrentControlSet\Control\Terminal Server\RAUnsolicited=4,0

;-------------------------------------------------------------------------------
;Generate an audit event when the audit log reaches a percent full
;threshold. This policy is set to generate an audit event when the security event
;log is 90 percent full.  If this is not adequate for local use, the
;administrator may adjust the percentage value for this key according to local
;requirements.
;-------------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\WarningLevel=4,90

;-------------------------------------------------------------------------------
;Generate administrative alerts when audit log is full.  Edit this key as
;necessary to specify an appropriate authorized administrative account(s) to
;receive the administrative alerts.
;-------------------------------------------------------------------------------
MACHINE\System\CurrentControlSet\Services\Alerter\Parameters\AlertNames=7,Administrator

;-------------------------------------------------------------------------------
;Remove default IPSec exemptions.
;-------------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\IPSec\NoDefaultExempt=4,1
```

```
;-------------------------------------------------------------------------------
;Make screensaver password protection immediate.  Sets the value of this key
;entry to 0 in order to make password protection effective immediately.
;-------------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ScreenSaverGracePeriod=1,0

;-------------------------------------------------------------------------------
;Make sure Windows XP Professional is using an authenticated time service.
;-------------------------------------------------------------------------------
MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type=1,Nt5DS

;-------------------------------------------------------------------------------
;Disable autorun. Disables autorun capabilities on all drives.
;-------------------------------------------------------------------------------
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255


;-------------------------------------------------------------------------------
;Event Log - Log Settings
;-------------------------------------------------------------------------------
;Audit Log Retention Period:
;0 = Overwrite Events As Needed
;1 = Overwrite Events As Specified by Retention Days Entry
;2 = Never Overwrite Events (Clear Log Manually)

[System Log]
RestrictGuestAccess = 1

[Security Log]
MaximumLogSize = 16384
RestrictGuestAccess = 1

[Application Log]
RestrictGuestAccess = 1

;-------------------------------------------------------------------------------
;system Services - Disable Services not Included in Common Criteria Evaluated
;Configuration.
;-------------------------------------------------------------------------------
[Service General Setting]
TrkWks,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ClipSrv,4,"D:AR(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;OICI;CCLCSWRPLO;;;IU)
(A;OICI;CCLCSWLORC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
NetDDEdsdm,4,"D:AR(A;OICI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWWPLORC;;;AU)(A;OICI;CCLCSWRPLO;;;IU)
(A;OICI;CCLCSWLORC;;;PU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
SMTPSVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TrkSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
Fax,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
MSFTPSVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
mnmsrvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
```

```
NetDDE,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;IU)
(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)"
RasAuto,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
SNMPTRAP,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TlntSvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
TermService,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)
(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
UtilMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)"
xmlprov,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
WmdmPmSN,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;RP;;;IU)
(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
RDSessMgr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
ShellHWDetection,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)
(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
sacsvr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
Tssdis,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
uploadmgr,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
AudioSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
stisvc,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
UMWdf,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
(A;;CCLCSWLOCRRC;;;IU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
WZCSVC,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)
(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
AppMgmt,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLORC;;;AU)(A;;CCLCSWRPLO;;;IU)
(A;;CCLCSWLORC;;;PU)(A;;CCLCSWRPLO;;;BU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
FastUserSwitchingCompatibility,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)
(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
TapiSrv,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLO;;;BU)"
RasMan,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPWPDTLOCRRC;;;PU)"
RemoteAccess,4,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CR;;;AU)(A;;CCLCSWLOCRRC;;;IU)
(A;;CCLCSWRPWPDTLOCRRC;;;PU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)"

;-------------------------------------------------------------------------------
;Set audit at the %SystemRoot%\Tasks folder.  This ensures that the creation and
;modification of Scheduled Tasks objects is audited when object audit is enabled
;in the Security Policy.
;-------------------------------------------------------------------------------
[File Security]
"%SystemRoot%\Tasks",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)
(A;OICI;0x1200a9;;;BU)S:AR(AU;OICISAFA;DCLCDTSDWDWO;;;S-1-5-7)(AU;OICISAFA;DCLCDTSDWDWO;;;WD)"
[Profile Description]
Description=Sablona zabezpeceni IS Vaclav.
```

3 APLIKAČNÍ VYBAVENÍ

3.1. Antivirový program

Pro antivirovou kontrolu a ochranu nainstalujte produkt Microsoft Security Essentials.

3.2. Prohlížeč PDF souborů

Nainstalujte prohlížeč PDF[1] souborů, aplikaci Adobe Acrobat Reader ve standardní konfiguraci.

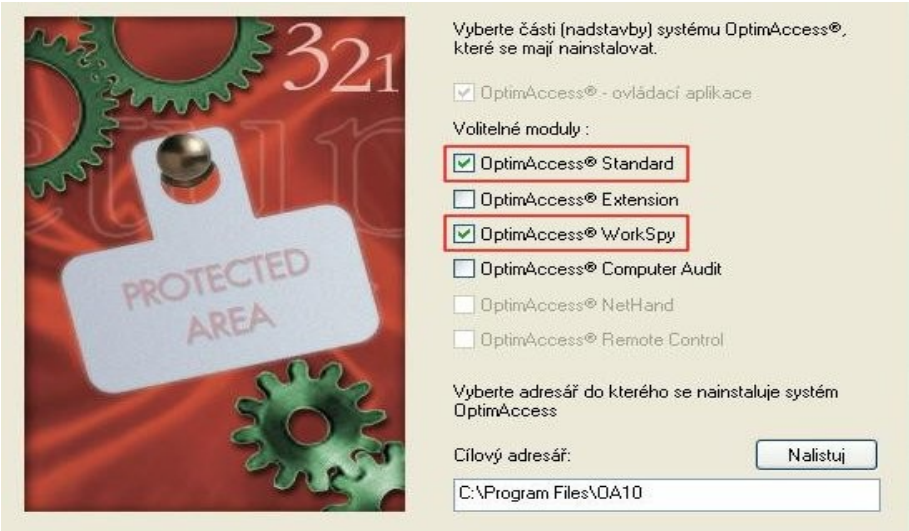
3.3. OptimAccess

Pro prosazování politiky bezpečného používání paměťových a jiných USB zařízení je v souladu s metodickým pokynem[2] Národního bezpečnostního úřadu a se závěry hodnocení[3] produktu použité softwarové řešení OptimAccess 10.5 od společnosti SODATSW spol. s r. o. Nastavení produktu vychází z metodického pokynu[4] NBÚ pro minimální nastavení softwarového produktu OptimAccess.

3.3.1. Instalace

Při instalaci vyberte pouze moduly Standard a WorkSpy, viz. obrázek č. 8.

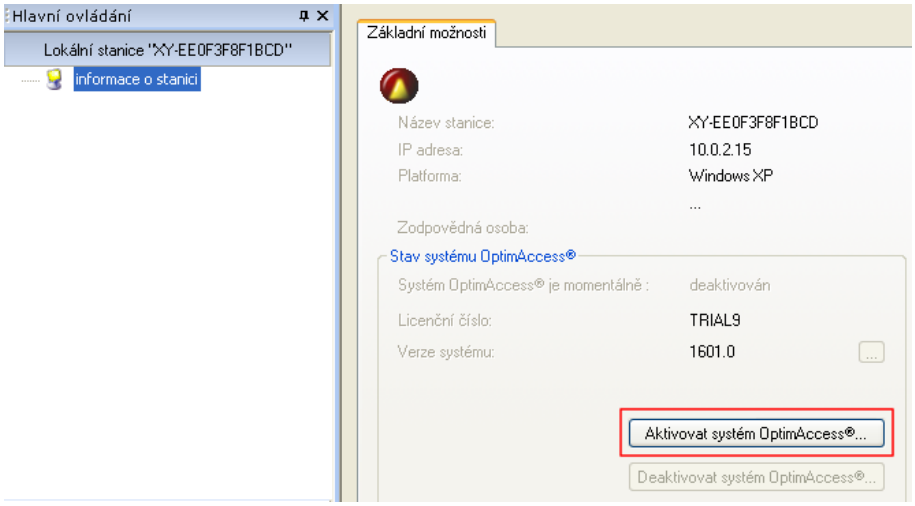
1 PDF – Portable Document Format, formát pro ukládání dokumentů nezávislých na softwaru i hardwaru kde byly vytvořeny
2 Používání FireWire a USB portů a bezpečnostní aspekty pamětí typu „flash“ (http://www.nbu.cz/download/nodeid-1009/)
3 Závěry hodnocení produktu OptimAccess (http://www.nbu.cz/download/nodeid-1107/)
4 Minimální nastavení produktu OptimAccess (http://www.nbu.cz/download/nodeid-1057/)



Obr. 8: OptimAccess - výběr modulů k instalaci

3.3.2. Aktivace

Pro správné fungování musí být program aktivován. Program vyzve k aktivaci při prvním spuštění. Pokud se tak nestane, proveďte aktivaci ručně stiskem tlačítka nacházející se v menu ***Informace o stanici***.



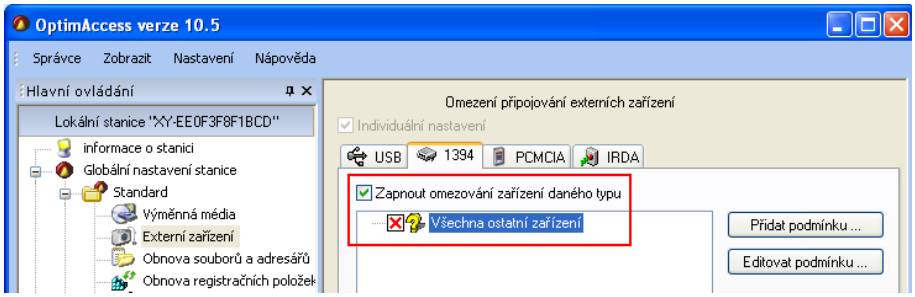
Obr. 9: OptimAccess - Aktivace programu

3.3.3. Nastavení

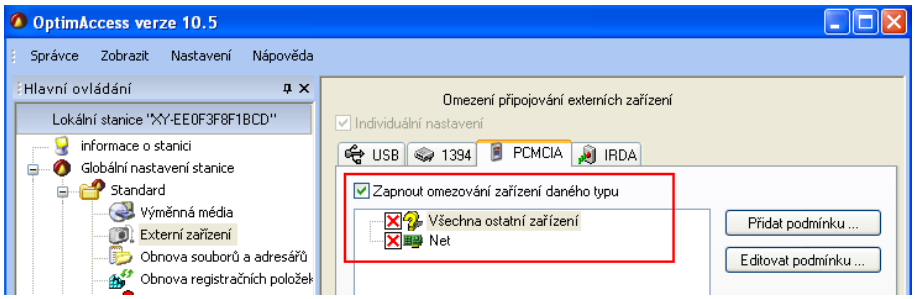
Nastavení je provedeno dle principu „Whitelist“, tedy nastaveno na nejvyšší zabezpečení - vše zakázáno/vypnuto. Přidávány jsou výjimky pro schválené, jednoznačně identifikovatelné a řádně evidované USB paměťové zařízení.

Modul Standard

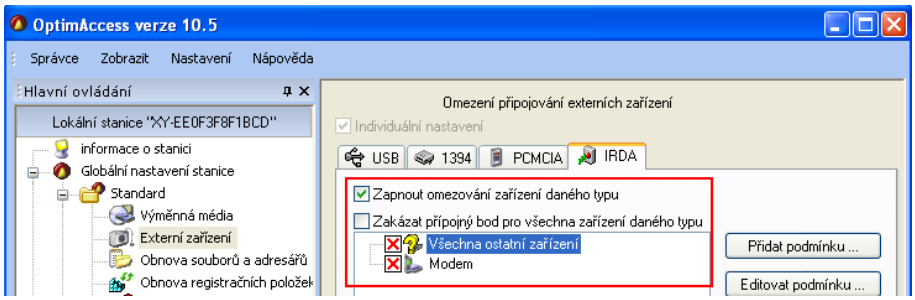
V modulu *Standard* pod položkou *Externí zařízení* zapněte omezování zařízení daného typu a zakažte všechna zařízení typu IEEE 1394 (FireWire), PCMCIA, IRDA, jak je znázorněno na následujících obrázcích č. 10, 11 a 12.



Obr. 10: OptimAccess - Omezení zařízení IEEE 1394 (FireWire)

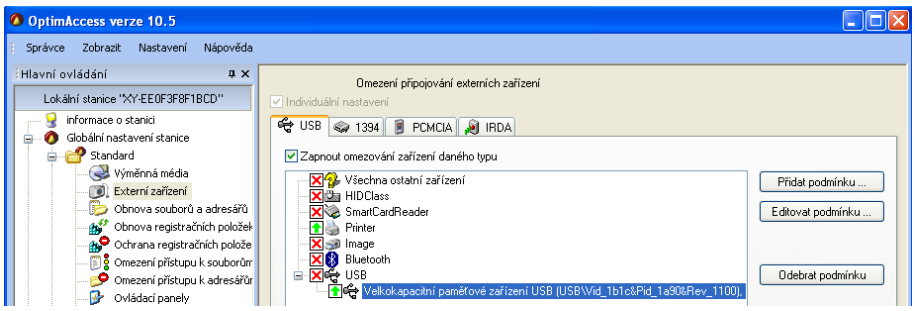


Obr. 11: OptimAccess - Omezení zařízení PCMCIA



Obr. 12: OptimAccess - Omezení zařízení IRDA

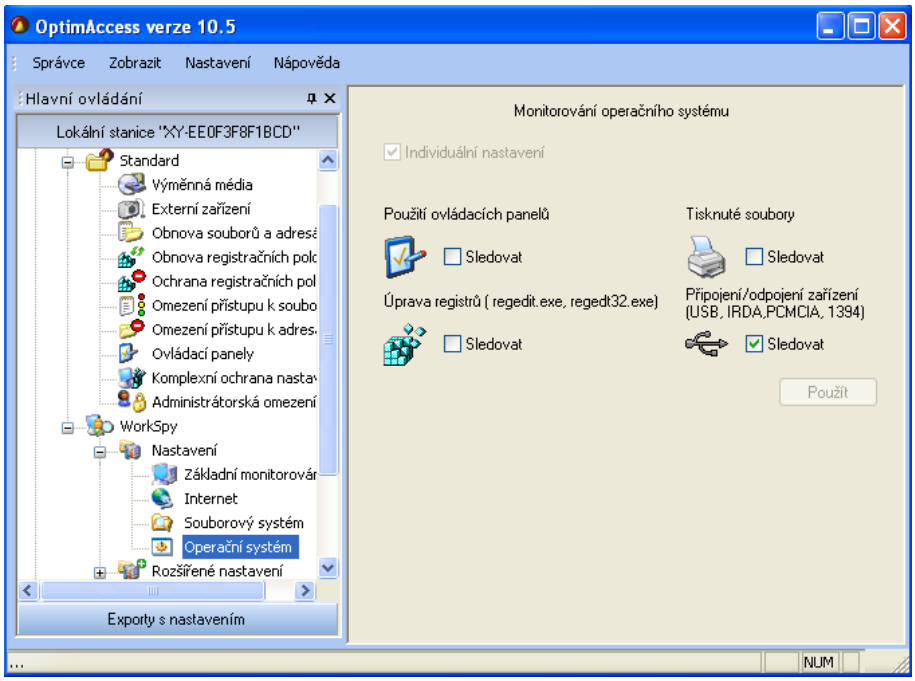
V záložce USB zapněte též *Omezování ostatních zařízení*. Pomocí tlačítka *Přidat podmínku* přidávejte výjimky pro schválené USB paměťová zařízení a nezbytná externí USB zařízení, jak je naznačeno na obrázku č. 13.



Obr. 13: OptimAccess - Výjimka pro USB zařízení

Modul WorkSpy

V modulu WorkSpy zapněte sledování připojení a odpojení USB zařízení. Provedete v sekci *Nastavení/Operační systém* zaškrtnutím políčka *Sledovat.*



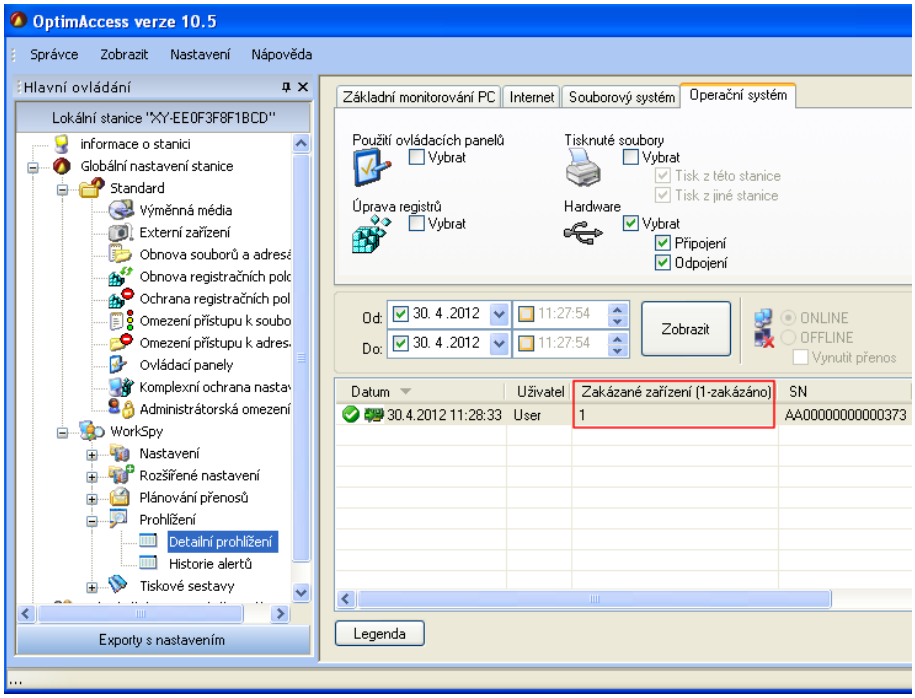
Obr. 14: OptimAccess - Sledování připojení a odpojení USB zařízení

3.3.4. Auditní záznamy

Auditní záznamy, které jsou aplikací generovány, je možné prohlížet a exportovat v modulu WorkSpy pod položkou *Prohlížení/Detailní prohlížení*. Zde je třeba v záložce *Operační systém* vybrat USB a zaškrtnout *Připojení* a *Odpojení.*

Export pro potřeby zálohy auditních dat se provádí pomocí tlačítka *Export* a auditní záznamy se ukládají do textového formátu odděleného oddělovačem, do formátu CSV.

Náhled na zobrazení auditních záznamů s ukázkou zaznamenání připojení nepovoleného zařízení ukazuje následující obrázek č. 15.



Obr. 15: OptimAccess - Prohlížení auditních záznamů, příklad zaznamenání připojení nepovoleného zařízení

3.4. Blancco – File Shredder

Pro bezpečné mazání souborů nainstalujte produkt Blancco – File Shredder 7.7. Na základě provedeného hodnocení[1] Blancco – File Shredder verze 7.7 je NBÚ schválen pro bezpečné mazání souborů a médií v systému.

Pro mazání vyberte standard *HMG Infosec Standard No: 5 ,The Enhanced Standard*.

3.5. OpenOffice.org

Jako kancelářský balík aplikací nainstalujte OpenOffice.org verze 3.3. Všechna nastavení ponechte ve výchozích hodnotách.

1 Hodnocení produktů společnosti Blancco Oy Ltd. (http://www.nbu.cz/cs/aktuality/585-hodnoceni-produktu-spolecnosti-blancco-oy-ltd/)

5 PROVOZNÍ BEZPEČNOSTNÍ DOKUMENTACE

5.1 Bezpečnostní směrnice bezpečnostního správce

Bezpečnostní směrnice bezpečnostního správce

Informačního systému **V**ÁCLAV

4 ZÁVÁDĚNÍ INFORMAČNÍHO SYSTÉMU

Bezpečnostní správce

1) aplikuje projektovou bezpečnostní dokumentaci
2) připravuje, spravuje a aktualizuje provozní bezpečnostní dokumentaci, provozně bezpečnostní dokumentaci a evidence, provozní dokumentaci tvoří:
   a) seznam uživatelů a jejich proškolení
   b) seznam osob spravující IS
   c) evidence médií
   d) provozní deník IS
   e) deník bezpečnostního správce IS
   f) deník správce IS
3) zajišťuje evidenci médií, včetně pevného disku
4) zajišťuje evidenci a uložení neutajovaných nosičů informací pro správu systému, neutajované dokumenty v nelistinné podobě pro ukládání auditních záznamů
5) zajišťuje označení komponent počítačové sestavy informačního systému
6) komponenty počítačové sestavy opatřuje ochrannými prvky
7) zajišťuje instalaci operačního systému a softwarového aplikačního vybavení
8) provádí fyzickou instalaci počítačové sestavy dle projektové dokumentace
9) provádí bezpečnostní nastavení dle *Nastavení bezpečnostních charakteristik OS*
10) svoji činnost zaznamenává do Deníku bezpečnostního správce
11) provádí zápis pověřených uživatelů do Evidence uživatelů
12) vytváří uživatelské účty pověřených uživatelů
13) provádí vstupní a periodické školení uživatelů a správců

5 KONTROLA INFORMAČNÍHO SYSTÉMU

1) kontroluje dodržování stanovených režimových opatření
2) provádí pravidelné (minimálně 1x měsíčně) kontrolu a zálohování auditních záznamů IS
3) provádí pravidelnou kontrolu ochranných prvků sestavy
4) provádí pravidelné (minimálně 1x měsíčně) bezpečné mazání volného místa na pevném disku sestavy

5) provádí pravidelnou (minimálně 1x měsíčně) aktualizaci antivirového programu
6) 1x ročně provádí vyhodnocení stavu informačního systému

6 KRIZOVÉ SITUACE, BEZPEČNOSTNÍ INCIDENTY A KOMPROMITACE

1) o incidentu provádí záznam do deníku bezpečnostního správce
2) provede prvotní šetření krizové situace nebo incidentu
3) prověřuje, zda mohlo dojít nebo došlo v souvislosti krizovou situací nebo vzniklým incidentem k zanedbání povinností při ochraně utajovaných informací
4) vyrozumívá Národní bezpečnostní úřad o porušení nebo předpokladu, že mohlo dojít k porušení ochrany utajované informace nebo kompromitaci

7 SERVISNÍ ČINNOST A OPRAVY

1) zajišťuje servis a opravy počítačové sestavy
2) před předáním do opravy odstraňuje ochranné prvky
3) je zodpovědný za vyjmutí všech paměťových nosičů informací ze sestavy před předáním do opravy

8 POZASTAVENÍ NEBO UKONČENÍ PROVOZU IS

1) pozastavuje provoz informačního systému na základě písemného pokynu vedoucího pracovníka s personální pravomocí
2) ukončuje provoz informačního systému na základě písemného pokynu vedoucího pracovníka s personální pravomocí
3) při ukončování provozu IS:
   a) provádí závěrečný audit systému (kontrolu a zálohu auditních záznamů)
   b) odstraňuje ochranné prvky
   c) zajišťuje řádné uložení pevného disku, případně jeho vymazání
   d) o činnostech provádí zápis do Deníku bezpečnostního správce
   e) provede uložení veškeré dokumentace informačního systému

5.2 Bezpečnostní směrnice správce

Bezpečnostní směrnice správce

Informačního systému **V**ÁCLAV

Vypracoval: Bc. Martin Kuška Dne: 26.4.2012

1 ÚVOD

Bezpečnostní směrnice správce navazuje na Návrh bezpečnosti informačního systému a přílohu Nastavení bezpečnostních charakteristik OS. Bezpečnostní směrnice stanovuje činnosti, postupy a povinnosti správce při zavádění, provozu a ukončování provozu informačního systému.

2 ZÁVÁDĚNÍ INFORMAČNÍHO SYSTÉMU

Správce

1) na pokyn bezpečnostního správce instaluje operační systém a příslušný schválený aplikační software v souladu s Návrhem bezpečnosti IS a Nastavení bezpečnostních charakteristik
2) bezpečnostnímu správci dokládá údaje o instalovaném hardwaru a softwaru

3 PROVOZ A KONTROLA INFORMAČNÍHO SYSTÉMU

Správce informačního systému v rámci provozu IS:

1) odpovídá za technický provoz informačního systému
2) provádí pravidelnou kontrolu ochranných prvků sestavy
3) na pokyn bezpečnostního správce provádí instalaci a odinstalaci schváleného softwaru
4) provádí pravidelnou (minimálně 1x měsíčně) aktualizaci antivirového programu
5) svou činnost zaznamenává do Deníku správce IS

Zakázané činnosti:

1) bez pokynu/souhlasu bezpečnostního správce instalovat do informačního systému jakýkoli software
2) provádění změn v konfiguraci, které jsou v rozporu s návrhem bezpečnosti IS nebo mají vliv na bezpečnost informačního systému
3) upravovat nebo mazat auditní záznamy

4 KRIZOVÉ SITUACE, BEZPEČNOSTNÍ INCIDENTY A KOMPROMITACE

1) neprodleně informuje bezpečnostního správce IS o zjištěném bezpečnostním incidentu, krizové situaci, kompromitaci nebo skutečnosti, která tomu nasvědčuje
2) o zjištěném bezpečnostním incidentu, krizové situaci, kompromitaci nebo skutečnosti, která tomu nasvědčuje, provede záznam do Deníku správce
3) spolupracuje s bezpečnostním správcem při uvedení informačního systému do schváleného stavu dle dokumentace
4) spolupracuje s bezpečnostním správcem při prověřování bezpečnostního incidentu, krizové situace, kompromitace nebo skutečnosti, která tomu nasvědčuje

5 SERVISNÍ ČINNOST A OPRAVY

1) spolupracuje s bezpečnostním správcem
2) zajišťuje servis a opravy počítačové sestavy

6 POZASTAVENÍ NEBO UKONČENÍ PROVOZU IS

1) spolupracuje s bezpečnostním správcem
2) na pokyn bezpečnostního správce odinstalovává operační systém a příslušný software
3) do deníku správce provádí zápis o provedených činnostech provedených v souvislosti s ukončováním provozu

5.3 Bezpečnostní směrnice uživatele

Bezpečnostní směrnice uživatele

Informačního systému **V**ÁCLAV

Vypracoval: Bc. Martin Kuška Dne: 26.4.2012

1 ÚVOD

Informační systém Václav je tvořen jedním nepřenosným osobním počítačem, včetně LCD monitoru, klávesnice a myši. K osobnímu počítači jsou připojeny schválené periferní zařízení, a to tiskárna, záložní zdroj napájení UPS. Napájení všech zařízení je vedeno přes přepěťový a vysokofrekvenční filtr schváleného typu. Všechna zařízení, správa systému, procesy a prostředky ke sběru, tvorbě, zpracování a ukládání utajovaných informací tvoří informační systém. Počítačová sestava není žádným způsobem propojena s jiným systémem, počítačovou sítí nebo jinými komunikačními kanály. Počítačová sestava je vybavena zabudovaným pevným diskem.

Informační systém umožňuje zpracování a ukládání utajovaných informací do stupně utajení **VYHRAZENÉ**.

Informační systém je provozován v provozním módu s nejvyšší úrovní. Všichni uživatelé musejí splňovat podmínky pro přístup k utajovaným informacím stupně Vyhrazené nebo a vyšší a všichni uživatelé nemusejí být oprávněni pracovat se všemi utajovanými informacemi, které jsou v systému obsaženy.

Všechna periferní zařízení informačního systému jsou viditelně označena informativními štítky s názvem informačního systému a stupněm utajení.

2 POKYNY PRO UŽIVATELE

K činnosti v informačním systému písemně pověřuje uživatele nebo jeho pověření ukončuje vedoucí pracovník s personální pravomocí. Proškolení uživatele provádí bezpečnostní správce IS. Vytvoření uživatelského účtu uživatele provádí bezpečnostní správce IS.

Uživatel užívá informační systém k vytváření, úpravě a ukládání utajovaných informací, případně neutajovaných informací. Uživatel se řídí bezpečnostní směrnicí uživatele, pokyny bezpečnostního správce.

Výkonem role bezpečnostního správce je pověřen:

Jméno a příjmení …....., kontakt …....

3 Povinnosti uživatele

Uživatel je povinen:

1) Před začátkem práce v IS zkontrolovat neporušenost ochranných prvků. V případě porušení nepoužívat počítačovou sestavu a neprodleně informovat bezpečnostního správce a do Provozního deníku provést záznam.
   Umístění ochranných prvků: 2x PC, 2x monitor, 2x tiskárna,2x klávesnice, 1x záložní zdroj UPS
2) Svou činnost řádně zaznamenávat do Provozního deníku.
3) Chránit své heslo, heslo je považováno za utajovanou informaci stupně Vyhrazené.
4) Při krátkodobém opuštění systému (do 30ti minut), obrazovku zamknout (klávesy CTRL+ALT+DEL) a zabezpečit pracoviště a zpracovávané dokumenty před neoprávněnými osobami.
5) Při delším opuštění (více než 30 minut) řádně ukončit práci a informační systém vypnout
6) Ukládat zpracovávané informace (soubory) pouze do vlastní složky Dokumenty
7) Zajišťovat administrativní bezpečnost zpracovávaných dokumentů a všech případných výstupů utajovaných informací dle platné vyhlášky
8) vkládat výhradně evidované a řádně označené nosiče informací a paměťová média
9) zajišťovat zaevidování a označení nosičů informací u bezpečnostního správce
10) provádět antivirovou kontrolu vkládaných nosičů informací
11) bezpečnostnímu správci hlásit jakékoli nestandardní chování systému, hardwaru a softwaru nebo jeho závadu a provést o tom záznam do provozního deníku
12) bezpečnostnímu správci neprodleně hlásit podezření na neoprávněnou manipulaci s daty, počítačovou sestavou nebo uživatelským účtem
13) účastnit se pravidelných školení

Obr. 16: Hologramová bezpečnostní plomba s evidenčním číslem

4 Zakázané činnosti uživatele

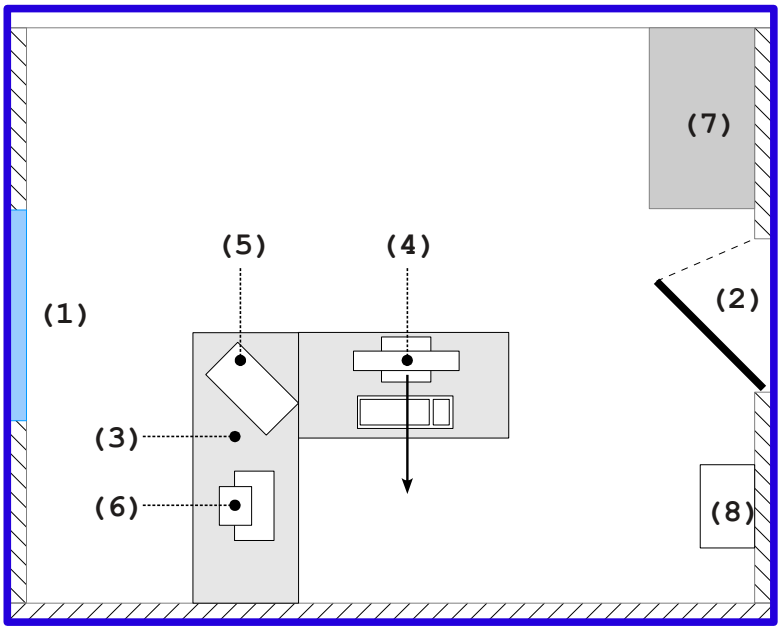
Uživateli je zakázáno:

1) Provádět v informačním systému jinou činnost, než ke které byl pověřen a vyplívá z jeho pracovních povinností
2) Používat cizí přístupová práva nebo se o toto pokoušet
3) Vkládat do sestavy neevidované nosiče informací
4) Spouštět na počítači software jiný než předinstalovaný a schválený
5) Upravovat nebo mazat nainstalovaný software, měnit konfiguraci hardwaru nebo softwaru
6) Přistupovat k datům jiných uživatelů nebo se o to pokoušet
7) Kopírovat nebo jinak šířit jakékoli části operačního systému, nainstalovaného softwaru
8) Deaktivovat nebo jinak omezovat činnost antivirového systému
9) Provádět neoprávněné kopie dat

5 Režimová opatření

1) Informační systém Václav je umístěn v objektu Čáslavská 36, Praha 9, v zabezpečené oblasti kategorie VYHRAZENÉ, místnosti č. A.03
2) Fyzické umístění počítačové sestavy odpovídá nákresu na obrázku
3) Měnit umístění PC sestavy je oprávněn pouze bezpečnostní správce
4) Na pracoviště systému je oprávněna vstupovat jen oprávněná osoba (uživatel, správce, bezpečnostní správce), jiné osoby (např. pracovník údržby) jen v doprovodu bezpečnostního správce
5) Pracoviště systému je v době nepřítomnosti oprávněné osoby řádně uzavřeno a uzamčeno v souladu s projektem fyzické bezpečnosti
6) Klíče od místnosti jsou v souladu s projektem fyzické bezpečnosti řádně označeny, uloženy a vydávány pouze oprávněným osobám proti podpisu ostrahou objektu.

Nákres místnosti s umístěním počítačové sestavy



Obr. 17: Nákres pracoviště systému

Legenda:

1. Okno
2. Dveře, vstup do místnosti
3. Pracovní stůl
4. Monitor s vyznačeným směrem natočení
5. Počítač
6. Tiskárna
7. Trezor
8. Skartovací zařízení

Hranice zabezpečené oblasti

6 ZPRACOVÁNÍ UTAJOVANÝCH INFORMACÍ

Při zpracování utajovaných informací je uživatel povinen:

1) Ukládat utajované informace v informačním systému do své složky Dokumenty
2) Výtisky obsahující utajované informace neprodleně po vyhotovení označit v souladu s administrativní bezpečností a v souladu s předpisy
3) K mazání souborů používat výhradně nástroj Blancco – File Shredder

4) Kontrolovat všechny výstupy na výskyt utajované informace, v případě nechtěného výstupu nebo uložení dokument nebo nosič řádně označit a zaevidovat nebo ho neprodleně skartovat na certifikovaném zařízení, které je na pracovišti instalováno. O události provést záznam do Provozního deníku

7 Nosiče utajovaných informací

1) Nosiče informací mohou být použity pouze ve schválených informačních systémech umožňující nakládání s utajovanými informacemi
2) Snižování nebo rušení stupně utajení nosičů informací je NEPŘÍPUSTNÉ

8 Nosiče neutajovaných informací

Nosiče neutajovaných informací používaných v informačním systému musejí být řádně označeny a evidovány

9 ZÁLOHOVÁNÍ A UKLÁDÁNÍ

Uživatel si svá data zálohuje dle vlastního uvážení za dodržení pravidel pro nakládání s nosiči dat s utajovanými informacemi.

Uložení nosičů dat utajovaných informací provádí do schváleného úložného objektu na pracovišti do své zapečetěné schránky.

ZÁVĚR

Cílem této práce bylo shrnutí platné legislativní úpravy ochrany utajovaných informací v České republice, vysvětlit problematiku bezpečnosti, hodnocení, tvorby dokumentace a návrhu informačního systému a navrhnutí projektu informačního systému.

První, teoretická část se věnuje ochraně utajovaných informací, je zde uveden přehled právní úpravy, včetně změn, které od 1.1.2012 vešly v platnost novelizací zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Je zde popsáno postavení a úkoly Národního bezpečnostního úřadu v problematice ochrany utajovaných informací, dále jsou uvedeny druhy zajištění ochrany utajovaných informací. Popsána je problematika utajovaných informací, které jsou nelistinného charakteru, v elektronické podobě a s tím spojená problematika úniku utajovaných informací kompromitujícím elektromagnetickým vyzařováním.

V druhé, praktické části je zpracován návrh projektu informačního systému pro nakládání a ukládání utajovaných informací do stupně utajení Vyhrazené. V návrhu je realizována projektová bezpečnostní dokumentace a provozně bezpečnostní dokumentace, včetně Nastavení bezpečnostních charakteristik operačního systému.

CONCLUSION

This thesis introduces the current legislation concerning the protection of classified information in the Czech Republic, explains problems connected to security, evaluation, creation of documentation and designing the information system and the project of the information system.

The first theoretical part focuses on the protection of classified information and presents the current legislation, including the changes which came into effect on 1 January 2012 via the amendment to the Act N. 412/2005 Coll. on Protection of Classified Information and Security Qualification. It describes the role and tasks of National Security Authority in the area of the classified information protection; it also lists ways to assure the protection of classified information. The thesis also describes problems connected with non-documentary and electronic classified information and the relevant problems connected with leaks of classified information via compromising emission.

The second practical part presents the design of the information system project for classified information processing and storage up to the level Restricted. The design of the project includes the project security documentation and operating security documentation, including the Setting of security properties of the information system.

SEZNAM POUŽITÉ LITERATURY

[1] SALIVAR, Jaroslav. *Novela zákona o ochraně utajovaných informací a bezpečnostní způsobilosti.* [online]. 2011 [cit. 2012-05-05]. Dostupné z: http://www.cicar.cz/analyzy/zobrazit-analyzu/novela-zakona-o-ochrane-utajovanych-informaci-a-bezpecnostni-zpusobilosti

[2] STEINER, František. *Případová studie analýzy rizik informační bezpečnosti.* In: [online]. [cit. 2012-05-06]. Dostupné z: http://bpm-tema.blogspot.com/2007/11/ppadov-studie-analzy-rizik-informan.html

[3] ČERMÁK, Miroslav. *Analýza rizik: Jemný úvod do analýzy rizik.* In: [online]. 20.5.2010. Dostupné z: http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/

[4] MICROSOFT CORPORATION. *Windows XP Common Criteria Configuration Guide 3.0* [online]. 2007. Dostupné z: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=20226

[5] MICROSOFT CORPORATION. *Windows XP Common Criteria Administrator Guide 3.0* [online]. 2007. Dostupné z: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=8807

[6] *CC_HiSec_XP_Professional_V3.inf* [šablona zabezpečení]. Ver. 3.0: Microsoft Corporation, 2008. Dostupné z: http://download.microsoft.com/download/5/8/e/58ef1d3a-9bdb-4e0e-a7b6-a3640d9900cb/CC_WS2K3-XP%20v3.0%20Security%20Templates.zip

[7] *Hodnocení produktů Microsoft Windows Server 2003 a Microsoft Windows XP*. In: Národní bezpečnostní úřad [online]. Dostupné z: http://www.nbu.cz/cs/aktuality/2624-hodnoceni-produktu-microsoft-windows-server-2003-a-microsoft-windows-xp/

[8] NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Minimální obsah bezpečnostní dokumentace pro malé informační systémy* [online]. 2007. Dostupné z: www.nbu.cz/download/nodeid-744/

[9] Fyzická bezpečnost (technické prostředky a další prvky fyzické bezpečnosti a jejich certifikace). Národní bezpečnostní úřad [online]. Dostupné z: http://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost/

[10] Česká republika. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. 2005, 143. ISSN 1211-1244

[11] Česká republika. Vyhláška ze dne 5. prosince 2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb. In: *Sbírka zákonů České republiky*. 2005, č. 523, 179. ISSN 1211-1244

[12] Česká republika. Vyhláška ze dne 21. prosince 2011, kterou se mění vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. In: *Sbírka zákonů České republiky*. 2011, č. 454, 155, s. 5882-5887.

[13] Česká republika. Vyhláška ze dne 16. prosince 2011 o zajištění kryptografické ochrany utajovaných informací. In: *Sbírka zákonů České republiky*. 2011, 150, s. 5712-5729.

[14] Česká republika. Vyhláška ze dne 23. listopadu 2011 o personální bezpečnosti a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. 2011, 127, s. 4535-4556.

[15] Česká republika. Vyhláška ze dne 7. prosince 2011 o průmyslové bezpečnosti. In: *Sbírka zákonů České republiky*. 2011, č. 405, 142, s. 5334-5365.

[16] Česká republika. Vyhláška ze dne 14. prosince 2005 o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. 2011, č. 528, 179, s. 10079-10115. ISSN 1211-1244.

[17] Česká republika. Vyhláška ze dne 21. prosince 2011, kterou se mění vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. In: *Sbírka zákonů České republiky*. 2011, 155, s. 5888-5916.

[18] Česká republika. Vyhláška ze dne 15. prosince 2005 o administrativní bezpečnosti a o registrech utajovaných informací. In: *Sbírka zákonů České republiky*. 2005, č. 529, 179, s. 10116-10151. ISSN 1211-1244.

[19] Česká republika. Nařízení vlády ze dne 7. prosince 2005, kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. 2005, č. 522, 179, s. 9950-9977. ISSN 1211-1244.

[20] Česká republika. Nařízení vlády ze dne 9. června 2008, kterým se mění nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. 2008, č. 240, 77, s. 3590-3592. ISSN 1211-1244.

[21] Česká republika. Zákon ze dne 26. listopadu 2004 o správních poplatcích. In: *Sbírka zákonů České republiky*. 2004, č. 634, 215, s. 11415-11501.

[22] ČSN EN 55022. *Zařízení informační techniky - Charakteristiky rádiového rušení - Meze a metody měření.* 1.říjen 1999.

[23] *Common Criteria : The Common Criteria Portal* [online]. Dostupné z: www.commoncriteriaportal.org

[24] Informace o hodnocení bezpečnosti informačních technologií COMMON CRITERIA (CC). In: NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. [online]. 2005, s. 6-7 [cit. 2012-05-07]. Dostupné z: http://www.nbu.cz/download/nodeid-757/

[25] NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Používání FireWire a USB portů a bezpečnostní aspekty pamětí typu „flash“*: Metodický pokyn, verze 1. Praha, 2007. Dostupné z: www.nbu.cz/download/nodeid-1009/

[26] NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. Minimální nastavení produktu OptimAccess. Dostupné z: http://www.nbu.cz/download/nodeid-1057/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BIOS	Basic Input-Output System
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Metodology
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
č.	Číslo
ČR	Česká republika
EAL	Evaluation Assurance Level
EMSEC	Emission Security
EU	Evropská Unie
HW	Hardware
IS	Informační systém
ITSEC	Information Technology Security Evaluation Criteria
KV	Kompromitující vyzařování
LAN	Local Area Network
NATO	Severoatlantická aliance (North Atlantic Treaty Organization)
NBÚ	Národní bezpečnostní úřad
NSA	Národní bezpečnostní agentura (National Security Agency)
obr.	Obrázek
OS	Operační systém
PC	Osobní počítač (Personal Computer)
PDF	Portable Document Format
Sb.	Sbírka zákonů
SW	Software
TCSEC	Trusted Computer System Evaluation Criteria
UPS	Uninterruptible Power Supply

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P 1: PROHLÁŠENÍ O SHODĚ PC, UPS A TISKÁRNY

ES prohlášení o shodě

dle zákona č. 22/1997 Sb. v platném znění

Výrobek : Personální počítač
Typ : AC PC
Modely : OfficePro (produktová řada)
Značka : AutoCont

Identifikační údaje výrobce :

ATCompus s.r.o.
Uhlířská 1064
710 00 Slezská Ostrava
Česká republika
IČO: 26217911
Zapsáno v obchodním rejstříku, vedeném Krajským soudem v Ostravě oddíl C., vložka 26849

ATCompus s.r.o. prohlašuje, že výše uvedený výrobek je ve shodě s těmito nařízeními vlády a normami :

Elektrická bezpečnost : nařízení vlády č.17/2003 Sb. v platném znění
ČSN EN 60950-1
Elektromagnetická kompatibilita : nařízení vlády č. 616/2006 Sb. v platném znění
ČSN EN 55022:1999
ČSN EN 61000-3-2:2001
ČSN EN 61000-3-3:1997
ČSN EN 55024:1999
ČSN EN 61000-4-2:1997
ČSN EN 61000-4-3:2003
ČSN EN 61000-4-4:2005
ČSN EN 61000-4-5:1997
ČSN EN 61000-4-6:1997
ČSN EN 61000-4-11:2005

V Ostravě dne 25.2.2008

Ing. David Kaděra
Vedoucí technického oddělení

ATC-ES-AC-OfficePro

PROHLÁŠENÍ O SHODĚ

My APC Praha

Za pruhy 243/2
140 00 Praha 4
Česká republika

Prohlašujeme na svou výlučnou zodpovědnost, že níže uvedený výrobek splňuje požadavky technických předpisů, že výrobek je za podmínek námi určeného použití bezpečný a že jsme přijali veškerá opatření, kterými zabezpečujeme shodu všech výrobků níže uvedeného typu, uváděných na trh, s technickou dokumentací a s požadavky příslušného nařízení vlády.

Výrobek: Nepřerušitelný zdroj napájení (UPS)

Typ: **Back-UPS RS BR500I, BR800I, BR800-FR, BR1000I, BR1000-FR, BR1500I, BR1500-FR**

Výrobce: APC Philippines, Caivte Epza, Roserio, Filipíny
APC India, Jigani Hobbi Anekal Taluk, India
APC b.v.,Ballybrit Business Park, Galway, Ireland

Výrobek je určen pro použití v informační technice.

Způsob posouzené shody: § 12, (4) a) zákona č. 22/1997 Sb.

Výše uvedený výrobek je ve shodě s normami

el. bezpečnost: ČSN EN 60950, ČSN EN 50091-1-1
EMC: ČSN EN 50091-2
ČSN EN 61000-3-2
ČSN EN 61000-3-3

a nařízením vlády

el. bezpečnost: NV č. 17/2003 Sb.
EMC: NV č. 18/2003 Sb.

Toto prohlášení vydáno na základě:
Certifikátů – CB TEST CERTIFICATE NEMKO No. 25695, 25698, 28318/A1
Prohlášení – CE Declaration of Conformity z 1/1/2004
Servisní dokumentace

Prohlášení shody s NV č. 17/2003 Sb. a NV č. 18/2003 Sb. provedeno pouze v rozsahu výše uvedených norem.

Místo vydání: APC Praha

Jméno: **Ing. Radek Micka**
technický zástupce

Datum vydání: 15. června 2005

Podpis:

Prohlášení o shodě

Prohlášení o shodě

Prohlášení o shodě

podle normy ISO/IEC 17050-1 a EN 17050-1, DoC č.: BOISB-0801-00-rel.1.0

Název výrobce:	Hewlett-Packard Company
Adresa výrobce:	11311 Chinden Boulevard, Boise, Idaho 83714-1021, USA

prohlašuje, že produkt

Název produktu:	Tiskárna HP LaserJet P2030 Series
Kontrolní číslo modelu[2]:	BOISB-0801-00
Provedení produktu:	VŠECHNA
	Tiskové kazety: CE505A

vyhovuje následujícím specifikacím produktu:

Bezpečnost:	IEC 60950-1:2001 / EN60950-1: 2001 +A11 IEC 60825-1:1993 +A1 +A2 / EN 60825-1:1994 +A1 +A2 (laserový/LED výrobek třídy 1) GB4943-2001
Elektromagnetická kompatibilita:	CISPR22:2005 / EN 55022:2006 – třída B[1] EN 61000-3-2:2000 +A2 EN 61000-3-3:1995 +A1 EN 55024:1998 +A1 +A2 FCC Název 47 CFR, díl 15 třída B / ICES-003, 4. vydání GB9254-1998, GB17625.1-2003

Doplňující informace:

Uvedený výrobek splňuje požadavky EMC směrnice 2004/108/EC a směrnice pro nízkonapěťová zařízení 2006/95/EC a je označen příslušným symbolem CE CE.

Toto zařízení splňuje ustanovení části 15 předpisů FCC. Výrobek může být provozován na základě následujících dvou podmínek: (1) zařízení nesmí vytvářet škodlivé rušení a (2) musí být schopno zvládat příjem jakéhokoliv rušení, včetně takového, které by mohlo ovlivnit jeho funkci.

1) Produkt byl testován v typické konfiguraci s počítačovými systémy Hewlett-Packard.

2) Pro registrační účely je tomuto zařízení přiděleno kontrolní číslo modelu. Toto číslo by nemělo být zaměňováno za marketingový název nebo za čísla produktu.

Boise, Idaho , USA

22. října 2007

Pouze dotazy týkající se předpisů:

Kontakt pro Evropu:	Vaše místní kancelář prodeje a služeb Hewlett-Packard nebo Hewlett-Packard GmbH, Department HQTRE / Standards Europe,, Herrenberger Strasse 140, , D-71034, Böblingen, (FAX: +49-7031-14-3143), http://www.hp.com/go/certificates
Kontakt pro USA:	Product Regulations Manager, Hewlett-Packard Company,, PO Box 15, Mail Stop 160, Boise, ID 83707-0015, , (telefon: 208-396-6000)

PŘÍLOHA P 2: CERTIFIKÁT INFORMAČNÍHO SYSTÉMU

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
Pošt. přihr. 49
150 06 Praha 56

Národní bezpečnostní úřad vydává podle § 46 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

CERTIFIKÁT
informačního systému

Evidenční číslo: **S000000**

Informační systém určený pro nakládání s utajovanými informacemi, verze 1.1
(název, verze)

Držitel certifikátu:
Sídlo: IČ:

Tento certifikát potvrzuje ověření a schválení způsobilosti informačního systému k nakládání s utajovanou informací do a včetně stupně utajení

Vyhrazené

Platnost od: 12. června 2006
Platnost do: 12. června 2011

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD 20

Náměstek ředitele
Národního bezpečnostního úřadu
Ing. Jaroslav ŠMID

Datum vydání : 8. června 2006

001575

Přílohy : Certifikační zpráva, 2 strany