Ochrana utajovaných informací v komunikačních a informačních systémech

Jan Svoboda

Bakalářská práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan Svoboda**
Osobní číslo:	**A11801**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Ochrana utajovaných informací v komunikačních a informačních systémech**

Zásady pro vypracování:

1. **Analyzujte nejčastější bezpečnostní rizika ochrany utajovaných informací v komunikačních a informačních systémech.**
2. **Ohodnoťte opatření ochrany utajovaných informací v komunikačních a informačních systémech v závislosti na výši újmy vzniklé České republice.**
3. **Navrhněte a realizujte hlavní prvky bezpečnostní politiky komunikačních a informačních systémů.**
4. **Realizujte návrh bezpečnostních opatření komunikačního a informačního systému v závislosti na vámi navrženém stupni utajení.**
5. **Vyhodnoťte návrh bezpečnostních opatření.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **HALBICH, Čestmír a Dagmar BRECHLEROVÁ. Bezpečnost Informačních Systémů: Vybrané Kapitoly Vyd. 1. Praha: Česká zemědělská univerzita, 2003. ISBN 80-213-1090-1.**
2. **DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008, 239 s. ISBN 978-80-86946-88-7.**
3. **ČANDÍK, Marek. Bezpečnosť informačných systémov, steganografia a digitálna vodotlač. [Ostrava: s.n.], 2005, 117 s. ISBN 80-239-5962-X.**
4. **POŽÁR, Josef. Informační bezpečnost. Plzeň: Aleš Čeněk, 309 s. Vysokoškolské učebnice (Aleš Čeněk). ISBN 80-868-9838-5.**
5. **PŘIBYL, Jiří. Informační bezpečnost a utajování zpráv. 1. vyd. Vydavatelství ČVUT, 2004, 239 s. ISBN 80-010-2863-1.**

Vedoucí bakalářské práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **7. března 2014**

Termín odevzdání bakalářské práce: **10. června 2014**

Ve Zlíně dne 7. března 2014

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

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/bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

ABSTRAKT

Bakalářská práce je zaměřena na ochranu utajovaných informací v komunikačních a informačních systémech. V první části bakalářské práci jsou představeny jednotlivé druhy bezpečnosti utajovaných informací a dále se práce zaměřuje na informační a komunikační systém. V praktické části bakalářské práce je představen fiktivní utajovaný informační systém, který se jmenuje IS UTB.

Klíčová slova:

Utajovaná informace * dostupnost * důvěrnost * integrita * bezpečnost * bezpečnostní politika * informační systém*

ABSTRACT

The Bachelor´s thesis is focused on the protection of classified information in communication and information systems. The bachelor thesis presents different types security of classified information and the work focuses on information and communication system. In the practical part of this work is presented model of a classified information system named IS UTB.

Keywords:

Classified information * availability * privacy * integrity * safety * security policy * informatic system *

Na tomto místě bych velmi rád poděkoval Ing. Marcelu Závorkovi a Mgr. Barboře Šachlové za pomoc a věcné připomínky k formální stránce této práce. Hlavně bych rád poděkoval mé rodině za podporu během celého studia. Na závěr děkuji všem, kteří byli ochotni mi pomáhat při tvorbě této práce.

OBSAH

ÚVOD

Potřeba utajovat informace doprovází lidstvo od jeho vzniku. Potřeba zavedení ochranných opatření pro zamezení vyzrazení utajovaných informací se neustále vyvíjela, a to podle aktuálně dostupných kryptografických metod, technologií a „know how“. Mezi první pokusy o dálkové předávání informací bylo její zapsání, nebo přímo vytetování na části lidských těl. Člověk se pak stal nositelem utajované informace a distribuoval ji dle pokynů původce utajované informace. S nástupem kryptografie se utajovaná informace transportovala v listinné podobě kurýrní službou (osobou, nebo poštovním holubem).

K obrovskému pokroku v distribuování utajovaných informací došlo za druhé světové války, kdy se ve velkém počtu začaly používat bezdrátové technologie a utajované informace se proto předávaly prakticky v reálném čase. V této nelehké době měly utajované informace obrovskou strategickou hodnotu, a proto bylo potřeba utajovanou informaci v maximální možné míře zašifrovat.

S nástupem výpočetní techniky a vznikem počítačových sítí vznikly obrovské možnosti v práci s utajovanými informacemi. Začaly vznikat informační systémy, které jsou schopny distribuovat utajovanou informaci konkrétnímu adresátovi. Obrovský pokrok zaznamenala kryptografie, kdy novodobé počítačové systémy používají extrémně složité algoritmy a při dodržení správných zásad zabezpečení je prakticky nemožné jejich následné prolomení. Bezpečnost utajované informace ale není závislá pouze na použité kryptografické metodě. Stejně důležitým faktorem je i personální bezpečnost, fyzická bezpečnost celého informačního systému, administrativní bezpečnost, počítačová a komunikační bezpečnost a bezpečnost proti kompromitujícímu vyzařování (viz. kapitola č. 2).

Tato práce je věnována ochraně utajovaných informací v novodobých komunikačních a informačních systémech. Pojem utajovaná informace vychází ze zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Ochrana utajovaných informací je spojena s dodržováním zákonných a podzákonných právních norem a jejich porušení může být kvalifikováno jako trestný čin. (1)

V první části této práce budou uvedeny všechny základní právní předpisy, které se ochrany utajovaných informací v komunikačních a informačních systémech týkají. Dále budou uvedeny základní principy ochrany utajovaných informací v souvislosti s právními normami České republiky. V druhé části této práce bude uveden příklad klasifikovaného

informačního systému s výčtem a obecným popisem bezpečnostní a provozní dokumentace. Budou popsána základní nastavení operačního systému, nároky na ochrany proti škodlivému softwaru, režimová opatření a řízení přístupu k utajovaným informacím.

V závěru této bakalářské práce bude uveden možný vývoj bezpečnosti komunikačních a informačních systémů s výčtem možných hrozeb.

I. TEORETICKÁ ČÁST

1 UTAJOVANÉ INFORMACE

Strategický význam jednotlivých utajovaných informací reflektuje na jejich míru zabezpečení. Hodnota jednotlivé utajované informace přímo odráží újmu, ke které by došlo jejím vyzrazením. Proto došlo ke klasifikaci utajovaných informací od nejnižšího stupně „VYHRAZENÉ“ po druhý stupeň „DŮVĚRNÉ“, třetí stupeň „TAJNÉ“ a nevyšší stupeň „PŘÍSNĚ TAJNÉ„. Samotný zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti pak udává, že seznámení se neoprávněnou osobou s utajovanou informací kategorie „VYHRAZENÉ“ by mohlo být pro stát nevýhodné. Následuje vznik prosté újmy vyzrazením utajované kategorie „DŮVERNÉ“, dále navazuje vážná újma u kategorie „TAJNÉ“ a mimořádně vážná újma vzniklá neoprávněným seznámením se s utajovanou formací klasifikovanou stupněm utajení „PŘÍSNĚ TAJNÉ“. (1)

1.1 Utajovaná informace

Pojem utajovaná informace definuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti v paragrafu 2, jako informaci v jakékoliv podobě zaznamenanou na jakémkoli nosiči a označenou v souladu se zákonem, a která je uvedena v seznamu utajovaných informací. Seznam utajovaných informací vydává Vláda ČR formou nařízení č. 522/2005, ve znění pozdějších předpisů. Z toho vyplývá, že utajovanou informací zdaleka není pouze dokument listinný, nebo elektronický. Utajovanou informací může být i předmět, technické zařízení, ale dokonce i budova, nebo prvek kritické infrastruktury, který má strategický význam pro Českou republiku a je potřeba ho ochraňovat v souladu se zákonem. (1) (2)

1.2 Druhy ochrany utajovaných informací

Pro celkovou ochranu utajovaných informací zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti definuje šest základních druhů bezpečnosti. Jedná se o personální bezpečnost, průmyslovou bezpečnost, administrativní bezpečnost, fyzickou bezpečnost, bezpečnost informačních a komunikačních systémů a kryptografickou bezpečnost. Při nastavovaní bezpečnostních opatření nesmíme ani jeden z těchto druhů bezpečnosti opomenout. (1)

1.2.1 Personální bezpečnost

Cílem personální bezpečnosti je umožnění přístupu k utajované informaci pouze osobám, které splňují podmínky uvedené v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Další základní podmínkou je, aby se osoba seznamovala jen s utajovanými informacemi, které nezbytně potřebuje k výkonu svého povolání. (1) (3)

Po splnění podmínek uvedených v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti fyzická osoba obdrží oznámení (pro kategorii „VYHRAZENÉ“), nebo osvědčení (pro kategorii „DŮVĚRNÉ“ až „PŘÍSNĚ TAJNÉ“). Oznámení osobám, pracujícím v služebním nebo pracovně právním poměru, vydává odpovědná osoba (pověřená Národním bezpečnostním úřadem), nebo v odůvodněných případech přímo Národní bezpečnostní úřad na dobu 5let. Aby osoba oznámení obdržela, musí prokázat, že je svéprávná, starší 18let a bezúhonná. Bezúhonnost osoba prokazuje výpisem z rejstříku trestů, který nesmí být starší jak 3 měsíce. Pokud oznámení vydala právnická osoba, tak jeho platnost zaniká ukončením pracovního poměru osoby, která oznámení vlastní. (1) (3)

Oproti tomu osvědčení fyzické osoby o splnění podmínek zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti vydává pouze Národní bezpečnostní úřad. Aby osoba splnila podmínky pro vydání osvědčení, musí splňovat podmínky pro vydání oznámení a dále musí osoba prokázat, že je plně svéprávná a bezpečnostně spolehlivá. Podmínka svéprávnosti znamená, že osoba určená k přístupu k utajované informaci netrpí žádnou poruchou, nebo obtížemi, které by měly vliv na její spolehlivost, nebo schopnost dodržovat zásady ochrany utajovaných informací. Tato způsobilost se ověřuje psychologickým vyšetřením, čestným prohlášením, nebo lékařským posudkem. Bezpečnostní spolehlivost znamená, že u osoby nebylo zjištěno žádné bezpečnostní riziko. Příkladem bezpečnostních rizik je činnost proti zájmům České republiky, činnosti potlačující základní práva a svobody, úmyslné porušování právních předpisů, nebo nepřiměřené majetkové poměry apod. Bezpečnostní spolehlivost ověřuje přímo Národní bezpečnostní úřad. Doba šetření se od podání žádosti pohybuje v rozmezí od 2 do 9 měsíců, přičemž platnost osvědčení je závislá na jeho stupni a je od 5 do 9 let. (1) (3)

1.2.2 Průmyslová bezpečnost

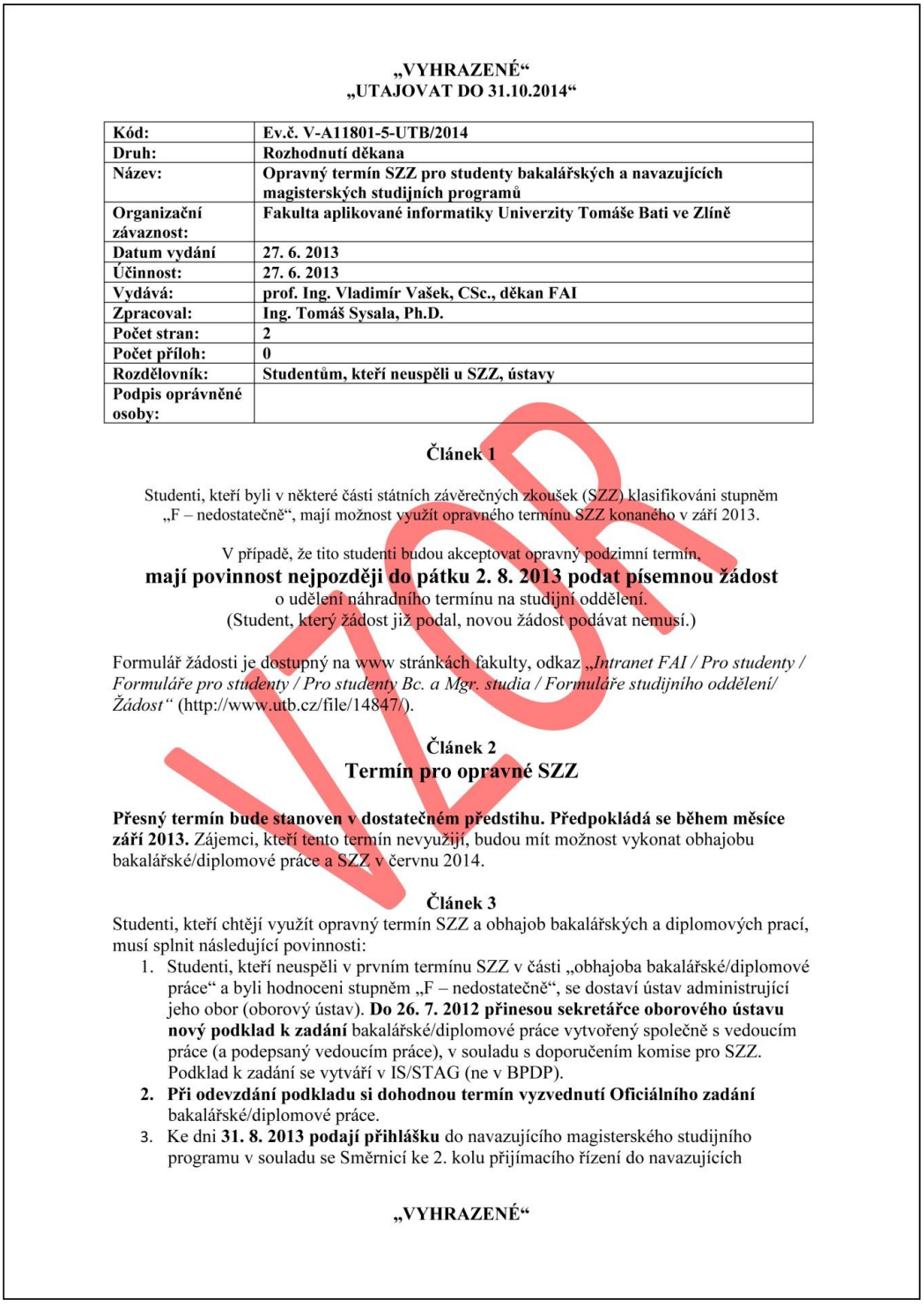
Tento druh bezpečnosti stanovuje podmínky přístupu k utajované informaci pro podnikatele. Podnikatel, který se potřebuje ke své činnosti seznamovat s utajovanými informacemi stupně utajení „VYHRAZENÉ“, musí Národnímu bezpečnostnímu úřadu doložit písemné prohlášení, že je schopen zabezpečit ochranu utajovaných informací. (1) (4)

Pokud podnikatel ke své činnosti potřebuje přistupovat k utajovaným informacím stupně utajení „DŮVĚRNÉ“ a vyšší, musí být držitelem platného osvědčení podnikatele. Pro vydání osvědčení musí podnikatel prokázat svou ekonomickou stabilitu, bezpečnostní spolehlivost, schopnost zabezpečit utajované informace a odpovědná osoba musí být držitelem osvědčení fyzické osoby na stejný nebo vyšší stupeň, než který požaduje. Ekonomickou stabilitou se podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti rozumí, že na podnikatele, který o osvědčení žádá, není vydáno rozhodnutí o úpadku, nebo na podnikatele nevyhlásil soud moratorium. Dále nesmí mít podnikatel nedoplatek na pojistném sociálního zabezpečení nebo dani z příjmů. Za důkaz ekonomické nestability se také považuje neplnění finančních závazků a rozhodnutí o exekuci na majetek podnikatele. Tento druh šetření provádí Národní bezpečnostní úřad a některé skutečností dokladuje podnikatel výpisy vydanými státní správou. Bezpečnostní spolehlivost podnikatele spočívá v hledání bezpečnostních rizik a postupuje se stejně jako u vydávání osvědčení fyzické osobě. (1) (4)

1.2.3 Administrativní bezpečnost

Administrativní bezpečnost obsahuje soubor opatření, která provádí původce a následně i adresát utajované informace při tvorbě a následném zpracování, ukládání a konečné skartaci utajované informace. Při tvorbě utajované informace zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a následný prováděcí právní předpis vyhláška NBÚ č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací předpisů definuje způsob vyznačení stupně utajení přímo na samotném dokumentu. Nezbytnou součástí dokumentu společně se stupněm utajení je i jeho název, evidenční údaje, původce a datum vzniku. Dokumentace obsahující utajované informace musí být řádně zaevidována v administrativních pomůckách. Administrativní pomůcky (sběrné a evidenční archy) musí být označeny stejným stupněm utajení jako utajovaná informace s nejvyšším stupněm utajení. Samotný právní předpis stanovuje

způsoby pořizování Opisů, kopií a výpisů. U stupně utajení „PŘÍSNĚ TAJNÉ“ lze pořídit kopii, opis a výpis pouze se souhlasem původce utajované informace. Naopak u ostatních utajovaných informací stupně „TAJNÉ“ a nižší lze pořizovat opisy, kopie a výpisy pouze se souhlasem přímého nadřízeného. Administrativní bezpečnost určuje požadavky na přepravu utajované informace, způsoby převzetí, předání a ukládání a skartaci. Při skartaci utajované informace musí být vždy součástí skartační řízení. (1) (5)



„VYHRAZENÉ“
„UTAJOVAT DO 31.10.2014“

Kód:	**Ev.č. V-A11801-5-UTB/2014**
Druh:	**Rozhodnutí děkana**
Název:	**Opravný termín SZZ pro studenty bakalářských a navazujících magisterských studijních programů**
Organizační závaznost:	**Fakulta aplikované informatiky Univerzity Tomáše Bati ve Zlíně**
Datum vydání	**27. 6. 2013**
Účinnost:	**27. 6. 2013**
Vydává:	**prof. Ing. Vladimír Vašek, CSc., děkan FAI**
Zpracoval:	**Ing. Tomáš Sysala, Ph.D.**
Počet stran:	**2**
Počet příloh:	**0**
Rozdělovník:	**Studentům, kteří neuspěli u SZZ, ústavy**
Podpis oprávněné osoby:	

Článek 1

Studenti, kteří byli v některé části státních závěrečných zkoušek (SZZ) klasifikováni stupněm „F – nedostatečně“, mají možnost využít opravného termínu SZZ konaného v září 2013.

V případě, že tito studenti budou akceptovat opravný podzimní termín,
mají povinnost nejpozději do pátku 2. 8. 2013 podat písemnou žádost
o udělení náhradního termínu na studijní oddělení.
(Student, který žádost již podal, novou žádost podávat nemusí.)

Formulář žádosti je dostupný na www stránkách fakulty, odkaz *„Intranet FAI / Pro studenty / Formuláře pro studenty / Pro studenty Bc. a Mgr. studia / Formuláře studijního oddělení/ Žádost“* (http://www.utb.cz/file/14847/).

Článek 2
Termín pro opravné SZZ

Přesný termín bude stanoven v dostatečném předstihu. Předpokládá se během měsíce září 2013. Zájemci, kteří tento termín nevyužijí, budou mít možnost vykonat obhajobu bakalářské/diplomové práce a SZZ v červnu 2014.

Článek 3

Studenti, kteří chtějí využít opravný termín SZZ a obhajob bakalářských a diplomových prací, musí splnit následující povinnosti:

1. Studenti, kteří neuspěli v prvním termínu SZZ v části „obhajoba bakalářské/diplomové práce“ a byli hodnoceni stupněm „F – nedostatečně“, se dostaví ústav administrující jeho obor (oborový ústav). **Do 26. 7. 2012 přinesou sekretářce oborového ústavu nový podklad k zadání** bakalářské/diplomové práce vytvořený společně s vedoucím práce (a podepsaný vedoucím práce), v souladu s doporučením komise pro SZZ. Podklad k zadání se vytváří v IS/STAG (ne v BPDP).
2. **Při odevzdání podkladu si dohodnou termín vyzvednutí Oficiálního zadání** bakalářské/diplomové práce.
3. Ke dni **31. 8. 2013 podají přihlášku** do navazujícího magisterského studijního programu v souladu se Směrnicí ke 2. kolu přijímacího řízení do navazujících

„VYHRAZENÉ“

VZOR

Obr. 1-1 Vzor označení utajovaného dokumentu

1.2.4 Fyzická bezpečnost

Fyzická bezpečnost je soubor opatření k fyzické ochraně utajovaných informací. V tomto směru se jedná o způsob ochrany zabezpečených objektů, zabezpečených oblastí a jednacích oblastí proti vniknutí neoprávněné osoby. (1) (6)

Národní bezpečnostní úřad definuje podmínky pro mechanické zábranné prostředky, elektrická zámková zařízení, prostředky zabezpečovacích a tísňových systémů, speciálních televizních systémů, zařízení elektrické požární signalizace, zařízení sloužících k vyhledávání nebezpečných látek a předmětů, zařízení fyzického ničení nosičů informací a zařízení proti pasivnímu a aktivnímu odposlechu utajované informace. Zařízení používaná k ochraně utajovaných informací musí vlastnit certifikát na požadovaný stupeň bezpečnosti vydaný Národním bezpečnostním úřadem. (1) (6)

Zabezpečenému objektu v tomto případě říkáme prostoru (budova, poschodí v budově, nebo ohraničený prostor), ve kterém se nacházejí jednací a zabezpečené oblasti. V zabezpečeném objektu je povoleno zpracovávat utajované informace, ale není možné je v něm projednávat, nebo ukládat. Právě pro ukládání a projednávání utajovaných informací je nutně zřídit pod-objekty (zabezpečené a jednací oblasti), které mají přísnější ochranná opatření. (1) (6)

Zabezpečené a jednací oblasti se klasifikují stupněm utajení, který odpovídá maximálnímu stupni utajení informace, která se v dané oblasti může ukládat, zpracovávat a projednávat. Pro dodržení standardu zabezpečení utajované informace je oprávněná osoba povinna zpracovat projekt fyzické bezpečnosti daného prostoru. V projektu fyzické bezpečnosti jsou uvedena všechna technická zařízení, minimální požadavky stavebních konstrukcí a ostatních prvků bezpečnosti, včetně režimových opatření, ostrahy a následného bodového hodnocení. Pro objekty kategorie „DŮVĚRNÉ“ a vyšší musí projekty fyzické bezpečnosti obsahovat přesné určení objektu a zabezpečených oblastí včetně jejich hranic, kategorií a tříd zabezpečených oblastí. Dalšími povinnostmi je vypracování analýzy rizik, způsob opatření fyzické bezpečnosti, provozní řád objektu a plán zabezpečení objektu a zabezpečených oblastí v krizových situacích. Naopak u objektů kategorie „VYHRAZENÉ“ postačuje určení objektu a zabezpečených oblastí včetně jejich hranic, kategorií a tříd zabezpečených oblastí a způsobu použití opatření fyzické bezpečnosti. (1) (6)

1.2.5 Bezpečnost informačních a komunikačních systémů

Tento druh ochrany utajovaných informací jasně specifikuje pojem informační a komunikační systém. Informační systém je podle paragrafu 34 odstavce 1, zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti jeden nebo více počítačů s programovým vybavením a nezbytnými periferiemi. Počítač jako systém je

schopný provádět sběr, tvorbu, zpracování, ukládání zobrazení a přenos utajovaných informací. Komunikačním systémem se dle paragrafu 35, odstavce 1, zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti rozumí systém, který zajišťuje přenos utajovaných informací mezi koncovými uživateli a tedy koncovými komunikačními zařízeními využívajícími přenosové prostředí, kryptografické prostředky a provozní podmínky a postupy. Použití komunikačních a informačních systému podléhá certifikaci Národního bezpečnostního úřadu a systémy nesmí být zprovozněny bez řádné provozní a bezpečnostní dokumentace. Podrobně bude ochrana utajovaných informací popsána v kapitole č. 2. (1) (7)

1.2.6 Kryptografická ochrana

Tento oddíl ochrany utajovaných informací přesně vymezuje kryptografický materiál, kryptografický prostředek, kryptografický dokument a další materiál nezbytný k zajištění činnosti kryptografické ochrany. Všechny součásti kryptografické ochrany podléhají certifikaci Národního bezpečnostního úřadu. Všechen kryptografický materiál musí být evidován v provozní dokumentaci a administrativních záznamních pomůckách. Předávání materiálu provozní obsluze, kurýrům kryptografického materiálu, podléhá požadavkům administrativní bezpečnosti. Dále tento oddíl vymezuje kryptografické pracoviště, což je místo, kde se nejen pracuje s kryptografickou technikou (probíhá šifrování utajovaných informací), ale i místo, kde se kryptografické prostředky testují, předávají, ukládají a vyrábí. Kryptografické pracoviště musí splňovat bezpečnostní standardy podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a podléhá schválení bezpečnostního ředitele dané organizace. (1) (8)

Obsluha kryptografické ochrany podléhá zvláštnímu režimu. Obsluha musí disponovat zvláštní odbornou způsobilostí a zahrnuje dobrou znalost platných právních předpisů, norem a směrnic (provozní dokumentace). Každý pracovník kryptografické ochrany, který je vyčleněn jako pracovník se zvláštní odbornou způsobilostí, musí úspěšně absolvovat zkoušku u Národního bezpečnostního úřadu, nebo u orgánu Národním bezpečnostním úřadem k tomuto účelu zmocněnému (na základě smlouvy). (1) (8)

2 BEZPEČNOST INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMŮ

Bezpečnost komunikačních a informačních systémů nakládajících s utajovanými informacemi upravuje vyhláška NBÚ č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízeních s utajovanými informacemi a o certifikaci stínicích komor. Samotná vyhláška pak vymezuje základní pojmy, jako jsou aktiva informačního systému (hardware, software, dokumentace), pasivní prvky, aktivní prvky, analýza rizik, identifikace a autentizace subjektu apod. (7)

Dále vyhláška NBÚ 528/2005Sb., vymezuje pojmy:

- **důvěrnost** utajované informace, což znamená, že utajovaná informace obsahuje atributy znemožňující její zneužití,
- **integrita** utajované informace představuje odolnost proti pozměnění utajované informace neoprávněnou osobou,
- **dostupnost** utajované informace je zajištění potřebného přístupu k utajované informaci pouze oprávněným osobám. (7)

Ve vyhlášce NBÚ č. 523/2005 Sb., jsou jednoznačně definované a dále rozepsané oblasti, které jsou nezbytné k dodržení bezpečnostního standardu. Těmito oblastmi jsou:

a) Počítačová a komunikační bezpečnost,
b) kryptografická ochrana,
c) ochrana proti úniku kompromitujícího vyzařování,
d) administrativní bezpečnost a organizační opatření,
e) personální bezpečnost,
f) fyzická bezpečnost informačního systému. (7)

Dále vyhláška NBÚ č. 523/2005 Sb., vymezuje povinnost vést bezpečnostní dokumentaci, která se dělí na projektovou bezpečnostní dokumentaci a provozní bezpečnostní dokumentaci. (7)

Projektová bezpečnostní dokumentace:

- bezpečnostní politika informačního systému,
- návrh bezpečnosti informačního systému,
- a testování bezpečnosti informačních systémů. (7)

Provozní bezpečnostní dokumentace:

- bezpečnostní směrnice informačního systému pro bezpečnostní správce, správce (administrátory) a uživatele. (7)

2.1 Bezpečnostní politika informačního systému

Bezpečnostní politika je strategický a koncepční dokument, který se zpracovává před samotným zřízením utajovaného informačního systému. V bezpečnostní politice jsou uvedeny základní nástroje, normy a postupy nezbytné k ochraně utajovaných informací s ohledem na zajištění důvěrnosti, integrity a dostupnosti celého informačního systému i jednotlivých utajovaných informací. Pro zajištění bezpečnosti je nutné vymezit základní hrozby a jejich míry rizika, které ohrožují informační systém (analýza rizik). Na základě analýzy rizik se v Bezpečnostní politice vymezí základní požadavky na jednotlivé oblasti bezpečnosti. Bezpečnostní politika obsahuje i způsob nastavení a zřízení jednotlivých přístupových rolí (uživatel, administrátor, bezpečnostní správce). Při nastavování bezpečnostní politiky je nutné vzít v úvahu, že je to dokument, na který navazuje ostatní bezpečnostní dokumentace. Bezpečnostní politika a její požadavky na bezpečnost musí korespondovat s požadovaným stupněm utajení. (7) (9) (10) (11)

2.1.1 Počítačová bezpečnost

Minimální bezpečnostní požadavky se podle vyhlášky NBÚ č. 523/200Sb., dělí na požadavky klasifikované stupněm utajení „VYHRAZENÉ“ a na požadavky pro informační systémy klasifikované podle stupňů utajení na „DÚVĚRNÉ, TAJNÉ a PŘÍSNĚ TAJNÉ“. (7)

Minimálními požadavky pro systémy stupně utajení „VYHRAZENÉ“ je povinnost zavést pro přístup do informačního systému jednoznačnou identifikaci a autentizaci všech uživatelů, administrátorů a bezpečnostního správce. Dále je to povinnost řízení přístupů do informačního systému tak, aby uživatel disponoval jenom takovými oprávněními, která jsou nutná ke zpracování utajovaných informací. Následuje povinnost zřídit nepřetržité

zaznamenávání činností systému a uživatelů tak, aby bylo možné provádění bezpečnostních auditů. Dalším opatřením je zajištění ochrany nosičů utajovaných informací před použitím v jiných informačních systémech (bezpečný výmaz, způsob ukládání, bezpečné přidělování) a nakonec zajištění důvěrnosti při přenosu utajovaných dat mezi odesílatelem a adresátem (použití kryptografie). (1) (7)

U informačních systémů klasifikovaných stupněm utajení „DŮVĚRNÉ“ a vyšším použijeme předchozí minimální požadavky, navíc ale použijeme k zajištění bezpečnostních funkcí programově technické mechanizmy (kryptografie nejen při přenosu, ale i při ukládání utajované informace). Tyto mechanizmy musí být neustále udržovány v provozu schopném stavu během celého životního cyklu informačního systému a u bezpečnostního správce musí k daným prostředkům být uložena dokumentace o jejich obsluze a aktualizaci. (1) (7)

2.1.2 Provozní bezpečnostní módy

Způsob přístupu do utajovaného informačního systému upravuje Národní bezpečnostní úřad svou vyhláškou č. 523/2005 Sb. Národní bezpečnostní úřad definuje čtyři druhy provozních módů:

a) Bezpečnostní provozní **mód vyhrazený**. Tento provozní mód lze použít pro utajované informační systémy různé klasifikace. Všichni uživatelé mohou zpracovávat všechny utajované informace, které jsou v informačním systému obsaženy, ale také musí být všichni držiteli osvědčení na nejvyšší stupeň utajení v informačním systému. V tomto přístupovém módu není povinnost upravovat oprávnění (mají všichni stejná oprávnění – vyjma administrátora a bezpečnostního správce). (7)

b) Bezpečnostní **mód s nejvyšší úrovní**. Oproti provoznímu módu vyhrazenému musí být dodrženy všechny požadavky na bezpečnost systému, protože tento mód umožňuje, aby v informačním systému pracovaly osoby, které nemají přístup ke všem utajovaným informacím. Přesto pro všechny uživatele platí, že musí být držiteli oznámení, nebo osvědčení na nevyšší stupeň utajovaných informací v informačním systému. (7)

c) Bezpečnostní provozní **mód s nevyšší úrovní a formálním řízením** přístupu se používá v rozsáhlých utajovaných informačních systémech, kde je přístup řešen z centrálního místa (serveru). (7)

d) Poslední bezpečnostní **mód víceúrovňový** umožňuje v jednom informačním systému zpracovávat různě klasifikované utajované informace, kdy oprávnění zpracovávat všechny utajované informace mají všichni uživatelé. Zároveň musí být všichni uživatelé držiteli oznámení nebo osvědčení na nevyšší stupeň utajovaných informací v informačním systému. Tento provozní mód se používá u rozsáhlého informačního systému. Musí zde být dodrženy všechny požadavky na bezpečnost a musí být zajištěn nepřetržitý přístup k utajovaným informacím (rozdíl oproti provoznímu módu vyhrazenému). Velký zřetel je tu dán na ochranu integrity celého systému a funkci povinného řízení systému. Tento informační systém musí být schopen označit výstupní utajovanou informaci a přiřadit vstupní utajované informaci její stupeň utajení. (7)

2.1.3 Bezpečnost počítačových sítí

Pro zachování důvěrnosti a integrity utajované informace při přenosu utajované informace uvnitř nějaké sítě musí být použity kryptografické prostředky schválené Národním bezpečnostním úřadem, ale i softwarové prostředky, které jsou schopny detekovat záměrné i náhodné změny utajovaných informací. Toto neplatí, pokud infrastruktura (síťové komunikační linky) je vedena uvnitř zabezpečeného objektu a samotné počítače jsou umístěny v zabezpečených oblastech. V tomto případě kryptografická ochrana nemusí být na požadované úrovni, nebo může být vyloučena zcela (záleží na analýze rizik a schválení Národního bezpečnostního úřadu). (7)

2.1.4 Bezpečnost dostupnosti a služeb utajované informace

Společně s důvěrností a integritou je dostupnost utajované informace jedním ze základních kriterií bezpečnosti. V rámci utajovaného informačního systému je povinnost zabezpečit, aby poskytovaná informace byla dostupná kdykoliv je to třeba, a to ve stanovené formě a na stanoveném místě. Proto je nutné zajistit řešení mimořádných událostí, které by měly negativní dopad na stav informací a přijmout adekvátní opatření, jako jsou periodická zálohování na jiné klasifikované nosiče utajovaných informací než samotný utajovaný pevný disk. (7)

2.1.5 Bezpečnost propojení informačních systémů

K propojení může dojít jen u certifikovaných informačních systémů. Rozdíl je, jestli se jedná o informační systémy klasifikované stejným nebo různým stupněm zabezpečení. Propojení informačních systémů schvaluje Národní bezpečnostní úřad a provádí to pouze

v případech, kdy je to nebytné pro provozní potřebu. Pokud dochází k propojování informačních systémů stejné klasifikace, tak se doplňuje pouze vhodným kryptografickým zařízením. Pokud ale dochází k propojení informačních systémů různé klasifikace, je nezbytné softwarovými prostředky zabezpečit, aby se do informačního systému nižší kategorie nedostaly utajované informace klasifikované vyšším stupněm utajení. Ve výjimečných případech se jako prostředek pro propojení dvou informačních systému může použít veřejná komunikační síť. (7)

2.1.6 Analýza rizik

Jak už bylo uvedeno výše, pro zajištění bezpečnosti je potřeba provést řádnou analýzu rizik. Při analýze rizik se zaměřujeme hlavně na použitá aktiva a další komponenty informačních systémů. Výstupem procesu analýzy rizik je seznam hrozeb ohrožujících části informačního systému. Nutností je provádět analýzu rizik komplexně a odborně. (7)

2.1.7 Nahrazení prostředků počítačové bezpečnosti

Některé prostředky bezpečnosti informačního systém je možno nahradit zvýšenou personální, fyzickou a administrativní bezpečností, ale i speciálními organizačními opatřeními. To vše ale pouze v odůvodněných případech a se souhlasem Národního bezpečnostního úřadu. Příkladem by mohlo být použití vyjímatelných nosičů utajovaných informací vydávaných oproti podpisu a standardně ukládaných v mimopracovní době v nějakém certifikovaném úschovném objektu dané kategorie. (7)

2.1.8 Ochrana mobilních a přenosných informačních systémů

Mobilní a jinak přenosné informační systémy se posuzují velmi specificky. Tato zařízení jsou koncipována pro přenášení, a proto i způsob přenášení musí podléhat analýze rizik včetně použitých dopravních prostředků. Při přenášení mobilního zařízení se postupuje stejně, jako by byl přenášen jakýkoli utajovaný paměťový nosič v souladu s vyhláškou NBÚ č. 525/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací. (7)

2.1.9 Ochrana proti kompromitujícímu vyzařování

Tento druh ochrany je velmi specifický a ověřování rizikového elektromagnetického vyzařování jednotlivých komponentů informačního systému je prováděno přímo Národním bezpečnostním úřadem nebo odbornou certifikovanou firmou. Vyhláška 523/2005 Sb.

stanoví, že měření elektromagnetického vyzařování a jeho následná ochrana se provádí u klasifikovaných informačních systémů stupně utajení „DŮVĚRNÉ“ a vyšších. (7)

2.1.10 Bezpečnost nosičů utajovaných informací

Každé paměťové medium informačního systému musí být řádně zaevidováno tak, aby byl jasně zaznamenán pohyb a vlastník. Dále musí být nosič utajované informace klasifikován na stupeň utajení nejvyšší uložené utajované informace. Na paměťovém mediu musí být uvedeno patřičné evidenční číslo. Dále musí být na nosiči utajované informace uveden název informačního systému a samozřejmě i stupeň utajení. Výjimkou je pouze nosič utajovaných informací zabudovaný v mobilním zařízení. V tomto případě se označuje celé paměťové zařízení a samotný nosič okamžitě po vyjmutí ze zařízení. (1) (5) (7)

Národní bezpečnostní úřad připouští i deklasifikací nosičů utajovaných informací, tedy snížení stupně utajení, nebo jeho úplné zrušení. Tento proces je ale možný pouze u nosičů utajovaných informací stupně utajení „TAJNÉ“ (pouze snížit) „DŮVĚRNÉ“ (snížit i zrušit) „VYHRAZENÉ“ (zrušit) za předpokladu, že na nosiči byly uloženy utajované informace nižšího stupně utajení, nebo dojde k provedení bezpečného výmazu. Bezpečný výmaz je způsob znemožnění obnovení uložených dat prováděný speciálními softwarovými prostředky. V rámci stupně utajení „PŘÍSNĚ TAJNÉ“ je deklasifikace nosiče možná jen za předpokladu prokázání skutečnosti, že na daném nosiči se nikdy nevyskytovaly utajované informace nejvyššího stupně utajení. (7)

Přesný způsob a podmínky bezpečnostního výmazu stanovuje Národní bezpečnostní úřad v bezpečnostním standardu, a pokud je v informačním systému možnost deklasifikace, tak musí být přesný postup uveden v provozní bezpečnostní dokumentaci. (7)

Pokud nosiče utajovaných informací již přestanou plnit svůj účel, nebo se stanou zcela nepotřebnými, je nezbytné provést jejich úplné zničení tak, aby bylo znemožněno jejich opětovné zapojení. (7)

2.1.11 Přístup k utajované informaci v informačním systému

Pro zajištění bezpečného přístupu do utajovaného informačního systému se zřizují tři základní role. Jedná se o správce systému (administrátor), bezpečnostního správce (garant bezpečnosti, někdy spojen s funkcí administrátora) a uživatele. Každý kdo potřebuje mít

přístup do utajovaného informačního systému, musí být držitelem platného oznámení, nebo osvědčení se shodným nebo vyšším stupněm utajení informačního systému. Výjimka je u bezpečnostního správce a administrátora. Administrátor a bezpečnostní správce musí být držiteli osvědčení, které je o minimálně jeden stupeň vyšší, než je stupeň utajení informačního systému (neplatí u kategorie „PŘÍSNĚ TAJNÉ„. Každému z uživatelů až na ojedinělé výjimky musí být přirazen jedinečný identifikátor (výjimkou v tomto případě může být užívání externího nosiče utajovaných informací vydávaného oproti podpisu). Uživatelům se přidělují pouze ta oprávnění, která potřebují k samotné práci v informačním systému. (7)

2.1.12 Odpovědnost za činnost

Odpovědnosti uživatelů, bezpečnostního správce a administrátora jsou uvedeny v provozní bezpečnostní dokumentaci. Při tvorbě utajovaných informací je odpovědnou osobou jejich tvůrce až do doby, kdy utajovanou informaci schválí nadřízená autorita. (7)

2.1.13 Personální bezpečnost při provozu informačního systému

Všichni uživatelé přistupují do systému na základě identifikace a autentizace. Řízení uživatelských účtů musí aktuálně korespondovat s přidělenými rolemi. Každý uživatel, bezpečnostní správce a administrátor musí být proškolen o povinnostech vyplývajících z provozní bezpečnostní dokumentace, a pokud uživatel přestane splňovat některé z povinností a podmínek k přístupu k utajované informaci, musí mu být uživatelský účet v informačním systému neprodleně uzamčen. Školení musí být provedeno před samotným přístupem do informačního systému s následnou periodou dlouhou jeden rok. (7)

2.1.14 Fyzická bezpečnost

Všechny komponenty (aktiva) informačního systému musí být ukládané v zabezpečených oblastech tak, aby zamezovaly přístupu k informačnímu systému neoprávněnou osobou. Nejedná se ale pouze o zabránění fyzického přístupu, ale i o ochranu proti možnosti dálkového odezírání. Míra zabezpečení zabezpečených oblastí a objektů musí úměrně odpovídat nejvyššímu stupni uložených utajovaných informací. Konkrétní požadavky pro fyzickou ochranu utajovaných informací jsou uvedeny ve vyhlášce NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. (7) (6)

2.1.15 Bezpečnost při instalaci informačního systému

Instalaci programů, které jsou významné pro bezpečnost informačního systému, provádí pouze bezpečnostní správce a administrátor. Vymezení těchto softwarových součástí a oprávněných rolí musí být uvedeno v bezpečnostní politice informačního systému. Lze definovat i komponenty, které si je schopen nainstalovat oprávněný uživatel sám. Instalaci součástí informačního systému osobami, které nesplňují podmínky zákona č. 412/2005Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti lze umožnit pouze v případě, je-li neoprávněná osoba pod přímým dohledem bezpečnostního správce. (7)

2.1.16 Bezpečné provozování informačního systému

Bezpečnost informačního systému je zajištěna splněním konkrétních požadavků vyplývajících z analýzy rizik a prostřednictvím neustálého prověřování a vyhodnocování chodu utajovaného informačního systému. Před prováděním dílčí změny v utajovaném informačním systému je nutné nejprve provést opětovnou analýzu dopadů této změny na bezpečnost a certifikaci Národním bezpečnostním úřadem. Při vybírání programového vybavení je nutné brát zřetel na integritu programového vybavení (legální a aktuální software) a ochranu proti působení škodlivého programového kódu (aktuální antivirový program). Schválené hardwarové a softwarové vybavení musí být uvedeno v provozní bezpečnostní dokumentaci a podléhá schvalovacímu procesu Národního bezpečnostního úřadu. Použité programové vybavení musí být řádně zálohované takovým způsobem, aby v případě potřeby bylo možné požadovaný software znovu přeinstalovat, nebo nainstalovat. Záloha programového vybavení musí být uložena tak, aby nedošlo k jejímu poškození (nejlépe jako samotná utajovaná informace). (1) (7) (10) (11) (9) (12)

Potenciální servis jako činnost je též nutné upravit v provozní bezpečnostní dokumentaci. Při opravování komponentů informačního systému, musí být vše zajištěno tak, aby neoprávněná osoba, nebo osoby servisující části informačního systému nepřišly do styku s utajovanou informací. K udržení bezpečného chodu informačního sytému je nezbytné i provádění pravidelné údržby tak, aby byla minimálně snížena rizika opotřebení nebo poškození, například nahromaděným prachem. Údržbu by měl provádět administrátor nebo bezpečnostní správce systému. Pokud se jedná o údržbu komponentů, které nemají přímý vliv na bezpečnost systému, tak tu může provádět i uživatel. (1) (7) (10) (11) (9) (12)

V provozní bezpečnostní dokumentaci musí být uveden i způsob a časový harmonogram zálohování auditních záznamů informačního systému, aby v případě jakékoliv krize bylo možné auditní záznamy vyhodnotit. Pro řešení krizových situací musí být v provozní bezpečnostní směrnici uveden jednoduchý scénář řešení. Významné krizové situace musí být v provozní bezpečnostní situaci vyjmenovány. (1) (7) (10) (11) (9) (12)

2.2 Komunikační systém

Dokumentace klasifikovaného komunikačního systému obsahuje:

a) bezpečnostní politiku komunikačního systému,

b) organizační a provozní postupy provozování komunikačního systému,

c) provozní směrnice pro bezpečnostní správu komunikačního systému,

d) provozní směrnice uživatele komunikačního systému. (7)

Rozdíl oproti dokumentaci utajovaných informačních systémů je tedy v povinnosti zřídit dokument zvaný organizační a provozní postupy provozování komunikačního systému. Tento dokument musí obsahovat způsob zajištění kryptografické ochrany, tedy šifrování v souladu s bezpečnostním standardem Národního bezpečnostního úřadu. Dále se v tomto dokumentu musí uveřejnit provozní a bezpečnostní správa včetně organizačních opatření a provozních zásad, jejímž cílem je ochrana utajovaných informací. (7) (13)

Konkrétní směrnice pro správce a uživatele budou již separátně obsahovat konkrétní povinnosti a zásady postupů a činností v utajovaných komunikačních systémech. (7)

2.3 Návrh bezpečnosti informačního a komunikačního systému

Jak bylo uvedeno v předchozí kapitole 2.1, návrh bezpečnostních opatření konkrétně navazuje na Bezpečnostní politiku informačního a komunikačního systému. V návrhu bezpečnosti informačního a komunikačního systému se již uvádí konkrétní kroky, systémová a organizační opatření k docílení požadovaného bezpečnostního standardu. Návrh bezpečnosti tedy již obsahuje konkrétní způsoby identifikací a autentizací uživatelů, řízení uživatelských rolí a přístupu k samotnému informačnímu systému (dostupné provozní módy). Dále se jedná o konkrétní bezpečnostní opatření pro hardware, programové vybavení, způsoby bezpečného přenosu dat mezi jednotlivými komponenty informačního a komunikačního systému i přenos dat mezi jinými

informačními systémy. V návrhu bezpečnosti informačního a komunikačního systému musí být i konkrétně upraveno použití opatření fyzické bezpečnosti, školení jednotlivých uživatelů, ukládání klasifikovaných nosičů utajovaných informací, způsoby provádění auditů systému, vyjmenované bezpečnostní incidenty a jejich reakce na ně, reakce na možné havárie a způsoby oprav jednotlivých komponentů. Konkrétní návrh bezpečnostních opatření zaměřený na počítačovou bezpečnost informačního systému stupně utajení „VYHRAZENÉ“ je uveden v praktické části této bakalářské práce. (7) (10) (11) (12)

2.4 Testování bezpečnosti informačních a komunikačních systémů

Testování bezpečnosti informačního systému je třetím krokem před samotným úspěšným zahájením provozu utajovaného informačního systému. Testují se všechny požadavky na bezpečnostní standard utajovaného informačního systému a výstup z tohoto testování musí mít listinou formu. Odpovědnou osobou je zde zřizovatel utajovaného informačního systému. (7)

2.5 Směrnice bezpečnostního správce a správce systému

Zatímco výše zmíněné dokumenty popisují povinnosti a požadavky na bezpečnostní standard všech oprávněných osob utajovaného informačního a komunikačního systému, Směrnice bezpečnostního správce a správce utajovaného informačního a komunikačního systému jsou zaměřeny pouze na ně osobně (bezpečnostního správce a administrátora). (7)

Směrnice správce a bezpečnostního správce systému v úvodu obsahuje jmenný seznam odpovědných osob organizace a bezpečnostní správy s přímými kontakty na ně. Jmenný seznam musí být vždy aktuální. Následuje výčet povinností správců, nebo správce, pokud je administrátor a bezpečnostní správce jedna osoba. (7)

Mezi tyto povinnosti patří zajištění personální bezpečnosti, kdy bezpečnostní správce vede seznam oprávněných uživatelů, záznamy o jejich školení a platnosti jejich osvědčení nebo oznámení. Správce dále odpovídá za dodržování fyzické bezpečnosti zabezpečených oblastí a objektů, kde se ukládají a zpracovávají utajované informace. Stejně významnou povinností je i odpovědnost za počítačovou bezpečnost, kde hlavními úkoly jsou zajištění provedení všech nastavení z návrhu bezpečnostních opatření, a tedy například požadavek na délku a kvalitu hesla, jedinečnou identifikaci a autentizaci, požadavek na řízení přístupu, bezpečností vstupů s výstupů, způsoby přenosu dat apod. Dále je nezbytná

povinnost bezpečnostního správce provádět periodické kontroly sytému a tedy programového vybavení, systémových nastavení operačního systému a kontroly funkčnosti hardwaru. Následuje povinnost dodržování administrativní bezpečnosti a tedy povinnost evidovat nosiče utajovaných informací a označit nosiče, komponentů i celého informačního systémů štítky s povinnými údaji. V neposlední řadě se jedná o činnosti spojené s ochranou proti kompromitujícímu elektromagnetickému vyřazování, komunikační bezpečnost apod. (7)

2.6 Směrnice uživatele

Obdobně jako směrnice správce a bezpečnostního správce, jednoznačně upravují tyto směrnice povinnosti a činnosti samotných uživatelů. Ve směrnicích uživatele jsou jmenovitě uvedeny odpovědné osoby a bezpečnostní správa organizace s telefonními kontakty. (7) (11) (10)

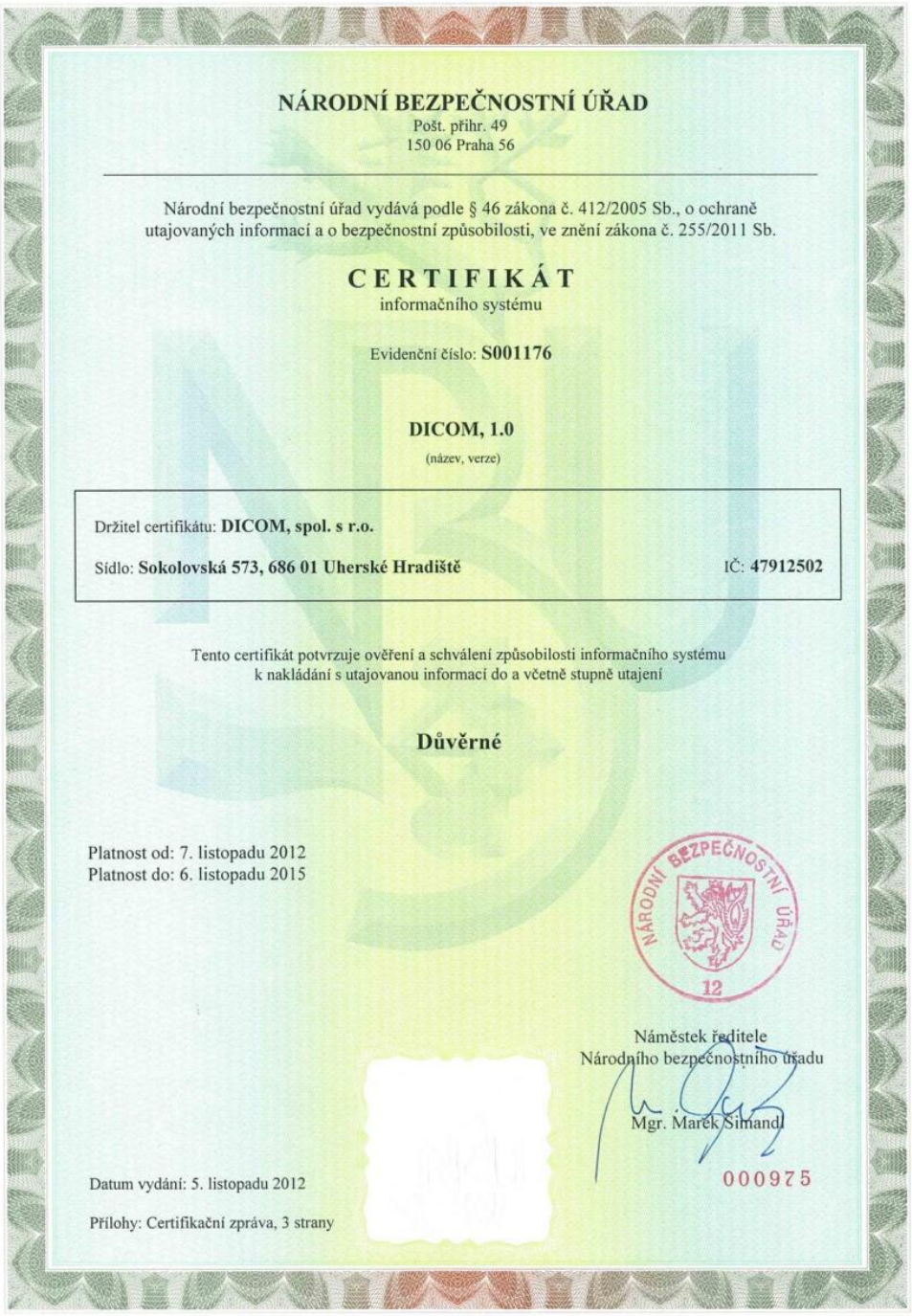
Mezi základní povinnosti uvedené v těchto směrnicích patří požadavky na tvorbu a kvalitu hesla, vysvětlení pojmu „need to know“ (seznamovat se pouze s takovými utajovanými informacemi, které jsou bezpodmínečně potřebné k výkonu funkce), způsoby a podmínky pro jedinečnou identifikaci a autentizaci, způsob ukládání utajovaných informací a přidělené diskové místo, nakládání s utajovanou informací včetně jejího ukládání do úschovných objektů, vymezení povinností spojených s reakcí na detekci narušení integrity důvěrnosti a dostupnosti spojenou se způsobem hlášení samotných bezpečnostních incidentů apod. (7) (11) (10)

2.7 Certifikace

Schvalování informačních a komunikačních systémů provádí Národní bezpečnostní úřad na žádost státního orgánu, nebo podnikatele (právnické, nebo podnikající fyzické osoby). V žádosti musí být uvedeny identifikační údaje osoby, informace a kontakt pověřeného pracovníka, stupeň a číslo osvědčení/oznámení/prohlášení osoby, nebo podnikatele, stručný popis systému a další údaje vyžadované podle vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi. (7)

Schvalování projektu probíhá formou správního řízení, kdy dochází k posouzení jednotlivých požadavků na bezpečnost. Posouzení probíhá až po zřízení informačního systému a k tomu potřebné dokumentace. Pokud Národní bezpečnostní úřad shledá splnění

všech podmínek, tak vydá souhlas s provozováním informačního a komunikačního systému formou přiděleného certifikátu. (7)



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, ve znění zákona č. 255/2011 Sb.

CERTIFIKÁT
informačního systému

Evidenční číslo: **S001176**

DICOM, 1.0
(název, verze)

Držitel certifikátu: **DICOM, spol. s r.o.**

Sídlo: **Sokolovská 573, 686 01 Uherské Hradiště** IČ: **47912502**

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

Důvěrné

Platnost od: 7. listopadu 2012
Platnost do: 6. listopadu 2015

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
12

Náměstek ředitele
Národního bezpečnostního úřadu
Mgr. Marek Šimandl

Datum vydání: 5. listopadu 2012

000975

Přílohy: Certifikační zpráva, 3 strany

Obr. 2-1 Ukázka certifikátu utajovaného informačního systému[1]

[1]Dostupně z: http://www.dicom.cz/cs/art/1261-certifikaty

II. PRAKTICKÁ ČÁST

3 NEJČASTĚJŠÍ BEZPEČNOSTNÍ RIZIKA V INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMECH

Nejčastější rizika informačního systému ohrožují jeho nejvíce zranitelná místa. I v tomto případě platí, že celý informační systém je tak bezpečný, jak bezpečné je nejslabší místo celého systému. Hrozby ohrožující informační systém se dělí do dvou základních hledisek, kterými jsou hledisko objektivní a subjektivní. Konkrétní případy jsou uvedeny v následujících kapitolách. Vzniklý stav ohrožující integritu, důvěrnost a dostupnost utajované informace se nazývá **bezpečnostní incident**. (10) (11) (12) (9)

3.1 Objektivní

Do objektivního rizika lze zahrnout všechny možné druhy živelných katastrof, poruch a havárií. Jsou to tedy taková rizika, která nejsou spojena s činností člověka. (9) (12)

3.1.1 Povodně

Jsou živelnou pohromou, na kterou je nutno brát zřetel tehdy, pokud se objekt, ve kterém je umístěn utajovaný informační systému, nachází v záplavové oblasti nebo poblíž nějakého vodního toku. (9) (12)

3.1.2 Požár

Je specifickou hrozbou, která může vzniknout přírodními vlivy, ale i jako porucha technických zařízení. Zvýšené riziko požáru je u objektu, který se nachází v zalesněném prostoru či areálu, nebo je samotný objekt klasifikován jako objekt se zvýšeným požárním nebezpečím (z důvodu výskytu hořlavin, výbušnin apod.) (9) (12)

3.1.3 Výpadek dodávek elektrické energie

Tento druh hrozby ohrožuje hlavně dostupnost utajované informace. Zvýšené riziko spojené s výpadkem elektrické energie se řeší instalací náhradního zdroje napětí, a to v buď přidaného velkokapacitního akumulátoru, případně naftového nebo benzínového agregátu. (9) (12)

3.1.4 Porucha

Je druh hrozby, která vzniká přerušením funkčnosti celého utajovaného informačního systému z důvodu závady na jednom či více komponentech. Samotná porucha může vzniknout přestárnutím části informačního systému, nebo na základě kolísavých dodávek elektrického napětí, nebo fyzickým opotřebením. (9) (12)

3.1.5 Havárie

Mezi objektivní hrozby lze havárii zahrnout, pokud vznikne na základě technické havárie, nebo jako následek požáru nebo povodně. Havárie je spojena s únikem nebezpečné látky, a to buď toxické, biologické, karcinogenní, nebo jinak ohrožující lidské zdraví. Riziko havárie je úzce spjaté s vzdálenosti od objektu, ve kterém se zpracovávají, ukládají, nebo vyrábí nebezpečné látky. Důležitým faktorem je i množství a druh nebezpečné látky v objektu. Potřebné informace podstupuje místně příslušný Hasičský záchranný sbor kraje, nebo hlavního města Prahy. (9) (12)

Ochranným opatřením ve všech výše uvedených případech je zpracování havarijního plánu, ve kterém je přesně uveden postup jednotlivých činností dotčených osob při reakci na kritickou událost. Ochrana života a zdraví má vždy přednost před ochrannou utajovaných informací. Utajované informace ale mají vždy přednost před ochranou majetku. (9) (12) (10)

3.2 Subjektivní

Tato rizika jsou vždy spojena s činností člověka, a to buď přímo uživatele, správce, popřípadě bezpečnostního správce, nebo osoby cizí, která nepatří mezi vybrané osoby s povoleným přístupem k utajované informaci. (9) (12)

3.2.1 Porušení povinnosti z provozní bezpečnostní směrnice

Tento druh rizika je spojen s vnitřním ohrožením, kdy se bezpečnostního incidentu dopustí osoba, která je oprávněná ve stanovaném rámci k přístupu do utajovaného informačního systému. Jedná se zejména o porušení povinností vyplývajících z bezpečnostních směrnic uživatele a bezpečnostních směrnic bezpečnostního správce a správce systému. (9) (12)

Mezi tato rizika patří především:

- Sdílení uživatelských nebo administrátorských účtů,
- neoprávněné použití administrátorského účtu,
- použití falešné identifikace a autentizace uživatele, administrátora nebo bezpečnostního správce,
- odhalení škodlivého kódu nebo viru,
- vícenásobné neúspěšné pokusy o přihlášení do informačního systému,
- potenciální nebo reálné prozrazení hesla,
- umožnění přihlášení do informačního systému takové osoby, která není držitelem platného oznámení, nebo osvědčení na daný stupeň utajení,
- pozměnění nastavení systému v rozporu s provozní bezpečnostní dokumentací,
- používání necertifikovaného informačního systému ke zpracování utajovaných informací. (9) (12) (10)

3.2.2 Sabotáž

Sabotáž je druh útoku, který napadá funkčnost utajovaného informačního systému, ale i konkrétní utajované informace tak, aby byla narušena jeho důvěrnost a integrita. Smyslem sabotáže je provést viditelné, ale i skryté změny v informačním systému, ale i konkrétních utajovaných informací, kdy původce může být jak pověřená osoba k přístupu do utajovaného informačního systému, tak i osoba zvenčí. Statisticky je prokázáno, že 80% ze všech sabotáží je prováděno vlastními zaměstnanci, které k tomu nejčastěji vedou nepřátelské vztahy s nadřízenými, vydírání, tíživá finanční situace, nebo jen chuť se nezákonně obohatit. Vůbec nejefektivnější způsob útoku (platí i pro teroristické a hackerské útoky) je spojení mezi vlastním zaměstnancem a osoby zvenčí. Proti těmto útokům je třeba zavést speciální systémová opatření, jejichž příklady jsou uvedeny v kapitole 6. (9) (12) (10)

3.2.3 Teroristický útok

Jeden z nejzákeřnějších a nejnebezpečnějších útoků je právě útok teroristický. Terorismus se snaží o politické a mocenské ovládnutí daného území prostřednictvím budování obav společnosti o vlastní život. Pro terorismus je význačné napadat strategicky

a společensky důležitá místa a objekty, aby dopad na společnost byl co největší. Zvýšené riziko je proto hlavně u informačních systémů zahrnutých do kritické infrastruktury apod. (9) (12) (10)

3.2.4 Hacker

Tento druh útoku se vyznačuje dálkovým překonáváním informačního systému, který je zpravidla napojen na veřejnou síť (internet). Jsou čtyři základní typy útočníků. Základní dělení vystihuje povahu útoku. (9) (12) (10)

Prvními jsou ti, kteří vykonávají činnost hackera za úplatu, a tedy tento druh činnosti je pro ně povoláním. Tento druh útoků se vyskytuje hlavně v komerční sféře a používá se k dosahování konkurenčních výhod, nebo k získání a následnému prodeji získaných osobních nebo citlivých údajů. (9) (12) (10)

Druhými jsou zaměstnanci státních organizací (zpravodajských služeb), kteří plní úkoly spojené s ochranou státu. Vyznačují se analyzováním potenciálních hrozeb, a to jak z vnitrostátního, tak i mezinárodního prostředí. (9) (12) (10)

Třetí kategorií jsou útočníci mající tento druh činnosti jako zálibu. Každé prolomení zabezpečení daného informačního systému je pro ně výzvou. U tohoto druhu útočníka většinou nedochází k následnému zneužití informací nacházejících se v informačním systému. (9) (12) (10)

Poslední kategorií jsou útočníci, které charakterizuje jejich amorální povaha a asociální postoje. Tito útočníci napadají veřejně dostupné informační systémy za účelem je poškodit, pozastavit nebo zcela vyřadit z činnosti bez absolutního pochopení důsledků, které vznikly z jejich činnosti. (9) (12) (10)

3.3 Projevy potenciálně napadeného informačního systému

V některých případech je možné, že se informační systém projevuje jinak než před napadením. Samotné detekce napadení je v některých případech schopen samotný uživatel, a to tak, že v co možná největší míře sleduje odchylky systému od normálního stavu. (9) (12)

Jedná se hlavně o výkonové změny informačního systému, kdy se prodlouží doba spouštění programů, čas ukládání dokumentů, startování nebo vypnutí operačního systému. Dalším možným projevem napadeného informačního systému mohou být samovolná

spouštění programů, potvrzování nestandardních upozornění, nebo naopak odepření spuštění vybraných programů nebo služeb celého utajovaného informačního systému. (9) (12)

4 OCHRANA UTAJOVANÝCH INFORMACÍ V ZÁVISLOSTI NA KLASIFIKACI INFORMAČNÍHO SYSTÉMU

Minimální bezpečnost je jednoznačně definována v §7, Vyhlášky NBÚ č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi. Níže uvedené minimální požadavky jsou pouze orientační a v konkrétním utajovaném informačním systému se mohou lišit. (7)

4.1 Vyhrazené

Pro informační systém kategorie „VYHRAZENÉ“ jsou definovány tyto minimální požadavky na počítačovou bezpečnost:

1) **Jednoznačná identifikace a autentizace** uživatele, administrátora a bezpečnostního správce. U této kategorie informačního systému lze přihlášení do operačního systému nahradit fyzickým vydáváním nosiče utajovaných informací oproti podpisu. Identifikace a autentizace se tak provádí ve výdejním místě. (7)
2) **Záznam a zkoumání auditních záznamů** zabezpečení utajovaného informačního systému. Obsahem auditních záznamů musí být historie přihlášení, počet přihlášení, záznam o pokusu změny uživatelských práv a mazání dat. Operační systém tuto možnost umožňuje. Je jen nezbytné zabezpečit zamezení neautorizovaného přístupu k auditním záznamům a dále jejich ukládání mimo informační systém tak, aby byla zajištěna ochrana před jejich změnou a zničením. (7)
3) Ochrana **utajovaných informací při přepravě** mezi původcem a adresátem. Původcem se v tomto směru nemyslí zpracovatel. Jedná se o zajištění bezpečného přenosu mezi jednotlivými komponenty informačního systému (tiskárna – počítač, počítač – přenosný nosič utajovaných informací, počítač – skener apod.). Bezpečnost je zajištěna neustálou kontrolou vstupních a výstupních zařízení včetně komunikačních kanálů, zamezením jejich výměny a modifikace. (7)

4) **Fyzická bezpečnost** se vyznačuje pouze základními opatřeními bez instalací zvláštních prvků bezpečnosti (mechanických zábranných systémů, elektronických zabezpečovacích systémů, CCTV apod.). Požadavky jsou pouze funkční zkoušky mechanických prostředků. (7)

4.2 Důvěrné

Minimální požadavky na počítačovou bezpečnost:

1) **Jednoznačná identifikace a autentizace** uživatele, administrátora a bezpečnostního správce s vyššími nároky na složitost hesla pro uživatele. (7)
2) Nastavení **přístupu k utajovaným informacím** tak, aby uživatel (zpracovatel utajovaných informací) měl pouze taková oprávnění, která jsou nutná ke zpracování utajovaných informací. V informačním systému musí být jasně rozděleny účty na účet pro zpracování utajovaných informací, účet pro zprávu systému a kontrolu bezpečnostních auditů. V účtu s plnými administrátorskými oprávněními se nesmí zpracovávat žádné utajované informace. (7)
3) **Záznam a zkoumání auditních záznamů** zabezpečení utajovaného informačního systému je prováděno ve stejné míře jako u informačního systému „VYHRAZENÉ“. (7)
4) **Paměťové nosiče utajovaných informací** musí být vyčleněny pouze pro konkrétní utajovaný informační systém. V žádném případě nesmí být použity v jiném informačním systému, a to i stejné nebo vyšší kategorie. Deklasifikace, nebo úplné odtajnění lze pouze po schválení Národním bezpečnostním úřadem a po provedeném bezpečném výmazu. (7)
5) **Ochrana utajovaných informací při přepravě** mezi původcem a adresátem.
6) **Ochrana proti kompromitujícímu vyzařování** v mezích a rozsahu bezpečnostního standardu Národního bezpečnostního úřadu (7).
7) Požadavkem **fyzické bezpečnosti kategorie „DŮVĚRNÉ“** je minimální tloušťka zdiva u zabezpečené oblasti a zabezpečeného objektu od 100 do 150mm podle použitého materiálu (u vyztuženého betonu muže být síla stěny nižší než 100mm). Síla stropu je 150mm a je vyžadováno použití certifikovaným mechanických zábranných systémů minimálně třídy II. Další

podmínkou je použití elektronické prostorové a plášťové ochrany prvku PZTS. Dále je možno využít základního systému kontroly vstupu. (7)

4.3 Tajné

Minimální požadavky na počítačovou bezpečnost:

1) **Jednoznačná identifikace a autentizace** uživatele, administrátora a bezpečnostního správce je možné dvěma způsoby. Prvním je použití uživatelského jména a hesla se zajištěním šifrování uložených dat, nebo použití uživatelského jména a autentizací předmětem (čipovou kartou, tokenem, USB klíčem apod.) (7)
2) Nastavení **přístupu k utajovaným informacím** se stejnými nároky jako u stupně utajení „DŮVĚRNÉ“. (7)
3) **Záznam a zkoumání auditních záznamů** zabezpečení utajovaného informačního systému pomocí speciálních aplikací a operačního systému. (7)
4) **Paměťové nosiče utajovaných informací** se stejnými nároky jako u stupně utajení „DŮVĚRNÉ“. (7)
5) Ochrana **utajovaných informací při přepravě** mezi původcem a adresátem. (7)
6) **Ochrana proti kompromitujícímu vyzařování** v mezích a rozsahu bezpečnostního standardu Národního bezpečnostního úřadu s vyššími nároky než u informačního systému „DŮVĚRNÉ“. (7)
7) Analýza **skrytého kanálu**, a tedy možnost nepřípustné komunikace uvnitř informačního systému. Dále ne nezbytné zajistit odpovídající řízení přístupu a dodržování pravidla „need to know“ mezi uživateli utajovaného informačního systému. Analýza skrytého kanálu se provádí u utajovaných systémů napojených na veřejné informační sítě. (7)
8) Zabezpečené oblasti, ve kterých je umístěn informační systém kategorie „TAJNÉ“, musí být prověřeny certifikovanou firmou na možný výskyt technického **zařízení určeného k nepozorovanému sběru dat** (utajovaných informací). (7)

9) Požadavkem **fyzické bezpečnosti kategorie „TAJNÉ“** je minimální tloušťka zdiva u zabezpečené oblasti a zabezpečeného objektu od 100mm do150mm podle použitého materiálu. Síla stropu je 150mm a je vyžadováno použití certifikovaných mechanických zábranných systémů minimálně třídy III. Další podmínkou je použití elektronické prostorové, plášťové ochrany, instalace tísňového, nebo kamerového systému prvků PZTS a přítomnost ostrahy u nebo v objektu. Při vstupu do zabezpečeného objektu musí být instalován systém kontroly vstupu podle bezpečnostního standardu a vstup návštěv podléhá kontrole. (7)

4.4 Přísně tajné

Minimální požadavky na počítačovou bezpečnost:

1) **Jednoznačná identifikace a autentizace** uživatele, administrátora a bezpečnostního správce pomocí identifikace uživatelským jménem a autentizací pomocí šifrovaného předmětu s šifrovaným přenosem. (7)
2) Nastavení **přístupu k utajovaným informacím** se stejnými nároky jako u stupně utajení „DŮVĚRNÉ“. (7)
3) **Záznam a zkoumání auditních záznamů** zabezpečení utajovaného informačního systému pomocí speciálních aplikací a operačního systému. (7)
4) **Paměťové nosiče utajovaných informací** není možné deklasifikovat. Jediným možným způsobem ukončení provozu je jejich skartace v certifikovaném prostředku. (7)
5) Ochrana **utajovaných informací při přepravě** mezi původcem a adresátem. (7)
6) **Ochrana proti kompromitujícímu vyzařování** v mezích a rozsahu bezpečnostního standardu Národního bezpečnostního úřadu s vyššími nároky, než u informačního systému „TAJNÉ“. (7)
7) Analýza **skrytého kanálu** a tedy možnosti nepřípustné komunikace uvnitř informačního systému. Dále je nezbytné zajistit odpovídající řízení přístupu a dodržování pravidla „need to know“ mezi uživateli utajovaného informačního systému. (7)

8) Zabezpečené oblasti, ve kterých je umístěn informační systém kategorie „PŘÍSNĚ TAJNÉ“ musí být prověřeny certifikovanou firmou na možný výskyt technického **zařízení určeného k nepozorovanému sběru dat** (utajovaných informací) (7)

9) Utajovaný informační systém tohoto stupně utajení nesmí **být přímo** ani **postupně napojován** na žádnou **veřejnou informační síť**. (7)

10) Požadavkem **fyzické bezpečnosti kategorie „PŘÍSNĚ TAJNÉ“** je minimální tloušťka zdiva u zabezpečené oblasti a zabezpečeného objektu od 150mm do 300mm podle použitého materiálu. Síla stropu je 150mm a je vyžadováno použití certifikovaných mechanických zábranných systémů minimálně třídy IV. Další podmínkou je použití elektronické prostorové, plášťové ochrany, otřesové detektory instalované do průlezů, instalace tísňového, nebo kamerového systému prvků PZTS a přítomnost ostrahy v objektu (příslušníci ostrahy jsou pouze členy ozbrojených sil nebo ozbrojených bezpečnostních sborů). Při vstupu do zabezpečeného objektu musí být instalován systém kontroly vstupu podle bezpečnostního standardu, vstup návštěv podléhá kontrole a po objektu se pohybují pouze s doprovodem. (7) (6)

5 ZÁKLADNÍ PRVKY INFORMAČNÍHO SYSTÉMU KATEGORIE „VYHRAZENÉ“

Jedná se o fiktivní bezpečnostní politiku níže uvedeného fiktivního informačního systému vymyšlenou pro potřeby bakalářské práce!

V této části práce bude uveden příklad bezpečnostní politiky utajovaného informačního systému. Systém ponese název Informační systém Univerzity Tomáše Bati (dále „IS UTB“) a bude zahrnovat jeden přenosný počítač (notebook), dva nosiče utajovaných informací (USB Flash paměť a CD-RW pro zálohu utajovaných informací) a jedno výstupní zařízení (tiskárnu).

5.1 Vymezení IS UTB

Bezpečnostní politika IS UTB zajišťuje ochranu integrity, důvěrnosti a dostupnosti dat a utajovaných informací v IS UTB uložených. V tomto oddíle jsou uvedeny minimální

požadavky na počítačovou bezpečnost, požadavky na systém, uživatele a výstupy z analýzy rizik IS UTB, který je předurčen ke zpracování utajovaných informací stupně utajení „VYHRAZENÉ“ podle nařízení vlády č. 522/2005 - Seznam utajovaných informací.

IS UTB je samostatný přenosný počítač uložený v zabezpečené oblasti kategorie „VYHRAZENÉ“ a je určený pro zpracování elektronických dokumentů vědeckých analýz, prognóz a hypotéz, které vyžadují speciální a utajovaný způsob nakládání.

5.2 Cíle bezpečnostní politiky IS UTB

Cíle bezpečnostní politiky spojuje ochrana utajovaných informací v IS UTB. Účelem bezpečnostní politiky je specifikovat hlavní cíle, podmínky a požadavky pro konkrétní „Návrh bezpečnostních opatření IS UTB“. Hlavními cíly bezpečnostní politiky jsou:

a) Ochrana důvěrnosti, integrity a dostupnosti utajovaných informací,

b) ochrana utajovaných informací, celého informačního systému a jeho částí před přístupem, modifikací, zničením a neoprávněnou osobou,

c) vymezení odpovědností osob přistupujících, spravujících a zřizujících IS UTB,

d) neprodleně reagovat na nově zjištěná rizika. (9) (12)

5.3 Výsledky analýzy rizik IS UTB

Analýza rizik IS UTB odráží seznam možných typů hrozeb, které mohou ohrozit integritu, důvěrnost a dostupnost utajovaných informací. Konkrétní protiopatření jsou v plné míře zohledněny v „Návrhu bezpečnostních opatření IS UTB“. Hrozby ohrožující IS UTB) zahrnuté umístění IS UTB na Fakultě aplikované informatiky, Nad stráněmi 4511:

Objektivní: **Požár** z důvodu velkého počtu návštěvníků celého areálu a zalesněného bezprostředního okolí.

Náhlý výpadek elektrického proudu z důvodu umístění budovy v krajském městě.

Selhání hardwarového a programového vybavení IS UTB a zvlášť závažné **poruchy nosiče utajovaných informací** (technická

nebo programová chyba je v dnešní době téměř běžnou záležitostí). (9) (12)

Subjektivní: **Krádež** utajované informace z důvodu velkého pohybu osob v areálu (nikoliv v objektu) a nemožnosti vyloučení konkurenčního zájmu jiných zahraničních organizací (státních i soukromých).

Neautorizovaný přístup osoby použitím speciálního programového vybavení umožňujícího prolomení zabezpečení systému a vstup do IS UTB bez identifikace a autentizace.

Sdílení identifikačních jmen a autentizačních hesel nelze nikdy vyloučit.

Instalace neschváleného programového vybavení uživatelem nelze z důvodu přístupu studentů zahrnutých do vědecké činnosti školy vyloučit.

Porušení uživatelských směrnic nelze nikdy vyloučit.

Napadení IS UTB programem se škodlivým kódem prostřednictvím přenosného paměťového zařízení nelze z důvodu přístupu studentů zahrnutých do vědecké činnosti školy vyloučit. (9) (12)

5.4 Organizace, odpovědnost a povinnost v IS UTB

Zřizovatelem a provozovatelem IS UTB je vedoucí funkcionář UTB, který určí bezpečnostní a provozní správu IS UTB. Provozní bezpečnostní správou je:

- **Bezpečnostní manažer IS UTB**,
- **Bezpečnostní správce IS UTB**,
- **Správce IS UTB**.

Z hlediska velikosti informačního systému se funkce bezpečnostního správce a správce IS UTB mohou sloučit.

Bezpečnostní manažer IS UTB je odborný pracovník pověřený vedoucím funkcionářem UTB, který je odpovědný za dodržování podmínek stanovených zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Je tedy ve

smyslu jmenovaného zákona garantem v oblasti tvorby provozně bezpečnostní dokumentace, analýzy rizik, kontroly dodržování zásad ochrany utajovaný informací apod. (1)

Bezpečnostní správce IS UTB je výkonným pracovníkem podřízeným Bezpečnostnímu manažerovi IS UTB, který je odpovědný za implementaci bezpečnostních opatření, nastavení a prvků do IS UTB. Dále je odpovědný za tvorbu bezpečnostní dokumentace na úrovni uživatele a kontrolu chodu IS UTB. (7)

Správce IS UTB je výkonným pracovníkem podřízeným Bezpečnostnímu manažerovi IS UTB a jeho úkolem je instalace operačního systému, programového vybavení a tvorba uživatelských přístupů v souladu s provozně bezpečnostní dokumentací. (7)

5.5 Certifikace IS UTB

IS UTB je možné používat až po vydané certifikaci Národním bezpečnostním úřadem. Žádost o certifikaci zasílá Úřadu vedoucí funkcionář. Žádost o prodloužení certifikace (opakované certifikaci) podává opět vedoucí funkcionář UTB v dostatečném předstihu tak, aby byl nový certifikát vydán dříve, než skončí platnost předešlému certifikátu. (7)

5.6 Požadavky personální bezpečnosti IS UTB

Uživatelé, kteří mají povolený přístup do IS UTB bezpečnostním manažerem musí být držiteli platného oznámení, nebo osvědčení fyzické osoby na stupeň utajení „VYHRAZENÉ“ či vyšší a musí být poučeni. Bezpečnostní manažer, bezpečnostní správce a správce systému IS UTB musí být držiteli minimálně osvědčení kategorie „DŮVĚRNÉ“ a musí být poučeni. (3) (7)

Všichni uživatelé musí být proškoleni o povinnostech a odpovědnostech spjatých s přístupem k IS UTB. Školení provádí Bezpečnostní správce IS UTB nejméně jednou ročně, případně pokud došlo ke změně v systému. Všichni uživatelé musí znát základní pravidlo „need to know“ a jeho význam před přístupem do systému. Účast na absolvovaném školení stvrzuje uživatel v bezpečnostní dokumentaci uložené u Bezpečnostního správce IS UTB. (7)

5.7 Požadavky administrativní bezpečnosti IS UTB

Všechny utajované listinné i elektronické dokumenty a nosiče utajovaných informací IS UTB musí být evidovány, označeny a předávány v souladu s Vyhláškou NBÚ č. 529/2005 Sb. o administrativní bezpečnosti a o registrech utajovaných informací. Na nosič, který z důvodu své velikosti nelze označit vyhláškou povinnými daty, se připevní štítek. Deklasifikace nosičů klasifikovaných informací je prostřednictvím Bezpečnostního manažera vázána schválením Národního bezpečnostního úřadu. (7) (5)

Přenosný počítač, nosič utajovaných informací a výstupní zařízení se označuje štítkem, na kterém jsou uvedeny název provozovatele, název informačního systému, stupeň utajení a evidenční číslo. (5) (7)

Obr. 5-1 Vzor nosiče (Flash disk) utajovaných informací

Ochrana celého IS UTB, jeho komponent a prvotních hesel je stejná jako ochrana samotných utajovaných informací. (7)

Přeprava utajovaných dat je možná pouze oprávněnou osobou (pověřenou bezpečnostním manažerem), nebo Národním bezpečnostním úřadem certifikovanou poštovní službou. (5)

Pokud některé nosiče utajovaných informací nebudou využívány, nebo budou ze systému vyjmuty, musí na nich být proveden bezpečný výmaz s minimálním sedmínásobným cyklem přepsání a přemazání. Deklasifikace nosičů utajovaných informací schvaluje prostřednictvím zřizovatele utajovaného systému Národní bezpečnostní úřad. (7)

Nosiče utajovaných informací, které nemohou být nadále využívány (porucha, nepotřebnost, nemožná deklasifikace) se musí skartovat v certifikovaných zařízeních a musí o tom být proveden zápis. (7)

Obr. 5-2 Vzor nosiče (CD-RW) utajovaných informací

5.8 Požadavky fyzické bezpečnosti IS UTB

Práce v IS UTB je možná pouze v zabezpečené oblasti a objektu kategorie „VYHRAZENÉ“ nebo vyšší a zabezpečené oblasti třídy II. Zpracovávat informace je možné v celém zabezpečeném objektu za dodržení níže uvedených podmínek:

1) Zabezpečení oblastí a objektu musí vycházet z projektu fyzické bezpečnosti a analýzy rizik se zaměřením na úpravu použití mechanických zábranných systémů, režimových opatření a použití technických prostředků střežení.

2) Přenosný počítač musí být v místnosti zabezpečeného objektu nebo oblasti umístěn tak, aby bylo zabráněno možnému odezírání utajovaných informací z výstupů IS UTB (tiskárna, monitor) neoprávněnou osobou.

3) Po ukončení činnosti v IS UTB se přenosný počítač a nosiče utajovaných informací ukládají (CD-RW, USB Flash disk) do úschovného objekty typu 0, podle vyhlášky NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. (6)

5.9 Počítačová bezpečnost IS UTB

5.9.1 Bezpečnostní provozní mód „Vyhrazený“

V IS UTB je implementován bezpečnostní provozní mód „Vyhrazený“. To znamená, že všichni uživatelé jsou oprávnění zpracovávat všechny utajované informace v IS UTB obsažené. V informačním systému IS UTB se mohou zpracovávat pouze utajované informace stupně utajení „VYHRAZENÉ“. (7)

5.9.2 Řízení přístupu

Do IS UTB se uživatel bude identifikovat uživatelským jménem a autentizovat heslem. Každý uživatel bude mít individuální přihlašovací údaje a nesmí je sdílet s jiným uživatelem. Účet správce systému bude společný s účtem bezpečnostního správce a bude mít jiný identifikátor než Administrátor. Účet „Guest“ bude přejmenován a deaktivován. Tvar identifikátorů a požadovaná síla hesla, délka jeho platnosti a maximální počet opravení špatně zadaného hesla bude uvedeno v Návrhu bezpečnostních opatření a kapitole 6.1.3. (10) (11) (9) (12)

5.9.3 Bezpečnost programového vybavení a instalace IS UTB

Přístup k IS UTB bude zabezpečen prostřednictvím licencované verze operačního systému Windows 8.1 Pro (s pravidelnou aktualizací) s upraveným interaktivním přihlašováním, které poskytne každé osobě, která zapne přenosný počítač informace o IS UTB a poučí jí o požadovaných základních povinnostech. Operační systém bude upraven tak, aby zaznamenával všechny činnosti uživatelů, správců a systému s následnou možností provedení auditu systému. Dále bude v operačním systému nastaven zabezpečený způsob přihlášení pomocí klávesové zkratky „Ctrl+Alt+Del“ a budou upraveny místní zásady zabezpečení, kde bude upraven i časový interval uzamčení účtu při nečinnosti. (7) (10) (11) (9) (12)

Základem programového vybavení je použití licencovaného antivirového balíčku a pravidelně aktualizovanou virovou databází. Ostatní programy nutné pro samotné zpracování musí mít řádnou licenci, musí být aktualizované a samotná modifikace vybraných programů musí být povolena pouze v nutných mezích. Samotný uživatel nesmí mít žádná oprávnění k instalaci jakéhokoliv programu. Všechny aktualizace provádí bezpečnostní správce, nebo správce systému prostřednictví neutajovaného paměťového media, které ale musí být řádně zaevidováno. (7) (10) (11) (9) (12)

5.9.4 Bezpečnost dostupnosti IS UTB

Zajištění dostupnosti utajované informace je zajištěno použitím hlavního a náhradního zdroje elektrické energie (akumulátoru) a v operačním systému musí být provedena nastavení směřující k zabezpečení maximální životnosti akumulátoru. IS UTB (přenosný počítač) není možné provozovat s vyjmutým akumulátorem (tedy pouze s připojením do elektrické sítě) tak, aby při výpadku elektrické energie hrozilo potenciální nebezpečí ztráty dat. (7) (10) (11) (9) (12)

5.9.5 Propojení IS UTB s jinými informačními systémy a veřejnou informační sítí

Propojení s jinými informačními systémy nebo připojení do veřejné informační sítě (například internet) je zakázáno. Výměna informací z jiných informačních systémů je možná prostřednictvím přenosných nosičů utajovaných informací (USB Flash disk). V nosiči je možné přenášet pouze neutajované informace a utajované informace stupně utajení „VYHRAZENÉ“. (7) (13)

6 KONKRÉTNÍ BEZPEČNOSTNÍ OPATŘENÍ INFORMAČNÍHO SYSTÉMU KATEGORIE „VYHRAZENÉ“

6.1 Přístup do systému

6.1.1 Přihlášení

Do operačního systému Windows 8 Pro IS UTB se uživatel nesmí přihlašovat pomocí Microsoft uživatelského účtu. V Systému musí být nastaveno klasické přihlašování pomocí zkratek (Ctrl+Alt+Del. (7)

6.1.2 Interaktivní přihlašování

V interaktivním přihlašování bude uvedena zpráva pro uživatele pokoušejícího se přihlásit:

„***Přihlašujete se do Informačního systému Univerzity Tomáše Bati ve Zlíně, v tomto systému jsou povoleny pouze činnosti vyplývající ze zákona č. 412/2005 Sb., o ochraně utajovaných informací a následných prováděcích právních předpisů Národního bezpečnostního úřadu.***

Pokud nejste oprávněnou osobou, odevzdejte tento přenosný počítač na nejbližší služebnu PČR, nebo přímo na některou z fakult Univerzity Tomáše Bati ve Zlíně. V případě potíží volejte 779 123 456 – Jan Svoboda.“

6.1.3 Nastavení uživatelských jmen a autentizačních hesel

Uživatelské jméno musí jednoznačně identifikovat oprávněnou osobu. Pro uživatele bude použit tvar přihlášení jmeno_prijmeni. Pokud se bude vyskytovat více uživatelů se stejným jménem a příjmením, rozliší se přihlašovací údaje číslem označujícím pořadí povolení přístupu do IS UTB. Uživatelské jméno správce systému bude ve tvaru AdminIS_UTB.

Příklad:

Jan2_Svoboda

Heslo pro uživatele musí mít minimální délku osm znaků. Dále musí obsahovat velká a malá písmena a alespoň jedno číslo. Heslo pro správce IS UTB musí mít minimální délku 14 znaků a musí obsahovat malé a velké písmeno, číslo a speciální znak. (11) (12)

Příklad hesla správce:

Heslo_Vzor@11801

Doba platnosti jednoho hesla je nastavena na minimálně 180 dní u uživatele. A heslo správce 60 dní. Po této době se již bez změny hesla nebude možné do systému přihlásit. Nastavena bude také 10 minutová doba odhlášení uživatele při nečinnosti.

V systému IS UTB bude dále nastaveno sledování historií hesel tak, aby nebylo možné používat podobná hesla za sebou v řadě a šifrování použitích hesel. (11) (12)

6.2 Auditní záznamy

Auditní záznamy se ve Windows 8 Pro řeší formou služby zvané prohlížeč událostí. Prohlížeč událostí vytváří protokol událostí. Protokol musí být archivován, a to s historií jeden rok. Proto se musí na diskovém oddílu pro něj vyčlenit 20 000KB prostor. Auditní záznamy musí být nastaveny pro zaznamenávání:

- správu účtu – Úspěšné pokusy, neúspěšné pokusy
- systémové události – Úspěšné pokusy, neúspěšné pokusy
- události přihlášení – Úspěšné pokusy, neúspěšné pokusy
- události přihlášení k účtu – Úspěšné pokusy, neúspěšné pokusy
- změny zásad auditu – Úspěšné pokusy, neúspěšné pokusy

6.3 Bezpečnost hardware

Každý uživatel před přihlášením do IS UTB provede kontrolu hardwaru, tiskárny a ostatních komponentů (klávesnice, myš, propojovací kabely), zda nejsou poškozeny, nebo jsou na nich patrné změny. (7) (11) (12)

Hardware musí být zabezpečen před modifikací, zničením, nebo zcizením neoprávněnou osobou. Síťová karta v přenosném počítači IS UTB musí být zakázána ve správci zařízení tak, aby uživatel nebyl schopen připojit IS UTB k jinému informačnímu systému. (7) (11) (12)

Tiskárna v době nečinnosti musí být vypnuta, a to z důvodu vymazání mezipamětí zařízení, ve kterém se ukládají tiskové úlohy. (7) (11) (12)

Na přenosném počítači, tiskárně a nosiči utajovaného systému bude připevněn štítek s informacemi o evidenci, stupněm utajení, s názvem provozovatele a označením IS UTB. Štítky budou umístěny na viditelném místě. (7) (11) (12)

Obr. 6-1 Vzor označení přenosného počítače pro IS UTB

7 VYHODNOCENÍ

Nejčastěji používané klasifikované utajované systémy jsou ty „VYHRAZENÉ“. Bezpečnostní standard utajovaného systému „VYHRAZENÝ“, nastavený Národním bezpečnostním úřadem, plně koresponduje s aktuálními hrozbami, a to jak vnitřními, tak i vnějšími.

Jediným tématem v bezpečnosti informačních systémů, na který by se podle mě měla odborná veřejnost zaměřit, je určitá „přeheslovatelnost“ společnosti. Je nepochybně významné a důležité používat silná hesla do IS. Na druhou stranu je třeba vzít v potaz, že každý občan, který několikrát v týdnu přijde do styku s výpočetní technikou, používá velkou řadu různých hesel (domácí OS, e-bankovnictví, piny, email, Facebook, Twitter, apod.). K tomu připočítejme několik hesel nutných k přihlášení do IS v zaměstnání a není divu, že někteří uživatelé si hesla zaznamenávají „kde se dá“. Zabezpečené databanky (aplikace) pro ukládání hesel podle mého názoru problém neřeší, protože stačí prolomit jedno heslo a otevřou se dveře do virtuálního života postiženého. Riziko ztráty soukromých dat, citlivých údajů a utajovaných informací je poté obrovské.

Na tento problém navazuje nízká bezpečnostní morálka uživatele, pro kterého jsou hesla do e-bankovnictví, emailu apod. často důležitější než do „VYHRAZENÉHO“ informačního systému. Riziko vyzrazení hesla podle mého názoru nesnižuje ani zahrnutí zapomenutí hesla do institutu „bezpečnostního incidentu“, protože uživatel si heslo jako ochranu před zapomenutím raději někam napíše. Přitom zapomenutí hesla a vygenerování nového je mnohem menší riziko, než jeho vyzrazení neoprávněné osobně prostřednictvím lístečku umístěného například pod klávesnicí pracovního počítače.

Řešením problému je podle mého názoru použití biometrických metod v utajovaných informačních systémech již od nejnižších stupňů zabezpečení. Problémy s heslem by tímto způsobem byly zcela odstraněny. Národní bezpečnostní úřad by v tomto případě pouze definoval použití konkrétních biometrických metod v závislosti na požadované úrovni zabezpečení ochrany utajovaných informací. Jedinou nevýhodou je samozřejmě cena. V souvislosti s ochranou utajovaných informací je ale tato nevýhoda zanedbatelná.

8 ZÁVĚR

O významu utajovaných informací pro potřeby státu, a tedy zajištěni suverenity, územní celistvosti, bezpečnosti ochrany kritické infrastruktury apod. není třeba pochybovat. Přes hrozby které ohrožují slabá místa informačních systémů, je jejich význam a přínos pro společnost obrovský. Elektronické dokumenty ve velmi krátké době zcela nahradí ty listinné, a to hlavně z důvodu značné ekonomické úspory, lepší mobility a snad i podpory ekologie.

Utajované Informační systémy ale už dávno neexistují pouze pro potřeby jednoho konkrétního státu nebo organizace. Naopak vznikají utajované informační systémy nadnárodních organizací (NATO, EU apod.), pro které jsou některé informace strategicky důležité a musely být zavedeny globální směrnice pro jejich ochranu. Díky moderním informačním technologiím probíhá mezinárodní výměna těchto informací (a stále jen určitých stupňů) již velmi rychle a státy tak na jednotlivé hrozby mohou reagovat v krátkém čase společně a velmi účinně. V rámci budování společné Evropy a neustále se rozvíjející organizace Severo-atlantické smlouvy je tento jev samozřejmý.

Podle mého názoru je globalizace a seskupování informačních systémů na mezinárodních úrovních velmi důležitým a potřebným procesem. Nemělo by se ale zapomínat na tvorbu lokálních a decentralizovaných částí globálních informačních systémů (subsystémů schopných samostatné činnosti). Lokálními v tomto směru nemyslím regionální (státní) části informačních systémů, ale přímo místní specializované pracoviště schopné do určité míry (časového horizontu) pracovat v off-line režimu, nezávisle na centrálních dodávkách elektrické energie.

Při tvorbě nových utajovaných informačních systémů se musí postupovat komplexně a dodržovat zásady všech druhů bezpečnosti. Nezbytností je i provedení kvalitní a úplné analýzy rizik a na to navazující bezpečnostní politika. Pokud si zřizovatel (právnická organizace, podnikající fyzická osoba) utajovaného informačního systému není jistý svými odbornými kvalitami, tak může využít zkušeností a znalostí některých renomovaných soukromých bezpečnostních služeb.

Po vzniku bezpečnostní politiky je následujícím krokem sestavení návrhu bezpečnostního opatření, ve kterém jsou již uvedeny konkrétnější způsoby zabezpečení a centrální odpovědnost. Již konkrétní opatření, povinnosti a odpovědnosti jsou uvedeny ve směrnicích správce, bezpečnostního správce a uživatele. Po sestavení úplné bezpečnostní

politiky dochází k ověřování (testování) bezpečnostních opatření. Posledním krokem ke spuštění utajovaného informačního systému je samotná certifikace Národním bezpečnostním úřadem.

Samotný certifikovaný utajovaný informační systém vyžaduje řadu neopomenutelných úkonů. Prvním je neustálé ověřování hrozeb (vnitřních, vnějších, objektivních, subjektivních) a při zjištění nové hrozby musí následovat okamžitá reakce. Následuje neustálá aktualizace operačního systému, antivirového balíčku a ostatního programového vybavení počítače. Nelze ani opomenout pravidelně školení oprávněných osob a ověřování splnění podmínek k jejich přístupu k utajovaným informacím.

Budoucnost utajovaných systémů vidím v implementací výše uvedené biometrie. Dále předpokládám implementaci utajovaných systémů do mobilních zařízení, a to z důvodu neustále se zkvalitňujících kryptografických metod a potřeby některých vlád mít strategické informace kdykoliv v osobní blízkosti.

9 SEZNAM POUŽITÉ LITERATURY

1. POŽÁR, Josef. *Informační bezpečnost.* Plzeň : Aleš Čeněk, 2005. str. 311. 80-86898-38-5.

12. ČANDÍK, Marek. *Bezpečnosť informačných systémov, steganografia a digitálna vodotlač.* Ostrava : autor neznámý, 2005. str. 117. ISBN: 80-239-5962-X.

9. HALBICH, Čestmír a BRECHLEROVÁ, Dagmar. Bezpečnost informačních systémů. *vybrané kapitoly.* Praha : Česká zemědělská univerzita v Praze, 2003. str. 104. ISBN: 80-213-1090-1.

11. PŘIBYL, Jiří. Informační bezpečnost a utajování zpráv. Praha : ČVUT, 2004. str. 239. ISBN: 80-01-02863-1.

10. DOUCEK, Petr, NOVÁK, Luděk a SVATÁ, Vlasta. *Řízení bezpečnosti informací.* První vydání. Praha : Kamil Mařík - Professional Publishing, 2008. str. 239. ISBN: 978-80-86946-88-7.

4. Zákon č. 412/2005 Sb. *, o ochraně utajovaných informací a o bezpečnostní způsobilosti.*

2. Vyhláška č. 523/2005 Sb. *, o bezpečnosti komunikačních a informačních systémů a dalších elektronickcých zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.*

7. NARÍZENÍ VLÁDY 522/2005 Sb. *kterým se stanoví seznam utajovaných informací.*

3. Vyhláška č. 528/2005 Sb. *, o fyzické bezpečnosti a certifikaci technických prostředků.*

5. Vyhláška č. 529/2005 Sb. *, administrativní bezpečnostia o registrech utajovaných informací, ve znění pozdějších předpisů.*

6. Vyhláška č. 363/2011 Sb. *, o personální bezpečnosti a o bezpečnostní způsobilosti.*

8. Vyhláška č. 432/2011 Sb. *, o zajištění kryptografické ochrany utajovaných informací ve znění vyhlášky č. 417/2013 Sb.*

10 SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

NBÚ	Národní bezpečnostní úřad
CCTV	*Closed Circuit Television,* Uzavřený televizní okruh
PZTS	Poplachové zabezpečovací a tísňové systémy
CD-RW	*Compact Disk ReWritable,* Vícenásobně přepisovatelný disk
USB	*Universal Serial Bus,* Univerzální sériová sběrnice
IS UTB	Informační systém Univerzity Tomáše Bati
Ev.č.	Evidenční číslo
NATO	*North Atlantic Treaty Organization, Severoatlantická organizace*
EU	Evropská unie

11 SEZNAM OBRÁZKŮ