Kryptografická ochrana

Cryptographic protection

David Tříska

Bakalářská práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2008/2009

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**David TŘÍSKA**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Kryptografická ochrana**

Zásady pro vypracování:

1. **Zpracujte jako manuál pro použití v PKB.**
2. **Popište požadavky NBÚ ve smyslu zák. č.412/2005 Sb.**
3. **Popište postup pracoviště PKB při zahájení procesu certifikace NBÚ.**
4. **Definujte pojem bezpečnostní spolehlivost a její význam v procesu ochrany utajovaných informací.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LAUCKÝ, VL. Řízení technologických procesů v PKB. Zlín 2005.**
2. **LAUCKÝ VL. Technologie komerční bezpečnosti II. Zlín 2007. ISBN 978-80-7318-631-9.**
3. **ZÁKON č. 412/2005 Sb. O ochraně utajovaných informací a o bezpečnostní způsobilosti.**
4. **ZÁKON č. 413/2005 Sb. O změně zákonů v souvislosti s přijetím zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.**
5. **MUSIL, R. Ochrana utajovaných skutečností. Eurounion, Praha 2001. ISBN 80-85858-93-2.**
6. **LÁTAL I. a kol. Bezpečnostní zásady ochrany podniku. Prospektrum, Praha 2000. ISBN 80-7175-091-3.**

Vedoucí bakalářské práce: **JUDr. Vladimír Laucký**

Datum zadání bakalářské práce: **20. února 2009**

Termín odevzdání bakalářské práce: **20. května 2009**

Ve Zlíně dne 20. února 2009

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Bakalářskou práci jsem zpracoval formou manuálu pro firmy, které přijdou do styku s utajovanými informacemi. Práce by měla sloužit jako návod, jak zacházet s utajovanými informacemi a jakým způsobem utajované informace chránit. Postupně se zabývám historií kryptografie a pojmy týkající se kryptografické ochrany, požadavky Národního bezpečnostního úřadu ve smyslu zákona č. 412/2005 Sb., postupem procesu certifikace prováděné Národním bezpečnostním úřadem a bezpečnostní spolehlivostí.

Klíčová slova: kryptografie, kryptografická ochrana, utajované informace, bezpečnostní politika, certifikace, Národní bezpečnostní úřad.

ABSTRACT

I processed the bachelor thesis as a manual for firms which get into touch with secret information. The thesis should serve as an instruction how to treat with secret information and how to protect them. I am gradually concerned with history of cryptography and conceptions dealing with cryptography protection, requirements of National security office by course of law č. 412/2005 Sb., procedure of certification process provided by National security office and security reliability.

Keywords: cryptography, cryptographic protection, classified information, security policy, certification, National Security Authority.

Děkuji vedoucímu bakalářské práce JUDr. Vladimíru Lauckému za odborné vedení, rady a věcné připomínky, kterých se mi během práce dostávalo. Velkou oporou mi byla boršická knihovnice, moje teta Petra Víchová. Dále bych rád poděkoval svým rodičům, přítelkyni a kamarádům za podporu, která mi byla poskytována během psaní bakalářské práce a po dobu celého studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk 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 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 – 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.

Ve Zlíně 20. května 2009 …….……

podpis diplomanta

OBSAH

ÚVOD

V době, ve které žijeme, se rychle rozmáhá trestná činnost, která již nemá hranice jen u hmotných krádeží, ale stále více se jedná o krádeže informací. Již před naším letopočtem přijít o významnou informaci znamenalo smrt, prohranou válku nebo ztrátu majetku. V dnešní době únik „tajné“ informace může znamenat pro stát nenávratný problém, pro firmy konkurz nebo ztrátu zakázky. Proto z kdysi primitivní disciplíny kryptografie se stává neodmyslitelná součást moderního světa. Organizace a vlády platí za kryptografickou ochranu utajovaných informací obrovské peníze, které by ovšem ztrátu utajovaných informací nenahradily. Ve hře jsou v mnoha případech životy lidí, které ani velkými penězi nahradit nejdou.

V bakalářské práci seznamuji čtenáře s bezpečnostními opatřeními, které musí organizace dodržovat při ochraně utajovaných informací. Patří sem režimová opatření, technické zabezpečení, fyzická ostraha a další. Nestačí se pouze zaměřit na správné uschování nebo uzamčení utajované informace. Do bezpečnostní politiky utajovaných informací patří také kryptografická ochrana. S bezpečným předáním informací jsou spojeny velké nároky. Pracovníci, kteří se zabývají kryptografickou ochranou, proto musí dnes a denně zdokonalovat ochranu v této oblasti.

Přijetí zákona č. 412/2005 Sb. a dalších právních norem z oblasti ochrany utajovaných informací přineslo profesionální přístup organizací k bezpečnostní politice. Zvýšila se bezpečnost utajovaných informací a veškerá manipulace s nimi spojená. Zákon č. 412/2005 Sb. je v podstatě návod pro organizace, jaké opatření zvolit, jak informace chránit a jak toho docílit. Zmíněné právní normy mají nesmírný význam pro úspěšné tvoření bezpečnostní politiky utajovaných informací.

I. TEORETICKÁ ČÁST

1 ÚVOD DO KRYPTOGRAFIE

Kryptografie je vědní obor, který se zabývá utajováním zpráv a jejich převodem do podoby, která je čitelná jen se speciální znalostí. Hlavním cílem šifrovacího systému je zamaskovat utajovanou zprávu tak, aby byla pro všechny nepovolané osoby nečitelná. Jedná se o proces, kdy z čitelného textu pomocí šifrovacího algoritmu a klíče vytvoříme text zašifrovaný. Kryptografii z hlediska použití dělíme na symetrickou a asymetrickou. Slovo kryptografie má kořeny v řečtině, „kryptós“ znamená skrytý a „gráphein“ znamená psát. Kryptografie tedy znamená „tajné psaní“.

1.1 Historie kryptografie

Kryptografie má na lidskou historii vliv téměř 4000 let, během kterých se stále vyvíjela a mnohokrát ovlivnila běh lidských dějin. Nejstarší zmínka se objevuje přibližně 1900 let před naším letopočtem. V africkém městě Menet Khufu vytesal písař do skály nápis, kde běžně používané hieroglyfy nahradil neobvyklými znaky. Záměr autora však nebyl skrýt význam zprávy, ale chtěl, aby nápis vypadal důstojně.

V prvopočátku kryptografie sloužila zejména k utajení vojenských informací. Již z dob starověkého Egypta a Mezopotámie jsou známy pokusy o šifrování textu. Šlo jen o drobnou úpravu písma, která postačovala svému účelu. První doložené zašifrování zprávy pochází z roku 480 př. n. l. za období řecko – perských válek v bitvě u Salamíny[1]. V 5. století př. n. l. použili Sparťané systém Skytale. Princip spočíval v tom, že autor zprávy omotal proužek kůže kolem dřevěné hole, která musela mít dán přesný průměr. Zpráva pak byla napsána na kůži podél tyče. Pás kůže se poté odmotal a vznikl tak pás s nečitelnou posloupností písmen. Zpráva byla čitelná jen na holi stejného průměru. Na svou dobu byl systém Skytale velmi promyšlený a ukazoval, jakým směrem se bude kryptografie dále vyvíjet.

[1] Salamina – řecký ostrov, asi 20 km západně od Atén.

Julius Caesar[2] se do historie kryptografie zapsal vynalezením šifry, která byla pojmenována Caesarova šifra. Princip šifry je založen na posunu písmen ve zprávě o předem dohodnutý počet. Kryptografie se po další staletí stále vyvíjela a byla známější ve více zemích.

V 16. století vynalezl Blaise de Vigenére[3] šifru, která nebyla prolomena po tři století. Vigenére vycházel z úvahy Leona Battistuta Albertiho, které navrhl použít více šifrovacích abeced. Při šifrování se abecedy pravidelně střídaly a měly tak zmást potenciální narušitele. Vigenérova šifra je odolná vůči frekvenční analýze, tím se myslí, že každé písmeno může být reprezentováno několika jinými písmeny. Další výhoda šifry spočívá v délce klíče, která není nijak omezena. Vigenérovu šifru prolomil až v 19. století Charles Babbage[4].

Charles Wheatstone[5] a Lyon Playfair[6] vynalezli roku 1854 bigramovou šifru a nese název Playfairova šifra. Princip šifry spočívá v tom, že se nešifrují samostatná písmena, ale jejich dvojice.

Joseph Mauborgne[7] po první světové válce přišel s nápadem uplatnit u Vegenérovy šifry náhodný klíč. Při použití náhodného klíče, který je stejně dlouhý jako otevřený text, vznikne šifra, u které lze dokázat matematicky její nerozluštitelnost. To dokázal roku 1940 Claude Shanon[8]. Nevýhoda spočívá v tom, že každý klíč se smí použít jen jednou. Šifra se používá jen zřídka, hlavní problém je generování náhodných klíčů.

---

[2] Julius Caesar – římský vojevůdce a politik.
[3] Blaise de Vigenére – francouzský diplomat a kryptogram.
[4] Charles Babbage – 1791 – 1871, britský matematik, filozof a informatik, jako první přišel s nápadem sestrojit programovatelný počítač.
[5] Charles Wheatstone – britský vědec a vynálezce, proslul vymyšlením Wheatstonova mostu.
[6] Lyon Playfair – 1818 – 1898, anglický vědec a poslanec, pojmenován podle něj Playfair kód.
[7] Joseph Mauborgne – americký vědec.
[8] Claude Elwood Shannon – 1916 – 2001, americký elektroinženýr a matematik, známý jako „otec informace“.

Obr. 1. Řecké skytale.

[zdroj obrázku uveden v použité literatuře, zdroj číslo [13]]

1.2 Válečná kryptografie

Počátkem 20. století se šifrovalo ručními šifrovacími klíči. O něco později se přešlo na šifrování pomocí „kódových knih“. Šifrování pomocí kódových knih umožňovalo zašifrovat pomocí dvou až pěti písmen kódového výrazu celé slovo nebo i celou větu.

Zašifrování a bezpečnému přenosu zpráv nebyla v armádě během druhé světové války věnována dostatečně velká pozornost. Správné použití kryptografie bylo podceněno i na nejvyšších místech velení armády, což mnohdy vedlo k málo zabezpečenému přenosu zprávy a darování informací protivníkovi. Největší problém bylo, že šifrování zůstalo na předválečné úrovni na začátku války i v jejím průběhu. Myslím si, že v dnešní době by se podobný problém u vyspělých armád stěží stal. Armády disponují nejlepší špičkovou technologií a navíc proti sobě zatím nejvyspělejší armády nevedou válečný konflikt. K úniku informací může dojít, ale ne v takové míře a dlouhé době jako během 2. světové války.

Chyby, jakých se radisté dopouštěli, byly neúmyslné. Pramenily z nedostatečného odborného zaškolení v kryptografii a podcenění protivníka. Válčící strany se bohužel mylně domnívaly, že jejich zabezpečení zpráv je dokonalé a pro nepřítele nerozluštitelné. Následek těchto chyb byl však tragický, zemřelo mnoho obyčejných lidí a vojáků. Chybné používání šifer a tajného přenosu zpráv není ve více než dvoutisícové historii kryptografie nijak ojedinělé.

Československí radisté v Londýně byli naprosto přesvědčeni o kvalitách a bezpečnosti svých ručních šifrovacích systémů. Způsob a metody luštění většiny těchto systémů byly popsány již na počátku třicátých let v kryptologické literatuře. Autoři ovšem o tom nevěděli nebo problému nevěnovali dostatečnou pozornost.

K utajení a bezpečnému přenosu zpráv v radiové síti během druhé světové války používali Němci šifrovací stroj Enigma. Američtí radisté zase šifrovací stroj M-2009b (Hagelin), Japonci šifrovací stroj Purpur, který tak pojmenovali Američané. Angličané, Francouzi, Italové a další používali podobné upravené kódy a jiné způsoby šifrování.

S blížícím se koncem války se do šifrování dostávaly moderní technologie s využitím elektronických součástek. V Bletchey parku byl roku 1943 sestrojen první počítač s názvem Collosus a sloužil pro prolamování šifer. Britská vláda jeho existenci tajila, proto byl dlouho považován za první počítač americký ENIAC[9]. S dalším vývojem byly počítače schopné zpracovávat stále větší množství dat za stále menší časový úsek. To vyžadovalo objevování nových algoritmů a nárůst délky jejich klíče.

1.2.1 Enigma

O sestrojení Enigmy se postaral německý vynálezce Arthur Scherbius. Roku 1918 získal patent na šifrovací zařízení s názvem Enigma. Scherbius dlouho nemohl sehnat odběratele kvůli její vysoké ceně. Německo si poté začalo uvědomovat slabinu v utajování zpráv a během 20 let koupilo přes 30 000 šifrovacích strojů Enigma.

Přístroj se skládal z klávesnice, šifrovací desky a signální desky. Šifrovací jádro tvořily 3 scramblery (gumové kotoučky), kterými vedly dráty. V roce 1938 byl zvýšen počet scramblerů na 5.

Němci se obávali, že spojenci budou mít k dispozici repliku stroje. Několik strojů se podařilo ukrást, zejména Poláci patřili mezi úspěšné luštitele. Při znalostech Enigmy a zachycení velkého počtu zpráv bylo možné vytvořit seznam, pomocí něhož šlo odhalit tzv. denní klíč. Po zmiňovaném navýšení scramblerů a zvýšení propojovacích kabelů z 6 na 10

[9] ENIAC – Electronic Numerical Integrator And Computer, jeho vývoj byl zahájen v roce 1943 v USA, sloužil pro účely americké armády.

ztratili Poláci šanci na dešifrování zpráv. Poláci tušili vojenský konflikt, proto své znalosti svěřili spojencům a všechny potřebné dokumenty k luštění Enigmy byly převezeny do Anglie. Dešifrování od té doby probíhalo v Bletchey parku v čele s Alanem Turingem[10]. Podařilo se odhalit slabiny německé komunikace, která spočívala v častém opakování klíčů zpráv.

Obr. 2. Enigma, verze se třemi rotory pro německou armádu.

[zdroj obrázku uveden v použité literatuře, zdroj číslo [6]]

1.2.2 Válečné šifrovací systémy

„Systém TTS (TTS = transpozice + transpozice + substituce), který sehrál rozhodující úlohu při průniku německých luštitelů do československé londýnské zpravodajské sítě. Fatální chybu našich zpravodajců, totiž předávání popisu způsobu šifrování, použitých klíčů (tj. knih, básní nebo písní, které sloužili pro výběr šifrovacích hesel), směrnice a

[10] Alan Turing – matematik, navrhl teoretický model počítače.

pokyny ke způsobu šifrování a jeho změnám stejným kanálem, kterým byly předávány šifrované zprávy (tj. vzduchem pomocí radiového vysílání), umožnila luštění a někdy dokonce jen dešifrování zpráv, které byly v radiové síti předávány v dalších letech. Němečtí luštitelé se postupně stali rovnocennými, ale tajnými účastníky československé vojenské zpravodajské sítě. V klidu četli zprávy naší rozvědky, a ta o tom neměla ani tušení. Velitelé i šifréři v Londýně byli tak neotřesitelně přesvědčeni o dokonalosti svého šifrování, že jimi nezacloumala ani některá závažná varování. Úniky informací připisovali žvanění, německým agentům, vyzrazením při mučení, ale nikdy nekvalitním šifrovacím systémům a amatérskému přístupu k šifrování. Způsob TTS používala rozvědka od počátku války v roce 1939 až do poloviny roku 1941, na některých směrech ještě o něco déle. K rozluštění systému nebylo ani zdaleka zapotřebí využít všech chyb, kterých se v té době šifréři dopustili.“[11]

Další systém STT už nebyl tak používaný jako systém TTS. Systém STT byl po válce vyzrazen německými luštiteli.

1.2.3 Kód Navahů

Američané během války v Tichomoří sáhli po originálním postupu šifrování. Ke komunikaci využili jazyk indiánského kmene Navahů[12]. Přenos zprávy probíhal jednoduchým způsobem, každá jednotka měla radistu – Navaha. Ten převzal zprávu v angličtině, poté ji přeložil do navažštiny, v navažštině ji posílal druhému radistovi, který zprávu zpět přeložil do angličtiny. Poměrně jednoduchý způsob, ale velmi efektivní.

Japonci byli tímto způsobem komunikace zaskočeni, nevěděli jak mají do způsobu komunikace proniknout. Používání kódu Navahů bylo velmi efektivní a rychlé.

Někteří odborníci později způsob komunikace kritizovali, ale během druhé světové války byl úspěšný.

---

[11] JANEČEK, Jiří. Válka šifer : Výhry a prohry československé vojenské rozvědky (1939-1945). Olomouc : Votobia, 2001. s. 251-252. ISBN 80-7198-505-8.

[12] Navahové – vlastním jménem Dené (lidé), indiánský kmen v USA (Arizona, Colorado, Nové Mexiko, Utah), celkem asi 150 000 osob.
[vysvětlení převzato z www.cojeco.cz/index.php?s_term=&s_lang=2&detail=1&id_desc=63805].

Jazyk Navahů bylo nutné upravit, protože indiánský kmen neznal výrazy typické pro válku, jako je bombardér nebo ponorka. Američané to vyřešili zavedením kódové knihy, ve které byly například různé typy bombardérů pojmenovány druhy ptáků. Lodě a ponorky zase pojmenovali podle druhů ryb. Podobně postupovali i u dalších slov, které neznal jazyk Navahů.

1.2.4 Purpurový kód

Purpurový kód, nazývaný také „Purpur“, představuje jeden z nejslavnějších šifrovacích systémů. Japonci začali purpurový kód používat od roku 1937. Jednalo se o komplexní systém, jeho rozluštění vyžadovalo vysoké intelektuální předpoklady.

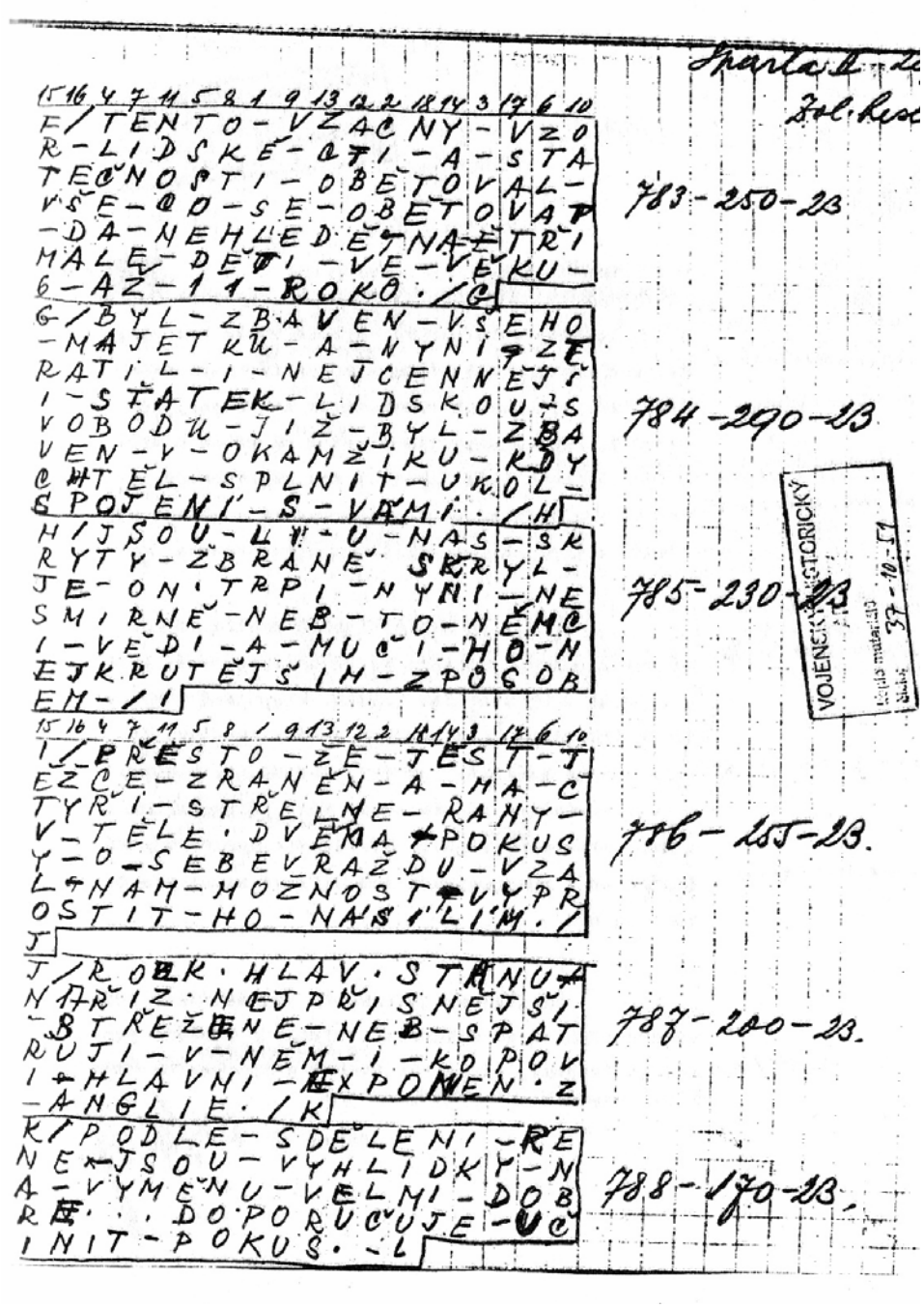
Friedman a jeho skupina v Munitions Building začali v roce 1937, krátce po zahájení jeho používání, purpurový kód odposlouchávat. Výsledků bylo dosaženo za nějaký čas, protože dlouho trvalo shromáždit dostatek podkladů k částečnému rozluštění.

Stroj na purpurový kód se skládal ze standardní baterie, stupňovitého přepínače, rozvodové desky. Vše bylo složitě propojeno. Japonský technik seděl u stroje, který představoval vstupní a výstupní zařízení. Pomocí sešitu, ze kterého opsal klíče na daný den, zapojil zásuvku do rozvodné desky. Následně nastavil rotory tak, aby každý z nich stál v pozici, která byla určena kódu v určitý den. Po nastavení obsluha napsala text, který byl zašifrován stejným způsobem jako ostatní části depeše. Paralelně zašifrovaná sdělení byla zapsána na druhém stroji.

Od roku 1939 začali s luštěním i námořní kryptologové. Problém bylo rozeznat v množství zašifrovaných dopisů určité pravidelnosti. První výraznější rozluštění zprávy v purpurovém kódu bylo z 25. září 1940. Britové se dověděli o tom, že Američané rozluštili Purpurový kód, a na konci roku 1940 podepsali dohodu zahrnující plnou výměnu kryptografických systémů.

1.2.5 Ukázka dešifrace dopisu

Část dešifrace dopisu Václava Morávka prezidentovi, ministrovi národní obrany a plk. Moravcovi z 28. 6. 1941:

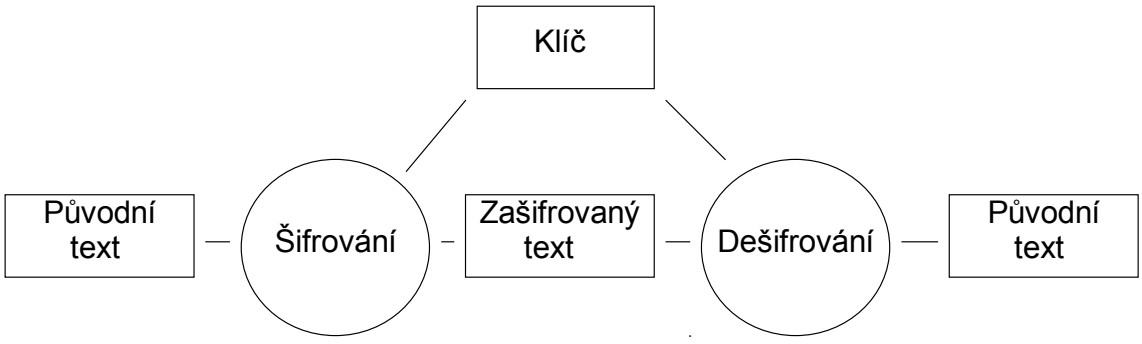


Obr. 3. Část dešifrace dopisu.

[zdroj obrázku uveden v použité literatuře, zdroj číslo [1]]

1.3 Symetrické šifrovací algoritmy

Pro zašifrování a dešifrování zprávy používají stejný šifrovací klíč. Používají se zejména pro zabezpečení ukládaných dat, např. na záložní média. Symetrické algoritmy jsou mnohem rychlejší než asymetrické, proto často bývají používány v kombinaci s asymetrickými, aby bylo využito jejich výhod.



Obr. 4. Princip symetrické kryptografie.

Nejznámější symetrické šifrovací algoritmy:

- DES,
- 3DES,
- IDEA,
- BlowFish,
- CAST a další.

a) DES

DES byl vyvinut firmou IBM[13]. V roce 1977 se stal americkou vládní normou pro šifrování. Délka klíče je 56 bitů. V současné době nelze DES považovat za bezpečný, vzhledem ke krátké délce klíče. V roce 1997 byl DES prolomen. Prolomení trvalo několika

[13] IBM - International Business Machines Corporation, fungující od 1888, mezi hlavní činnosti společnosti patří výroba a prodej počítačového software a hardware.

tisícům počítačů asi 4 měsíce, nyní však existují zařízení, které jsou schopné prolomit šifru za mnohem kratší dobu. DES patří do skupiny blokových šifer. Blokové šifrování rozdělí tok bitů textu na bloky o stejné velikosti, poslední blok popřípadě doplní a šifruje každý blok pomocí klíče zvlášť.

b) 3DES

Bloková šifra, která vznikla na popud prolomení DES, jedná se o jeho zesílenou variantu. Šifrovaná data jsou třikrát přešifrována algoritmem DES. Algoritmus ve své základní variantě využívá klíč dlouhý 112 bitů, což je vlastně dvojnásobek klíče DES. Algoritmus zaručuje vyšší bezpečnost, nevýhodou je výrazné snížení rychlosti, proto se dnes také pomalu přestává používat.

c) IDEA

Jedná se o blokovou šifru, klíč má délku 128 bitů a pracuje po 64bitových blocích. Šifrování pomocí IDEA je bezpečné, žádná úspěšná lineární slabost nebyla ohlášena. Bylo jen objeveno několik tříd slabých klíčů. IDEA je patentována v USA, Japonsku, Rakousku, Německu, Francii, Itálii a v dalších evropských zemích.

1.4 Asymetrické šifrovací algoritmy

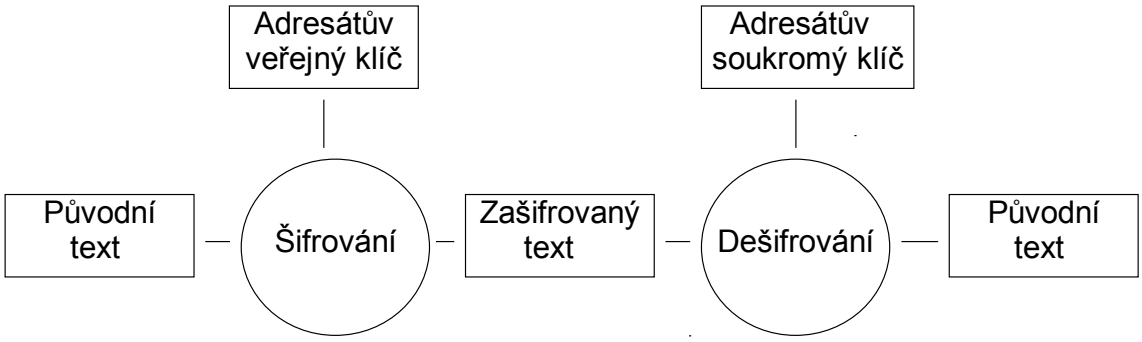
Výměna klíčů mezi odesílatelem a příjemcem zprávy byl problém. Řešila se otázka, jak šifrovací klíč vyměnit, aby se klíč nikdo další nedozvěděl. Pro distribuci klíčů se začaly využívat služby kurýrů. Situace začala být neřešitelná v době rozmachu elektronické komunikace a elektronického obchodování. Každý den se na cesty vydávali kurýři s kufříky, kde měli komunikační klíče pro daný den. Kurýři pracovali pro banky, státní instituce a armádu.

V roce 1975 přišel Whitfield Diffie[14] s myšlenkou asymetrické kryptografie. Pro šifrování a dešifrování dat se používají dva různé klíče, veřejný a soukromý. Veřejný klíč poskytujeme všem, od koho si přejeme dostávat šifrovaná data. Soukromý klíč si

[14] Whitfield Diffie – americký kryptograf.

chráníme, slouží jen pro naše používání. Soukromý a veřejný klíč společně nazýváme klíčový pár. Pokud chci zaslat někomu šifrovanou zprávu pomocí asymetrického algoritmu, musím znát vždy jeho veřejnou část klíče. Komunikující strany se nemusí vůbec setkat a přesto můžou mezi sebou bezpečně komunikovat. Asymetrická kryptografie vyřešila problém předání klíčů, není třeba sdílet žádné veřejné tajemství.

Princip asymetrické kryptografie spočívá v jednocestných funkcích, které jsou jedním směrem snadno proveditelné. Spočítat součin dvou prvočísel je snadné, ale určit z výsledku původní čísla zabere víc času. Pokud budeme pracovat jen s velkými čísly, je u jednocestných funkcí nemožné v reálném čase na původní čísla přijít. Nevýhoda asymetrické kryptografie je její nízká rychlost vzhledem k symetrické kryptografii.



Obr. 5. Princip asymetrické kryptografie.

Nejznámější asymetrické šifrovací algoritmy:

- RSA,
- DSA,
- Diffie Hellman,
- EIGanal a další.

a) RSA

Algoritmus vznikl v roce 1977, je vhodný pro podepisování i šifrování. Do roku 2000 byl patentovaný pro severní Ameriku. Bezpečnost je založena na principu, že je obtížné rozložit velká čísla, která jsou součinem velkých prvočísel. Při dostatečné délce klíče je algoritmus bezpečný, dnes je doporučováno 2048 bitů.

b) DSA

Vznikl v roce 1991 jako standard americké vlády. Algoritmus DSA představuje šifrování založené na veřejném klíči, lze ho použít pouze ke generování digitálních podpisů, ale ne k šifrování dat.

c) Diffie Hellman

Nejedná se o šifrovací algoritmus, ale o protokol, který umožňuje bezpečnou výměnu klíčů pro symetrické šifrovací algoritmy. Protokol neobsahuje metodu, která by umožňovala podpis zaslané zprávy. Neumožňuje ani provést autentizaci, což znamená potvrdit, že klíč skutečně pochází od určitého uživatele.

1.5 Elektronický podpis

Elektronický podpis můžeme chápat jako identifikační údaje autora elektrického dokumentu a je brán jako jeden z hlavních nástrojů identifikace a autorizace osob v prostředí internetu. Elektronický podpis zaručuje identifikaci podepsané osoby, ovšem nezaručuje integritu podepsaného dokumentu ani autentizaci podepsané osoby.

Zaručený elektronický podpis kryptografickými metodami zjišťuje:

- autentizaci – ověření identity autora dokumentu, autentický znamená původní, pravý. Autentizace je bezpečnostní opatření, které zajišťuje ochranu před falšováním identity.
- integritu – umožňuje dokázat, že po podepsání dokumentu nedošlo k žádné změně nebo dokument není jakýmkoliv způsobem poškozen.

U zaručeného elektronického podpisu se používá kryptografie s veřejným klíčem. Pro účely ve správním řízení je vyžadován zaručený elektronický podpis. V České republice platí zákon č. 227/2000 Sb., o elektronickém podpisu, podle kterého za určitých podmínek je možné elektronický podpis použít na místo podpisu klasického. Elektronický podpis je příslibem budoucnosti, ale jeho používání musí být dostatečně zabezpečené. Elektronický podpis vydávají tzv. certifikační autority, které byly akreditovány Ministerstvem informatiky (nyní pod Ministerstvem vnitra).

1.6 Hashovací funkce

Jednosměrné funkce, které musí splňovat definované podmínky. Hashovací funkce mapují řetězec libovolné délky na řetězec konstantní délky (ze zadaného velkého množství dat vrací mnohem menší objem dat, který však jednoznačně vypovídá o obsahu dokumentu). Výsledný otisk je závislý na všech bitech vstupního řetězce. Hashovací funkce se používají ke kontrole integrity dat, k porovnání dvou zpráv a pro tvorbu digitálních podpisů. Mezi dnes běžně používané Hash algoritmy patří SHA-1 a MD5. Zmíněné algoritmy fungují na stejných principech jako blokové šifry.

MD5 – hlavní funkce spočívá v kontrole integrity souborů, tzn. rychle otestují, zda dva soubory jsou stejné a to bez nutnosti porovnávat bit po bitu jednotlivých souborů.

SHA-1 – nástupce MD5, může být použit s algoritmem DSA u bankovních transakcí a v elektronické poště.

Požadavky na hashovací funkce:

- jednosměrnost funkce, tzn. jde snadno spočítat hash zprávy, ale musí být časově obtížné nebo nemožné nalézt původní zprávu z hashe.
- libovolně velké množství vstupních dat dává stejně dlouhý výstup.
- nelze najít dvě vstupní zprávy, které mají stejný výsledný hash.

1.7 Kvantová kryptografie

Kvantová kryptografie má své počátky v 80. letech minulého století. První kvantový kryptografický protokol navrhli Bennett a Brassard v roce 1984. Objevitelé definovali komunikační protokol využívající polarizaci fotonů a nesl označení BB84. V roce 1989 se podařilo teorii kvantové kryptografie ověřit. Základním prvkem je přenos sekvence pomocí stavu fotonů, který umožňuje bezpečný přenos zprávy a odhalení odposlechu. Kvantové kryptografické kanály neslouží jen k přenosu informace, ale i k výrobě a distribuci náhodného klíče. Klasická kryptografie používá k utajení informací metody z oboru matematiky a informatiky, kvantová kryptografie ke své činnosti využívá přírodní zákony. Závěrem lze říci, že bezpečnost kvantové kryptografie nezáleží na síle útočníka ani na technologické síle, obecně se jeví jako absolutně bezpečná.

Problém kvantové kryptografie představuje, kdy budou k dispozici opravdu použitelné kvantové počítače. Vědci na otázku nedokáží přesně odpovědět, zda to bude za 50 nebo 100 let. Potíže činní vytvořit jeden foton s konstantní polarizací a foton detekovat. Při současných možnostech vědy lze určit, že na detektoru částice je nebo není, ale určit množství je obtížné. Při přenosu také dochází k velkým ztrátám, podaří se přenést asi osminu informace. Proniknout do tajů kvantové kryptografie bude vědcům ještě nějaký čas trvat, než budou schopni odpovědět na všechny otázky. Možná za 50 let budeme moci říct, že kvantová kryptografie představuje slibnou budoucnost v oblasti přenosu zpráv a jeho kódování.

1.8 Kybernetický terorismus

Kybernetický terorismus (kyberterorismus) představuje útok proti informačním systémům, počítačovým programům a datům. Kyberterorismus se stal celosvětovou bezpečnostní hrozbou s nedozírnými následky, pronikl do oblasti státní sféry, soukromých sektorů, armády i osobního života. S velkým rozšířením kyberterorismu můžeme mluvit o kybernetické válce. Organizace vyvíjejí kybernetické strategie za účelem narušit a oslabit nepřítele, znemožnit jeho komunikaci. Informační systémy a s nimi spojená komunikace jsou natolik důležité, že jejich napadení nebo dokonce zničení představuje mnohdy obrovské hrozby. V souvislosti s hrozbami terorismu se kyberterorismem zabývá i Bezpečnostní informační služba.

Kybernetický terorismus představuje cíleně vedené útoky typu:

- DoS[15] útok – bývá namířen proti serveru nebo celé síti připojené k internetu. Cílem útoku je narušit provoz. Funguje na základě velkého počtu přicházejících požadavků na jeden server, který je pak zahlcen a nereaguje na požadavky uživatelů nebo se může celý zhroutit. Ve velkém množství případů bývá DoS útok použit jen k zahlazení stop pachatelů. Základní typy DoS útoku jsou útoky, které využívají

[15] DoS – Denial of Service, v českém překladu „odmítnutí služby“.

chyb v implementaci TCP/IP[16], útoky, které využívají nedokonalosti a nedostatky ve specifikaci TCP/IP a útoky hrubou silou.

- DDoS[17] útok – varianta DoS útoku, není veden z jednoho počítače, ale z velkého množství. Velké množství počítačů ve stejný moment pošle příkaz na oběť, kterou zasype přívalem dat.

Další typické útoky hackerů jsou Bombing (zahlcování služby pakety) a Defacement.

Proti takovým útokům se vyžaduje správné nastavení routerů[18], správné nastavení firewallů[19] a další. Nesmí dojít k podcenění zvláště v sektorech, kde se pracuje např. s údaji o zaměstnancích, obchodními tajemstvími a podobně.

1.9 Bezpečnostní informační služba

Zpravodajská instituce českého státu působící uvnitř jeho území. Fungování Bezpečnostní informační služby[20] (BIS) upravuje zákon č. 154/1994 Sb., O Bezpečnostní informační službě. BIS řídí a kontroluje vláda ČR. BIS se zabývá získáváním, shromažďováním a vyhodnocováním informací z oblasti terorismu, ochrany ekonomických zájmů státu, organizovaného zločinu, bezpečnosti informačních a komunikačních systémů, činnostmi ohrožující utajované informace a další.

V oblasti bezpečnosti informačních a komunikačních systémů jsou na BIS kladeny velmi specifické požadavky a náročné úkoly. Do této oblasti patří kriminální průniky do datových sítí, kyberterorismus a další podobné útoky. Současné problémy, které v oblasti bezpečnosti informačních systémů BIS řeší, představují podvody s elektronickou identitou, falšování elektronického podpisu a útoky na bankovní operace.

---

[16] TCP/IP – Transmission Control Protocol/Internet Protocol, česky primární transportní protokol, jedná se komunikační protokol.
[17] DDoS – Distributed Denial of Service, česky distribuované odmítnutí služby.
[18] Router – směrovač, síťové zařízení.
[19] Firewall – síťové zařízení, slouží k řízení a zabezpečení síťového provozu.
[20] Bezpečnostní informační služba – BIS, se dále zabývá oblastmi Extremismu, šíření zbraní hromadného ničení, obchodem s konvenčními zbraněmi a výbušninami, organizovaným zločinem, nelegální migrací, činnost cizích zpravodajských služeb na našem území.

Nové riziko, se kterým BIS bojuje, je „informační boj“, patří sem aktivity hackerů, kteří vyvíjí aplikace virů, které vyřazují nebo zcela ničí počítačové systémy. Útoky jsou zpravidla rozesílány jednotlivci nebo skupinami s cílem prosadit své představy, šířit vlastní teorii nebo poškodit protivníka.

Úkoly Bezpečnostní informační služby v oblasti elektronické komunikace vyplývají z dokumentu „Národní strategie informační bezpečnosti“, který byl v roce 2005 schválen vládou ČR. Prioritním cílem BIS je snaha snížit zranitelnost elektronických komunikačních systémů. Snaha předejít útokům a to odhalením takových případů, včetně jejich motivů.

Utajením si stát chrání informace důležité pro jeho bezpečnost. BIS má za úkol zpravodajsky chránit subjekty, které s utajovanými informacemi pracují. Při této činnosti se řídí zákonem č. 412/2005 Sb. Dále vyhodnocuje a označuje konkrétní místa, kde hrozí nebezpečí úniku informací. Když se BIS podaří získat informace o pokusu krádeže utajovaných informací, vykonává opatření proti útoku.

V neposlední řadě se BIS zabývá kontrašpionáží. BIS v případě kontrašpionáže brání stát před špiony jiných států, kteří chtějí získat zákonem chráněné utajované informace.

Na našem území působí zahraniční výzvědné agentury, které se zaměřují na prosazování politických nebo ekonomických potřeb jiných států. Cizí aktivity by mohly poškodit zájmy ČR nebo způsobit problémy. BIS sleduje pohyb cizích rozvědek na území ČR, větší pozornost věnuje službám států, kde existuje podezření, že jakýmkoliv způsobem podporují teroristické organizace. Pokud cizí agentury získávají informace z volně přístupných zdrojů, není potřeba proti nim zasahovat. Problém nastane v případě, kdy agenti začnou pracovat proti zájmům státu, ohrožovat demokratický systém a získávat naše občany jako své agenty. Usvědčit konkrétního „špiona“ z trestné činnosti, zadržet jej, předat vyšetřovateli a odsoudit, je zpravidla velmi obtížné. Špioni před vysláním do zahraničí procházejí speciálním výcvikem, zaměřeným na trestnou činnost špionáže a maximální ztížení dokazování a usvědčení z této trestné činnosti.

Důležitým úkolem kontrašpionáže je také prevence proti příjezdům pracovníků cizích výzvědných služeb, u kterých je riziko, že v případě pobytu v ČR budou pracovat proti zájmům našeho státu. V tomto smyslu hraje významnou roli výměna informací a spolupráce zpravodajských organizací všech demokratických zemí. Jsou-li k dispozici

potřebné poznatky, snaží se BIS informováním příslušných státních orgánů příjezdu těchto lidí zabránit. Součástí prevence jsou také výstrahy, kdy BIS – v případě nevyhnutelného kontaktu – upozorňuje na jejich dvojí roli, a tak varuje své adresáty před kontakty se zpravodajsky aktivními osobami, které u nás působí.

Důležité informace si tajné služby včetně BIS předávají komunikačními zařízeními a prostřednictvím informačních systémů. Komunikace a nakládání s informacemi je zabezpečeno moderními prvky kryptografické ochrany tak, aby se k nim nedostaly nepovolané osoby a informace nebyly zneužity.

1.10 Ruská FAPSI

Zkratka FAPSI znamená „Federální agenturu pro vládní komunikaci a informace“. Jedná se o ruskou elektronickou odposlechovou službu. Tato vládní agentura je zodpovědná za zpravodajskou a bezpečnostní vládní komunikaci. FAPSI má povolení sledovat vládní a soukromé bezpečnostní služby v Rusku. Sleduje také zahraniční obchod a důvěrné bankovní operace a má povolení pracovat v zahraničí.

FAPSI vznikla sloučením 8. a 16. hlavní správy KGB a byla založena prezidentským dekretem z 19. ledna 1993. Má podobnou strukturu jako americká Národní bezpečnostní agentura.

Obr. 6. Erb FAPSI

[zdroj obrázku uveden v použité literatuře, zdroj číslo [6]]

FAPSI dodává ruské vládě informace získané elektronickými metodami. Vlastní síť satelitů, které jsou určeny pro přenos vládních a zpravodajských informací.

V oblasti kryptografické ochrany má FAPSI povolení sledovat a zaznamenávat finanční transakce, soukromé připojení na internet a elektronickou komunikaci. Prezidentský dekret, podepsaný 3. dubna 1995, nařizuje FAPSI monitorovat a nahrávat všechny finanční operace v zemi. Zajímavostí je, že následně FAPSI požaduje od bank platbu za tuto službu. Získané peníze jsou rozděleny mezi FAPSI a Prezidentský program. Všichni poskytovatelé internetu v Rusku musí mít nainstalovaný speciální hardware, který umožňuje filtrování a dálkové ovládání internetového provozu. Poskytovatelé internetu musí také za zařízení platit FAPSI.

Mezi další hlavní úkoly FAPSI patří ochrana vládního a prezidentského informačního a komunikačního systému, bezpečné poskytování státního tajemství, organizování vnější činnosti zpravodajských služeb, poskytování nadřízeným orgánům státní moci spolehlivé informace a další činnosti.

1.11 Americká NSA

Zkratka NSA a CSS (National Security Agency/Central Security Service) v překladu znamená Národní bezpečnostní agentura/Centrální bezpečnostní služba. NSA je vládní organizace Spojených států amerických patřící pod ministerstvo obrany. Organizace vznikla 4. listopadu 1952.

Obr. 7. Sídlo NSA ve Fort Meade v Marylandu

[zdroj obrázku uveden v použité literatuře, zdroj číslo [6]]

Hlavním úkolem NSA je chránit národní bezpečnost Spojených států amerických. Zabraňuje zahraničním protivníkům získat přístup k utajovaným informacím. Shromažďuje, zpracovává a šíří informace pro podporu vojenských operací.

„Je odpovědná za sběr a analýzu zahraniční komunikace, koordinuje, řídí a provádí vysoce specializované činnosti, jejichž účelem je získávání zpráv zahraničních rozvědek. Je taktéž odpovědná za ochranu informačních systémů uvnitř vlády Spojených států a její komunikace s jinými agenturami. Výše zmíněné činnosti vyžadují značné prostředky pro kryptoanalýzu a kryptografii.“[21]

Obr. 8. Znak NSA

[zdroj obrázku uveden v použité literatuře, zdroj číslo [25]]

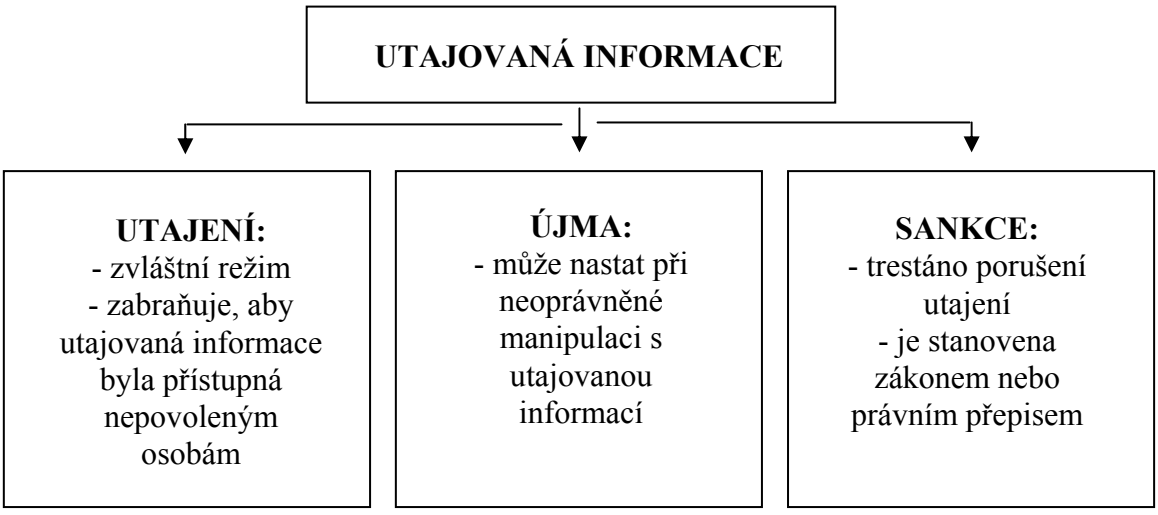
[21] *Wikipedie : Otevřená encyklopedie* [online]. 2001 , 6.1.2009 [cit. 2009-04-20]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/NSA>.

2 OCHRANA UTAJOVANÝCH INFORMACÍ

Důležitou částí bezpečnostní problematiky, se kterou se mnoho firem při své činnosti setkává, je problematika ochrany utajovaných informací. Ochrana utajovaných informací také nesmazatelně patří do PKB. Nejedná se o problematiku novou, přesto přístup k ní je zcela nový. Přístup k problému ochrany utajovaných informací nemůže být chápán ze strany subjektů jen jako formální, protože formální přístup představuje hrozbu pro utajované informace. Systém ochrany utajovaných informací a plnění podmínek pro získání potvrzení nebo certifikace musí být chápán jako aktivní proces. Organizace musí dodržovat zásady a pravidla, podle kterých dosáhnou nejefektivnějšího výsledku v práci s utajovanými informacemi.

2.1 Utajované informace

Jedná se o informace, na jejichž utajení má zájem fyzická osoba nebo právnická osoba. Zájem vyplývá ze skutečnosti, že při zneužití utajovaných informací vzniká určitá újma. Zájem o utajení informace chápeme zpravidla tak, aby utajení bylo zachováno a nepovolaná osoba se s utajovanými informacemi neseznámila. Ostatní instituty obdobné utajovaným informacím jsou obchodní tajemství, know – how, ochrana průmyslových práv, autorská práva a jejich ochrana, mlčenlivost, svobodný přístup k informacím a ochrana osobních údajů.



Obr. 9. Znaky utajované informace.

Základní znaky utajované informace jsou:

- utajování
- újma
- sankce

a) Utajování

Informaci, kterou považujeme za utajenou, musí podléhat zvláštnímu režimu, který omezuje znalost obsahu informace jen na určený počet fyzických osob. Tento zvláštní režim nazýváme režim utajení. Jedná se o souhrn nařízení, opatření a činností, které zajišťují, aby se s utajovanou informací nemohla seznámit nepovolaná osoba nebo aby s utajovanou informací nebylo nakládáno nežádoucím způsobem.

„Utajování je specifický systém ochrany utajované informace, který zajišťuje současně:

- důvěrnost utajovaných informací, tzn. že neoprávněná (neautorizovaná) osoba se s utajovanou informací nejen neseznámí, ale ani k ní nepronikne, aby nemohla s utajovanou informací neoprávněně nakládat jiným způsobem,
- integritu utajované informace, která znamená, že utajovaná informace nemůže být neoprávněnou osobou jakkoli modifikována (změněna, poškozena či zničena) a
- dostupnost utajované informace[22], tzn., že zajišťuje i rychlý a úplný přístup k utajované informaci pro oprávněné osoby.“[23]

b) Újma

Dalším z charakteristických znaků utajované informace je vznik újmy v případě neoprávněného nakládání s utajovanou informací. Podle újmy (hrozby) se jednotlivé

[22] Rudolf Musil ve své knize Ochrana utajovaných skutečností používá slovo skutečnost, slovo skutečnost bylo nahrazeno v zákoně č. 412/2005 Sb. slovem informace.

[23] MUSIL, Rudolf. *Ochrana utajovaných skutečností*. s. 1. vyd. Praha : Eurounion, 2001. s.26. ISBN 80-85858-93-2.

utajované informace klasifikují na příslušné stupně utajení. Zákon č. 412/2005 Sb.[24] v § 3 definuje újmu jako „poškození nebo ohrožení zájmu České republiky."

Podle závažnosti nebo ohrožení zájmu ČR se újma dělí na mimořádně vážnou újmu, vážnou újmu a prostou újmu. Zákon přesně definuje, co která újma přináší a způsobuje. Následky mohou představovat přímou finanční nebo materiálovou škodu, újmy na životě a zdraví osob a újmy, které se nedají pro svou povahu jednoznačně finančně vyčíslit. Poškození nebo ohrožení chráněného zájmu má důsledky, které nelze odstranit vůbec nebo pouze zmírnit následnými opatřeními.

c) Sankce

Jedná se o negativní následek pro toho, kdo porušil zákonem nebo předpisem stanovené povinnosti v souvislosti s utajovanými informacemi. Obecnou povinností všech fyzických osob je dodržovat obecné povinnosti stanovené právními předpisy týkajících se utajovaných informací. Dále také nutná omezení stanovená orgánem státu nebo organizací. Sankce představuje prostředek, kterým stát prosazuje svůj zájem na ochraně utajovaných informací a na dodržování stanovených pravidel. Sankce mají různou podobu, od sankcí finančních, majetkových až po sankce podle trestního zákona.

Zákon č. 412/2005 Sb. odstupňoval možný rozsah vzniklé újmy a vyjádřil význam chráněného zájmu pomocí klasifikace utajovaných informací do jednotlivých stupňů utajení. Každá utajovaná informace musí být správně označena příslušným stupněm utajení, který musí být správně stanoven.

Utajované informace se dělí do čtyř stupňů utajení:

a) „Přísně tajné", zkratka PT, nejvyšší stupeň utajení, vyzrazení takové informace neoprávněné osobě nebo její zneužití může způsobit zájmům ČR mimořádně vážnou újmu.

---

[24] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Nabyl účinnosti 1.1. 2006 a byl již sedmkrát novelizován zákonem č. 119/2007 Sb., zákonem č. 177/2007 Sb., zákonem č. 296/2007 Sb., zákonem č. 32/2008 Sb., zákonem č. 124/2008 Sb., zákonem č. 126/2008 Sb., zákonem č. 250/2008 Sb.

b) „Tajné“, zkratka T, druhý nejvyšší stupeň utajení, vyzrazení informace stupně „Tajné“ neoprávněné osobě nebo její zneužití může způsobit zájmům ČR vážnou újmu.

c) „Důvěrné“, zkratka D, jedná se o další nižší stupeň utajení, vyzrazení „Důvěrné“ informace neoprávněné osobě nebo zneužití informace může způsobit zájmům ČR prostou újmu.

d) „Vyhrazené“, zkratka V, vyzrazení informace stupně utajení „Vyhrazené“ neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy ČR, tzn. nedochází k újmě ani hrozbě újmy.

2.2 Bezpečnostní politika podniku ve smyslu ochrany utajovaných informací

Problematika týkající se bezpečnosti provází člověka od počátku jeho existence. Způsob zabezpečení se v průběhu historie měnil, avšak předmětem zabezpečení a ochrany bylo vždy zdraví a život, majetek, informace a znalosti. V mnoha případech spolu tyto skupiny souvisí, např. porušení utajení informace a její případná ztráta mohou vést ke ztrátám na majetku. Specifickou skupinou jsou znalosti získané na základě informací. Jedná se o znalosti a informace, jejichž zpracování je náročné a jsou méně dostupné většímu počtu lidí. Nejedná se tedy o veškeré informace, ale jen o informace s určitou hodnotou, často velmi významnou pro jejich nositele.

„Průmyslová špionáž, i když je specifickým druhem získávání informací, patří do nejstarší špionážní činnosti na světě, mnohem dříve docházelo k projevům průmyslové špionáže než k projevům špionáže vojenské.“[25]

Smyslem ochrany utajovaných informací, je najít bezpečný způsob, jak seznamovat určitý okruh lidí s utajovanými informacemi. A zároveň učinit opatření, aby se s utajovanými informacemi neseznamovaly nepovolané osoby. S tímto úkolem se musí vypořádat každý,

[25] LAUCKÝ, Vladimír. *Speciální bezpečnostní technologie.* 1. vyd. Zlín : [s.n.], 2009. 111 s. ISBN 978-80-7318-762-0.

kdo řeší otázky spojené s ochranou utajovaných informací. Tvoření bezpečnostní politiky a bezpečnostního projektu podniku nespočívá v dosazení prvků do předem dané šablony. Jedná se o přístup k řešení konkrétního problému v konkrétní organizaci, což vyžaduje odborné vzdělání a praxi.

Bezpečnostní politika organizace a bezpečnostní projekt organizace jsou dokumenty, které organizace předkládá NBÚ a žádá o provedení bezpečnostní prověrky. Dokument bezpečnostní politiky stanovuje základní zásady, opatření a vytyčuje hlavní směry, jakým se bude dosahovat ochrany utajovaných informací pro požadovaný stupeň utajení. Nepřináší však podrobný přehled všech jednotlivých prvků a postupů, jak dosáhnout stanoveného cíle.

2.2.1 Cíle organizace v oblasti ochrany informací

Předmětem ochrany jsou utajované informace, které organizace vytvoří nebo které jsou jí svěřeny. Zaměříme-li se na cíl organizace v oblasti ochrany utajovaných skutečností z hlediska prostředků ochrany, pak dostáváme tyto konkrétní cíle:

- zabránit seznámení nepovolané osobě s utajovanými informacemi.
- vytvořit opatření, aby se s utajovanými informacemi seznamovaly osoby, které splňují podmínky stanovené zákonem č. 412/2005 Sb.
- chránit utajované informace při jejich manipulaci, např. tvorbě, příjmu, evidenci, zpracování, ukládání a podobné činnosti.
- zabezpečit objekt nebo prostor, kde se utajované informace vyskytují, před nepovolanými osobami.
- učinit opatření, které zabrání poškození, znehodnocení, zničení nebo jiné ohrožení utajovaných informací.
- při zabezpečení utajovaných informací používat jen technické prostředky, kryptografické metody a informační systémy certifikované NBÚ.

Organizace musí posoudit, na základě své předpokládané činnosti a dosavadních zkušeností, zda jí budou utajované informace poskytovány jinou organizací nebo budou v organizaci přímo vznikat. Musí také umět posoudit druh utajovaných informací, zda utajovaná informace bude mít podobu běžného textu, technické dokumentace, výsledky

měření a další cenné informace. Dále je důležitý rozsah utajovaných informací, se kterými se organizace může seznamovat, a požadovaný stupeň utajení. Určení míst výskytu utajovaných informací má význam pro zpracování personální a administrativní bezpečnostní politiky. Musí být jasně určeno, kde utajované informace můžou vznikat, kde mají být uloženy nebo kde se s nimi může manipulovat.

2.2.2 Hodnocení míry rizik

Jedná se o jednu z nejdůležitějších oblastí bezpečnostní politiky ve smyslu ochrany utajovaných informací. Cílem je popsat hrozbu, stanovit rizika a rozsah možných následků, kdyby riziko nastalo. Zpravidla postačí formulovat hlavní nositele rizik, mezi které patří lidský faktor, provozní faktor (technologické procesy) a náhodné jevy nebo události. Dále je nutné definovat přiměřená opatření a prostředky k ochraně utajovaných informací. Projekt v rámci jednotlivých oblastí zabezpečení musí být zpracován podrobně a přesně. Bez znalosti možných hrozeb a míry rizika není možné vypracovat spolehlivý a účinný systém k ochraně utajovaných informací.

„Východiskem pro relevantní hodnocení míry rizik je příslušná analýza, tj. analýza rizik. Obecně lze říci, že v rámci analýzy rizik je v prvé řadě nutné definovat si jednotlivé prvky celého bezpečnostního systému v organizaci (lidi, utajované informace, organizačně režimová opatření, objekty, technická zařízení – PC, bezpečnostní techniku ad.) a na základě toho stanovit jednotlivé hrozby, které na tyto prvky působí. Rozhodující jsou ty hrozby, které způsobují snížení úrovně zabezpečení utajovaných informací nebo dokonce jeho úplné vyřazení, popř. které působí uvedeným způsobem přímo na utajované informace. Ne všechny hrozby působí na celý systém. Zpravidla působí pouze na určité jeho části – prvky, resp. na určitá místa – body v těchto prvcích, a to na místa, která jsou méně odolná a představují tak slabinu využitelnou ke způsobení škody nebo ztráty útokem na systém ochrany. Pro tato místa se vžil obecně název zranitelná místa.“[26]

[26] MUSIL, Rudolf. Ochrana utajovaných skutečností. s. 26, 1. vyd. Praha : Eurounion, 2001. ISBN 80-85858-93-2.

2.2.3 Místa výskytu utajovaných informací

Pracoviště nebo místa, kde se vyskytují utajované informace, jsou uvedena v bezpečnostní politice. Popis areálu, objektu a zabezpečené oblasti obsahuje bezpečnostní projekt ochrany objektu. Výkresová část zřetelně vyznačuje objekt i zabezpečenou oblast, tzn. jsou zřetelně vidět jejich hranice. Zjištění rizik a zranitelných míst ohrožení utajovaných informací představuje stěžejní činnost pro konečné splnění plánu.

Rozhodnutí, jaké prostředky ochrany a kde budou použity, závisí na posouzení řady aspektů. Podmínky vyplývají z utajovaných informací (o jaký druh se jedná, stupeň utajení a rozsah), konkrétního objektu a zabezpečené oblasti. Bezpečnostní projekt již závazně stanoví konkrétní prostředky ochrany utajovaných informací, jejich počet, způsob použití.

2.3 Personální bezpečnost

Politiku personální bezpečnosti musíme akceptovat ze dvou pohledů. První pohled řeší problematiku z hlediska zajištění bezpečnosti utajovaných informací na základě kvalitního výběru osob, které se mají seznamovat s utajovanými informacemi v organizaci. Druhý pohled řeší přístup k problematice i z hlediska personální práce s osobami, které jsou již určeny k seznámení s utajovanými informacemi. Personální bezpečnost není jen o správném výběru osoby, ale je nutné s nimi pracovat, zajišťovat jejich výcvik a informovanost o problematice utajovaných informací.

Personální bezpečnost je jedním ze základních druhů zajištění ochrany utajovaných informací. Ověřuje podmínky, které musí fyzická osoba splnit, aby mohla přijít do styku s utajovanými informacemi. Za zajištění proškolení fyzických osob, které mají přístup k utajovaným informacím, ručí odpovědná osoba. Jednou ročně je odpovědná osoba povinna zajistit proškolení osobám, které mají přístup k utajovaným informacím. Proškolení se týká právních předpisů v odvětví ochrany utajovaných informací. Podmínky, které musí fyzická osoba splnit, aby jí byl umožněn přístup k utajovaným informacím, jsou odlišné podle stupně utajení. Pro utajované informace stupně „Vyhrazené“ ověřuje podmínky odpovědná osoba nebo jí určená osoba. Pokud taková osoba není, tak ověření provede NBÚ. Pro stupně utajení „Důvěrné“, „Tajné“ a „Přísně tajné“ se splnění podmínek ověřuje v bezpečnostním řízení.

Ministerstva a další správní úřady jsou povinny každý rok do 31. října zpracovat a zaslat NBÚ personální projekt. Obsahem projektu je zhodnocení stavu za uplynulý rok a pravděpodobný počet osob, u kterých bude v dalším roce nutné provést bezpečnostní řízení. Bezpečnostní řízení je proces, který vede NBÚ nebo jiný ze zákona pověřený subjekt. Týká se oblasti personální bezpečnosti a slouží k ověření, zda fyzická osoba splňuje podmínky pro vydání osvědčení fyzické osoby a dokladu o bezpečnostní způsobilosti.

2.3.1 Přístup k utajované informaci

Fyzická osoba, která podepsala poučení, má oprávnění se seznamovat s utajovanými informacemi, které potřebuje k výkonu své funkce, pracovní nebo jiné činnosti. Poučení je dokument, který podepisuje fyzická osoba vždy před prvním přístupem k utajovaným informacím daného stupně. V rozsahu nepřesahujícím hranice poučení, tzn. o jaký stupeň utajení se jedná a rozsah utajované informace. Zajištění proškolení fyzických osob obstarává odpovědná osoba, která je povinna jednou ročně zajistit u osob, které mají přístup k utajované informaci, proškolení z právních předpisů. Platnost poučení končí zánikem platnosti oznámení o splnění podmínek pro přístup k utajovaným informacím, dokladu nebo osvědčení fyzické osoby.

Podmínky platnosti:

a) Platnost oznámení o splnění podmínek pro přístup k utajovaným informacím musí ověřovat ten, kdo ho vydal, a to každé tři roky ode dne jeho vydání.

b) Doklad o bezpečnostní způsobilosti platí po dobu 5ti let.

c) Platnost osvědčení fyzické osoby je různá, podle stupně utajení:

   - pro stupeň utajení „Důvěrné“ 9 let ode dne vydání.
   - pro stupeň utajení „Tajné“ 7 let ode dne vydání.
   - pro stupeň utajení „Přísně tajné“ 5 let ode dne vydání.

Fyzická osoba musí splnit určité podmínky, jestliže jí má být vydáno oznámení o splnění podmínek pro přístup k utajovaným informacím, osvědčení fyzické osoby nebo doklad o bezpečnostní způsobilosti. Podmínky jsou stanoveny zákonem a jejich splnění se ověřuje v bezpečnostním řízení, kromě podmínek pro stupeň utajení „Vyhrazené“. Všechny

požadované podmínky musí fyzická osoba splňovat, nelze žádnou pominout. Podmínky musí být splněny všechny současně, absence některé z podmínek způsobí, že nejsou splněna požadovaná kritéria a osvědčení nebo oznámení nebude vydáno.

Oznámení se vydá fyzické osobě, pro stupeň utajení „Vyhrazené“, která splňuje podmínky:

a) způsobilost k právním úkonům.

b) věk alespoň 18 let.

c) bezúhonnost.

Osvědčení se vydá fyzické osobě, pro stupeň utajení „Důvěrné“, „Tajné“ a „Přísně tajné“, která splňuje následující podmínky:

a) způsobilost k právním úkonům.

b) věk alespoň 18 let.

c) bezúhonnost.

d) státní občanství ČR, členské země EU nebo NATO.

e) osobní způsobilost.

f) bezpečnostní spolehlivost.

Tabulka ukazuje přehled možností držitelů jednotlivých dokumentů:

	Přístup k utajovaným informacím stupně utajení „**Vyhrazené“**	Přístup k utajovaným informacím stupňů utajení „**Důvěrné“** nebo „**Tajné“** nebo „**Přísně tajné“**	Výkon citlivé činnosti
Typ dokumentu nebo veřejné listiny nutný k přístupu či výkonu	Oznámení o splnění podmínek pro přístup k utajované informaci		
	Osvědčení fyzické osoby	Osvědčení fyzické osoby	Osvědčení fyzické osoby
	Doklad o bezpečnostní způsobilosti		Doklad o bezpečnostní způsobilosti

Tab. 1. Přehled dokumentů.

[zdroj uveden v použité literatuře, zdroj číslo [17]]

K utajovaným informacím bez platného osvědčení fyzické osoby a poučení mají podle zákona přístup prezident republiky, senátoři a poslanci parlamentu, členové vlády, Veřejný ochránce práv a jeho zástupce, soudci a členové Nejvyššího kontrolního úřadu, jeho prezident a viceprezident. Přístup k utajovaným informacím platí ode dne zvolení nebo jmenování výše uvedených osob do funkcí a platí po celou dobu jejího výkonu.

Další možností, jak přijít do styku s utajovanými informacemi je jednorázový přístup k utajovaným informacím. NBÚ ve výjimečných a odůvodněných případech může vydat souhlas, s dobou přístupu nejdéle 6 měsíců. Podmínka udělení spočívá v tom, že lze udělit souhlas pouze pro utajovanou informaci o jeden stupeň vyšší, než je současné platné osvědčení fyzické osoby. Žádost o jednorázový přístup je vždy písemná.

2.3.2 Bezpečnostní řízení

V oblasti personální bezpečnosti ověřuje, jestli fyzická osoba splňuje podmínky pro vydání osvědčení fyzické osoby. Bezpečnostní řízení vede NBÚ nebo jiný ze zákona oprávněný subjekt. Řízení je neveřejné a jednacím jazykem je čeština (vyjma zákonného výkonu práva příslušníka národní menšiny). Písemné dokumenty v cizích jazycích musí být předloženy jak v originále, tak i v překladu do českého jazyka, který je úředně ověřen. V případě osobní nepřítomnosti se může účastník nechat zastoupit advokátem nebo vybraným zástupcem, kterému udělil písemnou plnou moc. Délka bezpečnostního řízení o vydaní osvědčení fyzické osoby pro stupeň utajení „Důvěrné“ je 3 měsíce, pro stupeň utajení „Tajné“ 9 měsíců a pro stupeň utajení „Přísně tajné“ 12 měsíců.

Cílem řízení je zjistit stav nezbytný pro rozhodnutí o vydání nebo nevydání osvědčení fyzické osoby. Úkony, s řízením spojené, vedou k ověření pravdivosti údajů účastníků bezpečnostního řízení. Důležitými instituty během řízení jsou svědek, pohovor s účastníky řízení a znalec. Řízení končí rozhodnutím o nevydání osvědčení nebo dokladu, doručením osvědčení nebo dokladu. Řízení může být také zastaveno, např. když účastník bezpečnostního řízení zemře, je prohlášen za mrtvého nebo vezme žádost zpět.

2.4 Průmyslová bezpečnost

Podle § 15 zákona č. 412/2005 Sb.: „Lze podnikateli umožnit přístup k utajované informaci, jestliže jej nezbytně potřebuje k výkonu své činnosti a je držitelem platného osvědčení podnikatele (§ 54) příslušného stupně utajení, pokud zákon nestanoví jinak.“

Podnikatel je účastníkem bezpečnostního řízení a žádá o vydání osvědčení podnikatele. Rozhodnutí podat žádost o vydaní osvědčení podnikatele obvykle nastane za účelem obchodního kontaktu. Například zákazník požaduje, aby podnikatel byl držitelem platného osvědčení podnikatele. Z důvodu, že se bude seznamovat s utajovanými informacemi nebo u něho utajované informace budou vznikat. Podnikatel k utajovaným informacím přistupuje z pohledu dvou variant.

Podle § 20 zákona č. 412/2005 Sb., existují dvě formy přístupu podnikatele k utajované informaci:

a) „která u něho vzniká, nebo je mu poskytnuta, nebo

b) která u něho nevzniká, ani mu není poskytována, ale ke které mají přístup zaměstnanci podnikatele nebo osoby jednající jménem podnikatele nebo za podnikatele, a to v souvislosti s výkonem pracovní nebo jiné činnosti pro podnikatele na základě smlouvy.“

První zmíněná forma přístupu znamená, že utajovaná informace je poskytována na libovolném nosiči. To představuje, že podnikatel utajovanou informaci vytváří ve své firmě nebo je mu předána. Druhá forma přístupu podnikatele představuje seznámení s utajovanou informací. Pro podnikatele to představuje, že mu utajovaná informace není předána, ale podnikatel se s utajovanou informací pouze seznámí. Takové seznámení se zpravidla provádí při zadávání zakázky.

Dále je nutné stanovit stupeň utajení, v žádosti se stupeň utajení jednoznačně definuje a doplňuje se formou přístupu. Podnikatel nemůže v jedné žádosti požádat o rozdílný stupeň utajení. Stupeň utajení pro seznamování se s utajovanou informací a stupeň utajení pro poskytování, vznik nebo uchování se nesmí lišit. V případě, že chce podnikatel požádat o rozdílný stupeň, musí předložit dvě samostatné žádosti.

Žádost podnikatele upravuje § 96 zákona č. 412/2005 Sb. Stanovuje, co všechno podnikatel musí přiložit k žádosti, a dobu, do které je nutné zažádat NBÚ v případě používání osvědčení bezprostředně po uplynutí doby platnosti.

Dotazník podnikatele je vymezen v § 97 zákona č. 412/2005 Sb. a je v něm stanoveno, jaké položky dotazník obsahuje.

Podnikatel musí předložit písemnosti k ověření splnění podmínek pro vydání osvědčení podnikatele. Jedná se o originály nebo ověřené kopie, seznam těchto písemností je uveden

v § 2 vyhlášky o průmyslové bezpečnosti. Požadavky na doložení písemností se dělí podle toho, jestli se jedná o podnikatele, který je právnickou osobou nebo podnikající fyzickou osobou. Výjimkou je zahraniční osoba, která je podnikatelem podle zvláštního předpisu. Taková osoba musí doložit písemnosti obdobné uvedeným dokladům podle konkrétní země.

Bezpečnostní dokumentace podnikatele podle § 98 zákona č. 412/2005 Sb. představuje písemný dokument, který stanoví systém ochrany utajovaných informací u podnikatele. Dokumentace musí být průběžně aktualizována a § 98 obsahuje stanovené požadavky. Součástí bezpečnostního řízení žádosti podnikatele je také žádost o vydání osvědčení fyzické osoby. Seznam osob, které budou mít přístup k utajovaným informacím, je součástí bezpečnostní dokumentace podnikatele.

Podnikatel je povinen před vydáním i po vydání osvědčení podnikatele hlásit změny údajů v žádosti, tyto změny se oznamují NBÚ.

Platnost osvědčení podnikatele je podle § 55 zákona č. 412/2005 Sb. pro stupeň utajení „Vyhrazené“ 12 let, „Důvěrné“ 9 let, „Tajné“ 7 let a „Přísně tajné“ 5 let. Podnikateli lze umožnit za určitých podmínek jednorázový přístup k utajované informaci, přístup v mimořádných situacích nebo přístup k utajované informaci na základě uznání bezpečnostního oprávnění vydaného úřadem cizí moci.

2.4.1 Bezpečnostní řízení

Bezpečnostní řízení je proces, který vede NBÚ a slouží k ověření, zda podnikatel splňuje podmínky pro vydání osvědčení podnikatele. Délka řízení o vydání podnikatele NBÚ vykoná ve lhůtě 3 měsíce pro stupeň utajení „Vyhrazené“, 6 měsíců pro stupeň utajení „Důvěrné“, 9 měsíců pro stupeň utajení „Tajné“ a 12 měsíců pro stupeň utajení „Přísně tajné“. U žádosti, která nemá požadované náležitosti a nelze je hned odstranit, NBÚ písemně vyzve účastníka, aby nedostatky v žádosti odstranil. Doba na odstranění je 30 dnů, jinak NBÚ může zastavit řízení.

Rozhodnutí řízení NBÚ vydává nejen na základě údajů od účastníka řízení, ale také podle informací od příslušných orgánů státu, právnických nebo podnikajících osob. V průběhu řízení lze využít výslech svědka, pohovor s účastníkem nebo ustanovení znalce.

V určitých případech může dojít k přerušení řízení, podle § 112 zákona č. 412/2005 Sb. Řízení je přerušeno, jestliže:

- „u jiného orgánu státu probíhá řízení, které řeší otázku významnou pro vydání rozhodnutí (tzv. předběžná otázka),
- účastník řízení byl vyzván, aby odstranil nedostatky v žádosti nebo aby doplnil jiné požadované údaje,
- nelze provést výslech svědka,
- účastník řízení požádá o přerušení z důvodů bránících mu v účasti na řízení, nejdéle však na dobu 60 dnů,
- byl ustanoven znalec pro vypracování znaleckého posudku.“[27]

Řízení může NBÚ zastavit, když účastník bezpečnostního řízení:

- „vezme svoji žádost zpět,
- nesplňuje základní podmínky jako je věk, bezúhonnost a způsobilost k právním úkonům,
- neodstraní ve stanovené lhůtě nedostatky v žádosti,
- nedostaví se opětovně bez omluvy k pohovoru,
- nedá souhlas k provedení dalších nezbytných úkonů podle § 107 odst. 5 zákona,
- podá nepravdivou nebo neúplnou výpověď či neposkytuje jinou nezbytnou součinnost a na základě daného stavu nelze rozhodnout,
- zemře nebo je prohlášen za mrtvého.“[28]

2.5 Administrativní bezpečnost

Administrativní bezpečnost řeší otázky organizačních a administračních procesů v organizaci. Zaměřuje se především na vybudování firemního systému administrativního

---

[27] Národní bezpečnostní úřad [online]. 2007- , 16.1.2009 [cit. 2009-02-20]. Dostupný z WWW: <http://www.nbu.cz/cs/bezpecnostni-zpusobilost/bezpecnostni-rizeni/>.

[28] Národní bezpečnostní úřad [online]. 2007- , 16.1.2009 [cit. 2009-02-20]. Dostupný z WWW: <http://www.nbu.cz/cs/bezpecnostni-zpusobilost/bezpecnostni-rizeni/>.

zpracování, evidenci utajovaných informací, problematiku médií, tím se myslí, na čem je utajovaná informace zachycena a přenášena. Nesmí být zapomenuto na otázku ukládání, přenosu, manipulace a fyzické likvidace utajované informace. Administrativní bezpečnost utajovaných informací má za cíl realizovat administrativně organizační opatření, které zajistí ochranu utajovaných informací uložených na různých médiích, a to HDD, DVD, CD, papír a další. Ochrana musí být směřována na fyzickou ochranu médií, to znamená proti hrozbě fyzického zničení nebo poškození utajované informace, a na ochranu před seznámením nepovolaných osob s obsahem utajované informace.

Vznik nebo první výskyt utajované informace v organizaci musí být řádně zaevidován a označen. Označit utajovanou informaci znamená přidělit utajované informaci správný stupeň utajení, což je důležité, protože v případě nesplnění nebo nesprávného splnění se jedná o případ neoprávněného nakládání s utajovanou informací. Vyznačení stupně utajení na utajované informaci musí být zachováno po celou dobu trvání utajení.

Samozřejmě při nesprávném označení, nebo dokonce při neoznačení, může dojít k situaci, že se utajovaná informace dostane k neoprávněným osobám. Dále je nutné vyznačit název pro utajovanou informaci, to znamená, od koho informace pochází, evidenční označení a datum vzniku utajované informace. Značení utajovaných informací vyžaduje kromě stanovených zásad velkou pozornost. Lehce může dojít k omylu při značení a může vzniknout velká škoda.

Pravidla administrativní bezpečnosti jsou uvedena v § 21 až § 23 zákona č. 412/2005 Sb. a rozpracovaná ve vyhlášce č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.

Politika administrativní bezpečnosti utajovaných informací si klade v organizaci následující cíle:

- dodržovat zásady bezpečné manipulace s utajovanými informacemi v konkrétních podmínkách organizace,
- odpovědnost za prosazování zásad administrativní bezpečnosti v organizaci na každé funkční úrovni,
- přijetí a dodržování vnitropodnikových norem, které se týkají oběhu dokumentů v organizaci (patří sem také zásady archivace a skartace).

2.5.1 Administrativní pomůcky

Administrativní pomůcky používané k práci s utajovanými informacemi obsahují přesně stanovené náležitosti, jako např. jednací protokol, který může být ve formě knihy nebo sešitu.

Za administrativní pomůcky se považují:

- jednací protokol, který se používá pro evidování utajovaného dokumentu.
- pomocný jednací protokol slouží k zaznamenání pohybu utajovaného dokumentu v rámci orgánu státu, právnické osoby nebo podnikající fyzické osoby.
- manipulační kniha se používá při vytváření, převzetí a předání utajovaného dokumentu.
- doručovací kniha slouží pro zaznamenání předání utajovaného dokumentu.
- zápůjční kniha pro evidování zápůjček uloženého utajovaného dokumentu.
- kontrolní list pro vedení přehledu osob, které se s obsahem utajovaného dokumentu seznámily. Platí pro stupně utajení „Důvěrné“, „Tajné“ a „Přísně tajné“.
- sběrný arch se používá v jednacím protokolu, kde slouží jako rozšíření evidenčního záznamu, tzn. evidování většího počtu utajovaných dokumentů ke stejné věci.

Administrativní pomůcky je možné vést i v elektronické podobě, přičemž musí obsahovat všechny předepsané položky. Systém, ve kterém jsou vedeny, je zabezpečen proti neoprávněnému zásahu a přístupu osob. Dále systém musí zaznamenávat všechny provedené změny a jeho používání je schváleno odpovědnou osobou.

Záleží na organizaci, jak se rozhodne, jakým způsobem bude své administrativní pomůcky vést. Žijeme v moderní době plné počítačů, a tak si každý myslí, že administrativní pomůcky se vedou jen v elektronické podobě. Osobně si myslím, že řada organizací vede administrativní pomůcky psané ručně.

Pokyny k administrativním pomůckám:

- evidenci administrativních pomůcek vede bezpečnostní ředitel, ředitelem pověřená osoba nebo osoba pověřená vedením jednacího protokolu.
- kontrolní list k utajovanému dokumentu vyhotovuje osoba, která utajovaný dokument vyhotovuje nebo osoba pověřená vedením jednacího protokolu.

- údaje do všech administrativních pomůcek se zapisují způsobem (prostředkem), který zaručuje trvanlivost písma.
- administrativní pomůcky se ukládají tak, aby byla zajištěna jejich ochrana proti ztrátě nebo zneužití.
- jednací protokoly, pomocné jednací protokoly a doručovací knihy je možno vyřadit až když byly vyřazeny veškeré utajované dokumenty v nich zaznamenané nebo evidované.

2.6 Fyzická bezpečnost

Fyzická bezpečnost řeší ochranu objektů, kde utajované informace vznikají nebo jsou uchovány. Fyzická bezpečnost je celek opatření (ostraha, režimová opatření a technické prostředky). Musí být uvedeny prostředky, jaké budou k ochraně použity, dále rozsah, způsob a podmínky, při kterých budou použity. Organizace se musí rozhodnout, v kolika objektech bude zpracovávat a uchovávat utajované informace a jakým způsobem budou objekty zabezpečeny. Zda-li budou použity jen mechanické prostředky nebo elektronický zabezpečovací systém. Jestli také bude využito soukromé bezpečnostní služby nebo bude fyzická ostraha prováděna vlastními pracovníky. Popsané náležitosti pak organizace zpracuje do bezpečnostního projektu. Výběr a způsob použití prostředků ochrany utajovaných informací není libovolně na organizaci, ale musí se řídit vyhláškami NBÚ a splňovat určité minimální požadavky k ochraně vůči stupni utajení.

Cílem fyzické bezpečnosti utajovaných informací je stanovit opatření a pravidla, aby nedošlo k neoprávněnému nakládání s utajovanými informacemi. Bezpečnostní politika fyzické bezpečnosti stanovuje zásady, pravidla a opatření ve smyslu režimového opatření, technického zabezpečení nebo fyzické ostrahy. Fyzická bezpečnosti utajovaných informací vyžaduje několik základních otázek, od kterých se bude např. odvíjet výběr a způsob nasazení konkrétních technických prostředků. Provede se rozhodnutí, kde v organizaci a na jakých místech se utajované informace budou vyskytovat. Výsledkem rozhodnutí pak musí být přesné vymezení objektu a jeho zařazení do odpovídající kategorie, určení zabezpečené oblasti a její zařazení do odpovídající třídy a kategorie. Zákon č. 412/2005 Sb. v § 24 definuje pojmy objekt, zabezpečená oblast a jednací oblast.

Další postup spojený s fyzickou bezpečností vyžaduje volbu účinných opatření k ochraně objektů, ve kterých se vyskytují utajované informace. Bezpečnostní opatření jsou ostraha, režimová opatření a technické prostředky.

Základní principy fyzické bezpečnosti:

- pověření konkrétní osoby řízením odvětví ochrany utajovaných informací.
- jednoznačné rozdělení úloh jednotlivých osob v oblasti fyzické bezpečnosti.
- dodržovat požadavky předpisů na dokumentaci fyzické bezpečnosti a požadavky vnitřních předpisů firmy.
- zajistit systém vzdělávání a školení určených osob a ostatních zaměstnanců v oblasti fyzické bezpečnosti.
- nakládat s utajovanými informacemi v zabezpečené oblasti smí pouze určená osoba.
- postupovat v souladu s režimovými opatřeními a utajované informace zabezpečit předepsaným způsobem.
- zavedení klíčového režimu, který se týká objektu a zabezpečené oblasti.
- využití kombinace opatření fyzické bezpečnosti (ostraha, režimová opatření, technické prostředky) s ohledem na stupeň utajení a musí být realizována s ohledem na ekonomické, personální a technické možnosti organizace.
- bezpečnostní opatření musí být přijatelné pro zaměstnance společnosti, neměla by zvyšovat jejich pracovní zatížení.
- použité technické prostředky budou certifikovány NBÚ.
- odborné zajištění fyzické bezpečnosti.

2.7 Bezpečnost informačních systémů

Informačním technologiím, informačním systémům a jejich bezpečnosti je dnes věnována velká pozornost. Informace dnes představují v politickém a obchodním světě hodnotu, jež se stala zbožím a faktorem, který rozhoduje o úspěšnosti. Bezpečnost IS nelze řešit izolovaně, musí být součástí celkové bezpečnostní politiky organizace. Obecně lze říci, že každý IS je zranitelný, bezpečnostní politika pouze snižuje rizika útoku na informační systém.

Zákon č. 412/2005 Sb. v § 34 ukládá povinnost používat pro nakládání s utajovanými informacemi informační systémy certifikované NBÚ a písemně schválené odpovědnou osobou. Schválení IS musí odpovědná osoba písemně oznámit NBÚ do 30 dnů od datumu schválení. Požadavky na IS a podmínky jeho provozování 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 stínících komor. Certifikaci IS provádí Odbor informačních technologií NBÚ.

Bezpečnost IS řeší otázky s utajovanými informacemi v informačních systémech organizace pomocí bezpečného předání prostřednictvím informačních systémů. Utajované informace v IS musí být chráněny, aby:

a) k nim měly přístup pouze oprávněné osoby,

b) šlo vždy zjistit a zkontrolovat, kdo tyto utajované informace vytvořil, změnil nebo odstranil,

c) nemohly být náhodně vyzrazeny,

d) byly dostupné v době, kdy oprávněné osoby potřebují.

Podle odstavce 1 § 34 zákona č. 412/2005 Sb. je: „Informačním systémem nakládajícím s utajovanými informacemi se pro tyto účely tohoto zákona rozumí jeden nebo více počítačů, jejich programové vybavení, k tomu patřící periferní zařízení, správa tohoto informačního systému a k tomuto systému se vztahující procesy nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací.“

Oblast informačních systémů v organizaci vyžaduje speciální odborné znalosti, bez kterých není možné vypracovat příslušný projekt a následně realizovat. V popsané oblasti mají výhodu velké organizace s vybudovaným IS a odborným personálem. Ostatní organizace svěří vypracování dokumentace a realizaci opatření dodavateli s odbornými zkušenostmi. IS musí být certifikován NBÚ a písemně schválený do provozu odpovědnou osobou. Zabezpečení některých bezpečnostních funkcí informačního systému prvky počítačové bezpečnosti lze nahradit zvýšeným použitím prostředků personální bezpečnosti, administrativní bezpečnosti nebo organizačních opatření. Při nahrazování prostředků náhradním bezpečnostním mechanismem musí být plně zachována kvalita a úroveň bezpečnosti.

2.7.1 Bezpečnost v prostředí počítačových sítí

Při přenosu komunikačním kanálem musí být zajištěna ochrana důvěrnosti a integrity utajované informace. Hlavním a základním prostředkem pro zajištění důvěrnosti utajované informace při přenosu je kryptografická ochrana. Prostředkem pro zajištění integrity utajované informace při přenosu je spolehlivá detekce záměrné i náhodné změny utajované informace. Důvěrnost je utajení informace před neoprávněným přístupem. V praktickém použití bývá důvěrnost realizována prostřednictvím výběrového řízení přístupu a povinného řízení přístupu. Řízení přístupu představuje několik mechanismů a kontrol určených k zajištění pouze dovoleného přístupu v IS. Integrita představuje celistvost systému, články systému mohou být upraveny jen autorizovanou osobou.V rámci integrity musí být zachována shoda systému s reálným stavem.

Pro počítačovou síť v rámci objektu nebo zabezpečené oblasti postačuje fyzická ochrana všech komponentů komunikačního kanálu. Vzhledem ke komunikačnímu prostředí se zajišťuje identifikace a autentizace komunikujících stran, včetně ochrany identifikační a autentizační informace. Připojení sítě musí být zabezpečeno vhodným bezpečnostním rozhraním, aby bylo zamezeno průniku do informačního systému.

Realizaci zabezpečení počítačových sítí musí provádět odborníci z oblasti informačních systémů. Existuje řada spolehlivých algoritmů a programů, ale odborníci právě musí zajistit jejich správnou instalaci a používání.

2.7.2 Bezpečnostní požadavky

Ochrana utajovaných informací není jen otázkou zpracování koncepce bezpečnostní politiky a bezpečnostního projektu za účelem vykonání úspěšné bezpečnostní prověrky a získání osvědčení. Během práce s utajovanými informacemi jsou vyžadovány určité bezpečnostní požadavky. Bezpečnostní opatření v oblasti utajovaných informací musí být pravidelně kontrolovány, aby byla funkčnost zajištěna alespoň na minimální bezpečnostní požadavky.

Požadavky na ochranu mobilních a přenosných informačních systémů:

- informační systémy, které nejsou pevně na svém místě v objektu nebo v zabezpečené oblasti, jsou vystaveny většímu riziku.

- v analýze rizik se posuzují rizika mobilních informačních systémů spojená s dopravním prostředkem, ve kterém se budou informační systémy používat, a přenosných informačních systémů s prostředími, ve kterých se budou používat.
- v praxi zabezpečení mobilního nebo přenosného IS představuje větší problém, protože možnost využití prostředků objektové a fyzické bezpečnosti je omezena vzhledem k nepřenosnému IS . Využívá se více prostředků z oblasti kryptografie a informační technologie, jedná se však o vyšší ekonomické náklady na zabezpečení.
- organizace musí pečlivě zvážit, zda je používaní mobilních IS nezbytně nutné pro zpracovávání utajovaných informací.

Požadavky na ochranu proti kompromitujícímu elektromagnetickému vyzařování:

- odposlech lze chápat jako neautorizovaný vstup do IS. V dnešní době má odposlech mnoho podob, nejnebezpečnější způsob je s využitím kompromitujícího elektromagnetického vyzařování.
- informační systém nakládající s utajovanými informacemi stupně utajení „Důvěrné“ nebo stupně vyššího musí být zabezpečen proti kompromitujícímu elektromagnetickému vyzařování.
- úroveň zabezpečení závisí na stupni utajení a je dána bezpečnostními standardy.
- zabezpečení proti odposlechu znamená použití speciálních technických prostředků určených k boji proti odposlechu. Režimová opatření, která zabrání umístění odposlechových prostředků v blízkosti IS.

Požadavky na bezpečnost nosičů utajovaných informací:

- veškeré nosiče, na kterých jsou utajované informace a používají se v provozu informačního systému, musí být patřičně evidovány.
- vyměnitelný nosič určený informačnímu systému se vyznačuje stupněm utajení, názvem daného informačního systému a evidenčním číslem nosiče.
- nosiče zabudované do zařízení umožňujících uchování utajovaných informací musí být evidovány a označeny odpovídajícím stupněm utajení nejpozději po jejich vyjmutí ze zařízení.

- na nosiči, na kterém jsou utajované informace stupně „Přísně tajné“, nesmí být snížen stupeň utajení nosiče. Mimo případu, kdy je prokázáno, že během celé existence nosiče na něm byly uloženy jen utajované informace nižšího stupně.
- stupeň utajení „Tajné“ a „Důvěrné“ může být snížen, stupeň utajení „Vyhrazené“ může být zrušen. Popsané snížení nebo zrušení může proběhnout vymazáním utajovaných informací z nosiče, nebo v případě, že bylo prokázáno, že na nosiči během jeho existence byly uloženy jen utajované informace nižšího stupně nebo informace neutajované. Po vymazání nesmí být možné získat žádné zbytkové utajované informace. Postup bývá uveden v provozní bezpečnostní dokumentaci certifikovaného informačního systému. Výše popsané postupy jsou velmi důležitá záležitost a měla by jim být věnována maximální pozornost.
- nosič utajované informace musí být zničen tak, aby z něho nebylo možné utajovanou informaci získat zpět.

Požadavky na bezpečnost provozovaného informačního systému:

- bezpečnost informačního systému musí být pravidelně kontrolována a vyhodnocována.
- softwarové a hardwarové vybavení informačního systému musí odpovídat bezpečnostní dokumentaci.
- pravidelně provádět zálohování programového vybavení a utajovaných informací. Uložení zálohy, u které nemůže dojít k poškození při ohrožení IS.
- při servisní činnosti musí být vytvořena opatření, aby nebyla ohrožena bezpečnost informačního systému. Z nosičů utajovaných informací, které jsou přístupné při servisní činnosti, musí být vymazány utajované informace. Musí také být zabezpečen dálkový přístup k utajované informaci před zneužitím.
- u komponentů informačního systému, které zajišťují bezpečnostní funkce nebo ovlivňují bezpečnost informačního systému, provádí údržbu osoby, které splňují podmínky zákona pro přístup k utajovaným informacím.
- v bezpečnostní dokumentaci informačního systému musí být stanovena opatření pro řešení krizové situace, základní typy krizových situací.

2.7.3 Ochrana proti vzdálenému a lokálnímu přístupu

V informačních systémech je ochrana proti vzdálenému přístupu realizována pomocí firewallů. Firewall je síťové zařízení k řízení a zabezpečení síťového provozu. Firewall kontroluje komunikaci mezi sítěmi a dokáže filtrovat síťový provoz, čímž zabraňuje napadení počítačového sytému.

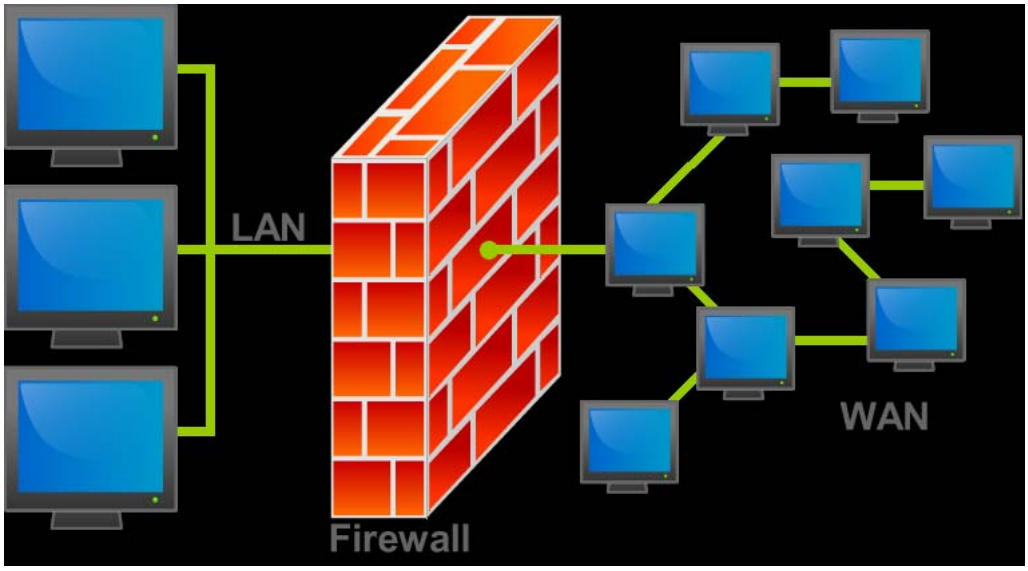
Základní typy firewallů:

a) Paketový firewall: Nejjednodušší a nejstarší typ firewallu. Určitá pravidla přesně uvádí, ze které adresy a portu může být doručen paket[29], a na jakou adresu a port bude doručen. Kontrola probíhá na třetí a čtvrté vrstvě modelu síťové komunikace. Zástupce paketového filtru je ACL[30].

b) Aplikační brány: Komunikace přes aplikační bránu se děje ve dvou spojeních. Princip činnosti spočívá, v tom že klient se připojí na aplikační bránu, která spojení zpracuje a klientovi otevře nové spojení k serveru, poté se klientem stala aplikační brána. Zástupce v aplikačních branách je např. The Firewall Toolkit.

Další typy firewallů jsou stavové paketové firewally a stavové paketové firewally s kontrolou protokolů.

[29] Paket – blok přenášený počítačovou sítí.
[30] ACL – Access Control Lists.



Obr. 10. Firewall hlídající provoz.

[zdroj obrázku uveden v použité literatuře, zdroj číslo [6]]

Ochrana proti neoprávněnému lokálnímu (místnímu) přístupu:

a) Ochrana Biosu[31] heslem: Při vniknutí do Case paměti (paměť na základní desce, ve které jsou uloženy informace o aktuálním čase, datumu a přístupová hesla) je heslo neúčinné, heslo lze resetovat odpojením baterie. Použije-li se heslo Biosu s kombinací fyzické ochrany např. zaplombování vstupu do skříně počítače, tak je bezpečné.

b) Heslo do operačního systému: U operačního systému Windows se vyžaduje heslo delší než 14 znaků za použití malých a velkých písmen, číslic a speciálních znaků. Při dodržení těchto požadavků se bude jednat o bezpečné heslo. V případě kratšího hesla než 14 znaků lze heslo poměrně snadno rozluštit. U systémů, které pracují s utajovanými informacemi, se v žádném případě nedoporučuje používat hesla, jako jsou: své jméno nebo příjmení, jméno svého psa nebo přítelkyně a další. Tyto typy hesel se dají snadno zjistit a útočníka napadne nejdřív vyzkoušet právě taková hesla.

[31] Bios – Basic Input-Output System, implementuje základní vstupně – výstupní funkce.

c) Tokeny: Na první pohled se podobají klasickým Flash diskům. Tokeny jsou upraveny pro záznam identifikačních klíčů, které ověřují identitu. Ochranu identity zajišťuje osobní heslo, které musí být samozřejmě sestaveno podle výše zmíněných kritérií. Nevýhody tokenů jsou především malá podpora systémů a fakt, že při ztrátě tokenu bez hesla se dá do systému proniknout.

d) Čipové karty: Ověřují identitu uživatele formou identifikačního hashe nebo ochranu pomocí bezpečného hesla. Nevýhody čipových karet jsou stejné jako u tokenů.

2.8 Bezpečnost komunikačních systémů

Bezpečnost komunikačních systémů představuje velmi důležitou oblast ochrany utajovaných informací, poptávka stále roste spolu s IS a informační technologií. Spolu s technickými prostředky musí být IS používané k práci s utajovanými informacemi povinně certifikovány NBÚ nebo jím pověřenou organizací. Pro komunikační systém nakládající s utajovanými informacemi je nutné zpracovat projekt bezpečnosti komunikačního systému. Komunikační systém definuje zákon č. 412/2005 Sb. § 35 odstavce 1.

Žádost o schválení projektu bezpečnosti komunikačního systému obsahuje:

a) „identifikaci žadatele,

b) jméno a příjmení kontaktního pracovníka a kontaktní spojení,

c) stupeň a číslo osvědčení podnikatele pro seznamování se s utajovanými informacemi, je-li žadatelem podnikatel,

d) název a stručný popis účelu a rozsahu komunikačního systému včetně stanovení jeho běžných provozních funkcí,

e) stupeň utajení utajovaných informací, se kterými bude komunikační systém nakládat a

f) identifikaci dodavatele jednotlivých komponent komunikačního systému majících vliv na bezpečnost komunikačního systému.“[32]

Schválení projektu se provádí posouzením předložených podkladů a kontrolou realizace projektu NBÚ. Kontrola se provádí v provozním prostředí schvalovaného komunikačního systému. Schválení projektu bezpečnosti komunikačního systému bývá následně písemně zasláno žadateli.

Komunikační systémy spolu s informačními systémy jsou nejrizikovější oblastí bezpečnostní politiky utajovaných informací. Často můžeme slyšet, že se někdo dostal do systému a následně zneužil citlivá data.

2.9 Kryptografická ochrana

Používání kryptografických prostředků je složité a vyžaduje odbornost. I přes tyto požadavky je používání kryptografických prostředků nutností občanů a organizací. Obrovské množství informací se přenáší po sítích a vyžaduje zajištění jejich ochrany. Jejich bezpečnost se pak provádí zejména prostředky kryptografické ochrany. Z toho vyplývá, že každý IS, který nakládá s utajovanými informacemi a využívá k přenosu utajovaných informací komunikační kanály, musí také využít prostředky kryptografické ochrany.

Problematiku kryptografie při ochraně utajovaných informací upravuje vyhláška č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací, a vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací. Vyhlášky se zabývají způsoby použití, nasazování a evidencí kryptografických prostředků, používáním klíčových materiálů a certifikací. Kryptografickou ochranu má na starosti odbor informačních technologií NBÚ.

---

[32] Národní bezpečnostní úřad [online]. 2007- , 16.1.2009 [cit. 2009-02-25]. Dostupný z WWW: <http://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-komunikacnich-systemu/projekt-bezpecnosti-postup-hodnoceni/>.

Bezpečnostní politika kryptografické ochrany určuje organizaci postupy a pravidla při ochraně utajovaných informací prostřednictvím kryptografie. Kryptografie je především využívána při práci s IS a při komunikaci prostřednictvím počítačových sítí. Lze používat pouze kryptografické prostředky, které jsou certifikovány NBÚ nebo pověřenou organizací. Kryptografická ochrana utajovaných informací představuje systém opatření pomocí kryptografických metod při zpracování, přenosu, ukládání a archivaci utajovaných informací. Jedná se o vysoce odbornou činnost, zákon č. 412/2005 Sb. přímo ke kryptografické ochraně určuje odborně způsobilé pracovníky a kryptografické prostředky certifikované NBÚ.

2.9.1 Hashovací funkce

Hashovací funkce je funkce, u které je libovolně velkému vstupu přiřazen výstup stanovené délky. Funkce musí být jednosměrná, to znamená, že z Hash funkce nesmí být možné odvodit původní zprávu. Požadujeme také bezkoliznost, což znamená, že nesmí být možné dostat dvě různé výchozí zprávy stejnou Hash funkcí. Pro potřeby kryptografie musí být funkce hashování jednosměrná.

V současné době, kdy vývoj kryptoanalýzy hashovacích funkcí je velmi rychlý a tyto funkce se uplatňují v bezpečnostních aplikacích, vydal NBÚ doporučení:

1) „Doporučuje se nadále nepoužívat hashovací funkce s výstupem menším než 160 bitů (např. hashovací funkce MD4, MD5, RIPEMD, HAVAL-128 atd.).
2) Doporučuje se neprodleně zahájit přípravu k přechodu od hashovaní funkce SHA-1 na novou generaci hashovacích funkcí třídy SHA-2 (SHA-224, SHA-256, SHA-384 a SHS-512).
3) Doporučuje se prozkoumat všechny bezpečnostní aplikace i kryptografické prostředky, ve kterých se využívá hashovacích funkcí, a odborně posoudit vliv nejnovějších kryptoanalytických útoků na jejich bezpečnost.“[33]

[33] Národní bezpečnostní úřad [online]. 2007- , 16.1.2009 [cit. 2009-03-05]. Dostupný z WWW: <http://www.nbu.cz/cs/ochrana-utajovanych-informaci/kryptograficka-ochrana/informace/>.

2.9.2 Zvláštní odborná způsobilost

U pracovníka kryptografické ochrany je vyžadována zvláštní odborná způsobilost podle zákona č. 412/2005 Sb. § 39. Pracovník také musí splňovat požadavky zákona č. 412/2005 Sb. § 38. Zvláštní odborná způsobilost obsahuje znalosti právních nařízení, provozních nařízení a bezpečnostních standardů v kryptografické ochraně utajovaných informací. Pracovník kryptografické ochrany musí být držitelem platného osvědčení fyzické osoby, to znamená minimálně pro stupeň utajení „Důvěrné“. Zvláštní odborná způsobilost se ověřuje zkouškou, která zahrnuje teoretické a praktické znalosti. Na základě úspěšně vykonané zkoušky vydá NBÚ nebo pověřený orgán osvědčení o zvláštní odborné způsobilosti na dobu 5ti let.

2.9.3 Označení a evidence kryptografického materiálu

Kryptografický materiál se ve většině případů označuje slovem „KRYPTO“, evidenčním číslem nebo jednacím číslem a stupněm utajení.

V případě kryptografického prostředku se nápis „KRYPTO“ a evidenční číslo vyznačí na popisný štítek kryptografického prostředku nebo přímo na kryptografický prostředek. Na popisný štítek se jiné údaje neuvádí.

Klíčový materiál se také značí slovem „KRYPTO“ a stupněm utajení. Jako evidenční číslo slouží evidenční označení materiálu stanovené výrobcem klíčového materiálu.

V případě kryptografické písemnosti v listinné podobě je nutné také písemnost označit slovem „KRYPTO“, a to v horní a dolní části na každé straně písemnosti. Vedle označení „KRYPTO“ se uvede stupeň utajení a evidenční číslo, popřípadě číslo jednací. Jedná-li se o kryptografickou písemnost v nelistinné podobě, tak se označení „KRYPTO“, evidenční číslo a stupeň utajení uvede na popisný štítek nebo přímo na kryptografickou písemnost.

Pracovník kryptografické ochrany, pověřený odpovědnou osobou, provádí v administrativních pomůckách evidenci kryptografického materiálu, pracovníků kryptografické ochrany, provozní obsluhy a kurýrů. Osoba, která kryptografickou písemnost vytváří nebo jí byla přidělena k vyřízení, musí kryptografickou písemnost zaznamenat v manipulační knize. Záznam je nutné provést ihned po přijetí kryptografické písemnosti.

Na konci kalendářního roku se jednací protokol uzavírá, poslední zápis se podtrhne, tím skončí přidělování čísel jednacích v tomto roce. Uvede se záznam o počtu použitých čísel jednacích, podpis pověřené osoby a její přímý nadřízený.

2.9.4 Manipulace s kryptografickým materiálem

Manipulace s kryptografickým materiálem představuje ukládání, přepravu, předávání a další činnosti spojené s kryptografickým materiálem. S kryptografickým materiálem se musí manipulovat tak, aby byla zajištěna ochrana kryptografického materiálu a splněny požadavky, které stanoví vyhláška č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací. Postupy manipulace s kryptografickým materiálem v organizaci by se měly dodržovat, protože jinak bezpečnostní politika ztrácí na významu.

Druhy manipulace s kryptografickým materiálem:

a) Předávání kryptografického materiálu:

   V rámci orgánu státu, právnické osoby nebo podnikající fyzické osoby se předání kryptografického prostředku eviduje na evidenční kartě kryptografického materiálu. Podpisy potvrzují převzetí kryptografického materiálu.

b) Odesílání kryptografického materiálu:

   Kryptografický prostředek se odesílá v obalu, který jde uzamknout. Přepravní obal se označí nápisem „KRYPTO“ a evidenčním označením kryptografického prostředku.

   Klíčový materiál se odesílá ve dvou obalech. V levé horní části vnitřního obalu se uvede odesílatel. V pravé horní části se uvede stupeň utajení a označení „KRYPTO“. Ještě v dolní části obalu se uvede název a úplná adresa adresáta. Obal musí být dostatečně kvalitní, aby neumožňoval získat informace o tom co je uvnitř. Nemělo by se jednat o průhlednou fólii nebo sáček. Vnější obal je přenosná schránka, která musí být zajištěna proti neoprávněné manipulaci. To znamená, že je zajištěna zámkem nebo plombou. Přenosná schránka musí být opatřena názvem, adresou orgánu státu, právnické osoby nebo podnikající fyzické osoby a dále

nápisem: „V případě nálezu neotvírejte a předejte neprodleně útvaru Policie ČR nebo Národnímu bezpečnostnímu úřadu!“[34]

Kryptografická písemnost se odesílá ve dvou obálkách. V levém horním rohu na vnitřní obálce se napíše odesílatel, číslo kryptografické písemnosti. V pravém horním rohu obálky se uvede stupeň utajení a označení „KRYPTO“. V dolní části název a úplná adresa adresáta. Kvalita obálky musí být taková, aby údaje uvnitř obálky nebyly čitelné. Nesmí se jednat o obálku, z které by proti světlu šel vyčíst obsah, obálky musí také být spolehlivě zalepeny.

c) Elektronický přenos kryptografického materiálu:

Jedná se o přenos kryptografické písemnosti elektronickou cestou telekomunikačními sítěmi.

Odesílateli elektronického přenosu se kryptografická písemnost vydá na základě podpisu. Odesílatel zaznamená kryptografickou písemnost v manipulační knize nebo v pomocném jednacím protokolu. Dále se v pomocném jednacím protokolu uvede způsob provedení elektronického přenosu, jméno a příjmení odesílatele.

Příjemce zaznamená přijetí kryptografické písemnosti do manipulační knihy nebo do pomocného jednacího protokolu a předá na základě podpisu pověřené osobě k zaevidování.

d) Příjem kryptografického materiálu:

Převzetí kryptografické zásilky pověřenou osobou se doručiteli potvrdí podpisem. Dále musí být uvedeno jméno a příjmení pověřené osoby, která zásilku přijímá, datum přijetí a razítko orgánu státu, právnické osoby nebo podnikající fyzické osoby. Objeví-li pověřená osoba u doručené zásilky zřetelné poškození obalu nebo nějakou podobnou závadu, informuje o tom odesílatele.

Při poškození je nutné sepsat záznam o poškození kryptografické zásilky, jehož vzor stanovuje vyhláška č. 524/2005 Sb. v příloze č. 5.

---

[34] z § 28 vyhlášky č. 524/l2005 Sb., O zajištění kryptografické ochrany utajovaných informací.

e) Přeprava kryptografické zásilky:

Kryptografické zásilky se nesmí přepravovat veřejnými dopravními prostředky. Výjimkou je letecká a námořní přeprava. Přepravu kryptografického materiálu stupně utajení „Důvěrné“ nebo vyšší stupeň provádí kurýr kryptografického materiálu. Zaškolení kurýra zajišťuje bezpečnostní správce kryptografické ochrany. Během přepravy nesmí dojít k neoprávněné manipulaci s obsahem kryptografické zásilky. To znamená její otevření a následné uzavření a podobné neoprávněné manipulace. Ke kryptografické zásilce, která obsahuje kryptografický prostředek nebo klíčový materiál, se vystavuje průvodní list kryptografické zásilky. Vzor průvodního listu je stanoven v příloze č. 6 vyhlášky č. 524/2005 Sb.

f) Přenášení kryptografického materiálu:

Kryptografický materiál se přenáší v zalepené obálce nebo v uzavřeném obalu. Na obalu a obálce musí být uvedeno označení orgánu státu, právnické osoby nebo podnikající fyzické osoby. Dále vyznačen stupeň utajení a označení „KRYPTO“.

Kryptografický materiál stupně utajení „Důvěrné“ a „Vyhrazené“ je možné přenášet pouze s povolením nadřízené osoby. Přenášení kryptografického materiálu stupně utajení „Tajné“ se děje pouze s písemným souhlasem nadřízené osoby a stupně „Přísně tajné“ pouze s písemným souhlasem odpovědné osoby.

Kryptografický materiál přenáší pracovník kryptografické ochrany. Když se přenáší kryptografický materiál stupně „Důvěrné“, „Tajné“ a „Přísně tajné“ musí být pracovník kryptografické ochrany doprovázen nejméně jednou osobou. Osoba doprovázející kryptografického pracovníka musí být k doprovodu pověřena odpovědnou osobou nebo osobou jí pověřenou. Pracovník kryptografické ochrany náležitě proškolí doprovázející osobu.

g) Ukládání kryptografického materiálu:

Kryptografické materiály se ukládají do všech druhů trezorů a uzamykatelných kovových skříní, které splňují požadavky zvláštního právního předpisu.

Po vyřízení se kryptografická písemnost vrací pověřené osobě k uložení. Osoba, která vyřizuje kryptografickou písemnost, uvede před uložením skartační znak a rok, ve kterém bude provedeno skartační řízení.

„Vyřízené kryptografické písemnosti se ukládají odděleně od ostatních utajovaných písemností u pověřené osoby posloupně podle čísel jednacích písemností nebo podle problematik do spisových svazků. Na spisovém svazku s uloženými kryptografickými písemnosti se vyznačí takový stupeň utajení, který má kryptografická písemnost nejvyššího stupně utajení v něm uložená. Kryptografické písemnosti ukládané do spisovného svazku se průběžně zapisují do seznamu uložených písemností, který je jeho součástí.“[35]

h) Zapůjčení kryptografické písemnosti:

Kryptografickou písemnost lze zapůjčit se souhlasem odpovědné osoby orgánu státu, právnické osoby, podnikající fyzické osoby nebo pověřeného pracovníka kryptografické ochrany. Pověřená osoba zaznamená zapůjčení kryptografické písemnosti do zápůjční knihy. Po uplynutí každých 6ti kalendářních měsíců od zapůjčení se kryptografické písemnosti předkládají pověřené osobě, aby provedla fyzickou kontrolu.

i) Vývoz kryptografického prostředku:

Podmínkou pro vývoz kryptografického prostředku z území ČR je, aby byl kryptografický prostředek certifikovaný a vývoz povolil příslušný úřad. Používání certifikovaného kryptografického prostředku orgánem státu mimo území ČR se nepovažuje za vývoz. Povolení vývozu lze udělit na základě podání písemné žádosti.

Výše popsané manipulace s kryptografickým prostředkem, kryptografickým materiálem nebo kryptografickou písemností vyžadují znalosti zákona č. 412/2005 Sb. a příslušných vyhlášek. Veškerá manipulace se nesmí nijak podcenit a musí se postupovat podle právních předpisů. Jakékoliv zjednodušování nebo měnění postupů je nepřípustné.

2.9.5 Výkon kryptografické ochrany

Výkon kryptografické ochrany upravuje § 38 zákona č. 412/2005 Sb. Výkon kryptografické ochrany se rozumí bezpečnostní správa kryptografické ochrany, speciální

[35] § 27, odstavec 3, vyhlášky číslo 524/2005 Sb. , O zajištění kryptografické ochrany utajovaných informací.

obsluha kryptografického prostředku a výroba klíčového materiálu. Výkon kryptografické ochrany provádí pracovník kryptografické ochrany.

Bezpečnostní správou kryptografické ochrany je organizační opatření personální, administrativní a fyzické bezpečnosti, bezpečnosti informačních a komunikačních systémů a kryptografické ochrany. Plnění bezpečnostní správy se zajišťuje dodržením minimálních bezpečnostních požadavků určujících nejnižší dovolenou úroveň bezpečného provozování kryptografických prostředků.

Bezpečnostní správu kryptografické ochrany vykonává:

a) bezpečnostní správce kryptografické ochrany – odpovídá za celé zajištění a bezpečné provádění kryptografické ochrany, zpracovává bezpečnostní dokumentaci kryptografické ochrany, dále zajišťuje zaškolení k provozní obsluze kryptografického prostředku.

b) správce kryptografického materiálu – odpovídá za bezpečné ukládání a evidenci kryptografického materiálu.

c) pracovník kryptografické ochrany – manipuluje s písemnostmi kryptografické ochrany, provádí instalaci kryptografického prostředku, nastavení a používání kryptografických klíčů, zajištění provozu a servisu kryptografického prostředku.

Rozsah činností a oprávnění pracovníka kryptografické ochrany a dalších osob, které zajišťují provoz kryptografického prostředku, se stanoví v provozní dokumentaci. Obsah provozní dokumentace je upraven v bezpečnostním standardu.

V provozní dokumentaci a bezpečnostních standardech se stanoví způsob a podmínky výroby, manipulace a ničení klíčových materiálů. Výroba klíčových materiálů musí být prováděna na kryptografickém pracovišti určeném k výrobě klíčového materiálu. Výrobu provádí pracovník kryptografické ochrany, který musí být držitelem platného osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. V osvědčení je uvedeno oprávnění k výrobě klíčových materiálů.

2.9.6 Kompromitující elektromagnetické vyzařování

Jedná se o elektromagnetické vyzařování, které může způsobit únik utajovaných informací stupně utajení „Důvěrné“, „Tajné“ nebo „Přísně tajné“. U stupně utajení „Vyhrazené“ není

požadováno žádné opatření z hlediska kompromitujícího vyzařování, požaduje se jen „Prohlášení o shodě“.

Při práci s utajovanými informacemi stupně utajení „Důvěrné“ se přihlíží k charakteru organizace, způsobu zpracování informací a rozsahu zpracování utajovaných informací stupně utajení „Důvěrné“. Rizika z oblasti kompromitujícího vyzařování jsou především způsobena zobrazováním utajovaných informací na monitoru, jejich vkládáním klávesnicí, tiskem a při ukládání na zálohovací média. Týká-li se takové zpracování utajovaných informací krizového plánování, zabezpečení důležitých objektů, vojenského a jaderného materiálu a dalších kritických oblastí, je nutné aplikovat přísnější požadavky.

Při zpracování utajovaných informací stupně utajení „Důvěrné“, „Tajné“ nebo „Přísně tajné“ se vyžaduje napájení ze síťového přívodu, který musí být vybaven vysokofrekvenčním filtrem. Potom u stupně utajení „Důvěrné“ lze použít libovolný typ, schválený ČSN a s útlumem minimálně 20dB v kmitočtovém pásmu 100 Khz – 30 Mhz. U stupně utajení „Tajné“ a „Přísně tajné“ se vyžaduje konzultace s oborem informačních technologií NBÚ.

U komponentů, které obsahují paměti typu RAM[36], je nutné vědět, že informace v paměti zůstávají i po odpojení napájecího napětí. Při provádění servisu nebo při nekontrolovatelné manipulaci s těmito komponenty je nutné obsah paměti přepsat neutajovanými informacemi. Uživatel by měl také vědět o možnosti umístění operativních prostředků („štěnic“). Nejčastější způsoby aplikace jsou v servisech, uklízečky nebo opraváři, a místech např. do klávesnice nebo přímo do PC.

Poslední fáze představuje vhodné umístění IS v rámci budovy. IS by měl být co nejdále od míst, jako jsou veřejné parkoviště nebo místnosti, do kterých nemá uživatel IS běžně povolen přístup. Doporučují se místnosti s minimálním počtem oken nebo okny do dvora objektu a místnosti ve vyšších patrech budovy. V neposlední řadě je nezbytné umístění IS v místnosti, tzn. dodržet určité vzdálenosti telefonů, faxů a metalických vedení (voda,

[36] RAM – random access memory, jedná se o typ paměti, ve které je možné opakovat zápis informací.

topení, klimatizace a podobné). Na první pohled by se mohlo zdát, že jde o detaily, které organizace nebudou akceptovat. Ale i tato opatření patří do bezpečnostní politiky utajovaných informací, které by neměly být zapomínány.

2.9.7 Měření kompromitujícího elektromagnetického vyzařování

Při provádění zónových měření je nutné dodržet určitý postup, který stanovuje NBÚ. Měření by mělo být prováděno následujícím způsobem:

1) Měření kompromitujícího vyzařování se provádí na písemnou žádost (kromě měření v procesu certifikace IS).
2) Zónové měření se provádí v pořadí podle datumu přijetí žádosti o měření (pořadí žadatelů se může změnit pouze s písemným souhlasem ředitele NBÚ nebo náměstka ředitele NBÚ). Pořadí může být také změněno ekonomickými hledisky NBÚ, např. několik měření ve stejném městě za krátký časový úsek. To obnáší převážení techniky a instalaci, tudíž je výhodné měření provést v jednom místě najednou.
3) Žádost o měření musí obsahovat identifikaci žadatele, údaje kontaktní osoby (telefon a e-mail), adresu místa měření, výkres budovy a označení místnosti, kde bude měření provedeno, plán okolí měřeného objektu s vyznačením kontrolovaného místa, stupeň utajení zpracovávaných informací a u IS v procesu certifikace číslo svazku a jméno pracovníka, kterému je přidělena certifikace IS.
4) Po přijetí žádosti bude žadatel informován a případně požádán o doplnění náležitostí, které jsou chybné nebo neúplné.
5) Před prováděným měřením bude žadatel informován o datumu a přibližném času měření.
6) Výsledky měření budou zaslány maximálně za 15 pracovních dnů. Mohou být také v kopii zveřejněny pracovníkovi, kterému je na NBÚ certifikace přidělena.

2.10 Osobní šifrátory

Během minulých let se stalo oblibou používat mobilní komunikační prostředky (mobilní telefony atd.) v důsledku klesající ceny a všestranné použitelnosti. Mobilní komunikační prostředky si oblíbily všechny skupiny obyvatelstva, ať jde o soukromé nebo pracovní využití. Používaní těchto mobilních komunikačních prostředků usnadňuje a zrychluje

práci, ale také přináší vážná rizika. Hlavní riziko spočívá v poměrně snadné možnosti odposlouchávání. Existují různá odposlechová zařízení a metody, které nejsou mnohdy ve správných rukou. Účinný způsob proti odposlechu je šifrování.

Od roku 2001 používala Česká republika jediný certifikovaný výrobek pro přenos utajovaných informací (do stupně utajení „Tajné“ a „NATO Secret“). Jednalo se o mobilní GSM telefon NSK 200.

„Národní bezpečnostní úřad 19. listopadu 2008 nově certifikoval zařízení švédské společnosti Sectra Communication AB, umožňující šifrování hlasových a datových komunikací – tzv. osobní hlasový a datový šifrátor Tiger® XS. Tento produkt je určen primárně pro použití ve vládních a bezpečnostních orgánech. Sectra je první společností, která získala pro své zařízení schválení Rady Evropské unie pro mobilní, hlasové a datové šifrování utajovaných informací do stupně utajení „SECRET UE“. V červenci 2008 bylo toto zařízení ohodnoceno i v NATO agenturou SECAN jako schopné chránit utajované informace NATO do stupně utajení „NATO SECRET“.“[37]

Informace o zařízení Tiger® XS:

- moderní zařízení podobné mobilnímu telefonu a schopné spolupracovat s většinou dnešních mobilních telefonů.
- osobní hlasový a datový šifrátor, velikost 118x68x22 mm a hmotnost 130g.
- umožňuje šifrování hlasu, šifrování datových přenosů a šifrování krátkých textových zpráv.
- zařízení může pracovat v různých sítích (např. GSM[38] a ISDN[39]).
- konstrukčně jsou vyrobeny tak, aby byly schopné spolupracovat i v sítích příštích generací.

---

[37] Národní bezpečnostní úřad [online]. 2007- , 16.1.2009 [cit. 2009-02-27]. Dostupný z WWW: <http://www.nbu.cz/cs/aktuality/590-osobni-sifratory/>.

[38] GSM - **G**lobální **S**ystém pro **M**obilní komunikaci, slovo pochází z francouzštiny „**G**roupe **S**pécial **M**obile“, jedná se o nejpopulárnější standard pro mobilní telefony na světě.

[39] ISDN - z anglického termínu **I**ntegrated **S**ervices **D**igital **N**etwork, v překladu Digitální síť integrovaných služeb.

O zařízení Tiger® XS projevily zájem z ministerstva vnitra, obrany, zahraničních věcí a zpravodajské služby. Zařízení Tiger® XS využívají vládní instituce ve více než polovině zemí EU.

Ke kryptografické ochraně telefonického a datového spojení se používá kryptofax a kryptotelefon. Zařízení představují bezpečnou komunikaci, která je před spojením šifrována.

Obr. 11. Zařízení Tiger® XS.

[zdroj uveden v použité literatuře, zdroj číslo [5]]

2.10.1 Odposlechy v mobilních sítích

„Odposlechy v mobilních sítích jsou v poslední době šlágrem sledovaným médii, ale i zaměstnávající politiky, kteří jsou čas od času přesvědčeni o jejich permanentním používání. Je jasné, že odpovídající technické prostředky pro monitorování hovorů

v mobilních sítích v ČR existují a jsou v majetku privátních firem, často ani neregistrovaných v asociacích bezpečnostních služeb.“[40]

Mobilní sítě mohou být odposlouchávány monitorováním provozu operátora nebo ve vzduchu. V dnešní době proti odposlechu existují poměrně kvalitní prostředky. Ovšem pro obyčejné uživatele odposlouchávání není v dnešní době až takový problém. Může hrozit, že se špion dozví, kam půjde dotyčný večer, s kým bude trávit víkend a podobně. Pro podnikatele a firmy hrozí větší nebezpečí - odposlouchávání utajovaných informací.

2.11 Šifrovací programy

Pro zabezpečení dat se používají různé šifrovací programy, které snižují riziko odcizení dat a jejich následné dešifrování. V dnešní době je na trhu značné množství šifrovacích programů, od méně spolehlivých až po profesionální šifrovací programy. Některé jsou dokonce volně šiřitelné a zdarma. Výrobci se předhání, že právě ten jejich program je vhodný a dostatečné bezpečný pro požadavky firem. Neexistuje však jednoznačná odpověď, která by určila, který program je nejlepší. Každý program má své výhody i nevýhody, které spočívají především v kvalitě, způsobu použití a v neposlední řadě i ceně. Záleží na bezpečnostním odborníkovi, který program vybere, k jakému účelu bude sloužit a jaký stupeň informací bude chránit.

Šifrovací program TrueCrypt:

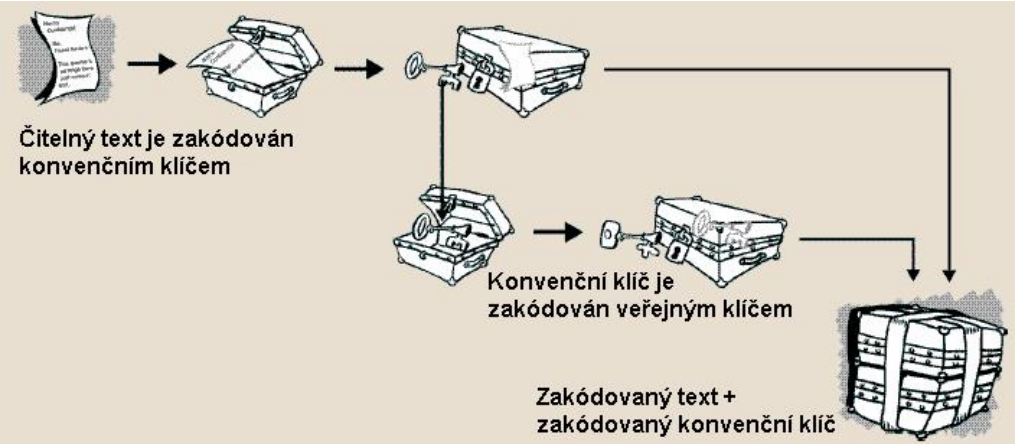
- velmi jednoduchý a kvalitní program.
- volně šiřitelný nástroj pro šifrování dat na disku, používá se v systémech Windows, Linux a Mac OS X.
- nabízí zašifrování souborů, složek i celých disků.
- využívá šifrovacích algoritmů DES, Triple DES, AES, Twofish a další.

---

[40] LAUCKÝ, Vladimír. *Speciální bezpečnostní technologie.* 1. vyd. Zlín : [s.n.], 2009. 161 s. ISBN 978-80-7318-762-0.

Šifrovací program PGP[41]:

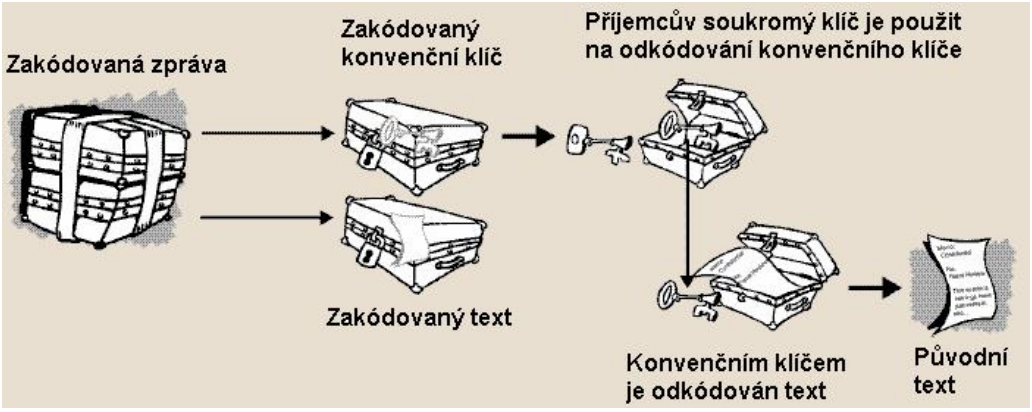
- jeden z nejznámějších a nejbezpečnějších programů, který umožňuje šifrování a podepisování. První verzi programu vydal Phil Zimmermann v roce 1991.
- založen na algoritmu RSA. Zdroje uvádí, že šifrování pomocí PGP je na úrovni šifrování armády USA.
- používá se na šifrování a dešifrování zpráv, digitální podepisování zpráv, ověřování identity odesílatele a správy klíče.



Obr. 12. Princip kódování PGP.

[zdroj uveden v použité literatuře, zdroj číslo [15]]

[41] PGP – Pretty Good Privacy, v české překladu „dost dobré soukromí“.



Obr. 13. Princip dekódování PGP.

[zdroj uveden v použité literatuře, zdroj číslo [15]]

II. PRAKTICKÁ ČÁST

3 CERTIFIKACE NBÚ

Důležitým prostředkem ochrany utajovaných informací je certifikace, upravuje ji § 46 zákona č. 412/2005 Sb. a další právní úpravy spojené s ochranou utajovaných informací. Certifikací se podle zákona rozumí postup ověřování způsobilosti technického prostředku, informačního systému, kryptografického prostředku, kryptografického pracoviště a stínící komory, za předpokladu použití k ochraně utajovaných informací. Certifikací se zjišťuje shoda výše uvedených prvků s bezpečnostními standardy. Na prostředky, které mají být certifikovány, jsou kladeny určité požadavky, které musí být splněny, aby prostředek byl certifikován. Bez průkazu kvality není výrobek brán jako plnohodnotný. Certifikace představuje důležitý ukazatel úspěšnosti výrobku.

Certifikaci provádí NBÚ nebo jím pověřené organizace. Právní rámec procesu certifikace je oprávněn upravit právním předpisem (vyhláškou) NBÚ. Právním předpisem stanoví NBÚ postupy a způsoby konkrétního certifikačního procesu a náležitosti certifikátu. V další části práce popíšu jednotlivé certifikace, náležitosti nutné k provedení správné certifikace a požadavky k získání certifikátu.

3.1 Národní bezpečnostní úřad

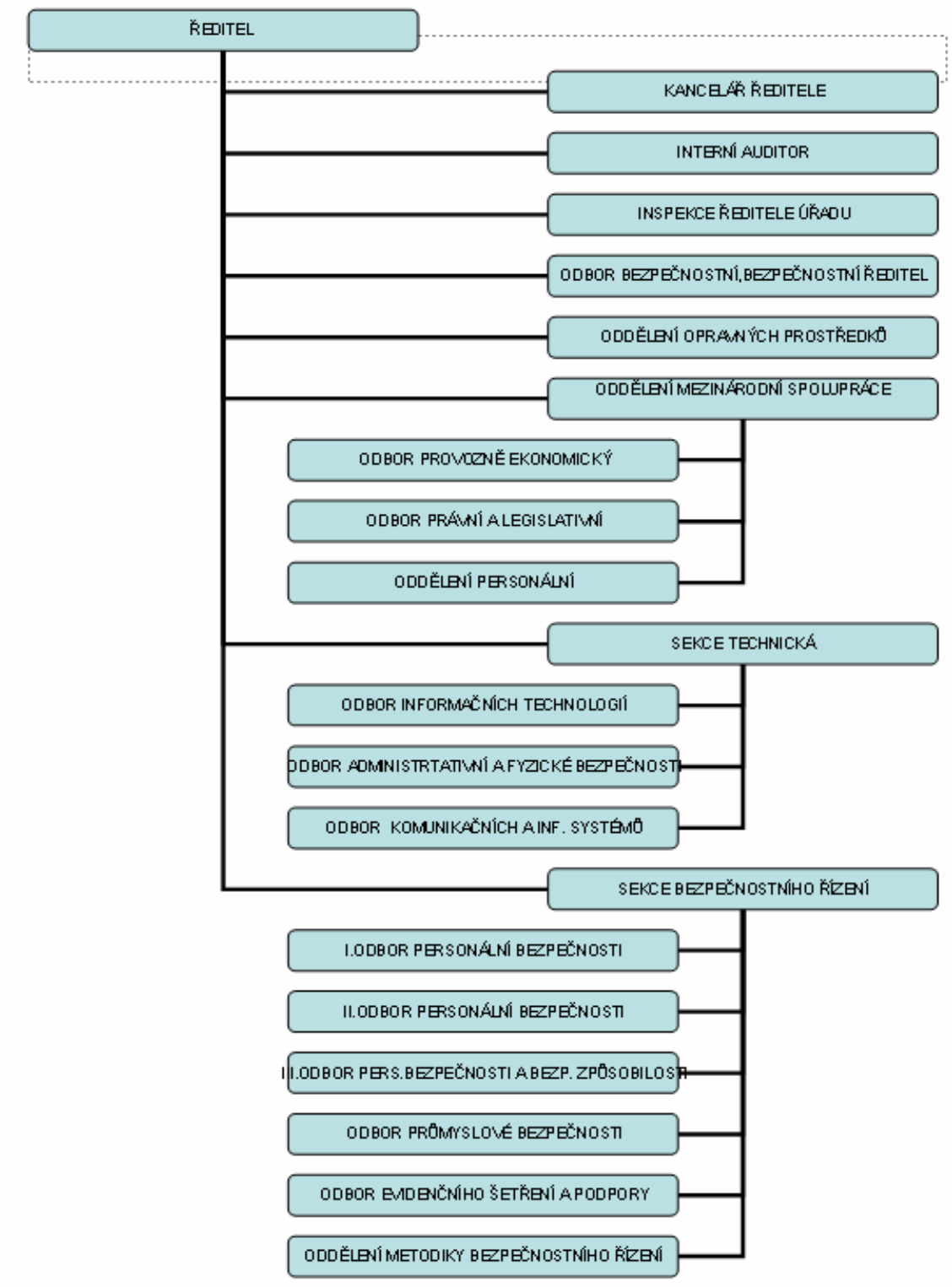
Národní bezpečnostní úřad je orgánem výkonné moci se sídlem v Praze. Plní funkci ústředního správního úřadu pro oblast obsahující ochranu utajovaných informací a bezpečnostní způsobilosti. Povinnosti NBÚ zahrnují výkon státního dozoru, metodickou činnost a zajištění postupu při ochraně utajovaných informací. Národní bezpečnostní úřad se řídí ve své činnosti zákonem č. 412/2005 Sb., O ochraně utajovaných informací a o bezpečnostní způsobilosti. Na webové adrese www.nbu.cz jsou k nahlédnutí další důležité informace, k dispozici je plné znění zákona č. 412/2005 Sb. a veškeré vyhlášky týkající se ochrany utajovaných informací. Najdete zde i Věstník Národního bezpečnostního úřadu.

Hlavní úkoly a činnosti Národního bezpečnostního úřadu:

- provádí certifikace kryptografického prostředku, kryptografického pracoviště, technického prostředku, informačního systému a stínící komory.
- má rozhodující slovo o vydání osvědčení fyzické osoby a osvědčení podnikatele, rozhoduje o vydání dokladu o bezpečnostní způsobilosti fyzické osoby a o zrušení platnosti osvědčení fyzické osoby.

- povoluje poskytování utajovaných informací v oblasti mezinárodního styku.
- vede ústřední registr a schvaluje zřízení registrů, zajišťuje výzkum, vývoj a výrobu národních kryptografických prostředků.
- plní stanovené úkoly ochrany utajovaných informací vyplývající z mezinárodních smluv, kterými je Česká republika vázána.
- za nedodržení povinností stanovených zákonem ukládá sankce, projednává přestupky, správní delikty, zpracovává znalecké posudky, odborná vyjádření v oblasti ochrany utajovaných informací.
- provádí vývoj a schvaluje národní šifrové algoritmy a utváří národní politiku kryptografické ochrany.
- zajišťuje činnost Národního střediska pro měření kompromitujícího elektromagnetického vyzařování, Národního střediska pro bezpečnost informačních systémů, Národního střediska komunikační bezpečnosti a Národního střediska pro distribuci kryptografického materiálu.
- zpracovává koncepci vzdělání svých zaměstnanců a organizačně ji zajišťuje.
- vydává Věstník, jedná se o periodickou publikaci určenou pro veřejnost a obsahuje důležité informace z oblasti ochrany utajovaných informací a bezpečnostní způsobilosti. Ve Věstníku jsou aktualizované seznamy certifikovaných technických prostředků. Věstník vychází dle potřeb NBÚ a zájmu čtenářů, nejméně však dvakrát za rok.

Národní bezpečnostní úřad je z hlediska organizace rozdělen do sekce ředitel, sekce provozně právní, sekce bezpečnostního řízení a technické sekce. Ředitele NBÚ jmenuje a také odvolává vláda. Služebně nadřízený řediteli NBÚ je předseda vlády, který též dohlíží na činnosti NBÚ. Jednotlivé sekce v sobě obsahují další odbory a oddělení. Každé oddělení má svého ředitele nebo vedoucího a úkoly, které zajišťuje a plní. Celá struktura NBÚ je vidět na obrázku na následující straně.



Obr. 14. Organizační schéma NBÚ .

[zdroj uveden v použité literatuře, zdroj číslo [12]]

3.2 Certifikace technického prostředku

Národní bezpečnostní úřad vystavuje certifikát podle § 47 zákona č. 412/2005 Sb. a dále se řídí vyhláškou č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

Výrobce, dovozce nebo distributor písemně zažádá NBÚ o certifikaci technického prostředku. Platnost certifikátu končí uplynutím doby jeho platnosti nebo rozhodnutím NBÚ o zániku platnosti certifikátu. Odebrání certifikátu NBÚ nastává v případech, kdy technický prostředek nesplňuje požadavky zákona č. 412/2005 Sb. a prováděcích právních předpisů nebo se neshoduje s posuzovaným technickým prostředkem. Při certifikaci technického prostředku se NBÚ řídí stanovenými certifikačními postupy, které vznikly s cílem sjednotit systém certifikace. Technické prostředky jsou určeny podnikatelským subjektům, které je používají k ochraně utajovaných informací. Technické prostředky musí splnit v rámci certifikace podle NBÚ požadavky certifikace. Certifikovaný prostředek potvrzuje požadovanou úroveň zabezpečení.

Žádost o certifikaci technického prostředku obsahuje:

- identifikace žadatele: název orgánu státu nebo firmy, sídlo, popřípadě jméno a příjmení odpovědné osoby a další údaje, které žádost vyžaduje. Žádosti se liší, jde-li o obchodní firmu (žadatel právnická osoba nebo fyzická osoba) nebo orgán státu.
- seznam a označení technických prostředků.
- seznam dokumentace: popis technického prostředku, prohlášení o nezávadnosti technického prostředku, certifikát shody.

Certifikát technického prostředku podle § 46 zákona č. 412/2005 Sb. obsahuje:

- „evidenční číslo certifikátu.
- název a typové označení technického prostředku,
- identifikaci výrobce technického prostředku obchodní firmou (dále jen "firma") nebo názvem, identifikačním číslem a sídlem, jde-li o právnickou osobu, nebo jménem, příjmením, rodným číslem a místem trvalého pobytu, jde-li o osobu fyzickou,
- identifikaci držitele certifikátu technického prostředku podle písmene c),
- hodnocení technického prostředku,

- datum vydání a dobu platnosti certifikátu a
- otisk úředního razítka a podpis oprávněného zástupce Úřadu[42] nebo v případě vydání tohoto certifikátu v elektronické podobě elektronický podpis oprávněného zástupce Úřadu podle zvláštního právního předpisu.“

Certifikát technického prostředku je vložen v příloze na konci práce.

Seznam certifikovaných technických prostředků:

a) „elektronická zámková zařízení a systémy pro kontrolu vstupů
b) zařízení elektrické zabezpečovací signalizace a tísňové systémy
c) zařízení fyzického ničení nosičů informací
d) mechanické zábranné prostředky
e) zařízení proti pasivnímu a aktivnímu odposlechu utajované informace
f) speciální televizní systémy
g) zařízení elektrické požární signalizace
h) zařízení sloužící k vyhledávání nebezpečných látek nebo předmětů.“[43]

NBÚ uvádí seznam certifikovaných technických prostředků na svých internetových stránkách www.nbu.cz a ve Věstníku NBÚ.

V zabezpečených oblastech kategorie „Vyhrazené“ se instalují certifikované nebo necertifikované technické prostředky. Kategorie „Důvěrné“ a vyšší vyžadují certifikované technické prostředky. Použití necertifikovaných technických prostředků je možné v případě, že nesníží požadovanou úroveň ochrany pro daný stupeň utajení.

---

[42] V zákoně č. 412/2005 Sb. se používá slovo „Úřad“, slovem je myšleno NBÚ (Národní bezpečnostní úřad).

[43] Národní bezpečnostní úřad [online]. 2007- , 16.1.2009 [cit. 2009-03-10]. Dostupný z WWW: <http://www.nbu.cz/cs/informacni-centrum/seznamy/seznam-certifikovanych-technickych-prostredku/>.

3.2.1 Trezory

Popisem všech certifikovaných technických prostředků se nebudu zabývat, vybral jsem si jen mechanické zábranné prostředky, blíže bezpečnostní úschovné objekty společnosti T-SAFE. Společnost se prezentuje na internetové adrese www.t-safe.cz.

Společnost T-SAFE s.r.o. vyrábí a dodává nábytkové trezory NT, stěnové trezory ST, skříňové trezory NTD, skříňové trezory AS, bezpečnostní trezorové dveře, skříně k úschově zbraní a střeliva a další výrobky, které jsou k dispozici na internetových stránkách společnosti. Společnost T-SAFE s.r.o. je členem sdružení výrobců trezorů v České republice „CZECH SAFE[44]“. Trezory jsou řazeny do příslušných bezpečnostních tříd a zkoušeny podle normy EN 1143-1[45]. Certifikaci provádí Akreditační orgán č. 3025 pro certifikaci výrobků společnosti TREZOR TEST s.r.o.

a) Nábytkové trezory NT:

- určeny k úschově peněžních hotovostí, šperků, léků, osobních zbraní a podobně.
- vyrábějí se ve 14 základních velikostech, navrženy k ukotvení do nábytku, stěny nebo podlahy.
- trezory jsou osazeny mechanickými zámky firmy MAUER nebo STUP.
- nebo mechanickými kombinačními zámky firem LA GARD, SARGENT & GREENLEAF a NL LOCK.
- můžou být také osazeny elektronickými zámky firem MAUER, LA GARD nebo NL LOCK.
- v mezistěnách korpusu je ohnivzdorná výplň.
- mají certifikaci podle EN 1143-1 pro bezpečnostní třídu I, II.
- certifikát dle ČSN 916012[46] pro bezpečnostní třídu Z3.

---

[44] CZECH SAFE – profesionální sdružení právnických a fyzických osob, které se zabývá výrobou, stavbou a péčí o jakost bezpečnostních úschovných objektů.

[45] EN 1143-1 – Bezpečnostní úschovné objekty – Požadavky, klasifikace a metody zkoušení odolnosti proti vloupání – Část 1: Skříňové trezory, ATM trezory, trezorové dveře a komorové trezory.

[46] ČSN 916012 – Bezpečnostní úschovné objekty – Požadavky, klasifikace a metody zkoušení odolnosti proti vloupání – Trezory se základní bezpečností.

- certifikát NBÚ, který ověřuje způsobilost technického prostředku typu 1C, 3 („Tajné“) a 4 („Přísně tajné“).

Nábytkový trezor NT 13:

- certifikát NBÚ ověřující způsobilost technického prostředku typu 1C, 3 („Tajné“).
- vnější rozměr: výška 305 mm, šířka 435 mm, hloubka 350 mm.
- vnitřní rozměr: výška 200 mm, šířka 330 mm, hloubka 220 mm, objem 15 l.
- hmotnost: bezpečnostní třídy Z3 37 kg a bezpečnostní třídy I 49 kg.

Obr. 15. Nábytkový trezor NT 13.

[zdroj uveden v použité literatuře, zdroj číslo [16]]

b) Skříňové trezory AS:

- určeny zejména pro firmy, úřady, soudy a místa, kde je potřeba mít bezpečně zajištěny doklady, smlouvy a jiné cennosti.
- rozvodový mechanismus v uzamčeném stavu je zajištěn klíčovým trezorovým zámkem, mechanickým kombinačním zámkem nebo elektronickým zámkem.
- certifikát shody ČSN 1143-1 v bezpečnostní třídě 0,I.
- certifikát NBÚ ve stupni utajení „Důvěrné“ a „Tajné“.

Skříňový trezor AS – ASJ 2:

- vnitřní rozdělení umožňuje uložení 3 pořadačů.

- rozvodový mechanismus v uzamčeném stavu je zajištěn klíčovým trezorovým zámkem, mechanickým kombinačním zámkem nebo elektronickým zámkem.
- povrchová barva šedá nebo černá.
- vnější rozměr: výška 1230 mm, šířka 600 mm, hloubka 500 mm.
- vnitřní rozměr: výška 1126 mm, šířka 496 mm, hloubka 382 mm, objem 213 l.
- hmotnost: bezpečnostní třídy 0 161 kg a bezpečnostní třídy I 171 kg.

Obr. 16. Skříňový trezor AS – ASJ 2.

[zdroj uveden v použité literatuře, zdroj číslo [16]]

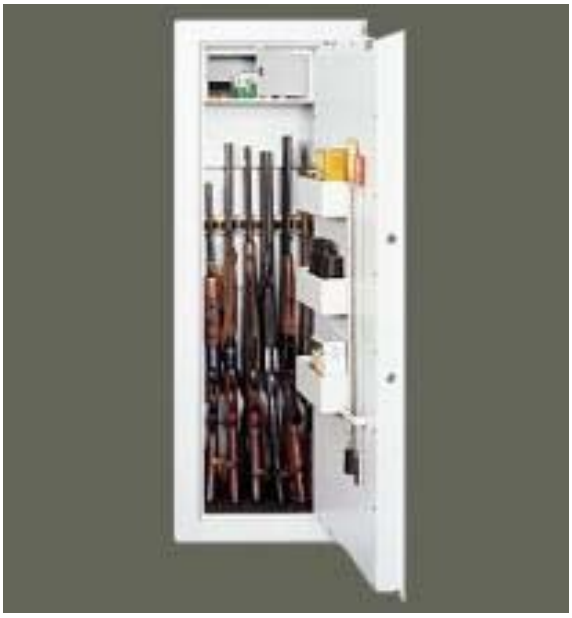
c) Trezory na zbraně TZ:

- jsou určeny k bezpečné úschově loveckých, sportovních a starožitných zbraní.
- vyrábí se ve dvou velikostech TZ 6 pro 3 až 6 zbraní a TZ 10 pro 7 až 10 zbraní.
- trezor je možno rozdělit, tak že část bude sloužit k uložení zbraní a druhá část k uložení cenných předmětů, šperků apod.
- jsou vybaveny uzamykatelnou schránkou na střelivo a hlavně zbraní jsou upevněny speciálními držáky.

- na mezistěnách trezoru je ohnivzdorná výplň – odolá proti slabému požáru.
- vyrábí se v černé a šedobílé barvě.
- certifikát podle EN 1143-1 pro bezpečnostní třídu 0, I.
- certifikát NBÚ ověřující způsobilost technických prostředků typu 2 („Důvěrné“) a 3 („Tajné“).

Trezor na zbraně TZ – TZ 6:

- vnější rozměr: výška 1600 mm, šířka 600 mm, hloubka 500 mm.
- vnitřní rozměr: výška 1496 mm, šířka 496 mm, hloubka 382 mm, objem 248 l.
- hmotnost: bezpečnostní třídy 0 210 kg a bezpečnostní třídy I 220 kg.



Obr. 17. Trezor na zbraně TZ – TZ 6.

[zdroj uveden v použité literatuře, zdroj číslo [16]]

Obr. 18. Archivační skříň AS – AS 10.

[zdroj uveden v použité literatuře, zdroj číslo [16]]

3.3 Certifikace informačního systému

Certifikaci informačního systému upravuje zákon č. 412/2005 Sb. v § 46 a § 48. Dále certifikaci upravuje vyhláška č. 523/2005 Sb.[47]. Orgán státu nebo podnikatel, který bude informační systém provozovat, zažádá písemně NBÚ. Na základě žádosti zpracuje NBÚ seznam náležitostí pro ověření způsobilosti informačního systému a časový harmonogram jejich doložení žadatelem. Žadatel musí k provedení certifikace předložit náležitosti, které jsou uvedeny na následující straně, aby NBÚ mohl provést hodnocení. Při provádění hodnocení NBÚ posuzuje předložené podklady a provede dodatečné testy. NBÚ vykonává dodatečné testy přímo u žadatele v provozním prostředí s účastí žadatele nebo dodavatele informačního systému. Odpovídá-li výsledek hodnocení způsobilosti informačního systému nakládat s utajovanými informacemi, žadatel poté dostane certifikát. Může nastat situace, že informační systém vyhovuje požadavkům jen pro nižší stupeň utajení, potom NBÚ vydá certifikát jen na tento stupeň utajení. V případě nesplnění podmínek NBÚ

[47] Vyhláška č. 523/2005 Sb., O bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.

rozhodne o nevydání certifikátu. Proti rozhodnutí NBÚ, že certifikát informačního systému nebude vydán, není odvolání přípustné. Zákon ukládá povinnost používat jen certifikované informační systémy. NBÚ vede seznam certifikovaných informačních systémů.

Doba platnosti certifikátu je omezena zákonem pro stupeň utajení „Přísně tajné“ a „Tajné“ nejdéle 2 roky, pro stupeň utajení „Důvěrné“ nejdéle na 3 roky a pro stupeň utajení „Vyhrazené“ maximálně 5 let. Platnost certifikátu informačního systému zaniká uplynutím doby jeho platnosti, zánikem platnosti osvědčení podnikatele, zrušením orgánu státu nebo rozhodnutím NBÚ o zániku platnosti certifikátu. NBÚ může rozhodnout o zániku certifikátu v případě, že informační systém přestal být způsobilý k nakládání s utajovanými informacemi. U informačního systému, který bude používán i po uplynutí doby platnosti certifikátu, musí žadatel požádat NBÚ o certifikaci informačního systému. Žádost musí být podána nejméně 6 měsíců před uplynutím doby platnosti původního certifikátu informačního systému. Certifikáty informačních systémů vydané podle zákona č. 148/1998 Sb.[48] se v době jejich platnosti berou jako certifikáty informačních systémů podle současně platného zákona č. 412/2005 Sb. Byla – li certifikace informačního systému zahájena před datumem 1.1. 2006, dokončí se podle zákona č. 412/2005 Sb.

Žádost o certifikaci informačního systému obsahuje:

- „identifikaci žadatele.
- jméno a příjmení kontaktního pracovníka žadatele a kontaktní spojení.
- stručný popis účelu a rozsah informačního systému.
- stupeň utajení utajovaných informací, se kterými bude informační systém nakládat.
- stanovení bezpečnostního provozního módu informačního systému aidentifikaci dodavatele informačního systému nebo jeho komponent ovlivňujících bezpečnost informačního systému.“[49]

---

[48] Zákon č. 148/1998 Sb., O ochraně utajovaných skutečností a o změně některých zákonů, byl nahrazen zákonem č. 412/2005 Sb.

[49] Národní bezpečnostní úřad [online]. 2007- , 16.1.2009 [cit. 2009-03-17]. Dostupný z WWW: <http://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-informacnich-systemu/certifikace-informacnich-systemu/postup-certifikace/>.

Žadatel k provedení certifikace předloží:

- „bezpečnostní politiku informačního systému a výsledky analýzy rizik.
- návrh bezpečnosti informačního systému.
- sada testů bezpečnosti informačního systému, jejich popis a popis výsledků testování.
- bezpečnostní provozní dokumentaci informačního systému.
- popis bezpečnosti vývojového prostředí.
- další podklady nezbytné k certifikaci informačního systému, vyplývající ze specifikace informačního systému.“ [50]

Na stránkách NBÚ je uveden seznam certifikovaných informačních systémů. V seznamu je uveden držitel certifikátu, stupeň utajení a doba platnosti certifikátu. Vzor certifikátu informačního systému je vložen v příloze na konci práce.

3.3.1 Informační systém

U informačních systémů jsem si vybral společnost KOMIX s.r.o., která se zabývá poskytováním řešení informačních systémů a analýzou informačních potřeb podniků. Jedná se o českou společnost založenou v roce 1992.

Společnosti KOMIX s.r.o. vlastní dva certifikované informační systémy podnikatelů. NBÚ vydal dne 15.3. 2006 certifikát pro informační systém podnikatele KOMIX s.r.o., který je určen pro zpracování utajovaných informací stupně utajení „Důvěrné“. Certifikát informačního systému KOMIX platí do 14.3. 2010. Společnost KOMIX se také pyšní certifikovaným informačním systémem stupně utajení „Vyhrazené“. NBÚ vydal tento certifikát 14.4. 2006 a je určen pro zpracování informací stupně utajení „Vyhrazené“. Certifikát informačního systému platí do 30.4. 2010.

---

[50] Národní bezpečnostní úřad [online]. 2007- , 16.1.2009 [cit. 2009-03-17]. Dostupný z WWW: <http://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-informacnich-systemu/certifikace-informacnich-systemu/postup-certifikace/>.

3.4 Certifikace kryptografického prostředku

Certifikace kryptografických prostředků upravuje § 46 a § 49 zákona č. 412/2005 Sb. a podle vyhlášky č. 525/2005 Sb.[51] NBÚ provádí výhradně certifikaci kryptografických prostředků, které budou využívány k ochraně utajovaných informací.

Certifikace kryptografického prostředku začíná podáním žádosti na NBÚ, která musí mít písemnou podobu. Žádá – li podnikatel, musí být držitelem platného osvědčení podnikatele pro přístup k utajované informaci. K provedení certifikace se NBÚ doloží nezbytná dokumentace. NBÚ rozhodne o přijetí žádosti, následně písemně oznámí žadateli postup certifikačního řízení. Odmítne-li NBÚ žádost, není přípustné odvolání a přezkoumání soudem je vyloučeno. Ověří – li NBÚ způsobilost kryptografického prostředku k ochraně utajovaných informací, je vydán certifikát. Platnost certifikátu stanovuje NBÚ na dobu nejdéle 5 let. Platnost certifikátu kryptografického prostředku končí uplynutím doby platnosti certifikátu nebo rozhodnutím NBÚ o zániku platnosti.

NBÚ stanoví požadavky na systémy tvořící kryptografickou ochranu utajovaných informací. Měly by se výhradně používat kryptografické prostředky, které mají kryptografické algoritmy v souladu s bezpečnostními standardy, které NBÚ schválil nebo vyvinul.

Podle odstavce 2 § 37 zákona č. 412/2005 Sb. je kryptografický prostředek: „utajovaný technický prostředek nebo softwarový produkt používaný ke kryptografické ochraně nebo prostředek nebo zařízení používané k výrobě nebo testování klíčového materiálu.“

Žádost o certifikaci kryptografického prostředku podle vyhlášky č. 525/2005 Sb. obsahuje:

- „identifikace žadatele:
    - obchodní firmou, popřípadě názvem, sídlem a identifikačním číslem, je-li žadatelem právnická osoba.
    - obchodní firmou, popřípadě jménem a příjmením, případě odlišujícím dodatkem, trvalým pobytem a místem podnikání, liší-li se od trvalého

[51] Vyhláška č. 525/2005 Sb., O provádění certifikace při zabezpečení kryptografické ochrany utajovaných informací.

pobytu, datem narození a identifikačním číslem, je-li žadatelem fyzická osoba, která je podnikatelem, nebo

- názvem, sídlem, identifikačním číslem a jménem a příjmením odpovědné osoby, jde-li o orgán státu,

- jméno a příjmení kontaktního zaměstnance žadatele a kontaktní spojení na něj,
- číslo platného osvědčení podnikatele a stupeň utajení utajované informace, pro přístup k níž osvědčení podnikatele opravňuje, je-li žadatelem podnikatel,
- obchodní název a úplné typové označení kryptografického prostředku,
- určení kryptografického prostředku (účel užití a stupeň utajení, pro který má být kryptografický prostředek používán),
- obchodní firmu, sídlo či místo podnikání výrobce kryptografického prostředku,
- způsob zajištění výroby a distribuce klíčového materiálu.“ [52]

Pro provedení certifikace kryptografického prostředku je zejména požadována dokumentace obsahující:

- „určení a vymezení způsobu použití kryptografického prostředku,
- typ uživatelského prostředí a systémové začlenění kryptografického prostředku,
- technický popis a návod k obsluze kryptografického prostředku,
- požadavky na instalaci a testování kryptografického prostředku,
- platná osvědčení kryptografického prostředku nebo již vydané certifikáty,
- popis řešení a struktury použitých kryptografických klíčů,
- blokové schéma a popis kryptografického prostředku s vyznačením součinnostních vazeb jednotlivých jeho částí.“[53]

---

[52] § 1, odstavec 1, vyhlášky č. 525/2005 Sb., O provádění certifikace při zabezpečení kryptografické ochrany utajovaných informací.

[53] § 5, odstavec 3, vyhlášky č. 525/2005 Sb., O provádění certifikace při zabezpečení kryptografické ochrany utajovaných informací.

3.5 Certifikace kryptografického pracoviště

Certifikaci kryptografického prostředku upravuje § 46 a § 50 zákona č. 412/2005 Sb. a vyhláška č. 525/2005 Sb. Certifikace kryptografických pracovišť je prováděna ve správním řízení.

Žádost o certifikaci kryptografického pracoviště se podává písemně na NBÚ podle § 50 zákona č. 412/2005 Sb. Náležitosti žádosti upravuje § 2 vyhlášky č. 525/2005 Sb.

K žádosti o certifikaci kryptografického pracoviště se přikládá:

- „dokumentace zabezpečení fyzické bezpečnosti kryptografického pracoviště, v rozsahu stanoveném ve zvláštním právním předpisu[54]),
- dokumentace provozně-bezpečnostního zabezpečení kryptografického pracoviště,
- prohlášení odpovědné osoby nebo jí pověřené osoby o splnění požadavků na fyzickou a personální bezpečnost kryptografického pracoviště.“[55]

Žádost a přiložená dokumentace se zasílá na adresu NBÚ odboru informačních technologií.

Žádost o certifikaci kryptografického pracoviště obsahuje:

- „identifikaci žadatele,
- jméno a příjmení kontaktního zaměstnance žadatele a kontaktní spojení na něj,
- číslo platného osvědčení podnikatele a stupeň utajení utajované informace, pro přístup k níž osvědčení podnikatele opravňuje, je-li žadatelem podnikatel,
- identifikaci kryptografického pracoviště (název, adresa a umístění),
- určení kryptografického pracoviště (účel, užití),
- seznam přikládané dokumentace nezbytné k provedení certifikace kryptografického pracoviště.“[56]

---

[54] Vyhláška č. 528/2005 Sb., O fyzické bezpečnosti a certifikaci technických prostředků.
[55] § 6, odstavec 1, vyhlášky č. 525/2005 Sb., O provádění certifikace při zabezpečení kryptografické ochrany utajovaných informací.
[56] § 2, vyhlášky č. 525/2005 Sb., O provádění certifikace při zabezpečení kryptografické ochrany utajovaných informací.

NBÚ po vyhodnocení žádosti kontaktuje písemně žadatele o podmínkách a postupu certifikace kryptografického pracoviště. Po ověření způsobilosti vydá NBÚ certifikát kryptografického pracoviště. Vzor certifikátu kryptografického pracoviště mám vložen v příloze práce. Na certifikátu je vyznačena kategorie kryptografického pracoviště, pro kterou je pracoviště certifikováno. Certifikát také obsahuje rozsah a popis činností, které je na pracovišti možno provádět.

Kategorie kryptografického prostředku vyjadřuje splnění stanovených minimálních požadavků na fyzickou, personální a administrativní bezpečnost kryptografického pracoviště. Při splnění požadavků je možné na pracovišti manipulovat a zpracovávat kryptografický materiál daného stupně utajení.

Kryptografické pracoviště se dělí na 8 kategorií. Přehled rozdělení je uveden v tabulce:

<table>
<tr><th rowspan="2">Kategorie kryptografického pracoviště</th><th rowspan="2">Maximální stupeň utajení KM</th><th rowspan="2">Minimální požadavek na zabezpečení oblasti: kategorie/třída</th><th colspan="2">Personální požadavky</th><th rowspan="2">Administrativní požadavky</th></tr>
<tr><th>Pracovník kryptografické ochrany, držitel osvědčení fyzické osoby pro stupeň</th><th>Oprávněnost seznamování se s veškerým KM na kryptografickém pracovišti</th></tr>
<tr><td>V/I</td><td rowspan="2">„Vyhrazené KRYPTO“</td><td>„Vyhrazené“/I</td><td rowspan="2">„Důvěrné“</td><td>Ano</td><td rowspan="8">Požadavky administrativní bezpečnosti pro manipulaci s KM</td></tr>
<tr><td>V/II</td><td>„Vyhrazené“/II</td><td>Ne</td></tr>
<tr><td>D/I</td><td rowspan="2">„Důvěrné KRYPTO“</td><td>„Důvěrné“/I</td><td rowspan="2">„Důvěrné“</td><td>Ano</td></tr>
<tr><td>D/II</td><td>„Důvěrné“/II</td><td>Ne</td></tr>
<tr><td>T/I</td><td rowspan="2">„Tajné KRYPTO“</td><td>„Tajné“/I</td><td rowspan="2">„Tajné“</td><td>Ano</td></tr>
<tr><td>T/II</td><td>„Tajné“/II</td><td>Ne</td></tr>
<tr><td>PT/I</td><td rowspan="2">„Přísně tajné KRYPTO“</td><td>„ Přísně tajné“/I</td><td rowspan="2">„Přísně tajné“</td><td>Ano</td></tr>
<tr><td>PT/II</td><td>„ Přísně tajné“/II</td><td>Ne</td></tr>
</table>

Tab. 2. Specifikace kategorií kryptografických pracovišť.

[zdroj uveden v použité literatuře, zdroj číslo [17]]

3.6 Certifikace stínící komory

Stínící komora se používá k ochraně utajovaných informací před jejich únikem kompromitujícím elektromagnetickým vyzařováním. Certifikaci stínící komory upravuje § 46 a § 51 zákona č. 412/2005 Sb. Stínící komory pro ochranu utajovaných informací musí být certifikovány NBÚ nebo příslušným orgánem. O certifikaci stínící komory se písemně žádá NBÚ. Dobu platnosti certifikátu stanovuje NBÚ, nejdéle však na dobu 5 let.

Žádost o certifikaci stínící komory obsahuje:

- „identifikace žadatele,
- jméno a příjmení kontaktního pracovníka žadatele a kontaktní spojení,
- stupeň a číslo osvědčení podnikatele (je-li žadatelem podnikatel),
- označení a umístění stínící komory,
- identifikaci výrobce stínící komory.“[57]

Certifikace stínící komory se provádí způsobem založeným na měření útlumových vlastností stínící komory a jejich porovnání s bezpečnostními standardy. Je-li stínící komora způsobilá k ochraně utajovaných informací, vydává NBÚ certifikát stínící komory.

Certifikační zpráva stínící komory obsahuje:

- „orientační popis stínící komory, jejího umístění a účelu používání,
- podmínky provozu stínící komory,
- typy změn, které vyžadují provedení opakované certifikace stínící komory.“[58]

---

[57] § 33, odstavec 1, vyhlášky č. 523/2005 Sb., O bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.

[58] § 35, vyhlášky č. 523/2005 Sb., O bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor.

4 BEZPEČNOSTNÍ SPOLEHLIVOST

Bezpečnostní spolehlivost upravuje § 14 a § 18 zákona č. 412/2005 Sb. Pro vydání osvědčení fyzické osoby musí být fyzická osoba bezpečnostně spolehlivá. Totéž platí u osvědčení podnikatele. Bezpečnostní spolehlivost splňuje osoba, u které není zjištěno bezpečnostní riziko. Bezpečnostní spolehlivost musí splňovat také podnikatel, kdyby ji jako jednu ze základních podmínek nesplňoval, nebude mu vydáno osvědčení podnikatele.

Bezpečnostním rizikem je podle odstavce 2 § 14 zákona č. 412/2005 Sb.:

- „závažná nebo opakovaná činnost proti zájmům České republiky, nebo
- činnost, spočívající v potlačování základních práv a svobod, anebo podpora takové činnosti.“

Bezpečnostní spolehlivost patří do personální bezpečnosti a představuje základní požadavek k přístupu k utajovaným informacím. Společnost si musí ověřit u zaměstnance, který žádá o osvědčení fyzické osoby, zda je bezpečnostně spolehlivý. Podmínkou je, zda u osoby není zjištěno bezpečnostní riziko, které jsem citoval výše. Podmínky bezpečnostní spolehlivosti se u fyzické osoby a podnikatele liší. Za bezpečnostní rizika fyzické osoby lze též považovat podle odstavce 3 § 14 zákona č. 412/2005 Sb.:

a) „zařazení do složky bývalé Státní bezpečnosti s rozvědným nebo kontrarozvědným zaměřením, zpravodajské správy Generálního štábu Československé lidové armády nebo odboru vnitřní ochrany Sboru nápravné výchovy anebo prokazatelnou spolupráci s bývalou Státní bezpečností nebo zpravodajskou správou Generálního štábu Československé lidové armády nebo odborem vnitřní ochrany Sboru nápravné výchovy,

b) užívání jiné identity,

c) úmyslné porušení právních předpisů, na jehož základě může nastat újma zájmu České republiky,

d) chování, které má vliv na důvěryhodnost nebo ovlivnitelnost osoby a může ovlivnit její schopnost utajovat informace,

e) styky s osobou, která vyvíjí nebo vyvíjela činnost proti zájmu České republiky,

f) pravomocné odsouzení pro trestný čin,

g) uvedení nepravdivé informace nebo zamlčení informace rozhodné pro objektivní zjištění skutečného stavu věci v řízení podle části čtvrté nebo nenahlášení změny údajů uvedených v příloze k této žádosti o vydání osvědčení fyzické osoby (§ 94) nebo v jiném materiálu poskytnutém Úřadu v příloze k této žádosti,

h) porušení povinnosti při ochraně utajovaných informací, nebo

i) zřejmě nepřiměřené finanční nebo majetkové poměry vzhledem k řádně přiznaným příjmům fyzické osoby.“

Na základě úspěšného bezpečnostního řízení vydá NBÚ osvědčení podnikatele. Poté může společnost nakládat s utajovanými informacemi daného stupně ve smyslu zákona č. 412/2005 Sb. Společnost získáním osvědčení podnikatele představuje pro zákazníky záruku, že s utajovanými informacemi bude zacházeno způsobem přesně stanoveným podle zákona č. 412/2005 Sb. a příslušnými prováděcími vyhláškami. Osvědčení podnikatele má i mezinárodní uznání, což představuje i spolupráci se zahraničními partnery.

Získané osvědčení podnikatele otevírá firmám větší možnosti uplatnění, jak na domácím trhu, tak na mezinárodním. Osvědčení umožňuje společnostem účastnit se veřejných soutěží, které vyhlašují subjekty státní správy. Patří sem oblasti informačních technologií spojených s přístupem k utajovaným informacím, poskytování služeb v objektech se zvláštním režimem vstupu.

Bezpečnostní spolehlivost nesplňuje podnikatel, u kterého bylo zjištěno bezpečnostní riziko. Bezpečnostní spolehlivost je jednou z podmínek pro vydání osvědčení podnikatele.

Podle odstavce 2 § 18 zákona č. 412/2005 Sb. „Bezpečnostním rizikem je činnost statutárního orgánu nebo jeho člena, člena kontrolního orgánu nebo prokuristy proti zájmům České republiky.“

Za bezpečnostní riziko lze též podle odstavce 3 § 18 zákona č. 412/2005 Sb. považovat:

a) „uvedení nepravdivé informace nebo zamlčení informace rozhodné pro objektivní a úplné zjištění skutečného stavu věci při ověřování podmínek pro vydání osvědčení podnikatele nebo nenahlášení změny údajů uvedených v žádosti podle § 96 nebo v jiném materiálu poskytnutém Úřadu k této žádosti,

b) kapitálové, finanční nebo obchodní vztahy k jiným fyzickým nebo právnickým osobám anebo k cizí moci, které vyvíjejí nebo vyvíjely činnost proti zájmům České republiky,

c) personální nestabilitu ve statutárním nebo v kontrolním orgánu nebo v osobách prokuristů,

d) je-li podnikatel akciovou společností s jinou formou akcií, než jsou akcie znějící na jméno,

e) je-li společníkem, který má rozhodující vliv na volbu nebo jmenování statutárního nebo kontrolního orgánu podnikatele, akciová společnost s jinou formou akcií, než jsou akcie znějící na jméno,

f) porušení povinnosti při ochraně utajovaných informací,

g) pravomocné odsouzení fyzické osoby, která je společníkem podnikatele, pro úmyslný trestný čin,

h) úmyslné porušení právních předpisů osobami oprávněnými jménem podnikatele nebo za podnikatele jednat, na jehož základě může nastat újma zájmu České republiky, nebo

i) vztah cizího státního příslušníka zaměstnaného podnikatelem k fyzickým osobám nebo právnickým osobám nebo k cizí moci, které vyvíjely nebo vyvíjejí činnost proti zájmům České republiky.“

ZÁVĚR

Organizace, které nakládají s utajovanými informacemi, musí dodržovat bezpečnostní politiku zaměřenou na ochranu utajovaných informací. Tato politika v sobě obsahuje především politiku personální bezpečnosti, politiku administrativní bezpečnosti, politiku fyzické bezpečnosti, politiku bezpečnosti informačních systémů a politiku kryptografické ochrany. Zmíněnou problematiku upravuje zákon č. 412/2005 Sb., zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti a další související právní předpisy. K dosažení bezpečnosti je nutné dodržovat všechny zmíněné politiky, nestačí mít jednu na vysoké úrovni a druhou vypustit. Budování bezpečnostní politiky vyžaduje seznámit pracovníky společnosti se všemi pravidly, nařízeními, a také definování jejich role v práci s utajovanými informacemi. Organizace si musí uvědomit, jaká rizika hrozí, a vynaložit veškeré dostupné prostředky na vybudování bezpečnostní politiky.

Politika kryptografické bezpečnosti v sobě zahrnuje, jak nakládat s kryptografickým materiálem. To znamená především jeho ochranu, manipulaci, uložení a šifrování. Důležité je neopomenout používání správných šifrovacích programů, hashovacích funkcí a dalších softwarů z oblasti ochrany informací. Kryptografický software a algoritmy vyžadují odbornou instalaci a bezpečné používání. Proto je důležité, aby tuto práci vykonávali specialisté přes informační technologii zaměřenou na datovou bezpečnost.

Nezbytným pravidlem je, aby všechny prostředky, které nakládají s utajovanými informacemi, byly certifikovány. Způsob provádění a postup certifikace stanovuje zákon č. 412/2005 Sb. a další právní předpisy (vyhlášky NBÚ). Certifikace je prováděna Národním bezpečnostním úřadem a pověřenými orgány.

Myslím si, že problematice ochrany utajovaných informací je v poslední době věnována velká pozornost. Státní orgány a soukromé organizace nepodceňují otázku ochrany informací. Nejdůležitější, a zároveň nejrizikovější skupinou, je bezpečnost informačních systémů, komunikačních systémů a s ní související kryptografická ochrana. Většina informací se posílá mezi sítěmi, mnohdy jde o informace tajné, u kterých vyžaduje přenos zvláštní opatření. Neustále vznikají nové programy, algoritmy a způsoby, jak zamezit úniku informací. Nezahálí ovšem ani protivníci, kteří využívají v mnoha případech nezákonné prostředky k získání tajných informací. Jde o různé odposlechy, získání osobních údajů, přístup do cizích počítačů a falešnou identitu.

ZÁVĚR V ANGLIČTINĚ

Organisations which dispose of secret information must observe the security policy focused on protection of secret information. This policy contains mainly policy of personal protection, policy of administrative protection, policy of physical protection, policy of information system and policy of cryptography protection. The mentioned problems are regularized by č.412/2005 Sb., law of secret information protection and of security competence and other related legal enactments. It's necessary to observe all the mentioned policies in order to reach the security. It's not enough to have one high-level policy and don't think about the others. Building the security policy demands to acquaint workers of company with all the rules, prescripts and to define their roles at work with secret information. Organisations must perceive which risks menace and expand all the instruments for building the security policy.

The policy of cryptography security contains how to dispose of cryptography material. This means mainly protection, manipulation, storage and encryption. It's important not to forget usage of right encryption programmes, hash functions and other softwares from information save area. Cryptography software and algorithms require a technical installation and safe usage. That's why it's important this work would be accomplished by information technology specialists focused on data security.

A necessary rule is that all the instruments, which dispose of secret information, would be certificated. The method of implementation and process of certification determines a law č. 412/2005 Sb., and other legal enactments (by NBÚ public notice). The certification is provided by National security office and comissioned authorities.

I think a big attention has been devoted to problems of secret information protection recently. State bodies and private organisations don't underestimate the question of information security. The most important and also the high-risk group is the security of information systems, communication systems and related cryptography security. Most of information is sent between networks. Many times it may be the secret information where transmission demand a special precaution. The new programmes, algorithms and methods how to prevent information leak are engendering constantly. Not even adversaries dawdle. They are exploiting illegal instruments to get the secret information. That could be various tappings, foreign computer access and false identity.

SEZNAM POUŽITÉ LITERATURY

[1] JANEČEK, Jiří. Válka šifer : Výhry a prohry československé vojenské rozvědky (1939-1945). Olomouc : Votobia, 2001. 345 s. ISBN 80-7198-505-8.

[2] MUSIL, Rudolf. Ochrana utajovaných skutečností. 1. vyd. Praha : Eurounion, 2001. 379 s. ISBN 80-85858-93-2.

[3] KUCHAŘ, Miloš. Bezpečná síť : Jak zajistíte bezpečnost vaší sítě. 1. vyd. Praha : Grada publishing, 1999. 92 s. ISBN 80-7169-886-5.

[4] Zákon číslo 412/2005 Sb. O ochraně utajovaných informací a bezpečnostní spolehlivosti.

[5] Národní bezpečnostní úřad [online]. 2007- , 16.1.2009 [cit. 2009-02-20]. Dostupný z WWW: <www.nbu.cz>.

[6] *Wikipedie : Otevřená encyklopedie* [online]. 2001 , 6.1.2009 [cit. 2009-01-20]. Dostupný z WWW: <www.cs.wikipedia.org/>.

[7] Vyhláška číslo 524/2005 Sb., O zajištění kryptografické ochrany utajovaných informací.

[8] Vyhláška číslo 529/2005 Sb., O administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb.

[9] Vyhláška číslo 523/2005 Sb., O bezpečnosti informačních systémů a certifikací stínících komor.

[10] Vyhláška číslo 528/2005 Sb., O fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.

[11] PIPER, Fred, MURPHY, Sean. *Kryptografie : Průvodce pro každého*. Pavel Mondschein. 1. vyd. Praha : Dokořán, 2006. 157 s. ISBN 80-7363-074-5.

[12] Národní bezpečnostní úřad [online]. 2007- , 16.1.2009 [cit. 2009-02-27]. Dostupný z WWW: <http://www.nbu.cz/cs/o-nas/organizacni-schema/ >.

[13] FOLTÝNEK, T., PŘICHYSTAL, J.. *Mendelova zemědělská a lesnická univerzita v Brně : Komprimace a šifrování* [online]. 2008 [cit. 2009-02-23]. Dostupný z WWW: <https://is.mendelu.cz/eknihovna/opory/index.pl?cast=7022>.

[14] PAUKERTOVÁ, Veronika. *Ikaros : Elektronická informační kriminalita* [online]. 2006 [cit. 2009-03-04]. Dostupný z WWW: <http://www.ikaros.cz/node/3554>.

[15] JAŠEK, Roman. *Studijní materiály : Datová bezpečnost.* Pro zimní semestr 2008.

[16] *T-SAFE, s.r.o. : Největší výrobce sejfů, trezorů a bezpečnostních skříní v České republice* [online]. 2008 [cit. 2009-03-11]. Dostupný z WWW: <http://www.t-safe.cz/>.

[17] *Věstník Národního bezpečnostního úřadu č. 2/2008.* Národní bezpečnostní úřad . 2008- . Praha : ISSN 1212-7086.

[18] PARMA, Antonín. *KOMIX s.r.o.* [online]. 2005 [cit. 2009-03-09]. Dostupný z WWW: <http://www.komix.cz/>.

[19] Vyhláška číslo 525/2005 Sb., O provádění certifikace při zabezpečení kryptografické ochrany utajovaných informací.

[20] Bezpečnostní informační služba : vnitřní zpravodajská služba České republiky [online]. 2008 [cit. 2009-03-12]. Dostupný z WWW: <http://www.bis.cz/index.html>.

[21] Virklis, a.s. [online]. 2007 [cit. 2009-03-15]. Dostupný z WWW: <http://www.virklis.cz/>.

[22] LAUCKÝ, Vladimír. *Speciální bezpečnostní technologie*. 1. vyd. Zlín : [s.n.], 2009. 223 s. ISBN 978-80-7318-762-0.

[23] *Agentura.RU* [online]. 2008 [cit. 2009-04-18]. Dostupný z WWW: <http://www.agentura.ru/>.

[24] *Specialista.info* [online]. 2005 [cit. 2009-04-18]. Dostupný z WWW: <http://www.specialista.info/>. ISSN 1801-4739.

[25] *National Security Agency* [online]. 2008 [cit. 2009-04-20]. Dostupný z WWW: <http://www.nsa.gov/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

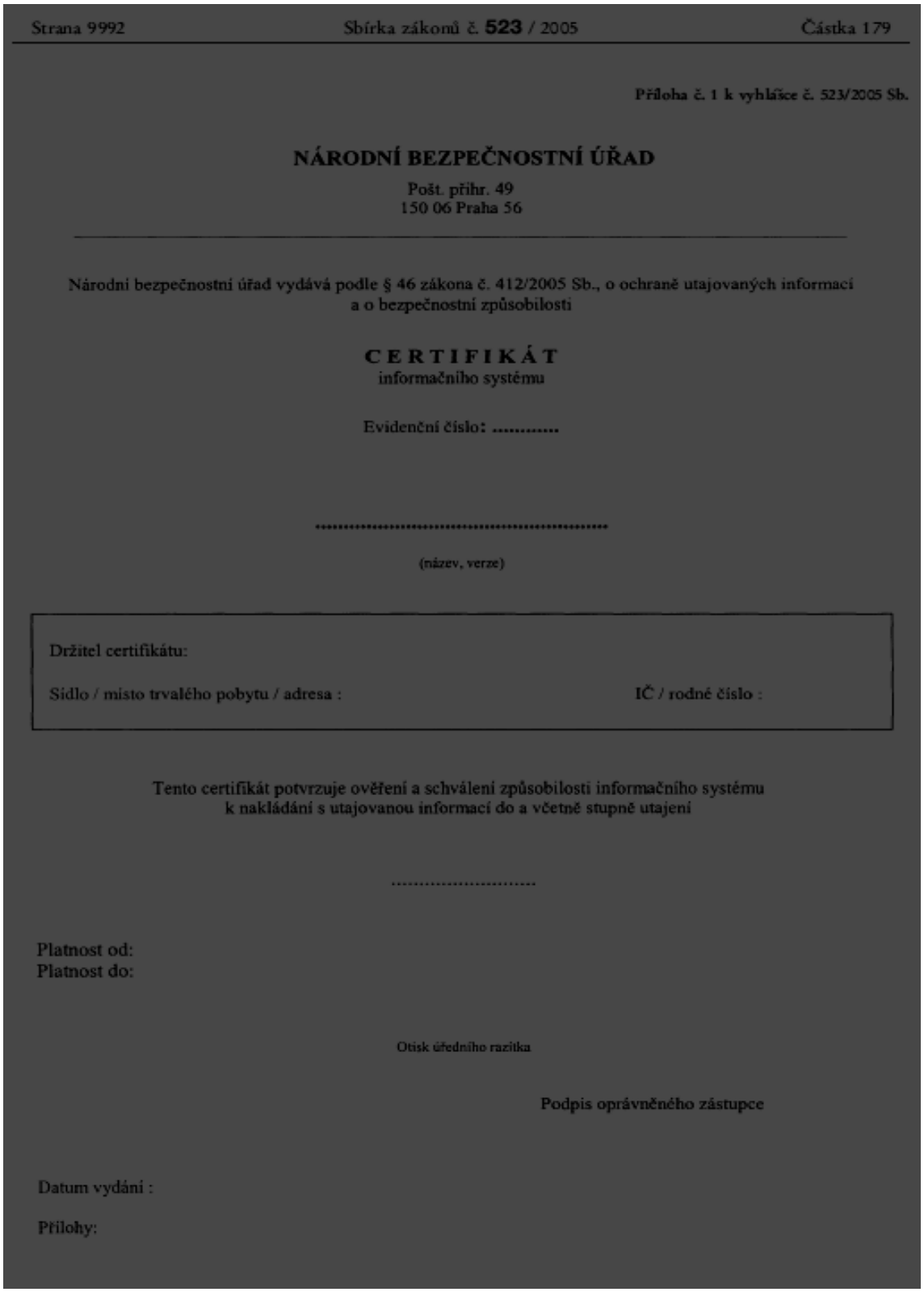
ČR	Česká republika.
NBÚ	Národní bezpečnostní úřad.
ad.	A další.
popř.	Popřípadě.
resp.	Respektive.
EU	Evropská unie.
IS	Informační systém.
NATO	Organizace Severoatlantické smlouvy.
HDD	Pevný disk.
DVD	Zapisovatelné médium.
č.	Číslo.
PKB	Průmysl komerční bezpečnosti.
př. n. l.	Před naším letopočtem.
RAM	Random access memory.
tzv.	Tak zvaný.
GSM	Groupe Spécial Mobile - Globální Systém pro Mobilní komunikaci.
ISDN	Integrated Services Digital Network - Digitální síť integrovaných služeb.
BIS	Bezpečnostní informační služba.
KM	Kryptografický materiál.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: CERTIFIKÁT INFORMAČNÍHO SYSTÉMU



Strana 9992 Sbírka zákonů č. 523 / 2005 Částka 179

Příloha č. 1 k vyhlášce č. 523/2005 Sb.

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: .....

.....

(název, verze)

Držitel certifikátu:

Sídlo / místo trvalého pobytu / adresa : IČ / rodné číslo :

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

.....

Platnost od:
Platnost do:

Otisk úředního razítka

Podpis oprávněného zástupce

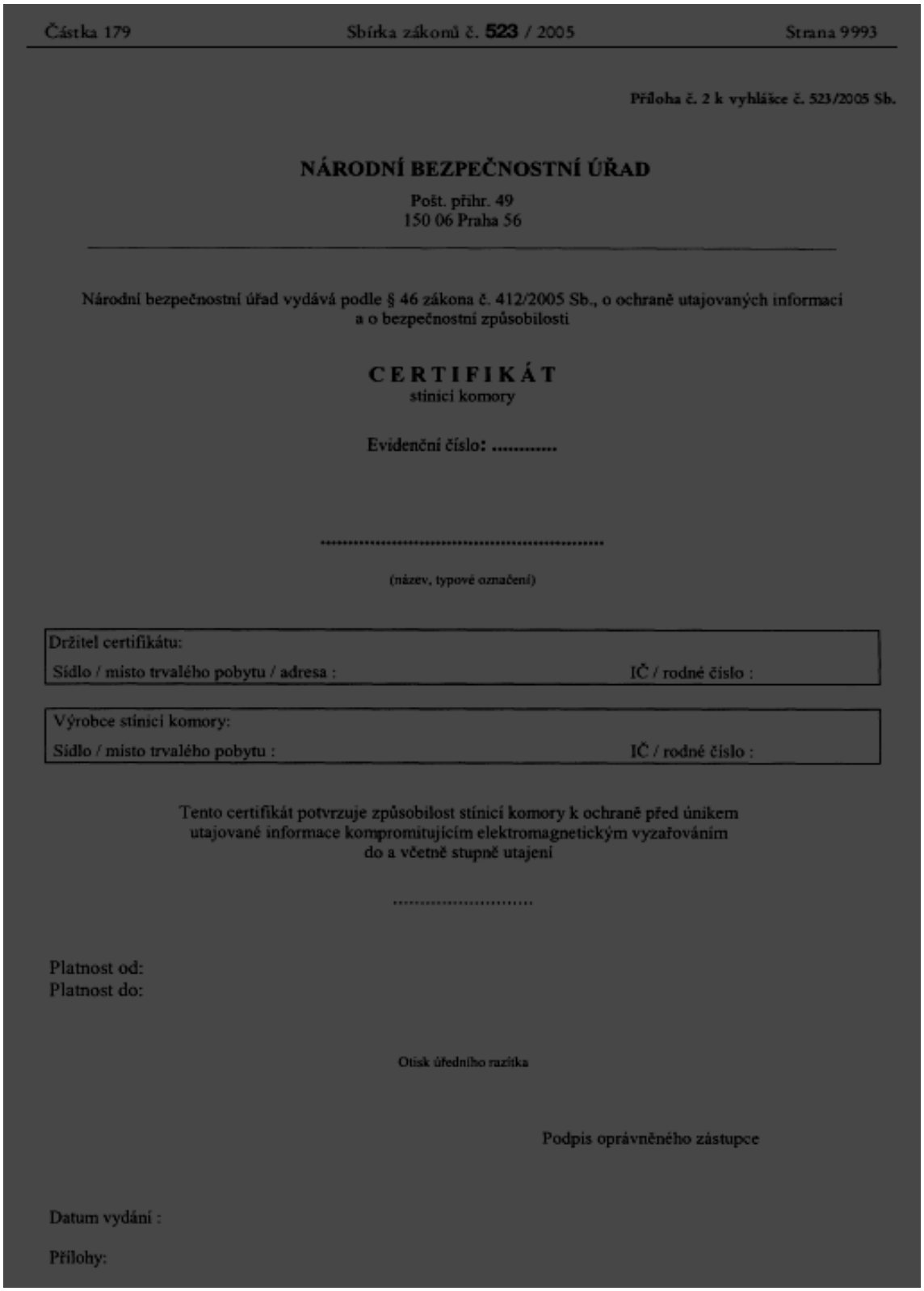
Datum vydání :

Přílohy:

Příloha 1. Certifikát informačního systému, příloha k vyhlášce č. 523/2005 Sb.

[převzato ze zdroje [5]]

PŘÍLOHA P II: CERTIFIKÁT STÍNÍCÍ KOMORY



Částka 179 Sbírka zákonů č. **523** / 2005 Strana 9993

Příloha č. 2 k vyhlášce č. 523/2005 Sb.

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
stínicí komory

Evidenční číslo: .....

.....

(název, typové označení)

Držitel certifikátu:
Sídlo / místo trvalého pobytu / adresa : IČ / rodné číslo :

Výrobce stínicí komory:
Sídlo / místo trvalého pobytu : IČ / rodné číslo :

Tento certifikát potvrzuje způsobilost stínicí komory k ochraně před únikem utajované informace kompromitujícím elektromagnetickým vyzařováním do a včetně stupně utajení

.....

Platnost od:
Platnost do:

Otisk úředního razítka

Podpis oprávněného zástupce

Datum vydání :

Přílohy:

Příloha 2. Certifikát stínící komory, příloha k vyhlášce č. 523/2005 Sb.

[převzato ze zdroje [5]]

PŘÍLOHA P III: CERTIFIKÁT TECHNICKÉHO PROSTŘEDKU

Částka 179 Sbírka zákonů č. 528 / 2005 Strana 10115

Příloha č. 2 k vyhlášce č. 528/2005 Sb.

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
technického prostředku

Evidenční číslo: .....

.....
(Název a typové označení technického prostředku)

Výrobce:
Sídlo/trvalý pobyt/ místo podnikání/adresa: IČ/ rodné číslo
Držitel:
Sídlo/trvalý pobytu/místo podnikání/adresa: IČ/ rodné číslo:

Tento certifikát potvrzuje ověření způsobilosti technického prostředku typu:

.....

Bodové hodnocení technického prostředku podle přílohy č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků:

.....

Platnost certifikátu do:
Datum vydání certifikátu:

Otisk úředního razítka

Podpis oprávněného zástupce

Přílohy:
(Příloha je nedílnou součástí certifikátu a lze je reprodukovat pouze společně)

Příloha 3. Certifikát technického prostředku, příloha k vyhlášce č. 528/2005 Sb.

[převzato ze zdroje [5]]

PŘÍLOHA P IV: CERTIFIKÁT KRYPTOGRAFICKÉHO PROSTŘEDKU

Částka 179 Sbírka zákonů č. 525 / 2005 Strana 10013

Příloha č. 1 k vyhlášce č. 525/2005 Sb.

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

kryptografického prostředku

Evidenční číslo: .....

.....
(název, typové označení kryptografického prostředku)

Identifikace držitele certifikátu

Obchodní firma /jméno a příjmení/název orgánu státu:
IČ:
Sídlo/trvalý pobyt/místo podnikání:

Identifikace výrobce kryptografického prostředku

Obchodní firma /název orgánu státu:
IČ:
Sídlo/trvalý pobyt/ místo podnikání:

kterým se potvrzuje způsobilost kryptografického prostředku pro ochranu utajovaných informací do a včetně stupně utajení

.....

Platnost certifikátu od:

Platnost certifikátu do:

Datum vydání certifikátu:

Otisk úředního razítka

Přílohy: (např. certifikační zpráva)

Podpis oprávněného zástupce

Příloha 4. Certifikát kryptografického prostředku, příloha k vyhlášce č. 525/2005 Sb.

[převzato ze zdroje [5]]

PŘÍLOHA V: CERTIFIKÁT KRYPTOGRAFICKÉHO PRACOVIŠTĚ

Strana 10014 Sbírka zákonů č. 525 / 2005 Částka 179

Příloha č. 2 k vyhlášce č. 525/2005 Sb.

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

kryptografického pracoviště

Evidenční číslo: .....

.....
(označení kryptografického pracoviště)

Identifikace držitele certifikátu:

Obchodní firma/jméno a příjmení /název orgánu státu:

IČ:

Sídlo/trvalý pobyt/místo podnikání:

Identifikace kryptografického pracoviště:

Specifikace (umístění, kategorie):

kterým se potvrzuje způsobilost kryptografického pracoviště k provádění činností kryptografické ochrany v rozsahu

.....
(specifikace vykonávaných činností)

Platnost certifikátu od:

Platnost certifikátu do:

Datum vydání certifikátu:

Otisk úředního razítka

Přílohy: (např. certifikační zpráva)

Podpis oprávněného zástupce

Příloha 5. Certifikát kryptografického pracoviště, příloha k vyhlášce č. 525/2005 Sb.

[převzato ze zdroje [5]]